ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

Қ.И Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті

Автоматика және ақпараттық технологиялар институты
Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚҰДАЙБЕРГЕНОВ ДӘУЛЕТБЕК МҰХТАРҰЛЫ

Блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды зерттеу

ДИПЛОМДЫҚ ЖҰМЫС

6В06201 «Телекоммуникация» білім беру бағдарламасы

Алматы 2024

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті коммерциялық емес акционерлік қоғам

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

ҚОРҒАУҒА ЖІБЕРІЛДІ
Кафедра меңгерушісі
техн.ғыл.кан
_____Е.Таштай
«30» 05 2023 ж.

ДИПЛОМДЫҚ ЖҰМЫС

Тақырыбы «Блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды зерттеу»

6В06201 «Телекоммуникация» білім беру бағдарламасы

Орындаған: Д.М.Құдайбергенов

Пікір беруші
Халықаралық ақпараттық технологиялар университеті
т.ғ.к., қауымдастырылған профессор
_____ Л.Б.Илипбаева
«28» 05 2024 ж.

Д.Ж. Утебаева, ЭТжҒТ
каф. сениор-лекторы,
т.ғ.м., PhD докторы
_____ Д.Ж.Утебаева
«19» 05 2024 ж.

Алматы 2024

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ

Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті
коммерциялық емес акционерлік қоғам

Автоматика және ақпараттық технологиялар институты

Электроника, телекоммуникация және ғарыштық технологиялар кафедрасы

6В06201 «Телекоммуникация» білім беру бағдарламасы

БЕКІТЕМІН
Кафедра меңгерушісі
тех.ғыл.кан.
_____ Е. Таштай
«___» _____ 2023 ж.

Дипломдық жұмыс орындауға
ТАПСЫРМА

Білім алушы: Құдайбергенов Дәулетбек Мұхтарұлы
Тақырыбы: «Блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды зерттеу»
Университет ректорының “ 4 ” желтоқсан 2024 ж. № 548 П/Ө бұйрығымен бекітілген
Аяқталған жобаны тапсыру мерізімі «30» 04. 2024 ж.

Жұмыстың бастапқы мәліметтері: 1. Блокчейн технологиясы. 2. ГОСТ 17363-2010 Жабдықтау тізбегінде радиожиілік сәйкестендіруді қолдану. Ультра жеңіл RFID аутентификациясын жасау жүйесін зерттеу. 3. ГОСТ 24729-2008 Заттарды басқару үшін радиожиілік сәйкестендіруді қолдану. Ультра жеңіл RFID аутентификациясын жасау жүйесін Блокчейн технологиясымен жобалау.

Дипломдық жұмыста қарастырылатын мәселелер тізімі:
а) Блокчейн технологиясының қауіпсіздік үшін қолданыс аясы мен техникалық мүмкіндіктері.
б) Ультра жеңіл RFID аутентификациясын жасау жүйесін жобалау.
Сызбалық материалдар тізімі (міндетті сызбалар дәл көрсетілуі тиіс): Блокчейн арқылы ультра жеңіл RFID аутентификациясы жобасының құрылымдық сұлбасы.

Сызбалық материалдар 20 слайдпен берілсін.

Ұсынылатын негізгі әдебиет:

1. Бельский Владимир Сергеевич, Грибоедова Екатерина Сергеевна, Царегородцев Кирилл Денисович, Чичаева Анастасия Александровна БЕЗОПАСНОСТЬ RFID-СИСТЕМ
2. Федотова Вероника Вячеславовна, Емельянов Богдан Георгиевич, and Типнер Людмила Михайловна. "Понятие блокчейн и возможности его использования" European science, no. 1 (33), 2019, pp. 40-48.
3. Шольц Юрген, Шелер Торстен, Соколов Юрий Игоревич, Коцоева Валерия Сергеевна, and Элькина Анна Андреевна. "Технология blockchain. Принципы работы и перспективы применения"

Дипломдық жұмысты (жобаны) дайындау

КЕСТЕСІ

Бөлімдер атауы, қарастырылатын мәселелер тізімі	Ғылыми жетекшіге және кеңесшілерге көрсету мерзімі	Ескерту
Диплом жұмысының тақырыбын талдау	04.01.2024 -01.02.2024	Орындалды
Теориялық ақпарат	01.02.2024 -01.03.2024	орындалды
Жабдықтар жұмысының есебі және жұмысты рәсімдеу	01.03.2024 -30.05.2024	Орындалды

Дипломдық жұмыс (жоба) бөлімдерінің кеңесшілері мен норма бақылаушының аяқталған жұмысқа(жобаға) қойған

қолтаңбалары

Бөлімдер атауы	Кеңесшілер (аты, әкесінің аты, тегі, ғылыми дәрежесі, атағы)	Қол қойылған күні	Қолы
Диплом жұмысының тақырыбын талдау	Д.Ж. Утебаева, ЭТжҒТ каф. сениор-лекторы, т.ғ.м., PhD докторы	1.03.2024	

Теориялық ақпарат	Д.Ж. Утебаева, ЭТжҒТ каф. сениор-лекторы, т.ғ.м., PhD	30.05.2024	
Норма бақылау	Досбаев Ж.М., ЭТжҒТ каф.сениор-лекторы PhD докторы	27.05.2024	

Ғылыми жетекшісі _____ Д.Ж. Утебаева
(қолы)

Тапсырманы орындауға алған білім алушы _____ Д.М. Құдайбергенов
(қолы)

Күні«_9_»_12_2024ж

АҢДАТПА

Қазіргі таңда RFID радиожиілік сәйкестендіру технологиясын әр түрлі салаларда қолдануда. Өндіріс салалары, заттарды есепке алу жағдайында, қолжеткізуді басқару, ауруханаларда науқастар туралы ақпаратты тез дәрежеде алу, жануарларды есепке алу, автотұрақтарды басқару және тағыда басқа салаларды айтуға болады. Бұл салалардың барлығы дерлік RFID карталары мен белгілердің деректерін құрылғы жадысында немесе оларға қосымша қосылған жадылық құрылғыда сақтайды. Сол себепті бұл деректерді құрылғыға тікелей қосылусыз өзгерту және өңдеуді біршама қиындатады. Бұл қиындықты шешу үшін RFID радиожиілік сәйкестендіру құрылғысынан алынатын деректерді сақтаудың балама түрлерін қарастыру ұсынылған. Олардың бірі блокчейн технологиясы.

Бұл жұмыстың мақсаты блокчейн технологиясын зерттеу, RFID технологиясы арқылы ультра жеңіл сәйкестендіру құрылғысын жасау және бұл құрылғыны блокчейн технологиясымен жобалау болып келеді.

Бірінші бөлімде блокчейн технологиясы, оның пайда болу тарихы, жұмыс жасау принципітері көрсетілген. Қолданылатын транзакциялар, олардың жүзеге асырылуы, деректерді сақтайтын блоктардың құрылуы және қолданылуы, майнерлердің блоктарды жасаудағы қолданатын дәлелі және қандай жағдайда блокчейндегі блоктар тізбегі істен шығуы мүмкіндігі сипатталады. Блокчейнді қолданатын пайдаланушылардың атқаратын рөлдері, қосылу режимдері және консенсус механизмінің алгоритмдері жазылған.

Екінші бөлімде RFID технологиясының жұмысы, қандай бөліктері бар және олардың әрекеттесуі, жүйелердің негізгі сипаттамасы және қолданылатын стандарттары, антеннамен RFID картасының арасындағы жұмыс жасайтын өрістер аймағы, RFID тегдерінің қолданатын қуат көзі бойынша түрлері, жұмыс жиіліктері мен сәйкесінше деректерді қабылдау арақашықтығы және жады түрлері жазылған. Бұл технологияның қолдану аясы көрсетілген. RFID құралын модельдеу үшін қолданылған бағдарламалар, керекті құрал-жабдықтар туралы жазылған. RFID қолжеткізу құралының шыққан нәтижесі көрсетіліп, жұмыс жасау принципі сипатталып жазылған.

Үшінші бөлімде ультра жеңіл RFID аутентификация құралын блокчейн технологиясымен жобалау көрсетілген. Жобаны модельдеу үшін қолданылған бағдарламалар және осы бағдарламада құрастырылған құрылымдық сұлбалары көрсетілген. Қолданылған құрал-жабдықтары мен компонентері жайында жазылған. Сәйкестендіру және қолжеткізу құралының жұмыс істеу алгоритмі көрсетілген. Жобаның жұмыс жасауына қажетті бағдарламаның сипаттамасы және жұмысы жазылған. Блокчейн технологиясымен жұмыс жасайтын ультра жеңіл RFID сәйкестендіру құралының моделінің суреті қосылып, RFID карталары мен тегтеріндегі деректерді жадыға жеңіл сақтау үшін ұсынылған шешімдер көрсетілген. Шыққан нәтижелері тиісінше суреттерде көрсетілген. Жобаға қажетті бағдарламалық кодттары А қосымшасына бекітілген.

АННОТАЦИЯ

В настоящее время технология радиочастотной идентификации RFID используется в различных областях. В случае обрабатывающей промышленности это управление запасами, управление поставками, быстрая информация о пациентах в больницах, учет животных, управление парковками и многое другое. Почти все эти отрасли хранят данные RFID-карт и меток в памяти устройства или на подключенном запоминающем устройстве. Вот почему немного сложнее изменять и редактировать данные без прямого подключения к устройству. Для решения этой проблемы предлагается рассмотреть альтернативные способы хранения данных с устройства RFID-радиочастотной идентификации. Одним из них является технология блокчейн.

Целью данной работы является изучение технологии блокчейн, создание сверхлегкого устройства идентификации с использованием технологии RFID и разработка этого устройства с использованием технологии блокчейн.

В первой части показана технология блокчейн, история ее появления, принципы работы. В нем описываются используемые транзакции, их реализация, создание и использование блоков, в которых хранятся данные, доказательства, которые майнеры используют для создания блоков, и при каких условиях цепочка блоков в блокчейне может выйти из строя. Описаны роли пользователей, использующих блокчейн, режимы подключения и алгоритмы механизма консенсуса.

Во второй части описывается работа RFID-технологии, какие есть части и их взаимодействие, основные характеристики систем и используемые стандарты, площадь рабочих полей между антенной и RFID-картой, типы RFID-меток. Виды по используемому источнику питания, рабочим частотам и соответственно дальности приема данных и типам памяти. Указана сфера применения данной технологии. Описано программное обеспечение, используемое для моделирования RFID-устройства, и необходимое оборудование. Показаны выходные данные устройства доступа RFID и описан принцип работы.

В третьей части показана конструкция сверхлегкого оборудования RFID-аутентификации с технологией блокчейн. Показаны программы, используемые для моделирования проекта, и структурные схемы, созданные в этой программе. Написано об используемом оборудовании и комплектующих. Показан алгоритм работы средства идентификации и доступа. Написано описание и работа программы, необходимой для работы проекта. Прилагается изображение модели сверхлегкого устройства RFID-идентификации, использующего технологию блокчейна, демонстрирующее предлагаемые решения для удобного хранения данных в памяти на RFID-картах и метках. Результаты показаны на фотографиях. Необходимые программные коды для проекта прилагаются к Приложению А.

ANNOTATION

Currently, RFID radio frequency identification technology is used in various fields. In the case of the manufacturing industry, these are inventory management, supply management, quick information about patients in hospitals, animal accounting, parking management and much more. Almost all of these industries store RFID card and tag data in device memory or on a connected storage device. This is why it is a little more difficult to change and edit data without connecting directly to the device. To solve this problem, it is proposed to consider alternative methods for storing data from an RFID radio frequency identification device. One of them is blockchain technology.

The purpose of this work is to study blockchain technology, create an ultra-lightweight identification device using RFID technology, and develop this device using blockchain technology.

The first part shows blockchain technology, the history of its appearance, and principles of operation. It describes the transactions used, their implementation, the creation and use of the blocks in which the data is stored, the evidence miners use to create the blocks, and under what conditions the block chain in the blockchain can fail. The roles of users using the blockchain, connection modes, and consensus mechanism algorithms are described.

The second part describes the operation of RFID technology, what parts there are and their interaction, the main characteristics of the systems and the standards used, the area of the working fields between the antenna and the RFID card, and the types of RFID tags. according to the power source used, operating frequencies and, accordingly, data reception range and memory types. The scope of application of this technology is indicated. The software used to simulate the RFID device and the required hardware are described. The output of the RFID access device is shown and the operating principle is described.

The third part shows the design of an ultra-light RFID authentication tool with blockchain technology. The programs used to model the project and the block diagrams created in the program are shown. Written about the equipment and components used. The algorithm of operation of the identification and access tool is shown. A description and operation of the program necessary for the project has been written. Attached is an image of a model of an ultra-lightweight RFID identification device using blockchain technology, demonstrating proposed solutions for convenient memory storage of RFID cards and tags. The results are shown in the photographs. The necessary program codes for the project are attached to Appendix A.

МАЗМҰНЫ

КІРІСПЕ

Кәзіргі уақытта цифрлық ақпарат өміріміздің барлық салаларында маңызды рөл атқарады. Осы себепті біздің цифрлық әлемде қауіпсіздік пен аутентификация мәселесі барған сайын маңызды мәселеге айналуда. Сондықтан ақпараттық қауіпсіздік пен деректер ресурстарын басқаруда тиімді шешім ретінде RFID радиожиілікті сәйкестендіру және блокчейн технологияларын қарастыру ең дұрыс қадам деп айтуға болады [1]. Блокчейн технологиясы аутентификацияда өте үлкен рөл атқара алады. Бастапқыда биткойн сынды криптавалюталардың желілеріндегі қолданылатын транзакциялардың қауіпсіздігін қамтамасыз ету үшін жасалған технология ретінде іске асырылған, кәзіргі аутентификация мен сәйкестендіруді басқару үшін әртүрлі салаларда қолданыс тапты. Блокчейн технологиясының орталықсыздандырылған желісі және үздіксіз жаңартылатын сипаты оны қауіпсіз және сенімділігі жоғары сәйкестендіру жүйелерін құруда таптырмас керемет құрал етеді [2]. Ультра жеңіл RFID аутентификациясының негізгі мүмкіндіктеріне электр тоғын төмен тұтыну мен жоғары өнімділігін айтуға болады. Бұл дегеніміз қуттандырып тұратын батареяларды ауыстыру немесе үнемі қайта зарядтауды қажет етпейтін және ұзақ уақыт жұмыс істей алатын құралды жасауға мүмкіндік береді. Осы себепті RFID сәйкестендіру құралын әртүрлі салаларда қолдануға мүмкіндік береді. Мысалы: логистика, денсаулық сақтау, көлік тұрақтарында есепке алу, заттар саудасында немесе бөлшектер саудасында тексеру және есепке алу, жануарларға арналған табу және есепке алу белгілері де бар. Логистика мен тауарды жеткізу тізбектерін басқару өнімділікті жақсартады, шығындарды азайтады, өнімдерді тиімді қадағалап сақтау орындарын басқаруға мүмкіндік береді [3]. Блокчейн технологиясын ультра жеңіл RFID аутентификациясымен бірге пайдалану сәйкестендіру мен қолжеткізуді басқару процесіне қауіпсіздік пен сенімділіктің қосымша жоғары деңгейін береді. Блокчейн әрбір орындалған транзакциялар мен сәйкестендіру орындалған туралы деректерді үздіксіз жаңартып сақтайды және басқаруға мүмкіндік береді [4].

Кәзіргі кезде көптеген салаларда радиожиілік сәйкестендіру технологиясын қолдануда, бірақ көп жерде блокчейн технологиясын қолданудың қиындықтарымен арпалас болуынан өнеркәсіпте RFID технологиясын жеңіл деректер қорына қосуды жөн көреді. Осы себепті мен RFID технологиясын блокчейн арқылы жобалауды қарастырғым келеді. Оның артықшылықтарын бағалап, ультра жеңіл әрі арзан жолын ұсынғым келеді. Осы жолда зерттеу жүргізу үшін блокчейн технологиясын қарастырып, сәйкестендіру жолдарын қарастырамын. Ультра жеңіл RFID аутентификациясын блокчейн технологиясымен жасау мақсатында ардуино микроконтроллерлері көмегімен жобалайтын боламын. Деректерді блоктарға бөлу мен қолжеткізуді басқару үшін бөліктерді басқару микроконтроллер көмегімен жүзеге асырылатын болады.

1 Блокчейн технологиясы

1.1 Блокчейн ұғымы

Қазіргі уақытта блокчейн технологиясы кең салалар мен үлкен аудиторияның назарын аударып керемет жетістіктерге әкеліп отыр. Бұл технологияны әртүрлі салаларда қолдануда: банкинг, маркетинг, медецина, жоғары оқу орындары, машина жасау секілді салаларды келтіруге болады. Оның себебі бұл технология бір орталықта басқарылмайтын және деректер мен ақпарат ағымын сақтаудағы иновациялық жүйе өз құрылымын немесе деректер қорын бөлек блоктар арқылы қалыптастырады. Бұл блоктар өзара бір-бірімен бірегей тізбекті код арқылы байланыста болады. Осы бірегей тізбектің арқасында блоктар ішінде сақталған ақпараттың дәйектілігі сақталады және оны өзгертулер мен басқа жақтан жою және манипуляциялардан сақтайды. Соның арқасында бұл технологияның сенімділігі жоғары және көп жақты қолдануға бейімді болып тұр. Блокчейн ағылшын тілінен аударғанда (blockchain – тізбектей қосылған блоктар немесе блоктар тізбегі) білдіреді. Блокчейн технологиясы – бұл деректерді бір тізбекте байлансытырылған, көптеген ақпараттық құрылғыларға таратуға болатын және деректермен ақпараттарды сақтайтын және шифрлайтын технология болып табылады. Блокчейн технологясының басты аспетілерінің бірі оның жоғары қауыпсіздігі және орталықсыздандырылуы болып табылады. Бұл оның деректерін орталықтан басқарусыз деректерді сақтауға және таратуға мүмкіндік береді және басқа жақтан көрсетілетін өзгертулерден сақтайды. Осының арқасында деректер жүйесінің ашық және сінімді жұмысы қамтамасыз етіледі, ал желі қолданушыларының арасында өзара сенім пайда болады [5].

Блокчейн технологиясы қолдану аясы өте кең салаларда дамыған, қаржы, логистика, үкімет, жоғары оқу орындары, метептер, ойын-сауық орындары, денсаулық сақтау және ауруханалар, т.б. көптеген орындарда қолданыс тапқан. Бағдарламалық қамтамасыздандыруы жағынан әдеттегі келісімдері ақпарат қорларын ұрлау, өзгерту, жоюдан сақтап басқада көрсетілетін схемалардан айналып өтіп, шартты міндеттерді орындайтын автоматтандырылған жүйелердің жаңа көкжиегіне қол жеткізеді. Блокчейн технологиясы деректерді өңдеу, қаржылық және бизнес саласындағы процестерді зерттеу және басқарудағы иновациялық және перспективалық шешімдерін болжап, жетілдіруге көмектеседі [2].

Блокчейн технологиясы арқылы ақпаратты бөлісуге, тексеруге және сақтауға мүмкіндік береді. Бұл операциялардың барлығы бір-бірімен қосылып біріктірілген блоктар арқылы жүзеге асырылады. Блокчейн технолониясы бірнеше қолданушылармен үлестірілген түрде жұмыс істейді, бұл қатысушылар немесе қолданушылар міндетті түрде бір-бірінен тәуелсіз болуы қажет. Қолданушылар бір желілік топқа қосылу үшін олар бір деңгейлі байланысты қолдана алуы тиіс. Бұрынғы клиентті серверлік архитектурадан айырмашылығы түйіндік желілердің әрқашанда бір бекітілген рөлде болмауында, олар уақыт өте келе өгеріп тұруы мүмкін. Осыған сәйкес P2P желісін қабылдау

коммуникациялық парадигма мақсаттарын дұрыс түрде қолдайтындықтан желі ішіндегі ресурстарды орталықсыздандырады және желі арқылы таратылады [6]. Бұл құрылым желі конструкциясындағы ақпаратты орталықтандыратын провайдерлер мен серверлердің болуын қолдамайды. Оның нәтижесі ретінде биліксіз орталықсыздандырылған жүйе болып табылады. Осылайша блокчейн технологиясын әртүрлі мақсаттарда қолдануға болады. Бұл технологияны бір жаңа жүйе бастамасы ретінде қолданудың алдында орталықсыздандырудың тиімді аспетілерін немесе қолданысқа қажетті жағын қарастырып алған жөн [7].

Блокчейн технологиясының дамуындағы маңызды мәселелер ретінде:

- Байланыс және ақпарат тарату, транзакция деректері. Бұл жағдайда криптографиялық сақтау ұяшықтары жоғары қауіпсіздікпен қарастырылады және реттеледі. Желі түйіндері арасында да олардың жарамдылығы және тасымалдану және сақталу тәртібі қарастырылады [5].
- Реттеліп таратылатын хаттамалар. Бұл шешімде хаттамалар белгіленген сценарии арқылы жұмыс жасайды және шешімдер шығарады. Бұл оның реттілігі мен қауіпсіздігін қамтамасыз етеді. Мұндай шешімнің алғашқы мысалы ретінде биткойнді айта кетуге болады. Биткойн 2008 жылы анонимді түрде транзакцияларды орындайтын криптовалюта ретінде ұсынылды. Биткойннің қолдану аясын блокчейн технологиясын кірістіру және қолданудың классикалық түрі деп түсіндіруге болады. Осы арқылы цифрлық, бөлінген және орталықтандырылмаған төлемдерді жүргізетін, анонимділік пен қауіпсіздікті қамтамасыз ететін блокчейндік жүйе деп қарастырылады.

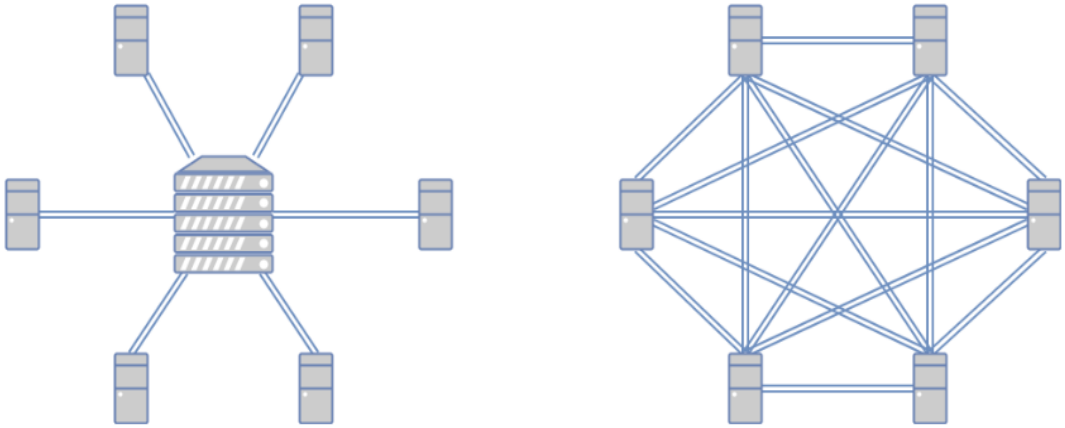
Биткойндегі блокчейн оны зиянды шабуылдардан қорғау үшін немесе басқа жақтан түсетін өзгертулерден сақтау үшін құрастырылған жүйе. Бұл жүйе ең алдымен блоктарды өзгертуші және транзакцияларды бөлуші шабуылдардың алдын алу үшін жасақталған, бірақ ол басқада аспектілерді қолдайды. Олар: толығымен анонимділік, блоктардың шағын мөлшері және жүйедегі процестердің толығымен тұрақтылығы.

Биткойн өз қолданушыларына тек псевдоним немесе лақап ат қана береді, осының арқасында анонимділік сақталады. Блоктар шағым мөлшерде бөлінеді, осы арқылы орындалатын транзакциялармен операциялардың саны шектеледі, оны орындалатын опереция лардағы бір блок немесе тексерілген транзакциялар арқылы тексереді. Биткойнның операциялар орындалуы 1 мб көлемінде шектеледі. Осылайша блоктарды блоктарды белгілі бір мөлшерде бөліп тізбектей операция орындалады. Биткойн құрылымы оны тексерулер мен қайта құрып алатын бағдарламалардан қорғап тұру немесе тексеру жұмысын қиындату үшін құрастырылған. Соның салдарынан өте жоғары қуаттылықты, энергияны қажет етеді [8].

Биткойн жағдайынан тыс қарастырғанда, блокчейн технологиясы орталықтандырылмаған ортада түпнұсқалық, тұтастық және қауіпсіздік сынды үшінші тараптағы қолданушыға артықшылықтарын қамтамасыз ету үшін бағытталғын жүйе. Бастапқы классикалық блокчейн толығымен ашық және орталықтандырылмаған жүйені құрып, жұмыс істей алады. Сонымен қатар толық бағдарламадағы кодтардың орындалуын қолдау үшін жасалған

хаттамалық өзгерістер бағдарламалық түрде қолданылатын келісімшарттар негізінде орналастыруды да жеңілдетеді [5].

Блокчейн репликацияланған таратылған дерек қоры немесе деректер сақталған, үздіксіз қосылған блоктар тізбегі деп айтуға болады. Толығырақ түсіну үшін, кәзіргі кезде IT нарықта көбіне қолданылатын желі архитектіраларын қарастыру қажет. Кәзіргі кезде қолданылатын архитектураның ең көп таралған екі түрі бар. Желі архитектурасының түрлері 1.1-суретте көрсетілген.



1.1-сурет – Желі архитектурасының түрлері

Бірінші түрі, клиент – сервер желісі. Бұл тәсілмен желі архитектурасын ұйымдастыру барлығын орталықтандырылған басқаруды білдіреді. Бұл дегеніміз, барлық деректер мен жүйелік орындалу логикасы орталық сервер ішінде орналасқан. Осы арқылы клиенттердің құрылғыларына түсірілетін жұмыс жүктемесі азаяды және өнімделігі төмендейді және деректерді өңдеудің жылдамдығы жоғары дәрежесі қамтамасыз етіледі. Бұл әдіс кәзіргі кезде кең таралған.

Екінші түрі, бір дәрежелі пирингті желі. Бұл желіні орналастыру тәсілінде барлық клиенттер орталықтандырылмаған желіде басқарушы құрылғы жок, барлық қолданушылар бірдей жәрежеде тең құқыққа ие болып келеді. Бұндай желі моделінде әрбір қолданушы немесе клиент тек тұтынушы емес, оған қоса қызмет көрсетуші бола алады. Тең дәрежелі желілердің ең бірінші нұсқасы 1990 жылы жасалған p2p қосымшасы болып келеді. Бұл қосымшаның ең танымал түрлеріне, «napster» және «bionc» файлдармен бөлісу қызметтері жатады. Сондай ақ кәзіргі кездегі деректерді бөлісудегі торрент клиенттерінің негізі болып табылатын «bittorrent» хаттамаларын қоса айтуға болады. Орталықтандырылмаған желі негізіндегі жүйелер әлі де қолданыста, бірақ қолданушы клиенттердің қажеттіліктеріне орай клиент – сервер жүйелерін қолдану әлде қайда жиірек болып келеді [2].

1.2 Блокчейн технологиясының пайда болу тарихы

1991 жылы Стюарт Хабер және Скотт Сторнет ғалымдары орталықтандырылмаған және бәріне ашық деректер қорын құру туралы жазбалары шығады. Ол құжаттардың ішінде өзгермитін ақпарат – деректер қоры және орталықтардырылмаған деректер базасының іргелі принциптері беріледі, деректерді жинау қорының дәйекті сұлбасы сипатталады. Осы жұмыстың патенті 2004 жылға дейін беріледі.

2008 жылдың қаңтар айында криптография тақырыпшаларында ең бірінші биткойн жайлы мәлімет пайда болады. Ол құжаттың авторы «Сатоси Накамото» сынды есіммен шыққан адам болды. Ол өз жұмысында криптовалютаның, дәлірек айтқанда биткойнның жұмыс істеу принциптері мен блокчейн технологиясының жұмысын жазған болатын. 2009 жылдың басында ең бірінші блокчейн проект ашылған болатын. Ол проектті Накамото бастап блоктарды генерациялауға арналған тұңғыш бағдарлама шығарды [9].

2013 жылы осы проектке ұқсас блокчейн технологиясын қолданатын криптовалюталық проекттер шыға бастады. Мысалы: Ncoin және Litecoin. Осы арқылы блокчейнді қолданудың басқада жолдары пайда бола бастады.

2015 жылы Ethereum проектінің бастамасы болды. Бұл проекттің арқасында блокчейнді қолданудың жаңа функционалды деңгейге көтерді, жаңа смарт қосымшаларды қолдануға мүмкіндік берді. Жаңа орталықсыздандырылған бағдарламаны қолданысқа шығарды. (Dapps) бағдарламасы арқылы көптеген смарт қолданушылардың назарын аударды.

