МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.056.5

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система забезпечення цілісності електронних документів на основі технології блокчейн

Виконавець: Б.Ю. Носань
Керівник: к.т.н., доцент М.Б. Гумен
Нормоконтролер: к.т.н., доцент М.Б. Гумен

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«__» _____ 20__ р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Носаня Богдана Юрійовича

1. Тема: Система забезпечення цілісності електронних документів на основі технології блокчейн

затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.

2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.

3. Вихідні дані: проаналізувати розвиток електронного документообігу в Україні та тенденцію використання блокчейн технології.

4. Зміст пояснювальної записки: аналіз існуючих систем документообігу; аналіз можливостей технології блокчейн для побудови систем електронного документообігу; визначення проблем та ризиків використання технології блокчейн; розробка системи забезпечення цілісності електронних документів на основі блокчейн.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	15.04.2021	*Виконано*
2.	Аналіз літературних джерел	16.04.2021	*Виконано*
3.	Обґрунтування вибору рішення	17.04.2021	*Виконано*
4.	Збір інформації	18.04.2021-25.04.2021	*Виконано*
5.	Дослідження загальної характеристики електронного документообігу	26.04.2021-02.05.2021	*Виконано*
6.	Дослідження та аналіз можливостей технології блокчейн для побудови систем електронного документообігу	03.05.2021-10.05.2021	*Виконано*
7.	Розроблення системи забезпечення цілісності електронних документів на основі технології блокчейн	11.05.2021-29.05.2021	*Виконано*
8.	Перевірка на антиплагіат	07.06.2021	*Виконано*
9.	Оформлення і друк пояснювальної записки	09.06.2021	*Виконано*
10.	Оформлення презентації	10.06.2021	*Виконано*
11.	Отримання рецензій від рецензента	14.06.2021	*Виконано*

Здобувач вищої освіти Б.Ю. Носань

(підпис, дата)

Керівник дипломної роботи М.Б. Гумен

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, загальним обсягом робота складає 76 сторінок, має 4 рисунків та 1 таблицю. Список використаних джерел містить 40 найменувань і займає 4 сторінки.

Метою дипломної роботи є створення системи забезпечення цілісності електронних документів на основі технології блокчейн. В дипломній роботі розглянуті переваги та недоліки документообігу на технології блокчейн, а також цілісності інформації, яка передається через цю.

Запропонована система може використовуватися у реальних практичних системах документообігу. Створення цієї системи може використовуватись в будь якій галузі де є документообіг, а також зменшить витрати на документообіг.

Ключові слова: блокчейн, система документобігу, інформація, хеш, інформаційна система.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. Даний постінформаційний етап розвитку суспільства пов'язаний із поступовим упровадженням і використанням електронних документів та електронного документообігу. Електронний документообіг має безліч переваг перед паперовим, основні з них: швидкість надходження документів до адресатів, зручність редагування та архівації документів тощо [1, с. 37].

В умовах жорсткої конкуренції ефективно можуть вести справи ті підприємства, які мають можливість оперативно одержувати інформацію. Вирішенню цієї проблеми, а також удосконаленню інформаційного забезпечення управління сприяє впровадження електронного документоообігу. З огляду на це важливим є подальше дослідження організації та методики електронного документоообігу на вітчизняних підприємствах.

Глобалізація невпинно змінює світ і наше середовище а інтернет та інформаційні технології виступають елементами цього руху. Блокчейн — є певною новою та фундаментальною технологією, яка дозволяє вивести цей процес на зовсім інший рівень.

Швидкий розвиток інформаційних та цифрових технологій підвищує попит до соціальних мереж, пошукових систем та on-line магазинів, що відповідно вимагає вдосконалення та введення інновацій у фінансово кредитних механізмах. Коли в фінансовій сфері йде постійна боротьба за клієнта, а також виникає необхідність оптимізації витрат, це породжує створення нових технологій, зокрема такого явища – як блокчейн. Якщо в світі поняття блокчейну є досить поширеним, то в Україні це є порівняно нова категорія, яка потребує детальнішого розвитку та вивчення.

Аналіз останніх досліджень і публікацій. Питанням організації та методики електронного документообігу в різні часи займалися як вітчизняні, так і зарубіжні вчені-економісти, зокрема Г. Асєєв, М. Білуха, О. Бочаров, В. Буркус, Т. Бутинець, Ф. Бутинець, О. Войналович, Т. Давидюк,

І. Двойленко, К. Дударєва, В. Євдокимов, П. Жежнич, В. Завгородній, С. Івахненков, І. Капля, І. Кірієнко, П. Клімушин.

Дослідження в галузі віртуальних активів спираються на теоретичні праці вітчизняних та зарубіжних вчених, практичні розробки і нормативно-правову базу державного регулювання в цій галузі. В українській економіці розробки теорії та практики присвячені праці таких авторів, як С.В.Волосович, В.С. Гава, О.В. Карпов, С.В. Науменкова, І.П.Ситник, Н.Г. Яцків та інші. Більшість вчених вважають, що такі технології, як «блокчейн» міцно завойовують своє місце в інформаційноцифровій системі, проте й досі існує ряд проблем, що не дозволяє впровадити їх в щоденну діяльність.

Тому вважаємо за потрібне більш детально дослідити питання сутності блокчейн, його можливості, перспективи розвитку та проблеми пов'язані з ними у світі та Україні. Водночас залишається актуальним дослідження ризиків, які мають місце при використанні даної технології.

Метою даної дипломної роботи є створення системи забезпечення цілісності електронних документів на основі технології блокчейн з урахуванням аналізу розвитку електронного документообігу в України, сучасних тенденцій використання блокчейн технології, а також визначення проблем та ризиків від їх застосування.

