РЕФЕРАТ

Пояснювальна записка: 118с., 29 рис., 5 табл., 4 додатки., 20 джерел.

Об’єкт дослідження: система бездротової передачі інформації.

Предмет дослідження: децентралізована АСКОЕ звикористанням технології блокчейн.

Мета дипломної роботи: проведення модернізації систем енергопостачання об’єктів комунального сектору, як елементу масштабної адаптованої системи Smart Grid

В першому розділі проаналізовано сучасні ринкові потреби у сфері господарювання та шляхи їх вирішення. Були розглянуті причини створення АСКОЕ та використання для її модифікації криптовалюти ІОТА.

В спеціальній частині розглянуті причини та переваги використання технології ZigBee для вирішення поставленої проблеми, запропоновані конкретні продукти та вирішення питання децентралізації за допомогою криптовалюти ІОТА.

В економічній частині проведений розрахунок капітальних витрат при розробці та введення в експлуатацію автоматизованної децентралізованої системи моніторингу енергоносіїв з використанням технології блокчейн.

Наукова новизна полягає у модернізації існуючих систем моніторингу енергоносіїв заради уникнення хищення енергоресурсів та підвищенні якості послуг, які надають енерговиробники.

ЕНЕРГОНОСІЇ, СИСТЕМИ МОНІТОРИНГУ, ДЕЦЕНТРАЛІЗАЦІЯ, АВТОМАТИЗАЦІЯ, бЛОКЧЕЙН

РЕФЕРАТ

Пояснительная записка: 118с., 29 рис., 5 табл., 4 приложения., 20 источников.

Объект исследования: система беспроводной передачи информации.

Предмет исследования: децентрализованная АСКУЭ с использованием технологии блокчейн.

Цель дипломной работы: проведение модернизации систем энергоснабжения объектов коммунального сектораКак элемента масштабной адаптированной системы Smart Grid

В первой главе проанализированы современные рыночные потребности в сфере хозяйствования и пути их решения. Были рассмотрены причины создания АСКУЭ и использования для ее модификации криптовалюты IOTA.

В специальной части рассмотрены причины и преимущества использования технологии ZigBee для решения поставленной проблемы, предложены конкретные продукты и решения вопроса децентрализации с помощью криптовалюты IOTA.

В экономической части произведен расчет капитальных затрат при разработке и введении в эксплуатацию автоматизированной децентрализованной системы мониторинга энергоносителей с использованием технологии блокчейн.

Научная новизна заключается в модернизации систем мониторинга энергоносителей во избежание хищення энергоресурсов и повышении качества услуг, оказываемых энергопроизводители.

ЭНЕРГОНОСИТЕЛИ, СИСТЕМЫ МОНИТОРИНГА, ДЕЦЕНТРАЛИЗАЦИЯ, АВТОМАТИЗАЦИЯ, БЛОКЧЕЙН

ABSTRACT

Explanatory note: 118p., 29 fig., 5 tab., 4 apps., 20 sources.

The object of the research: wireless systems.

Purpose of the study: decentralized automated electricity metering system using blokchain technology.

The aim of the thesis: modernization of energy objects utilities sector, As part of a large-scale system adapted Smart Grid

The first section analyzes the current market needs for management and solutions. Were considered reasons for the creation and use automated electricity metering system for its modification cryptocurrency IOTA.

As a special part discussed the reasons and advantages of ZigBee technology to solve the problem, suggested specific products and the issue of decentralization using cryptocurrency IOTA.

In the economical part the capital expenditure in developing and commissioning of decentralized automated electricity metering system using technology blokcheyn was calculated.

Scientific novelty lies in the modernization of existing energy monitoring systems for avoiding energy epyaei and improving the quality of services provided by power producers.

ENERGY, MONITORING SYSTEM, DECENTRALIZATION, AUTOMATION, BLOKCHAIN

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АСКОЕ — автоматизовані системи контролю та обліку енергоресурсів;

БСМ — бездротова система моніторингу;

ДД — дистанційний дисплей;

МБО — модуля будинкового обліку;

МКЗ — маршрутизатор каналів зв'язку;

ПО — прилад обліку;

ППП — проміжний приємо-передаючий пристрій;

ПППм — мобільний проміжний приємо-передаючий пристрій;

ПППс — стаціонарний проміжний приємо-передаючий пристрій;

ТН — трансформатор напруги;

ТС — трансформатор струму;

ТП — трансформаторна підстанція;

ЦЗІ — центр збору інформації;

RF — радіо канал.

ЗМІСТ

С.

ВСТУП

Сучасна цивілізована торгівля енергоресурсами і система їх раціонального споживання засновані на використанні автоматизованого приладового енергообліку, що зводить до мінімуму участь людини на етапі вимірювання, збору і обробки даних і забезпечує достовірний, точний, оперативний і гнучкий, адаптований до різних тарифних систем облік з боку як постачальника енергоресурсів, так і споживача. З цією метою споживачі (постачальники) створюють на своїх об'єктах автоматизовані системи контролю та обліку енергоресурсів (АСКОЕ). При наявності АСКОЕ підприємство повністю контролює весь процес енергоспоживання і має можливість за погодженням з постачальниками енергоресурсів мінімізувати свої енергоплатежі. Завдяки АСКОЕ вдається виявити і усунути всередині підприємства все непродуктивні витрати енергоресурсів,

Багато споживачів вже усвідомили свою зацікавленість в розрахунках з постачальником енергоресурсів з якимось умовним нормам, договірним величинам або застарілим і неточним приладів, а на основі сучасного і високоточного приладового обліку. Першим кроком в напрямку забезпечення економії енергоресурсів і зниження фінансових втрат є точний енергооблік. А в ринкових умовах переваги у виробництві конкурентоспроможної продукції будуть у тих підприємств, які вже здійснюють повний автоматизований контроль всіх процесів енергоспоживання.

Метою створення системи є зниження експлуатаційних витрат за рахунок оптимального управління процесом електроенергоснабженія, а саме:

- заміна фізично і морально застарілих комплексів програмно-технічних засобів;
- забезпечення безпеки функціонування об'єктів;
- зниження витрат живої праці;
- досягнення оптимального завантаження обладнання (особливо - опорних підстанцій);

- оптимізація режимів роботи технологічного обладнання;
- підвищення надійності енергопостачання кінцевих споживачів за рахунок своєчасної ліквідації аварійних і передаварійних ситуацій.

Пропонована система контролю і управління, призначена для цілеспрямованого ведення технологічного процесу і забезпечення суміжних і вищестоящих систем управління оперативної та достовірної інформацією. В рамках цих завдань система забезпечує:

- децентралізований контроль і вимірювання технологічних параметрів (струми, напруги, миттєві потужності);
- непряме вимірювання (обчислення) параметрів процесу (техніко-економічних показників, непрямих змінних);
- віддалене управління об'єктами електроенергохозяйства;
- підготовку та передачу інформації в системи управління (в відділ обліку або відділ реалізації електроенергії).

Дана загальна концепція організації системи, опис передбачуваних типів технологічних об'єктів управління, принципів організації зв'язку між об'єктами і короткий опис принципів функціонування системи.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Стан питання

У сучасному світі отримання енергоресурсів вкрай актуальне завдання. Проблеми, пов'язані з видобутком, транспортуванням, переробкою, розподілом і продажем енергоресурсів впливають на всі сфери життєдіяльності людини. Розглядаючи сучасну ситуацію генерації енергії, не можна не згадати про зміни в сформованій системі. Крім традиційних джерел генерації енергії (з використанням ТЕЦ, АЕС, ГЕС та ін.) На сучасному ринку з'являються рішення, коли споживач перестає тільки споживати електроенергію, починаючи генерувати її, і потенційно може віддавати її «надлишок» іншим споживачам. Одним із прикладів подібних рішень є використання сонячних панелей, вітряних електростанцій та інших збирачів вільної енергії. Фактично, вводиться поняття розподілених джерел енергії, при якому відбувається заміщення традиційної централізованої системи генерації енергії. Це є дуже важливим моментом для розвитку економіки і як наслідок, з'являється необхідність створення розподілених систем для моніторингу та спостереження за генерацією енергії. Використання таких систем на рівні підстанцій пропонує можливість для децентралізованого обліку і контролю інтелектуальних мереж, що підвищує надійність і точність в зборі даних обліку енергоспоживання. Крім того, завдяки використанню таких систем, з'являється можливість відстежувати дисбаланс напруги, який призводить до високих втрат енергії, зниження напруги в мережі і менш ефективному плануванню енергоспоживання.

1.2 Результати досліджень

Згідно з багатьма джерелами в США до 40% енергії втрачається через необізнаність споживачів про витрати і втрати в електричних мережах, використовуючи нові способи обліку енергії, можливо не тільки запобігати втраті енергії, а й отримувати прибуток за рахунок продажу надлишкової

енергії. Застосування «розумних» мереж, можливо більш довгострокове планування розширення системи електромереж, що збільшує загальну економічну ефективність електрогенеруючих підприємств. Крім того, можливе зменшення середньої тривалості відмови енергомереж, за рахунок зменшення перевантаження загальної потужності мережі завдяки своєчасному відстеженню короткочасних стрибків і провалів енергоспоживання. Надалі, отримані дані про енергоспоживання окремих ділянок мережі, можливо використовувати в рамках «bigdata» - акумуляції інформації у величезних дата-центрах, які виробляють подальший аналіз всієї мережі і її окремих ділянок, зокрема. Одним із прикладів використання розподілених систем створення системи Yipetal в Університеті Малайї, Малайзія. Використовуючи статистичні методи, були побудовані дві схеми відстеження крадіжки енергії на основі регресійного аналізу. Завдяки цим схемам, можливо відстеження аномального споживання електроенергії, на основі якого можна зробити висновок про можливу крадіжку електроенергії або дефекті вимірювальної системи. Іншим прикладом, є дослідження Zhouetal, проведене в Китаї, в місті Куншане, провінції Діжангсу. У ньому за допомогою використання «bigdata» були зібрані дані про енергоспоживання приватних споживачів низьковольтних мереж та представлені типові схеми споживання електроенергії, отриману інформацію можна використовувати для більш ретельного і раціонального планування при будівництві енергомереж. Ще одним прикладом, є проведена політика в країнах Євросоюзу, націлена на повсюдне впровадження «розумних» систем збору інформації і «розумних» лічильників. Згідно з документом ЕС, 2009a, до 2020 року не менше 80% користувачів мають бути обладнані «розумними лічильниками». На даний момент, тільки в 6 з 27 країн виконали необхідний мінімум заходів. Чималою проблемою, є вартість програми розгортання «розумних» мереж в різних областях, а також неузгодженість в розгортанні різних мереж. Ключовим способом зменшення витрат, є розробка і одночасне введення систем обліку електроенергії та газу. Розглядаючи досвід Великобританії та Нідерландів,

видно, що одночасна установка даних систем на 13% дешевше, ніж роздільна установка. Використовуючи системи зі зворотним зв'язком (що дозволяє оцінювати витрати в реальному часі) спонукає споживачів використовувати менше ресурсів. У дослідженні Zhouetal проведено порівняння п'яти європейських країн (Швеції, Фінляндії, Данії, Німеччини та Нідерландів) на предмет кореляції швидкості впровадження «розумних» лічильників і проведеної державної політики. За його результатами, лідерство займають ті країни (Фінляндія і Швеція), в яких державна політика сприяла використанню «розумних» лічильників, а також сприяла усуненню бар'єрів щодо впровадження і дослідження даних систем з боку сторонніх організацій. Німеччини та Нідерландів) на предмет кореляції швидкості впровадження «розумних» лічильників і проведеної державної політики.

1.3 Проблеми сучасної електроенергетики

Однією з найважливіших проблем сучасної електроенергетики є зростання втрат електроенергії, якие визначається як різниця між відпущеної в мережу і оплаченої електроенергією. Так, в деяких виробничих відділеннях відносні втрати досягають 15-20%, а в муніципальних і районних електричних мережах 25-50%. Сукупність усіх втрат включає технологічні та комерційні втрати (рисунок 1.1).

Серед технологічних втрат виділимо три складові:

- Технічні втрати електроенергії в елементах електричних мереж, обумовлені фізичними процесами перетворення електричної енергії в теплову енергію, супутні її передачі по електричних мережах;
- Витрати електроенергії на власні потреби підстанції, викликані необхідністю забезпечення роботи технологічного обладнання підстанцій і потребами життєдіяльності обслуговуючого персоналу;
- Інструментальні втрати - втрати електроенергії, пов'язані з інструментальними похибками її вимірювання.

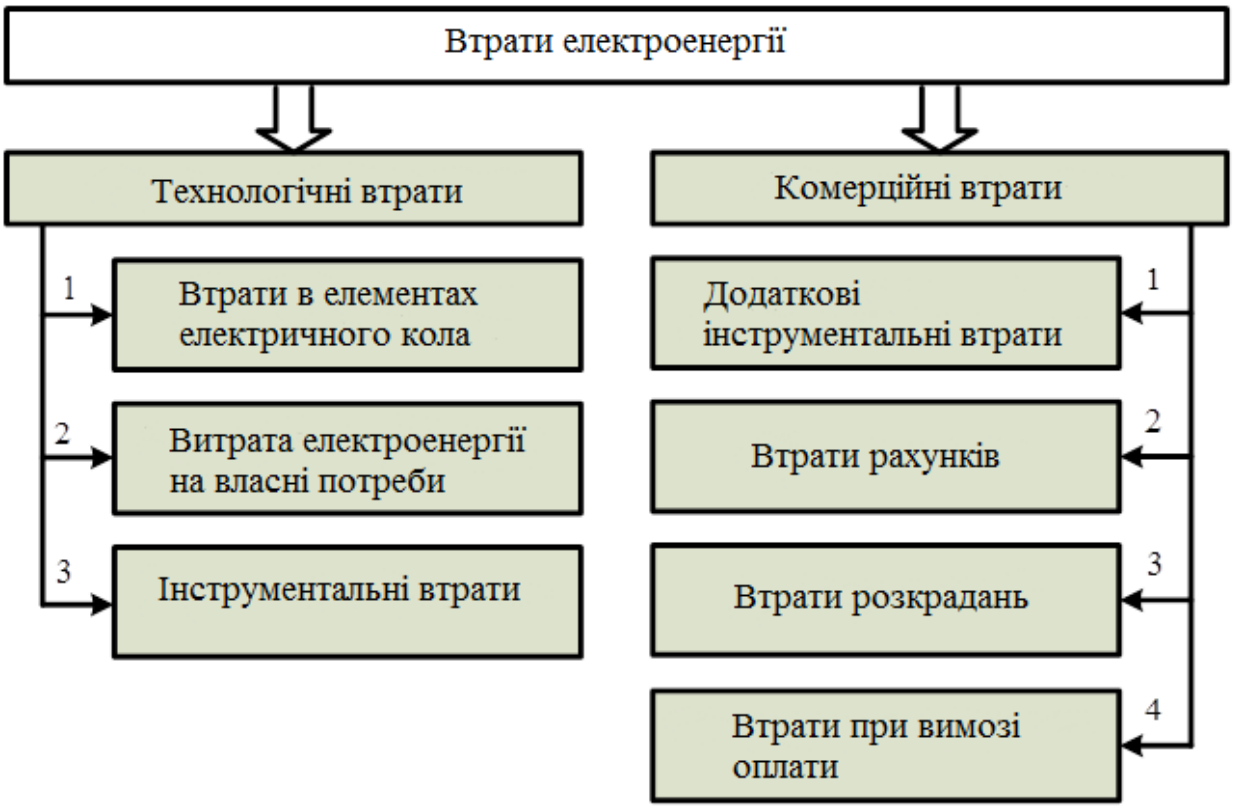

Рисунок 1.1 — Структура втрат електроенергії [18]

Основна причина зростаючого рівня електричних втрат - зростання комерційних втрат, велика частка яких припадає на електричні мережі напругою 0,4 кВ. Комерційні втрати обумовлені розкраданнями електроенергії, заниженням побутовими споживачами показань лічильників при оплаті, затримкою платежів, несплатою рахунків та недосконалістю організації контролю над споживанням енергії. Їх величину обчислюють як різницю між фактичними (відліковими) і технологічними втратами.

Комерційні втрати представимо чотирма групами (рисунок 1.1). Додаткові інструментальні втрати - втрати, зумовлені похибками систем обліку електроенергії. Породжені використанням вимірювальних трансформаторів струму (ТС) і напруги (ТН), лічильників і т. д. В ненормованих умовах роботи із заниженими класами точності.

Основний метод зниження інструментальних втрат - вдосконалення приладів обліку, заміна існуючих приладів обліку електроенергії на сучасні (з

більш високим класом точності). На підприємствах енергопостачальників приймаються програми заходів з модернізації відповідного обладнання, виділяються значні власні фінансові кошти. Однак, проведення цих заходів у відриві від інших, зокрема спрямованих на підвищення збирання платежів, не забезпечує отримання очікуваного економічного ефекту.

Слід зазначити, що вирішення цієї проблеми можливе лише на базі комплексних підходів, що включають крім названих заходів створення автоматизованих засобів моніторингу та контролю з розширенням функцій приладів обліку, що дозволяють використовувати їх в складі автоматизованих систем комерційного обліку електроенергії (АСКОЕ).

- Втрати при виставленні рахунків обумовлені недостатньою або помилковою інформацією про укладені договори, використанні спеціальних тарифів або пільг. Їх частка в структурі комерційних втрат мінімальна. Тут також ефективне використання автоматизованих засобів на базі обчислювальної техніки.

- Втрати через розкрадань електроенергії породжені несанкціонованим підключенням споживачів, шахрайством з приладами обліку і т. д. У сільській місцевості та в районах індивідуальної житлової забудови рівень втрат через розкрадання електроенергії, як правило, вище, ніж в міських багатоповерхових кварталах. Зниження цієї складової втрат вимагає поряд з ручним контролем енергопостачальників за допомогою перевірки цілісності пломб і правильності включення приладів обліку залучення додаткових технічних і організаційних заходів, що дозволяють оперативно виявляти місця несанкціонованих підключень споживачів до ліній електропостачання. Істотна роль у вирішенні цього питання може бути відведена засобам автоматизації, в тому числі АСКОЕ,

- Втрати при вимозі оплати викликані несвоєчасною оплатою за спожиту електроенергію пізніше встановленого терміну, тривалими або безнадійними боргами і неоплачуваними рахунками. У структурі фінансових

втрат електропостачальної організації основну роль грають втрати, зумовлені несплатою електроенергії і втрати через затримки платежів.

Ступінь оплати електроенергії населенням окремими енергопостачальними компаніями істотно коливається: від 30 до 95%, складаючи в середньому по країні 65-70%. Це викликано, перш за все, існуючою системою розрахунків за електроенергію після її споживання. Основна причина затримки оплати - відсутність механізмів та можливостей своєчасного контролю енергопостачальниками термінів і сум оплати спожитої електроенергії, а також відсутність технологічних, юридичних і фінансових можливостей оперативного впливу на неплатників.

1.4 Вирішення проблем енергомоніторінгу

Накопичений електроснабжаючими організаціями досвід показує, що основним засобом зниження втрат по цій компоненті слід визнати впровадження АСКОЕ з можливістю оперативного впливу на процес енергопостачання та переказ абонентів на передоплату. Розширення функціональних можливостей АСКОЕ в напрямку реалізації функцій оперативного індивідуального диспетчерського управління режимами електропостачання безлічі територіально розрізнених абонентів, включаючи функції автоматичного і ручного відключення абонентів дистанційно, не виїжджаючи на місце - дієвий засіб боротьби з комерційними втратами електроенергії.

1.5 Структура АСКОЕ

Автоматизована система комерційного обліку електроенергії будується як багаторівнева система і включає в себе програмно-технічні засоби підприємства енергопостачальників та абонентів (рисунок 1.2). Нижній рівень АСКОЕ складають програмно-технічні засоби енергоспоживачів, включаючи прилад обліку (ПО) і дистанційний дисплей (ДД) зв'язок між якими здійснюється по радіо каналу (RF).

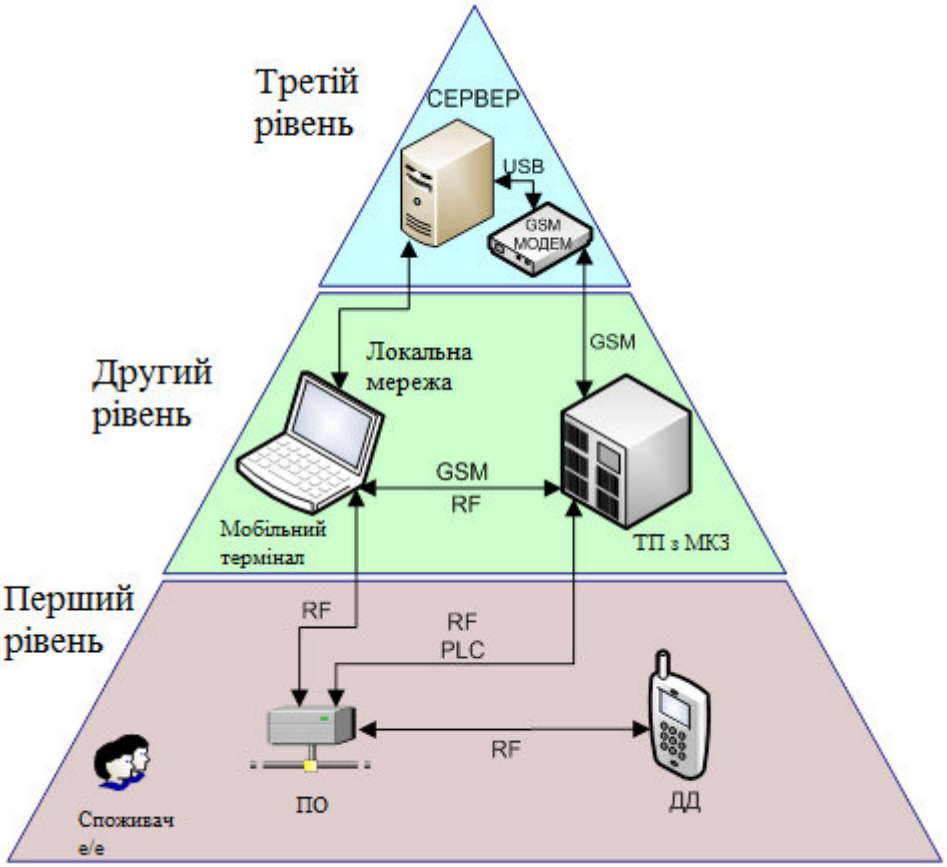

Рисунок 1.2 — Структурно-функціональна схема АСКОЕ [18]

Другий рівень АСКОЕ об'єднує трансформаторну підстанцію (ТП) з встановленим в неї маршрутизатором каналів зв'язку (МКЗ), і мобільний термінал, зв'язок між якими здійснюється як по радіо (RF), так і по GSM каналу. Дані пристрої забезпечують виконання функцій збору і тимчасового зберігання даних, зібраних з приладів обліку. Мобільний термінал контролера наділений функціями зчитування зберігається в пам'яті лічильника інформації і забезпечує корегування виконання команд управління лічильниками, а також вибірковий контроль правильності розрахунків. Контролер має можливість, перебуваючи поблизу контрольованого споживача, дистанційно контролювати вміст пам'яті його лічильника. Інший варіант передбачає застосування установленого на трансформаторну підстанцію маршрутизатора каналу зв'язку, за допомогою якого передаються всі дані з ПО.

Третій рівень системи виконаний на основі сервера бази даних і призначений для зберігання інформації і формування різних звітів в залежності від вимоги енергопоснабжающіх організацій.

Основа установки лічильників і підключення абонентів до АСКОЕ, програмування лічильника і формування параметрів особового рахунку - договір, в якому визначають:

- Встановлену потужність електрообладнання споживача;
- Величини установок спрацьовування захистів по напрузі;
- Рівень обмеження потужності при наявності боргу;
- Регламент оплати, включаючи схему оплати, моменти часу і порядок зміни тарифів, форми зараховуються платежів (банк, каса, картки оплати) і т.д.

Впровадження АСКОЕ дозволяє знизити комерційні втрати. Разом з тим слід зауважити, що несанкціоновано спожита електрична енергія все-таки проведена і найчастіше використовується корисно. Тому основний ефект зменшення споживаної електроенергії тут полягає в більш економному використанні електроенергії споживачем у разі її повноцінного оплати.

Технологічні ж втрати електроенергії безпосередньо пов'язані з неефективним витрачанням електроенергії. Основа їх зниження - моніторинг стану електричних мереж і використовуваного при передачі електроенергії обладнання.

1.6 Ефективність використання електричної енергії

Ефективність використання електричної енергії у споживача визначається двома факторами. По-перше якістю одержуваної електроенергії від електропостачальної організації і по-друге станом використовуваного обладнання. Так, зниження величини напруги, наприклад, на 10% веде до зниження крутного моменту асинхронного двигуна на 20% і збільшення споживаного струму і електричної енергії. Наявність безлічі гармонік призводить до виникнення знакозмінних моментів на валу двигуна і також

збільшує споживану енергію і призводить до зниження рівня технічного стану обладнання. З іншого боку, експлуатація несправного або з низьким рівнем працездатності обладнання веде до зниження ефективності використання споживаної енергії.

Тому важливим аспектом даної проблеми є моніторинг (спостереження, накопичення, збирання, первинна обробка інформації, оцінка поточного і прогнозованого стану) якості електричної енергії і обладнання. Зауважимо також, що споживачі мають право знати якість що надходить до них електричної енергії, що обумовлює необхідність контролю якості електричної енергії не тільки на стороні електропостачальної організації, але і введення в системи обліку електричної енергії функцій моніторингу та подання інформації про поточний стан якості електричної енергії на стороні споживача.

Велика кількість різних показників, що визначають якість електроенергії, з одного боку, і відмінності показників, використовувані для оцінки стану обладнання, з іншого, - ускладнюють комплексну оцінку стану енергетичної системи в цілому, включаючи весь ланцюжок від виробників до споживачів електроенергії, обумовлюють необхідність залучення сучасних методів обробки інформації. Тому з метою комплексування інформації про стан обладнання та якості електроенергії, забезпечення її доступності для люд й з різним рівнем технічної підготовки пропонується єдина комплексна система індикаторів стану.

Таким чином, основним напрямком зниження електричних втрат і підвищення ефективності виробництва і використання електричної енергії є широке впровадження інформаційних технологій і засобів автоматизації, розробка ефективних методів оцінки стану електричних мереж і якості електричної енергії, що забезпечують агрегування і комплексування та інформації про втрати, якість електричної енергії, стані обладнання та електричних мереж.