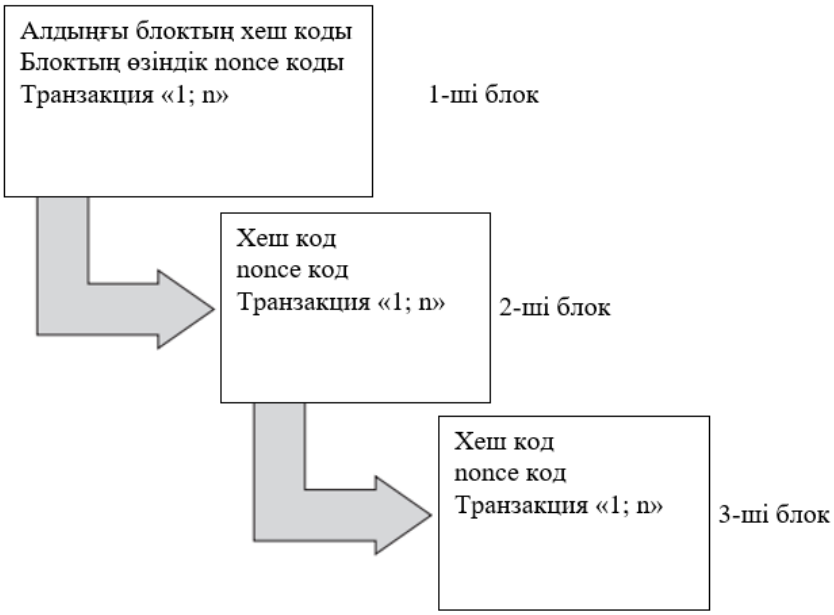
2018 жылы көптеген блокчейн проетілердің дамуы басталды. Осы аралықта блокчейнді әртүрлі өнеркәсіп салаларында дами бастады. Ол салалардың ішіне қаржы, логистика, басқармалар, денсаулық сақтау орнидары, оқу орындары, тағыда басқалары жатады.

Кәзіргі таңда блокчейн технологиясы көптеген салалардың назарын аударып келеді және бұл технологияны жаңа иновацияларға бастамасы ретінде қолданады [10].

1.3 Блокчейн технологиясының жұмыс істеу принциптері

Кәзіргі таңда блокчейн технологиясына негізделген, кең таралған және әрбір бөлімі мұқият құжатталған жүйе болып биткойнді айтуға болады. Блокчейн технологиясы биткойн пирингті төлеу жүйесінің негізі болып табылады. «Блокчейн технологиясы. жұмыс принциптері және қолдану аясы» мақаласында блокчейн технологиясының жұмысын биткойн жүйесі арқылы түсіндіріледі. Бұл жүйеде жаңа блоктарды құру үшін «майнинг» технологиясы қолданылады. (Майнинг – деп жүйедегі пайдалы ресурстарды табу, өндіруді айтады). Майнинг процесінде «nonce – number used once» шамасы алынады, бұл шама уақыт аралығы көрсетілген бір реттік сандық код түрінде болады. Осы арқылы блоктың хеш коды алынады. Nonce шамасымен алынған блоктарды

бұзып алып жүйеге шабуыл жасау үшін үшінші тараптағы қолданушы зиянкестерде, жүйе қолданушылардың ақпараттық құрылғыларының 51 пайызына сәйкес есептеу қуаты бар ақпараттық құрал қажет болады. «51 пайыздық шабуыл» термині осыдан шыққан деп айтуға болады. Майнинг немесе жаңа блокты шығару кезінде орындалған жұмыстың дәлелі ретінде консенсус алгоритмінің «pow» хаттамасы қолданылады. Әрбір блок өзіне жазылған деректерден басқа алдыңғы блоктың хеш коды мен өзінің nonce кодын қамтиды [11].



1.2-сурет – Блокчейн технологиясы арқылы блоктар тізбегінің құрылу сұлбасы

Блокчейн технологиясының функциясын қолдану, блоктағы жазылған деректерді өзгерту барлық кейінгі тұрған блоктардың хешінің өзгеруіне алып келеді. Осылайша блоктардағы жазылған деректерді өзгертуден сақтайды. Блокчейн технологиясы арқылы блоктар тізбегінің құрылу сұлбасы 1.2-суретте көрсетілген.

Қолдану аясына қарамастан блокчейн технологиясының келесі функциялары қолданылады.

- өзгерістерді растау, деректерді жазу және кейіннен сақтау.
- мәліметтерді рұқсатсыз өзгертуден қорғау.
- деректермен «тікелей», ортадағы үшінші тарапсыз, қосымша шығындарсыз алмасу мүмкіндігі.
  желіге қатысушылар арасындағы ашықтықты қамтамасыз ету.

Биткойн ең көп тараған және жақсы зерттелген блокчейн негізіндегі жүйесі болғанымен де, оның көптеген кемшіліктері байқалады:

Биткойн қаражатын ұстап тұрған қолданушы аккаунтының құпия сөзін жоғалту барлық биткоин қаражат жинақтарын жоғалтуға алып келеді.

Биткойн әмиянының құпия сөзін қалпына келтіру немесе өзгерту мүмкін емес, сол себепті құпия сөзді өзіндік қолдануышының көшіріп алуы арқылы ғана жүзеге асырылады.

Транзакцияның төмен жылдамдығы, транзакцияны тексеру, есептеу және оған арнайы жаңа блок құру көп уақыт алады. Ең үлкен транзакцияны аяқтау уақыты 5 сағатқа дейін созылуы мүмкін

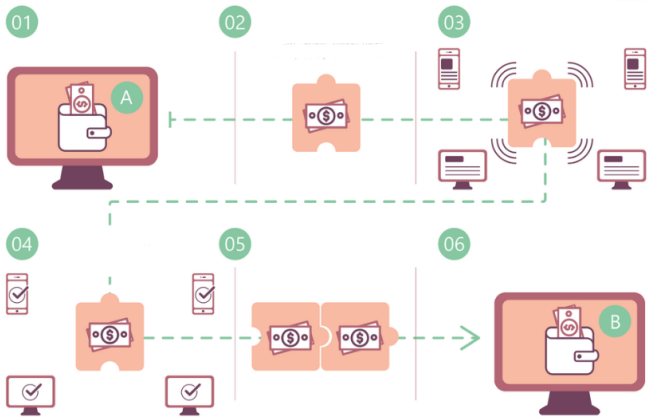
Биткойн транзакцияларының коды ашық түрде шығарылады, сол себепті үшінші тараптағы қолданушы жүйеге зиян тигізу ықтималдығы пайда болады.

Шағын дәрежедегі ықтималдылыққа қарамастан, 51 пайыз шауылы биткойн сұранысы мен айырбас бағасына кері әсер тигізуі мүмкін.

Блокчейн деректері анонимді емес болып келеді. Бұл дегеніміз транзакциядағы әмияннның хеш коды жалпыға ортақ көрінуі мүмкін [12].

Менің ойымша жоғарыда айтылған блокчейн технологиясының кемшіліктеріне сүйене келе, оның танымалдылығы мен қол жетімділігіне қарамастан, бұл технологияны қызмет көрсету, өнер кәсіп немесе бизнес сегментінде қолдану мүмкіндігі өте төмен дәрежеде деген ойдамын.

Биткойнді ең қарапайым ақша бірліктерін алмастыру жүйесі ретінде қарастырғанның өзінде бір шама кемшіліктер байқалады. Дәлірек айтқанда, тұрақсыз айырбас бағасы, биткойн жаңа технология болғандықтан оның құны әр дайым тұрақты емес болып келеді. Биткойн жүйесі оған ұзақ мерзімде инвестиция жасауға болмайтындай етіп жасалған, себебі биткойн шегі 21 миллионға жеткенде тоқтатылатындай етіп жасалған. Шегіне жеткен кезде озіндік тұрақты бағасы шығады деп ойлаймын. Кәзіргі таңда оның безгісіз күйі оның қолдануы аясын шектеп отыр, оның себебі банктік бірлестіктер оның не екенін және қалай реттеуге болатындығын білмейді. Жалпыға қолжетімді айырбастау нүктесінің жоктығы, оны қарапайым ақшаға айырбастауын шектейді. Бұл операциялардың барлығы бір платформа арқылы ғана жүзеге асырылатындығында болып тұр [11].

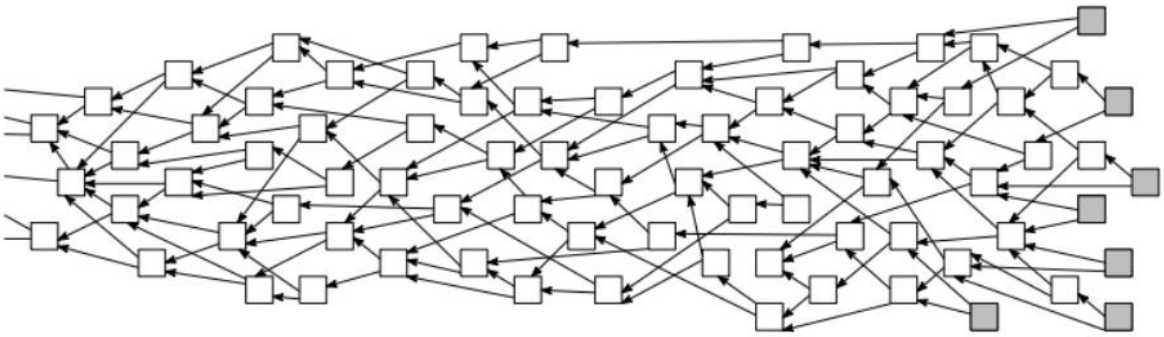


1.3-сурет – Криптовалюта негізіндегі блокчейннің жұмыс істеу принципі

1.3-суретте криптовалюта негізіндегі блокчейннің жұмыс істеу принципі көрсетілген. Ең алдымен жүйе қолданушысы, мысалы «Дәулетбек» екінші жүйе

қолданушысына «Алишерге» ақша жібермекші. Бұл транзакция желіге жіберіліп блок түрінде жиналады. Бұл блок транзакция деректері, өзіндік бір реттік код және алдыңғы блоктың хеш нөмірін қамтиды. Жиналған блоктар жүйе қолданушыларының әр қайсысына жіберіліп тексеріледі. Егер қате шықпаған жағдайда әрбір жүйе қолданушысы жиналған блокты өзінің тізбегіне қосады. Осыдан кейін жиналған және тексерілген блок жалпы транзакцияларды қамтитын блоктар тізбегіне қосылады. Осылайша блокчейн негізіндегі жүйеде ақша бір қолданушыдан екінші қолданушыға жіберіледі [12].

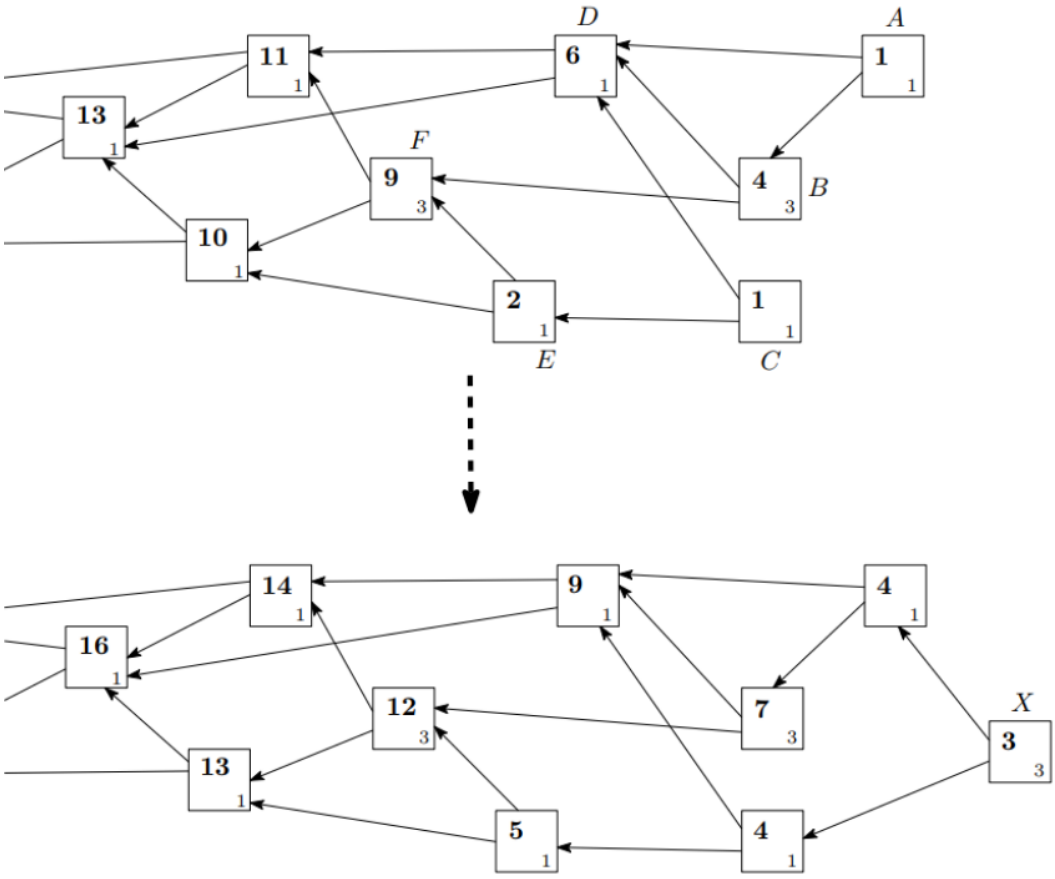
Биткойн жүйесінен басқа да танымал жүйелердің бірі - IOTA жүйесі. Ол кең таралмаған және қолдану аясы тар жүйе болып саналады. Бұл жүйенің жұмыс істеу принципі интернет заттардың қосымшаларын қолдануға негізделген. IOTA жүйесінің көмегімен жұмыс істей алатын заттардың ауқымы өте кең. Мысалы: смарт заттар жүйесі, смарт үй, адам денсаулығының көрсеткішін бақылайтын заттар, интернет заттар қасымшасы арқылы жұмыс жасай алатын электронды құрылғылар, автономды көлік басқару жүйесі, қала аралық тасымалдау құрылғылары [13].



1.4-сурет – IOTA жүйесіндегі транзакцияларды және кез келген басқа операцияларды растау принциптерінің сұлбасы

IOTA техналогиясының негізгі функциясы микротөлемдер жүргізу мүмкіндігі және деректерді қауіпсіз жіберу мүмкіндігі болып табылады. Биткойнде қолданылатын тексеру операциясы пайдаланушылардан бөлек түрде жасалады, сондықтан транзакцияларды растау үшін майнерлер жасалған жұмысы үшін комиссия төленуі шарт. Ал IOTA-да бұндай операциялар микротөлемдерде жұмыс істейді, сондықтан толықтай өзін өзі қамтамасыз етіп, майнерлер көмегінсіз жүзеге асырылады, жүйе пайдаланушылары басқа пайдаланушылардың транзакцияларын өздері растай алады. Бұл үшін IOTA жүйесінде DAG желісі қолданылады. Транзакцияларды растау және мақұлдау процесі 1.4-суреттегі сұлбада көрсетілген. DAG желісі толығымен транакциялардан тұрады. Жаңа транзакция пайда болған жағдайда, бұл транзакция алдында тұрған екі транзакцияны мақұлдай алуы тиіс. Мысалы: егер А және Б екі транзакциясының арасында кемінде екі түйін бар болса, онда АБ транзакциясын жанама түрде мақұлдайды деген сөз. Демек транзакция көбірек тікелей және жанама мақұлдауларды алған сайын, оны қолданылып отырған

жүйеде қабылдау ықтималдығы артады. Транзакцияның жалпы салмағы осы транзакцияның ішкі салмағы және осы операцияны тікелей немесе жарнама растайтын барлық транзакциялардың ішкі салмағының қосындысы ретінде анықталады [14].



1.5-сурет – IOTA желісіндегі транзакция түйіндерінің салмағын табу сұлбасы

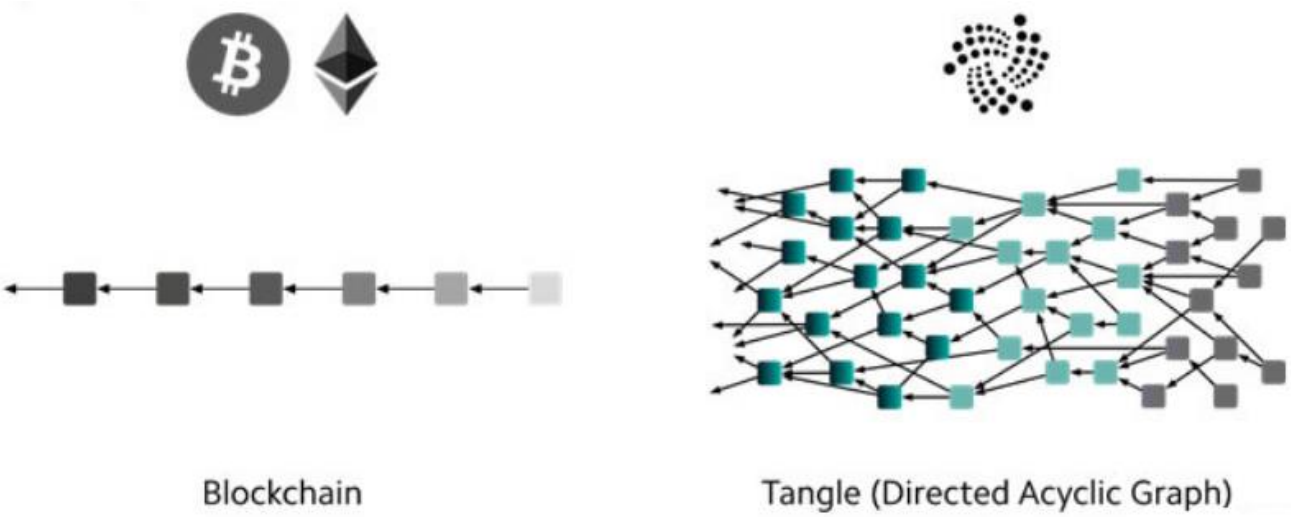
Мысалы 1.5-суретте берілген сұлбада F транзакциясы тікелей немесе жанама түрде А,Б,С,Е транзакцияларымен бекітілген. F транзакциясының салмағы 9=3+1+3+1+1, F транзакциясының өзінің салмағы және қосылған транзакциялардың салмағын алып отыр. Берілген суретте расталмаған транзакциялар тек А және С болып тұр. Егер бұл жүйеге Х жаңа түйіні қосылған жағдайда А және С түйіндері мақұлданады және кейінгі түйіндердің салмағы 3-ке артады, себебі Х-тің салмағы 3-ке тең.

Транзакцияны растау үшін түйін мынадай әрекеттерді орындайды:

- Алгоритмге сәйкес транзакцияны растау үшін басқа екі түйінді таңдайды.
- Таңдалған екі транзакциялардың жұмысын және қателердің болмауын тексереді. Егер қателер табылса басқа түйіндерді таңдайды.
- Транзакция жарамды болуы үшін криптографиялық амалдың орындалуын

қадағалайды. Мысалы: қарастырылып отырған түйін бір реттік кодты көрсетуі тиіс, қосылған түйіндердің хеші nonce кодымен бірге бір кодты құрады, осы шыққан кодта нөлдердің бекітілген саны болуы тексеріледі.

- Түйіндер қайта-қайта іске қосылу арқылы оларды басқа транзакциялармен мақұлдау ықтималдылығы жоғары болады. Егер шыңды таңдау алгоритмінің 100 рет таңдалған түйіні 95 рет орындалған болса, оны 95 пайызға сенімді деп қарастырады [15].



1.6-сурет – Блокчейн және тангл технологиялары

Блокчейн және тангл технологияларына мысал 1.6-суретте көрсетілген. «Блокчейн қалай жұмыс істейді» және «IOTA деген не» мақалаларын қарастыра отырып IOTA жүйесінің блокчейнді қолданатын жүйелерге қарағанда мынадай артықшылықтарын байқадым:

- Деректерді қорғаудың жоғары деңгейі. Биткойнға келтірілген мысалда белгілі болғандай желіге 51 пайыздық шабуыл болған жағдайда желі істен шығады делінген. Ал IOTA желісінде қолданушы блоктардың 33 пайызын қамтып отырған болса оны автоматты түрде жабады және тексеруден өткізеді.
- Транзакциялық коммисиялардың болмауы. Себебі барлық транзакциялар нақты уақыт мезетінде жүзеге асырылады. Биткойнда аударымның алатын уақыты бірнеше сағатқа созылуы мүмкін.
- Жіберілетін деректерді байланысты түйіндер тексеріп, растауы арқылы жоғары сенімділік пен қауіпсіздік және тез әрекет ету уақытын қамтамасыз етуі.
- Деректерді растайтын үшінші тараптың болмауы. Осыған байланысты транзакциялық коммиссия болмайды және микротөлемдер жүзеге асырылады.

Осы айтылған артықшылықтарына қарамастан, жүйенің үлкен кемшіліктері байқалады. Олар: жүйені реттеудің қиындығы, блокчейнға қарағанда өте үлкен есептеу қуатының керектігі жүйені қолданудағы қиындықтарға алып келеді [12].

1.4 Бөліп есепке алу технологиясы

Осы жылға дейінгі компьютерлік архитетуралар мен технологиялардың және олармен байланысты өзгерістер мен жаңартуларға көз жүгіртіп қарасақ, олардың қолданатын хаттамалары, инфрақұрылымдары, деректерді сақтау, кодтық тұрғыдағы операцияларды орындау, ақпаратты өңдеу және есептеудің арасындағы шыққан нәтижелермен ресурстарды орталықтандыру, одан кейін орталықсыздандыру арасында белгелі бір даму бағыты немесе осы жүйеге бейімділік тұр деп есептеуге болады. Осы процестерді орындайтын мэйнфреймдер немесе өнімділігі өте жоғары, өте ауқымды, басқаруларға төзімді, үлкен көлемде жедел және сыртқы жадысы бар, деректерге енгізулер мен түзетуді орындай алатын, ақауларға төзімді серверлер орталықтандырылған және есептеу процестерінің ресурстарының көп бөлігін қамтиды. Бұл есептеу мүмкіндіктері қолданушылар, клиенттен, клиенттік нысындар мен бөлінген қашықтағы серверлерге таратылып жүзеге асырылады.

Бұл қолдану тәсілдері қолданыстағы интернет пен деректерді сақтайтын және өңдейтін мәліметтер базасының жүйелерін дамытуға көмектесетін клиент және сервер архитектурасын құруға алып келеді.

Фреймдерде орналасқан үлкен деректер қоры бөліп таратылған архитектураға көшіріліп қарастырылуы мүмкін, деректер бұл жағдайда түйіннен түйінге немесе серверлерге көшіріледі, көшірілген деректер базасы немесе жиынтығы колданушылар мен клиенттер нысанында қол жетімді болады және өңделеді, осы операциялардан кейін тексеріліп серверлердің біріне қайта жазылып деректер синхрондалады.

Уақыт өте келе интернетте ақпарат пен деректерді бұлттық сақтау және есептеулер архитектурасы әртүрлі процестерді орындаушы, есептеуші құрылғылармен жаһандық түрде қол жеткізуге мүмкіндік береді, ал негізгі ақпараттық құралдар, компьютерлер және майнфрэймдер ең алдымен ірі компаниялар, корпорациялар және үкіметтің қажеттіліктерін орындау үшін жасалған. Бұл қарастырылған интернет-бұлттық архитектура аппараттық құрылғылар жағынан орталықсыздандырылғанымен, қолданбалы деңгейде деректерді орталықтандырып қолдануға алып келеді.

Кәзіргі таңда бұл технологиялар орталықтандырылған есептеулерден, деректерді сақтаудан және ақпаратты өңдеуден орталықтандырылмған архитектуралық шешімдер мен жүйелерге ауысуды көрсетеді деген ойдамын. Бөліп есепке алу технологиясы осы инновацияның негізгі көзі болып табылады.

Таратылған жүйелердің кейбірі, мысалы, рұқсат етілмеген блокчейн аралық түйіндерді қажет етпей, кейінгі қолданушыларға цифрлық деректерді немесе активтерді бақылауды қамтамасыз етуге мүмкіндік береді.

Ал рұқсат етілген блокчейндер орталықтандырылмаған архитектураны қолдана отырып, ақпарат пен деректерді сақтап, қауіпсіздігін қамтамасыз етеді және логикалық орталықтандырылуын сақтауға тырысады [16].

1.5 Рұқсат етілген және рұқсат етілмеген қатысу режимдері

Кәзіргі қолданыстағы орталықтандырылған сақтау жүйелері деректер қорының көшірмесін жүргізу, жүктеу және өңдеу үшін тек бір адамға рұқсат береді және сол адам арқылы ғана жүзеге асырылады. Бұл адам сол деректер қорының иесі немесе әкімшісі болуы керек.

Осы себепті бұл нысан қандай деректер егізілеп жатқанын және басқа қандай деректерді енгізуге болатындығын тексеріп, рұқсат етілгенін басқарып отырады. Бөліп есепке алу технологиясы пайда болған кезде жүйеде таратылған деректерді сақтау процесі түбегейлі өзгерді. Бұл дегеніміз бірнеше ақпараттық құрылғылар таратылған деректердің көшірмесін сақтайды. Жіберілген деректер барлығына бірдей теңдей таратылып сақталады және үлес қосуға мүмкіндік береді. Бөлінген деректер арасындағы түйіндер өзгерісі барлық ақпараттық құрылғылармен қолданушыларда бірдей көрінеді және таралады. Ал деректер дұрыстығын қадағалау үшін қосалқы түйіндер және келісім блоктары қолданылады. Осы ортақ ақиқатқа жету нәтижесі түйіндер арасындағы консенсус деп аталады [17].

Блокчейн қолданылатын желіге қол жеткізуге арналған екі жұмыс режимі бар. Олар: рұқсат етілген және рұқсат етілмеген. Рұқсат етілген режимді көбіне бәріне ортақ немесе ашық деп атайды. Егер қолданушыға немесе қатысушыға рұқсат берілсе оған тек өзгерістер енгізуге қатысты шектеулер қойылады, тек оқу және тексеру функцияларын қолдана алады. Жүйеде рұқсат етілген блокчейндік түйіндер қатысушыларды алдын ала таңдап, алардың желідегі кез келген әрекетін шектеп отырады.

Интернетке қосылған кез келген адам желіге қосылып орындалған операциялар мен транзакцияларды қарастырып оқи алады. Сондықтан рұқсат етілген, барлығына ортақ деп қарастырылады. Мұнда қатысушылардың желіде зиян келтіретін әрекеттерін тексеріп отырмайды, керісінше толық қолжетімді блокчейндердің желіге қосылу рұқсаттарын ақ тізімге енгізіп отырды, осының арқасында қауіпсіздік тәуекелдерін азайтып отырады.

Барлық қолданушылар үшін транзакциялар жазбасын көрсетудің орнына, ақ тізімге кірген пайдаланушыларға ғана көрінетін түйіндердің жеке желісі ретінде қарастырылады.

Рұқсат етілмеген қатысу немесе «жеке жүйе» деп қатысушылардың бір ұйымда болатын және бір мақсатты немесе бәріне ортақ қажеттілікті жүзеге асыратын жүйе ретінде қарастыруға болады. Бұл жүйеде пайдаланушыларға деректерді оқуға, өңдеуге, жүктеуге және өзгерістер енгізуіне рұқсат берілген. Барлық жасалып отырған өгерістер жаңа блок ретінде сақталып оған дейінгі блоктармен байланысып тұрады.

Бұл деректер өзгерісін пайдаланушылардың барлығына бірдей көшірмесі сақталады. Ал жүйе ішіндегі қауіпсіздікті қосалқы түйіндер мен логикалық блоктар қамтамасыз етіп отырады [18].