З поставленої мети випливають такі **завдання**:

- встановити поняття та види документообігу;
- проаналізувати систему електронного документообігу;
- охарактеризувати властивості ефективної системи електронного документообігу;
- проаналізувати можливості технології блокчейн для побудови систем електронного документообігу;
- з'ясувати особливості використання блокчейн у побудові програмних продуктів;
- визначити основні принципи побудови роботи технології блокчейн;

- охарактеризувати основні етапи розроблення системи забезпечення цілісності електронних документів на основі технології блокчейн.

Предметом даного дослідження є система забезпечення цілісності електронних документів на основі технології блокчейн.

Об’єктом даного дослідження є електронний документообіг.

Практична цінність полягає в тому, що результати дослідження можуть бути використані для проектування систем інформаційної безпеки з метою забезпечення конфіденційності інформації та надійності її захисту.

Методами дослідження є методи роботи з електронними документами; методи пошуку, обробки і зберігання інформації; методи автоматизації різних діловодних функцій;

РОЗДІЛ 1. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

1.1 Поняття та види документообігу

Предметом документообігу є створення наукових знань про документ в єдності його інформаційної та матеріальної складових, про закони, що регулюють створення та функціонування документів у суспільстві.

В інформаційній галузі діють закони прискорення розвитку науки, внаслідок чого потужність документо-інформаційного потоку постійно зростає, відбувається концентрація і розпорошеність публікацій у періодичних виданнях, старіння інформації. Все це призводить до серйозних труднощів у роботі з документами та інформацією, яку вони містять.

Водночас значення інформації в житті людей постійно зростає. Відмінною рисою сучасної епохи є інформатизація всіх сфер людської діяльності. Інформаційні ресурси розглядаються як багатство, що не поступається за вартістю та потенційним впливом природним ресурсам [2, с. 6].

Поняття "документ" є центральним, фундаментальним у концептуальній системі управління документами. Він відображає ознаки реальних об'єктів, які служать об'єктами практичної діяльності для створення, збору, аналітичної та синтетичної обробки, зберігання, пошуку, розповсюдження та використання документальної інформації в суспільстві.

Це поняття широко використовується у всіх сферах соціальної діяльності, в тому числі в діяльності ремонтно-транспортних підприємств. Майже в кожній галузі знань існує одна або декілька версій її розуміння відповідно до особливостей тих об’єктів, яким надано статус документа. У цьому актуальність цього дослідження.

Документ - основний вид ділового спілкування, який фіксує та передає інформацію, підтверджує її достовірність та об’єктивність.

Документ - це матеріальний об'єкт, що містить інформацію у фіксованій формі, складений у звичному порядку та має юридичну силу відповідно до законодавства.

Юридична сила документа - це властивість, надана документу правовими нормами, що засвідчується складом та розташуванням його реквізитів, зовнішніми ознаками та об’єктами його дії.

Документи виконують офіційні, ділові та оперативні функції, оскільки вони є письмовими доказами, джерелом інформації довідкового характеру.

Система документації - це сукупність документів, взаємопов’язаних між собою за характеристиками походження, призначенням, видом, сферою діяльності та єдиними вимогами щодо їх реєстрації.

Документи, що складають одну систему документації (СД), пов’язані єдністю цільового призначення і в комплексі забезпечують документацію про певну функцію управління або вид діяльності [3, с. 90].

Надання документації - це лише одна складова дошкільного навчального закладу, друга її складова - організація роботи з документами. Організація роботи передбачає організацію робочого процесу, зберігання та використання документів у поточній діяльності організації.

Документообіг - це сукупність взаємопов’язаних процедур, що забезпечують переміщення документів від моменту їх створення (отримання) до завершення виконання або відправлення у зовнішнє середовище.

Невід’ємною частиною знань про документ є ознайомлення з основними вимогами до їх оформлення. Основні вимоги до оформлення документів містяться в Державному стандарті України. Актуальність цього дослідження полягає у необхідності надати інформацію про основи стандарту України в галузі діловодства.

Отже, документ є основним засобом спілкування. Він повинен мати таку форму та зміст, що:

- сприяти більш ефективному переміщенню інформації від органів влади;

- забезпечити, щоб одержувач точно розумів зміст документа;

- забезпечити досягнення цілей управління.

Обсяг інформації різного характеру в наш час настільки великий, що в деяких випадках простіше і дешевше повторити дослідження, зробити винахід чи навіть відкриття, ніж знайти інформацію про нього в документах [4, с. 6].

Отже, протягом усього періоду розвитку науки і культури відбувається процес накопичення інформації та знань, які фіксуються в документах. Кількість документів постійно збільшується.

Однією з найважливіших тенденцій розвитку сучасного суспільства є інформатизація, яка в умовах українського суспільства є одним з основних факторів формування України як європейської держави, важливою передумовою її входження у світовий інформаційний простір [5, с. 15]. Встановлення партнерських відносин між організаціями, установами, підприємствами, установами здійснюється та регулюється за допомогою документів - носіїв певної інформації.

У наш час існує потреба у добре підготовлених висококваліфікованих фахівцях, від яких значною мірою залежить якісна підтримка документації. Всі ці процеси, що піднімають людство до нової ери розвитку та глобальних прогресивних змін, здійснюються людьми - кваліфікованими спеціалістами, менеджерами документів, інформаційними працівниками, менеджерами інформаційних систем, керівниками інформаційних служб.

На сучасному етапі управління документами є однією з найбільш перспективних професій, оскільки саме від неї залежить підтримка документації для всіх сфер діяльності суспільства. Спеціальність "Управління документами та інформаційна діяльність" існує лише в Україні. Вперше навчання за цією спеціальністю розпочалось у 1995 році на факультеті бібліотекознавства та інформатики Харківської державної академії культури (КДАК).