1.7 Криптовалюта IOTA

Оскільки для побудови АСКОЕ потрібно використати технології, які дозволять зробити її децентралізованою, відмінним рішенням буде використати криптовалюту IOTA.

IOTA -криптовалюта, розроблена спеціально для Інтернету Речей. Вона не схожа ні на один інший проект, що робить її унікальною і дуже багатообіцяючою. IOTA здатна стати тим транзакційних паливом, яке забезпечить реалізацію розумних підприємств за участю машин, об'єднаних в одну мережу. З'явилася вона на ринку в 2015 році і практично відразу потрапила в ТОП 10 найперспективніших представників свого класу. Творцями є Девід Сонстебо (David Sonstevbo), Сергій Іванчегло (Sergey Ivancheglo), Домінік Шейнер (Dominik Schiener) і Сергій Попов (Serguei Popov). Основною метою розробників було створення власної грошової одиниці, за допомогою якої можна було б здійснювати транзакції з різних гаджетів зі світу «Інтернету речей». IOTA заснована на концепції Tangle, який представляє собою розподілений обліковий журнал. За словами розробників, вона має велику кількість переваг в порівнянні з блокчейном біткоіну. Особливо це відноситься до здійснення мікроплатежів (наприклад, одноцентових). Справа в тому, що в основних криптовалютах, здійснення мікротранзакцій пов’язане з низкою проблемних аспектів: високі комісії майнерів і тривалий час для їх підтвердження іншими користувачами. У новій криптовалюті немає подібних труднощів. У ній відсутні майнери. І власники монет самі можуть підтверджувати угоди інших користувачів. Комісії всередині системи не передбачаються. Тим самим, платежі можна здійснювати в реальному часі. Близько 2.78 квадрильйонів монет IOTA створені одноразово. Їх велика кількість дозволяє використовувати coin для мікроплатежів.

Команда розробників криптовалюти, працює з 2011 року над новими архітектурними рішеннями блокчейна біткоіна та консенсус-протоколами. Протягом останніх декількох років розробляє абсолютно унікальну

архітектуру, засновану з нуля. У 2016 році створено спеціальний фонд IOTA, що дозволило значно збільшити ресурси і темпи розвитку платформи.

За даними порталу coinmarketcap.com капіталізація IOTA становить понад 4 млрд доларів США (приблизно 362 тис. BTC), і цей показник перевищує в два рази рекламованого вихідця з Китаю NEO і на 1 млрд менше вже закоренілого Litecoin.

IOTA повністю децентралізована, а відрізняється від інших криптовалют вона повною відсутністю комісії за транзакції і простотою реалізації. Якщо порівняти її з тими ж Біткоїн, де чітко виділяються між собою користувачі і Майнер, то тут ці дві категорії об'єднані в одне ціле. Наприклад, для здійснення транзакцій в Bitcoin, користувач відправляє запит майнеру, який підтверджує запит, використовуючи свої системні ресурси. Щоб провести транзакцію, вам потрібно підтвердити дві операції від інших користувачів Тангла (Tangle).

1.7.1 Переваги криптовалюти IOTA

Засновники нової криптовалюти постаралися за допомогою реалізації своєї ідеї усунути основні проблеми, характерні для інших блокчейнів, які ми перерахували вище. У зв'язку з цим вона має свої унікальні переваги. Основні з яких:

- Повна децентралізація - завдяки відсутності необхідності в видобувачів валюти, майнери не зможуть об'єднуватися в групи і створювати так звані пули, що значно знижує ймовірність хакерських атак і призначених для користувача втрат матеріального плану.
- Відсутність комісій за проведення транзакцій - система Tangle, виходячи з принципу своєї роботи, передбачає неоплачувані угоди. Так, звичайні транзакції з іншими криптовалютами перевіряються і схвалюються майнерами, які її видобувають. У новій технології кожна нова транзакція формує новий блок ланцюга і підтверджує сама себе шляхом підтвердження двох інших, що йдуть перед нею. І так до нескінченності. Ланцюг

масштабується і самоідентифікується. Фахівці вважають, що така особливість IOTA може в перспективі стати драйвером для багатьох нових бізнес-моделей.

- Високі показники масштабованості - швидкість проведення транзакцій залежить від кількості користувачів, і чим їх більше - тим краще, в той час, як при класичній схемі велика кількість операцій вимагає наявність високої обчислювальної потужності. В сучасних блокчейн-мережах існують конкретні обмеження по масштабованості, високим апаратним вимогам і транзакційним комісіям. У новій технології, масштабованість і адаптивність до високорівневих системам, де пристрої здійснюють тисячі і мільйони угод - звичайна ситуація.

- Робота в режимі офлайн - власникам криптовалют немає потреби постійно перебувати підключеними до мережі, так як сама концепція даної системи має на увазі синхронізацію з глобальною мережею. У Blockchain кожен учасник мережі синхронізується із загальною системою з метою здійснення платежу. Tangle не має таких жорстких вимог, дозволяючи користувачам об'єднуватися в кластери і навіть проводити розрахунки за допомогою монет в оффлайн середовищі.

- Прості мікро- і нанотранзакції - для IOTA проведення мікроплатежів є буденною справою і безліч переказів невеликих сум ніяк не позначиться на працездатності всієї системи.

1.7.1 Вирішення проблем у криптовалюті

Розробники IOTA хочуть вирішити наступні проблеми:

- Централізація майнінгу - як показує історія, майнери схильні об'єднуватися у великі групи. Це призводить до централізації і можливості здійснення атаки 51%. Ця можливість в світі Інтернету Речей є абсолютно неприйнятною.

- Застаріла криптографія - хоча промислових квантових комп'ютерів поки не існує, можливість їх появи в майбутньому слід враховувати.

- Труднощі проведення мікроплатежів - наявність комісій за транзакції для майнерів і протидії спам-атакам робиться критичним в світі Інтернету Речей.
- Нетерпимість до поділу - криптовалюти на основі блокчейна не можуть існувати, коли одна частина мережі відокремлена від цілого. Також неможливо довільне відділення частини мережі.
- Дискримінація учасників - існуючі криптовалюти є однорідними системами з чітким поділом ролей (є емітенти, які стверджують угоди). Такі системи створюють неминучу дискримінацію, яка в свою чергу створює конфлікти і змушує членів мережі витрачати ресурси на вирішення конфліктів.
- Межі масштабованості - деякі криптовалюти мають жорсткі обмеження по максимальній швидкості транзакцій, і це обмеження не може бути знято в рамках децентралізованої природи.
- Високі вимоги до апаратної частини - криптовалюти, які походять від Біткоїну, використовують свій оригінальний сценарій на основі методу PoW. Інші валюти працюють на PoS, подібним з використовуваним в банках, але додають додаткові функції. Обидва методи істотно підвищують вимоги до апаратної частини через складну логіку обробки транзакцій.
- Необмежене зростання даних - збереження всіх транзакцій призводить до швидкого зростання даних, і цю неефективність можна видалити навіть за допомогою алгоритмів стиснення даних.

1.7.3 Протокол Tangle

Протокол Tangle тим чи іншим чином вирішує всі вищевказані проблеми, в той же час він сумісний з блокчейном. Iota не збирається повністю замінювати Біткоїн, вона більше схожа на платформу «розумних контрактів», таку як Ethereum і Rootstock. Клієнтом підтримується більшість операційних систем, а для запуску протоколу досить недорогого мікроконтролера з 16 кб оперативної пам'яті.

Однак криптовалюта може мати ряд недоліків, які ще не виявлені, оскільки проект перебуває в стадії розробки, що не дозволяє об'єктивно оцінити недоробки, а також можливі негативні сторони. Проте, слід зауважити, що творці провели колосальну роботу. Вони ретельно продумують кожну дрібницю, намагаються забезпечити відмовостійке функціонування мережі і в повній мірі задовольнити найрізноманітніші призначені для користувача вимоги.

Це криптовалюта, в якій реалізований абсолютно новий підхід як в структурі, так і напрямку розвитку. Тут немає потреби в майнерах, так як за валідацію відповідають самі користувачі, які проводять транзакції, а легковажність грошової одиниці дозволяє використовувати її в пристроях зі світу «Інтернет речей». За словами самих розробників, дана криптовалюта покликана стати найбезпечнішою і популярною з усіх існуючих нині. До IOTA також позитивно ставляться експерти зі світу криптографії, так як її розвиток зачіпає не тільки світову мережу, а й реальний світ, а все більшу кількість різних гаджетів, які використовують люди для спрощення власного життя, в черговий раз підтверджують її надійність і її перспективи у недалекому майбутньому.

1.7.4 IOTA та Інтернет Речей

Перспективність IOTA вимірюється перспективністю сфери, яку покликана обслуговувати ця платформа. Ще в 2015 році індустрія Інтернету Речей «оцінювалася» в 1,6 трильйонів доларів. До 2025 року очікується, що галузь зросте до 6,2 трильйонів доларів, а кількість активних пристроїв до 2020 перевищить позначку в 50 мільярдів.

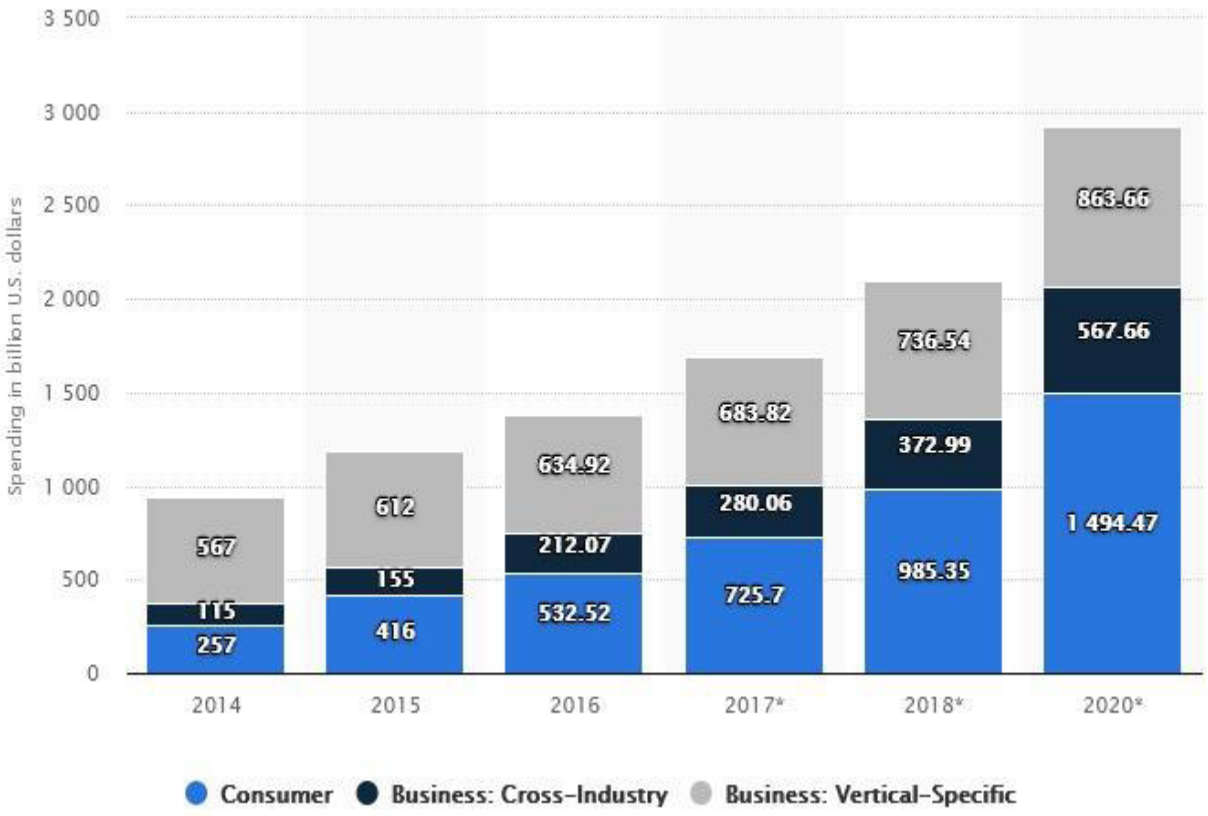

Рисунок 1.3 — Фінансова оцінка індустрії Інтернету Речей

Під Internet of Things мають на увазі мережу, в якій фізичні предмети взаємодіють один з одним за рахунок вбудованих технологій. Зараз повноцінної мережі немає - є скоріше автономні осередки. Наприклад смарт-квартири, де світло, електрику та опалення регулюється автоматично. Але ж квартири можна об'єднувати в будинки, будинки в міста, а міста в цілу мережу.

Інтернет Речей здатний змінити економічні та соціальні процеси, багато в чому рационализировав їх. Вперше цю концепцію запропонував дослідник MIT Кевін Ештон у своїй доповіді з модернізації логістичної системи Procter & Gamble. За два десятиліття бекграунд змінився - тепер кількість пристроїв, підключених до Інтернету, вимірюється мільярдами, з'явилися такі речі як хмарні обчислення, IPv6, зросла роль бездротових мереж, з'явилися численні сенсорні датчики і девайси.

IOTA здатна зв'язати воєдино практично всі процеси в екосистемі IoT за рахунок налаштування ланцюгів транзакцій і здатності проводити мікро транзакції в величезних кількостях. Проблем з масштабністю у Tangle на

відміну від blockchain немає. Причому платформа реалізована так, що пристрій для взаємодії з іншими вузлами не повинен мати безперебійного доступу до Інтернету. Для деяких «машин» досить буде підключатися раз на місяць або навіть на рік - все залежить від функціоналу. Це дозволить економити заряд батареї або навіть електрику.

1.7.5 Принцип роботи IOTA і опис системи

Замість традиційного блокчейна в мережі IOTA використовується DAG (Рисунок 1.4) спрямований ациклічний граф, який називається Tangle (клубок):

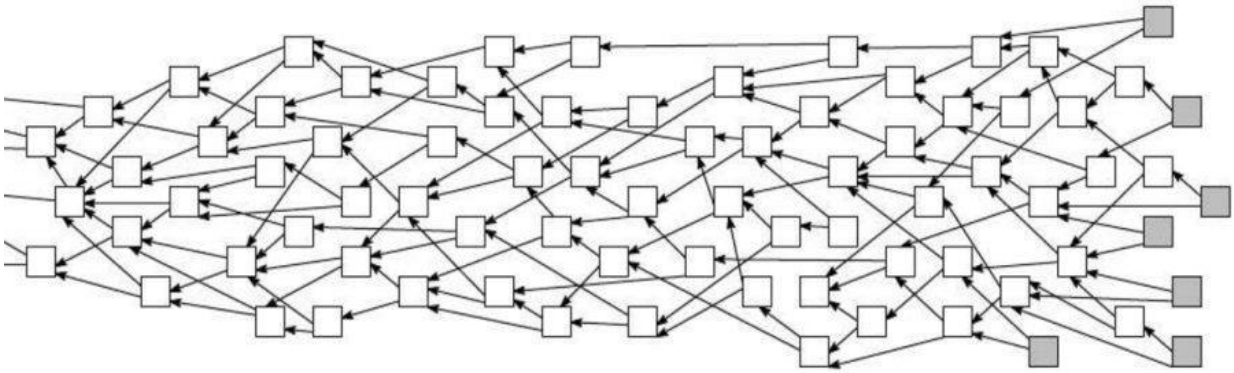

Рисунок 1.4 — Схема спрямованого ациклічного графу

Мережа DAG складена з транзакцій. Коли з'являється нова транзакція, вона повинна схвалити дві попередні транзакції, ці схвалення представлені спрямованими стрілками (час йде зліва направо). Якщо між двома транзакціями A і B існує шлях довжиною щонайменше в два ділянки, вважається, що A опосередковано схвалює B.

Вузли перевіряють відсутність конфліктів і не схвалюють (прямо чи опосередковано) конфліктуючі транзакції. Ідея полягає в тому, що, у міру того, як транзакція отримує все більше прямих і непрямих схвалень, прийняття її системою збільшується. Іншими словами, при великому числі схвалень, подвійна витрата стає практично неможливою. Для цього використовується поняття ваги транзакції - це кількість роботи, яке вклав в транзакцію

випускаючий вузол (на практиці це 3 ^ n, де n - ціле число), і кумулятивної ваги, який представляє собою суму власної ваги транзакції і ваг всіх попередніх транзакцій,що прямо або побічно схвалили її.

Щоб провести транзакцію, вузол виконує наступні дії:

- Вузол вибирає дві інші транзакції для затвердження відповідно до алгоритму. Загалом, ці дві транзакції можуть збігатися.
- Вузол перевіряє, чи не конфліктують ці дві транзакції і не схвалюють вони суперечливі транзакції.
- Щоб вузол видав дійсну транзакцію, вузол повинен вирішити криптографічне завдання, схоже з завданням в blockchain Bitcoin. Це досягається шляхом знаходження nonce (Nonce («нонс») - числовий параметр, шуканий в ході майнінгу (алгоритмі PoW) і записується в заголовок блоку. Власне, метою майнінгу, як змагального процесу за право додати блок транзакцій в блокчейн, і є підбір такого Nonce, щоб шуканий хеш блоку (Block Hash) був менше деякого заданого числа Target, що рівнозначно отриманню хеша блоку, що починається з певного числа нульових бітів.) таким чином, що хеш цього nonce, об'єднаного з деякими даними зі схваленої транзакції, має конкретну форму. У разі протоколу біткойнов хеш повинен мати як мінімум зумовлене число початкових нулів.

Важливо зауважити, що iota-мережа є асинхронною. Вузли не обов'язково бачать один і той же набір транзакцій. Слід також зазначити, що tangle може містити конфліктуючі транзакції. Вузлам не потрібно досягати згоди щодо того, які дійсні транзакції мають право бути в книзі, тобто всі вони можуть бути в Tangle. Однак в разі виникнення конфліктних транзакцій слід вирішити, які з них не будуть підтверджені.

Основне правило, яке використовується вузлами для вибору між двома конфліктуючими транзакціями, полягає в наступному: вузол багато разів виконує алгоритм вибору вершини (див. Атака ланцюжка паразитів і алгоритм вибору нової вершини) і бачить, яка з двох транзакцій найімовірніше буде опосередковано схвалена обраною вершиною. Наприклад, якщо транзакція

була обрана 97 разів за 100 прогонів алгоритму вибору вершин, ми говоримо, що це підтверджується достовірністю 97%.

Слід також врахувати наступне питання: що спонукає вузли здійснювати транзакції? Кожен вузол обчислює деяку статистику, одна з яких - кількість нових транзакцій, отриманих від сусіднього вузла. Якщо один конкретний вузол поводиться пасивно, він буде вилучений його сусідами. Тому, навіть якщо вузол не ініціює транзакції і, отже, не має прямого стимулу для обміну новими транзакціями, які схвалюють його власну транзакцію, у нього все ще є стимул для участі.

Після введення деяких позначень в розділі «Ваги», обговоримо алгоритми вибору двох транзакцій для затвердження, правила вимірювання загального схвалення транзакції (розділи «Стабільність системи і зрізи» і «Як швидко росте кумулятивний вага?»), та можливі сценарії атаки (розділ «Можливі сценарії атак »).

Слід зазначити, що ідея використання DAG в просторі криптовалюти була на слуху протягом деякого часу. Зокрема, протокол GHOST, який пропонує модифікацію протоколу біткойнов, роблячи основний регістр деревом замість ланцюжка блоків. Така модифікація зменшує час підтвердження і покращує загальну безпеку мережі.

1.7.6 Ваги

Вага транзакції пропорційна обсягу роботи, яку інвестиційний вузол інвестував в неї. У поточній реалізації iota вага може приймати тільки значення 3^n, де n - натуральне число, яке належить деякому непорожньому інтервалу допустимих значень (Цей інтервал також повинен бути кінцевим - див. «Великомасштабну атаку» в розділі «Можливі сценарії атак»). Фактично, не важливо знати, як вага була отримана на практиці. Важливо тільки, щоб вага кожної транзакції була цілим позитивним числом. Загалом, ідея полягає в тому, що транзакція з великою вагою більш «важлива», ніж транзакція з меншою вагою. Щоб уникнути спаму і інших атак, передбачається, що жодна

сутність не може генерувати надлишок транзакцій з «прийнятними» вагами за короткий проміжок часу.

Одним з понять, які потрібні, є сукупна вага транзакції: вона визначається як власна вага конкретної транзакції плюс сума власних ваг всіх транзакцій, які прямо або побічно схвалюють цю транзакцію. Алгоритм обчислення сумарної ваги показаний на малюнку 1. Квадрати представляють транзакції, невелике число в нижньому - правому куті кожного квадрата позначає власну вагу, а напівжирним шрифтом - сукупна вага. Наприклад, транзакція F прямо або опосередковано схвалена транзакціями A, B, C, E. Сукупна вага F дорівнює 9 = 3 + 1 + 3 + 1 + 1, що є сумою власної ваги F і власних ваг A, B, C, E.

Визначимо таке поняття, як несанкціоновані транзакції в графі Tangle. У верхній частині зображення, показаному на малюнку 1, вершинами є A і C. Коли нова транзакція X прибуває і стверджує A і C в нижній частині зображення, X стає єдиною вершиною. Сукупна вага всіх інших транзакцій збільшується на 3, завдяки власній вазі X.

Для обговорення алгоритмів затвердження потрібно ввести дві додаткові змінні. Для транзакції в Tangle вводяться:

• висота: довжина найдовшого орієнтованого шляху до початку;

• глибина: довжина найдовшого зворотного орієнтованого шляху до деякої вершини.

Наприклад, G має висоту 1 і глибину 4 на малюнку 2 через зворотній шлях F, D, B, A, а D має висоту 3 і глибину 2. Також потрібно представити поняття оцінки. За визначенням, оцінка транзакції є сумою власних ваг всіх транзакцій, схвалених цією транзакцією, плюс власниа вага самої транзакції. На малюнку 2 єдиними кінцями є A і C. Транзакція A прямо або побічно стверджує транзакції B, D, F, G, тому оцінка A дорівнює 1 + 3 + 1 + 3 + 1 = 9. Аналогічно, оцінка C дорівнює 1 + 1 + 1 + 3 + 1 = 7.

Щоб зрозуміти представлені аргументи, можна сміливо припустити, що всі транзакції мають власну вагу, рівну 1. З цього моменту дотримуємося цього

припущення. Відповідно до цього припущенням сукупна вага транзакції X стає рівним 1 плюс кількість транзакцій, які прямо або побічно схвалюють X, і оцінка стає рівною 1 плюс кількість транзакцій, які прямо або побічно схвалені X.

Зауважимо, що серед тих, які визначені в цьому розділі, сукупна вага є найважливішим параметром, хоча висота, глибина і оцінка коротко також увійдуть до деяких обговорень.

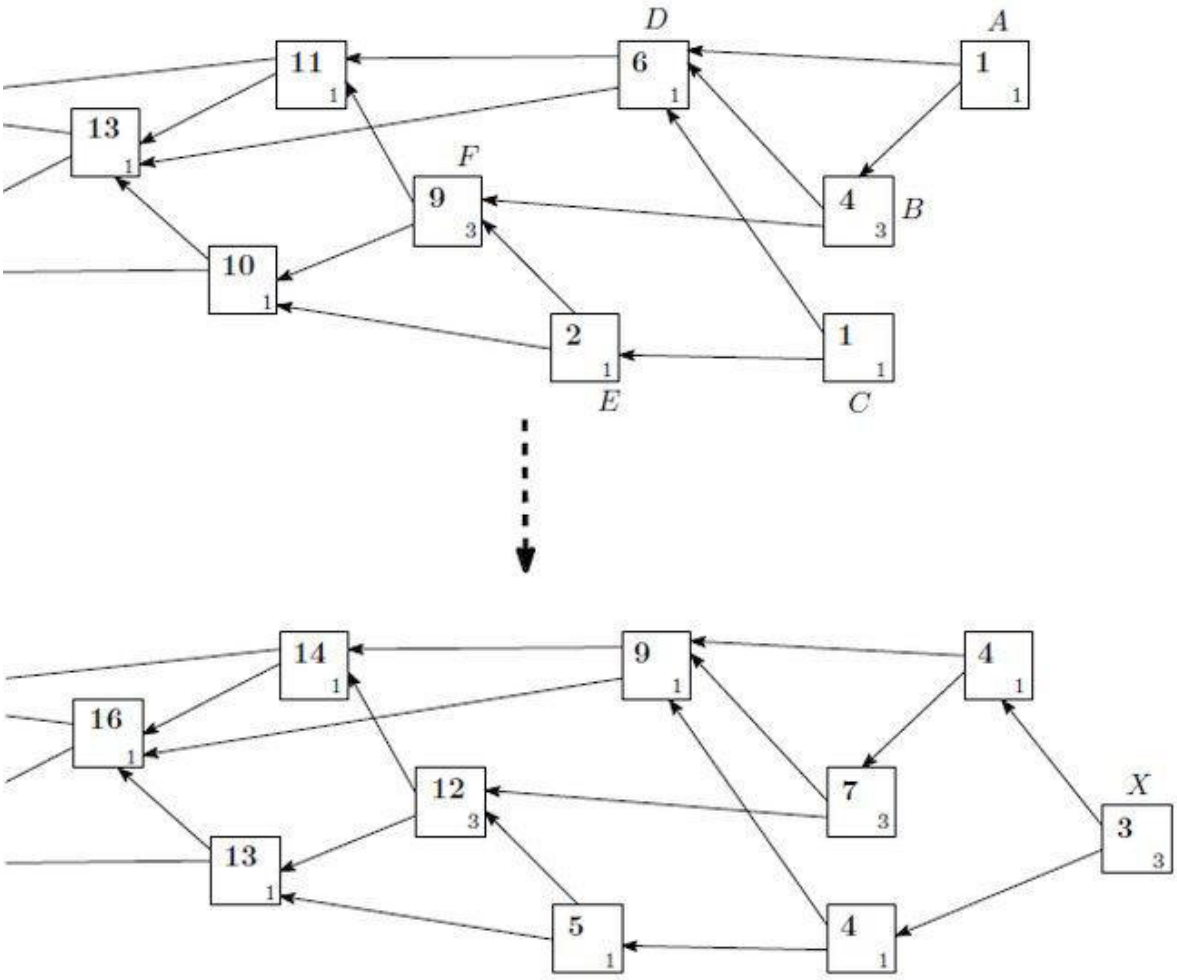

Рисунок 1.5 — DAG з присвоєнням ваги до і після недавно випущеної транзакції, X. Квадрати представляють транзакції, невелике число в нижньому-правому куті кожного квадрата позначає власну вагу, а напівжирним шрифтом позначена сукупна вага.