1.6 Блокчейнде қолданылатын транзакциялар

Жалпылай алғанда блокчейндегі транзакциялардың барлығы дерлік қаржылық операциялар емес және транзакция деректерін, қолданылып отырған ақпараттарды жай ғана тасымалдап немесе сақтап қана қоймайды. Блокчейндегі деректер алмасулары немесе транзакция активтерін жай ғана алмасумен шектелмей, оған қоса сақтау, тексеру, сұрау, пайдалану секілді есептеу операцияларының орындалуын қамтиды [17]. Әрбір орындалған немесе тасымалданып, сақталатын транзакция тексеруден өткеннен кейін жаңа блокқа орналастырылады, кейін транзакцияларды тіркеп отыратын кітапқа қосылады, блоктар тізіміне оған дейінгі сақталған алдыңғы блоктармен байланыстырылып қосылады. Бұл орындалған операциялар жүйенің сол сәттегі күйін және пайдаланушылардағы блокчейннің сақталған көшірмесін жаңартуға, оған керекті жана ақпаратты, деректер қоры жазылған блокты жүйеге қосуға алып келеді. Пайдаланушылар қолданып отырған желідегі басқада пайдаланушылармен өзара әрекеттескенде, жаңа операциялар немесе жаңа ақпараттың қосылуы кезінде, бір немесе бірнеше транзакциялардың желі арқылы тексеріледі, таратылады және расталады [19]. Қандай да бір блокчейнге негізделген жүйеде немесе «транзакциялық операцияның орындалуы» кезінде қадамдарының орындалу тәсілдерімен ерекшеленеді. Бұл қадамдардың орындалуы транзакция жасалған сәтте басталып, транзакция тексеріліп, орындалып, блокчейнге сақталған уақытта ғана аяқталады. Блокчейндегі орындалатын транзакциялардың төрт маңызды кезеңдері белгілі. Олар: жасап шығару немесе құрастыру. Бұл жерде әрбір блокчейн алдын ала реттелген мөлшердегі деректерді қабылдайды, осы арқылы оның артықшылықтары мен кемшіліктерін анықтап алуға болатын жағдайна алып келеді. Бір жағдайларда деректер үлгілері нақты бір блокчейннің қосымшаларына арнап жасалған, ал басқа түрлері әртүрлі мақсаттарда қолдануға болатындай өте икемді етіп жасалған. Деректерді немесе транзакцияларды жіберуші жіберілетін ақпараттың үлгісіне сәйкес тасымалдану нысанының, басқаша айтқанда цифрлық активтің қалайша шығарылып, қандай мақсаттарға сәйкес қолданатындығын анықтауы тиіс. Сонымен бірге транзакциялар орындалатын нысанын орындауға қажетті шарттарды, дәлірек айтқанда жүйенің осы сәттегі күйін жаңартудағы орындалатын шарттары көрсетілуі тиіс. Қабылдап алынған үлгіге байланысты өтеу критерийлері қарапайым қадамдар немесе нақты келісім шарттар арқылы келістірілген болуы мүмкін.

Таралу немесе тарату кезеңі: бұл кезеңде транзакция тексеруші қосымша түйіндеріне таратылады. Транзакцияларды тиімді тасымалдау олардың өңдеу жылдамдығына әсер етеді. Осының арқасында блокчейндер теріс әсер ететін өзгертулер мен манипуляцияға төзімділікті сақтайды және желінің өнімділігін оңтайландырады. Жарамды транзакция блоктары барлық түйіндерге өзінің көшірмесін жаңарту үшін желі бойынша блокчейндегі барлық блоктарға таралады.

Тексеру кезеңі: бұл өте маңызды қадамдардың бірі, себебі ол барлық қолданылып жатқан блокчейн негізіндегі жүйелерді сипаттайды деп айтуға болады. Бұл кезеңде блоктарда жиналған деректер және транзакциялар тексеріліп, жарамды болып, әрі қарай орындалуы және есептелуі үшін бекітілген келісімге келу, басқаша айтқанда консенсус месханизмінің орындалу сатыларына сәйкес болуы керек. Осы қадамдар орындалғаннан кейін транзакциялар ары қарай жіберіліп блоктар күйі жаңартылады және блокчейнге қосылуға рұқсат беріледі.

Растау кезеңі: транзакция блоктары тексеріліп болып блокчейенге қосылғаннан кейін олар бұдан былай жойылмайтын, өзгертілмейтін деректер тізіміне немесе блоктарға бекітіледі және расталады, әрі қарай блоктарды жалғастырады және активтерді нақты тасымалдау үшін қолданылады. Осы маңызды бөлікке жету үшін ол келімге келу процедурасының соңа дейін жетуі тиіс. Яғни осы түйіндер блоктардың бір тізбегі бойынша қосылып, белгілі бір мақсатта орындалуы керек. Блокты қалыптастыру кезінде алғашқы тексеру қадамдары орындалады, оны орталықпен байланыстырады. Транзакциялар кейін расталып қол қойылады, оның түп нұсқалығы тексеріледі. Бұл деректерді басқа блоктармен қосып, деректерді тарату кезеңіне дейін қосымша түйіндерде тексеру операциялары орындалады [10].

Тексеру және растау блокчейнге түпнұсқалық, тұтастық және ерекшелік сипаттарын береді. Блоктарды құру процесі тексеру кезеңінің маңызды, әрі ажырамас бөлігі. Бірақ блокчейннің сипатына байланысты әр түрлі немесе бөлек болуы мүмкін. Блокчейндегі тексеру процестері орындалатын транзакциялар мен қадамдар немесе процестер, олардың тәртібіне қатысты орындалатын келісімге келудің көрінісі болып табылады. Блокчейндегі транзакциялар блоктарға енгізілген кезден бастап немесе осы нәтижелер бөлек блоктарға жиналып, реттелгеннен кейін ол деректер қорының бөлігі ретінде рәсімделеді және сақталады. Кез келген желі түйіні жасақталған немесе алдын ала жазылған ережелері мен заңдылықтары бойынша блоктарды құра алады. Жаңадар құрылған блоктарды тексеру және мақұлдау процесі, дәлірек айтқанда блоктық ұсынысты қамтамасыз ету үшін мүмкін болатын көшбасшы түйіндер деп аталатын, деректерді шектеулі сақтайтын түйіндерді қолдануға болады. Бұл процесте олардың біреуі де жарамды болып табылады. Негізгі түйінді таңдау, тексеру және растау процесі валидация процедурасымен біріктірілуі мүмкін немесе одан толығымен бөлек процесс болуы мүмкін. Расталып, рұқсат берілген блокчейндер сайлану және тексеру кезеңдерінің арасында оларды тікелей бөлуге мүмкіндік беретін консенсус хаттамаларын қолданады. Бастаушы блоктардың рөлін келісімге келу шарттары арқылы валидаторлар рөліне алып келуге болады. Көшбасшы ретінде рәсімделу үшін желі пайдаланушылары өздері жасап шығарған блоктарды растау үшін күш салуы қажет. Блокчейн технологиясының орталықтандырылмаған ерекшелігіне, сипатына байланысты бастамашы немесе жетекші түйіндер тексеруші ретін де ұсынылған транзакциялар блогын растау процедурасынан өткеннен кейін өзгеріп кетуі мүмкін сипатқа ие. Ерекше жағдай

ретінде биткойндегі блокчейндерді айтуға болады. Бұл жерде жетекші блоктар мен валидаторлар кездейсоқ сайланып отырады [20].

1.7 Блокчейн қатысушылары мен олардың сәйкес рөлдері

Бұл бөлімде блокчейндегі пайдаланушылар және түйіндерде орындалатын процестердің атқаратын негізгі рөлдерін, жұмысын түсіндіріп жаздым.

Транзакция тараптары. Блокчейн транзакциялары бір немесе бірнеше блокчейн пайдаланушыларымен байланысты қолданушылардың екі түрін көрсетеді: деректерді жіберуші, таратушы және деректерді қабылдаушы. Бұл екі тараптың арасындағы өзара әрекеттесулер мекенжай деңгейінде орындалады. Жіберуші тараптағы мекенжай және қабылдаушы тарапындағы мекенжайлар арасындағы деректер ағынын, дәлірек айтқанда цифрлық активтерді тасымалдау операциясын жүзеге асырады.

Деректерді жіберуші деп деректер қорын транзакциялар арқылы қабылдаушы тарапындағы түйіндерге жіберетін түйін, деп түсіндім. Деректерді жіберуші міндетті түрде транзакцияны жасаушы тараппен, деректерді тасымалдауды бастау құқығын тексеруші түйінмен және деректерді ұстаушы тараппен бердей болмауы керек.

Ақылды немесе смарт келісім. Бұл тізбектен тыс немесе шарттар рұқсат етілген түйін арқылы басқарылатын транзакциялардың «жабық немесе құлыпталған» тізбегін құруды қамтиды. Бұндай тізбектің немесе тасымалданатын деректердің иесі болмауы мүмкін. Бірақ көп жағдайда деректерді жіберуші тасымалдау нысанының, яғни цифрлық активтердің түпнұсқалығын тексеріп, растау үшін транзакцияларға рәсімделген «жабық кілттермен» қол қоюға жауапты болып саналады.

Деректерді алушы тесеріліп, расталып, қол қойылып жіберілген деректерді, активтерді, немесе құжаттарды қабылдайтын желі пайдаланушысы. Оған транзакциялар арқылы хабарламадағы жіберушінің ашық кілтін қалпына келтіру және транзакция деректерінің түпнұсқалығын тексеру арқылы жүзеге асырылады. Кез келген блокчейн түйінін қалпына келтіруге болады. Транзакция авторы мен қолтаңба иесі арасындағы деретер алмасу, желідегі бұрмаланған деректерден арылу үшін және қолтаңбаны тексеру үшін орындалатын шаралар болып табылады [18].

Жетекші түйіндер: уақытша басшының немесе «диктатордың» рөлін атқарып тұратын, осының арқасында керекті мақсаттарға сай келісімге жету үшін қолданылатын түйіндер. Бұл түйіндер блокчейн тізбегіне енгізуге сай, дайын блокты тағайындап ұсыну керектігін шешеді және блоктың дұрыс ұсынылғанын тексеруге де жауапты болады. Басшы түйіндерді блоктау туралы ұсыныс қабылданған соң бірден биліктен шешіледі. Шешім қабылдау құқығы бар аралықта қосымша блоктар оның шешімін растай алмайды. Бұл уақыт өткеннен кейін басшының жұмысын атқара алатын жаңа түйіндер мен блоктар сайланады. Көшбасшыларды сайлау қадамдары блокчейн жүйелерінде

қабылданған консенсус механизміне алдын ала енгізілген. Рұқсат етілген және рұқсат етілмеген блокчейндер валидаторға блоктарды ұсынуға жауапты түйіндерді орнату үшін бекітілген әдістерді қолданады.

Түйіндерді тексеру: осыған дейін айтып өткендей, пайдаланушылар консенсус алгоритмін басқарады және жетекші түйіндер жіберген ұсыныстары бойынша келісімді орнатуға жауапкершілік атқарады. Тексеру кезіндегі сәйкестіктерді блоктау, қай жерде қандай блокты жариялап, бекіту керектігін тексеру түйіндері арасындағы консенсус механизмдеріне сай шешім қабылдайды. Кәзіргі уақытқа дейінгі ұсынылған транзакциялар ағынына назар сала отырып, оны сипаттау үшін бөлек-бөлек рөлдерге бөлінген қолданушылар мен желі түйіндері екендігін, одан басқа мәні жоқ екендігін көрсетеді. Бірінші кезеңде транзакция тарапынан, дәлірек айтқанда деректерді жіберуші мен деректерді қабылдап алушының арасында байланыс орнатылады, содан кейін транзакциядағы жетекші түйінге жіберіледі. Олар өз кезегінде жіберілген транзакциялардың жарамдылығын тексереді, осы транзакцияларды блоктарға жинауға және жиналған блоктарды тексеруге лайықты түйінді ұсынуға жауапты болады. Соңғы кезеңдерде тексеру түйіндері блоктың сенімділігін тексеріп оған растау процедурасы жүргізіліп сенімділігін тағайындайды. Рұқсат берілген ортада әрбір түйін блок ұсынысы мен тексеру процедурасын қайталамай өзіне бекітілген жұмысын немесе рөлін орындайды. Бұндай шешім рұқсат етілген блокчейндерде қабылданған, ауқымды дауыс беруге негізделген консенсус механизмінің процедураларын орындайды. Оның орнына ашық қол жетімді блокчейндер қолданыстағы деректерді, блоктарды тіркеп, ақпаратты жеткізу үшін түйіндердегі орындайтын рөлдерінің қайталануын қамтамасыз етеді[19].

Блокчейн транзакциялары осы үш негізгі процестерді орындап белгілі бір мақсаттарды орындап, пайдаланушыларды нәтижелерімен қанағаттандыру үшін жасақталған жүйе. Бірақ кейбір рұқсат етілген блокчейндерде түйіндерге басқа да әртүрлі тапсырмалар тағайындалады, осының арқасында олардың ауқымдылығы жақсартылып, аяқтауды тексеріп мақұлдау, басқарушы түйінді сайлау, тапсырыс беру сынды процестерді орындауға мүмкіндіктері пайда болады.

1.8 Консенсус механизмі

Консенсус сөзінің мәні ортақ қызығушылық пен мүдделердің, белгілі бір мақсаттардың жақындасуын білдіреді. Консенсус ортақ мақсатқа жету үшін әрекеттесетін агенттермен көп агенттік жүйелерді жасау, қолдану, алу мәселесін іске асырады. Агенттер олардың жағдайына байланысты белгілі бір мүдделерге, құндылықтар мен әрекетке келуі керек.

Консенсустың менің күнделікті қолданатын жүйелердге қандай қатысы бар деген сұраққа мынадай мысал келтіруге болады. Мысалы ретінде википедия сайтын алайын, бұл жағдайда консенсус механизмдері жасырын түрде іске асырылады, өйткені бұл базаға шығарылатын ақпарат редакциядан өтіп,

жариялағанға дейін қоғамдастыққа барлығына көрінетіндей ақпаратты жіберген сайын оны басқа да редакторлар қабылдап, рұқсатын беріп, жалпыға шығаруы керек. Ал тексеру және өңдеуді басқа редактор жасайтын болса және бұл түзетулер қабылданатын болса, жүйе алдыңғы сұраныстан бас тартып, жаңа консенсусқа көшеді [19].

1.8.1 Бөлінген жүйелер мен блокчейндегі консенсус

Көптеген жүйелерді үйлестіру есептері күрделі жүйелер динамикасында, сонымен қатар информатика мен коммуникацияда кеңінен қолданылады. Осындай жүйелерде консенсус хаттамалары консенсус процесі кезінде сәтсіздікке ұшырауды болдырмайтын агенттермен жұмыс жасауы тиіс. Мәселен, 1978 жылы ұсынылған екі жақты міндеттеме хаттамасы, басқаша айтқанда 2PC хаттамасы түйіндер орындалатын транзакцияларды алдын ала орындау және тексеру кезеңдерін кеңейтілген түрде және таратылған ортада транзакцияны өңдеуге мүмкіндік береді. Соның өзінде, 2PC пайдаланылған кезде кез келген түйіндегі ақаулар мен бұрмаланулар консенсус процедурасына қауіп төндіреді. Осыған байланысты ақауларға төзімділік процестерін және байланыс ақаулары туындаған жағдайда жүйенің күтілгендей жұмысын жалғастыруға мүмкіндік беретін процестің сипаты адал түйіндерде туындаған ақаулар, бұларды басқа жағдайда жүйе жұмысындағы ақаулар деп атайды және зиянды еректер жасайтын түйіндер немесе византиялық сәтсіздіктер пайда болуы кезінде де өзінің бастапқы күйінде де жұмыс істей алу қабілетін жоғалпауы болып тұр. Ақырлы күй машиналарының жұмыс жағдайындағы деректердің көшірмесін жасау әдісі қателер мен деректердің бұрмалануына төзімді консенсус хаттамаларын құруға мүмкіндік береді. Сенімді орталарда сәтсіздіктер мен туындайтын қиындықтар мен қателерге төзімді, оған қоса қосымша сенімсіз тараптардың желілеріндегі византиялық сәтсіздіктердің алдын алып атырады. Бөліп қарастырылатын ортада соңғы күйдегі машиналар бірнеше түйіндерде қайталанып, жұмыстарын орындап отырады. Олар үшін бірдей бір уақытта дамымаса да, жұмыс жасау кезінде дәйекті, дұрыс, әрі бір бірімен келістірілген көшірмелерге ие болуы үшін олардың қабылдайтын сұраулардың жалпы реттілігін алдын ала келістіріп алған дұрыс болады. Соңғы есептеу машиналарындағы деректер көшірмелерін сақтау протоколдарының ең танымал класы византиялық ақауларға төзімділік хаттамасы немесе BFT хатамасы болып саналады [21].

Бөлінген деректер қорындаға келісім шарттардағы алғашқы тәсілдерді консенсустың бөліп басқаруға қатысты бастапқы шешімі деп қарастыруға болады. Бірінші буындағы блокчейндер милиондаған пайдаланушылардың арасында ең ықтимал жолдармен байланыс орнатады, осылайша келісім шарттарының соңғы нәтижесі жүйенің бастапқы келісім шарттарына қарағанда жүйе пайдаланушылары үшін жоғары дәрежеде қарастырылатын болды. Осы жүйелердің қателерге қарсы төзімділігі жүйе ішіндегі зиянды түйіндердің аз дәрежеде болуын және жұмыс жасауының нәтижесінде ғана сипатталады. Осы

идеяның негізгі мәні, жүйедегі түйіндер арасында есептеу шығындарын тауып, есептеп отыру. Бұның барлығы транзакциялардағы блоктардың қалыпты жұмыс жасау туралы дәделін алу үшін жасалады, осылайша бастапқы дәрежеде жұмыс істесмейтін түйіндерден арылып немесе жойып отырады. Сонымен қатар жүйе пайдаланушылардың электронды деректер қорында немесе электронды поштасында спам, белгісіз ақпараттар, зиян келтіруші деректер болмайды. Блокчейн қолданылу аясы кеңейгендіктен және криптовалюталардың танымалдылығының артуына байланысты ауқымдылық пен өнімділікке қойылатын талаптар айтарлықтай өзгерістерге ұшырады. Бірінші буындағы блокчейндердің әлсіз жақтары, оның бөлінген есептеулер арқылы негізгі технологияны тереңірек талдауға алып келді. Шектелген ауқымдылығымен жасалған жұмысты дәлелдеу, верификациялау процедурасын мұқият қарастыру және жоғарғы кідірісті болдырмау үшін тым көп есептеу ресурстарын жұмысайтын түйіндердің жұмысын ықтималды етуді керек етті. Жасалған жұмысты дәлелдеу процедурасына тиісті түзетулер энергияны ысырап қылмай, жоғары деңгейлі масштабтауға кепілдік бере алатын болды [22].

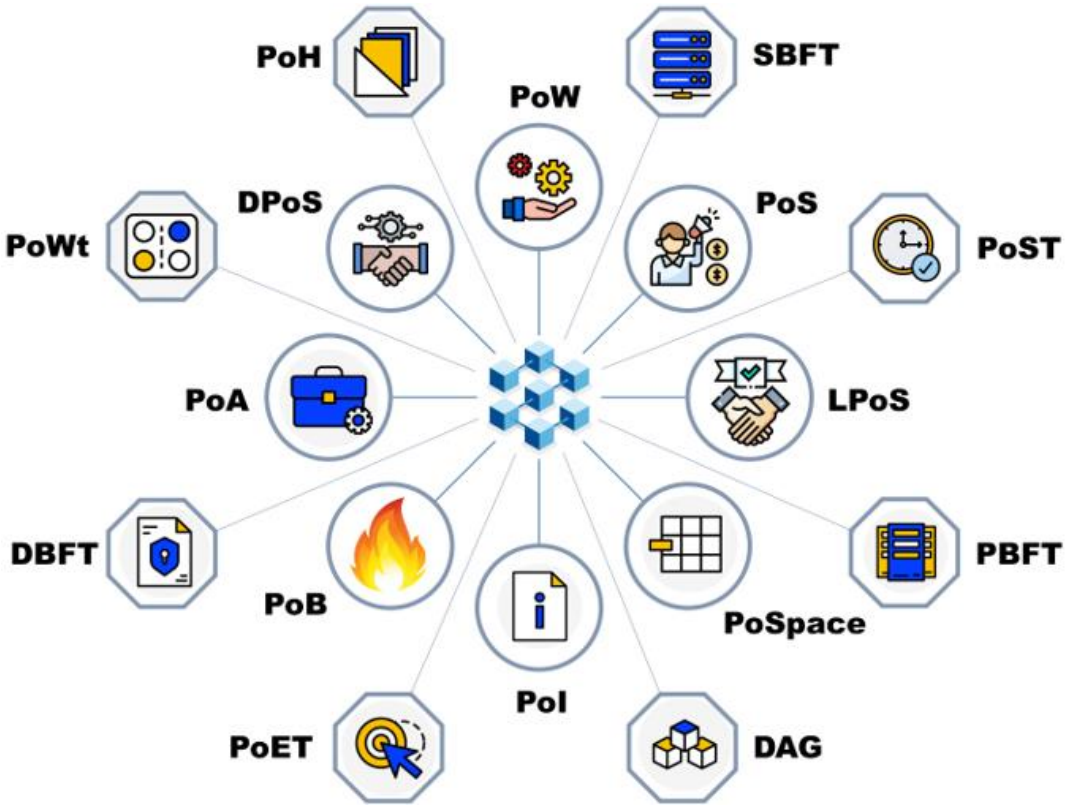
1.9 Консенсус механизмінің алгоритмдері

Жүйедегі күрделілік пен ауқымдылық мәселелерін өтеу үшін жұмыстың орындалуын дәлелдейтін механизмге (PoW) бірнеше ұқсас нұсқалары ұсынылды. Бұл идеяның мәні PoW консенсусын сипаттайтын және пайдасыз есептеулерді жүргізетін транзакцияларды тексеру үшін жасалған алгоритміне балама ретінде ауыстыру болды. PoW консенсусы орындайлатын процеске жұмсалатын күш пен энергияға негізделген көшбасшыны сайлаумен сипатталатын хаттамалар алгоритмдерінің PoX (Proof of X consensus) класын құрайды. Proof of X Consensus немесе PoX протоколдары рұқсатсыз блокчейндерге арналған және осы блоктардың көшбасшысына беріледі.

Сайлау процесі. Рұқсатсыз орталарда әрбір түйіннің осы жұмысты орындағаны үшін қандай да бір күш, энергия жұмысағанын дәлелдеу арқылы көшбасшы болу мүмкіндігі бар. Бұл деген есептеу процесі, ақшалай немесе жіберілген деректерді, цифрлық активтерді жинақтап сақтаушы сипатта болуы мүмкін немесе блокчейн желісінде жұмыс жасау үшін, өзін орнату әрекеттерін көрсетуі мүмкін [23].

Жұмыстың орындалуының дәлелі. Транзакция блогын тексеруге тырысатын блокчейн түйіндері белгілі бір қиындықтарға сәйкес талаптарға жауап беретін блоктың хэш мәнін табуы керек болады. Бұл тексерушілерді майнерлер деп атайды. Осы тексерулерді жүргізіп блокты желіге шығарған тексеруші майнер осы блокты растай алады. Сондықтан да жетекші майнерлер тексеру түйіндері ретінде жұмыс істейді. PoW консенсустың толығымен орындалуына кепілдік бере алмайды, осы себепті транзакция келісімдері толық блокчейндегі тізбекке бекітілген кезде ғана қарастыруға болады.

Дәлелдеу жұмысының үлесі және виртуалды майнингке баламалар. PoS механизмі PoW механизміне нақты майнингтен виртуалды майнингке өтуін іске асырады. Басқаша айтқанда, қосымша күш пен энергияны қолданусыз өндіруді білдіреді. Бұл жүйеде жетекші түйінді таңдау механизмі желі қолданушылардың үлесін тағайындау нәтижесінде жатыр. Бұл идеяның мәні, көптеген міндеттемелері бар қолданушылар блокчейнге шабуыл жасауы екіталай болуында. PoS консенсусының бірнеше түрлері бар. Олардың жұмысының негізгі мәні, біріншіден үлкен үлесі бар құрамалардың дауыс құқықтарының орталықтандыруын болдырмау, екіншіден басқа жақтан болатын шабуылдарға төтеп беру болып келеді. Бір жағанан блоктарды тексеру немесе валидациялаудың төмен есептеу құнына байланысты мүмкіндігінше қолайлы нәтиже алу болып табылады. Бұл шешімдер әдете валидаторлардың керекті үлесті тауып, тиесілі ресурстарды бөліп беруін талап етеді. Осы сияқты PoET және POI шешімдерін іске асырудың баламалары орталықтарндыру тенденцияларымен күресі болып табылады, яғни шыққан ресурстарды бір жерде жинақтауға қарсы тұру. Осы себепті кездейсоқ таймерге сүйене отырып сол арадағы жетершіні таңдап отырады. Лайықты жетекшіні табылған соң желідегі таранзакция ағыны мен мөлшерін көбейту үшін ынталандырады. Оның үстіне жасалған операциялар тиімді болуы үшін механизм шектеулі таңдаулармен жұмыс істей алады [19]. 1.7-суретте блокчейндегі консенсус алгоритмдерінің түрлері көрсетілген.



1.7-сурет – Блокчейндегі консенсус алгоритмдерінің түрлері

Proof of work (PoW) аударғанда «жұмыстың дәлелі» деп түсінуге болады. Бұл кең таралған және ең танымал консенсус алгоритмдерінің бірі. Блокчейндегі блокты жасап шығарып тізбекке қосу үшін майнер криптографиялық функцияның хешін табады, ол үшін көптеген күрделі математикалық есептеулерді орындайды. Осы орындалған жұмысты желіге дәлел ретінде қалыптастырады. PoW өз уақытында үлкен жаңалық болды, алғашқы криптовалютаны шығаруға үлкен пайдасы тиді. PoW алгоритмін қолданудағы ең қарапайым мысал: блокчейн. Ол орталықсыздандырылған жүйенің керемет деңгейін және жоғары қауіпсіздігін қамтамасыз етті. Бұл жүйеде кез келген қолданушы қосылып, майнер бола алады. Ал жоғарғы қауіпсіздік деңгейі биткойнді бұзудан сақтап тұрады. Биткойнді бұзу үшін айтылып өткендей «51 пайыз шабуыл» қажет болады. Бүгінгі бұзу үшін керек болатын есептеу қуатының көлемін жинау іс жүзінде мүмкін емес болып табылады. Бұның барлығы PoW алгоритмінің артықшылықтарына жатады. Бұған қарамастан кемшіліктеріде жоқ емес. Ең алғашқы және үлкен кемшілігіне жоғары энергия тұтынуды жатқызуға болады. Себебі желі өскен сайын ақпараттық құралдардың майнинг кезінде энергияны көбірек тұтынатын болады, сәйкесінше желінің жалпы энергия тұтыну өсе береді. Көптеген есептеулерді жүргізу көп уақытты талап етеді, сондықтан PoW алгоритмін енгізу кезінде желінің өткізу қабілеті бәсеңдей бастайды. PoW желілерінің дамуымен майнерлердің өндіру жұмысы қиындайды, оның салдарынан комиссия арта бастайды. PoW алгоритмінің осындай кемшеліктерін шешу үшін қолданушылар жаңа шешімдерді іздейді, осылайша жаңа консенсус алгоритмдері пайда болады [23].

Proof of Stake (PoS) «меншік құқығын растау» дегенді білдіреді. Танымал консенсус алгоритмдерінің бірі. Бұл консенсус алгоритмінде майнинг болмайды. Есептеулер жүргізіп жаңа блок құруда жасалатын жұмыстың дәлелінің орнына криптовалюталардың белгілі сақталған немесе мұздатылған көлемін дәлел ретінде көрсетеді. Бұл түйіндерді нода немесе валидаторлар деп атайды. Олардағы сақталған криптовалютаның көлемі «стек» деп аталады. Егер бір түйіндегі валидаторда неғұрылым көп «мұздатылған криптовалюта» болса транзакцияны растау ықтималдылығыда, орындалған жұмысына сыйақы алу ықтималдылығы да соған сәйкес өседі. Бұл алгоритм кәзіргі кезде көптеген блокчейндерде қолданылады. Мысалы: etherium, bitcoin, tron, bsc «binance smart chain» және т.б. PoS алгоритмінде жоғарыда айтылған PoW алгоритмінің жоғары қуат тұтыну, үлкен есептеу қуаты бар жабдықтар керектігі сынды кемшіліктері жоқ. PoS желілерінде транзакцияларға қойылатын комиссия төмен, ал өткізу қабілеті жоғары болады. Бірақ бұның бәріне қарамастан PoS аогоритмінің кемшіліктері ді бар. Бірінші кемшілігі, бұл орталықтандыру қауіпі. Екіншісі, криптовалютаның басым көлемі валидаторлардың шағым бөлігімен басқарылу қауіпі пайда болады. Бұл жағдайда олардың желіге әсер ете алатындай күйге жетеді [24].

Delegated Proof of Stake (DPoS) «өкілетті меншік иелігін растау» дегенді білдіреді. Бұл жоғарыда айтылған PoS алгоритмінің бір түрі, оның басты айырмашылығы алгоритмді орталықтандыру қауіпінен сақтау болып келеді.