На сьогоднішній день понад 20 навчальних закладів України займаються підготовкою спеціалістів з документообігу. Створені курси, підручники, існує

достатня кількість навчально-методичного забезпечення, що повністю забезпечує якісну професійну підготовку випускників університетів.

Різні аспекти формування та розвитку діловодства вивчали провідні вчені, зокрема, Н. Кушнаренко, В. Бездрабко, С. Кулешов, Ю. Столяров, А. Швецова-Горілка, А. Діденко, Ю. Палеха, Т. Сморжанюк, І. Морозюк, Л. Філіппова, Т. Волкотруб, А. Коваль, Н. Гайсинюк, М. Слободяник, А. Мамрак. Документ відображає ознаки реальних об’єктів, які служать об’єктами діяльності для створення, збору, аналітичної та синтетичної обробки, зберігання, пошуку, розповсюдження та використання документальної інформації в суспільстві.

Слово "документ" походить від латинського слова "docere" (знати, свідчити), від якого також походять слова доцент і лікар. Буквальний переклад слова «документ» - доказ, довідка, сертифікація, джерело.

Термін "документ" широко використовується в усіх сферах суспільної діяльності. Майже кожна галузь знань має одну або кілька версій свого розуміння відповідно до специфіки тих об’єктів, яким надано статус документа. Це по-різному розуміється в таких наукових дисциплінах, як: інформатика, бібліотеко-, бібліографічна-, архівна-, музеєзнавство, а також у відповідних спеціальних сферах діяльності - бібліотеці, музеї, архівознавстві та бібліографії. Звідси її неоднозначність, що ускладнює спілкування та взаєморозуміння між фахівцями в документо-комунікативній сфері. Визначення загального значення поняття «документ» є головним завданням теоретичного документообігу (документології).

Протягом тривалого історичного періоду значення поняття "документ" постійно змінювалося. До цього часу застосовувались різні визначення, або надавали йому широке значення, а потім звужували його розуміння до будь-якого виду.

Автором першого в Україні підручника «Документація» для студентів університетів культури є Н. Кушнаренко, де науково обґрунтовані визначення терміна «документ» [6, с. 87].

Міжнародно визнаним є визначення документа як "записаної інформації, яка може бути використана як одиниця в інформаційному процесі". Це визначення було розроблено та схвалено Міжнародною організацією зі стандартизації (ISO) за участю Міжнародної федерації бібліотечних асоціацій, Міжнародної федерації документації, Міжнародної ради з архівів та Міжнародної організації інтелектуальної власності.

Відповідно до стандарту ISO, інформація може бути записана будь-яким способом фіксації будь-якої інформації, тобто з використанням не тільки письмових знаків, але також зображень, звуку тощо. Це визначення дозволяє посилатися на документи всі матеріальні об'єкти, які використовується для передачі інформації в суспільстві (включаючи музейні експонати, пам’ятки архітектури тощо).

В Україні офіційно прийнято три визначення документа, зафіксованих у низці державних стандартів України:

- записана інформація, яку можна розглядати як одиницю в процесі інформаційної діяльності (ДСТУ 2392-94) [4, с. 10];

- матеріальний об'єкт з інформацією, зафіксованою техногенним методом для її передачі в часі та просторі (ДСТУ 3017-95)

- матеріальний об’єкт, що містить інформацію у фіксованому вигляді, оформлений у звичному порядку та має юридичну силу відповідно до чинного законодавства (ДСТУ 2732-94) [7, с. 42].

"Термінологічний словник інформатики" тлумачить "документ" таким чином: "матеріальний об'єкт, що містить фіксовану інформацію і спеціально призначений для її передачі та використання".

Велика радянська енциклопедія дає таке визначення: "документ - це матеріальний об'єкт, що містить інформацію у заданій формі і спеціально призначений для її поширення в просторі та часі".

У "Термінологічному словнику бібліотечної справи та суміжних галузях знань" пояснюється: "документ - це матеріальний об'єкт, на якому зафіксована інформація у вигляді тексту, звукозапису або зображення, призначений для

передачі в часі та просторі з метою збереження та громадського користування "[4].

«Документ призначений для« термінологічного словника з теорії та практики наукової інформації »- це матеріальний об’єкт, що містить інформацію у фіксованому вигляді» [8, с. 13].

А. Михайлов, А. Черний, Р. Гіляревський визначають документ як матеріальний об'єкт, що містить нерухому інформацію, спеціально призначену для її передачі в просторі та часі, та такий, що використовується в публічній практиці.

А. Коршунов запропонував таке визначення поняття "документ - це будь-який матеріальний носій, на якому особа закріпила (закріпила) соціальну інформацію" [9, с. 6].

Ю. Столяров вважає, що документ - це будь-яка неінформація (створена людським розумом, на відміну від інформації неживої природи), зафіксована в просторі та часі з метою її використання, передачі, зберігання.

Українська дослідниця типології документів Г. Швецова-Горілка вважає доцільнішим визначати документ як матеріальний об’єкт будь-який запис інформації, зазначаючи, що запис може бути зроблений будь-яким способом, розробленим людиною: словесно-письмовим, живописно-графічний, живописний, музичний, картографічний; запис інформації, призначеної для читання комп’ютера, запису звуку або переміщення [10, с. 44].

На думку Н. Кушнаренка, для ведення діловодства в даному випадку найбільш прийнятним є визначення документа як такого, який є двосторонньою одиницею - поєднанням матеріального об’єкта інформації, зафіксованим придуманим людиною методом. Без однієї з цих сторін немає жодного документа.

Це визначення дає змогу обмежити коло основних документів - об’єктів документальної комунікативної діяльності, зосередитись на понятті, що використовується бібліотекознавством, бібліографією, бібліологією та деякими іншими суміжними галузями знань.