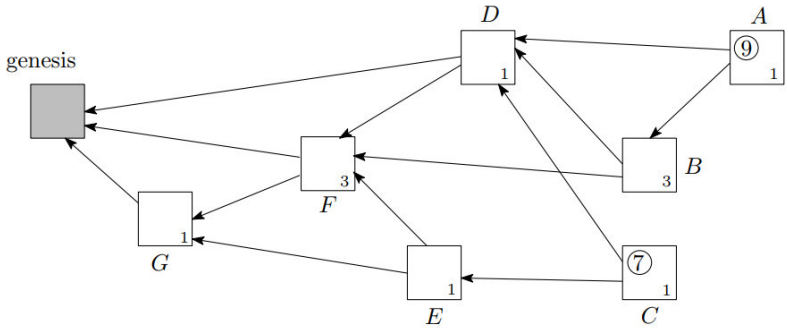

Рисунок 1.6 — DAG з власними вагами, призначеними кожній транзакції, і оцінки, розраховані для транзакцій A і C.

1.7.7 Стабільність системи і зрізи

Нехай L(t) - загальна кількість вершин в системі в момент часу t. Очікується, що стохастичний процес L(t) залишиться стабільним (при додатковому припущенні, що процес є однорідним за часом). Точніше, очікується, що процес буде позитивним рекурентним. Зокрема, з позитивною рекурсії слідує, що межа P[L(t)=k] при $t\to\infty$ повинен існувати і бути позитивним для всіх $k\geq 1$. Очікується, що L(t) буде коливатися навколо постійного значення, і не буде прагнути до нескінченності. Якщо L(t) прагнула до нескінченності, багато несанкціонованих транзакцій залишиться позаду.

Для аналізу властивостей стійкості L(t) потрібно зробити деякі припущення. Одне з припущень полягає в тому, що транзакції видаються великою кількістю незалежних одиниць, тому процес транзакцій, що входять, може бути змодельований точковим процесом Пуассона. Нехай λ - швидкість цього пуассоновского процесу. Для простоти припустимо, що ця швидкість залишається постійною в часі. Припустимо, що всі пристрої мають приблизно одну і ту ж обчислювальну потужність і нехай h - середній час, необхідний пристрою для виконання розрахунків, необхідних для здійснення транзакції. Потім припустимо, що всі вузли поводяться таким чином: для того, щоб зробити транзакцію, вузол вибирає дві транзакції випадковим чином і

затверджує їх. Слід зауважити, що в цілому, «чесним вузлам» не рекомендується приймати цю стратегію, оскільки вона має ряд практичних недоліків. Зокрема, вона не забезпечує достатнього захисту від «ледачих» або шкідливих вузлів (див. Розділ «Атака ланцюжка паразитів і алгоритм вибору нової вершини»). З іншого боку, ми все ще розглядаємо цю модель, оскільки її легко аналізувати, і вона може дати уявлення про поведінку системи при використанні більш складних стратегій вибору вершин.

Зробимо ще одне спрощуюче припущення, що будь-який вузол в момент його здійснення транзакції спостерігає не фактичний стан tangle, а стан в момент h одиниць часу назад. Це означає, зокрема, що транзакція, прив'язана до tangle в момент часу t, стає видимою в мережі в момент часу t+h. Ми також припускаємо, що кількість вершин залишається приблизно незмінною в часі і зосереджена навколо числа $L_0>0$. Надалі ми будемо обчислювати L_0 як функцію від λ і h.

Зауважимо, що в даний момент часу t ми маємо приблизно λh «прихованих вершин» (які з'явилися на часовому інтервалі [t-h,t) і тому ще не видимі для мережі); також припустимо, що зазвичай є r "виявлених вершин" (які були прикріплені до часу t-h і нагадують вершини в момент часу t), тому $L_0=r+\lambda h$. Можна тоді припустити, що в момент часу t є також приблизно λh місць, які були б вершинами в момент часу t-h, але більше ними не є. Тепер подумаємо про нову транзакцію, яка надходить в цей момент; то транзакція, яку вона обирає для затвердження, є вершиною з ймовірністю $r/(r+\lambda h)$ (оскільки навколо вузла, який видав транзакцію, існує близько r вершин, відомих вузлу, який ініціював транзакцію, а також приблизно λh транзакцій, які більше не є вершинами, хоча цей вузол думає, що вони є вершинами), тому середнє число обраних вершин одно $2r/(r+\lambda h)$. Головне спостереження полягає в тому, що в стаціонарному режимі ця середня кількість обраних вершин має дорівнювати 1, так як в середньому нова транзакція не повинна змінювати кількість кінців. Вирішуючи рівняння $2r/(r+\lambda h)=1$ по r, отримуємо $r=\lambda h$, і тому

$$L_0 = 2\lambda h \tag{1.1}$$

Відзначимо також, що якщо правило полягає в тому, що нова транзакція посилається на k транзакцій замість 2, то аналогічний розрахунок дає

$$L_0^{(k)} = \frac{k\lambda h}{k-1} \tag{1.2}$$

Це, звичайно, узгоджується з тим, що $L_0^{(k)}$ має прагнути до λh при $k\to\infty$ (в основному, єдиними вершинами будуть ті, які до сих пір невідомі мережі).

Також (повертаючись до випадку двох транзакцій для затвердження) очікуваний час для схвалення транзакції в перший раз становить приблизно $h+L_0/2\lambda=2h$. Це пов'язано з тим, що, за нашим припущенням, протягом перших h одиниць часу транзакція не може бути схвалена, і після цього потік схвалення Пуассона до неї має швидкість приблизно $2\lambda/L_0$. (Згадаймо припущення, в якому говориться, що якщо ми незалежно класифікуємо кожну подію пуассоновского процесу відповідно до списку можливих підтипів, то процеси подій кожного підтипу є незалежними пуассоновским процесами.)

Зауважимо, що в будь-який фіксований час t набір транзакцій, які були вершинами в певний момент $s\in[t,t+h(L_0, N)]$ зазвичай являє собою зріз. Будь-який шлях від транзакції, що виникла в момент часу $t'>t$, повинен пройти через цей набір. Важливо, щоб розмір нового зрізу в tangle іноді ставав невеликим. Потім можна використовувати невеликі скорочення в якості контрольних точок для можливої обрізки DAG і інших задач.

Важливо зауважити, що вищезгадана «випадкова» стратегія затвердження на практиці не дуже хороша, тому що вона не заохочує схвалення вершин (непідтверджених транзакцій). «Лінивий» користувач може постійно стверджувати фіксовану пару дуже старих транзакцій, тому не вносить вклад в утвердження більш пізніх транзакцій, не будучи покараним за таку поведінку. Крім того, шкідливий об'єкт може штучно збільшити кількість

вершин, ініціювавши безліч транзакцій, які стверджують фіксовану пару транзакцій. Це дозволить майбутнім транзакціям вибирати ці вершини з дуже високою ймовірністю, відмовляючись від вершин, що належать «чесним» вузлам. Щоб уникнути подібних проблем, потрібно прийняти стратегію, яка віддає пріоритет «кращим» вершинам. Один приклад такої стратегії представлений в розділі «Атака паразитним ланцюгом і алгоритм вибору нової вершини» нижче.

Можна розрізняти два режими (рисунок 1.7).

• Низьке навантаження: середня кількість вершин мала і часто стає 1. Це може статися, коли потік транзакцій настільки малий, що не представляється можливим, щоб кілька різних транзакцій схвалювали одну і ту ж вершину. Крім того, якщо затримка в мережі дуже низька, і швидкість обчислення пристроїв висока, малоймовірно, що з'явиться багато вершин. Це також справедливо у разі, коли потік транзакцій досить великий. Більш того, слід припустити, що немає нападників, які намагаються штучно збільшити кількість вершин.

• Високе навантаження: кількість вершин велика. Це може статися, коли потік транзакцій великий, а затримка обчислень разом із затримкою в мережі робить можливим, що кілька різних транзакцій схвалюють одну і ту ж вершину.

Цей поділ досить неформальний, і між цими двома режимами немає чіткої межі. Проте можна розглянути ці дві різні крайнощі.

Ситуація в режимі низького навантаження відносно проста. Перше твердження відбувається при середній шкалі порядку λ^{-1}, так як одна з перших декількох вхідних транзакцій схвалить цю вершину.

Розглянемо тепер режим великого навантаження, де L_0 велика. Як вже згадувалося вище, можна припустити, що потоки Пуассона дозволів до різних вершин, які є незалежними і мають приблизну швидкість $2\lambda/L_0$. Тому очікуваний час транзакції для отримання її першого твердження становить близько$L_0/(2\lambda)=h$.

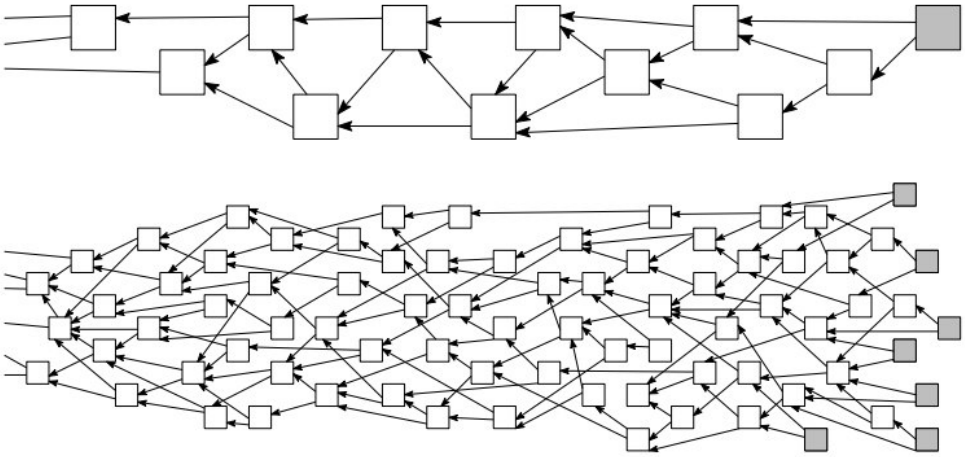

Рисунок 1.7 — Низьке навантаження (верхня) і високе навантаження (нижня) режими вхідного потоку транзакцій. Білі квадрати представляють собою перевірені елементи, а сірі квадрати представляють собою вершини.

Проте, варто зазначити, що для більш складних стратегій схвалення (Ця перевага «кращої» якості вершин в майбутніх реалізаціях iota), може бути поганою ідеєю пасивно очікувати, поки угода не буде схвалена іншими. Це пов'язано з тим, що «кращі» вершини будуть з'являтися і далі і будуть кращими для затвердження. Скоріш, в разі, коли транзакція очікує затвердження протягом інтервалу часу, набагато більшого, ніж $L_0/2\lambda$, хорошою стратегією було б просувати цю приховану транзакцію з додатковою порожньо транзакцією (Порожня транзакція - це транзакція, яка не включає передачу токена, але все одно повинна схвалити дві інші транзакції. Слід зазначити, що створення порожньої транзакції сприяє безпеці мережі). Іншими словами, вузол може випустити порожню транзакцію, яка стверджує свою попередню транзакцію разом з однією з «кращих» вершин, щоб збільшити ймовірність отримання схвалення порожньої транзакції.

Виявляється, що стратегії затвердження, засновані на висотах і оцінках, можуть бути уразливі для конкретних типів атак, см. Розділ («Атака ланцюжка паразитів і алгоритм вибору нової вершини»). Тим часом, як і раніше стоїть

розглянути стратегію вибору частих вершин, коли транзакція, що входить, схвалює дві випадкові вершини. Цю стратегію найлегше аналізувати і тому вона може дати певне уявлення про якісну та кількісну поведінки Tangle.

1.7.8 Як швидко наростає сукупна вага

Припустимо, що мережа знаходиться в режимі низького навантаження. Після того, як транзакція буде схвалена кілька разів, її сукупна вага буде рости зі швидкістю λ, оскільки всі нові транзакції побічно посилаються на цю транзакцію.

У разі, коли мережа знаходиться в режимі високого навантаження, стара транзакція з великою кумулятивною вагою буде відчувати збільшення ваги зі швидкістю λ, оскільки по суті всі нові транзакції побічно посилаються на неї. Більш того, коли транзакція спочатку додається в tangle, їй може знадобитися деякий час для затвердження. У цей проміжок часу сукупна вага транзакції поводиться випадковим чином. Щоб охарактеризувати швидкість, з якою наростає сукупна вага після того, як транзакція отримала кілька тверджень, визначимо H(t), як очікувану сукупну вагу в момент часу t (для простоти ми починаємо відлік часу в той момент, коли наша транзакція з'явилася в мережі, тобто h одиниць часу після її створення) і K(t) як очікувану кількість вершин, які схвалюють транзакцію в момент часу t. Також скоротимо h: = h (L_0, N). Ми робимо спрощуюче припущення, що кількість вершин залишається приблизно постійною у значенні L_0 з плином часу. Ми працюємо зі стратегією «схвалити дві випадкові вершини» в цьому розділі. Очікується, що якісна поведінка буде приблизно однаковою для інших осмислених стратегій.

Нагадаємо, що транзакція, що входить в мережу в момент часу t, зазвичай вибирає дві вершини для затвердження на основі стану системи в момент часу t-h, оскільки вузол повинен виконувати деякі обчислення і перевірки до фактичної видачі транзакції. Неважко побачити, що (за умови, що K (•) - фактична кількість вершин, а не тільки очікуване число) ймовірність

транзакції, що схвалює хоча б одну з «наших» вершин в tangle $1-(1-\frac{K(t-h))}{L_0})^2 = \frac{K(t-h)}{L_0}(2-\frac{K(t-h))}{L_0})^{16}$. Аналогічно для δ> 0 можна записати

$$H(t+\delta) = H(t) + \lambda\delta\frac{K(t-h)}{L_0}(2-\frac{K(t-h))}{L_0}) + o(\delta) \tag{1.3}$$

і, отже, вивести наступне диференціальне рівняння

$$\frac{dH(t)}{dt} = \lambda\frac{K(t-h)}{L_0}(2-\frac{K(t-h)}{L_0}) \tag{1.4}$$

Щоб мати можливість використовувати (1.4), нам потрібно спочатку вирахувати K(t). Це не тривіальне завдання, так як вершина в момент часу t-h може не бути вершиною в момент часу t, а загальна кількість вершин, що підтверджують вихідну транзакцію, збільшується на 1 в разі, коли транзакція, що входить, стверджує таку вершину. Важливе зауваження полягає в тому, що ймовірність того, що вершина в момент часу t-h залишається вершиною в момент часу t, становить приблизно 1/2. (Щоб переконатися в цьому, варто згадати обговорення з розділу «Стабільність системи і зрізи»: звичайне число вершин 2λh, а протягом інтервалу довжиною h нові λh-вершини замінять половину старих.) Тому в момент часу t приблизно половина K(t-h) вершин залишаються в непідтвердженому стані, а інша половина отримає хоча б одне твердження. Позначимо через A множину K(t-h)/2 вершин в момент t-h, які все ще є вершинами в момент часу t, і нехай B позначає залишившийся набір K(t-h)/2 вершин, які вже були затверджені у часі t. Нехай p_1 - вірогідність того, що нова транзакція схвалить принаймні одну транзакцію з B і не схвалить транзакції з A. Крім того, нехай p2 - ймовірність того, що обидві схвалені транзакції належать A. Іншими словами, p1 і p2 - ймовірності того, що поточна

кількість «наших» вершин збільшується або зменшується на 1 після прибуття нової транзакції. Маємо

$$p_1 = \left(\frac{K(t-h)}{2L_0}\right)^2 + 2 \times \frac{K(t-h)}{2L_0}\left(1 - \frac{K(t-h)}{L_0}\right), \qquad (1.5)$$
$$p_2 = \left(\frac{K(t-h)}{2L_0}\right)^2.$$

Щоб отримати перший вираз, зауважимо, що p_1 рівно ймовірності того, що обидві схвалених вершини належать B плюс вдвічі більше ймовірності того, що перша вершина належить B, а друга вершина не належить A∪B. Аналогічно (1.4) диференційне рівняння для K (t):

$$\frac{dK(t)}{dt} = (p_1 - p_2)\lambda = \lambda \frac{K(t-h)}{L_0}\left(1 - \frac{K(t-h)}{L_0}\right) \qquad (1.6)$$

Важко вирішити (1.6) точно, тому робиться подальше спрощення припущень. Насамперед зазначимо, що після того, як K(t) досягне рівня εL_0 при фіксованому $\varepsilon > 0$, воно буде рости дуже швидко до $(1-\varepsilon)L_0$. Тепер, коли K(t) мало по відношенню до L_0, можна відкинути останній коефіцієнт в правій частині (1.6). Отримаємо спрощену версію (1.6), нагадавши, що $\lambda h/L_0 = 1/2$

$$\frac{dK(t)}{dt} \approx \frac{1}{2h} K(t-h) \qquad (1.7)$$

з граничною умовою K(0)=1. Будемо шукати рішення виду K(t)=exp(c(t/h)); підставивши це в (1.7), отримаємо

$$\frac{c}{h}\exp\left(c\frac{t}{h}\right) \approx \frac{1}{2h}\exp\left(c\frac{t}{h} - c\right), \qquad (1.8)$$

Отже

$$K(t) = \exp\left(W\left(\tfrac{1}{2}\right)\frac{t}{h}\right) \approx \exp\left(0.352\frac{t}{h}\right) \qquad (1.9)$$

є наближеним рішенням, де W (•) - так звана W-функція Ламберта. Беручи логарифм обох сторін в (6), знаходимо, що час, коли K(t) досягає εL_0

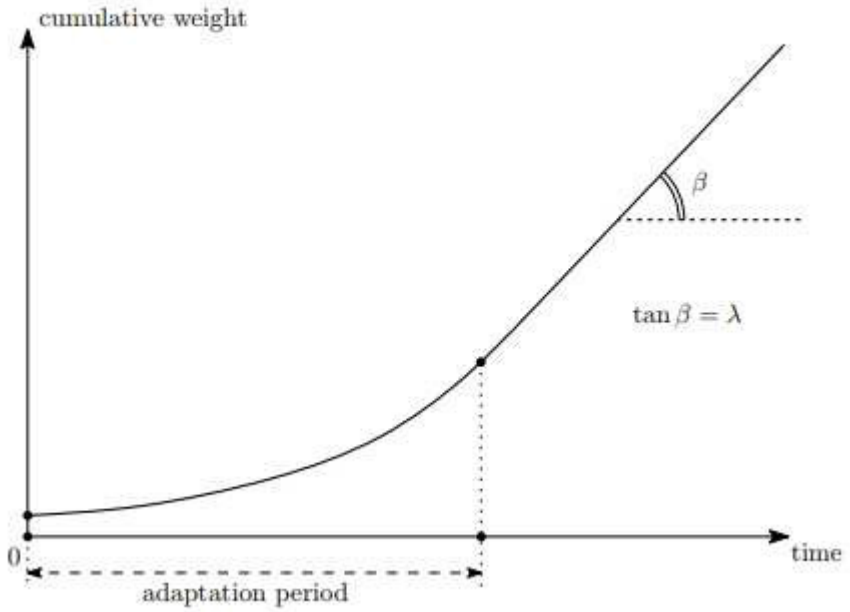

Рисунок 1.8 — Графік сукупної ваги проти часу для режиму високого навантаження.

Приблизно

$$t_0 \approx \frac{h}{W\left(\frac{1}{2}\right)} \times \left(\ln L_0 - \ln \varepsilon^{-1}\right) \lesssim 2.84 \cdot h \ln L_0. \tag{1.10}$$

Повертаючись до (1.4) і підставляючи останній член в правій частині, отримаємо, що протягом «періоду адаптації» ($T \leq t_0$ з t_0, як в (1.10))

$$\begin{aligned} \frac{dH(t)}{dt} &\approx \frac{2\lambda}{L_0} K(t-h) \\ &\approx \frac{1}{h \exp\left(W\left(\frac{1}{2}\right)\right)} \exp\left(W\left(\frac{1}{2}\right)\frac{t}{h}\right) \\ &= \frac{2W\left(\frac{1}{2}\right)}{h} \exp\left(W\left(\frac{1}{2}\right)\frac{t}{h}\right) \end{aligned}$$

тому

$$H(t) \approx 2\exp\left(W\left(\frac{1}{2}\right)\frac{t}{h}\right) \approx 2\exp\left(0.352\frac{t}{h}\right). \tag{1.11}$$

Нагадаємо також, що після періоду адаптації сукупна вага H (t) лінійно зростає зі швидкістю λ. Підкреслимо, що «експоненціальне зростання» не означає, що сукупна вага зростає «дуже швидко» протягом періоду адаптації. Швидше, поведінку показано на hbceyre 1.8.

1.7.9 Можливі сценарії атаки

Почнемо з обговорення сценарію атаки, коли зловмисник намагається «випередити» мережу:

1. Зловмисник відправляє платіж торговцю і отримує товар після того, як продавець вирішує, що угода має досить велику сукупну вагу.
2. Нападаючий видає транзакцію з подвійними витратами.
3. Зловмисник використовує свою обчислювальну потужність для випуску багатьох невеликих транзакцій, які схвалюють транзакцію з подвійними витратами, але не схвалюють первісну транзакцію, яку вони відправили торговцю прямо або опосередковано.
4. Нападаючий може мати безліч ідентифікаторів Sybil, які не зобов'язані стверджувати вершини.
5. Альтернативним методом для пункту 3 було б для зловмисника випустити велику транзакцію з подвійними витратами, використовуючи всю свою обчислювальну потужність. Ця транзакція буде мати дуже велику власну вагу і буде схвалювати транзакції до законної транзакції, використованої для оплати торговцю.

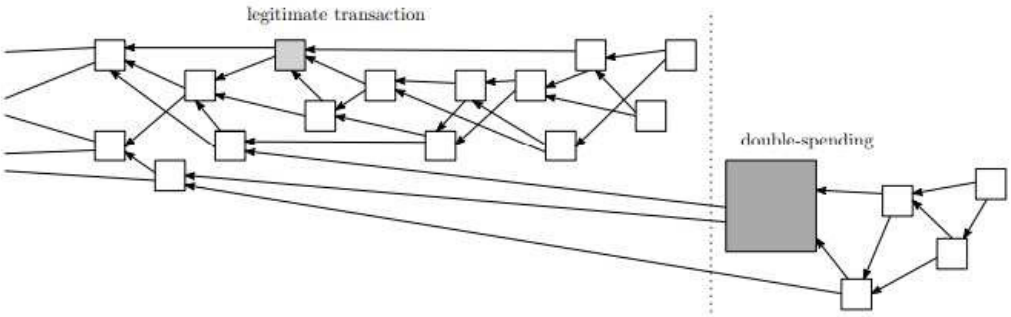

Рисунок1.9 — Атака «великої ваги»

6. Нападаючий сподівається, що незаконна транзакція випередить законну. Якщо це станеться, основний потік продовжить рости з подвійною транзакції, і законна гілка з початковим платежем торговцю стає непомітною (рисунок 5).

Фактично, можна показати, що стратегія однієї великої транзакції з подвійними витратами збільшує шанси атакуючого на успіх. В «ідеальній» ситуації цієї математичної моделі ця атака завжди досягає успіху.

Нехай $W^{(n)}$ - час, необхідний для отримання nonce, яке дає транзакцію з подвійними витратами вагою не менше 3^n. Можна припустити, що $W^{(n)}$ є експоненціально розподіленою випадковою величиною з параметром (З очікуванням μ^{-1} 3^N) $\mu 3^{-n}$, де μ являє обчислювальну потужність зловмисника.

Припустимо, що продавець приймає законну транзакцію, коли її сукупна вага стає не менш ніж w_0, що відбувається через t_0 одиниць часу після початкової транзакції. Розумно очікувати, що сукупна вага зростає з лінійною швидкістю λw, де λ - загальна швидкість прибуття транзакцій, випущених в мережі чесними вузлами, а w - середня вага загальної транзакції. Типова загальна вага легітимної гілки в цей час дорівнює $w_1=\lambda w t_0$.

Нехай [x] - найменше ціле число, більше або рівне x, певне $n_0 = \left\lceil \frac{\ln w_1}{\ln 3} \right\rceil$, так що $3^{n0} \geq w_1$[21]. Якщо зловмисникові вдалося отримати nonce, який дає транзакції з подвійними витратами вага не менше 3^{n0} протягом тимчасового інтервалу довжини t_0, тоді атака вдалася. Імовірність цієї події

$$\mathbb{P}[W^{(n_0)} < t_0] = 1 - \exp(-t_0 \mu 3^{-n_0}) \approx 1 - \exp(-t_0 \mu w_1^{-1}) \approx \frac{t_0 \mu}{w_1}. \quad (1.12)$$

Це наближення справедливо в разі, коли $t_0\mu/w_1$ мало, що є розумним припущенням. Якщо ця «негайна» атака не вдалася, зловмисник може продовжувати шукати nonce, який дає вагу 3^n для n> n0, і сподіватися, що в той момент, коли він його знайде, загальна вага легітимної гілки менше 3^n. Імовірність виникнення цієї події

$$\mathbb{P}[\lambda w W^{(n)} < 3^n] = 1 - \exp\left(-\mu 3^{-n_0} \times (3^{n_0}/\lambda w)\right) = 1 - \exp(-\mu/\lambda w) \approx \frac{\mu}{\lambda w}. \quad (1.13)$$

Тобто, хоча μ/λw зазвичай повинно бути невеликим числом, на кожному «рівні» n атака досягає успіху з постійною ймовірністю. Отже, вона буде успішною. Звичайний час до досягнення успіху становить приблизно $3^{\lambda w/\mu}$. Хоча ця величина може бути дуже великою, ймовірність того, що «перша» атака вдасться, не є незначною. Тому потрібні контрзаходи. Один такий контрзахід обмежував б власну вагу зверху або навіть встановлював би його на постійне значення. Як згадувалося в розділі «Стабільність системи і зрізи», це може бути не кращим рішенням, оскільки воно не забезпечує достатнього захисту від спаму.

Тепер обговоримо ситуацію, коли максимальна власна вага обмежениа значенням 1 і оцінимо ймовірність успіху атаки.