Яғни оның басты кемшілігінен сақтайды. DPoS алгоритімін қолданатын желіде транзакцияларды тексеру, растау және мақұлдау рұқсатын активті ұстаушы береді. Рұқсат беру кезінде сол немесе басқа мақұлдаушы валидаторға дауыс береді. Кез келген пайдаланушыда белгелі бір мөлшерде криптовалюта бар болса, бұл қатысушы желідегі валидатор бола алады. Бірақ кез келген уақытта валидаторға берілген дауыстар басқа валидаторға берілуі мүмкін болады. Бұл алгоритмнің де кемшіліктері байқалады. Мысалы: желіде қатысушылардың төмен дәрежедегі белсенділігі байқалса PoS алгоритмдеріне сәйкес жұмыс жасай бастайды. DPoS алгоритмдерін қолданатын желіге Tezos-ті жатқызуға болады [21].

Leased Proof of Stake (LPoS) бұл алгоритмді PoS-тың модификациясы деп қабылдауға болады, «жалға алынған үлестің дәлелі» деп аударылады. Бұл алгоритмнің PoS, DPoS, PoW алгоритмдерінен ерекшелігі криптовалюта бөлігін немесе үлесін жалға алуға болатындығында. LPoS алгоритмінің көмегімен желідегі жаңа қатысушы да валидатор бола алады. Барлық желі қатысушылары өздеріндегі криптавалютаны валидатордың иелігіне бере алады (арендаға берген секілді). Валидаторға криптовалютаны берген жағдайда қолданушы әмиянынан алынбайды және аударымдар болмайды. Криптовалюта қолданушының әмиянында қалады, қатып қалған түрде болады. Оны қолданушы өз иелігінде сақтайды, бірақ өз мақсаттары үшін қолдана алмайды. Бұл алгоритмнің басты кемшілігі желіні орталықтандыру қауіпінде жатыр. Осы алгоритм арқылы валидаторлар ериптавалютаның біршама бөлігін жалға алу арқылы монополузациялауы мүмкін саналады. LPoS алгоритмін қолданудағы мысал ретінде «waves» блокчейн жүйесін айтуға болады.

Proof of authority (PoA) «өкілетті дәлелдеу», бұл консенсус алгоритмі желідегі валидатордың өкілеттілігіне (өкілеттілік, бедел - авторитет) негізделген. Валидаторлар өз беделін дәлел ретінде қолданады. Желі қолданушылары валидаторларға дауыс береді, осы арқылы валидаторлардың бір бірінен өкілеттелігі бойынша айырмашылық туындайды. Валидаторлар істелген жұмысы үшін сыйақы алмайды, бұл осы алгоритмнің басты кемшілігі болып табылады. Сондықтан бұл алгоритмді көбіне жеке блокчейндерде қолданады [24].

Proof of Importance (PoI) бқл алгоритм валидатордың маңыздылығына негізделген, «маңыздылық дәлеліле» негізделген. Валидатордың транзакцияларды растау кезінде алгоритм мұздатылған криптавалютаны ғана емес, валидатордың қызметіне де төленетін сыйақыны да ескереді. Валидаотрды бағалау кезінде орындаған транзакциялар, желідегі онлайн болаған уақыт аралығы секілді параметірлер ескеріледі. Осыдан валидатордың жасаған үлесі мен белсенділігі жоғары болса, ол желі үшін соншалықты маңызды болып табылады. Осы алгоритмді пайдаланудың мысалы, NEM блокчейн жүйесі [23].

Proof of Space (PoSp) бұл алгоритм қолданылатын бос кеңістекке негізделген, «кеңістікті дәлелдеу» дегенді білдіреді. Қатысушылар орындалған жұмыс пен транзакцияларды дәлелдеу үшін ақпараттық құралдағы сақтау дисктеріндегі бос орынды қолданады. Бұл бос орын блокчейннің функцияларына

негізделген, тізбектегі кейінгі блокты тексеру үшін хэш кодтарын толтыру үшін қолданылады. Осы алгоритм бойынша жұмыс істейтін желіге (BCoin, BrustC) жатады.

Proof of Space Time (PoST) бұл алгоритм PoSp түріне жатады. Айырмашылығы, қолданушылардың желіге қосқан үлесі ретінде дисктегі бөленген бос орынды ғана емес, осы бос орынды бөлуге кеткен уақытты да ескереді. Бұған мысал ретінде Chia-ны келтіруге болады [24].

Proof of Elapsed Time «жұмысалған уақыт дәлелі». Бұл алгоритм intel процессорларының SGE (Software guard extension) ережелер жиынтығына негізделген. Жұмыс істеу принципі кездейсоқ түрде жүреді.

Майнинг кезінде блокқа кездейсоқ күту уақыты қойылады, бөлінген түйін осы уақытта өшеді немесе жұмыс жасамайды деп айтуға болады. бірінші іске қосылған түйін блокты тексеру және растау құқығына ие болады. Алгоритм берілген уақыттың шынымен кездейсоқ екендігіне кепілдік береді. Бұның барлығы жүйеге артық жүктеме түсірмеу үшін қолданылады. Бұл алгоритм жеке блокчейндерде қолданылады, оны қолдану үшін белгілі ережелерге сәйкес жұмыс жасай алатын intel процессорларын керек етеді.

Proof of Burn (PoB) «жағып жіберу дәлелі». Бұл алгоритм криптовалютаның жоғалтуын, жоюын немесе жағуын іске асырады. PoB алгоритмінің көмегімен майнер криптовалютаны арнайы (жабық, тұйық) әмиянға жібереді. Бұл әмияннің жеке кілті болмайды, сол себепті оған кіру мүмкіндігі болмайды.

Осы арқылы криптавалютаның бір бөлігі айналымнан алынып тасталынады. Алгоритм бойынша «жану» дәлелденгеннен кейін майнер келесі блокты құруға деген ықтималдылығы артады және сол блок үшін сыйақы алу мүмкіндігі пайда болады. PoB алгоритмінде үлкен есептеу қуатын қажет етпейді және криптавалютаның шығарылу мөлшері шектеулі болғандықтан оның бағасыда сәйкесінше өседі [21].

BFT негізіндегі гибритті алгоритмдер. BFT хаттамалары шектеулі саны бар блокчейндерде жақсы жұмыс істей алады. Сол себепті олар қоғамдық жүйелер үшін емес, жабық жүйелер үшін қолданған қолайлы болады. BFT алгоритмдері барлық пайдаланушылардың кем дегенде үштің екі бөлігі адал болған жағдайда желінің жұмыс қабілеттілігіне кепілдік бере алады.

BFT негізіндегі әртүрлі опциялар түйіндерді тексеру үшін қосымша рұқсаттармен жұмыс жасайды. Бұл хаттамаларды масштабтау үшін гибридті алгоритмдер қолданылады. Олардың біріншісі пайдаланушылар мен түйіндер қауымдастығын құру үшін, ал екіншісі келісімге келу үшін пайдалану арқылы PoX және BFT – ді біріктіруге мүмкіндік береді.

Алгоритмдердің бұл класы блоктарды генерациялау кезеңін бөледі. Блоктарды тексеру кезеңі, бұл процест тәуелсіз және әртүрлі қатысушылармен басқарылады. Бұл бір процесс болуы мүмкін бірақ түйіндердің рөлдері әртүрлі болады [25].

1.10 Блокчейнді қолданысқа енгізу

Көп жағдайда деректер қорының реестірі қажет болатын кездер туындайды. Яғни деректер транзакциялар түрінде сақталып, ортақ қолдануы керек жағдай. Деректер желі арқылы берілуі тиіс жаңартуларға жататын тізілімнің күйін құрайды. Сақталған деректерді ортақ пайдаланудың қажеті керек емес кезде, күрделі криптографиялық архитектуралар сақталған деректерге қолжетімділікті қамтамасыз ету үшін қажет емес болады. Сондықтан да осы айтылған операциялар мен алгоритмдер керекті нәтижеге алып келмитін болса, әрине қажет емес болады, оның орнына қолданыстағы дәстүрлі шешімдерге жүгінген дұрыс болады деп ойлаймын.

Блокчейнді жүйеге енгізу деректерді бірнеше желі пайдаланушылары сақтау және ортақ пайдаланудың қажетілігі болған жағдайда ғана дұрыс шешім бола алады. Блокчейнде бірнеше пайдаланушылар жазбалар енгізуге және бірнеше тараптар арасында консенсус процедурасына қатысу және шешімдер қабылдау рұқсатына ие болуы керек. Блокчейн бизнесте «құлыпталған жазу» құқығы бар иерархиялық клиент – сервер жүйелерінен бөлінген реестірге жазуға қабілетті бірнеше түйіндері бар орталықтандырылмаған P2P желісімен өзара әрекеттесуге көшуге мүмкіндік береді [22].

Блокчейн сенімсіз субъектілер арасындағы өзара әрекеттесуді қамтамасыз етіп тұрады, орталықтандырылған органдардың кез келген араласу мүмкіндігін айналып өтеді. Орталықтандырылмаған жүйелерге деген қажеттілік, желі пайдаланушылары арасында орталықтандырылған жүйеге сенімін жоғалтқан сайын туындайды. Қалай дегенімен де, орталықтандырылған жүйеден орталықтандырылмаған жүйеге көшу міндетті түрде толық, тез, әрі радикалды болуы шарт емес. Блокчейндер кейбір функцияларды ғана ортадықсыздандыруы мүмкін, ал қалған басқада фунциялары орталықтандырылған болып қалады. Блокчейн сенім сөзінің мәніне өзгеріс жасады деп айтуға болады. Ол ендігі тексеру процесіне жауапты субъектілердің жеке басына қатысты болмай, хаттаманың архитектурасына қатысты болатынын сипаттайды. Блокчейн жүйесіндегі пайдаланушылар валидаторлардың хаттамаларды орындауға мәжбүрлейтін, орындалмаған жағдайда жазалайтын және кез келген ауытқуларды мүмкін етпитін, әрі болдырмайтын технологияға сенеді. Осыған байланысты сыртқы үшінші тарап және таңдалған мүшелерден құралған топ жұмыс жасайды. Сыртқы үшінші тараптың қолданылуы, жүйеге техникалық қызмет көрсетудің істен шыққан жағдайда ауыстырылуы мүмкін сыртқы ұйымдарды жұмысқа қосады және соларға тапсырылады. Бұл жағдайда желі қолданушылары мен дизайнерлеріне орналастыруға ыңғайлы, оңай, әрі сенімді үшінші тарап қолдайтын орталықтандырылған архитектураны таңдауы тиіс болады. Таңдалған мүшелер тобы деп, жүйені қадағалап, жаңартуға жауапты түйіндер болып саналады және жүйенің реестріне қатысады. Олардың тұлғалары белгілі немесе белгісіз де болуы мүмкін. Бұл түйіндер мақсатты әрекеттерді жасайтын таңдау әдістерінің маңызды аспекті болып саналады. Ішінара орталықтандырылған жүйелер таратылған реестрді қабылдау, консенсусқа

жауапты топты құру және сыртқы сенімді жүйелермен байланысты құрылымдау сияқты бірқатар мүмкіндіктерді қамтиды. Кез келген адамға ашық қолжетімділікті қамтамасыз етудің орнына блокчейндер пайдаланушыларға оқу және жазу, рұқсат параметрлерін береді немесе алып тастай алады. Транзакциялар журналын оқуға бір рұқсат беруден бастап транзакцияларды тексеру мүмкіндігіне дейін рұқсаттарды арттыруға болады. Блокчейндер тапсырма бойынша желідегі қатысушыларды таңдап оларға керекті желі аспектілерін қолдануға рұқсат береді [26].

Қолжетімділікті басқару. Бұл жағдайда желі пайдаланушыларының тұлғасы толығымен белгілі болуы керек. Содан кейін ғана деректер тізімінде кез келген өзгертулердің түрін енгізуге рұқсат беріледі. Бұның барлығы сенімділіктің әртүрлі деңгейлері мен әртүрлі түйін рөлдеріне байланысты болуы мүмкін. Транзакцияларды тексеру үшін сыртқы айнымалыны байланыстыру үшін тағайындалған насанға сену немесе сенбеу керектігін таңдауға болады. Түіндер арасындағы рөлдерде кез келген шектеулерге қарамастан, тексеру процесін шектеулі ортаға сеніп тапсыруды шешкеннен кейін барлығы дұрыс жұмыс істеп тұрғаны тексеріледі. Осы блоктардың тұтастығы мен түпнұсқалығын тексеруді көп жағдайда валидаторлардың өздері жүзеге асырады және бір бірімен байланысты блоктардың жарамдылығын қайта тексеруден өткізеді. Блокчейн мөлдірлігі кез келген желі қатысушысына қолжетімді блоктың тиесілі хаттамаларға сәйкес орындалғанын тексеруге мүмкіндік береді, өйткені осы кезде барлық желі түйіндерінің пайдаланушыларға көрінісі бірдей болады. Басқа жағынан бұл тексерістер қатысушылардың немесе пайдаланушылардың арасындағы көзқарастары әртүрлі болған жағдайда орталық түйінге тапсырылады [27].

2 Ультра жеңіл RFID аутентификациясын жасау жүйесін зерттеу

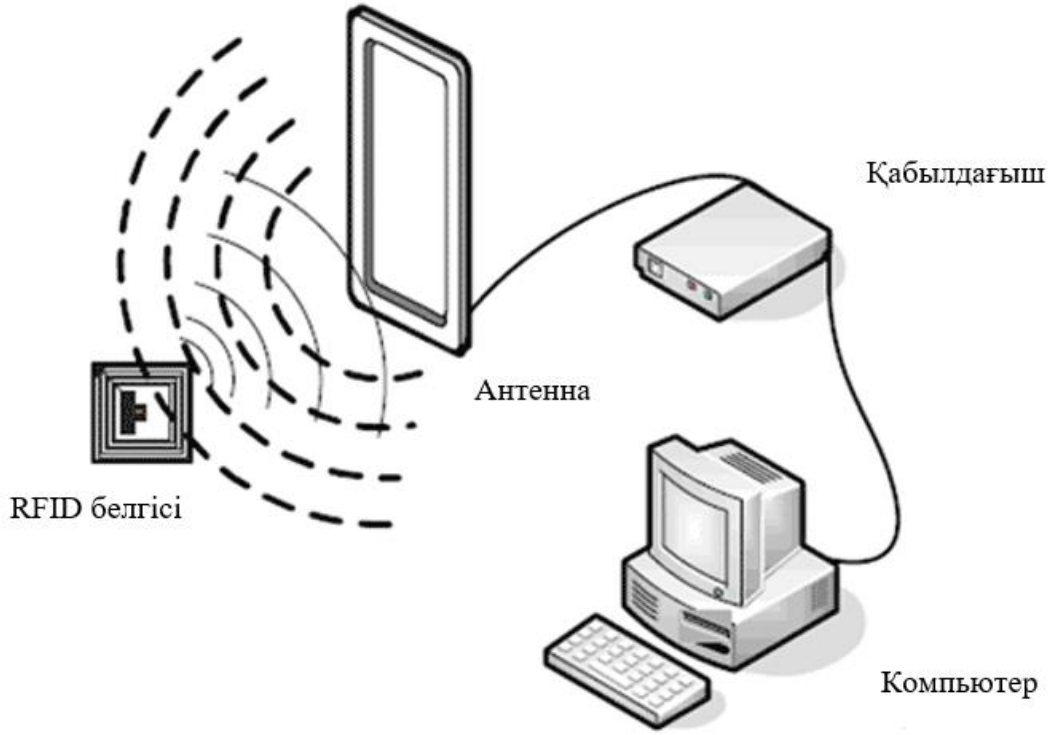
2.1 RFID радиожиілікті сәйкестендіру жүйесі

Осы уақытқа дейін (RFID) радиожиілік сәйкестендіру технологиясының белсенді дамуының арқасында сақталған ақпаратты оқу және беру үшін радиотолқындарды пайдалана отырып объектіні тез және дәл анықтау немесе аутентификациялау мүмкіндігін ұсынды. Кәзіргі таңда қолжетімділікті басқару жүйелері, бөлшек сауда, логистика, төлем жүйелері, жануарларды есепке алу жүйелері, ауруханалар, оқу орындары және басқа да көптеген салалар RFID технологиясын тиімді пайдалануда. RFID тегтері нарығы жыл сайын бірдей қарқынмен кеңейіп келеді. RFID көптеген артықшылықтарды ұсынады. Мысал ретінде, RFID тегтерінің кейбір түрлері арзан және пайдаланудың қарапайымдылығына байланысты ішкі қуат көзін қажет етпейді. Тегтерді ондаған метр қашықтықтан оқуға болады және олардың кішкентай өлшеміне байланысты әртүрлі нысандарға оңай жабыстырылады. Соңғы жылдары бұл технологияның танымалдылығының жылдам өсуі бұл артықшылықтардың себебі болып табылады. Кез келген жаңа және тез дамып келе жатқан технология сияқты, талап етілетін ашық халықаралық стандарттарды құру процесі әлі де аяқталмаған [28].

2.1-сурет – RFID белгілерінің түрлері

2.1-суретте RFID белгілерінің түрлері көрсетілген. Бастамада RFID жүйесі қолданысқа шыққан сәтте, бұл технологияны логистикада тауарларды бөлу және

табу үшін қолданылатын. Кәзіргі кезде RFID технологиясын қолдану аясы үлкен және түрлері сан алуан болып келеді. Мысалы, кізіргі кезде қолданылатын «оңай» карталары, шәкіртақыны алатын банктік карталар, үйге кіру кезінде қолданылатын домофондық кілттер, метрода турникеттен өтуде салатын тиын түріндегі RFID берлгілер, ауруханаларда қолданылатын білезіктер, төлем жүргізу және ақпарат алу үшін жапсырма түріндегі белгілерде жатады. Оған қоса болашақта шығатын xiaomi компаниясының «su7» автокөлігі xiaomi smart watch сағатымен RFID арқылы бұғатталып ашылатын болады екен.



2.2-сурет – RFID жүйесінің негізгі компоненттері

2.2-суретте RFID жүйесінің негізгі компоненттері көрсетілген. RFID белгілері (транспондерлері) және қабылдағыштары RFID жүйесінің құрамдас бөліктері болып табылады. Қабылдағыштар антенналары транспондерлерді қуаттандыру және деректерді беру үшін пайдаланылуы мүмкін радиоарна жасайды [29].

Төменде RFID оқу құралының негізгі бөліктері берілген:

- басқару блогының радиожиілік модулі (таратқыш және қабылдағыш), жады және орталық процессор;
- сигналды қабылдайтын және жіберетін байланыс элементі (антенна);
- тұрақты қуатпен қамтамасыз ететін бөлігі. Сонымен қатар, көптеген қабылдағыштар алынған деректерді басқа жүйеге, мысалы, басқару жүйесіне немесе дербес компьютерге тасымалдауға мүмкіндік беретін қосымша интерфейспен жабдықталған.

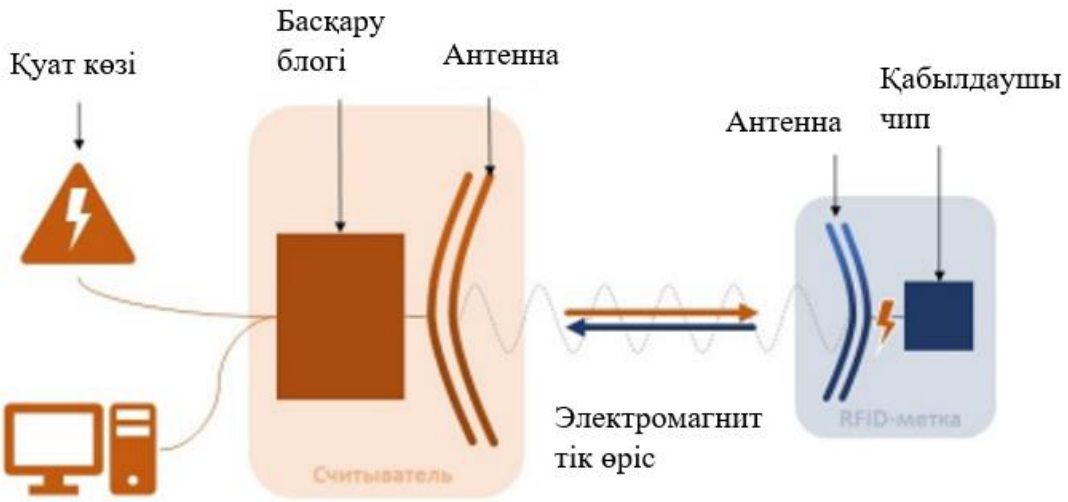
RFID тегінде әдетте екі бөліктен тұрады:

• сигналдарды жіберетін және қабылдайтын байланыс элементі (антенна); жадтан, процессордан, таратқыштан және қабылдағыштан, сондай-ақ ақпаратты өңдейтін басқа компоненттерден тұратын чип.

RFID белгісі жиі пассивті элемент болып табылады, яғни RFID оқу құрылғысынан айырмашылығы оның жеке қуат көзі жоқ (бірақ кейбір белгілер «белсенді» деп аталады, яғни олар тәуелсіз қуат көзімен жасалған). Пассивті белгілер жұмыс істеуге қажетті барлық энергияны RFID оқу құрылғысынан өндірілетін электромагниттік өріс арқылы алады [28].

2.2 RFID жүйесі элементтерінің өзара әрекеттесу принциптері

Жақын өрісте жұмыс істеу және алыс өрісте жұмыс істеу белгілердің жұмыс жиілігі мен қабылдағыш қашықтығына байланысты электромагниттік өзара әрекеттесу түрін және жауап сигналының қалай берілетінін анықтау үшін пайдаланылуы мүмкін екі әдіс болып табылады. Қабылдағыш пен белгі жеткілікті жақындаған кезде электромагниттік байланыс орын алады, энергияны белсендіреді және белгіге тасымалдайды. Бұл өзара әрекеттесу формасы немесе тег пен қабылдағыш арасындағы байланыс түрі, тег қай қабылдағыш өрісінде жұмыс істейтініне (жақын немесе алыс) байланысты өзгеруі мүмкін. Жақын жердегі жұмыс жағдайында бұл механизмдерге сыйымдылық немесе индуктивті антенналар жатады, әсер ететін электромагниттік толқын тудыратын токтардан туындайтын байланыс. RFID жүйесінің негізгі компонентерінің әрекеттесу сұлбасы 2.3-суретте көрсетілген.



2.3-сурет – RFID жүйесінің негізгі компонентерінің әрекеттесу сұлбасы

Сәйкестендіру мақсатында белсенді тег қабылдағышқа сигналмен жауап береді. Бұл ең қарапайым жұмыс істеу кезінде RFID тегі өзінің бірегей идентификаторынан басқа ештеңе жібермейтінін білдіреді. Сұраныс-жауап негізіндегі екі жақты ақпарат алмасу криптографиялық есептеулерді

жеңілдететін барған сайын күрделі жүйелерде орын алады. Өзара әрекеттесу тараптары өздерін сәйкестендіруі және бір-бірін аутентификациялауы керек (бір жақты немесе екі жақты). Қосымша деректер осы уақытта тараптар арасында ашық немесе қауіпсіз түрде жіберіледі. Деректер қабылдағыш пен тег арасында контактісіз түрде жіберіледі. Ол тұрақты көзден қуат алатындықтан және белсенді таратқыш болғандықтан, қабылдағыш кез келген дерлік физикалық ақпаратты беру техникасын (модуляция) қолдай алады және шығыс сигналды өздігінен жасай алады. Тегте немесе белгіде белсенді таратқыш болмағандықтан, ақпарат тегтен қабылдағышқа, кейін қабылдағыштан белгіге сигналының модуляциясы (оның бірегей өзгерісі) арқылы беріледі, содан кейін оны қабылдағыш тіркейді. Нәтижесінде, барлық хаттамаларда қабылдағыш байланысты бастайды, ал RFID тегі тек хабарларға жауап береді. Бұл жағдайда модуляция механизмін таңдау тег үшін қатты шектелген және тег пен қабылдағыш арасында болатын өзара әрекеттесу сипатына байланысты. Сәйкестендіру туралы шешім деректерді өңдеу аяқталғаннан кейін және RFID тегіне қосылу аяқталғаннан кейін қабылданады [29].

2.3 RFID жүйелерінің негізгі сипаттамалары

Қазіргі уақытта көптеген ерекше RFID жүйелері қол жетімді болып табылады. Белгілі бір баламаны таңдау бір-бірімен тығыз байланысты бірнеше факторларды қарастыратын келісімге келу формасы ретінде түсінуге болады. Осы факторлардың барлығы ең жақсы RFID жүйесін таңдау процесін жеңілдету мақсатында қарастырылады. Жүйені таңдау процедурасы жиі екі кезеңге бөлінеді:

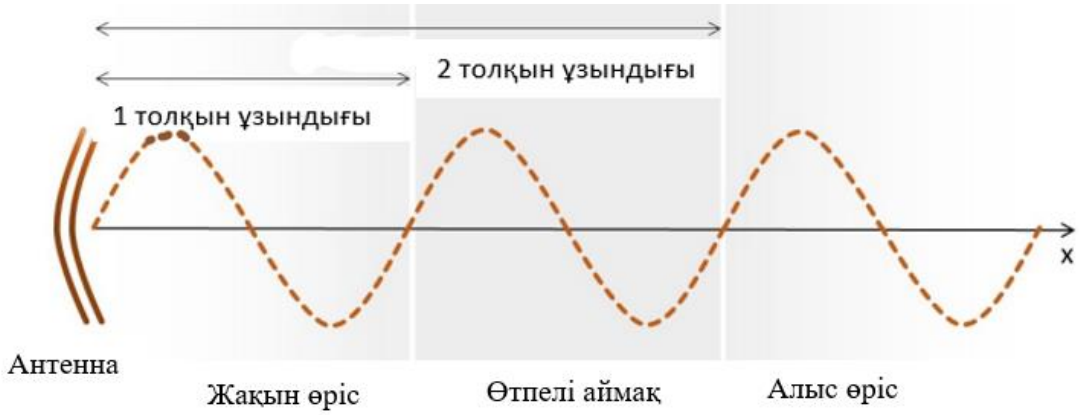
Бірінші қадам ретінде жаһандық ISO стандартына сәйкес RFID тегтерінің түрін таңдау ұсынылады. Осы кездегі ең негізгі сипаттамалар, яғни жиілік және диапазон негізінен қарастырылып отырған RFID жүйесінің қаншалықты кеңінен қолданылатынына негізделген.

Екінші кезеңде қолданылатын чиптің түрі анықталған соң RFID тег чипінің нақты техникалық ерекшеліктерін анықтау ұсынылады. Бұл жағдайда белгіленген RFID жүйесінің қауіпсіздік қажеттіліктері мен бюджеттік шектеулер соңғы технологиялық сипаттамалардың негізгі анықтаушылары болып табылады. Мысалы, құны төмен чиптің шағын ауданы оған қажетті қауіпсіздік мүмкіндіктерін беретін күрделі криптографиялық хаттаманы жүзеге асыруға кедергі жасайды, ал бюджеттік жадтың құбылмалылығы кез келген есептегіштерді пайдалануды болдырмайды және статикалық ішкі күйлері бар тізбектерді ғана пайдалануға мәжбүр етеді [28].

2.3.1 RFID тегтерінің физикалық сипаттамалары

Жақын және алыс өрістер. RFID тегтері мен қабылдағыштары жақын немесе алыс өрістерде жұмыс істейтін етіп конфигурацияланады. Қабылдағыш

антеннасының бір толқын ұзындығының аймағында қабылданса жақын өріс деп аталатын сигнал беру аймағы жатады. Антеннадан толқын ұзындығынан екі есе үлкен арақашықтықта орналасқан аймақ алыс өріс деп аталады. Антеннаның жақын және алыс аймақтары 2.4-суретте көрсетілген.



2.4-сурет – Антеннаның жақын және алыс аймақтары

Жақын аймақта жұмыс істеу сипаттамалары келесідей болады:

Антеннаның түрі: өлшемдері толқын ұзындығынан айтарлықтай аз болатын кішкентай жақтаулар (катушкалар) пайдаланылады.

Өрістің шығу процесін былайша сипаттауға болады: жақын өрісте электр және магнит өрістері қосылмаған және қолданылатын антенна түріне байланысты біреуі екіншісінен күштірек болуы мүмкін: қарапайым диполь электр өрісін береді, ал шағын контур магнит өрісін береді.

Тег пен оқу құралы арасындағы байланыс түрі сыйымдылық (электр өрісі) немесе индуктивті (магниттік өріс) болуы мүмкін. Индуктивті байланысқан жүйелер қол жетімді жақын өрістегі RFID жүйелерінің ең жиі қолданылатын түрі болып табылады. Жақын өрістегі RFID жүйелері негізгі орам (оқушы антеннасы) арқылы өтетін ток өзінің айналасында магнит өрісін тудырады және ол оған енген кезде екінші орамда индукциялық ток пайда болады, ол чипті зарядтау үшін қолданылады. Өріс кернеулігінің төмендеуінің сипатын былай сипаттауға болады. Электр өрісінің кернеулігі $1/r^3$ пропорционалды түрде төмендейді, ал магнит өрісінің кернеулігі $1/r^2$ пропорционалды түрде төмендейді, мұндағы r - антеннадан қашықтық. Бұл айырмашылықтар, ең алдымен, өабылдағын антенна мен тег арасындағы индуктивті байланыстарды қолданудың танымалдылығына жауап береді. Жақын аумақта жұмыс істейтін жүйелерде айтарлықтай жұмыс ауқымы шектеулері бар, көп жағдайда 1 метрге дейін деп есептеледі, өйткені қуаттың төмендеуі ұзақ қашықтықта маңызды болады [29].