У бібліотечній, бібліографічній, книгопродажній, інформаційній діяльності вони працюють зі спеціально виготовленими об’єктами, тобто документами, призначеними для одночасного виконання двох основних для документа функцій - це збереження та передача інформації в часі та простору. Документ має ряд властивостей, що відрізняють його від інших об’єктів. Сукупність властивостей - це цілісна система, яка виконує функції, покладені на нього суспільством. Зв'язок між властивостями документа досить тісний, тому їх можна розділити лише умовно.

Найважливіші властивості такі:

1) атрибутивність, тобто наявність цілісних компонентів, без яких вона не може існувати;

2) функціональність - пункт призначення для передачі інформації в просторі та часі;

3) структура - тісний зв’язок елементів та підсистем, забезпечує єдність і цілісність документа [11, с. 7].

Визначте такі атрибути документа:

1) наявність змістової семантики, тобто документ є носієм думки, яка передається знаками, сукупністю послідовно розташованих знаків, що передають зміст документа (повідомлення), є його обов’язковою ознакою;

2) стабільна матеріальна (матеріальна) форма документа повинна забезпечувати його тривале зберігання та забезпечувати можливість багаторазового використання та переміщення інформації в просторі та часі;

3) на основі призначення для використання в соціальному спілкуванні статус документа мають лише ті об’єкти, які спочатку призначені для зберігання та передачі інформації у просторі та часі, а отже, документи є носіями інформації, спеціально створеними особою забезпечити певні комунікативні цілі;

4) повнота повідомлення, тобто документ не може бути повним, якщо він містить фрагментарне неповне повідомлення.

Отже, саме документ є центральним і фундаментальним у концептуальній системі управління документами, є результатом цілеспрямованої діяльності, що відбувається в рамках колективних дій, і утворює функціональну підсистему ДКС [12, с. 12].

Ця практична діяльність містить важливі елементи: - документацію, метою якої є створення будь-якого змістовного повідомлення. Цей процес включає дві частини: інтелектуальну (творчу) - впорядкування документа, та технічну - його виготовлення; - розробка, метою якої є змістовна та формальна оцінка документа. На основі цієї оцінки здійснюється літературна, наукова та технічна обробка авторського повідомлення - видавнича обробка; технічна та аналітично-синтетична обробка отриманих у фонд бібліотеки, інформаційного центру, архіву, музею тощо; - розповсюдження, мета якого - донести документ до споживача.

Існує два види такої діяльності:

1) розповсюдження документів за допомогою книжкової торгівлі, передплати тощо;

2) надання документів, що зберігаються у фондах служб з обробки, зберігання та розповсюдження документів - інформаційних центрів, бібліотек, архівів тощо;

- збереження, метою якого є забезпечення довгострокової фізичної цілісності та захист документів від передчасного знищення. Він містить державний та відомчий облік документів, створення та підтримку оптимальних умов зберігання, здійснення їх консервації, відновлення, біохімічного захисту, створення та поповнення страхових фондів; - використання, метою якого є вивчення документа, отримання з нього необхідної інформації.

Споживчу активність можна розглядати стосовно:

а) документ, як матеріальний об’єкт, можна на деякий час придбати або позичити для читання;

б) документ як повідомлення, прочитаний, вивчений - залежно від рівня сприйняття та мети;

- переробка, мета якої - здати документ на брухт для подальшої переробки.

Процес включає ідентифікацію документів із термінами зберігання, які втратили практичну цінність, відбір їх для знищення та здачу на брухт для переробки. Кожен окремий процес є специфічним, його особливості залежать від типу та типу документа.

Зараз робляться спроби уніфікувати технологічні процеси, для яких розробляються єдині стандарти (ДСТУ) для видавництв, поліграфічних компаній, бібліотек, органів НТІ, архівів тощо.

Це дає змогу впорядкувати роботу зі створення, обробки, розповсюдження, зберігання, використання та розпорядження документами, зменшити та найефективніше усунути розбіжності в методах та використовувати електронні обчислювальні технології.

Документація вивчає систему документів, тобто систему, що складається з документів. Система документального спілкування (ДКС) - це підсистема соціального спілкування, що забезпечує створення, обробку, зберігання та розповсюдження документальної інформації в суспільстві. Система документообігу - це сукупність усіх документів, відправники документальної інформації (автор, видавець), її споживачі (читач, слухач, глядач), професійні посередники (бібліотекарі, бібліографи, спеціалісти з питань інформації та документації), виробничі процеси (створення, обробка , збереження, розповсюдження документів) та взаємозв'язок між ними, обумовлений як внутрішніми властивостями системи, так і зовнішнім середовищем її соціального функціонування.

Відсутність хоча б одного з елементів БКС призводить до непослідовності системи [13, с. п’ятнадцять].

У документо-комунікаційній системі існує три історично сформовані підсистеми: атрибутивна, функціональна та управлінська. Атрибутивна підсистема DKS - це сукупність відносно незалежних рівнів документообігу,

сформованих відповідно до того чи іншого атрибута документа: - рівень первинного документа - це всі первинні документи з відповідними каналами.

Цей рівень - це галузь бібліотечної, архівної, музейної діяльності; - вторинний документальний рівень - галузь інформаційної, бібліографічної та бібліотечної діяльності. Функціональна підсистема БКС - це сукупність незалежних рівнів БКС, сформованих за видами документальної діяльності. Існує два контури функціональної підсистеми БКС: рівень документації; рівень обробки, розповсюдження, зберігання, використання та розпорядження документами.

Між атрибутивною та функціональною підсистемами БКС існує тісний зв'язок, і їх можна розглядати окремо лише теоретично. Підсистема управління БКС - це постійне, безперервне впорядкування атрибутивної та функціональної підсистем БКС.