Припустимо, що дана транзакція отримала сукупна вага w_0 під час t_0 після моменту її випуску і що період адаптації для цієї транзакції завершений. У цій ситуації сукупна вага транзакції лінійно зростає зі швидкістю λ. Тепер уявімо, що зловмисник хоче влаштувати транзакцію з подвійними витратами. Для цього зловмисник таємно готує транзакцію з подвійними витратами і починає генерувати безглузді транзакції, які схвалюють транзакцію з подвійними витратами, коли первісна транзакція була видана продавцю. Якщо гілка атакуючого випереджає законну гілка в якийсь момент після того, як продавець вирішує прийняти законну транзакцію, то атака з подвійною витратою буде успішною. Якщо цього не відбудеться, то транзакція з подвійними витратами не буде схвалена іншими, оскільки законна транзакція набуде більш повної ваги, і по суті все нові транзакції побічно підтвердять її. У цьому сценарії транзакція з подвійними витратами буде залишатися непоміченою.

Як і раніше, нехай μ позначає обчислювальну потужність зловмисника. Ми також робимо спрощує припущення, що транзакції поширюються миттєво. Нехай G_1, G_2, G_3, ... позначають експоненціальні випадкові величини з

параметром μ[24] і визначимо $V_k = \mu G_k$, $k \geq 1$. Звідси випливає, що V1, V2, V3, ... експоненціальні випадкові величини з параметром 1.

Припустимо, що в момент часу t_0 торговець вирішує прийняти транзакцію з сумарною вагою w_0. Оцінимо ймовірність того, що зловмисник успішно подвоїть витрати. Нехай $M(\theta)=(1-\theta)^{-1}$ - моментна функція експоненціального розподілу з параметром 1. Відомо, що для $\alpha \in (0,1)$ виконується

$$\mathbb{P}\Big[\sum_{k=1}^{n} V_k \leq \alpha n\Big] \approx \exp\big(-n\varphi(\alpha)\big), \tag{1.14}$$

де $\varphi(\alpha)=-\ln\alpha+\alpha-1$ є перетворенням Лежандра $\ln M(\theta)$. Як загальний факт, зрозуміло, що $\varphi(\alpha)>0$ для $\alpha \in (0,1)$. Нагадаємо, що очікування експоненційної випадкової величини з параметром 1 також дорівнює 1.

Припустимо, що $\mu t_0/w_0<1$, в іншому випадку ймовірність того, що гілка атакуючого в кінцевому підсумку випередить законну гілку, буде близька до 1. Тепер, щоб переважити w_0 в момент часу t_0, зловмисник повинен мати можливість випускати принаймні w_0 транзакції з максимальною власною вагою m за час t_0. Тому, використовуючи (9), знаходимо ймовірність того, що транзакція з подвійними витратами має більшу сумарну вагу в момент часу t0 приблизно

$$\begin{aligned}\mathbb{P}\Big[\sum_{k=1}^{w_0/m} G_k < t_0\Big] &= \mathbb{P}\Big[\sum_{k=1}^{w_0} V_k < \mu t_0\Big] \\ &= \mathbb{P}\Big[\sum_{k=1}^{w_0} V_k < w_0 \times \frac{\mu t_0}{w_0}\Big] \\ &\approx \exp\Big(-w_0\varphi\Big(\frac{\mu t_0}{w_0}\Big)\Big).\end{aligned} \tag{1.15}$$

Для того щоб зазначена ймовірність була малою, w_0/m повинно бути великим і $\varphi(\mu t_0/w_0)$ не може бути дуже малою.

Зауважимо, що в момент $t \geq t_0$ сукупна вага законної транзакції приблизно дорівнює $w_0+\lambda(t-t_0)$, оскільки ми припустили, що період адаптації завершено,

тому сукупна вага зростає зі швидкістю λ. Аналогічно (10), можна знайти ймовірність того, що транзакція з подвійною витратою матиме більшу сумарну вагу в момент часу $t \geq t_0$ приблизно

$$\exp\left(-(w_0 + \lambda(t - t_0))\varphi\left(\frac{\mu t}{w_0 + \lambda(t - t_0)}\right)\right). \tag{1.16}$$

Тоді має бути вірно, що ми маємо $\mu t_0/w_0 \geq \mu/\lambda$, так як сукупна вага зростає зі швидкістю менше λ при адаптації. Можна показати, що ймовірність успішної подвійної витрати має порядок.

$$\exp\left(-w_0\varphi\left(\max\left(\frac{\mu t_0}{w_0}, \frac{\mu}{\lambda}\right)\right)\right). \tag{1.17}$$

Наприклад, нехай μ=2, λ=3, так що потужність зловмисника трохи менше, ніж у решти мережі. Припустимо, що транзакція має сукупну вага 32 по часу 12. Тоді $\max(\mu t_0/w_0, \mu/\lambda)=3/4$, $\varphi(3/4)\approx 0.03768$ і (12) потім дає верхню межу приблизно 0,29. Якщо припустити, що μ=1 і зберігає всі інші параметри в цілості, то $\max(\mu t_0/w_0, \mu/\lambda)=3/8$, $\varphi(3/8)\approx 0{,}35558$ і (12) дає приблизно 0,00001135, досить різка зміна.

З наведеного вище обговорення важливо визнати, що нерівність λ>μ має бути істинною для безпеки системи. Іншими словами, вхідний потік «чесних» транзакцій повинен бути більшим у порівнянні з обчислювальною потужністю зловмисника. В іншому випадку оцінка (12) була б марною. Це вказує на необхідність додаткових заходів безпеки, таких як контрольно-пропускні пункти, в перші дні існування системи на основі Tangle.

При виборі стратегії для визначення того, яка з двох суперечливих транзакцій дійсна, потрібно бути обережним при використанні сукупної ваги в якості показника прийняття рішення. Це пов'язано з тим, що сукупна вага може бути використана для атаки, аналогічної тій, яка описана в розділі «Атака ланцюжка паразитів і алгоритм вибору нової вершини», а саме: зловмисник може заздалегідь підготувати транзакцію з подвійними витратами,

створити секретний потік, що посилається на неї, а потім поширювати цю гілку після прийняття продавцем законної транзакції. Кращим способом вирішення двох конфліктних транзакцій може бути той, який описаний в наступному розділі: запустити алгоритм вибору вершин і подивитися, яка з двох транзакцій опосередковано схвалена обраною вершиною.

1.7.10 Атака ланцюжка паразитів і алгоритм вибору нової вершини

Розглянемо наступну атаку (рис. 6): зловмисник таємно створює гілку, яка іноді посилається на основну гілку, щоб отримати більш високий бал. Зверніть увагу, що оцінка чесних вершин становить приблизно суму всіх власних ваг в основній гілці, в той час як оцінка транзакцій атакуючого також містить суму всіх власних ваг в паразитному ланцюжку. Оскільки затримка мережі не є проблемою для зловмисника, який створює гілку поодинці (Це пов'язано з тим, що зловмисник завжди може стверджувати свої власні транзакції, не покладаючись на будь-яку інформацію з іншої мережі), вони можуть дати більше висоти паразитним транзакціям, якщо вони використовують досить сильний комп'ютер. Більш того, зловмисник може штучно збільшити кількість вершин в момент атаки, створюючи багато нових транзакцій, які схвалюють транзакції, які вони видали раніше в ланцюзі паразитів (рис. 6). Це дасть зловмисникові перевагу в разі, коли чесні вузли використовують деяку стратегію вибору, яка включає простий вибір між доступними вершинами.

Щоб захиститися від цієї атаки, будемо використовувати той факт, що основна гілка повинна мати більшу потужність хешування, ніж атакуючий. Таким чином, основний потік Tangle здатний виробляти більше збільшення сукупної ваги для більшої кількості транзакцій, ніж атакуючий. Ідея полягає у використанні алгоритму Маркова ланцюга Монте-Карло для вибору двох вершин для посилання.

Нехай H_x - поточна кумулятивна вага ділянки. Нагадаємо, що ми припустили, що всі власні ваги рівні 1. Тому сукупна вага вершини завжди дорівнює 1, а сукупна вага інших ділянок становить не менше 2.

Ідея полягає в тому, щоб розмістити деякі частинки, т.зв. блукаючі елементи в місцях Tangle і дозволити їм йти до вершин випадковим чином. Вершини, «обрані» елементами, є кандидатами на схвалення. Алгоритм описується наступним чином:

1. Розглянемо всі ділянки на інтервалі [W, 2W], де W досить велике,

2. Незалежно помістимо N елементів в місця в цьому інтервалі,

3. Нехай ці елементи виконують незалежні дискретні випадкові пересування «у напрямку до вершин», що означає, що перехід від x до y можливий тоді і тільки тоді, коли y стверджує x

4. Два випадкових блукаючих елемента, які дійдуть до набору вершин, будуть перебувати на двох обраних вершинах, які будуть схвалені. Однак може бути розумним змінити це правило в такий спосіб: спочатку скасувати ті блукаючі елементи, які досягли вершин занадто швидко, тому що вони, можливо, досягли одну з «ледачих вершин».

5. Вірогідності переходу елементів визначаються наступним чином: якщо y стверджує x, то ймовірність переходу P_{xy} пропорційна $\exp(-\alpha(H_x-H_y)$, тобто

$$P_{xy} = \exp\big(-\alpha(\mathcal{H}_x - \mathcal{H}_y)\big)\Big(\sum_{z:z\rightsquigarrow x} \exp\big(-\alpha(\mathcal{H}_x - \mathcal{H}_z)\big)\Big)^{-1}, \qquad (1.18)$$

де $\alpha > 0$ - параметр, який потрібно вибрати.

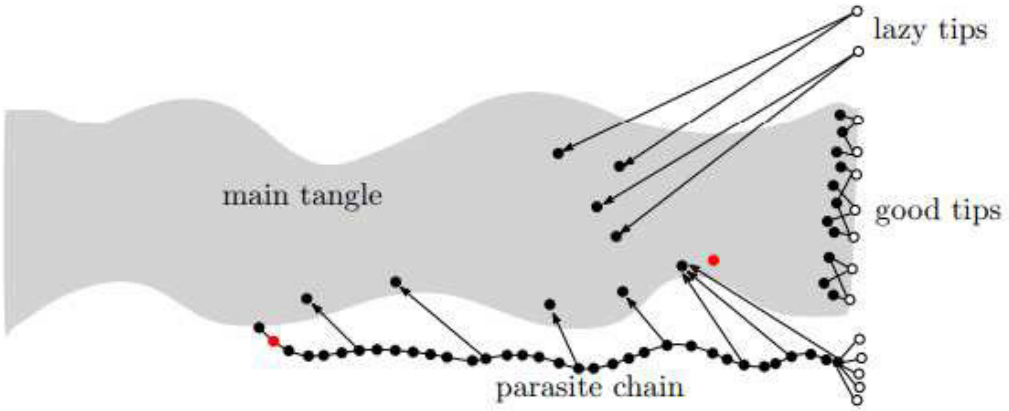

Рисунок 1.10 — Візуальне уявлення алгоритму вибору вершин для чесних вершин, а також паразитного ланцюжка. Два червоних кола вказують на спробу влаштувати подвійну витрату зловмисником.

Слід звернути увагу, що цей алгоритм є «локальним», тобто не потрібно переміщувати потік назад до початку для виконання відповідних обчислень. Зокрема, зверніть увагу, що не потрібно обчислювати сукупні ваги для всього потоку. У більшості випадків необхідно розрахувати сукупну вага для елементів, які побічно стверджують початкову точку відправки блукаючих елементів.

Щоб перевірити, що алгоритм працює за призначенням, спочатку розглянемо «ледачі вершини». Ці вершини навмисно схвалюють деякі старі транзакції, щоб уникнути виконання перевірки (рис. 6). Навіть якщо частка знаходиться в місці, схваленому лінивою вершиною, малоймовірно, щоб лінива вершина була обрана, тому що різниця між кумулятивними вагами була б дуже великою, а P_{xy} була б невеликою.

Потім розглянемо цей альтернативний вид атаки: зловмисник таємно будує ланцюжок, що містить транзакцію, яка перенесе баланс зі свого облікового запису на інший обліковий запис під його контролем, позначений як саме ліве червоне коло на малюнку 6. Потім зловмисник видає транзакцію в основному потоці, представленому правим червоним колом, і чекає, поки торговець прийме її. Паразитний ланцюг іноді посилається на основний потік.

Однак сукупна вага в паразитного кола не дуже велика. Слід зазначити, що паразитний ланцюг не може посилатися на основний потік після транзакції торговця. Крім того, атакуючий може спробувати штучно роздути кількість вершин у свого ланцюга паразитів в момент атаки (рис. 6). Ідея атакуючого полягає в тому, щоб змусити вузли, що випускають нові транзакції, посилатися на ланцюжок паразитів, щоб чесна гілка в потоці залишилася непоміченою.

Легко зрозуміти, чому алгоритм вибору Маркова Ланцюги Монте-Карло не вибиратиме одну з вершин зловмисника з великою ймовірністю. Обгрунтування ідентично сценарієм ледачої вершини: місця на ланцюжку паразитів матимуть сукупну вага, яка набагато менше, ніж місця, які посилаються на основний потік. Тому не представляється можливим, щоб випадковий блукаючий елемент завжди стрибав в ланцюг паразитів, якщо він не починається там, і ця подія не дуже ймовірна, можливо, тому, що основний потік містить більше місць.

В якості додаткової міри захисту можна спочатку запустити випадкове блукання з великим α (так що воно фактично «майже детерміновано»), щоб вибрати «вершину моделі»; потім використовувати випадкові блукання з малим α для вибору фактичної вершини, але перевірити, чи відповідають (опосередковано) транзакції, на які робиться посилання, з вершини моделі.

Зауважимо також, що для випадкового блукання, яке завжди рухається до вершин, дуже просто і швидко обчислити розподіл ймовірності виходу з допомогою прямої рекурсії; це те, що не бажано, щоб вузли робили. Проте, можна змінити підхід у такий спосіб: на кожному кроці блукаючий елемент може відступити (тобто Вийти на один крок від вершин) з ймовірністю (скажімо) 1/3 (і розділити залишилися 2/3, як і раніше). У будь-якому випадку, переміщення дійде до вершин дуже швидко (бо у неї є дрейф у напрямку до вершин), але буде не так просто розрахувати міру виходу.

Слід вказати, чому вузли будуть слідувати цим алгоритмом. Розумно припустити, що принаймні велика частка вузлів буде слідувати еталонному алгоритму. Крім того, через обчислювальні і мережеві затримки алгоритм

вибору вершин швидше буде працювати з минулим варіантом потоку щодо моменту, коли видається транзакція. Можливо, було б непогано навмисно перемістити цей варіант на більш пізній проміжок часу в минулому (Спочатку блукаючий елемент знаходить колишню вершину щодо цього моменту, а потім він продовжує йти до «фактичним» вершин в поточному потоці) в еталонному алгоритмі з причин, які будуть пояснені далі. Уявіть собі «егоїстичний» вузол, який просто хоче максимально швидко збільшити шанси на підтвердження його транзакції. Алгоритм Маркова Ланцюга Монте-Карло цього розділу, який приймається значною частиною вузлів, визначає розподіл ймовірності на безлічі вершин. Ясно, що природним першим вибором для егоїстичного вузла було б обрати вершини, в яких досягається максимум цього розподілу. Однак, якщо багато інших вузлів також поводяться егоїстично і використовують ту ж стратегію, яка є розумним припущенням, тоді всі вони програють. Багато нових транзакцій будуть схвалювати ті ж дві вершини приблизно в один і той же час, що створює занадто багато конкуренції між ними для подальшого затвердження. Також має бути ясно, що вузли не будуть відразу «відчувати» сукупне збільшення ваги, викликане цим масовим схваленням тих же двох вершин, оскільки вузли використовують минулий стан. З цієї причини, навіть егоїстичний вузол повинен використовувати певний алгоритм затвердження випадкової вершини з розподілом ймовірностей для вибору вершини, яка близька до розподілу ймовірності, за умовчанням проводиться це за допомогою алгоритму вибору опорної вершини. Також не затверджується, що це «агрегований» розподіл ймовірності дорівнюватиме розподілу ймовірності за умовчанням в присутності егоїстичних вузлів. Однак наведений вище аргумент показує, що він повинен бути близький до нього. Це означає, що ймовірність того, що багато вузлів спробують перевірити одні і ті ж «погані» вершини, залишиться малою. У всякому разі, немає великого стимулу для вузлів бути егоїстичними, бо можливий виграш становить лише невелике зниження часу підтвердження. Це по своїй суті відрізняється від інших децентралізованих конструкцій, таких

як біткойн. Важливим фактом є те, що у вузлів немає причин відмовитися від алгоритму вибору вершин Маркова Ланцюга Монте-Карло.

1.7.11 Атака поділу

Була запропонована наступна схема атаки проти запропонованого алгоритму Маркова Ланцюга Монте-Карло. У режимі високого навантаження зловмисник може спробувати розділити потік Tangle на дві гілки і підтримувати баланс між ними. Це дозволить обом гілкам продовжувати рости. Зловмисник повинен помістити як мінімум дві конфліктуючі транзакції в початок поділу, щоб не допустити, щоб чесний вузол ефективно з'єднував гілки, посилаючись на них одночасно. Потім нападник сподівається, що приблизно половина мережі сприятиме кожній гілці, щоб вони могли «компенсувати» випадкові коливання навіть при відносно невеликій кількості обчислювальних потужностей. Якщо ця методика працює, зловмисник зможе витратити ті ж кошти на дві гілки.

Щоб захиститися від такої атаки, потрібно керуватися правилом «гострий поріг», через що занадто складно підтримувати баланс між двома гілками. Прикладом такого правила є вибір самого довгого ланцюгу в мережі Bitcoin. Переведемо це поняття в tangle, коли він піддається атаці розщеплення. Припустимо, що перша гілка має загальну вагу 537, а друга гілка має загальну вагу 528. Якщо чесний вузол вибирає першу гілку з ймовірністю, дуже близькою до 1/2, тоді нападник, ймовірно, зможе підтримувати баланс між гілками, Однак, якщо чесний вузол вибирає першу гілку з ймовірністю, що набагато перевищує 1/2, тоді зловмисник, ймовірно, не зможе підтримувати баланс. Нездатність підтримувати баланс між двома гілками в останньому випадку обумовлена тим, що після неминучого випадкового коливання мережа швидко вибирає одну з гілок і відмовляється від іншої. Для того, щоб алгоритм Маркова Ланцюга Монте-Карло працював таким чином, потрібно вибрати дуже швидко спадну функцію f і ініціювати випадкове блукання в вузлі з великою глибиною, так що дуже ймовірно, що блукання

починається до поділу гілки. В цьому випадку блукаючий елемент з високою ймовірністю вибере «важчу» гілку, навіть якщо різниця в сукупній вазі між конкуруючими гілками мала.

Варто відзначити, що завдання зловмисника дуже складне через проблеми з синхронізацією мережі: вони можуть не знати про велику кількість недавно випущених транзакцій. Ще один ефективний спосіб захисту від атаки на поділ буде полягати в тому, щоб досить потужний суб'єкт миттєво створив велику кількість транзакцій на одній гілці, тим самим швидко змінюючи баланс потужності і ускладнюючи для зловмисника усунення цієї зміни. Якщо зловмисникові вдасться зберегти розкол, найостанніші транзакції будуть мати приблизно 50% підтвердження довіри, і гілки не будуть рости. У цьому випадку «чесні» вузли можуть прийняти рішення почати вибірково давати свою згоду на транзакції, що відбулися до поділу, в обхід можливості схвалити конфліктуючі транзакції на розділених гілках.

1.7.12 Стійкість до квантових обчислень

Відомо, що досить великий квантовий комп'ютер може бути дуже ефективним для вирішення проблем, що спираються на ипроби та помилки, для знаходження рішення. Хорошим прикладом такої проблеми є процес пошуку nonce для створення блоку біткойнов. На сьогоднішній день необхідно перевірити в середньому 268 несетів, щоб знайти відповідний хеш, який дозволяє генерувати новий блок. Відомо, що квантовому комп'ютеру буде потрібна операція $\Theta(\sqrt{N})$ для вирішення проблеми, аналогічної задачі в біткойні, зазначеної вище. Ця ж проблема потребує $\Theta(N)$ операцій на класичному комп'ютері. Таким чином, квантовий комп'ютер буде близько $\sqrt{268}=234\approx17$ мільярдів раз більш ефективний при видобутку блоку біткойнов, ніж класичний комп'ютер. Крім того, варто відзначити, що якщо блок-ланцюг не збільшує свою складність у відповідь на підвищену потужність хешування, буде збільшуватися швидкість осиротілих блоків.

З тієї ж причини атака «великої ваги» також буде набагато ефективнішою на квантовому комп'ютері. Однак обмеження ваги зверху, як це було запропоновано, ефективно запобігло б також і квантову комп'ютерну атаку. Це очевидно в iota, тому що кількість nonce, яке потрібно перевірити, щоб знайти відповідний хеш для видачі транзакції, не є невиправдано великим. В середньому близько 38. Таким чином, ККД для «ідеального» квантового комп'ютера матиме порядок $3^8 = 81$, що вже цілком прийнятно. Що ще більш важливо, алгоритм, який використовується в реалізації iota, структурований таким чином, що час пошуку nonce ненабагато більше часу, необхідного для інших завдань, необхідних для здійснення транзакції. Остання частина є набагато стійкішою до квантових обчислень і, отже, надає потоку набагато більший захист проти супротивника з квантовим комп'ютером в порівнянні з блочним ланцюгом (біткойн).

Починаючи з 11 липня 2016 року, протокол IOTA працює в бета версії, при цьому ряд проблем ще не вирішено. Зокрема, виділено можливий вектор атаки «великої ваги»: якщо зловмисник зможе надати своїй транзакції вагу, що перевищує кумулятивну вагу легітимного ланцюжка то він зможе провести подвійну витрату. Це може стати реальною загрозою для всієї мережі. Як контр-заходи пропонується обмеження власної ваги транзакції зверху.

1.7.13 Майнінг

IOTA має специфічну структуру, в якій замість звичного для криптовалюта блокчейна використовується так званий DAG - спрямований ациклічний граф. При даній структурі все хеші є спочатку сгенерірованни, а система не потребує майнерыв, так як функції посередників виконують самі користувачі.

1.7.14 Перспективи криптовалюти IOTA

Відразу ж варто сказати, що інтернет речей цікавий не тільки IOTA, а й великим корпораціям, в числі Samsung, Google і навіть Microsoft. Слід

розуміти, що співпрацю з деякими з них вже налагоджено. У найближчому майбутньому, адміністрація IOTA планує залучити більше великих компаній до розробки.

1.7.15 Прогнози

IOTA є однією з небагатьох довгопланових криптовалют. За прогнозами фахівців кількість з'єднань в світі «Інтернету речей» до 2020 року досягне позначки в 50 млрд, що значно позначиться на потребі користувачів в надійної білінгової мережі з транзакціями без комісій.

За заявами деяких експертів зі світу криптографії, вона має величезний потенціал, але для забезпечення масовості необхідно її розуміння, в першу чергу, з боку користувачів. Для цього було створено спеціальний підрозділ IOTA-CORE, основним завданням якого є забезпечення надійного співробітництва з компаніями по всьому світу.

1.8 Висновки

Перехід економіки на ринкові методи господарювання висуває жорсткі вимоги до достовірності і оперативності обліку електричної енергії. Ці вимоги можуть бути задоволені тільки шляхом створення автоматизованих систем контролю та обліку електроенергії.

Основна мета створення технічних АСКОЕ - максимальна автоматизація і зниження трудовитрат при отриманні точної, достовірної та оперативної інформації про енергоспоживання підприємства і його окремих підрозділів для вирішення наступних завдань:

- дотримання заданих режимів електроспоживання;
- отримання інформації про повне енергоспоживанні окремих підрозділів підприємства для визначення виробничої енергоємності продукції, що випускається;

- проведення аналізу енергоспоживання з метою розробки та ефективного впровадження організаційних і технічних заходів, спрямованих на раціональне використання енергоресурсів;
- автоматизація фінансових розрахунків з енергопостачальною організацією (при перекладі системи в розряд комерційних).

Постійне подорожчання енергоресурсів вимагає розробки і впровадження комплексу заходів з енергозбереження, що включають жорсткий контроль поставки / споживання всіх видів енергоресурсів, обмеження і зниження їх частки в собівартості продукції. Сучасна АСКОЕ є вимірювальним інструментом, що дозволяє економічно обгрунтовано розробляти, здійснювати комплекс заходів з енергозбереження, своєчасно його коригувати, забезпечуючи динамічну оптимізацію витрат на енергоресурси в умовах мінливої економічної середовища, таким чином АСКОЕ є основою системи енергозбереження промислових підприємств. Перший і найнеобхідніший крок в цьому напрямку, який треба зробити вже сьогодні, - це впровадити автоматизований облік енергоресурсів, дозволяє враховувати і контролювати параметри всіх енергоносіїв по всій структурної ієрархії підприємства з доведенням цього контролю до кожного робочого місця. Завдяки цьому будуть зведені до мінімуму виробничі і невиробничі витрати на енергоресурси, це дозволить вирішувати спірні питання між постачальником і споживачем енергоресурсів вольовими, директивними заходами, а об'єктивно на підставі об'єктивного автоматизованого обліку.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Створення мережі

Слід сформулювати вимоги, яким повинна задовольняти технологія зв'язку для її успішного застосування для вирішення поставлених завдань. З огляду на дискретний енергозберігаючий режим роботи бездротової мережі енергомоніторингу побудова P2P мережі на рівні координаторів є актуальним завданням, що вимагає оптимального рішення при реалізації блокчейн архітектури системи. Очевидно, що оптимальним варіантом з точки зору простоти і зручності було б об'єднання всіх пристроїв, що беруть участь в обміні інформацією, в єдину інформаційну мережу, яка працює в одному стандарті.

База даних є основою системи управління даними лічильників. Вона надає такі послуги як збір даних, перевірка, настройка, зберігання і розрахунок у відповідності з різними додатками, призначеними для різних груп користувачів системи. Крім того, вона повинна також забезпечувати такі функції, як віддалений доступ, підключення / відключення абонента, перевірка статусу харчування і т. д. Основне завдання системи управління даними - зробити її відкритою і досить гнучкою для інтеграції додатків і надання більш якісних послуг клієнтам при забезпеченні безпеку даних. Платформа P2P для моніторингу енергоспоживання вимагають систем зв'язку, що забезпечують її функціонування.

Також технологія зв'язку повинна забезпечувати необхідну дальність і швидкість з'єднань. А якщо взяти до уваги те, що мережа може бути доповнена новими вузлами, то від технології зв'язку потрібна можливість масштабування. Також, комунікаційна технологія повинна забезпечувати надійність і безпеку передачі інформації. Високошвидкісні технології Wi-Fi, Wi-Max, Bluetooth, Wireless USB призначені в першу чергу для обслуговування комп'ютерної периферії і пристроїв мультимедіа. Вони оптимізовані для передачі великих обсягів інформації на високих швидкостях, працюють в основному по

топології «точка-точка» або «зірка» та малопридатні для реалізації складних мереж з великою кількістю вузлів.