Келесі сипаттамалар алыс өріс жұмысын анықтайды:

Антенна түрі: жартылай толқынды дипольдер сияқты резонанстық антенналар жиі пайдаланылады. олардың өлшемдері әдетте олар жіберетін сигналдың толқын ұзындығына сәйкес келеді. Бұл сипаттама қысқа толқын ұзындығы дұрыс өлшемдегі антенналарды пайдалануға мүмкіндік беретін

жоғары жиілікте алыс өрістік байланыс жүйелері жұмыс істейтінін көрсетеді. Бұдан басқа, толқын ұзындығы ондаған немесе жүздеген метрден асатын жүйелер бұл секторда пайдалануға арналмаған.
Өріс күші төмендеу сипаты келесідей: электр және магнит өрісінің кернеулігі 1/r пропорционалды түрде төмендейді, мұндағы r – антеннаның қашықтығы. Қорытындылай келе, бұл мүмкіндік алыс өрісте өзара әрекеттесетін жүйелердің айтарлықтай қашықтықта жұмыс істей алатынын білдіреді. Оқу диапазонында дәлірек шектеулерді орнату жүйенің жақын өрісте жұмыс істеген кезінде мүмкін болады, өйткені бұл кезде кернеу мен қуат айтарлықтай тезірек төмендейтін жағдайда болады [30].

2.4 RFID тегтерінің қуат көзі бойынша түрлері

RFID тегтері пайдаланатын энергия көзіне байланысты пассивті немесе белсенді болып жіктеледі. Қабылдағыштың электромагниттік өрісі пассивті RFID тегтерінің жұмыс істеуіне қажетті барлық энергиямен қамтамасыз етеді. Олардың жеке қуат көзі болмайды. Белсенді RFID тегтеріндегі ішкі автономды батареясы чиптің жұмыс істеуі үшін қажетті энергияның барлығын немесе бір бөлігімен қамтамасыз етіп отырады. RFID тегтерінің тағы бір түрі, жартылай белсенді тег. Бұл тег түрінде қосымша қуат көзі де, белсенді таратқыштың болуыда ескеріледі. Жартылай белсенді тегтердің белсенді таратқышы бар, бірақ батареясы жоқ, ал белсенді тегтерде осы элементтердің екеуі де болады. Ал пассивті тегтерде бұл екі элемент болмайды. Пассивті RFID тегтерінің негізгі сипаттамалары келесідей, деректерді тұрақты жадта сақтай алмайды, себебі олар оқу құралынан жойылған кезде ақпаратты сақтай алмайды, шексіз дерлік қызмет ету мерзімі бар, өйткені олар автономды қуат көзін ауыстыруды қажет етпейді, ықшам болуы мүмкін және өндіруге арзанырақ болады. Жұмыс істеу үшін қуаттырақ RFID оқу құралдарын қажет етеді.

Белсенді RFID тегтерінің негізгі сипаттамалары мынадай. Олар деректерді тұрақты жадта сақтай алады. Автономды қуат көзінде жинақталған энергия көлеміне байланысты олардың қызмет ету мерзімі шектеулі болады. Олар көлемі жағынан үлкенірек және өндіруге және ұстауға қымбатырақ. Олар ұзақ қашықтықта жұмыс істей алады, қуаттылығы аз RFID оқу құралдарын пайдалануға мүмкіндік береді [31].

2.5 RFID жұмыс істеу жиілігі мен қабылдау арақашықтығы

ISO 18000 сериясының стандарты RFID тегтері пайдаланатын әрбір операциялық жиілік жолағы үшін арнайы әзірленген. Ультра жоғары жиілікті тегтер (UHF және SHF) ұзақ қашықтықта оқуға арналған (UHF тегтері үшін ондаған метр, SHF тегтері үшін жүздеген) және қабылдағышқа қатысты ақпарат тасымалдау жылдамдығын арттыруға мүмкіндік береді. Олар көбінесе алыс

өрісте қолданылады. Осыған қарамастан, осы жиілік диапазонына сәйкес келетін жақын өрістегі RFID жүйесінің шешімдері бар. Әдетте бұл құрылғылардың жұмыс ауқымы толқын ұзындығының аздығына байланысты ондаған сантиметрмен шектеледі. LF және HF диапазонының тегтері үшін тег пен қабылдағыш арасындағы қашықтық үшін дәлірек шектеулерді орнатуға болады, олар тек жақын өрісте жұмыс істей алады және бір метрге дейін қысқартылған оқу радиусы бар. ISO стандарттарына сәйкес, оқу диапазонына негізделген HF диапазонының тегтері үшін басқа түрлері бар [32]. RFID тегтерінің жұмыс істеу жиілігі бойынша түрлері 2.1 кестеде көрсетілген.

2.1 кесте - RFID тегтерінің жұмыс істеу жиілігі бойынша түрлері

Жиіліктер диапазоны	Вакумдағы толқын ұзындығы	ISO стандарты	Жиілігі
125 кГц	230м	ISO 18002	Төмен жиілік - LF
13,56 МГц	2,2м	ISO 18003	Жоғары жиілік - HF
860 МГц	30 см	ISO 18006	Ультражоғары жиілік - UHF
2,45 ГГц	11 см	ISO 18004	Микротолқындар - SHF

2.2 кесте - Сканерлеу қашықтығы бойынша HF диапазонының тегтері

Оқу арақашықтығы	ISO стандарты	Белгі немесе тег түрі
1 см-ден төмен	ISO 10536	Жақсы әрекеттесетін тег
10 см-ден төмен	ISO 14443	Жақын өрістегі тег
1 м-ден төмен	ISO 15696	Алыс өрістегі тег

Ең ұзын толқын ұзындығы мен төмен жиілікті тегтерді LF жиілік диапазоны анықтайды. Бұл тегтерді радиожиілік сигналдарына қарсы, мысалы, су мен металлға жақын аймақтарда пайдалану мүмкіндігі ұзағырақ толқын ұзындығының қоршаған ортаның кедергілеріне сезімталдығының төмендеуімен мүмкін болады. LF тегтерінің өндірісте жиі қолданылуы жануарларға ілдіретін микрочиптері болып табылады. Практикалық тұрғыдан алғанда, жоғары жиілікті тегтер ең кең таралған және криптографиялық операцияда қолдауды жиі пайдаланады. Олар өте танымал, өйткені олар қауіпсіздік стандарттары жоғары жүйелерде қолданылуы мүмкін, өйткені олар жақын жерде жұмыс істейді. Сканерлеу қашықтығы бойынша HF диапазонының тегтері 2.2 кестеде көрсетілген. Сондықтан, мысалы, метро карталары сияқты транзиттік карталар үшін тегтің сканерлеу радиусы он миллиметрден аспауы өте маңызды. Егер олай болмаса, турникетте бір-бірінің қасында кезекте тұрған басқа қолданушылардың

көптеген карта көрсеткіштері бір біріне кедергі келтіріп қиындықтар туындайды. Криптографиялық әдістермен ғана тоқтатылуы мүмкін емес релелік шабуылдардан тиімдірек қорғаныс әлеуеті шағын оқу радиусы бар тегтердің пайдасына тағы бір дәлел болып табылады. Релелік шабуылдардың алдын алу үшін рұқсат етілген оқу қашықтығы шектеулі орталарда сигналдың таралу жылдамдығын ескере отырып, жауап беру уақытын шектеу қолданылады, бұл қашықтық неғұрлым қысқа болса және сигнал қоршаған ортада неғұрлым баяу таралса, тәсіл соғұрлым тиімдірек жұмыс істейді [33].

2.3 кесте - RFID тегтерінің жұмыс істеу жиілігі және қолдану аясы

Жиілік диапазондары	Стандарттары	Қолданылу аясы
Төмен жиілікті RFID белгілері 125 кГц - LF	ISO 14223	Көліктік тану тегтері, жануарларға қойылатын белгілер. (мәселен, сиырға тағатын сырға тәріздес тегтер)
Жоғары жиілік диапазонындағы RFID белгілері 13,56 МГц - HF	ISO 14443	Төлем жүргізу бағдарламалары, қолжеткізуді басқару технологиялары, логистикадағы тану үшін қолдану, смарт карталар.
Ультражоғары диапазондағы RFID белгілері 860 МГц - UHF	ISO 18006 ISO 18185	Логистикаға арналған контейнерлерді тану бағдарламалары.
Микротолқындар диапазонындағы RFID белгілері 2,45 ГГц - SFH	ISO 17363	Заттар мен тауарларды идентификациялау.

UHF тегтері шын мәнінде HF тегтеріне қарағанда аз таралғандықтан және көбінесе өндірістік шығындарға көбірек талаптар қоятындықтан, олар жақын жерде жұмыс істей алмайды. Бірақ, өнеркәсіпте, ғылымда немесе медицинада қолданылатын жабдық жеткілікті құнды болса мұндай тегтерді пайдалану кепілді болуы мүмкін. RFID тегтерінің жұмыс істеу жиілігі және қолдану аясы 2.3 кестеде көрсетілген. Оқу бірнеше метрде сәтті болуы керек және жүкті сәйкестендіру жүйелері мен логистикалық қосымшалар жағдайында тегтің оқырманға қатысты қозғалуына мүмкіндік беруі керек. Осындай тапсырмаларды өнеркәсіпте қолданылатын UHF және SHF тегтері орындай алады. RFID белгілерінде өте ұзақ қашықтықта жұмыс істеуді қамтамасыз ету үшін қажетті қуатты алуға мүмкіндік беретін тәуелсіз энергия көзі жиі қолданылады [34].

2.6 RFID құралдарындағы жады түрлері

RFID белгілері, тегтері немесе транспондерлеріндегі орналасқан чиптерде жадының екі түрі бар: тұрақты жад (RAM, SRAM, DRAM және т.б.) және

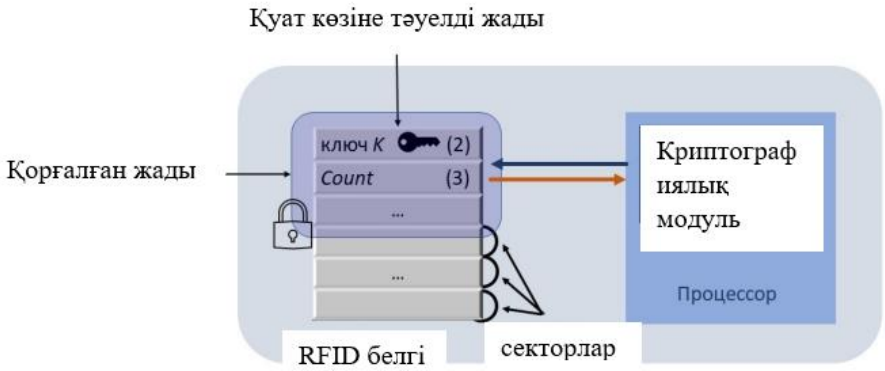
тұрақты емес жад (ROM, EEPROM және т.б.). RFID тегтері тұрақты жадты қажет етпейді, өйткені оларда деректерді сақтау шектеулі және анықтаушы ақпаратты ғана оқи алады. Дегенмен, күрделірек функционалдығы бар тегтерді пайдаланған кезде көбірек жад және деректерді жылдам оқу қажет болады, бұл белгілі бір тұрақсыз жедел жады түрлерін пайдалануды қажет етеді. Тұрақты емес жад түріне негізделген RFID тегтерін оқу және жазу үшін үш санат бар.

Тек оқуға арналған (Read Only): жадта сақталған деректерді өзгерту мүмкіндігі жоқ RFID тегі.

Бір рет жазу және бірнеше рет оқу (WORM): пайдаланушыға деректерді ішінара немесе толық бір рет жазуға және бірнеше рет оқуға мүмкіндік беретін RFID тегі.

Бірнеше рет жазумен және бірнеше рет оқу (RW): өзгертуге және оқуға болатын деректерді сақтайтын жады бар RFID тегі, жад блоктарының қайта жазу циклдерінің әдеттегі диапазоны жүз мыңнан бір миллионға дейін саналады.

Күрделі жады бар RFID тегтері, сөзсіз, күрделірек криптографиялық әдістерді енгізуге мүмкіндік береді және қауіпсіздіктің жоғары деңгейін ұсынады, бірақ тегтің құны да айтарлықтай өседі. RFID тегінің жады белгілі бір түрін таңдау тегтің қауіпсіздік мүмкіндіктері мен оның құны арасында таңдауды қажет етеді. Тек оқуға арналған RFID тегтері криптографиялық протоколдарды қолдамайтынын ескеру керек, өйткені оларға кілт жазу мүмкін емес [35]. 2.4-суретте RFID белгісіндегі жадымен әрекеттесу сұлбасы көрсетілген.



2.4-сурет – RFID белгісіндегі жадымен әрекеттесу сұлбасы

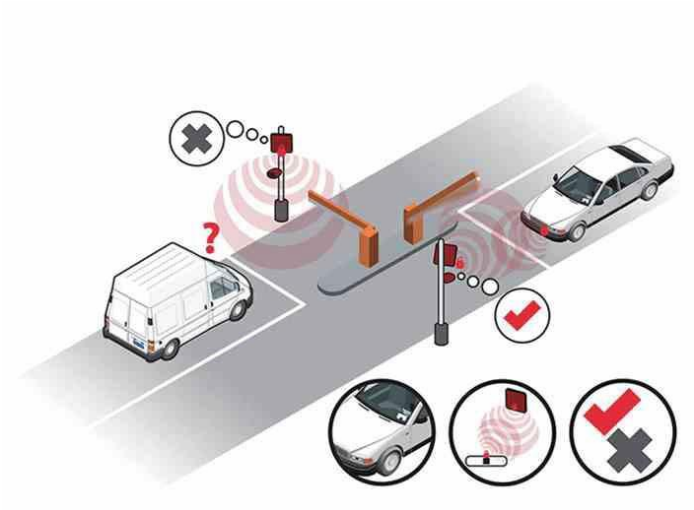
Сырттан қол жетімсіз және құпия протокол параметрлерін сақтайтын қорғалған жады аймағын пайдалану тегтердің мүмкіндіктерін кеңейту үшін қажет. Жадтың бұл түрі әдетте құпия сөздерді, кіру есептегіштерін және физикалық кедергілерді болдырмауды қоса алғанда, криптографиялық емес әдістер арқылы қорғалады. Кейбір RFID тегтерінде жеке кілттерді, пайдаланушы жады секторларына кіру рұқсаттарын және басқа маңызды деректерді сақтау үшін пайдалануға болатын конфигурация жады бар. RFID тегін жекелендіру процесі конфигурация жадын бағдарламалауды қамтиды. Конфигурация жадын бағдарламалау процедурасының соңында жадтың белгілі бір аймақтарын блоктайтын сақтандырғыштардың дәйекті түрде қарастырылып жадты бір рет

бағдарламаланатын етеді (OTP - бір рет бағдарламаланған жады). Әдетте, мұндай жадқа кіру үшін бірегей құпия сөз қажет. Әртүрлі қатынау есептегіштерінің мәндерін қайта жазылатын конфигурация жадысы бар тегтерде де сақтауға болады. Мысалы, рұқсат етілген құпия сөзді тексеру әрекеттерінің сәтсіз санын шектеу үшін бірегей пәрменді пайдалануға болады. Егер бұл шектен асып кетсе, қорғалған жад сегменті шексіз құлыпталады. Бұл құпия сөздерді бұзып кірудің алдын алады. Кейбір RFID тегтерінің жадты блоктаудан басқа қосымша мүмкіндігі бар: оларда ашылған кезде үзілетін белгілі бір цикл бар, бұл тегтің толық сенімді емес екенін көрсетеді. Бұл мүмкіндік тегтерді өзгертуге төзімді етеді және физикалық ашуды болдырмайды. Бұл сценарийде тег қате нәтижелерді қайтара береді, дәл деректерге қол жеткізуді болдырмайды, бұл қауіпсіздіктің қосымша деңгейі ретінде қызмет ете алады [36].

2.7 RFID технологиясын қолдану аясы

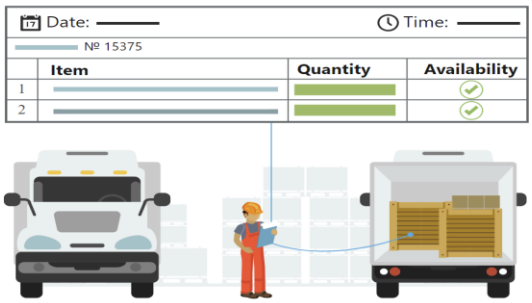
RFID жүйелерінің қолдану аясы өте үлкен. Бұл технология заттарды, объектілерді сәйкестендіру және есепке алу үшін кәсіп орындарға қажет болады. Жануарларды есепке алу үшін фермаларда қолданыла алады. Кәзіргі таңда ауруханалда науқастардың келіп түсу уақыты, сырқаты, жазылған тиесілі дәрі дәрмектері мен қабылдау уақытына дейін керекті деректер сақталуы мүмкін. Біздің бұл технологияны күнделікті қолданып жүрген аймақтарымыз ол, метро мен автобустарда онай арқылы жол ақысын төлеу кезінде, үлкен дүкендерде заттар сатып алу кезінде төлем ақы жүргізу үшін қолданылатын caspi gold сынды карталар, ойын сауық орындарына кіру кезіндегі кішкентай балаларға қолына тағатын браслеттер, шағын автотұрақтарға көлік жақындаған кезде шлакбаумның ашылу үшін сәйкестендіру, киім дүкендерінде ұрлыққа қарсы жапсырылатын жапсырмалар және тағыда басқа бөлімдерді айтуға болады. RFID технологиясы кәсіпорындарда бизнес процестің тиімділігін арттыру және адами фактордың әсерін тиісінше азайтуға мүмкіндік береді.

Автотұрақтарға көліктерді өткізу және есепке алу үшін және шлакбаумдарды автоматтандыру үшін қолдану. RFID технологиясын автокөлік пен шлакбаумдарда қолдану 2.6-суретте көрсетілген.



2.6-сурет – RFID технологиясын автокөлік пен шлакбаумдарда қолдану

Үлкен жүк көліктеріндегі тауарларды есепке алу, жұмысшының жұмыс рейстері мен жұмыс уақытын есепке алу және адами фактордың алдын алу үшін зат тасымалдауда қолдану. 2.7-суретте зат тасымалдау кезінде есепке алу көрсетілген.



2.7-сурет – Зат тасымалдау кезінде есепке алу

Кір жуу және тоқыма өнеркәсібінде тауарларды алу және жіберу үшін қолдану. Бұл жағдайда RFID компонентері суға батыру, дірілге, соққыға және температураның күр өзгеріп кетуіне төзімді әрі иілгіш болғаны қажет. тоқыма заттарына RFID белгілерін қолдану 2.8-суретте көрсетілген.

2.8-сурет – Тоқыма заттарына RFID белгілерін қолдану

Ақылды қойма және логистикада қолдану мүмкіндігі. Заттармен материалдарды есепке алу, олардың бір орыннан екінші орынға өтуін қадағалау және бақылау, затқа тапсырысты жинау кезіндегі қателіктерді болдырмау және осының бәріне жұмысалатын артық шығынды болдырмауға көмектеседі. RFID технологиясын логистикада қолдану 2.9-суретте көрсетілген.

2.9-сурет – RFID технологиясын логистикада қолдану

Сауда орындарында заттарға жапсырылатын сейкестендіру белгілерін айтуға болады. Бұл жапсырмалар тауарды тізімнен тез тауып ақысын алуға және ұрлыққа қарсы тұруға көмектеседі. RFID жапсырмаларын тауарларға қолдану 2.10 суретте көрсетілген.

2.10-сурет – RFID жапсырмаларын тауарларға қолдану

Кітап дүкендері мен кітапханаларда қолдану. Кітаптарды тез табуға тексеруге және ұрлыққа қарсы тұруға көментеседі. RFID жапсырмаларын кітаптарға қолдану 2.11-суретте көрсетілген.

2.11-сурет – RFID жапсырмаларын кітаптарға қолдану

Адамдарды тану және сәйкестендіру үшін қолдану. Сәйкестендіру және қолжеткізу үшін, жұмысшының қозғалысын бақылау және қауіпсіздігін арттыру үшін қолданылады. Қорғалған жерлерге бөтен адамдардың кіруінен сақтандырып тұрады. RFID технологиясы арқылы қолжеткізуді басқару 2.12-суретте көрсетілген.

2.12-сурет – RFID технологиясы арқылы қолжеткізуді басқару

Инвентаризация мен компания мүлкін есепке алу үшін RFID белгілері мен тегтерін қолдану. Инвентаризация уақытын қысқарту, туаурларды дәл есепке алу, адами факторды қысқарту, барлық тауарлардың дұрыс сұрыпталуы және қауіпсіздігі қамтамасыз етіледі. 2.13-суретте RFID арқылы мүлікті есепке алып басқару көрсетілген.

2.13-сурет - RFID арқылы мүлікті есепке алып басқару

Жүк контейнерлерін аз уақытта табу, тексеру және есепке алу. Көптеген контейнерлер арасынан керектісін табу, оны ашпай ақ ішіндегі заттарды тексеру. Тасымалдау жолын, заттар мен мүліктің қауіпсіздігін қамтамасыз етеді. 2.14-суретте жүк контейнерлерін сәйкестендіру арқылы есепке алу көрсетілген.

2.14-сурет – Жүк контейнерлерін сәйкестендіру арқылы есепке алу

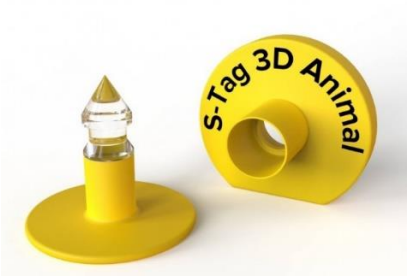
Қымбат әшекей бұйымдарындың қоймадағы жағдайы, түрі, саны, қолданылған металдар қоспасы, өлшемі, бағасы сынды барлық ақпараттың бір ғана кішкентай ілмек-белгіде болуы жұмысқа кететін уақытты қысқартады және автоматты түрде есепке алады. Зергерлік бұйымдағы RFID белгісі 2.15-суретте көрсетілген.

2.15-сурет – Зергерлік бұйымдағы RFID белгісі

Үй жануарлары мен төрт түлікті есепке алу және қолданылған дәрі-дірмек туралы ақпарат. Кәсіргі кезде қандай да бір үй жануарына ит мысықтан бастап жылқы, сиырға дейін сәйкестендіру белгілерін қолданады. Олар ит пен мысыққа арналған жағалар болуы мүмкін. Оның ішінде мекен-жай мен телефон нөмірі болуы мүмкін. Жоғалған сәтте тез табуға көмектесетін ақпарат және ветеринарға арналған вакциналық егу туралы ақпараттар болуы мүмкін. RFID чипі бар жануарлар жағасы 2.16-суретте көрсетілген.

2.16-сурет – RFID чипі бар жануарлар жағасы

Төрт түлік малға қоятын сырға тәрісдес белгіде болуы мүмкін. Оның ішінде салмағы, қойылған вакциналар түрі, т.б. процедуралар жазылуы мүмкін. Зоотехникалық есепке арналған RFID тегтері 2.17-суретте көрсетілген.



2.17-сурет – Зоотехникалық есепке арналған RFID тегтері

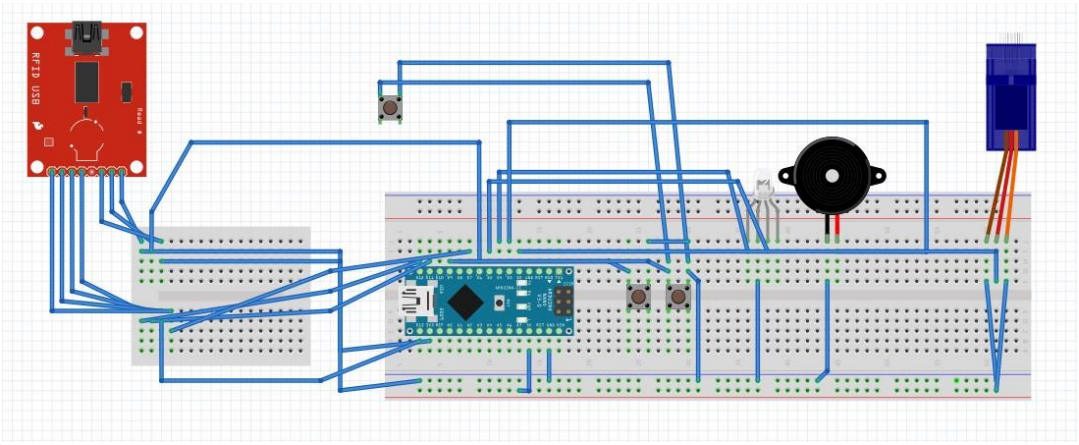
Ал медецинада науқастарға білезік тәріздес түрін қолданады. Бұл RFID тегі науқастың келіп түскен күні, сырқаты, салдары, ем түрі, ұсынылған дәрі-дәрмектер, өзі туралы ақпарат, қан тобы, тұрып жатқан мекен жайы жазылады. 2.18-суретте науқастарға берілетін RFID білезігі көрсетілген.

2.18-сурет – Науқастарға берілетін RFID білезігі

2.8 RFID сәйкестендіру және қолжеткізу құрылғысын әзірлеу

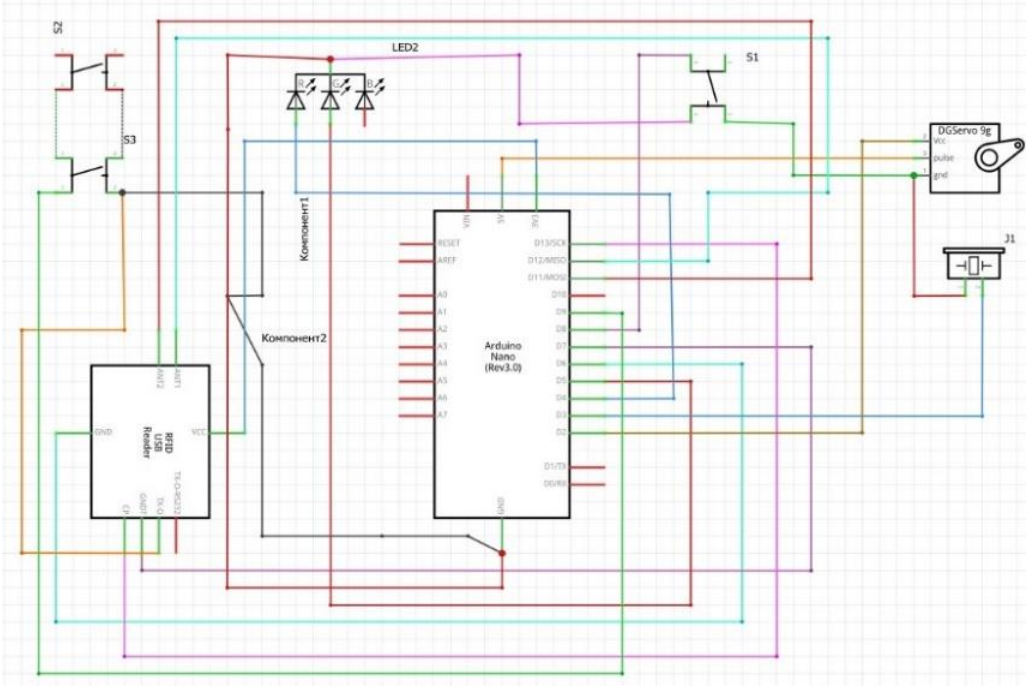
RFID сәйкестендіру және қолжеткізу құрылғысын әзірлеу барысында қолданылған құралдар мен бағдарламаларды сипаттап әр кезеңде орындалған жұмыстарға тоқталып өтетін боламын.

Құрылғыны жасаудан бұрын оның жұмыс істеу алу мүмкіндігі мен құрылғыны құрастырудағы қиындықтарды алдын ала қарастырып, жұмыс барысында шыққан қаталерді дүзеу үшін модельдеуге арналған «tinkercad» және «fritzing» бағдарламаларын қолдандым. Fritzing бағдарламасы арқылы құралды модельдеу 2.19-суретте көрсетілген. Бұл бағдарламалар ардуино негізіндегі микроконтроллерлерді модельдеп, сұлбаларға қосып, құрастырылған құралдарды сынап көруге мүмкіндік береді.