Він містить регулювання, зміну (при збереженні якісної специфіки) знакової системи, засобів запису, сприйняття та відтворення інформації, вдосконалення матеріальної основи та форми документа, приведення їх у відповідність із зростаючими документальними потребами суспільства, як а також регулювання всіх процесів, пов'язаних зі створенням та функціонуванням документа [14, с. 13].

Колекція документів створює потоки документів, масиви, ресурси, кошти тощо. Документообіг (ДП) - це організована сукупність документів (первинних чи вторинних), які функціонують у соціальному середовищі. ГП зазначається як сукупність документів, що змінюються з часом, що знаходяться в динаміці. ГП характеризується інтенсивністю, вираженою кількістю одиниць публікацій, видань, одиниць зберігання тощо в одиницю часу (місяць, рік).

Масив документів (DM) - це сукупність незмінних у часі документів (книг, приміток, карт, записів, дисків тощо). ДМ характеризується кількістю, вираженою в одиницях видань, публікацій, обліку, зберігання. Окрім тимчасових, DM може мати й інші обмеження: змістове, мовне, територіальне тощо [7, с. 33].

Документні ресурси (ДР) - це впорядкована сукупність документів, що слугують засобом або об’єктом документообігу (переміщення документів) або поповнення фонду документації. Це документальні ресурси книговидавців, редакцій газет, журналів, підприємств, що мають редакційно-видавничі відділи та копіюють та тиражують підрозділи студій, фірм та асоціацій, копіюють фотодокументи; магазини, колекціонери бібліотек, пошта.

Документація - сукупність документів, відібраних спеціально для певного предмета: наукові (фіксація курсу та результатів наукових досліджень), науково-технічні (фіксація процесу та результатів наукових досліджень, технічні розробки, а також напрямки та методи їх впровадження у виробництво), організаційно-адміністративні та ін.

Фонд документів - сукупність документів, зосереджених у бібліотеках, інформаційних центрах, архівах, музеях тощо. Специфіка фонду документів полягає в тому, що різні документи, зібрані у фонді, відбираються відповідно до завдань, потреб користувачів (читачів, слухачів , глядачі) тієї чи іншої документальної структури, організованої певним чином [15, с. 34].

Таким чином, документ є центральним та основним у концептуальній системі управління документами. Протягом тривалого періоду цей термін набув багатьох змін і сьогодні служить об'єктом створення, збору інформації для його використання в суспільстві (простір і час).

1.2 Система електронного документообігу

Документообіг в державі є системою, матеріалізує процеси збору, перетворення, зберігання інформації, а також процеси управління: підготовку та прийняття рішень, контроль за їх виконанням. На рівні установи спеціальні служби допомагають адміністрації вирішувати управлінські завдання, забезпечуючи підготовку і рух документів, доставку їх до виконавців та зацікавлених осіб. До таких служб в науковій установі належать канцелярія, відділ кадрів, бухгалтерія, юридичний відділ, плановий відділ, архів та інші. Стрімке зростання обсягів інформації, використовуваної в управлінській

діяльності установи, його структурна складність і швидка оновлюваність робить необхідним використання інтегрованих систем електронного документообігу (СЕД) [2, с. 89].

Ефективне впровадження технологій електронного урядування неможливо без розгортання систем електронного документообігу із застосуванням технологій електронного цифрового підпису. Електронний документообіг є одним з головних технічних елементів системи електронного управління, адже саме він забезпечує циркуляцію електронних документів, які є основою нової форми взаємодії держави і суспільства. Звернення за допомогою документа є необхідною умовою надання послуги державою громадянинові [3, с. 2].

Однак кожен документ повинен мати встановлений законодавством набір реквізитів, до яких відноситься, зокрема, підпис - елемент, підтверджує авторство документа [4, с. 6].

Для чіткості подальшого викладу зазначимо, що під поняттям "електронний документ" відповідно до закону України "Про електронні документи та електронний документообіг", розуміти документ, інформація в якому зафіксована у вигляді електронних даних, серед яких обов'язкові реквізити документа. Електронний документообіг (обіг електронних документів) - сукупність процесів створення, обробки, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності - з підтвердженням факту отримання таких документів [1, с. 37]. Також будь-який документ повинен бути ідентифікований певної юридичною або фізичною особою, його створила. У паперових документах використовують підпис і печатку, а для електронних документів введена електронна підпис. Такий реквізит - це дані про особу, наведені в електронній формі, додаються або логічно з'єднані з електронним документом і служать для ідентифікації [5, с. 4].

Як відомо, будь-який підпис, то звичайний або цифровий, виконує зазвичай три функції: посвідчення, що той, хто підписався, є тим, за кого ми його приймаємо (функція авторизації) особа, підписалася, не може відмовитися від підписаного нею документа; підтвердження, що відправник підписав саме той документ, який відправив, а не будь-який інший. Інакше кажучи, йому не можна нав'язати інший або схожий документ, оскільки у нього є підписана копія оригіналу.

Поява перших електронних обчислювальних машин (ЕОМ) в середині минулого століття безпосередньо пов'язана з необхідністю складних математичних обчислень. Розвиток технічних засобів непередбачувано швидко дозволив розширити сферу функціонального застосування ЕОМ за межі обчислювальних задач і використовувати їх для автоматизації технологічних процесів у виробництві, а також напрямків людської діяльності, пов'язаних з обробкою інформації.

В середині 80-х років розвиток технічних засобів автоматизації отримав потужний імпульс, викликаний успіхами в мікроелектронних технологіях: в результаті створення персонального комп'ютера (ПК) потужні засоби обробки інформації стали доступні і звичайні користувачі. Високу ефективність застосування технічних засобів автоматизації інформаційних технологій звернув увагу В. М. Глушков, який до деталей передбачив тенденції розвитку цієї галузі, і виклав їх у книзі "Основи безпаперової інформатики" [6, с. 4].