Протокол ZigBee - це стандарт для недорогих, малопотужних бездротових мереж з комірчастою топологією. Низька вартість дозволяє широко застосовувати дану технологію для бездротового контролю і спостереження, а завдяки малій потужності сенсори мережі здатні працювати довгий час, використовуючи автономні джерела живлення. Протокол був розроблений альянсом компаній ZigBee. Цей альянс служить органом, що визначає для ZigBee стандарти високих рівнів; він також публікує профілі додатків, що дозволяє виробникам вихідних комплектуючих випускати сумісні продукти. Нижні рівні для даного стандарту розроблені IEEE і визначаються стандартами IEEE 802.15.4-2006. протоколволодіє важливими, з точки зору застосування в даному проекті, перевагами:

- Він орієнтований на переважне використання в системах розподіленого мульти-мікропроцесорного управління зі збором інформації з інтелектуальних датчиків, де питання мінімізації енергоспоживання і процесорних ресурсів є визначальними.
- Надає можливість організації самостійну конфігурацію мереж зі складною топологією, в яких маршрут повідомлення автоматично визначається не тільки числом справних або включених / виключених на поточний момент пристроїв (вузлів), але і якістю зв'язку між ними, яке автоматично визначається на апаратному рівні.
- Забезпечує масштабованість - автоматичне введення в роботу вузла або групи вузлів відразу після подачі живлення на вузол.
- Гарантує високу надійність мережі за рахунок вибору альтернативного маршруту передачі повідомлень при відключеннях / збої в окремих вузлах.
- Підтримує вбудовані апаратні механізми шифрування повідомлень AES-128, виключаючи можливість несанкціонованого доступу в мережу.

2.1.1 Організація мережі ZigBee

ZigBee - відносно новий стандарт бездротового зв'язку, який спочатку розроблявся як засіб для передачі невеликих обсягів інформації на малі відстані з мінімальним енергоспоживанням. Фактично цей стандарт описує правила роботи програмно-апаратного комплексу, що реалізує бездротове взаємодія пристроїв один з одним.

Стек протоколів ZigBee являє собою ієрархічну модель, побудовану за принципом семиуровневой моделі протоколів передачі даних у відкритих системах OSI (Open System Interconnection). Стек включає в себе рівні стандарту IEEE 802.15.4, що відповідають за реалізацію каналу зв'язку, і програмні мережеві рівні і рівні підтримки додатків, визначені специфікацією ZigBee. Модель реалізації стандарту зв'язку ZigBee представлена на рисунку 2.1

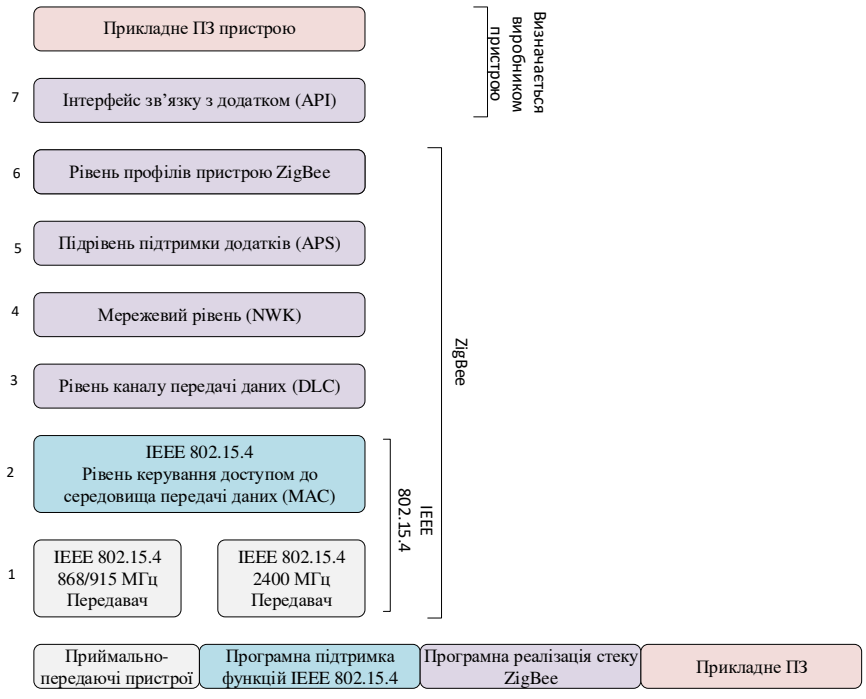

Рисунок 2.1 — Багаторівнева модель стандарту зв'язку ZigBee

Стандарт IEEE 802.15.4 визначає два нижніх рівні стека: рівень доступу до середовища (MAC) і фізичний рівень передачі даних в середовищі

поширення (PHY), тобто нижні рівні протоколу бездротової передачі даних. Альянс визначає програмні рівні стека ZigBee від рівня каналу передачі даних (Data Link Control) до рівня профілів пристроїв (ZigBee Profiles). Прийом і передача даних по радіоканалу здійснюється на фізичному рівні PHY, який визначає робочий частотний діапазон, тип модуляції, максимальну швидкість, число каналів. Рівень PHY здійснює активацію-дезактивацію приймача, детектування енергії сигналу на робочому каналі, вибір фізичного частотного каналу, індикацію якості зв'язку при отриманні пакету даних і оцінку вільного каналу.

Далі в структурі стека ZigBee слід рівень контролю доступу до середовища IEEE 802.15.4 MAC, який здійснює вхід і вихід з мережі пристроїв, організацію мережі, формування пакетів даних, реалізацію різних режимів безпеки (включаючи 128-бітове шифрування AES), 16- і 64- бітну адресацію.

Рівень MAC забезпечує різні механізми доступу в мережу, підтримку мережевих топологій від «точка-точка» до «комірчастої мережі», гарантований обмін даними (ACK, CRC), підтримує потокову і пакетну передачі даних.

Для запобігання небажаних взаємодій можливе використання тимчасового поділу на основі протоколу CSMA-CA (протокол множинного доступу до середовища з контролем несучої і запобіганням колізій).

Тимчасовий поділ ZigBee базується на використанні режиму синхронізації, при якому підлеглі мережеві пристрої, більшу частину часу знаходяться в «сплячому» стані, періодично «прокидаються» для прийому сигналу синхронізації від мережевого координатора, що дає їм змогу всередині локальної мережевої осередку знати, в який момент часу здійснювати передачу даних. Даний механізм, заснований на визначенні стану каналу зв'язку перед початком передачі, дозволяє істотно скоротити (але не усунути) зіткнення, викликані передачею даних одночасно кількома пристроями. Стандарт 802.15.4 грунтується на полудуплексной передачі даних (пристрій

може або передавати, або приймати дані), що не дозволяє використовувати метод CSMA-CA для виявлення колізій - тільки для їх запобігання.

У специфікації стека передбачені три типи пристроїв: координатор, маршрутизатор і кінцевий пристрій.

Координатор ініціює мережу, управляє її вузлами, зберігає інформацію про налаштування кожного вузла, задає номер частотного каналу і ідентифікатор мережі PAN ID, а в процесі роботи може бути джерелом, приймачем і ретранслятором повідомлень.

Маршрутизатор відповідає за вибір шляху доставки повідомлення, переданого по мережі від одного вузла до іншого, і в процесі роботи також може бути джерелом, приймачем або ретранслятором повідомлень. Якщо маршрутизатори мають відповідні можливості, вони можуть визначати оптимізовані маршрути до певної точки і зберігати їх для подальшого використання в таблицях маршрутизації.

Термінал не бере участі в управлінні мережею та ретрансляції повідомлень, будучи тільки джерелом / приймачем повідомлень.

Слід виділити підтримку складних топологій мереж. Саме за рахунок цього, при відносно малій максимальної дальності зв'язку двох прилеглих пристроїв, можливо розширити зону покриття мережі в цілому. Також цьому сприяє 16-бітна адресація, що дозволяє об'єднувати в одну мережу понад 65 тис. Пристроїв.

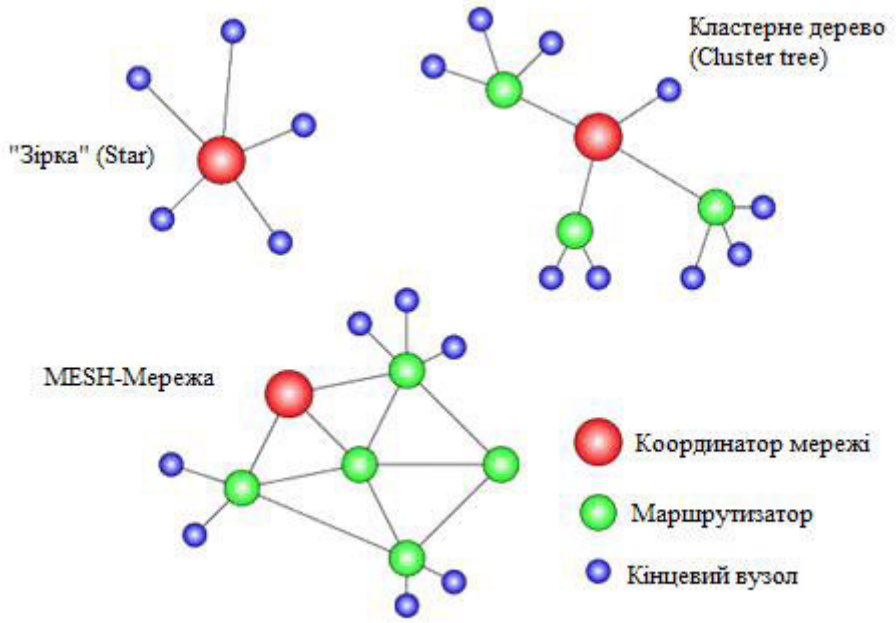

Рисунок 2.2 — Топології мереж ZigBee

Бездротові мережі на базі стандарту IEEE 802.15.4 представляють собою альтернативу проводовим з'єднанням в розподілених системах моніторингу та управління і відрізняються більш гнучкою архітектурою, вимагають менших витрат при їх установці і експлуатації.

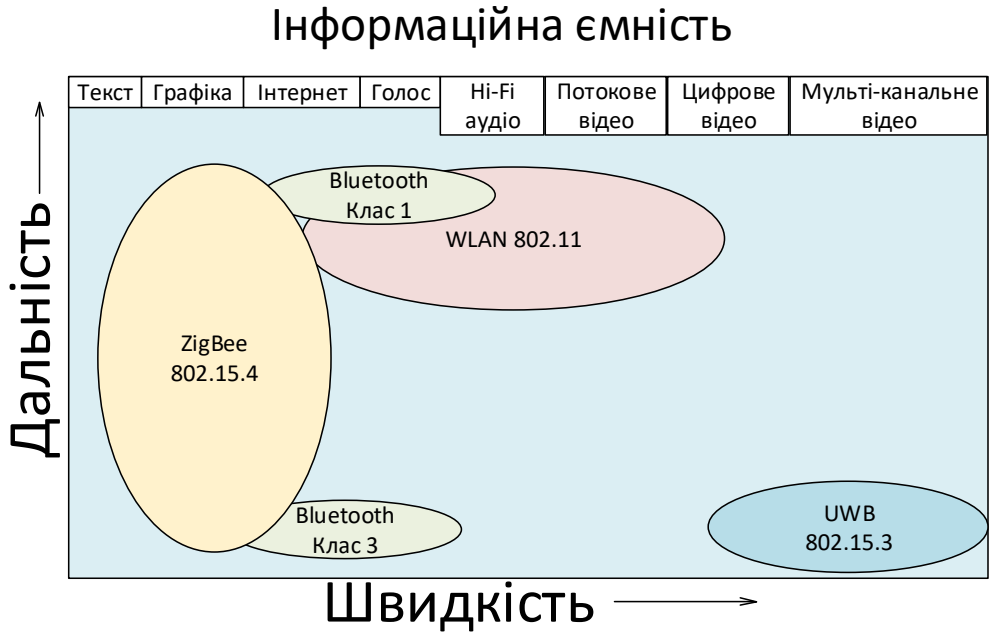

Рисунок 2.3 — Класифікація основних бездротових стандартів

Застосування технології ZigBee / 802.15.4 дозволяє розробляти бездротові інтерфейси з мінімальними витратами завдяки простоті схемотехніки, мінімальної кількості зовнішніх пасивних елементів, використання готового програмного забезпечення стека малих обсягів. Стандарт дозволяє створювати мережі з многоячейковой топологією, обслуговувати таким чином дуже велике число вузлів і збільшувати дальність зв'язку без додаткових витрат на підсилювачі потужності.

2.1.2 Специфікація стандарту IEEE 802.15.4

Специфікація ZigBee-стека визначає мережевий рівень, рівні безпеки і доступу до додатка і може використовуватися спільно з рішеннями на базі стандарту 802.15.4 для забезпечення взаємодії між різними пристроями. Специфікації стандарту IEEE 802.15.4 представлені у таблиці 1.

Таблиця 2.1 — Специфікація стандарту IEEE 802.15.4

стандарт	802.15.4 ZigBee ™		
частота	868 МГц	915 МГц	2,4 ГГц
Число каналів / крок	1 / -	10/2 МГц	16/5 МГц
Географія поширення	Європа	Америка	Увесь світ
Макс. швидкість, модуляція	20 кбіт / с, BPSK	40 кбіт / с, BPSK	250 кбіт / с, O-QPSK
Вихідна потужність, ном.	0 dBm (1 мВт)	0 dBm (1 мВт)	0 dBm (1 мВт)
дальність	10-100м		
Чутливість (специфікація)	-92dBm	-92dBm	-85dBm
Розмір стека	4-32 кбайт		
Термін служби батареї	Від 100 до 1000 і більше днів		
Розмір мережі	65536 (16-бітові адреси), 264 (64-бітові адреси)		

Глобальна специфікація ZigBee для бездротових додатків, заснована на єдиному стандарті 802.15.4, спочатку націлена і сфокусована на додатках моніторингу та контролю, розподілених мережах датчиків, на розгортанні бездротових інформаційних мереж для недорогих низькоспоживаючі систем, що використовуються в комерційній, промисловій і домашньої автоматики. Одним з основних переваг стандарту 802.15.4 / ZigBee є простота установки і обслуговування подібних систем. Особливості специфікації ZigBee дозволяють з легкістю розгортати бездротові персональні мережі: «ви просто виймаєте пристрій з коробки, вставляєте батареї і робите просту операцію на зразок натискання клавіші - тримайте два пристрої один до одного, натискаєте кнопки і тримайте до тих пір, поки не загоряться зелені світлодіоди» . Таким чином відбувається об'єднання двох пристроїв в мережу або прив'язка, наприклад, вимикача світла до певної лампі. Реалізація даного принципу передбачає впровадження ZigBee-модулів в усі нові прилади і системи. В результаті з'являється можливість створення єдиної мережі сумісних пристроїв від різноманітних виробників.

Основним способом зниження вартості кінцевого рішення ZigBee є наявність великого числа потенційних і існуючих ринків і збільшення обсягів поставок електронних компонентів від виробників. Ринок побутових пристроїв просто величезний і обчислюється мільярдами одиниць.

Вартість рішень, що базуються на стандарті 802.15.4 / ZigBee, зараз становить близько 25 $ (в ціну входять мікроконтролер, радіотрансівер, програмний стек). Однак все залежить від складових елементів схеми. Деякі рішення дозволяють використовувати вже існуючий мікроконтролер (МК) в системі, в інших додатках необхідний додатковий МК.

Створення бібліотеки єдиних профілів пристроїв, що працюють в мережі ZigBee, покликане забезпечити сумісність обладнання від різних виробників. Призначені для користувача профілі (набір сервісів, необхідний для пристроїв певного типу, наприклад систем освітлення або пожежних датчиків), що

знаходяться на самій вершині стека ZigBee, надають типові програмні модулі для використання в окремих додатках

2.1.3 Топологія мережі ZigBee

Стек ZigBee може використовувати широкий конфігурації мережі і дозволяє поєднувати пристрої за наступними топологиям: «точка-точка», «зірка», «кластерне дерево» і «многоячейковая мережу». Мережеві функції стека забезпечують сканування мережі для детектування активних каналів, ідентифікацію пристроїв на активних каналах, створення мережі на незадіяних каналах і об'єднання з існуючою мережею в зоні персональної бездротової мережі, розпізнавання підтримуваних сервісів згідно з визначеними профілями пристроїв, функції маршрутизації. Це дає їм змогу автоматично входити в мережу і виходити з неї, виключає небажані наслідки «збою в одній точці» за рахунок наявності декількох маршрутів до кожного вузла.

Головний секрет економічності полягає в тому, що вироби на основі ZigBee передають невеликі обсяги даних і працюють зі швидкістю близько 250 Kbit / s, тобто є досить повільними пристроями. Втім, для отримання даних від датчиків типу "включено / вимкнено" цього цілком вистачає. Важливіше економічність і простота пристрою - саме ці переваги забезпечують затребуваність ZigBee для повсякденного використання.

Інша особливість технології - простота масштабування мережі, що функціонує за технологією ZigBee. Без будь-яких переробок або додаткової адаптації на основі ZigBee може бути побудована мережа з декількох датчиків або створена гігантська система з багатьох сотень радіосенсеров. Для стандарту, який претендує на масовість і орієнтованого на непідготовлених користувачів, якість по-справжньому унікальне.

Мережа ZigBee - самоорганізована, і її робота починається з формування. Пристрій, призначений при проектуванні координатором персональної мережі (PAN координатор), визначає канал, вільний від перешкод, і очікує запитів на підключення. Пристрої, які намагаються

приєднатися до мережі, розсилають циркулярний запит. Поки PAN координатор - єдиний пристрій в мережі, відповідає на запит і надає приєднання до мережі тільки він. Надалі приєднання до мережі можуть надавати також приєдналися до мережі маршрутизатори. Пристрій, що одержав відповідь на циркулярний запит, обмінюється з приєднує пристроєм повідомленнями, щоб визначити можливість приєднання. Можливість визначається здатністю присоединяющего маршрутизатора обслужити нові пристрої на додаток до раніше підключеним.

2.1.4 Вступ в мережу (приєднання)

Існує два способи приєднання: MAC асоціація і повторне мережеве приєднання (NWK rejoin).

MAC асоціація доступна будь-якого пристрою ZigBee і здійснюється на MAC рівні. Механізм MAC асоціації наступний:

- Пристрій, що дозволяє приєднатися до нього, виставляє на MAC рівні дозвіл на приєднання.
- Пристрій, що вступає в мережу, виставляє на MAC рівні запит на приєднання і передає циркулярний запит маячка.
- Отримавши маячок від пристроїв, готових підключити приєднується пристрій, останнім визначає, в яку мережу і до якого пристрою воно бажає приєднатися, і виставляє на MAC рівні вимога про вступ з прапорцем «повторне приєднання» в значенні FALSE.
- Потім вступає пристрій направляє на вбрання для приєднання пристрій запит приєднання і отримує відповідь з присвоєним йому мережевою адресою.

При MAC асоціації дані передаються не зашифрованими, тому MAC асоціація не є безпечною.

Повторне мережеве приєднання всупереч назві може застосовуватися і при первинному приєднання. Воно виконується на мережевому рівні. При цьому, якщо вступає пристрій знає поточний мережевий ключ, обмін пакетами

може бути безпечним. Ключ може бути отриманий, наприклад, під час налаштування.

При повторному підключенні приєдналася пристрій виставляє на мережевому рівні запит приєднання і обмінюється з підключає пристроєм пакетами «запит приєднання» - «відповідь на запит приєднання».

2.1.5 Динаміка мережі

Крім випадків приєднання нових пристроїв структура мережі змінюється і у випадках, коли пристрої залишають мережу і повторно приєднуватися в інших місцях (це відбувається, наприклад, у разі перезавантаження пристрою).

На рисунку нижче - приклад перепідключення. Пристрій з адресою «0E3B» перепідключатися як «097D», а потім як «0260». Щоразу воно приєднується до іншого маршрутизатора і отримує адресу з наявного в розпорядженні присоединяющего маршрутизатора діапазону адрес.

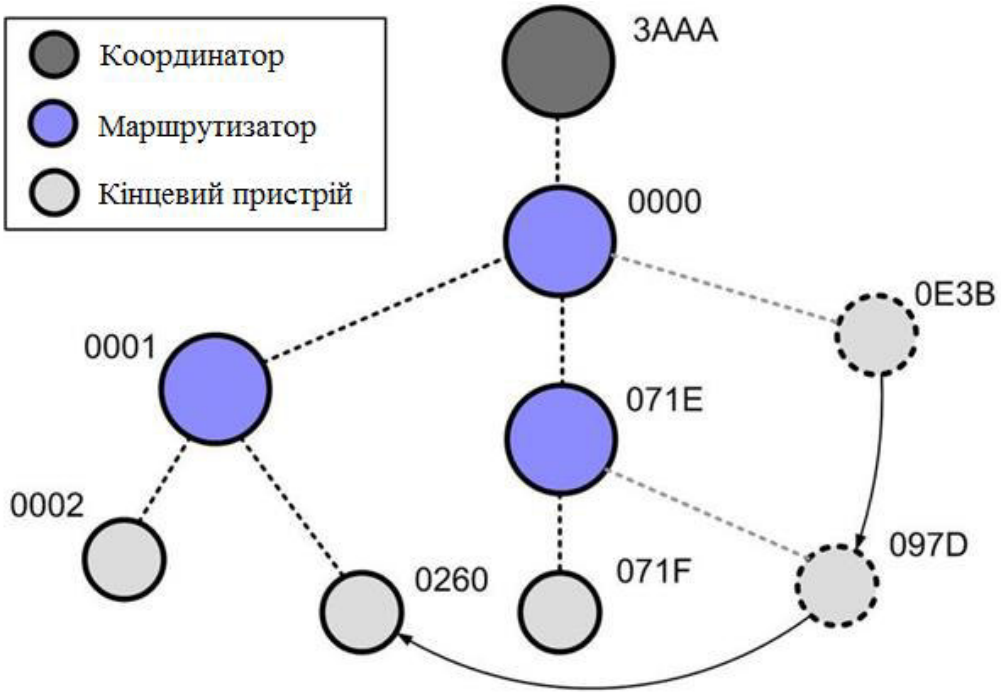

Рисунок 2.4 — Перепідключення кінцевого пристрою в деревовидної мережі [19]

2.1.6 Мережеві протоколи

Протоколи, регламентовані стандартами IEEE 802.15.4 і ZigBee 2007 Specification, забезпечують формування та функціонування бездротової сенсорної мережі. Стандарт IEEE 802.15.4 визначає фізичний і MAC рівні, а специфікація ZigBee визначає мережевий рівень і рівень додатків. На рисунку 2.5 показаний стек протоколів ZigBee.

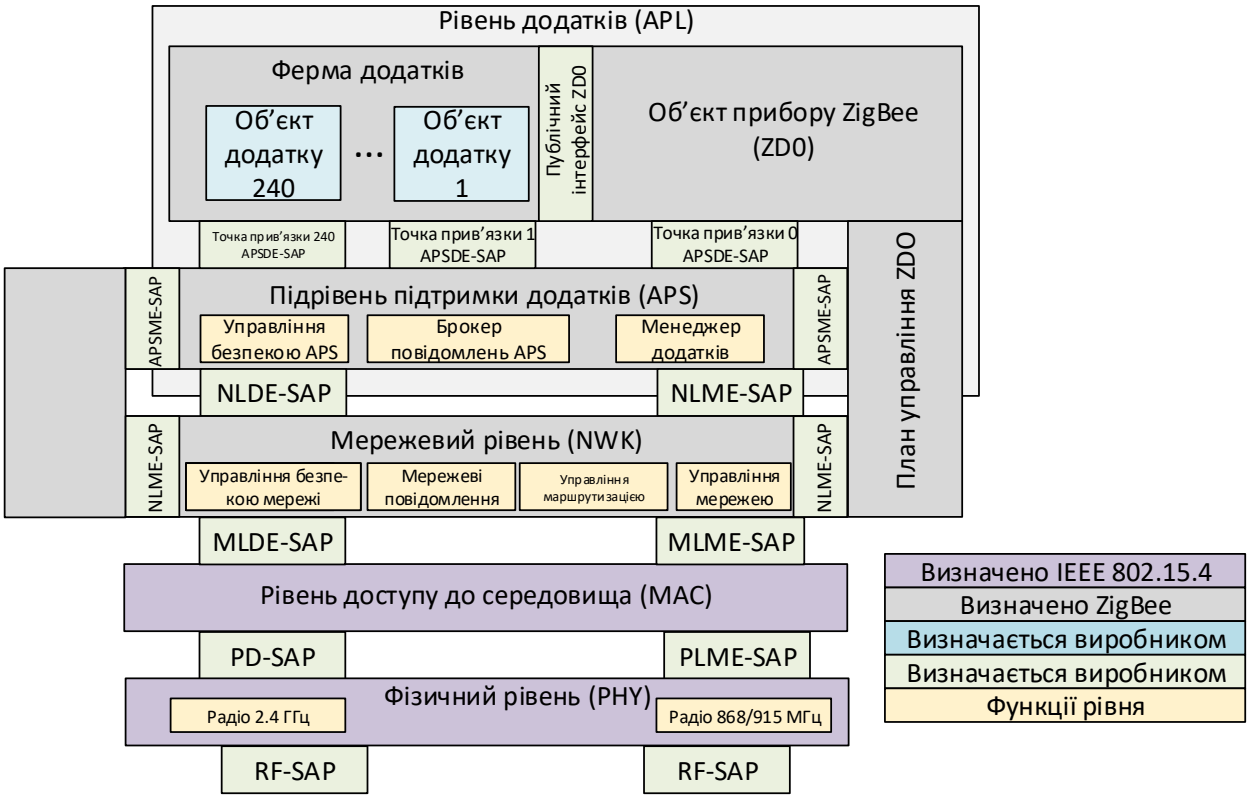

Рисунок 2.5 — Стек протоколів ZigBee [19]

2.1.7 Введення ZigBee-мережі

Радіочастотна продукція компанії MaxStream [1] добре відома світовим розробникам завдяки радіочастотним модулів XBee / XBeePro і закінченим радіомодемів діапазону 2,4 ГГц. Компанія MaxStream з 1999 року випускає виключно радіочастотні продукти для діапазонів 900 і 2400 МГц (рис. 2.6). У

2006 році компанія MaxStream була придбана компанією Digi, яка завдяки цьому посилила свої позиції на ринку бездротових пристроїв.