2.19-сурет – Fritzing бағдарламасы арқылы құралды модельдеу

«Fritzing» бағдарламасы құрылғыны әзірлеу процесінде автоматты түрде құрылымдық сұлбасын және бастапқы түрдегі прототипінің дизайнын көрсете алады. Бағдарламаның мақсаты зерттеушілер аудиториясы, дизайнерлер, радиоәуесқойлар секілді интерактивті электр жабдықтармен айналысатын мамандарға арнап жасалған қосымша болып табылады. AVR микроконтроллерлерін бағдармалау, компонентерімен байланытыру, өңдеу және сынап көру сынды жұмыстарды жүргізуге болатын бағдарламалық платформа. Бұл қосымшаны көбіне «DIY» жасаушылар қолданады. RFID сәйкестендіру құралының принципиалдық сұлбасы 2.20-суретте көрсетілген.

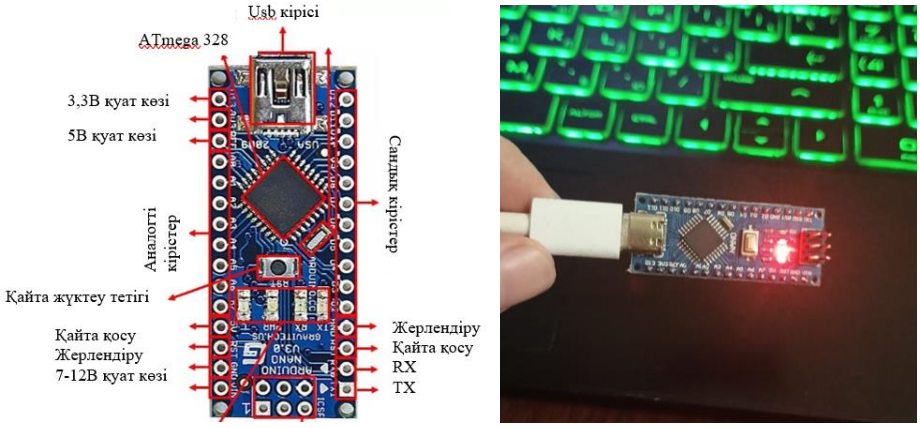


2.20-сурет – RFID сәйкестендіру құралының принципиалдық сұлбасы

Сәйкестендіру және қолжеткізу құралын жасау үшін ардуино микропроцессорлары мен қосымша бөліктерін қолдандым. Яғни Arduino nano,

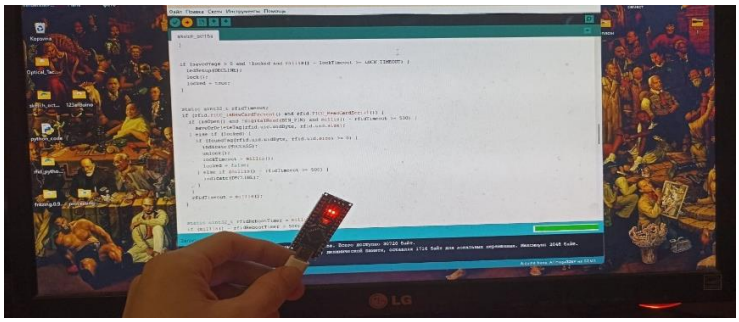
mfrc522, sg90, 5v zummer, батырмалар, дарық диодтары және қосу сымдарын қолдандым.

Arduino – бұл цифрлық құрылғыларды, дәлірек айтқанда олардың прототиптері мен макеттерін жасауға арналған платформа. Оның ішіне ақпараттық құралдар мен платалар, чиптер және бағдарламалық қамтамасыз ету ортасы кіреді [37]. Мысалы Arduino микроконтроллері менің құрастырған құралымда орталық басқарушы ретінде қолданылады. Ол RFID белгілерінен қабылданған деректерді өңдеп деректер қорына жібереді, егер RFID тегтері мен белгілерінен қабылданған деректер дұрыс болған жағдайда қолданушыға рұқсат береді. Arduino nano микроконтроллерлерінің құрылымы 2.21-суретте көрсетілген.



2.21-сурет – Arduino Nano микроконтроллері

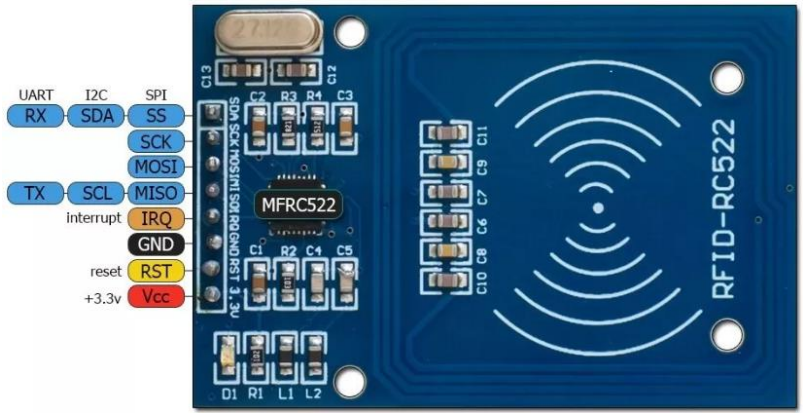
Arduino nano микроконтроллерін бағдарламалау үшін «Arduino IDE» бағдарламасы қажет болады. Бұл бағдарлама Arduino nano микроконтроллеріндегі орналасқан atmelga328ob контроллеріне керекті кодты енгізуге және ары қарай EEPROM жадына жазылған бағдарламалық кодты қолдану үшін бастапқы орнатуларды жасауға қажетті бағдарлама. 2.22-суретте Arduino IDE бағдарламасы арқылы Arduino nano микроконтроллерін бағдарламалау процесі көрсетілген.



2.22-сурет – Arduino IDE бағдарламасы арқылы Arduino nano микроконтроллерін бағдарламалау процесі

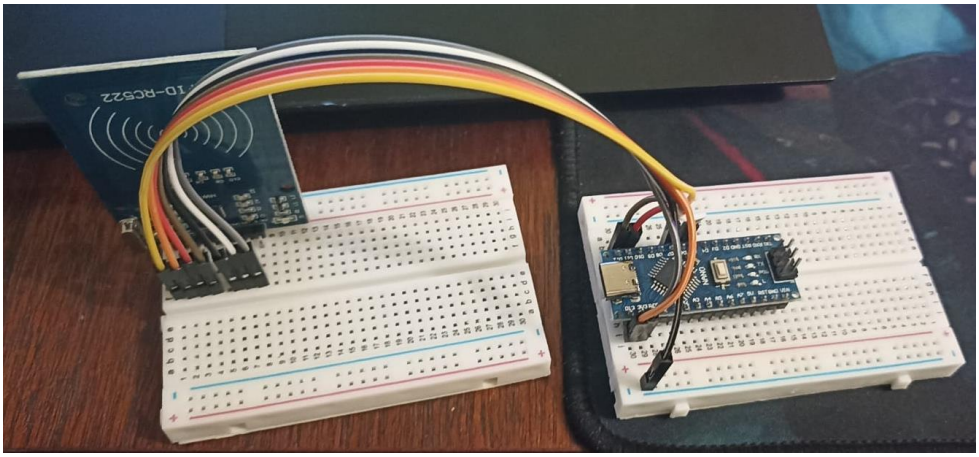
Бұл бағдарлама микроконтроллерге орнатылатын скечты тексеріп компиляциялай алады. Бұл процесс әрбір жаңа бағдарламалық кодты орнату кезінде орындалады. Бұл процесс микропроцессорда келешекте туындайтын қателерден сақтайды.

Келесі қолданылған құрал MFRC522 RFID оқу модулі. RFID құралдары әртүрлі диапазон жиіліктерінде жұмыс жасайды: LF (125-134 кГц), HF (13,56 МГц), UHF (860-960 МГц). MFRC522 модулі LF (125-134 кГц) жиілігінде жұмыс істейді. Деректерді белгіден оқу қашықтығы 0-20 мм, деректерді алу жылдамдығы 1МБит/с, пішімі 40\60 мм [38]. Пішімі кішкентай және қабылдау қашықтығы жақсы болғандықтан оны керекті макеттің немесе құрастырып отырған модельдің ішіне орналастыруға қолайлы, әрі өте икемді құрал.



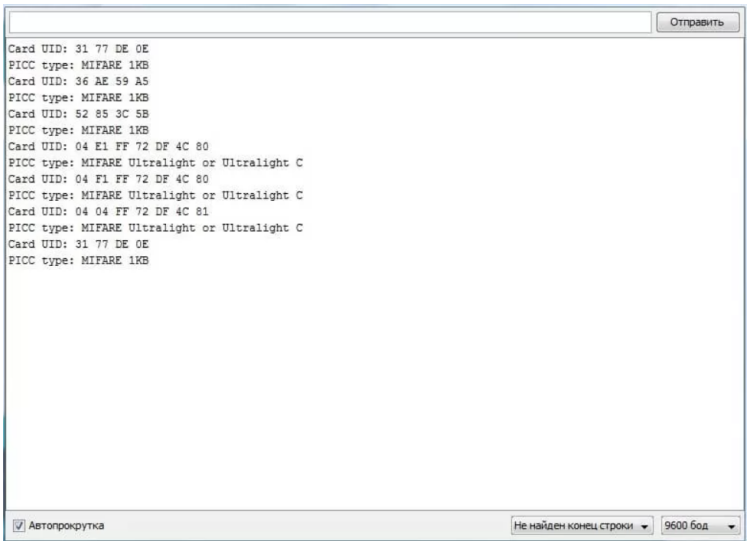
2.23-сурет – MFRC522 модулі

2.23-суретте MFRC522 модулінің түрі және ақпараттық кірістері көрсетілген. Ұсынылған RC522 модулі тегтердегі деректерді дұрыс қабылдап микроконтроллерге жіберуі тиіс. Қате шыққан жағдайда RST пині арқылы тез арада қосылып қайтадан деректерді оқи алуы қажет. 2.24-суретте RC522 модулін Arduino nano микроконтроллеріне қосу процесі көрсетілген.



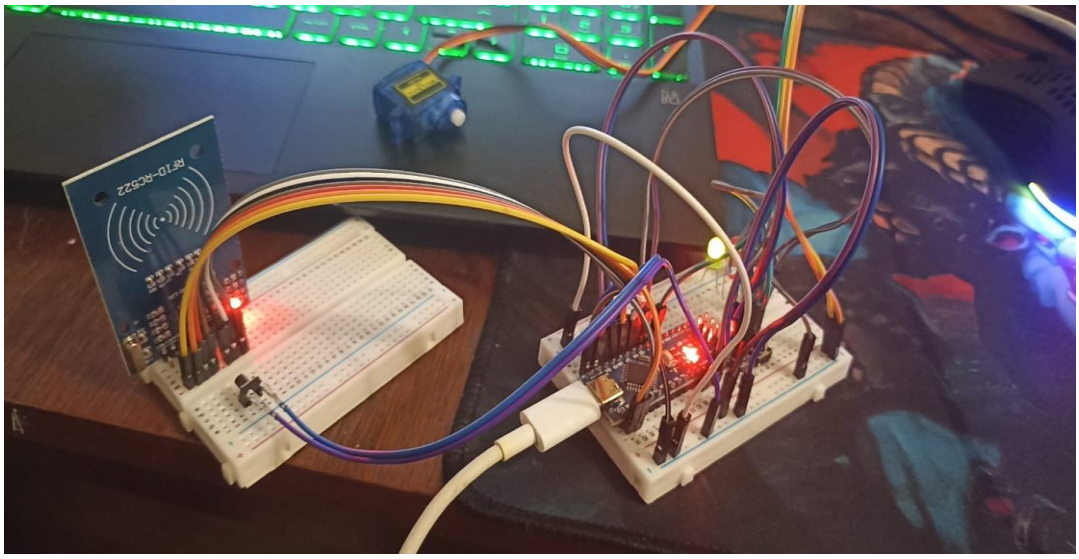
2.24-сурет – RC522 модулін Arduino nano микроконтроллеріне қосу

Суретте көрсетілген оқу құралы мен микроконтроллерін қосу арқылы оқылған RFID тегтері Arduino IDE бағдарламасында мынадай нәтижеде көрсетіледі. Бұл жерде оқылған белгінің ID нөмірі, түрі және жадының көлемі көрсетілген. 2.25-суретте RFID тегтерін оқу нәтижесі көрсетілген.



2.25-сурет – RFID тегтерін оқу нәтижесі, оқылған белгілердің ID нөмірлері

Мен жасаған RFID сәйкестендіру және қолжеткізуді басқару құралының түрі 2.26-суретте көрсетілген.



2.26-сурет – RFID сәйкестендіру және қолжеткізуді басқару құралы

2.26-суретте өзім құрастырған RFID сәйкестендіру және қолжеткізуді басқару құралы ұсынылған. Менің жұмысымның «ультра жеңіл RFID аутентификациясын жасау жүйесін зерттеу» бөлімінде arduino nano микроконтроллерін пайдалана отырып RFID аутентификациясы арқылы

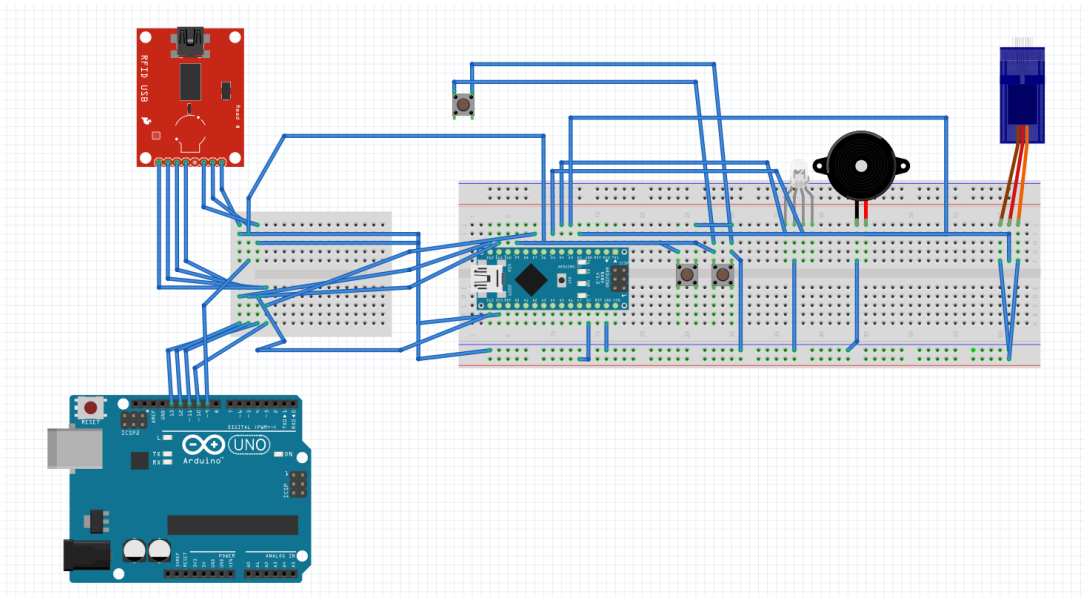
қолжеткізуді басқаратын құрал жасауды керек болды. Ұсынылған құрылғыда RFID картасы мен белгілері арқылы электронды құлыпқа арналған басқару модулін әзірлеуді талап етті. Құлыптау механизмдері ретінде sg90 сервожетегін қолдандым. Егер картадан оқылған деректер жадыда сақталған деректермен сәйкес келсе, сервожетекке сигнал жіберіліп құлыпты ашады. Оқылған деректерді өңдеуді және салыстыруды atmega328 микроконтроллері іске асырады. Өңделген деректерді сақтау EEPROM жадында орындалады. Егер картасыз жетекті құлыптау керек жағдайда орындалатын шектеу батырмасын, жаңа картаны тіркеу функциясы атқаратын және құлыпты ашу үшін қолданылатын батырмаларды қостым. Картадағы деректерді оқу барысында қолжеткізу берілген немесе берілмеген жағдайды көрсетіп тұратын дыбыстық және жарықтық индикаторларды қостым, бұл индикаторлар (RGB жарық диодтары және зуммер) бола алады. Ал қолданылып отырған карта бұдан былай керек емес болған жағдайда картаның деректерін жадыдан жойып тастайтын батырманы қостым.

Бұл құралдың жұмыс істеу принципін былай сипаттауға болады. Ең алдымен қолданушының картасын жадыға тіркеу қажет. Ол үшін картаны rc522 RFID қабылдағышына әкеліп ашу немесе тіркеу батырмасын басу керек. Қабылдағыш антенна картағы жазылған ID кодын қабылдап arduino nano микроконтроллеріне жібереді. Қабылданған деректер atmega328 микроконтроллерінде өңделіп, eeprom жадында сақталады. Осылайша карта тіркеледі. Бұл тіркелген картаны rc522 қабылдағышына қойған кезде картадағы деректер микроконтроллерге жіберіліп салыстырылады. Егер бұл карта тіркелеген болса индикатор белгі береді және сервожетекке сигнал жібереліп құлып ашылады. Керісінше жағдай туындаса, бұл карта қолданушысы ары қарай жіберілмейді және индикаторлар бұғаттау белгісін беріп құлып ашылмайды. Егер тіркелген карта жоғалған жағдайда сервожетекті ашу батырмасын басып құлыпты ашып алып, жаңа карта тіркеу қажет болады. Бірден бір карта тіркелмеген жағдайда сервожетек ашық түрде болады, оны шектеу батырмасымен жауып қоюға болады. Макетте қолданылатын индикаторлар карта арқылы және батырма арқылы ашу кезінде белгі беріп отырады. RGB жарық диодтарын қолдану кезінде, карта қабылданған жағдайда жасыл, ал қайтарылған жағдайда қызыл түспен жанады. Зуммер қолдану кезінде сервожетек ашылып жабылғанда бір сигналдан беріп отырады. Картаны тіркеу кезінда бір сигнал және картаны жою кезінде үш дыбыстық сигнал береді.

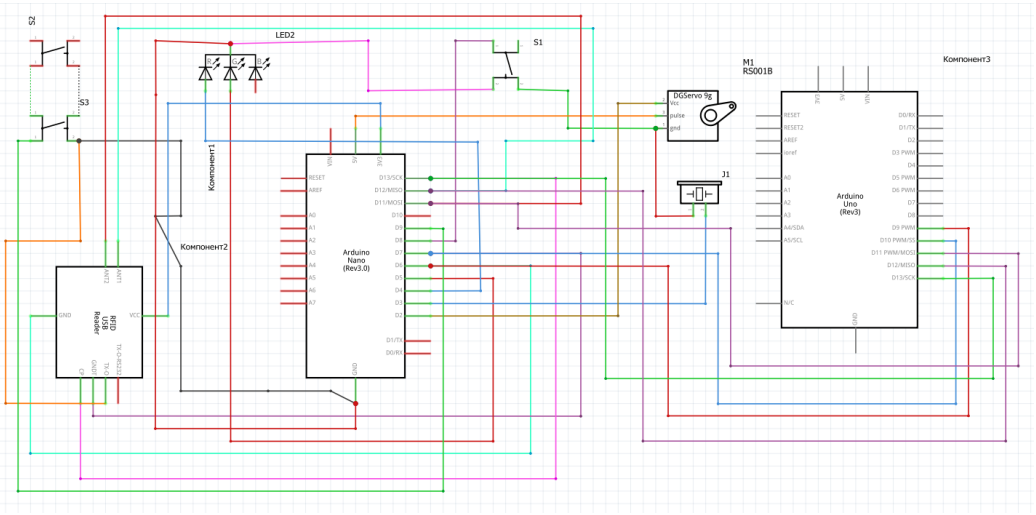
3 ультра жеңіл RFID аутентификациясын жасау жүйесін блокчейн технологиясымен жобалау

3.1 Жобаны бағдарлама арқылы модельдеу және тексеру

RFID сәйкестендіру және қолжеткізу жүйесін блокчейн технологиясымен жобалау үшін оны ең алдымен керекті барламада модельдеп тексеру керек болды. Бұл жобаны модельдеу үшін «fritzing» бағдарламасын қолдандым. Бұл бағдарлама арқылы жобаның бастапқы макетін жасап керекті сызбаларды алуға болады. Мен бұл бағдарламада екінші бөлімде көрсеткен «RFID сәйкестендіру және қолжеткізуді басқару құралын» моделдедім. Ал ендігі мақсатым RFID сәйкестендіру және қолжеткізу құралын Блокчейн технологиясымен қосу болып тұр. Ол үшін мен екінші бөлімде fritzing бағдарламасында құрастырған сұлбаға деректерді қабылдап, блоктарға бөліп, eeprom кірістірілген жадында сақтап шыққан нәтижені кестеге шығарып көрсететін құралдың сұлбасын құрастырдым. Блокчейн технологиясымен жұмыс істейтін RFID сәйкестендіру және қолжеткізуді басқару құралының құрылымдық сұлбасы 3.1-суретте, принципиалдық сұлбасы 3.2-суретте көрсетілген.



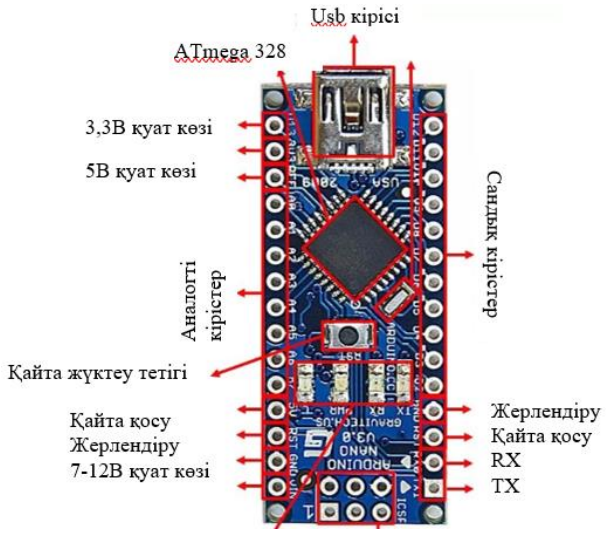
3.1-сурет – Блокчейн технологиясымен жұмыс істейтін RFID сәйкестендіру және қолжеткізуді басқару құралының құрылымдық сұлбасы



3.2-сурет – Блокчейн технологиясымен жұмыс істейтін RFID сәйкестендіру және қолжеткізуді басқару құралының принципиалдық сұлбасы

3.2 Қолданылған құрал-жабдықтар мен компонентер

3.1-суретте көрсетілген сәйкестендіру құралында Arduino nano және Arduino uno микроконтроллерлері, rc522, зуммер, sg90 сервожетегі, батырмалар, жарық диодтары және дәнекерлеусіз жеңіл қосуға арналған тақта қолданылды. Arduino цифрлық құрылғылар мен алардың макеттерін жасауға көмектесетін құрал. 3.3-суретте Arduino Nano, 3.4-суретте Arduino Uno микроконтроллерлері көрсетілген.



3.3-сурет – Arduino Nano микроконтроллері

3.4-сурет – Arduino Uno микроконтроллері

RC522 құралы өзінің өріс аумағында оқылған белгі мен тегтердің деректерін микроконтроллерге жібереді. LF (125-134 кГц), HF (13,56 МГц), UHF (860-960 МГц). MFRC522 модулі HF (13,56 МГц) жиіліктерінде жұмыс жасайды. Менің жасаған құралым LF жиілік диапазонында жұмыс істейді. Егер RFID тегтерінен алынған деректер дұрыс болмай қалған жағдайда «rst» кірісіне сигнал келіп тегтегі деректерге қайта сұраныс жіберіледі. RC522 құралының мақсаты электромагниттік өрісте картадағы деректерді қабылдап, оны цифрлық түрде микроконтроллерге жіберу болып табылады. RC522 құралы 30 суретте көрсетілген.

Зуммер немесе электромеханикалық дыбыс шығарғыш, ол жұмыс жасау үшін бес вольт кернеу беру керек. 3.5-суретте зуммер дыбыс шығарғышы көрсетілген. Блокчейн технологиясымен жұмыс істейтін RFID сәйкестендіру және қолжеткізу құралында ол қарапайым дыбыс шығарушы ретінде қолданылады. Ол сервожетекті ашу кезінде және тегтерді сақтау немесе жою кезінде дыбыс шығарады. Зуммер шығаратын дыбысты өзгерту мүмкін емес болып табылады, себебі оның резонанстық жиілігі тұрақты болып келеді.

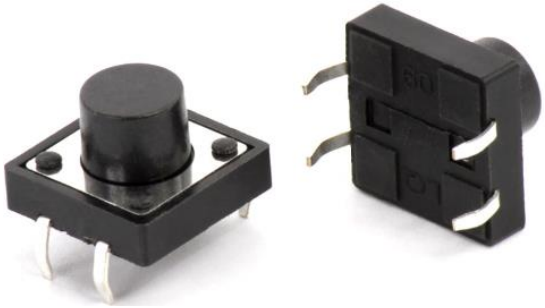
3.5-сурет – Зуммер

Sg90 сервожетегі женің, әрі жоғары сапалы сервожетек. Ол Arduino микроконтроллерлері арқылы жүзеге асырылады. Оның айналу бұрышы 0-90

және 0-180 градусқа дейін. Оны шағын механизмдер құрастыру үшін қолданады. Бұл сервожетек түрі пластик пен нейлоннан жасалған, бұл оған салмағын азайтуға мүмкіндік береді, бірақ ішкі бөліктерінің төзімділігі мен беріктігі төмендейді. Sg90 сервожетегі 3.6-суретте көрсетілген.

3.6-сурет – Sg90 сервожетегі

Тактілік батырмалар деп электр жеелісін ашатын немесе жабатын қарапайым құрылғыларды айтады (3.7-сурет). Менің жобамда бұл батырмалар сервожетекті құлыптайтын және ашатын, жаңа картаны сақтайтын немесе бастапқы картаны жоятын функцияға ие.

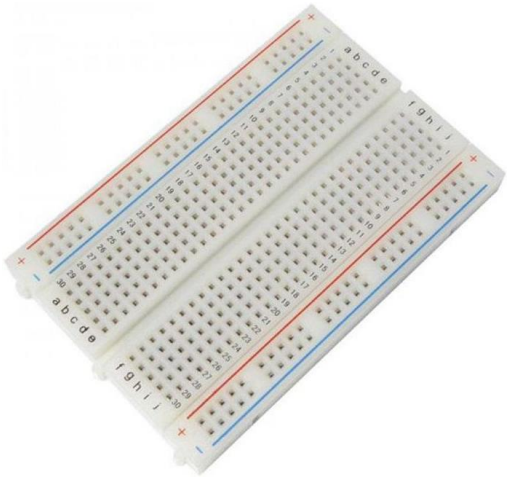


3.7-сурет – Тактілік батырмалар

Жарық диодтары құралдарда индикатор есебінде қолданылады (3.8-сурет). Жарық диодының өлшемі 5мм. Оның ішінде линза және рефлектор орналасады. Диодтың ішінен өткен тоқ кристал арқылы өткен кезде жарыққа айналады, оны линза және рефлектор сыртқа шашыратады.

3.8-сурет – Жарық диодтары

Дәнекерлеусіз қосуға арналған макеттік тақта (3.9-сурет). Ол 400 қосушы түйреуіштен тұрады. Екі шетіндегі қосу орындары қуат беруге және жер қосуға арналған. Ортасында 5 қосу контактілерінің 60 тобы орналасқан. Бұл макеттік тақта арқылы элементтердің барлығын орналастыруға және дәнекерлеусіз қосып сынап көруге мүмкіндік береді.