Зокрема, він вказав на необхідність використання комп'ютерних мереж, загальних (корпоративних) і розподілених баз даних. У впровадженні і використанні електронних документів В.М. Глушков ввів термін "безпаперова інформатика", а автоматизацію організаційного управління виділив в окремий розділ у вищезгаданій книзі.

Подальший розвиток систем електронного документообігу стримується НЕ стільки технічними можливостями сучасних засобів автоматизованої обробки інформації, скільки відсутністю відповідних нормативно-правових актів, що забезпечують захист авторських прав у галузі інформаційних

технологій та нормалізують правовий статус електронних документів . Вирішенню цих проблем частково сприяють закони України "Про електронні документи та електронний документообіг" (No 851 - IV) та "Про електронні цифрові підписи" (No 852 - IV) від 22 травня 2003 року, однак , висновки експертів свідчать про те, що вони не відповідають європейським стандартам та необхідності внесення значних змін та доповнень. Ця проблема є предметом уваги на державному рівні. Так, Указом Президента України No 1497/2005 від 20 жовтня 2005 р. "Про пріоритетні завдання впровадження новітніх інформаційних технологій" передбачено "... законодавчу базу для розробки та впровадження новітньої інформації технологій та адаптації українського законодавства з цих питань до законодавства Європейського Союзу, зокрема, шляхом:

- підготовка законопроекту про внесення відповідних змін до Національної програми інформатизації щодо визначення стратегічних напрямків розвитку інформаційного суспільства та вдосконалення механізмів реалізації державної політики у цій галузі;

- підготовка проектів нормативно-правових актів щодо впровадження електронного документообігу, здійснення експортно-імпортних операцій, процедур сертифікації з використанням електронних цифрових підписів, захисту авторських прав у галузі інформаційних технологій »[7, с. 90].

На виконання цього Указу Верховна Рада України 4 листопада 2005 року своєю постановою затвердила "Завдання Національної програми інформатизації на 2006-2008 роки", яке передбачає комплексне вирішення низки правових та організаційних проблем, що перешкоджати широкому впровадженню перспективних інформаційних технологій у сфері управління, зокрема визначенню організаційно-правової бази для впровадження електронного документообігу з використанням електронних цифрових підписів, розвитку інформаційної системи "електронний уряд", забезпеченню -захист вірусної інформації, захист національного сегменту Інтернету, боротьба з комп’ютерною злочинністю.

Впровадження сучасних інформаційних технологій в освіту та наукові дослідження має особливе значення. Враховуючи важливість цих галузей для досягнення стратегічних цілей соціального розвитку та місце країни у світовому співтоваристві, Державною програмою "Інформаційно-комунікаційні технології в освіті та науці" було затверджено постановою уряду від 7 грудня 2005 року.

Незважаючи на заявлену організаційну недосконаліть передумов для створення повноцінних систем електронного документообігу, наявні технічні можливості дозволяють організувати документообіг в межах окремої установи та підрозділів, щоб значна частина рутинної роботи виконувалась за допомогою технічних засобів. Для досягнення найменших затрат праці та підвищення ефективності роботи з документами необхідно ретельно продумати схему організації їх руху від моменту створення до моменту завершення роботи з ними [8, с. п’ятнадцять].

На сучасному етапі розвитку завдання полягає в систематичній автоматизації процесів організації документообігу, поступово замінюючи «паперові» технології електронними. Зрозуміло, що протягом певного періоду ці процеси існуватимуть паралельно, а електронні технології будуть лише допоміжним засобом, що дублює практику роботи з документами, правильною в юридичному аспекті.

Створення інтегрованої системи електронного документообігу передбачає, перш за все, забезпечення швидкого та зручного переміщення документів (указів, постанов, законів, наказів, аналітичних звітів, повідомлень, звітів тощо), що забезпечить збільшення ефективність процесів управління завдяки значному скороченню періоду підготовки та прийняття рішень завдяки автоматизації процесів колективного створення та використання документів в установах.

Наступні основні вимоги стосуються системи електронного документообігу: масштаб, розподіл, модульність та відкритість. Масштабна потужність потрібна для того, щоб система могла підтримувати будь-яку

кількість користувачів (здатність системи збільшувати ємність визначалася потужністю відповідного програмного забезпечення) [9, с. 65].

Архітектура систем управління документами повинна підтримувати взаємодію розподілених сайтів для роботи з документами в географічно розподілених організаціях. Також система повинна складатися з окремих інтегрованих модулів. Модульність потрібна на випадок, якщо користувачеві системи не потрібно негайно реалізовувати всі компоненти системи робочого циклу, або коло завдань установи вужче, ніж весь спектр завдань робочого циклу. Нарешті, система повинна мати відкритий інтерфейс для можливої подальшої обробки та інтеграції з іншими розподіленими системами.

Електронний документ (електронний запис) - документ, який створюється і використовується лише в межах комп’ютерної системи.

Закон України "Про електронні документи та електронний документообіг" зазначає, що електронний документ (ЕД) - це документ, в якому інформація фіксується у формі електронних даних, включаючи обов'язкові реквізити документа. Юридична сила електронного документа не може бути відмовлена лише через те, що він має електронну форму.

Оригінал ЕД вважається електронною копією документа з обов’язковими реквізитами, в тому числі з електронним цифровим підписом його автора, накладення якого завершує створення документа.

Впровадження інформаційних технологій ініціювало дискусії та дослідження концепції ЕД, її відмінностей та особливостей порівняно з традиційним паперовим документом.