Рисунок 2.6 — Радіочастотні продукти MaxStream

MaxStream використовує в своїх продуктах як стандартні протоколи передачі даних (IEEE 802.15.4, ZigBee), так і власний формат передачі даних, побудований на основі протоколу з «стрибучими частотами». Ідеологія компанії - надавати споживачам радіочастотні модулі готовими до роботи «прямо з коробки». При поставці клієнту в кожен модуль встановлюється фірмове ПО від MaxStream, яке дозволяє передавати дані в прозорому режимі і керувати модулем за допомогою спрощеного набору AT-команд. Повністю готові радіочастотні модулі MaxStream дозволяють працювати із серйозною системою бездротової передачі даних навіть не досвідченому в цій області інженеру.

Компанія MaxStream з 2005 року випускає ZigBee модулі XBee / XBee-Pro Series 1, які дозволяють будувати бездротові мережі на основі стандарту IEEE 802.15.4. Модулі XBee / XBee-Pro побудовані на базі трансивера MC13193 і мікроконтролера MC9S08GT60 від компанії Freescale. Модулі XBee дуже популярні на ринку ZigBee-сумісних пристроїв, проте не мають повноцінної прошивки для побудови мережі з Mesh-топологією. У зв'язку зі змінами в апаратної частини модулів XBee / XBee-Pro Series 1, що раніше були доступні Beta-версії ZigBee прошивок (8 × 13, 8 × 14 і 8 × 17) більш не підтримуються компанією MaxStream / Digi. При цьому компанія не планує знімати модулі XBee / XBee-Pro Series 1 з виробництва. Ці модулі прекрасно підходять для побудови систем передачі 802.15. 4 з топологією «точка - точка»

або «зірка» і забезпечують більшу пропускну здатність і менші значення затримок у порівнянні з ZigBee. Компанія також надає всю необхідну інформацію по використанню модулів першої серії в якості апаратної частини для розробки систем на базі оригінального ПЗ від компанії Freescale - SMAC, 802.15.4, або BeeStack (ZigBee 2006). Порівняльні технічні характеристики модулів серії 1 і 2 наведені в таблиці 1. Велика вихідна потужність і підвищена чутливість нової серії забезпечують більшу дальність зв'язку. Струм споживання в режимі очікування знижено з 10 до 1 мкА, що дає їм змогу на батарейках працювати кілька років від одного комплекту батарей. Сьогодні в новій серії представлені тільки модулі стандартної потужності. Компанія також надає всю необхідну інформацію по використанню модулів першої серії в якості апаратної частини для розробки систем на базі оригінального ПЗ від компанії Freescale - SMAC, 802.15.4, або BeeStack (ZigBee 2006). Порівняльні технічні характеристики модулів серії 1 і 2 наведені в таблиці 1. Велика вихідна потужність і підвищена чутливість нової серії забезпечують більшу дальність зв'язку. Струм споживання в режимі очікування знижено з 10 до 1 мкА, що дає їм змогу на батарейках працювати кілька років від одного комплекту батарей. Сьогодні в новій серії представлені тільки модулі стандартної потужності. Компанія також надає всю необхідну інформацію по використанню модулів першої серії в якості апаратної частини для розробки систем на базі оригінального ПЗ від компанії Freescale - SMAC, 802.15.4, або BeeStack (ZigBee 2006). Порівняльні технічні характеристики модулів серії 1 і 2 наведені в таблиці 1. Велика вихідна потужність і підвищена чутливість нової серії забезпечують більшу дальність зв'язку. Струм споживання в режимі очікування знижено з 10 до 1 мкА, що дає їм змогу на батарейках працювати кілька років від одного комплекту батарей. Сьогодні в новій серії представлені тільки модулі стандартної потужності. Порівняльні технічні характеристики модулів серії 1 і 2 наведені на рисунку 2.7. Велика вихідна потужність і підвищена чутливість нової серії забезпечують більшу дальність зв'язку. Струм споживання в режимі очікування знижено з 10 до 1 мкА, що дає їм змогу

на батарейках працювати кілька років від одного комплекту батарей. Сьогодні в новій серії представлені тільки модулі стандартної потужності. Порівняльні технічні характеристики модулів серії 1 і 2 наведені в таблиці 1. Велика вихідна потужність і підвищена чутливість нової серії забезпечують більшу дальність зв'язку. Струм споживання в режимі очікування знижено з 10 до 1 мкА, що дає їм змогу на батарейках працювати кілька років від одного комплекту батарей. Сьогодні в новій серії представлені тільки модулі стандартної потужності.

Таблиця 2.2 — Порівняльні технічні характеристики модулів

Параметр	Xbee series 1	XBee Series 2
Дальність дії в будівлі, м	До 30	До 40
Дальність (пряма видимість), М	До 100	До 120
Вихідна потужність	1 мВт (0 дБм)	2 мВт (+3 дБм)
Швидкість у радіоканалі, біт/с	250.000	
Чутливість приймача	-92 дБм (1% PER)	-95 дБм (1% PER)
Напруга живлення, В	2.8-3.4	2.1-3.6
Ток при предачі, мА	45 (при 3.3 В)	35
Ток при прийомі, мА	50 (при 3.3 В)	38
Ток у режимі сна, мкА	<10	<1
Частотний діапазон	ISM 2,4 ГГц	
Розмір, см	2,43×2,76	
Температурний діапазон, °С	-40…85	
Варіанти антен	Чип-антена, чвертьхвильовий штир, роз’єм UFL	Чип-антена, чвертьхвильовий штир, роз’єм UFL чи RPSMA
Мережева топологія	Точка-точка, зірка	Точка-точка, зірка, Mesh
Число каналів	16 частотних каналів	
Можливості адресації	PAN ID, Channel & Source/Destination	

2.1.8 Особливості модулів XBee Series 2

Нові модулі XBee Series 2 (рис. 3) побудовані на апаратно-програмній платформі компанії Ember. Компанія Ember є промоутером ZigBee альянсу і бере активну участь в розробці специфікації ZigBee Pro. Компанія однією з перших розробила трансивер для 802.15.4 і має в своєму портфелі кілька варіантів ZigBee стека. Модулі XBee Series 2 виконані на однокристальному чипі EM-250, який являє собою трансивер IEEE 802.15.4 і 16-розрядний мікроконтролер на ядрі XAP2b со вбудованою пам'яттю 128 кбайт. Великий обсяг Flash-пам'яті дозволив розмістити в модулі як ZigBee-стек EmberZNet, так і власне ПО від MaxStream, яке надає доступ до стека ZigBee с допомогою спрощеного інтерфейсу у вигляді AT-команд, або так званих API-фреймів. Модулі XBee Series 2 сумісні по типорозміру, функцій висновків (табл. 2) і радіоінтерфейсу з модулями XBee / XBeePro, проте відрізняються набором керуючих команд і не можуть працювати в єдиній мережі. Конструктивно модулі випускаються з чотирма варіантами підключення антени - чіп-антена, антена у вигляді четвертьволнового штиря, без антени з роз'ємом UFL або RPSMA. Модулі не передбачають завантаження власного додатки розробника поверх вбудованого ZigBee-стека - для управління модулем необхідно мати зовнішній хост-процесор, в якості якого може виступати будь-який мікроконтролер - від найпростішого 8-бітного до 32-розрядної ARM або ПК. Головне управління модулем проводиться за допомогою хост-процесора з послідовного UART-інтерфейсу. Швидкість обміну задається рівною 9600 біт/с при виробництві, але може змінюватися користувачем. Порти введення / виводу доступні для хост-процесора через відповідні AT-команди (ATDx). Вбудоване ПО підтримує ряд службових функцій, реалізованих на певних висновках модуля, наприклад, світлодіод індикації успішного запуску і приєднання до мережі, кнопка для відправки повідомлення на координатор або вихід аналогової індикації рівня сигналу.

Рисунок 2.8 — Модулі XBee series 2

Таблиця 2.3 — Призначення входів та виходів модулів XBee Series 2

Вихід	Назва	Напрямок	Опис
1	VCC	-	Живлення
2	DOUT	Вихід	UART Data Out
3	DIN/CONFIG	Вхід	UART Data In
4	DIO 12	Вихід/Вхід	Цифровий вхід/вихід 12
5	RESET	Вхід	Перезапуск модуля (Сигнал довжиною не менш 200 мс)
6	PWMO/RSSI/DIO10	Вихід/Вхід	ШИМ вихід 0; індикатор потужності застосованого сигналу, цифровий вхід/вихід
7	PWM/DIO11	Вихід/Вхід	Цифровий вхід/вихід 11
8	[зарезервовано]	-	Не під’єднувати
9	DTR/SLEEP_RQ/DIO8	Вихід/Вхід	Контроль сплячого режиму або цифровий вхід/вихід 8
10	GND	-	Земля
11	DIO4	Вихід/Вхід	Цифровий вхід/вихід
12	CTS/DIO7	Вихід/Вхід	Управління обміном даними Clear-to-Send чи цифровий вхід/вихід

Продовження таблиці 2.3

13	ON/SLEEP/DIO9	Вихід	Індикатор статусу модему чи цифровий вхід/вихіід 9
14	[зарезервовано]	-	Не під’єднувати
15	Associate/DIO5	Вихід/Вхід	Ассоційований індикатор , цифровий вхід/вихід 5
16	RTS/DIO6	Вихід/Вхід	Управління обміном даними Request-to-send, цифровий вхід/вихід 6
17	AD3/DIO3	Вихід/Вхід	Аналоговий вхід 3 чи цифровий вхід/вихід 3
18	AD2/DIO2	Вихід/Вхід	Аналоговий вхід 2 чи цифровий вхід/вихід 2
19	AD1/DIO1	Вихід/Вхід	Аналоговий вхід 1 чи цифровий вхід/вихід 1
20	AD0/DIO0/кнопка ідентифікації	Вихід/Вхід	Аналоговий вхід 0, цифровий вхід/вихід 0 чи кнопка ідентифікації вузла

- Мінімально необхідна кількість виходів для прийому та передачі даних VCC, GND, DOUT, DIN
- Мінімальна кількість виходів для оновлення програмного забезпечення: VCC, GND, DIN, DOUT, RTS, DTR
- Направлення сигналу визначається відносно модуля
- Модуль має внутрішній підтягуючий резистор 30 кОм на лінії RESET
- Підтягуючі резистори на входах можна налаштувати командою ATPR
- Невикористані виходи залишають непідключеними

2.1.9 Режими зниженого енергоспоживання

Модулі XBee Series 2 можуть працювати в сплячому режимі. В цьому режимі кінцевий пристрій знаходиться в режимі низького енергоспоживання і виходить з нього при необхідності отримання або передачі даних. Робота кінцевого пристрою в стані сну підтримується його батьківським пристроєм (координатором або маршрутизатором). Батьківський пристрій зберігає RF-пакет, призначений для дочірнього пристрою, протягом максимального часу, встановленого параметром SP. Параметр SP батьківського пристрою повинен бути більше або дорівнює найбільшому з параметрів SP для всіх його дочірніх пристроїв, щоб виключити втрату даних на батьківському пристрої. Коли кінцевий пристрій «прокидається», він відправляє запит батьківського пристрою для отримання інформації про наявність очікують отримання даних. Після отримання запиту батьківський пристрій відправить кінцевому пристрою RF-відповідь і збережені дані (якщо такі дані були отримані під час сну дочірнього пристрою). Після виходу зі стану сну кінцевий пристрій кожні 100 мс буде відправляти запит батьківському пристрою для перевірки наявності нових RF-даних. Тривалість перебування кінцевого пристрою в цьому активному стані можна задавати параметром ST.

Залежно від типу, кожен пристрій має певні мережеві функції:

- координатор сканує мережу і визначає вільні канали для організації мережі;
- маршрутизатор (FFD) сканує мережу, знаходить активні канали та намагається увійти до складу існуючої мережі або створює власну персональну мережу на правах координатора, якщо немає активних каналів або не відбулося об'єднання з активною мережею. Якщо відбулося об'єднання, згідно з правилами вже існуючої мережі координатор примикає до локальної мережі та перекладається в ранг маршрутизатора і передає всю інформацію про локальної мережі координатору існуючої мережі. З сигнального пакета синхронізації від координатора новостворений

маршрутизатор отримує необхідну інформацію про тимчасові параметри мережі для виявлення наступних сигнальних пакетів;

- кінцевий RFD пристрій завжди намагається увійти всуществующую мережу.

Топологія «кластерне дерево» забезпечує масштабованість мережі і розширення зони покриття, не вимагаючи додаткових витрат на інфраструктуру. Мережа типу «кластерне дерево» може включати в себе кілька підмереж з топологією «зірка» і пристроями з обмеженими функціями (RFD). Крім топологій типу «зірка» та «кластерне дерево» технологія ZigBee підтримує многоячейковий принцип побудови мереж. При такій топології будь-який мережевий вузол може виконувати також функції маршрутизатора для інших пристроїв в мережі. Якщо виникла перешкода на шляху сигналу від одного вузла до іншого (бетонна або металева перешкода і т.п.), вибирається альтернативний маршрут для передачі даних адресату. Більш щільна концентрація мережевих вузлів призводить до більш захищеною, надійної системи. Якщо один з вузлів вийшов з ладу, маршрут автоматично визначається через інші вузли мережі, і в результаті мережа стає самовідновлювальні.

Всі вузли mesh-мережі здатні виявляти інші вузли і, розпізнавши один одного, обчислювати оптимальний шлях передачі пакетів, максимальну швидкість обміну, частоту виникнення помилок і час очікування. Розраховані значення передаються сусіднім вузлам, а оптимальний шлях передачі трафіку вибирається виходячи з потужності сигналів. Процеси виявлення вузлів і вибору шляху йдуть постійно, тому кожен вузол підтримує поточний список сусідів і при зміні їх розташування може швидко обчислити найкращий маршрут. Якщо якийсь вузол вилучається з мережі (для технічного обслуговування або внаслідок збою), сусідні вузли швидко змінюють конфігурацію своїх таблиць і заново визначають маршрути потоків трафіку.

Існує три види транзакцій передачі даних. Одна з них пов'язана з передачею даних координатору, якому передає інформацію мережеве

пристрій. Друга транзакція пов'язана з пересилкою даних від координатора до інших мережних пристроїв. До третього виду транзакцій відноситься обмін даними безпосередньо між мережевими пристроями. У топології зірка використовуються тільки дві транзакції, так як можливий інформаційний обмін тільки між координатором і мережевим пристроєм. У топології P2P можлива реалізація всіх трьох видів транзакцій.

Механізм кожного типу обмінів залежить від того, чи підтримує мережу передачу маяків. Мережі PAN з підтримкою маяків використовуються в мережах, які або вимагають синхронізації, або підтримують мережеві пристрої, що вимагають малої затримки відгуку, такі як периферія PC. Якщо мережа не потребує синхронізації або малих затримках, вона може не використовувати кадри-маяки для стандартних обмінів. Однак маяки в будь-якому випадку потрібні для відновлення мережі.

Коли мережевий пристрій хоче передати дані координатору в мережі PAN з підтримкою кадрів-маяків, воно спочатку намагається детектувати кадр-маяк (beacon). Коли маяк виявлений, пристрій синхронізується зі структурою суперкадра. У відповідний момент часу, пристрій передає свій інформаційний кадр, використовуючи доменний алгоритм CSMA-CA, координатору. Координатор може опційно підтвердити успішну доставку шляхом посилки кадру підтвердження. Дана послідовність дій відображена на рисунку 2.10.

Рисунок 2.10 — Передача даних координатору в PAN з використанням маяків (beacon)

Коли мережевий пристрій хоче передати дані в мережі PAN без підтримки маяків, він просто посилає інформаційний кадр координатору, використовуючи бездоменной схему CSMA-CA. Координатор опционно підтверджує успішну доставку даних посилкою кадру підтвердження. Дана послідовність операцій відображена на рисунку 2.11.

Рисунок 2.11 — Комунікації з координатором в PAN без міток

Коли координатор хоче передати дані мережевого пристрою в мережі PAN з підтримкою маяків, він визначає з мережевого маяка, які дані очікують відправки. Пристрій періодично прослуховує мережеві маяки (beacon), і якщо є очікує відправки повідомлення, передається MAC-команда запиту даних, з використанням доменного механізму CSMA-CA. Координатор підтверджує отримання запиту даних за допомогою відповідного кадру (ACK). З використанням доменного механізму CSMA-CA очікує відправки кадр даних пересилається, якщо можливо, то відразу після підтвердження. Пристрій може підтвердити успішне отримання даних шляхом відправки кадру підтвердження. На цьому транзакція завершується. При успішному завершенні транзакції буде видалено зі списку які мають бути надіслані, який був записаний в маяку.

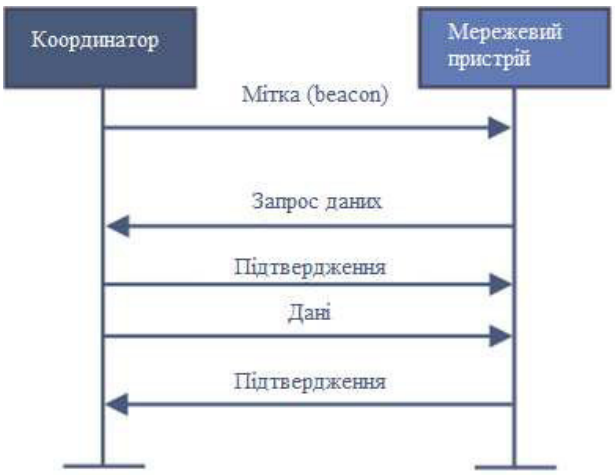

Рисунок 2.12 — Передача даних з комунікатора мережі PAN, що використовує маяки

Коли координатор хоче передати дані мережевого пристрою в мережі PAN без підтримки маяків, він запам'ятовує дані для відповідного пристрою і виконує запит даних. Мережеве пристрій може встановити контакт з координатором шляхом відправки MAC-команди запиту даних, використовуючи механізм бездоменного CSMA-CA, зі швидкістю обміну, заданої додатком. Координатор підтверджує успішне отримання інформаційного запиту за допомогою кадру підтвердження. Якщо інформаційний кадр чекає відправки, координатор посилає влаштуванню кадр даних, використовуючи бездоменной механізм CSMA-CA. Якщо кадру даних, що чекає відправки немає, координатор фіксує цей факт або в пакеті підтвердження, наступного за запитом даних, або в інформаційному кадрі з нульовою довжиною поля даних. Якщо потрібно, пристрій підтверджує успішне отримання кадру даних. Послідовність дій для даної схеми відображена на рис. 2.13.

Рисунок 2.13 — Телекомунікації з координатора в мережу PAN без маяків

Оптимізація енергоспоживання є пріоритетним завданням при побудові ZigBee мереж. Одним з рішень цього завдання є стратегія зв'язку, заснована на передачі даних лише у випадку їх надходження і подальше очікування підтвердження в разі успішного прийняття пакету з боку адресата. При цьому кожен пристрій може ініціювати передачу в будь-який момент. Очевидним недоліком даного методу є вірогідність інтерференції при одночасній передачі даних декількома пристроями. Однак можливість накладення зводиться до мінімуму завдяки вкрай малій тривалості активного циклу пристрою, випадковості моменту передачі і, як правило, невеликим обсягам, що передається.

Надійність з'єднання підвищується за рахунок використання протоколу CSMA-CA. Стратегія простого множинного доступу може бути застосована тільки до з'єднань типу «точка - точка» або «зірка». Вона підходить не всім додаткам. Для запобігання небажаної взаємодії можливе використання протоколу множинного доступу з тимчасовим поділом (TDMA). Технологія ZigBee/802.15.4 гарантує тимчасові інтервали за принципом схожим із технологією TDMA, але застосування даного поділу можливо тільки спільно з режимом синхронізації і тимчасового поділу, що є більш складним і менш енергоефективним алгоритмом в порівнянні зі звичайним TDMA-доступом. Тимчасовий поділ ZigBee базується на використанні режиму синхронізації,

при якому підлеглі мережеві пристрої, більшу частину часу знаходяться в «сплячому» стані, періодично «прокидаються» для прийому сигналу синхронізації від мережевого координатора, що дає їм змогу всередині локальної мережевої осередку знати, в який момент часу здійснювати передачу даних. Координатор керує обміном, виділяє канали та здійснює виклики з інтервалом від 15 мс до 252 сек. Передача сигнальних пакетів визначає пропускну здатність, забезпечує малий час очікування черги доступу і виділення 16 тимчасових інтервалів однакової тривалості, на кожному з яких виключені колізії в мережі.

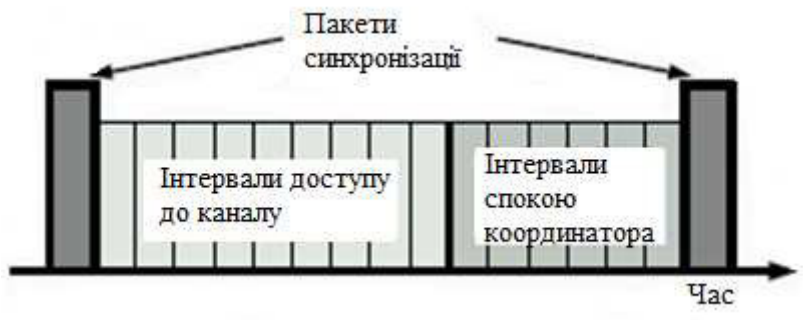

Рисунок 2.14 — Синхронізований доступ в мережу ZigBee

Часовий інтервал доступу кожного з вузлів мережі визначається або координатором, або за допомогою механізму CSMA-CA. Інтервали спокою необхідні для реалізації енергозберігаючих режимів мережевого координатора при роботі від автономного джерела живлення. Недолік - стан очікування сигналу синхронізації призводить до незначного збільшення енергоспоживання через наявність невеликих тимчасових розбіжностей, що змушує пристрою «прокидатися» трохи раніше, щоб не пропустити сигнал. Функція синхронізованого доступу застосовується в мережах з розширеною топологією, таких як «кластерне дерево» і «многоячейковая мережу».

В таблиці 2. наводяться відмінності в пересиланнях даних між координатором і вузлом мережі для випадків простого множинного доступу і доступу з функцією синхронізації. Стандартний множинний доступ може мати місце в системах безпеки і охорони будівель при організації ZigBee- мережі

різноманітних датчиків (проникнення, руху, диму і т.д.). Умовами застосування можна вважати загальний час стану спокою систем порядку 99,9%, перехід пристроїв в активний стан в псевдовипадкові моменти часу для повідомлення координатору про свою присутність в мережі. У момент датчик відразу переходить в активний стан і передає сигнал тривоги. При цьому координатор, який працює від мережі живлення, постійно знаходиться в активному стані і приймає сигнали від усіх кінцевих мережевих пристроїв.

Таблиця 2.4 — Протоколи пересилань для двох стратегій доступу в мережу

Напрямок передачі даних	синхронізований доступ	Простий множинний доступ
До координатору	очікуваний сигнальний пакет -синхронізація з мережею -Передача даних в певний момент по протоколу CSMA / CA -Підтвердження прийому	-Передача даних в момент появи даних по протоколу CSMA / CA - підтвердження прийому
від координатора	-повідомляє наявність нових даних -ожіданіе пакета даних, якщо є нові, пристрої під запитує дані в опред.інтервал часу протоколу CSMA / CA -Підтвердження отримання запиту	-Зберігання даних, поки немає запиту -посилает запит по протоколу CSMA / CA -передає підтвердження отримання запиту від пристрої. -пересилка даних

Синхронізований доступ дозволяє координатору мати автономне живлення завдяки відсутності випадкових пересилань від кінцевих пристроїв.

Реєстрація в мережі в даному випадку відбувається наступним чином:

• термінал відразу після подачі живлення чекає сигналу синхронізації від координатора існуючої мережі ZigBee (часовий інтервал очікування сигналу 0,015 ... 252 с);

• обмін первинною інформацією з координатором і очікування відповіді;

• перехід в стан спокою, «пробудження» в моменти, які визначаються координатором мережі ZigBee;

• після закінчення сеансу зв'язку з кінцевим пристроєм координатор також переходить в стан спокою.

Даний спосіб доступу передбачає незначне збільшення вартості задаючих час ланцюгів в кожному з вузлів мережі. Більш тривалі інтервали стану спокою припускають наявність точних времязадающих ланцюгів, а ранній перехід в активний стан для впевненого прийому сигнального пакета збільшує споживання електроенергії приймаючою стороною. Максимальне значення періоду синхронізації (252с) прагненням обмежити граничну точність ланцюга часу.

2.1.10 Побудова ZigBee мережі з Mesh-топологією на базі модулів XBee Series 2

В кінці 2007 року компанія MaxStream (з 2006 року входить до групи компаній Digi) випустила нові ZigBee-модулі популярної лінійки XBee. Модулі XBee Series 2 призначені для побудови повноцінної ZigBee-мережі у відповідності зі специфікаціями ZigBee-2006 і ZigBee-Pro. розглядаються особливості апаратної і програмної реалізації нових модулів, дані короткі технічні характеристики і розглянуті практичні питання організації ZigBee-мережі з Mesh-топологією (чарункова мережа, де кожен пристрій може зв'язуватися з будь-яким іншим пристроєм як безпосередньо, так і через проміжні вузли мережі, іменовані маршрутизаторами).

«Smart Energy Web-ZB» - це інноваційний продукт, що сполучає в собі новітні технології бездротових систем, що самоорганізуються та мереж з простотою монтажу та

інсталяції. Він являє собою апаратно-програмні засоби, що дозволяють будувати автоматизовані системи обліку та управління енергоспоживанням як сконцентрованих, так і віддалено розташованих побутових і дрібномоторному споживачів. Система не вимагає заміни приладів обліку споживачів, а може використовувати наявну приладову базу. «Smart Energy Web-ZB» - реалізує останню тенденцію щодо перенесення бізнес-додатків в Інтернет і відрізняється тим, що відсутня необхідність установки клієнтської частини програмного забезпечення. Відкритий для зареєстрованого користувача доступ до даних і можливість управління підключенням окремих споживачів з будь-якого, підключеного до Інтернет,

Система розроблена спеціально для дистанційного знімання показань із лічильників електроенергії в густонаселених районах (багатоквартирні житлові будинки і адміністративні будівлі) і на території приватної (котеджної) забудови.