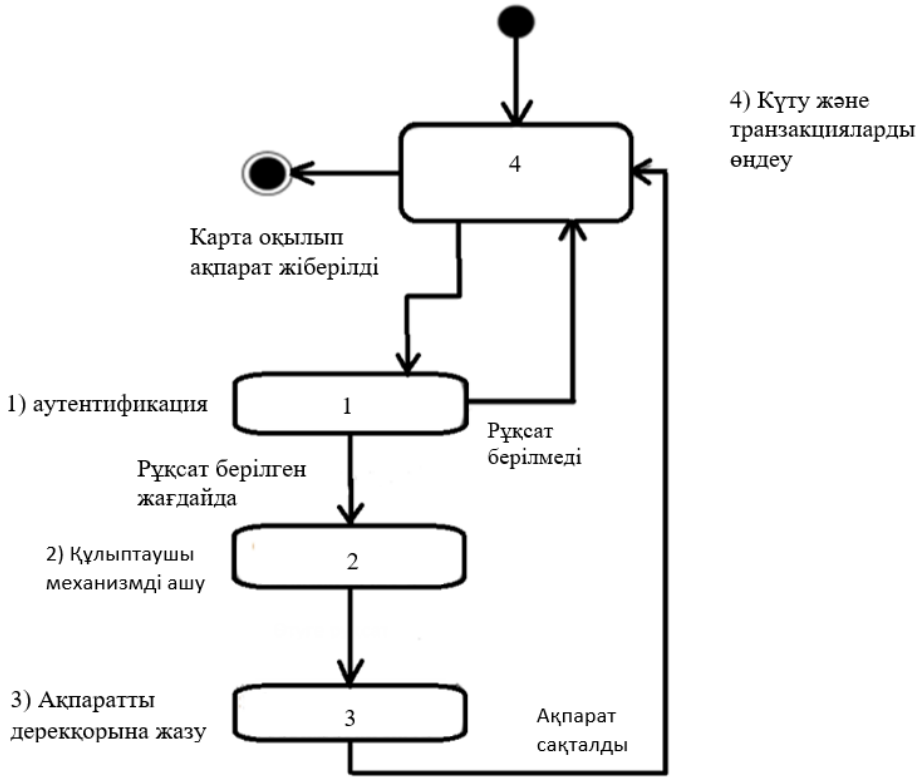


3.9-сурет – 400 нүктелік макеттік тақта

3.3 Жобаның жұмыс жасауы үшін қажетті бағдарламаларды қолдану

Жобаның керекті компонентерін микроконтроллерлерге қосудың алдында Arduino nano және Arduino uno микроконтролерлеріне жұмыс жасауы үшін қажетті бағдарламаны орнату қажет. Бұл бағдарламалық кодты Arduino IDE бағдарламасы арқылы жасауға болады. Жүктелетін бағдарламалық код микроконтроллердің eeprom жадына сақталады. Бұл код микроконтроллердің қай шығысынан қандай сигнал жіберу шартын сипаттайды. Соның арқасында компоненттер керекті реттілікпен жұмыс жасайды және қажетті ақпаратты микроконтроллерге қайта жібере алады. Жобаның жұмыс жасауына қажетті код А қосымшасында бекітілген.

Жоба бөліктеріне жүктелген бағдарламалық кодтың жұмыс алгоритмі 3.10-суретте көрсетілген.



3.10-сурет – Сәйкестендіру және қолжеткізуді басқару құралының жұмыс алгоритмі көрсетілген сұлба

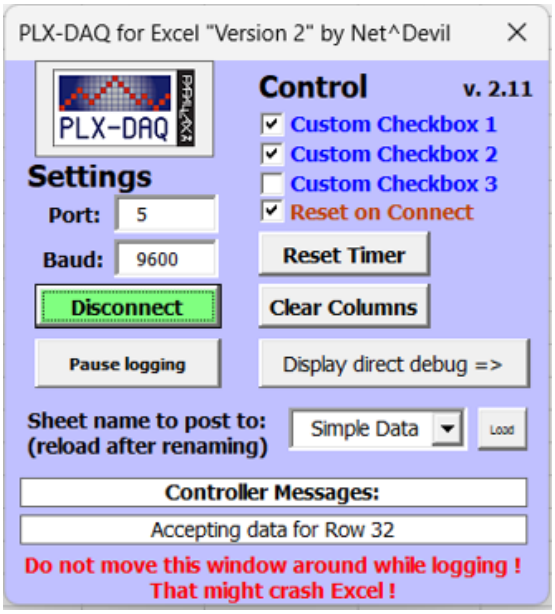
3.10-суретте RFID технологиясы арқылы жұмыс істейтін сәйкестендіру және қолжеткізуді басқару құралының жұмыс істеу алгоритмі көрсетілген. Бұл құралдың жұмысы былай жүзеге асырылады. Ең алдымен қолданушы рұқсат картасын қолданады, оқитын құрылғыдан ары қарай деректер беріледі және аутентификация процесі орындалады. Аутентификация нәтижесінде негізделіп жүйе ары қарай әрекет етеді. Рұқсат берілген жағдайда құлыптаушы механизмді ашады және өтуге рұқсат береді. Ал рұқсат берілмеген жағдайда карта иесінің әрекетін қабылдамай бастапқы күйіне оралады. Осы операцияларды орындау барысында жүйе барлық операцияларды деректер қорына жазып отырады. Осылайша радиожиіліктік сәйкестендіру технологиясына және микроконтроллерлік басқарудағы платформаға негізделген, пайдаланушының аутентификациясын техникалық және бағдарламалық түрде жүзеге асырады. 3.10-суретте көрсетілген алгоритм арқылы жұмыс істейтін, арнайы контактісіз кілт картасын пайдаланатын қолжеткізу процесін жеңілдетуге мүмкіндік береді.

Қолжеткізуді басқарудың автоматтандырылған жүйелері ақпараттық инфрақұрылымның құрамдас бөлігі және заманауи қауіпсіздік жүйесінің ажырамас бөлігі болып табылады. Қол жеткізуді басқару жүйелері деп кәсіп орындар, оқу орындары, емханалар секілді орындарда бейтаныс адамдардан шектейтін, сондай-ақ қозғалысты бақылайтын, бағдарламалық, аппараттық,

әдістемелік құралдар жиынтығын айтады [39]. Қолжеткізуді басқару жүйесі қолданылатын орындағы қауіпсіздік деңгейін көтеруге, сонымен қатар оны қамтамасыз етудегі шығындарды азайтуға мүмкіндік бере алады. Оған қоса қолжеткізуді басқару жүйелері қызмет көрсету үшін қызметкерлердің көп санын талап етпейді және энергияны тұтыну шығындары өте төмен болады [36].

RFID белгісін қабылдағышқа апарған сәтте жақын өріске кіріп деректер алмаса бастайды. Бұл деректерді антеннадан қабылдап алған соң оны цифрлық код түріне түрлендіріп микроконтроллерге жібереді. Микроконтроллер өз кезегінде жадына сақталған картаның ID кодымен салыстырып сәйкестік шыққан сәтте белгі беріп серво жетекті ашады және деректердің уақытын келіп түскен уақытын белгілеп осы деректерді деректер қорына жібереді. Менің жобамда деректер қорын көрсететін интерфейс ретінде excel кестесі қолданылады. Бұл кестеге деректерді микроконтроллерден қабылдап, сәйкесінше блоктарға бөліп тексеруші нөмірін береді. Data block бөлігінде блоктарға түрленген деректердің кэш нөмірі жазылады. Осы арқылы керекті блокты тауып алуға болады. Nonce бөлігінде осы блоктың қандай блоктармен қосылғанын сипаттайтын код жазылады. Осы код арқылы қандай блоктармен әрекеттесіп тұрғанын бақылауға болады. Осылайша блоктардан құралған тізбек орындалады. ID бөлімінде карта, тег немесе белгінің өзіндік сәйкестендіру коды HEX түрінде жазылады. Себебі екілік код түрінде үлкен матрица түрінде жазылып үлкен аумақты алып отырар еді. Қалған бөліктерде карта туралы бөлек сақталатын деректер шығарылады. Олар карта ұстаушысы жайында ақпарат болып келеді. Картаның оқылған сәттегі уақыты мен күні «Date» және «Time» бағандарға енгізіледі және картаны қолданған сәттен қайта қолданған сәтке дейін канша уақыт өткені жайлы жазылады. Белгіленген уақыт секунтар түрінде көрсетіледі.

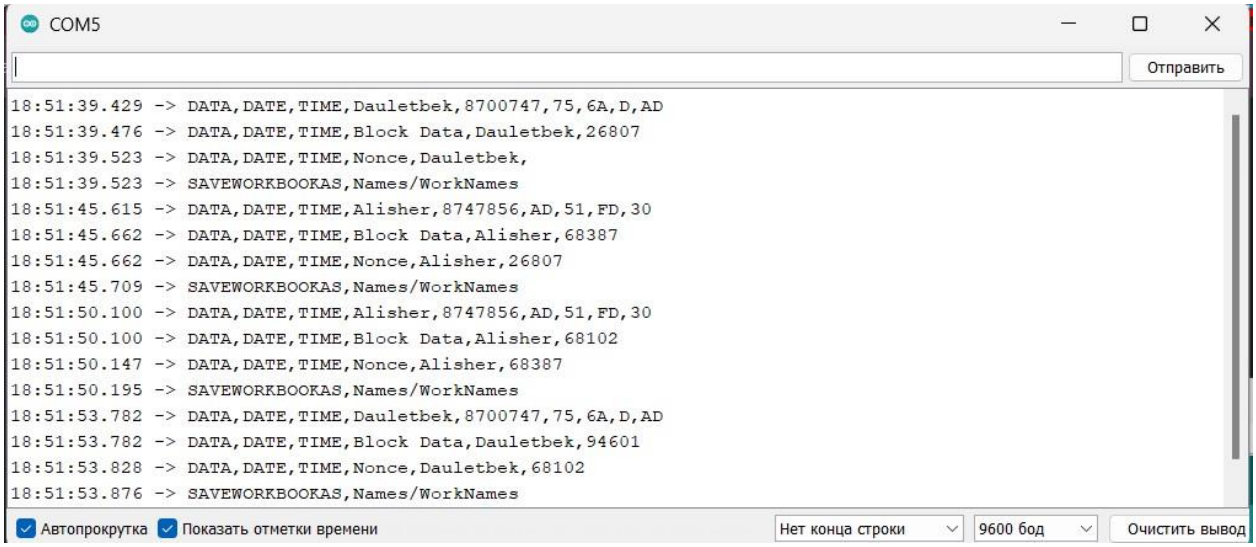
Карталардан қабылданған деректерді кестеге шығару үшін «Process Logging Extension» бағдарламасын қолдандым. Бұл бағдарлама Arduino микроконтролерінен жіберілетін деректерді excel бағдарламасының кестесіне жібере алады. Ол үшін микроконтроллер қосылған сериялық портты көрсетіп бағдарламалық кодта деректерді жіберу жолын енгізу қажет. Arduino микроконтроллеріне жүктелген бағдарламалық код немесе скетч деректердің қабылданып, өңделіп ары қарай жіберілуін қадағалайды. Ал PLX бағдарламасы осы деректерді қай сериялық порттан қабылдап алып, алдын ала жазылған бағдарламалық кодта бекітілген кесте ұяшықтарға шығару керектігін басқарып жүзеге асырады. PLX микроконтроллерге қосылған әртүрлі қабылдағыштар мен сенсорлардан алынған деректерді өңдеу, бақылау және визуализациялау үшін күрделі кодтармен жұмыс жасайтын деректер қорын қолданусыз жүзеге асыруға көмектесетін бағдарлама. Бұл бағдарлама арқылы деректерді талдау, өңдеу және визуализациялау жеңіл жүзеге асыралады. Process Logging Extension бағдарламасы 3.11-суретте көрсетілген.



3.11-сурет – Process Logging Extension бағдарламасы

PLX бағдарламасы арқылы микроконтроллерге қосылу үшін «Port» бөлімінде қажетті микроконтроллер қосылған сериялық портты таңдап, деректер қандай жылдамдықпен жіберілетінін жазу керек. Менің жағжайымда 5-ші сериялық порт арқылы Arduino uno микроконтроллері 9600 бод жылдамдығымен деректерді тасымалдайды. Control бөлімінде неше бөлім қарастырылады және қайта қосылу кезінде кестені тазалау қажет пе екенін таңдап қоюға болады. «Clear columns» батырмасы арқылы кез келген сәтте кесте бағандарын тазалауға болады. «Pause logging» батырмасы арқылы деректерді сақтау тоқтатылады. «Display direct debug» батырмасы арқылы болып жатқан процестер мен шыққан қателерді бақылауға болады. «Controller messages» бөлімінде кәзіргі орындалған процесс жазылады. Осы бағдарлама арқылы Arduino микроконтроллерінен келген деректерді сақтап визуализациялау нәтижесі Б қосымшасында көрсетілген.

Деректерді қабылдау және жіберу процесін «Arduino IDE» бағдарламасының сериялық порт мониторыннан бақылауға болады. Бұл жерде «COM5» сериялық порты арқылы қабылданған RFID карталарының деректерін тексеруге болады, яғни карта ұстаушы есімі, нөмірі, картаның ID нөмірі, қолданылған күні мен уақыты, блоктар тіқбегіндегі нөмірімен қандай блокпен сәйкес екенін білуге болады. 3.12-суретте компьютерге қосылған микроконтроллердің «COM5» сериялық порты арқылы деректерді бақылау терезесі көрсетілген.



3.12-сурет – Компьютерге қосылған микроконтроллердің «COM5» сериялық порты арқылы деректерді бақылау

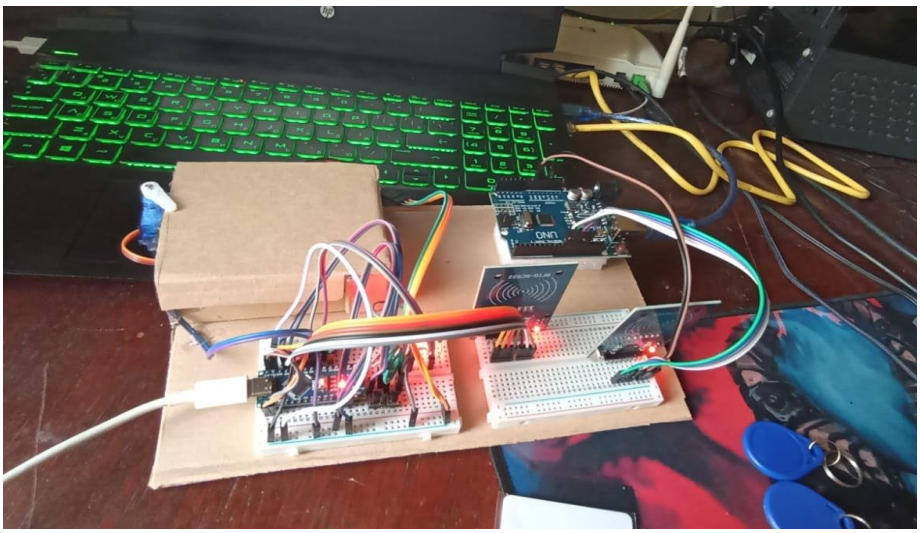
3.4 Блокчейн технологиясымен жұмыс жасайтын ультра жеңіл RFID сәйкестендіру құралы

Блокчейн арқылы жұмыс жасайтын RFID сәйкестендіру құралының жұмысы негізгі екі микроконтроллер арқылы іске асырылады. arduino nano және arduino uno микроконтроллерлері. Бұның себебі микроконтроллерлер қолданатын eeprom жадының сақтау орнының көлемі аздығы болып табылады. Arduino nano микроконтроллері жалғанған басты бөліктерімен басқаруды қамтамасыз етеді. Arduino uno қабылданған RFID тегтерінің ID кодын тексеріп, сәйкесінше блоктарға бөліп кестеге сақтайды, компьютердегі интерфейске шығарады.

Бұл жобаға ұқсас жұмыстарда RFID оқу құралы мен arduino микроконтроллерін қолдану арқылы қолжеткізуді басқару құралы көрсетілген. Мысалы: «использование многофакторной аутентификации для защиты данных от несанкционированного доступа при работе на эвт [40]» мақаласында автоматтандырылған жүйелерді күнделікті қолдануда бірнеше пайдаланушылар компьютермен жұмыс істеу кезінде компьютер жадында сақталған деректерге қолжеткізудің алдын алу мақсатында рұқсат етілмеген қолжеткізуді болдырмас үшін көп факторлы аутентификацияны пайдалануды ұсынады. Бұл мақалада аутентификация құралының сұлбасы берілген. Ұсынылған сұлба бойынша arduino uno микроконтроллері, rc522 оқу құралы, LCD1602 экраны және fpm10a саусақ ізін сканерлеу құралы жалғанған. Ұсынылған жоба артықшылықтарына оқылған деректерді кішігірім экранға шығару және карта мен белгілерден басқа саусақ ізін қолдана алу мүмкіндігінің болуында. Кемшіліктеріне бәріне қолжетімді емес кітапханалар, құралдың жұмыс жасауына қажетті криптографиялық функциялардың болмауы, құрал жұмысына қажетті деректер

қорын қолдану және қосымша бөліктерді қосу үшін жадының жеткіліксіздігі болып келеді.

«Аутентификация пользователей на Arduino с RFID [41]» мақаласында arduino көмегімен жасалған RFID сәйкестендіру құралы арқылын «InterSystems Cache» бағдарламасымен жобалауды ұсынды. Бұл мақалада пайдаланушы жүйеге немесе сервиске кіру кезінде бағдарлама одан логин және құпиясөзге сұраныс жасайды. Оны картадағы деректерді оқу арқылы жүзеге асыруға болады. Құпия сөзді ауыстыру керек жағдайда жүйеге сұраныс жасау коды жайында, қате шыққан жағдайда жүйеге қайта сұраныс жасау туралы және бұл құралды болашақта басқармалы кілттермен өзгерту мүмкіндігін қосу жайында айтылған. Бұл жобаның артықшылығы оның кең функционалдығында тұр. Кілттердегі деректер мен құпия сөздерді желі арқылы басқару және өңдеу. Кемшіліктеріне сипатталған бағдарламаға ғана сәйкес жасалған құрал және оның икемділігі болып тұр. Бұл құралды басқа мақсаттарда немесе басқа да бір бағдарламаға қосу үшін қолдану іске аспайды. Себебі бағдарламалық коды жағынан «intersystem cache» бағдарламасына арнап жасалуында болып тұр.

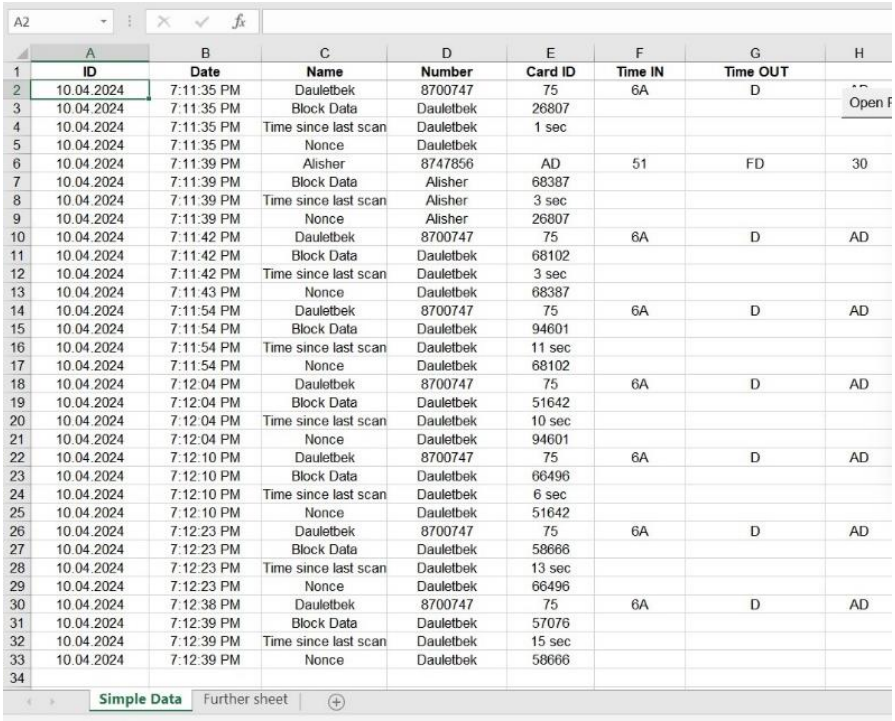


3.13-сурет – Блокчейн технологиясымен жұмыс жасайтын ультра жеңіл RFID сәйкестендіру құралы

3.13-суретте мен жасаған блокчейн арқылы жұмыс істейтін RFID сәйкестендіру құралы көрсетілген. Бұл құралдың жұмыс істеу алгоритмі мынадай. Ең алдымен карта иесі RC522 оқу құралына картаны немесе RFID белгісін жақындатады. Картамен оқу құралының арасы 2 см-ден кем болуы қажет.

RC522 өз кезегінде картадағы деректерді қабылдап микроконтроллерге жібереді. Arduino uno микроконтроллері деректерді қабылдап өңдеп 1 мб-қа дейін орын алатын блоктарға бөледі. Блоктарға картадағы деректер, дәлірек айтқанда, карта ұстаушы аты-жөні, нөмірі, картаның ID нөмірі, блоктың өзіндік хэш коды және бұл блоктың алдында блоктар тізбегі бар болса nonce коды жазылады. Картаны басу мен блокты тіркеу кезіндегі күні және дәл уақыты

жазылады. Егер картаны қайта басу орындалса деректерді қайта оқып сақтайды және картаны алдыңғы қабылдау мен осы қабылдау арасында неше уақыт өткені жазылады.



	A	B	C	D	E	F	G	H
1	ID	Date	Name	Number	Card ID	Time IN	Time OUT	
2	10.04.2024	7:11:35 PM	Dauletbek	8700747	75	6A	D	
3	10.04.2024	7:11:35 PM	Block Data	Dauletbek	26807			
4	10.04.2024	7:11:35 PM	Time since last scan	Dauletbek	1 sec			
5	10.04.2024	7:11:35 PM	Nonce	Dauletbek				
6	10.04.2024	7:11:39 PM	Alisher	8747856	AD	51	FD	30
7	10.04.2024	7:11:39 PM	Block Data	Alisher	68387			
8	10.04.2024	7:11:39 PM	Time since last scan	Alisher	3 sec			
9	10.04.2024	7:11:39 PM	Nonce	Alisher	26807			
10	10.04.2024	7:11:42 PM	Dauletbek	8700747	75	6A	D	AD
11	10.04.2024	7:11:42 PM	Block Data	Dauletbek	68102			
12	10.04.2024	7:11:42 PM	Time since last scan	Dauletbek	3 sec			
13	10.04.2024	7:11:43 PM	Nonce	Dauletbek	68387			
14	10.04.2024	7:11:54 PM	Dauletbek	8700747	75	6A	D	AD
15	10.04.2024	7:11:54 PM	Block Data	Dauletbek	94601			
16	10.04.2024	7:11:54 PM	Time since last scan	Dauletbek	11 sec			
17	10.04.2024	7:11:54 PM	Nonce	Dauletbek	68102			
18	10.04.2024	7:12:04 PM	Dauletbek	8700747	75	6A	D	AD
19	10.04.2024	7:12:04 PM	Block Data	Dauletbek	51642			
20	10.04.2024	7:12:04 PM	Time since last scan	Dauletbek	10 sec			
21	10.04.2024	7:12:04 PM	Nonce	Dauletbek	94601			
22	10.04.2024	7:12:10 PM	Dauletbek	8700747	75	6A	D	AD
23	10.04.2024	7:12:10 PM	Block Data	Dauletbek	66496			
24	10.04.2024	7:12:10 PM	Time since last scan	Dauletbek	6 sec			
25	10.04.2024	7:12:10 PM	Nonce	Dauletbek	51642			
26	10.04.2024	7:12:23 PM	Dauletbek	8700747	75	6A	D	AD
27	10.04.2024	7:12:23 PM	Block Data	Dauletbek	58666			
28	10.04.2024	7:12:23 PM	Time since last scan	Dauletbek	13 sec			
29	10.04.2024	7:12:23 PM	Nonce	Dauletbek	66496			
30	10.04.2024	7:12:38 PM	Dauletbek	8700747	75	6A	D	AD
31	10.04.2024	7:12:39 PM	Block Data	Dauletbek	57076			
32	10.04.2024	7:12:39 PM	Time since last scan	Dauletbek	15 sec			
33	10.04.2024	7:12:39 PM	Nonce	Dauletbek	58666			
34								

Simple Data | Further sheet

3.14-сурет – RFID карталары мен тегтерінен оқыған деректерді кестеге шығару

3.14-суретте карталардан қабылданған деректерді блоктарға бөліп кестеге енгізу процесі көрсетілген. Картадағы деректерді оқу кезінде оның дәл уақыты енгізіледі, блоктың өзіндік кэш коды беріледі және алдыңғы блоктың nonce коды жазылып бекітіледі. Мысалы: бірінші картаға мен туралы ақпарат тіркелген. Сондықтан бірінші картаны оқу құралына басқан кезде «Date» бағанына картаны басқан уақыты және күні көрсетіліп, «Name» бағанына менің аты-жөнім «Dauletbek» деп шығарылады. «Number» бағанына тіркелген нөмір телефоным «8700747» түрінде жазылады. Card ID бөлігіне картаға жазылған өзіндік ID коды шығарылады, ол «HEX» түріндегі код ретінде беріледі. Менің картамдың ID коды «75 6A D AD» түрінде көрсетілген. «Block data» бөлігіне жасалған блоктың хэш нөмірі жазылады. «Nonce» бөлігіне алдыңғы блоктың хэш коды жазылады. Nonce коды арқылы блоктың қай блокпен байланысып тұрғанын қарастыруға болады. «Time since last scan» картаны әрбір оқу сәттерінің аралығы секунттармен көрсетілген.

Arduino nano микроконтроллері қабылданған деректерге сәйкес қосылған модульдерді басқарады. Егер деректер жадысында сақталған картаны қабылдаған жағдайда зуммер және жарық диодтары сәйкес белгі береді және сервожетек ашылады. Керісінше жағдай туындаса немесе карта дұрыс емес қабылданса жарық диодынан қызыл түс жанып дыбыс шығарушы зуммердеп екі

рет қысқа дыбыс беріледі. Егер жаңа картаны тіркеу қажет болса оны бағдарламалық түрде кодқа енгізіп, осы кодты микроконтроллерге қайта енгізу қажет болар еді. Бірақ мен бұл туындаған қиындықты былайынша шештім. Маған жаңа картаны сақтау немесе бар картаны жою керек болған сәтте серво жетекті батырма арқылы ашып, ашу және сақтау батырмасын басып тұрып картаны оқу құралына қою қажет. Егер жаңа карта сақталса зуммер екі рет белгі береді, ал сақталған картаны қайта жақындатып батырманы басып тұрсам сақталған карта жадынан жойылады және үш рет дыбыстық индикатор беріледі. Ол үшін бағдарламалық кодқа «saveordelete» және «foundtag» бөлімдерін қостым. Егер жадыда карталар туралы ақпарат жоқ болған дағдайда сервожетекті ашық түрде ұстап тұру үшін «indicade savetags < max_tags/ indicade decline» бөлімін қостым. Осы арқылы сервожетек өздігінен жабылып қалмайды және жаңа карталарды қосу үшін бағдарламалық кодты қайта жызып жүктеу қажет емес болады.

MFRC522 модулінің оқу қашықтығын бағалау үшін сигнал қуатының қашықтығына кері квадраттық тәуелділік заңына негізделген формуланы қолдануға болады.

Оқу қашықтығын бағалау формуласын келесі түрде көрсетуге болады:

$$d \approx \sqrt{\frac{At}{4\pi}} \tag{2.1}$$

мұндағы d – карта мен қабылдағыш арасындағы қашықтық;

At – қабылдаушы антеннаның ауданы;

π – 3.14159.

$$\mathrm{At} = 0.04\text{м} \cdot 0.06\text{м} = 0.0024\text{м}^2$$

$$\mathrm{d} \approx \sqrt{0.0024/4 \cdot 3.14159}$$

$$\mathrm{d} \approx \sqrt{0.0024/12.56636}$$

$$\mathrm{d} \approx \sqrt{0.0138} \approx 13{,}8\ \text{мм}$$

Осылайша, 40 х 60 мм антеннасы бар MFRC522 модулі үшін болжалды оқу қашықтығы шамамен 0,0138 метр немесе 13,8 миллиметрді құрайды.

ҚОРЫТЫНДЫ

Бұл дипломдық жұмыста блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды қарастырдым. Блокчейн технологиясын, оның мүмкіндіктері мен ерекшелігін атап өттім. Оған ұқсас технологиямен салыстырып екеуінің қолдану және жұмыс істеу аймағына мысал келтірдім. Бір бірінен артықшылығы мен кемшіліктерін сипаттадым.

Arduino микроконтроллерлерін қолдану арқылы RFID технологиясымен жұмыс жасайтын ультра жеңіл аутентификация құралын жасадым. Оның мүмкіндіктерін сипаттап, қолдану аясына мысалдар келтірдім. Аутентификация құралын модельдеп қажетті дүзетулер керек болған жағдайда құралдың моделін өңдеу және қайта қарастыру мақсатында fritzing бағдарламасын қолдандым. Принципиалдық сұлбасын қарастырып, бағдарлама арқылы жасалған құрылымдық сұлбасының көмегімен аутентификация құралын құрастырдым.

Ультра жеңіл RFID аутентификация құралын блокчейн технологиясымен қосу үшін деректерді қабылдап, өңдеп, компьтер интерфейсіне шығару мақсатында қосымша arduino uno микроконтроллерін қолдандым. Бұл микроконтроллер карталардан қабылданған деректерді өңдеп, блоктарға бөледі. Картаның қолданған дәл уақыты, күні, картаның өзіндік ID коды мен пайдаланушының картаға тіркелген деректерін шығарады. Бұл блоктарға бөлінген деректерді бағдарламалауға арналған Arduino IDE бағдарламасының монитор порты арқылы тексеруге болатындығы мені қанағаттандырмағандықтан, деректерді компьтердің интерфейсіне шығарып, кестеге сәйкесінше орналастыратын дәрежеге жеткіздім. Деректерді сериялық порттан қабылдап кестеге шығару үшін PLX бағдарламасын қолдандым. Осы күнге дейін жасалған тәжірибелерге мысал келтірдім, олардың артықшылықтары мен кемшіліктерін жаздым. Өзім құрастырған құрылғының мүмкіндіктерін ұсынып оларды салыстырдым.