Наприклад, деякі експерти вважають, що ЕД може служити свідченням дій чи взаємодій та містити інформацію про їх зміст. Інші вважають, що він повинен бути відомий своїми метаданими та даними, пов’язаними з іншими даними, тобто інформацією, що визначає його соціальну визначеність та розуміння. У той же час різні набори метаданих ЕД завжди повинні бути юридичним, діловим, організаційним, процедурним підтвердженням справжності, тобто доказом того, що ЕД відповідає зазначеному документу,

створеному або залишеному зазначеним автором чи організацією, а також час зазначений на ній відповідає часу створення або передачі [10, від. 76].

Створюючи електронний документ та залучаючи його до системи документації, слід пам’ятати, що термін зберігання ЕД повинен становити принаймні строк, встановлений законодавством для відповідних документів на папері, і якщо такий термін зберігання неможливий для збереження слід передбачити автентичність, заходи щодо тиражування або періодичного копіювання. ...

Систематичний підхід до вивчення документів полягає в аналізі всіх його властивостей, особливостей та функцій.

Властивості документа - це сукупність характерних якостей, які можна розглядати як спеціальну цілісну систему, призначену для виконання функцій, покладених на документ.

Основними властивостями службового документа повинні бути:

• - атрибуція - наявність інтегральних компонентів, без яких вона не може існувати)

• - функціональність - призначення для передачі в часі та просторі;

• - структурованість (тісний зв’язок елементів та підсистем, забезпечує її єдність і цілісність).

Сервісний документ повинен також мати такі властивості:

• - бути носієм та служити джерелом необхідної інформації, оскільки саме в документах інформація фіксується вперше;

• - мають юридичну вагу, економічне значення, оскільки саме воно може служити письмовим доказом, засобом засвідчення чогось;

• - зробити можливим витяг інформації з архівів та обробку в поточній діяльності установи [11, с. 12]

При укладанні офіційних документів доповідачі певною мірою обмежуються у виборі та підборі слів, їх поєднанні, розташуванні; творчість як така відсутня. Укладач документа повинен дотримуватися встановлених правил і не відступати від них, тобто дотримуватися певних нормативних актів, у свою

чергу, забезпечить відповідність стандартизації мови та схеми документів. Тому кажуть, що документи укладаються, а не пишуться.

Ознаки службового документа - це характерні ознаки, що відрізняють документ від інших матеріальних об'єктів.

Основні особливості офіційного документа включають:

- наявність семантики вмісту,
- стабільна матеріальна (реальна) форма,
- бути придатним для використання в соціальному спілкуванні,
- повнота повідомлення.

Функції документа (від лат. - виконання) - це призначення документа, його роль у системі соціальних комунікацій.

Функції документа визначають орієнтацію характеристик документа на виконання його цільового призначення, соціально-словесні засоби його реалізації. Вони реалізуються чи не реалізуються під час функціонування документа (тобто під час його використання) залежно від того, яку орієнтацію на певне функціонування заклав автор документа в його характеристиках.

Основна функція документа - передавати їм соціальну інформацію. Серед функцій документа виділяють загальну та спеціальну.

Розгляд документа як системи дозволяє виділити певні групи його функцій, зокрема, функції двох його компонентів: інформації (документальної інформації) та її носія, в свою чергу, можна розглядати як сукупність функцій елементів кожного з компонентів. Отже, інформаційна функція, зазначає проф. С. Кулешова, колективно виконують такі елементи інформаційної складової, як зміст, реквізити, креслення, малюнки, довідковий апарат документів, перелік джерел тощо, і кожен з них у межах цієї функції реалізує свою специфічну функцію [13, с. 98]

В. Євдокимов зазначає, що в сучасних умовах виділяються такі тенденції розвитку електронного документообігу:

- оскільки електронний та паперовий документообіг існуватимуть паралельно протягом тривалого періоду часу, необхідне їх максимальне поєднання та узгодження дій на підприємстві;

- внутрішній електронний документообіг зараз ефективно функціонує, у зовнішньому документообігу можна виділити такі сфери: клієнт-банк, звітність на оптичних та магнітних носіях.

Однак розвиток банківської справи вимагає ефективності документообігу, можливо, шляхом переведення його в електронну форму;

- відбувається розмивання меж між зовнішнім та внутрішнім документообігом: корпоративні системи включають своїх контрагентів як користувачів; постачальники використовують дані планування виробництва для прогнозування обсягів і графіків поставок; дистриб'ютори та / або дилери розміщують замовлення, координують та відстежують їх виконання (для цього вони використовують системи SCM - управління ланцюгами поставок) [15, с. 26].

Варто зазначити, що ви можете додати до зовнішнього робочого процесу: подання електронної звітності за каналами зв'язку, отримання довідки про відсутність заборгованості за податками та зборами, що контролюються ДПС, обмін податковими накладними та квитанціями їх акцепт між контрагентами, обмін контрактами, актами, рахунками-фактурами між контрагентами тощо [15, с. 4].

Процес електронного документообігу заснований на інтегрованій електронній обробці облікової та звітної інформації, включаючи формування первинних електронних документів, процедуру обробки інформації, автоматизований банк даних тощо. Електронний документообіг призначений для забезпечення процесів створення, контролю доступу та розподілу великих обсягів документів у комп’ютерних мережах, а також контролю за рухом документів на підприємстві.

1.3 Властивості ефективної системи електронного документообігу

Україна поступово інтегрується в європейське співтовариство, цей процес вплинув на динаміку розвитку внутрішнього економічного та інформаційного середовища. У таких умовах для розвитку вітчизняного бізнесу особливо важливо створити ефективно діючу систему документальних комунікацій, оскільки знання в сучасному світі є основою економічної діяльності. Тому в останнє десятиліття з'явились і набули поширення нові інструменти для ефективного забезпечення процесів управління. У тому числі мова йде про програмне забезпечення, призначене для обробки документів [16, с. чотири].