Технологія ZigBee Smart Energy з 24 вересня 2009 року є основним стандартом для взаємодії домашніх пристроїв в рамках програм США і ЄС щодо оптимізації енергоспоживання. Чому ZigBee?

- ZigBee є єдиним глобальним стандартом бездротового зв'язку, що стимулює розвиток легко розгортаються недорогих мереж малої потужності для моніторингу і контролю.
- Застосування технології ZigBee на території України можливо без оформлення ліцензій на частоту 2,4 ГГц.
- Це бездротове рішення направлено на істотне (до 80%) скорочення витрат кінцевого користувача на розгортання системи, часу монтажу системи, робіт з технічного обслуговування і експлуатації автоматизованої системи.
- Відкритий протокол ZigBee, заснований на стандарті IEEE 802.15.4 для бездротових приватних мереж, забезпечує функціональність сьогодні і простоту інсталяції в майбутньому.
- Можливість інтеграції в Інтернет за допомогою GPRS- або прямого TCP / IP з'єднання істотно знижує вимоги до каналу передачі даних і капітальні витрати на побудову системи збору даних.

Основною областю застосування цієї технології є системи обліку енергоресурсів та управління об'єктами житлово-комунального господарства.

Основні переваги:

- Безконтактний збір даних про споживання енергоресурсів.
- Віддалене управління підключенням абонента до мережі і регулювання споживання.
- Дистанційний моніторинг балансу енергоносія по об'єкту.
- Мінімальні інвестиції в інсталяцію і простота установки.
- Істотне скорочення терміну монтажу за рахунок використання існуючої арматури.
- Відсутність неврахованих втрат енергоресурсу і підключення до системи збору даних при першому включенні.
- Можливість підключення всіх видів енергоносіїв до однієї системи Складові аспекти економічної ефективності
- Погашення або реструктуризація боргу за поставлений енергоносій безпосередньо при первинній інсталяції системи.
- Контроль несанкціонованих підключень шляхом ведення балансу.
- Зниження технічних втрат при доставці енергоносія споживачеві.
- Ліквідація комерційних втрат шляхом усунення безоблікового споживання і можливістю обмеження аж до відключення окремого абонента.
- Зниження (до 30%) загального споживання енергоресурсів на об'єкті та збільшення (до 50%) корисного відпуску.
- Можливість переведення абонента на оплату за рахунками за фактично використаний енергоносій.
- Конвертація даних в білінгову систему.

Призначення системи «Smart Energy Web-ZB»

- Автоматичне зчитування показань приладів обліку споживання електроенергії, встановлених у абонентів
- Збір свідчень за запитом оператора

- Пряме управління енергоспоживанням абонентів
- Віддалене відключення (підключення) абонента
- Оцінка небалансу і виявлення розкрадання електроенергії
- Аналіз споживання електроенергії (побудова графіків навантаження на основі 15, 30 або 60-хвилинного періоду інтеграції)
- Прийом і аналіз інформації про аварійні стани і сигналів тривоги, що надходять з місць установки лічильників і додаткових аварійних датчиків
- Обробка і зберігання даних з лічильників електроенергії і відображення отриманої інформації в зручному для аналізу вигляді

Система створена на базі специфікації ZigBee, завдяки чому легко сумісна з іншими компонентами, які використовуються в АСКОЕ енергопостачальних організацій та відкрита для подальшої модернізації і розширення.

Система підтримує роботу з усіма лічильниками електроенергії, обладнаними телеметричним або інтерфейсним виходом і включеними до Держреєстру засобів вимірювальної техніки України.

«Smart Energy Web-ZB» - комплект стаціонарного радіообладнання і програмного забезпечення для дистанційного знімання показань із лічильників електроенергії з подальшою передачею показань по Інтернет для зберігання, обробки та аналізу. Система заснована на передачі показань лічильників і сигналів управління по існуючим каналах кабельного або мобільного Інтернету. За допомогою такої системи енергопостачальні компанії можуть дистанційно вести контрактні взаємини з абонентами, реалізовувати програми управління енергоспоживанням абонентів, надавати їм розширений пакет послуг. Архітектура системи є дворівневою і дозволяє підключати до віддаленого терміналу аналізу та управління необмежене число абонентів. Файл-сервер системи дистанційно керує всією системою, двосторонній інформаційний потік містить свідчення обслуговуються лічильників і команди управління. Управління системою здійснюється з будь-

якого пристрою, що має вихід в Інтернет і встановлений веб-браузер. Архітектура системи представлена на рис.

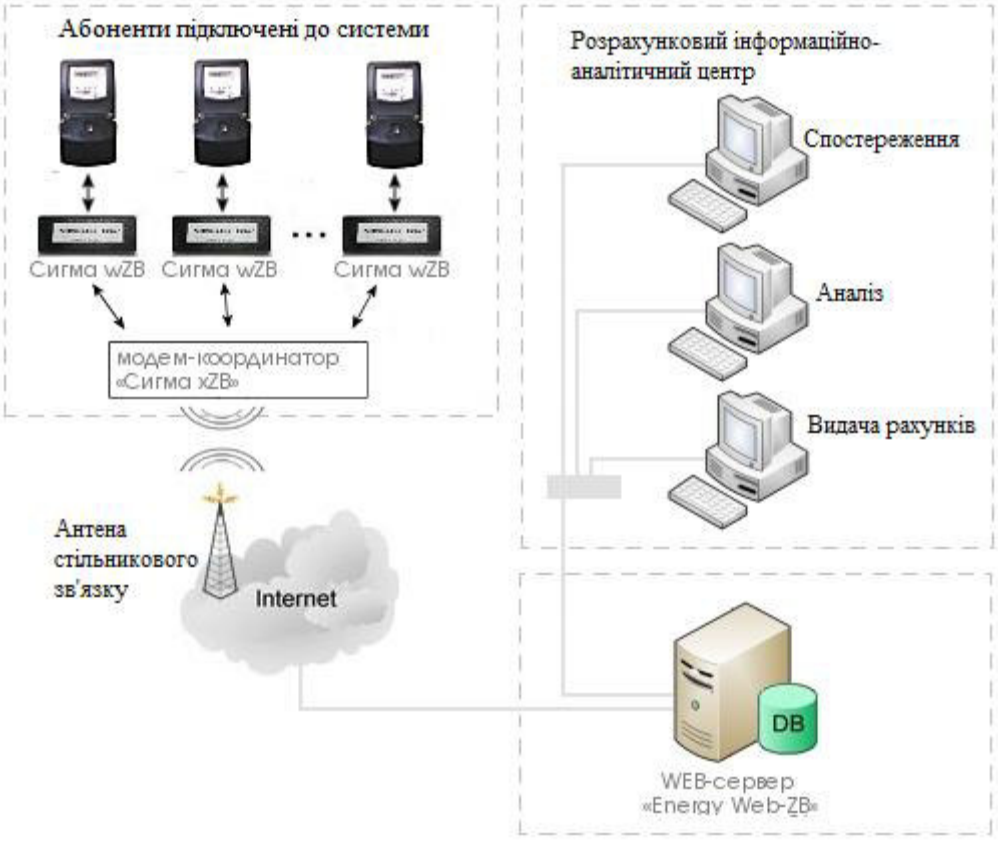

Рисунок 2.13 — Локальна мережа «Smart Energy Web-ZB»

Локальна мережа «Smart Energy Web-ZB» складається з:

- лічильників електроенергії;
- модулів зняття показань із лічильників електроенергії «Сигма wZB», які підключаються до лічильників електроенергії;
- модем-координатора «Сигма xZB», що забезпечує функції самоврядування, самовідновлення та конфігурації, і який забезпечує роботу с необмеженим числом модулів «Сигма wZB»;
- нергетичного WEB-сервера «Energy Web-ZB».

Модуль зняття показань із лічильників електроенергії та управління споживанням «Сигма wZB» призначений для збору з лічильників електроенергії інформації, її обробки і передачі в персональних бездротових мережах по протоколу IEEE 802.15.4 / Zigbee, на модем координатор.

Передана інформація містить:

- серійний номер лічильника;
- останні показання лічильника;
- показання лічильника на початок місяця;
- добові показання лічильника за поточний місяць;
- спроби зовнішнього впливу на вимірювальну схему;

Рисунок 2.14 — Лічильник електроенергії «Сигма wZB»

Технічні характеристики модуля «Сигма wZB»:

- Несуча частота: 2,4 ГГц.
- Повна відповідність стандарту IEEE 802.15.4: специфікація ZigBee.
- Радіус дії в мережі ZigBee: в приміщенні: 10 - 20 м, на відкритій місцевості: 30 - 40 м (при потужності модуля 1 мВт) або до 1200 м (при потужності модуля 7 5Мвт).
- Швидкість передавання даних в мережі ZigBee: до 115 Кб / с.
- Комунікаційний інтерфейс: імпульсний S0 вихід з МЕК 62053-31.
- Кількість датчиків, що підключаються зовнішнього впливу: 1.

• Кількість ланцюгів управління: 1.

• Використовувані RF модулі: XBee (виробництва DIGI) або ServicZB (власного виробництва).

Варіанти конструктивного виконання модуля «Сигма wZB»:

• вбудований під нижню кришку лічильника (для лічильників виробництва Компанії СЕА);

• в окремому корпусі (для лічильників інших виробників).

Модем координатор «Сигма xZB» призначений для збору з модулів «Сигма wZB» інформації і її обробки для подальшої передачі в персональних бездротових мережах по глобальній мережі Інтернет або GSM-каналам зв'язку на енергетичний WEB-сервер «Energy Web-ZB».

Технічні характеристики модем координатора «Сигма xZB»:

• Несуча частота: 2,4 ГГц.

• Повна відповідність стандарту IEEE 802.15.4: специфікація ZigBee.

• Радіус дії в мережі ZigBee: в приміщенні: 10 - 40 м, на відкритій місцевості: 30 - 1200 м.

• Швидкість передавання даних в мережі ZigBee: до 115 Кб / с.

• Джерело живлення: 220В змінного струму.

• Комунікаційний інтерфейс: GSM / GPRS.

• Антенний інтерфейс: SMA.

• Використовувані RF модулі: XBee (виробництва DIGI) або ServicZB (власного виробництва).

У енергетичному WEB-Сервері «Energy Web-ZB» застосована новітня мережева технологія SaaS (Software-as-a-Service) - програма у вигляді сервісу, з використанням Internet-технології, яка дозволяє домогтися зниження вартості корпоративних інформаційних систем.

Функції сервера:

• збір і зберігання даних енергоспоживання кожної точки обліку;

• дистанційне конфігурування кожної точки обліку та пристрої збору і передачі даних;

• управління захистом інформації;

• управління системним годинником;

• генератор звітів;

• формування XML-звітів;

• функції абонентського сервісу;

• диспетчеризації;

• ведення журналу подій.

Сервер підтримує необмежену кількість клієнтів (адміністратор, директор, користувач, споживач і т.д.). Перераховані функції реалізовані у вигляді окремих прав доступу до додатків через стандартний браузер.

Для захисту вимірювальних даних і параметрів комплексу від несанкціонованих змін передбачена багаторівнева система захисту.

Впровадження системи «Smart Energy Web-ZB» дає високий економічний ефект, який забезпечується:

• Можливістю роботи з різними електронними лічильниками і з різними інтерфейсами зв'язку, без заміни вже встановлених електронних лічильників.

• Застосуванням технології ZigBee, яка є єдиним глобальним стандартом бездротового зв'язку, що стимулює розвиток легко розгортаються недорогих мереж малої потужності для моніторингу і контролю.

• Застосування технології на території України можливо без оформлення ліцензій на частоту 2,4 ГГц.

• Відкритий протокол ZigBee, заснований на стандарті IEEE 802.15.4 для бездротових приватних мереж, забезпечує функціональність сьогодні і простоту інсталяції в майбутньому.

• Бездротове рішення з використанням технології ZB направлено на істотне (до 80%) скорочення витрат кінцевого користувача на розгортання

системи, часу монтажу системи, робіт з технічного обслуговування і експлуатації автоматизованої системи.

На основі технології ZigBee можна будувати як гібридні системи, що використовують різні типи каналів передачі даних, так і системи з передачею даних тільки по каналах ZigBee, наведемо узагальнену структурну схему автоматизованої системи енергетичного обліку.

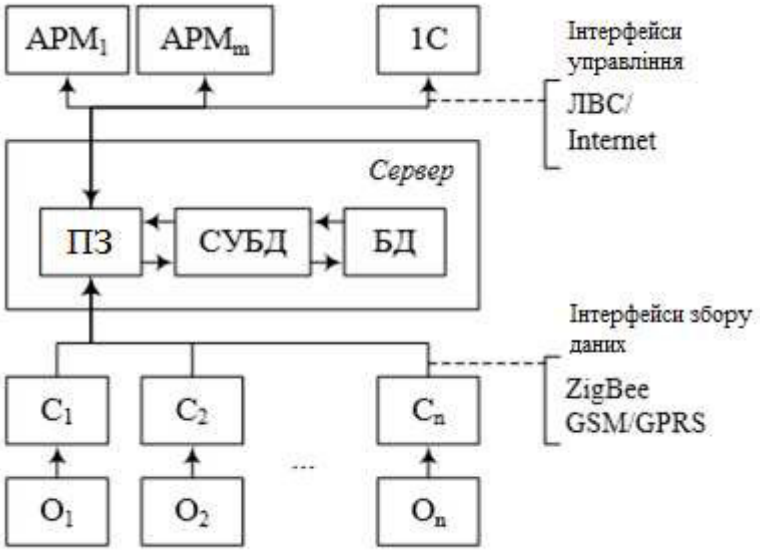

Рисунок 2.15 — Узагальнена структурна схема автоматизованої системи енергетичного обліку

Збір даних про фактичне споживання енергії може здійснюватися як з кожного лічильника С1 ... Cn, встановленого у об'єкта споживача О1 ... On, так і з модуля будинкового обліку МБО по радіоканалу стандарту ZigBee з можливістю дублювання передачі по мережі GSM / GPRS.

Кожен лічильник, що входить в систему, має персональний мережеву адресу - ID. Сучасні лічильники електричної енергії дозволяють здійснювати облік споживання по 4-6 тарифами. Збір даних з вузлів обліку виробляє проміжний приємо-передаючий пристрій (ППП). Збір може виконуватися в мобільному і в стаціонарному варіантах. При прибутті мобільного ППП (ПППм) в зону прийому автоматично виробляються настройка мережі, опитування всіх приймально-передавачів в зоні прийому, фіксація отриманих даних, з подальшою «вивантаженням» в центр збору інформації - ЦЗІ.

Процедура збору інформації займає кілька хвилин. Цей варіант може застосовуватися для збору інформації з віддалених об'єктів (котеджні селища, сільська місцевість, поодинокі споруди та ін.). Стаціонарні ППП (ПППс) встановлюються на вузлах будинкового обліку та / або точках введення в багатоквартирні будинки. ПППс здатні передавати сигнал на відстань до 4 км. Стаціонарні пристрої, що знаходяться в зоні взаємного прийому, утворюють мережу, яка дозволяє передавати дані з кожного вузла обліку безпосередньо в центр збору інформації, минаючи мобільні пристрої. Такий варіант застосовний на територіях із щільною забудовою і не вимагає наявності додаткових каналів зв'язку для передачі даних в центр. З урахуванням наведених вище функціональних особливостей наведемо структурну схему підсистеми збору даних автоматизованої системи енергообліку.

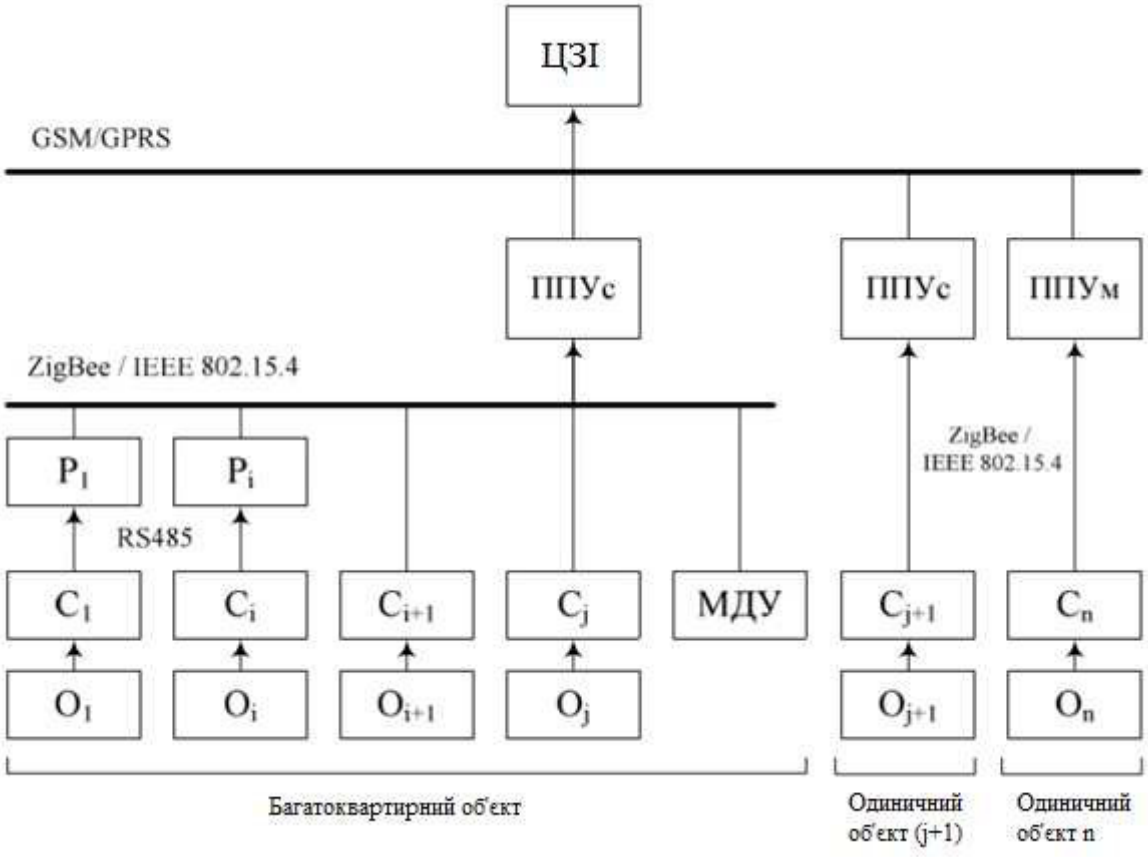

Рисунок 2.16 — Структурна схема підсистеми збору даних автоматизованої системи енергетичного обліку

Модулі Pi, Ci + 1 ... Cj, а також ПППс і ПППм дозволяють створити систему збору даних, в якій модулі виступають не тільки в якості приймачів

сигналів з досліджуваних об'єктів, але і в якості ретрансляторів сигналів інших модулів в разі, коли відстань до ППП перевищує допустиме. Бездротові модулі пов'язані з лічильниками і в той же час пов'язані між собою, таким чином, з'являється можливість знаходити найбільш короткий шлях від лічильника до ППП, а також в разі виходу з ладу якогось з модулів ретрансляторів дозволяє уникнути припинення надходження даних на ЦЗІ. У зв'язку з тим, що модулі використовуються в якості ретрансляторів, витрата енергії батарей збільшується, це необхідно враховувати при розрахунку енергоспоживання автономних модулів.

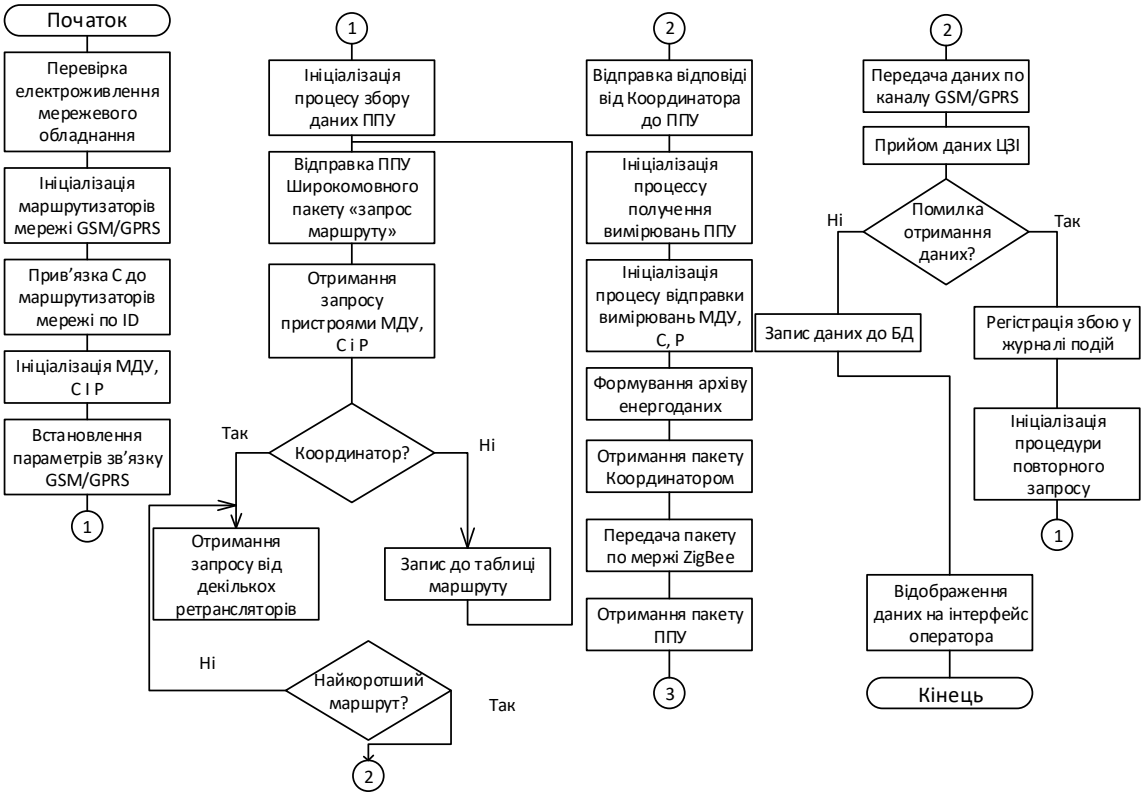

Рисунок 2.16 — Алгоритм роботи підсистеми збору даних автоматизованої системи енергетичного обліку

У процесі експериментального дослідження алгоритму збору даних на основі технології ZigBee були виявлені наступні особливості. Максимальна відстань, при якому підтримувалися найбільша допустима швидкість передачі даних в умовах відсутності прямої видимості в житловому багатоквартирному

16-поверховому будинку з залізобетонними перекриттями зі слабкими радіоперешкодами, склало 10 м, що відповідає 3 поверхах будівлі. Максимальна зона досяжності радиомодема склала 45 м, що відповідає 15 поверхах будівлі. На рис. 4 представлена залежність якості сигналу зв'язку в процентах від відстані міжмодемом координатором «Сигма xZB» і модулем «Сигма wZB». Якість сигналу зв'язку реєструється мережевим маршрутизатором ZigBee NI 9297 і відображається в програмі настройки модуля, підключеного за допомогою послідовного інтерфейсу до ПК.

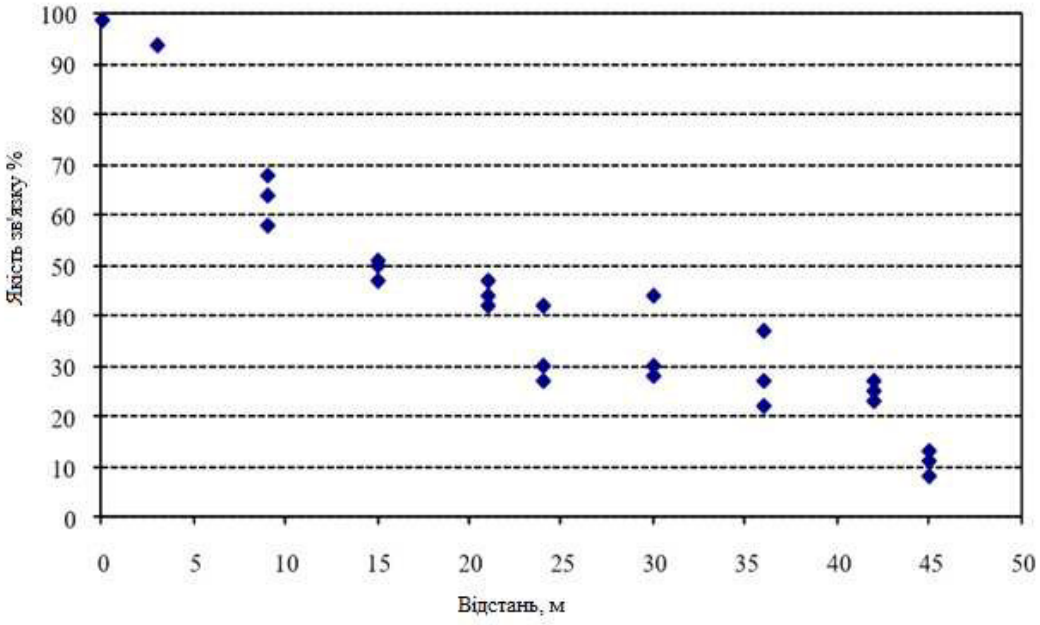

Рисунок 2.17 — Залежність рівня сигналу від відстані

Незважаючи на гнучкість мережі ZigBee, при необхідності можна розділити пристрої між декількома ППУ, знизивши навантаження і збільшивши швидкість передачі даних на ЦЗІ. Так як ППУ може підключатися не безпосередньо до конкретного ЦЗІ, а до ЛВС, то можна необмежено розширити мережу, і тоді все ППУ будуть підключені до одного й того ж ЦЗІ. Слід зазначити, що на верхньому рівні - інтерфейсів управління вирішуються контрольні та аналітичні завдання енергоспоживання. Контрольні завдання дозволяють визначити втрати, пов'язані з неповною оплатою спожитої енергії.

Аналітичні завдання дозволять більш раціонально розподіляти енергоресурси між споживачами, а також визначати місця втрат енергії.

2.2 Застосування технології блокчейн для модернізації централізованих рішень бездротових мереж моніторингу

Для успішної роботи додатків БСМ потрібно злагоджена робота і управління великою кількістю розподілених і слабо пов'язаних польових смарт-пристроїв, які ідентифікують і довіряють один одному. Хоча обрана платформа ZigBee забезпечує інтеграцію пристроїв в мережу і орієнтується на децентралізовану апаратно-програмну платформу, поточні рішення засновані на централізованій інфраструктурі. До недоліків централізованої інфраструктури відносяться, серед іншого, високі експлуатаційні витрати, низька сумісність з іншими централізованими інфраструктурами, і реальні загрози національній безпеці в окремих точках відмови, які будуть описані в наступних розділах.