Блокчейн арқылы жұмыс істейтін ультра жеңіл RFID аутентификация құралының жұмыс істеу принципін жазып, құралдың дайын макетінің суретін ұсындым. Құралдың жұмыс жасауына қажетті бағдарламалық кодты А қосымшасына тіркеп қойдым.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

[1] Бельский Владимир Сергеевич, Грибоедова Екатерина Сергеевна, Царегородцев Кирилл Денисович, Чичаева Анастасия Александровна БЕЗОПАСНОСТЬ RFID-СИСТЕМ // International Journal of Open Information Technologies. 2021. №9. URL: https://cyberleninka.ru/article/n/bezopasnost-rfid-sistem

[2] https://cyberleninka.ru/article/n/ponyatie-blokcheyn-i-vozmozhnosti-ego-ispolzovaniya/ Федотова Вероника Вячеславовна, Емельянов Богдан Георгиевич, and Типнер Людмила Михайловна. "Понятие блокчейн и возможности его использования" European science, no. 1 (33), 2019, pp. 40-48.

[3] https://www.1cbit.ru/blog/rfid-tekhnologiya-chto-etotakoe/?utm_ referrer= https%3A%2F%2Fwww.google.com%2F/«RFID-технология: что это такое. Применение RFID», г.Алматы, фев. 2020.

[4] https://cyberleninka.ru/article/n/tehnologiya-blockchain-printsipy-raboty-i-perspektivy-primeneniya/ Шольц Юрген, Шелер Торстен, Соколов Юрий Игоревич, Коцоева Валерия Сергеевна, and Элькина Анна Андреевна. "Технология blockchain. Принципы работы и перспективы применения" ЭТАП: экономическая теория, анализ, практика, no. 6, 2017, pp. 67-76.

[5] https://www.tadviser.ru/index.php/Блокчейн-Blockchain, г.Москва, июн. 2022.

[6] https://ust.kz/blokchein_tehnologiyasy_blockchain/ Тотаева А.Т., Блокчейн технологиясы. фев. 2024.

[7] https://habr.com/ru/articles/687636/ Oracle labs., «Что все неправильно понимают в блокчейне»., сен. 2022

[8] https://3commas.io/ru/blog/xranenie-informacii-v-blokchejne/ Марк Лецюк. Хранение информации в блокчейне. Авг. 2020.

[9]]https://tech.vestnik.shakarim.kz/jour/article/view/368/300/ Темирханова С.Е., Коккоз М.М. ИЗУЧЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН И ЕЕ ПОТЕНЦИАЛЬНОГО ПРИМЕНЕНИЯ В ОБРАЗОВАНИИ. Вестник Университета Шакарима. Серия технические науки. 2022;(4(8)):56-63.

[10] https://aws.amazon.com/ru/what-is/blockchain/ ?aws-products- all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc/ июл.2023

[11] https://cyberleninka.ru/article/n/tehnologiya-blockchain-printsipy-raboty-i-perspektivy-primeneniya/ Шольц Юрген, Шелер Торстен, Соколов Юрий Игоревич, Коцоева Валерия Сергеевна, and Элькина Анна Андреевна. "Технология blockchain. Принципы работы и перспективы применения" ЭТАП: экономическая теория, анализ, практика, no. 6, 2017, pp. 67-76.

[12] https://finswin.com/kripto/terminologiya/blokchejn.html/ Владимир Ким. «Как работает блокчейн»., окт. 2020.

[13] Discussion of IOTA weaknesses and possible implementation of Proof-of work method/ URL: https://amp.reddit.com/r/Iota/comments/6fdzdd/ weaknesses/ 2020.

[14] https://profinvestment.com/iota/ редакция profinvestment, Сергей В., «Криптовалюта IOTA (Йота) — полный обзор: перспективы и прогноз, история создания, принцип работы, преимущества и недостатки»., мар. 2024.

[15] https://gerchik.com/stati/kriptovalyuta-iota-perspektivnaya-i-ne -takaya-kak-vse/ Эксперты редакции gerchik trading ecosystem., «КРИПТОВАЛЮТА IOTA - ПЕРСПЕКТИВНАЯ И НЕ ТАКАЯ КАК ВСЕ»., янв. 2023.

[16] https://selectel.ru/blog/about-blockchain/ О технологии блокчейн., Санкт-Петербург, янв 2019.

[17] https://101blockchains.com/ru/ Lana Gubanova., «50 основных вопросов и ответов по блокчейну»., фев. 2019.

[18] https://safe-surf.ru/specialists/article/5278/658923/ Войтов Матвей, директор по маркетингу корпоративной блокчейн-платформы Waves Enterprise., ноя. 2020.

[19] https://vc.ru/u/ 1304906-crypto-smi/ 580248-chto-takoe- noda-v-blokcheyne/ cryptosmi., «что такое нода в блокчейне»., янв. 2023.

[20] https://aussiedlerbote.de/2022/02/zachem-nuzhna-validaciya/ Юрий Андреев., «Зачем нужна валидация и чем полезен стекинг»., фев. 2022.

[21] https://cyberleninka.ru/article/n/algoritmy-dostizheniya-konsensusa-v-blokcheyn-sisteme/ Чахкиев Магомед Темирланович (2022). АЛГОРИТМЫ ДОСТИЖЕНИЯ КОНСЕНСУСА В БЛОКЧЕЙН СИСТЕМЕ. StudNet, 5 (3), 1737-1745.

[22] https://enecuum.com/technology?lang=ru/_ENQ., «гибридный алгоритм консенсуса BFT»., сен. 2020.

[23] https://www.ixbt.com/live/crypto/ chto-takoe-algoritm-konsensusa-dostupno-obyasnyaem.html #:~:text=%/ Беляев Артем., «Как работает блокчейн: что такое алгоритм консенсуса»., май. 2023.

[24] https://www.tadviser.ru/a/614491/ news@tadviser.ru/ Алгоритм консенсуса Proof-of-Work (PoW) Proof-of-Stake (PoS)., авг. 2021.

[25] https://www.cryptoprofi.info/?p=961/Cryptoprofi., «Виды алгоритма консенсуса различных блокчейнов»., ноя. 2019.

[26] https://vc.ru/crypto/ 398036-tehnologiya-blockchain- tipy-sfery-primeneniya- preimushchestva-i-nedostatki/ Руслан У., CryptoCloud., «Технология blockchain: типы, сферы применения, преймущества и недостатки»., май. 2022.

[27] https://polygant.net/ru/blog/sfery-primeneniya-blokchejna /polygant., «сферы применения блокчейна»., г.Алматы, окт. 2022.

[28] Das Raghu. RFID Forecasts, Players and Opportunities 20192029. The complete analysis of the global RFID industry. — URL: https://www.idtechex.com/en/researchreport/ rfidforecastsplayersandopportunities-20192029/700

[29] Бельский Владимир Сергеевич, Грибоедова Екатерина Сергеевна, Царегородцев Кирилл Денисович, Чичаева Анастасия Александровна БЕЗОПАСНОСТЬ RFID-СИСТЕМ // International Journal of Open Information Technologies. 2021. №9. URL: https://cyberleninka.ru/article/n/bezopasnost-rfid-sistem (дата обращения: 03.03.2024).

[30] Потапова к.а. идентификация данных с помощью rfid-меток // Вестник науки. 2023. №10 (67). URL: https://cyberleninka.ru/article/n/identifikatsiya-dannyh-s-pomoschyu-rfid-metok

[31] https://scanport.ru/ blog/ rfid-schityvatel-v idy-funkczii-oblasti-primeneniya/ RFID считыватель — виды, функции, области применения/2021.

[32] https://nvgn.ru/ blog/ rfid-vse-o -technologii- radiochastotnoy-identifikacii/Elvina Sharafutdinova/ RFID - все о технологии радиочастотной идентификации. Дек. 2020.

[33] Черепков Сергей Технология RFID - радиочастотная идентификация. Опыт использования и перспективные направления // Компоненты и Технологии. 2020. №53. URL: https://cyberleninka.ru/article/n/tehnologiya-rfid-radiochastotnaya-identifikatsiya-opyt-ispolzovaniya-i-perspektivnye-napravleniya

[34] Месропян, Катрин. RFID — радиочастотная идентификация / Катрин Месропян, А. А. Романенко, М. Ю. Житарев. // Молодой ученый. — 2023. — № 35 (482). — С. 15-19. — URL: https://moluch.ru/archive/482/105771

[35] https://habr.com/ru/ articles/ 592403/ «RFID идентификация. Беспроводные технологии», ноя. 2021.

[36] https://www.1cbit.ru/ blog/ rfid-tekhnologiya- chto-eto-takoe/?utm_referrer=https%3A%2F%2Fwww.google.com%2F/«RFID-технология: что это такое. Применение RFID», г.Алматы, фев. 2020.

[37] Омельченко Е. Я., Танич В. О., Маклаков А. С., Карякина Е. А. Краткий обзор и перспективы применения микропроцессорной платформы Arduino // ЭС и К. 2019. №21. URL: https://cyberleninka.ru/article/n/kratkiy-obzor-i-perspektivy-primeneniya-mikroprotsessornoy-platformy-arduino.

[38] https://ieeexplore.ieee.org/document/8598865/Michail Sidorov, Ming Tze Ong, Ravivarma Vikneswaren Sridharan, Junya Nakamura, Ren Ohmura., Jing Huey Khor, jan. 2019.

[39] Бужинская Надежда Владимировна, Васева Елена Сергеевна, Искандаров Рустам Наильевич, Шубина Наталья Валерьевна Система контроля и управления доступом на базе микроконтроллеров Arduino // Вестник ДГТУ. Технические науки. 2019. №1. URL: https://cyberleninka.ru/article/n/sistema-kontrolya-i-upravleniya-dostupom-na-baze-mikrokontrollerov-arduino/.

[40] Кротов А.В., Кутузов А.В. Использование многофакторной аутентификации для защиты данных от несанкционированного доступа при работе на ЭВТ // Современные научные исследования и инновации. 2022. № 1 [Электронный ресурс]. URL: https://web.snauka.ru/issues/2022/01/97352/

[41] https://habr.com/ru/ companies/ intersystems/ articles/279893 /Аутентификация пользователей на Arduino с RFID/

ҚОСЫМША А

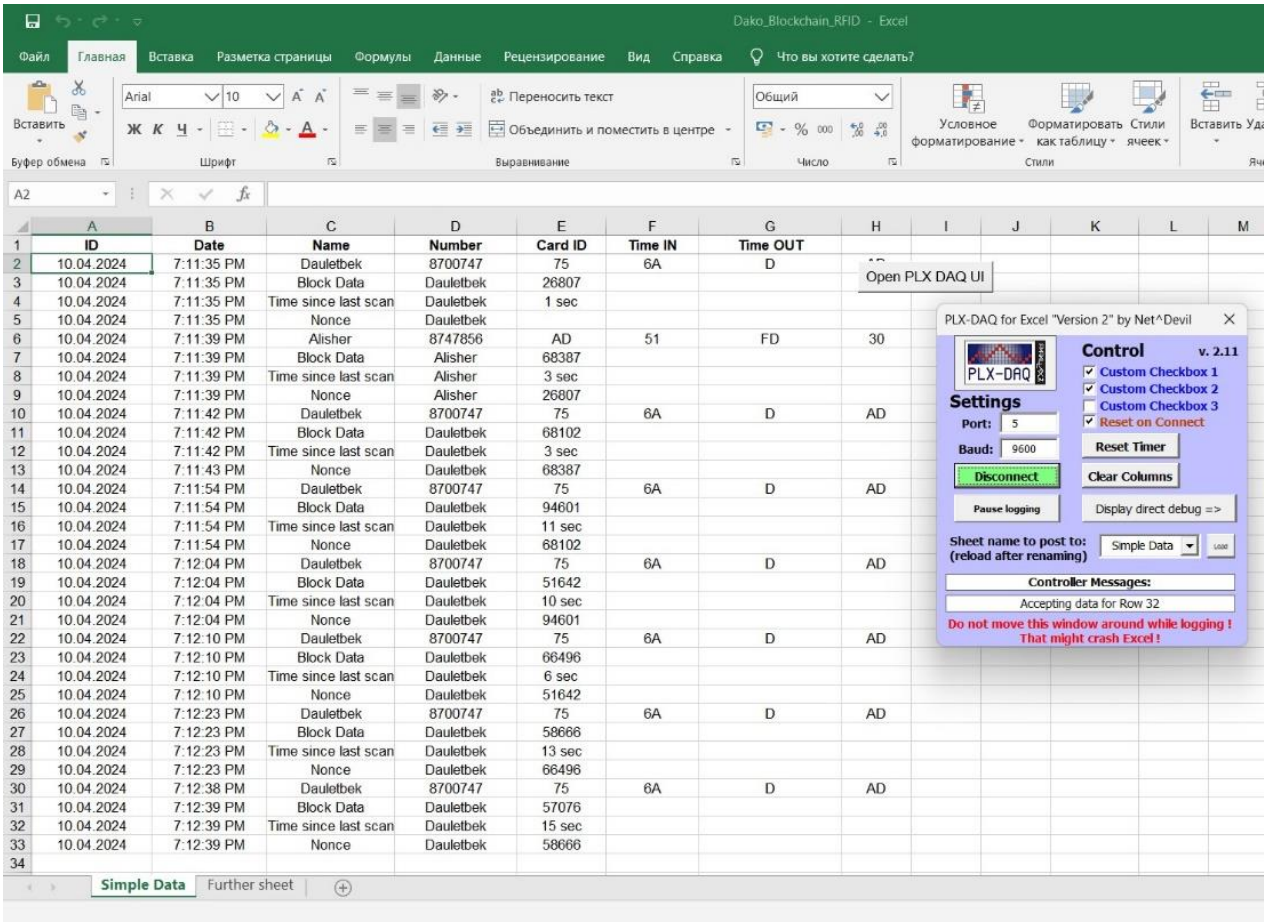
Блокчейн арқылы жұмыс істейтін ультра жеңіл RFID аутентификация құралының жұмыс істеуіне қажетті бағдарламалық код.

```
#include <SPI.h>
#include <MFRC522.h>

#define SS_PIN 10 //RX
#define RST_PIN 9

MFRC522 mfrc522(SS_PIN, RST_PIN); //

byte card_ID[4]; //card UID size 4byte
byte Name1[4] = {0x75, 0x6A, 0x0D, 0xAD}; //
byte Name2[4] = {0xAD, 0x51, 0xFD, 0x30}; //
byte Name3[4] = {0x63, 0xEC, 0xED, 0xFD}; //
byte Name4[4] = {0xB3, 0xA4, 0x5A, 0xFA}; //

int const RedLed = 6;
int const GreenLed = 5;
int const Buzzer = 8;

String Name; //user name
long Number; //user number
String previousBlockCode = ""; //
unsigned long previousScanTime = 0; //

void setup() {
  Serial.begin(9600); //
  SPI.begin();  //
  mfrc522.PCD_Init(); //

  pinMode(RedLed, OUTPUT);
  pinMode(GreenLed, OUTPUT);
  pinMode(Buzzer, OUTPUT);
}

void loop() {
  //
  if (!mfrc522.PICC_IsNewCardPresent()) {
    return; //got to start of loop if there is no card present
  }
```

```
  //
  if (!mfrc522.PICC_ReadCardSerial()) {
    return; //if read card serial(0) returns 1, the uid struct contians the ID of the read
card.
  }
  unsigned long currentTime = millis(); //
  unsigned long timeSinceLastScan = currentTime - previousScanTime; // Calculate
time since last card scan

  for (byte i = 0; i < mfrc522.uid.size; i++) {
    card_ID[i] = mfrc522.uid.uidByte[i];

    if (card_ID[i] == Name1[i]) {
      Name = "Dauletbek"; //
      Number = 8700747; //
    } else if (card_ID[i] == Name2[i]) {
      Name = "Alisher"; //
      Number = 8747856; //
    } else if (card_ID[i] == Name3[i]) {
      Name = "Alibek"; //
      Number = 8708361; //
    } else if (card_ID[i] == Name4[i]) {
      Name = "Ruslan"; //
      Number = 8777138; //
    } else {
      digitalWrite(GreenLed, LOW);
      digitalWrite(RedLed, HIGH);
      goto cont; //go directly to line 85
    }
  }

  //
  String blockCode = generateBlockCode();

  //
  Serial.print("DATA,DATE,TIME,");
  Serial.print(Name);
  Serial.print(",");
  Serial.print(Number);
  Serial.print(",");
  for (int i = 0; i < mfrc522.uid.size; i++) {
    Serial.print(card_ID[i], HEX);
    if (i < mfrc522.uid.size - 1) {
      Serial.print(",");
```

```
    }
  }
  Serial.println();

  //
  Serial.print("DATA,DATE,TIME,Block Data,");
  Serial.print(Name);
  Serial.print(",");
  Serial.println(blockCode);

  //
  Serial.print("DATA,DATE,TIME,Time since last scan,");
  Serial.print(Name);
  Serial.print(",");
  Serial.print(timeSinceLastScan / 1000); //
  Serial.println(" sec");

  //
  Serial.print("DATA,DATE,TIME,Nonce,");
  Serial.print(Name);
  Serial.print(",");
  Serial.println(previousBlockCode);

  //
  previousBlockCode = blockCode;
  previousScanTime = currentTime;

  digitalWrite(GreenLed, HIGH);
  digitalWrite(RedLed, LOW);
  digitalWrite(Buzzer, HIGH);
  delay(30);
  digitalWrite(Buzzer, LOW);
  Serial.println("SAVEWORKBOOKAS,Names/WorkNames");

  delay(1000);
cont:
  delay(2000);
  digitalWrite(GreenLed, LOW);
  digitalWrite(RedLed, LOW);
}

String generateBlockCode() {
//
}
```

ҚОСЫМША Б



	A	B	C	D	E	F	G	H
1	ID	Date	Name	Number	Card ID	Time IN	Time OUT	
2	10.04.2024	7:11:35 PM	Dauletbek	8700747	75	6A	D	
3	10.04.2024	7:11:35 PM	Block Data	Dauletbek	26807			
4	10.04.2024	7:11:35 PM	Time since last scan	Dauletbek	1 sec			
5	10.04.2024	7:11:35 PM	Nonce	Dauletbek				
6	10.04.2024	7:11:39 PM	Alisher	8747856	AD	51	FD	30
7	10.04.2024	7:11:39 PM	Block Data	Alisher	68387			
8	10.04.2024	7:11:39 PM	Time since last scan	Alisher	3 sec			
9	10.04.2024	7:11:39 PM	Nonce	Alisher	26807			
10	10.04.2024	7:11:42 PM	Dauletbek	8700747	75	6A	D	AD
11	10.04.2024	7:11:42 PM	Block Data	Dauletbek	68102			
12	10.04.2024	7:11:42 PM	Time since last scan	Dauletbek	3 sec			
13	10.04.2024	7:11:43 PM	Nonce	Dauletbek	68387			
14	10.04.2024	7:11:54 PM	Dauletbek	8700747	75	6A	D	AD
15	10.04.2024	7:11:54 PM	Block Data	Dauletbek	94601			
16	10.04.2024	7:11:54 PM	Time since last scan	Dauletbek	11 sec			
17	10.04.2024	7:11:54 PM	Nonce	Dauletbek	68102			
18	10.04.2024	7:12:04 PM	Dauletbek	8700747	75	6A	D	AD
19	10.04.2024	7:12:04 PM	Block Data	Dauletbek	51642			
20	10.04.2024	7:12:04 PM	Time since last scan	Dauletbek	10 sec			
21	10.04.2024	7:12:04 PM	Nonce	Dauletbek	94601			
22	10.04.2024	7:12:10 PM	Dauletbek	8700747	75	6A	D	AD
23	10.04.2024	7:12:10 PM	Block Data	Dauletbek	66496			
24	10.04.2024	7:12:10 PM	Time since last scan	Dauletbek	6 sec			
25	10.04.2024	7:12:10 PM	Nonce	Dauletbek	51642			
26	10.04.2024	7:12:23 PM	Dauletbek	8700747	75	6A	D	AD
27	10.04.2024	7:12:23 PM	Block Data	Dauletbek	58666			
28	10.04.2024	7:12:23 PM	Time since last scan	Dauletbek	13 sec			
29	10.04.2024	7:12:23 PM	Nonce	Dauletbek	66496			
30	10.04.2024	7:12:38 PM	Dauletbek	8700747	75	6A	D	AD
31	10.04.2024	7:12:39 PM	Block Data	Dauletbek	57076			
32	10.04.2024	7:12:39 PM	Time since last scan	Dauletbek	15 sec			
33	10.04.2024	7:12:39 PM	Nonce	Dauletbek	58666			
34								

A1-сурет - деректерді excel кестесіне PLX бағдарламасы арқылы шығару нәтижесі көрсетілген

Қ.И. СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

Дипломдық жұмысқа

СЫН-ПІКІР

Құдайбергенов Дәулетбек Мұхтарұлы

6В06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: «Блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды зерттеу»

а) графикалық бөлімі 30 бет
б) түсіндірме жазбасы 65 бет

ЖҰМЫСҚА ЕСКЕРТУ ЖАЗУ

Бұл дипломдық жұмыста блокчейн арқылы жұмыс жасайтын ультра жеңіл RFID аутентификациясын жасау зерттеледі. Қолжеткізуді басқару мақсатында жаңа қолданбалар ұсынылады.

Бірінші бөлімде блокчейн технологиясы мен оның жұмыс істеу принципі, қолдану аясы мен осыған ұқсас технологияларға шолу жасалған.

Екінші бөлімде ультра жеңіл RFID аутентификациясын жасау жүйесі зерттелген. Қолжеткізу басқару құралының құрылымдық және принципиалдық сұлбалары ұсынылған.

Үшінші бөлімде ультра жеңіл RFID аутентификациясын жасау жүйесін блокчейн технологиясымен жобалау көрсетілген. Құралдың жұмыс істеу принципі жазылған және сұлбалары көрсетілген.

Графикалық және мәтіндік материалдар МСТҚ талабына сәйкес жазылған. Студент Құдайбергенов Дәулетбек дипломдық жобаны жоғарғы оқу орындарының талаптарына сай және тиісті көлемде сонымен катар жеткілікті жоғарғы дәрежеде орындаған.

Жұмыстың бағасы

Жалпы, дипломдық жұмысқа "өте жақсы" (95%) деген баға, ал студент Құдайбергенов Дәулетбек 6В06201 – Телекоммуникация білім беру бағдарламасының «техника және технологиялар бакалавры» дәрежесіне лайықты деп санаймын.

Сын-пікір беруші:
Халықаралық ақпараттық технологиялар университеті
т.ғ.к., қауымдастырылған профессор
Л.Б.Илипбаева
«19» 05 2024 ж.

Подпись указанного лица заверяю
Менеджер по персоналу
Мухамеш

Ф КазНИТУ 706-17. Рецензия

Қ.И. СӘТБАЕВ атындағы ҚАЗАҚ ҰЛТТЫҚ ТЕХНИКАЛЫҚ ЗЕРТТЕУ УНИВЕРСИТЕТІ
КОММЕРЦИЯЛЫҚ ЕМЕС АКЦИОНЕРЛІК ҚОҒАМЫ

ҒЫЛЫМИ ЖЕТЕКШІНІҢ ПІКІРІ

дипломдық жобаға

Құдайбергенов Дәулетбек Мұхтарұлы

6В06201 «Телекоммуникация» білім беру бағдарламасы

Тақырыбы: «Блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды зерттеу»

Бұл дипломдық жұмыс блокчейн негізіндегі ультра жеңіл RFID аутентификация жүйесін құруды зерттелді. Қол жеткізуді басқаруда пайдалану үшін жаңа бағдарламалық қосымшалар ұсынылады.

Бірінші бөлім блокчейн технологиясының жұмыс жасау принциптерін, оны қолдану аясын және осыған ұқсас технологиялар сипатталған.

Екінші бөлімде RFID технологиясы және ультра жеңіл RFID аутентификация жүйесі зерттелген. Қолжеткізуді басқару құралының құрылымдық және принципиалдық сұлбалары көрсетілген.

Үшінші бөлімде блокчейн негізіндегі ультра жеңіл RFID аутентификация жүйесін жасау қарастылған. Құралдың жұмыс принципі сұлбалармен көрсетіліп, сипаттап жазылған.

Графикалық және мәтіндік материалдар МСТҚ талабына сәйкес жазылған. Студент Құдайбергенов Дәулетбек дипломдық жобаны жоғарғы оқу орындарының талаптарына сай және тиісті көлемде сонымен қатар жеткілікті жоғарғы дәрежеде орындаған.

Жұмыстың бағасы

Жалпы, дипломдық жұмысқа «өте жақсы» (95%) деген баға, ал студент Құдайбергенов Дәулетбек 6В06201 – Телекоммуникация білім беру бағдарламасы бойынша «ақпараттық коммуникациялық технологиялар бакалавры» дәрежесіне ұсынамын.

Ғылыми жетекші
ЭТжҒТ каф. аға оқытушысы, PhD,
Д.Ж.Утебаева
«30» 05 2024 ж.

HR Қызметі

Университеттің жүйе администраторы мен Академиялық мәселелер департаменті директорының ұқсастық есебіне талдау хаттамасы

Жүйе администраторы мен Академиялық мәселелер департаментінің директоры көрсетілген еңбекке қатысты дайындалған Плагиаттың алдын алу және анықтау жүйесінің толық ұқсастық есебімен танысқанын мәлімдейді:

Автор: Құдайбергенов Дәулетбек Мұхтарұлы

Тақырыбы: Блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды зерттеу

Жетекшісі: Дана Утебаева

1-ұқсастық коэффициенті (30): 1.5

2-ұқсастық коэффициенті (5): 0.8

Дәйексөз (35): 1.3

Әріптерді ауыстыру: 5

Аралықтар: 0

Шағын кеңістіктер: 8

Ақ белгілер: 0

Ұқсастық есебін талдай отырып, Жүйе администраторы мен Академиялық мәселелер департаментінің директоры келесі шешімдерді мәлімдейді :

☒ Ғылыми еңбекте табылған ұқсастықтар плагиат болып есептелмейді. Осыған байланысты жұмыс өз бетінше жазылған болып санала отырып, қорғауға жіберіледі.

☐ Осы жұмыстағы ұқсастықтар плагиат болып есептелмейді, бірақ олардың шамадан тыс көптігі еңбектің құндылығына және автордың ғылыми жұмысты өзі жазғанына қатысты күмән тудырады. Осыған байланысты ұқсастықтарды шектеу мақсатында жұмыс қайта өңдеуге жіберілсін.

☐ Еңбекте анықталған ұқсастықтар жосықсыз және плагиаттың белгілері болып саналады немесе мәтіндері қасақана бұрмаланып плагиат белгілері жасырылған. Осыған байланысты жұмыс қорғауға жіберілмейді.

Негіздеме:

27.05.2024
Күні

Кафедра меңгерушісі

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Құдайбергенов Дәулетбек Мұхтарұлы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды зерттеу

Научный руководитель: Дана Утебаева

Коэффициент Подобия 1: 1.5

Коэффициент Подобия 2: 0.8

Микропробелы: 8

Знаки из здругих алфавитов: 5

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

27.05.2024
Дата

Заведующий кафедрой

Протокол

о проверке на наличие неавторизованных заимствований (плагиата)

Автор: Құдайбергенов Дәулетбек Мұхтарұлы

Соавтор (если имеется):

Тип работы: Дипломная работа

Название работы: Блокчейн арқылы ультра жеңіл RFID аутентификациясын жасауды зерттеу

Научный руководитель: Дана Утебаева

Коэффициент Подобия 1: 1.5

Коэффициент Подобия 2: 0.8

Микропробелы: 8

Знаки из здругих алфавитов: 5

Интервалы: 0

Белые Знаки: 0

После проверки Отчета Подобия было сделано следующее заключение:

☒ Заимствования, выявленные в работе, является законным и не является плагиатом. Уровень подобия не превышает допустимого предела. Таким образом работа независима и принимается.

☐ Заимствование не является плагиатом, но превышено пороговое значение уровня подобия. Таким образом работа возвращается на доработку.

☐ Выявлены заимствования и плагиат или преднамеренные текстовые искажения (манипуляции), как предполагаемые попытки укрытия плагиата, которые делают работу противоречащей требованиям приложения 5 приказа 595 МОН РК, закону об авторских и смежных правах РК, а также кодексу этики и процедурам. Таким образом работа не принимается.

☐ Обоснование:

27.05.2024
Дата

проверяющий эксперт