Децентралізація інфраструктури БСМ дає переваги, в тому числі скорочення обсягу даних, переданих в Інтернет для обробки і аналізу, поліпшення безпеки та конфіденційності інформації. Забезпечення достовірності цих операцій означає досягнення розподіленого консенсусу з польовим пристроїв БСМ. Зараз сформувалося три принципово різних підходи до вирішення завдання передачі та обробки інформації різними платформами існуючих рішень - рішення IBM Research на базі технології Hyperledger Fabric, рішення консорціуму IOTA на базі протоколу Tangle, в основі якого лежить DAG (Directed Acyclic Graph), і технології Qubic і перспективний підхід проекту Radix, заснований на Tempo Ledger технології. Ці підходи об'єднує можливість роботи на різних апаратних засобах, а функціональна мова програмування дозволяє спростити аналіз, щоб довести правильність коду і надає великого значення паралелізму, що означає, що різні частини більшої програми можуть запускатися одночасно, щоб використовувати переваги декількох процесорів або навіть декількох пристроїв.

Proof-of-work (PoW) - механізм консенсусу вважається вельми енерговитратній технологією. З огляду на важливість (PoW) - механізму консенсусу, IBM Research розробляє новий метод реалізації цього механізму використовуючи обчислювальні потужності пристроїв Інтернету речей.

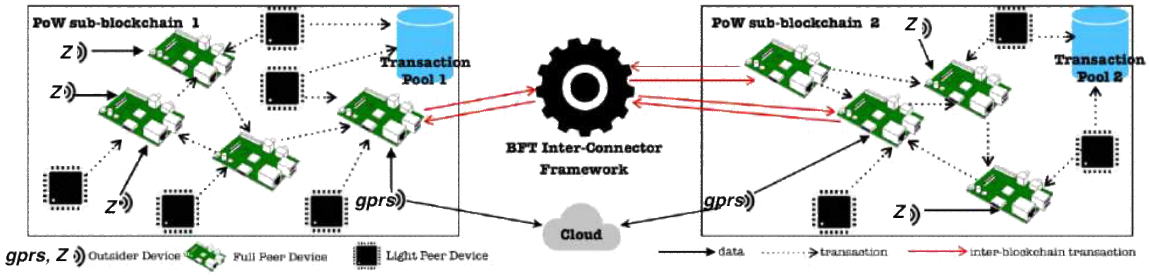

Рисунок 2.18. Гібридний БСМ-блокчейн

Однією з найбільших проблем в інтеграції blockchain в IoT є масштабованість. Через великої кількості пристроїв і обмежень ресурсів розгортання blockchain в IoT є особливо складним. Оптимальна архітектура блокової ланцюга повинна масштабироваться для багатьох пристроїв введення-виведення (вони стають одноранговими вузлами в ланцюжку блокчейна), і вона повинна обробляти високу пропускну здатність транзакцій. Hybrid-IoT, платформа, розробленаIBM Research, Використовує як блок-схеми PoW, так і протоколи Bytantine Fault Tolerant (BFT) для досягнення масштабованості. По-перше, блок-схеми PoW забезпечують розподілений консенсус серед багатьох пристроїв IoT, рівноправних вузлів блокової ланцюга в кластерному суб-блокчейне. Hybrid-IoT використовує структуру межкластерних з'єднань BFT для забезпечення взаєморозуміння між блоковими ланцюжками.

Обрана структура віртуалізованних пристроїв введення-виведення, представлених одноранговими вузлами Hybrid-IoT з різними ролями в рамках окремої блок-ланцюга PoW, доводить ефективність конструкції блокової ланцюга PoW, яка також запобігає уразливості системи безпеки.

Пристрої мережі IoT мають вкрай широкий діапазон обчислювальної потужності і енергоресурсів, а деякі з них не можуть вирішувати складні

завдання, передбачені PoW. Поділ вузлів по групах дозволяє алгоритму вирішувати, яка пропорція в кожній групі повинна здійснювати Майнінг, в залежності від обсягу енергії, використовуваної кожним вузлом. У цій моделі тільки деякі Ноди (вузли) здійснюють повне PoW.IBM виявила, що при розміщенні вузлів в кластерах по 250 од., Тільки 7% цих подблокчейнов виконували PoW, досягаючи найкращого результату з точки зору економічності, масштабування і безпеки.

IOTA, розроблена з урахуванням концепції масштабованості, представила концепцію спеціальної платформи смарт-контрактів під назвою Qubic, що працює поверх основного протоколу IOTA. Індивідуальні Qubic - це, по суті, розподілені на основі кворуму обчислювальні завдання. Qubic використовує IOTA Tangle для упаковки і поширення кубиків від їх власників до оракулів, які будуть їх обробляти. Технічно метод Tangle є ациклічним графом - це метод циклічної передачі, при якому цикли можуть виконуватися паралельно. Кубики можуть жити на Tangle в сплячому стані. Коли конкретні вхідні дані стають доступними або змінюються, вони «прокидаються» і починають обробку, що може привести до того, що каскад інших кубиків прокидається в міру появи нових результатів. Це дозволяє створити дуже динамічне середовище програмування, що дозволяє додавати нові кубики в будь-який час і прив'язувати їх до будь-яких вхідних даних. Після обробки кубика, досягнутого кворуму і результатів, відправлених в Tangle, відбуваються дві речі: qubic знову переходить в сплячий режим, очікуючи наступного зміни входів, і спрацьовує каскадний ефект, так що залежний qubic розгортаються і починають обробку з новими входами.

RADIX запропонував однорангові з'єднання вузлів з логічними годинами для генерації тимчасового докази хронологічного порядку подій. Radix домігся рішення для обох проблем таким чином, що йому не потрібен PoW (Майнінг), йому не потрібно PoS (доказ частки) і йому не потрібні головні вузли для підтвердження транзакцій.Система є безпечною, надаючи вузли з історичної записом згенерованих тимчасових доказів. RADIX DLT має лінійну

масштабованість. Це означає, що чим більше вузлів додано в мережу, тим більше вона буде масштабироваться. На відміну від поточних рішень, кожен додається вузол збільшує пропускну здатність Radix-мережі. Radix дозволить навіть обмеженим ресурсами пристроїв брати участь в якості вузлів в мережі. Вузол Radix можна буде запускати на пристрої з розміром пам'яті 16 МБ і процесором 100 МГц. Це зробить децентралізацію ще більш досконалою.

Маркери Radix (RAD) використовують децентралізовану технологію leger (DLT) для запису транзакцій. RadixDLT пропонує систему, яка покращує, хоча і відрізняється, технологію блокування з точки зору масштабованості. RadixDLT зберігає всі транзакції і замовлення в протоколі в глобальній розподіленої книзі, званої Tempo Ledger. Ця книга складається з трьох основних компонентів: до складу мережного кластера вузлів, глобальної бази даних регістрів, розподіленої по вузлах, і алгоритму для генерації криптографически безпечної записи тимчасово упорядкованих подій. [15]

2.2 Висновки

Децентралізована АСКОЕ об'єднує всі прилади обліку (лічильники), встановлені в селищі або багатоквартирному будинку в єдину структуру. Показники лічильників з певною періодичністю автоматично передаються на веб ресурс. На підставі цих даних визначається справність мереж, відсутність витоків, розраховується споживання електроенергії в кожній квартирі і виставляються рахунки мешканцям. Тут же враховуються всі платежі, внесені мешканцями в рахунок оплати за електроенергію. Всі дані можуть зберігатися досить довгий час і використовуватися для аналізу - наприклад, для побудови прогнозів споживання, визначення проблемних ділянок внутрішньобудинкової проводки і так далі. Так само можливе отримання довідки про споживання електроенергії за будь-який з минулих періодів. Крім того система може постійно в режимі реального часу зіставляти показання всіх приладів обліку (квартирних, під'їзних, загальнобудинкових), що дозволяє оперативно визначати небаланс або перевитрата енергії на певній ділянці і

вживати відповідних заходів щодо їх усунення. Можна сказати, що АСКОЕ - це молодша сестра АИИС КУЕ. Основна різниця в тому, що АИИС КУЕ встановлюється на підприємствах, які отримують енергію з оптового ринку, а АСКОЕ працює тільки в роздрібному сегменті (невеликі підприємства, комунальний сегмент, бізнес-об'єкти та ін.). Саме в житлові квартали (і селища) АСКОЕ стала проникати зовсім недавно. Сектор ЖКГ досить складний для охоплення системами енергообліку. Особливо це стосується багатоквартирних будинків. Тому, до речі, сьогодні АСКОЕ більш активно встановлюються в котеджних селищах, а не в багатоповерхівках. Через кожну точку обліку в котеджному селищі (через лічильник в котеджі) проходить більш потужний потік електроенергії, ніж через лічильник в квартирі. А значить установка АСКОЕ в котеджної забудови дозволяє отримати більш значимий (в абсолютних цифрах) ефект економії. Виділяються наступні проблеми електропостачання в котеджному селищі, з якими АСКОЕ повинна боротися: - недоврахована споживання; - підключення в обхід лічильника, прихована проводка; - несплата рахунків за електроенергію; - проблематичність або відсутність доступу контролерів до приладів обліку. Ціна АСКОЕ для житлового сектора - визначальний фактор. Створення системи дозволяє економити на кожну точку обліку порівняно небагато отже, вартість установки і експлуатації АСКОЕ не повинна перевищувати досить жорсткий ліміт. Наступний важливий момент це функціонал АСКОЕ. Дуже важливо знайти баланс між функціоналом, ціною і надійністю АСКОЕ. Що стосується функціоналу, то він може бути досить широким. Наявність АСКОЕ в житловому будинку або котеджному селищі дозволяє ліквідувати втрати в ліфтовому і насосному господарстві, налагодити раціональний графік роботи освітлення і інших внутрішньобудинкових систем. Іноді аналіз режимів споживання за місяць-два і більше - дозволяє виявити прорахунки в організації роботи внутрішньобудинкових систем (наприклад, знаходження обладнання під навантаженням без необхідності). На перше місце користувачі і виробники АСКОЕ ставлять завдання боротьби з розкраданнями і зниження втрат з вини

недообліку спожитої енергії. Якщо енергоспоживання квартир (котеджів) контролюється АСКОЕ, то вже протягом доби несправний лічильник буде ідентифіковано. Система обліку автоматично зводить баланс енергії прийшла в будинок (в селище) і врахованої лічильниками на вході в кожну квартиру. Це ж зведення балансу в сукупності з рядом прийомів дозволяє дуже оперативно припиняти спроби розкрадання енергії. Саме завдяки всім цим властивостям, АСКОЕ є ефективним інструментом енергозбереження у внутрішньобудинкових і внутрірайонних мережах. Економічний ефект залежить (крім ціни і надійності) ще і від умов експлуатації та від бажання організації, що експлуатує АСКОЕ. При цьому досить коректною формули для розрахунку економічної ефективності АСКОЕ в комунальному господарстві ще не виведено. Поки головним в оцінці є вже напрацьований досвід і думки експертів. Наявний досвід говорить, що установка системи поквартирного обліку електроенергії дозволяє знизити енергоспоживання на кілька відсотків (у виняткових випадках - до 20%). Застосування АСКОЕ в приватному секторі може знизити комерційні та технічні втрати. З 40-60% (досить поширені цифри) до 2-10%. При подібному розкладі термін окупності системи складає від 8 місяців до 1,5-2 років.

3 ЕКОНОМІЧНИЙ РОДІЛ

3.1 Мета

Метою розділу є економічне обґрунтування доцільності створення та введення в експлуатацію автоматизованної децентралізованої системи моніторингу енергоносіїв з використанням технології блокчейн.

В економічній частині дипломного проекту виконані наступні розділи: Розрахунок капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення

• Розрахунок річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування.

• Визначення річного економічного ефекту від впровадження об'єкта проектування.

• Визначення та аналіз показників економічної ефективності запропонованого в дипломному проекті проектного рішення.

• Висновок про економічну доцільність проектного рішення.

Побудова системи з використанням бездротової технології вимагає інвестицій, які в першу чергу будуть спрямовані на придбання закордонного

обладнання. Дана система модернізує існуючі системи моніторінгу енергоресурсів, доповнюючи бездротовими модулями Zigbee. Технічне обслуговування та моніторинг мережі проводитимуть місцеві кадри.

Система буде вводитися у пробному режимі для під'їзду, який включає 20 квартир. Отже для організації даної системи закуповується обладнання, на загальну суму 49418 грн.

Перелік апаратного і програмного забезпечення, необхідного для розробки пристрою, і їх вартість представлені в таблиці 3.

Таблиця 3.1 – Устаткування моніторингу мережі

Найменування	Характеристика	Вартість в гривнях
1 Ноутбук	2 Dell Inspiron 15 3567 Intel Core i3 2.3/ 4 Гб/ 1 Тб/ DVD-RW	20598
Комплект оборудований Maxstream XBee Series 2 (XB24-BPDK PBF)	20 модулей XBee Series 2 и 20 переходных плат с интерфейсами RS-232 и USB. Программное обеспечение в комплекте	28820

3.2 Визначення трудомісткості розробки та опрацювання програмного продукту

Нормування праці в процесі створення ПЗ істотно ускладнено через творчій характер праці програмістів. Проте трудомісткість розробки і опрацювання ПЗ може бути розрахована на основі системи моделей з певною точністю оцінки.

Трудомісткість створення ПЗ визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації:

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д} \quad (3.1)$$

$$t = 30 + 7 + 19 + 19 + 140 + 31 = 246 \text{ годин},$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_{д}$ – тривалість підготовки технічної документації на ПЗ.

Складові трудомісткості визначаються на підставі умовної кількості операторів у програмному продукті $\boldsymbol{Q}$.

Умовна кількість операторів у програмі:

$$Q = q \cdot c\,(1 + p) \quad (3.2)$$

$$Q = 200 \cdot 1.4\,(1 + 0.07) = 299,$$

де q – очікувана кількість операторів;

c – коефіцієнт складності програми;

p – коефіцієнт корекції програми в процесі її опрацювання.

Коефіцієнт складності програми ***c*** визначає відносну складність програми щодо типового завдання, складність якого дорівнює одиниці. Діапазон його зміни – 1,25...2,0.

Коефіцієнт корекції програми ***p*** визначає збільшення обсягу робіт за рахунок внесення змін в алгоритм або програму внаслідок уточнення технічного завдання. Його величина знаходиться в межах 0,05...0,1, що відповідає внесенню 3...5 корекцій і переробці 5-10% готової програми.

Оцінка тривалості складання технічного завдання на розробку ПЗ $t_{тз}$ залежить від конкретних умов і визначається дипломником на підставі експертних оцінок за узгодженням із керівником проекту.

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікації програміста можливо оцінити за формулою:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k} \tag{3.3}$$

$$t_в = \frac{299 \cdot 1.5}{80 \cdot 0.8} = 7 \text{ годин}$$

де B – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, B = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом - до 2 років – 0,8;

Тривалість розробки блок-схеми алгоритму:

$$ta = \frac{Q}{(20...25) \cdot k} \tag{3.4}$$

$$ta = \frac{299}{20 \cdot 0.8} = 19 \text{ годин}$$

Тривалість складання програми за готовою блок-схемою:

$$tпр = \frac{Q}{(20...25)\cdot k} \tag{3.5}$$

$$tпп = \frac{299}{20\cdot 0.8} = 19 \text{ годин}$$

Тривалість опрацювання програми на ПК:

$$tопр = \frac{1,5Q}{(4...5)\cdot k} \tag{3.6}$$

$$tопр = \frac{1,5\cdot 299}{4\cdot 0.8} = 140 \text{ годин}$$

Тривалість підготовки технічної документації на ПЗ:

$$t_{Д} = \frac{Q}{(15...20)\cdot k} + \frac{Q}{(15...20)}\cdot 0,75 \tag{3.7}$$

$$t_{Д} = \frac{299}{20\cdot 0.8} + \frac{299}{18}\cdot 0,75 = 31 \text{годин}$$

3.3 Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту *Кпз* складаються з витрат на заробітну плату виконавців програмного забезпечення *Ззп* і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК *Змч*:

$$К_{пз} = З_{зп} + З_{мч} \quad (3.8)$$

$$К_{пз} = 22890 + 624 = 23514 \text{ грн}.$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{пр} \quad (3.9)$$

$$З_{зп} = 246 \cdot 93 = 22890 \text{грн}$$

де *t* – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot С_{мч} + t_{д} \quad (3.10)$$

$$З_{мч} = 140 \cdot 4.23 + 31 = 624 \text{ грн}$$

де *tопр* – трудомісткість налагодження програми на ПК, годин;

tд – трудомісткість підготовки документації на ПК, годин;

Смч – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot С_{е} + \frac{Ф_{зал} \cdot Н_{а}}{F_{р}} + \frac{К_{лпз} \cdot Н_{апз}}{F_{р}} \quad (3.11)$$

$$C_{мч} = 0.22 \cdot 2 \cdot 1.68 + \frac{10299 \cdot 0.33}{1920} + \frac{10000 \cdot 0.33}{1920} = 4.23 \text{ грн}$$

де P – встановлена потужність ПК, кВт;

$C_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920.)

Визначена таким чином вартість створення програмного забезпечення *Кпз* є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пз} + К_{аз} + К_{н} \quad (3.12)$$

$$К = 23510 + 28820 + 48820 = 101150 \text{ грн}$$

Де $К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

3.4 Розрахунок поточних (експлуатаційних) витрат

Річні поточні (експлуатаційні) витрати на функціонування системи складають:

$$С = С_к + С_{ак} \quad (3.13)$$

$$С = 471352 + 70700=542052 \text{ грн}$$

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С = С_н + С_а + С_з + С_{єв}+ С_{ел} + С_{тос}, \quad (3.14)$$

$$С = 20000 + 33720 + 340080+ 74820 + 709 + 2023=471352 \text{ грн}$$

Де $С_н$ – витрати на навчання адміністративного персоналу й кінцевих користувачів

$С_а$ – Річний фонд амортизаційних відрахувань

$С_{єв}$ – Єдиний соціальний внесок

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} \quad (3.15)$$

$$С_з = 312000+ 28080=340080 \text{ грн}$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \quad (3.16)$$

$$С_{ел} = 0.22 \cdot 1920 \cdot 1.68=709 \text{ грн}$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$Ц_е$– тариф на електроенергію, грн/кВт·годин.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначаються у відсотках від вартості капітальних витрат (1-3%).

3.5 Оцінка можливого збитку від атаки (злому) на вузол або сегмент корпоративної мережі

Слід розрахувати величину відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), грн на місяць;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

І – число атакованих вузлів або сегментів корпоративної мережі;

N – середнє число атак на рік.

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \quad (3.1)$$

$$U = 2500 + 21530 + 1035 = 25065 \text{ грн}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \quad (3.2)$$

$$П_п = \frac{12000 + 10000}{176} \cdot 20 = 2500 \text{грн}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч} \quad (3.3)$$

$$П_в = 568 + 957 + 20000 = 21530 \text{ грн}$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ВИ} \quad (3.4)$$

$$П_{ви} = \frac{20000}{176} \cdot 5 = 568 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{ПВ} = \frac{\sum Зо}{F} \cdot t_В \quad (3.5)$$

$$П_{пв} = \frac{24000}{176} \cdot 7 = 957 \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи

із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_Г} \cdot (t_П + t_В + t_{ВИ}) \quad (3.6)$$

$$V = \frac{67200}{2080} \cdot (20 + 7 + 5) = 1035$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum_i \sum_n U. \quad (3.7)$$

$$B = 3 \cdot 16 \cdot 25065 = 1203005$$

3.6 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \quad (3.8)$$

$$E = 1203005 \cdot 0.7 - 542052 = 300051,$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

3.7 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Оцінка економічної ефективності системи захисту інформації, розглянутої у спеціальній частині дипломного проекту, здійснюється на основі визначення та аналізу наступних показників:

• сукупна вартість володіння (ТСО);

• коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

• термін окупності капітальних інвестицій $Т_о$.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K} \tag{3.9}$$

$$ROSI = \frac{300051}{101150} = 2.996$$

де Е – загальний ефект від впровадження системи інформаційної безпеки грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Оскільки організація здійснює фінансування капітальних інвестицій систему інформаційної безпеки за рахунок позикових коштів, тобто за рахунок

банківського кредиту, то в якості бажаного значення $E_н$ варто приймати величину плати за кредит (кредитної ставки) $N_{кр}$.

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину банківської кредитної ставки з урахуванням інфляції:

$$ROSI > (N_{кр} + N_{інф})/100, \quad (3.10)$$
$$2.996 > (20 + 108.9)/100$$
$$2.996 > 1.289$$

де $N_{кр}$ – банківська кредитна ставка, %;

$N_{інф}$ – річний рівень інфляції, %.

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} \quad (4.5)$$
$$T_O = \frac{1}{2.996} = 0.337 \text{ років}$$

3.8 Висновки

У ході виконання економічної частини диплому було виявлено що розробка та введення в експлуатацію системи моніторингу енергоресурсів з використанням бездротової та блокчейн технології є економічно доцільним, Оскільки загальнийекономічний ефект від впровадження системи дорівнює *300051 грн.*

Також, оскільки організація здійснює фінансування капітальних інвестицій у систему інформаційної безпеки за рахунок позикових коштів, тобто за рахунок банківського кредиту, використовуючи формулу

ROSI>($N_{кр}$+$N_{інф}$)/100 було отримане значення ROSI = 2.996, яке є більшим ніж величина банківської кредитної ставки з урахуванням інфляції (1.289). враховуючи це, та термін окупності капітальних інвестицій, який становить приблизно чотири місяці, можна вважати проект успішним, оскільки навіть при введенні в експлуатацію системи з невеликою кількістю вузлів можна спостерігати позитивний економічний ефект.

ВИСНОВКИ

ПЕРЕЛІК ПОСИЛАНЬ

1 The impact of informational feedback on energy consumption—a survey of the experimental evidence.Faruqui, A., Sergici, S., Sharif, A., 2010. Energy Vol 35, pp. 1598–1608. URL: doi.org/10.1016/j.energy.2009.07.042 (circulation date: 20.07.2017).

2 Smart meters in the Netherlands – revised financial analysis and policy advice – By order of the Ministry of Economic Affairs. KEMA, 2010 (circulation date: 20.07.2017).

3. Smart meter deployment in Europe: A comparative case study on the impacts of national policy schemes. S. Zhou, M. Brown. // Journal of Cleaner ProductionVol 144, 15 Feb 2017, pp. 22-32. URL: doi.org/10.1016/j.jclepro.2016.12.031 (circulation date: 20.07.2017).

4. Е.С.Семенистая, Н.С. Линник, А.А.Горбунов Обзор существующих схем деления систем учета расхода энергоресурсов и воды и разработка схемы деления нового типа // Инженерный вестник Дона, 2016, №4 URL: ivdon.ru/ru/magazine/archive/n4y2016/3860.

5. Е.С. Семенистая, И.Г. Анацкий, Ю.А. Бойко Разработка программного обеспечения автоматизированной системы контроля и учета энергоресурсов и воды // Инженерный вестник Дона, 2016, №4 (Електронний ресурс) / Спосіб доступу: URL:ivdon.ru/ru/magazine/archive/n4y2016/3897.

. Д.Панфилов. Введение в беспроводную технологию Zigbee стандарта 802.15.4 // Электронные компоненты. - №12. – 2004.

7. М.Соколов. Программно-аппаратное обеспечение беспроводных сетей на основе техологии Zigbee/802.15.4 // Электронные компоненты. - №12. – 2004 .

8. Семенов Ю.А. Беспроводные сети ZigBee и IEEE 802.15.4.: Михаил Крикун (Електронний ресурс) / Спосіб доступу :http://book.itep.ru/4/41/zigbee.htm.

9. Дмитриев В. Технология Zigbee// Компоненты и технологии. – №1. – 2004.

10. ZigBee/802.15.4. – Компоненты беспроводных технологий: сайт компании «Компел» (Електронний ресурс) / Спосіб доступу: http://www.compel.ru/catalog/wireless/zigbee.

11. Estimating ZigBee transmission range in the ISM band. – Electronic Design Strategy (Електронний ресурс) / Спосіб доступу: http://www.edn-europe.com/estimatingzigbeetransmissionrangeintheismband+article+1608+Europe.html.

12. IOTA Developer portal (Електронний ресурс) / Спосіб доступу: https://docs.iota.org/.

13. BitBetNEWS (Електронний ресурс) / Спосіб доступу: https://www.bitbetnews.com/prognoz-kriptovaljut/kriptovaljuta-iota-ee-perspektivy-i-prognoz-2018.html.

14. DISTRIBUTED LAB Blockchain experts (Електронний ресурс) / Спосіб доступу: https://distributedlab.com/blog/ru/main-principles-of-iota.

15. Ковальова Ю.В., Бабенко Т.В., "ЗАСТОСУВАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН В ЕНЕРГЕТИЧНИХ СИСТЕМАХ"/ VII Міжнародній науково-практичній конференції " Фізико-технологічні проблеми передавання, оброблення та зберігання інформації в інфокомунікаційних системах", Чернівці, 2018.

16 ZigBee alliance. (Електронний ресурс) / Спосіб доступу: http://www.zigbee.org.

17 Зуб М. А.: Исследование алгоритмов маршрутизации в динамических сетях на базе технологии ZigBee (Електронний ресурс) / Спосіб доступу: http://masters.donntu.org/2010/fknt/zub/diss/index.htm.

18. Прошин И.А., Егоров С.В., Шепелев М.В. АВТОМАТИЗАЦИЯ УЧЁТА ЭЛЕКТРИЧЕСКОЙ ЭНЕРГИИ КАК СРЕДСТВО ПОВЫШЕНИЯ ЭНЕРГЕТИЧЕСКОЙ ЭФФЕКТИВНОСТИ // Технические науки - от теории к практике: сб. ст. по матер. XXXIII междунар. науч.-практ. конф. № 4(29). –

Новосибирск: СибАК, 2014 (Електронний ресурс) / Спосіб доступу https://sibac.info/conf/tech/xxxiii/38004.

19. HABR Сети ZigBee. Зачем и почему? (Електронний ресурс) / Спосіб доступу: https://habr.com/post/155037/.

20 Олег Пушкарев Построение ZigBee-сети с Mesh-топологией на базе модулей XBee Series 2 (Електронний ресурс) / Спосіб доступу: http://www.wireless-e.ru/assets/files/pdf/2007_4_42.pdf.