Сьогодні важливо мати доступ до інформаційних ресурсів і скоротити час, витрачений на вирішення проблем, пов'язаних з документообігом. Саме електронний документообіг відкриває можливості для вдосконалення, тривалого зберігання документів, управління електронним архівом з урахуванням процедур списання та знищення документів. Розробка програм для вдосконалення документообігу активно проводиться як українськими, так і іноземними компаніями, безсумнівно, доводить актуальність досліджуваного питання [1, с. 54].

Слід зазначити, що електронний документообіг у сучасному світі став глобальним і розгалуженим, проте не всі відносини між його учасниками регулюються спеціальними законами чи іншими юридичними документами. Розвиток електронного документообігу, пов'язаний не лише з технологіями, а й із законодавством, вимагає професійних підходів, чіткої взаємодії традиційно віддалених галузей знань.

Ринок електронного документообігу розвивається дуже динамічно. Життя підтвердило актуальність проблеми: на додаток до традиційно зростаючого попиту великих підприємств, сектор малого та середнього бізнесу починає відчувати зростаючу потребу в автоматизації документообігу. Протягом наступних трьох років внутрішній ринок систем документообігу збільшуватиметься на 70% на рік [17, с. 64].

Електронний документообіг включає: створення документів, їх обробку, передачу, зберігання, виведення інформації, що циркулює в організації чи на підприємстві, на основі використання комп’ютерних мереж.

Загалом під управлінням електронним документообігом прийнято розуміти організацію руху документів між підрозділами підприємства чи організації, групами користувачів чи окремими користувачами. У той же час переміщення документів означає не їх фізичний рух, а передачу прав на їх використання на повідомлення конкретних користувачів та контроль за їх виконанням.

Основні принципи організації електронного документообігу:

- одноразова реєстрація документа;

- можливість паралельного виконання різних операцій з метою скорочення часу руху документів та підвищення ефективності їх виконання; - безперервність руху документа;

- єдина база документальної інформації для централізованого зберігання документів і виключає можливість дублювання документів;

- ефективно організована система пошуку документів;

- розроблена система звітності, що дозволяє контролювати рух документа в процесі документообігу [18, с. 73].

Електронний документообіг включає, крім контрольованого руху готових документів як всередині організації, так і поза нею, також етап підготовки документів та вільний обмін інформацією через комп’ютерні мережі. Тому завдання комплексного аналізу програмних засобів, представлених на сучасному ринку України, є актуальною сьогодні. Основні системи електронного документообігу, які використовуються на українському ринку:

1. Documentum. Основне призначення системи - управління документами, знаннями та бізнес-процесами на великих підприємствах та організаціях.

2. Система LanDocs в основному орієнтована на діловодство та архівне зберігання документів.

3. Система Delo забезпечує повний журнал дій користувачів з документами.

4. Система BOSS-Referent призначена для використання у великих корпораціях зі складною ієрархічною структурою.

5. Docs Fusion та Docs Open. Вони є однією з найпопулярніших систем електронного архівування у світі.

6. Система Optima Workflow призначена для формалізації стандартних процедур роботи з документами.

7. «M.E.Doc IS» - це програма, яка допоможе у роботі з документами різного типу і призначена для роботи зі звітами, податковими накладними, актами, накладними тощо [2, с. 23].

Сьогодні ринок продуктів електронного документообігу стрімко розвивається. Розробляється і впроваджується нове, більш прогресивне програмне забезпечення, завдяки якому діяльність підприємств переходить на якісно новий рівень. І вибір тієї чи іншої категорії електронних систем документообігу повинен виходити з мети та завдань, які є головними для підприємства. Правильний вибір допоможе пришвидшити офісні процеси та позитивно вплинути на діяльність підприємства [19, с. п’ять].

Для оптимізації та полегшення роботи з документами доцільно використовувати програму M.E.Doc, за допомогою якої ви можете легко та швидко:

- створити всі необхідні документи; - підписувати документи електронним цифровим підписом (ЕЦП);

- обмінювати податкові накладні та квитанції для їх реєстрації з контрагентами;

- запрошувати та отримувати витяги з цього реєстру;

- перевіряти, шифрувати та зберігати електронні документи в єдиній системі;

- надсилати звіти до контролюючих органів за лічені секунди;

- отримувати квитанції про отримання та обробку надісланих документів (звітів, податкових накладних тощо);

- обмінюватись податковими накладними та квитанціями, а також актами, контрактами з контрагентами;

- реєструвати податкові накладні, отримувати реєстраційні квитанції / виписки з реєстру;

- надсилати звіти до контролюючих органів;

- створювати податкові накладні, звіти, акти, рахунки, накладні, контракти та інші документи;

- перевіряти, друкувати та зберігати документи на електронних носіях;

- зашифрувати та підписати електронним цифровим підписом [19, с. 12].

У системі "ME.Doc" електронні документи стають електронними оригіналами документів завдяки використанню електронного цифрового підпису. Не потрібно витрачати дорогоцінний час на надсилання податкових накладних та інших первинних документів поштою або факсом. Ви можете надіслати електронний документ за допомогою системи M.E.Doc за 1 хвилину. А для надсилання документів у паперовій формі потрібно 4-6 днів. Не потрібно витрачати гроші на папір, пошту чи кур’єрські служби.

Не потрібно доплачувати за систему M.E.Doc - обмін первинними документами входить у стандартний пакет послуг. Під час аналізу системи електронного документообігу на підприємстві було виявлено, що через великі обсяги інформації існує необхідність у створенні програми, яка дозволяє зберігати її найбільш зручним та якісним способом. Ця можливість у комп’ютерному середовищі забезпечується архівуванням файлів.

Компанія «1С» випустила програму, що забезпечує автоматизацію повного циклу обробки офіційних та внутрішніх документів комерційних підприємств та бюджетних установ за підтримки як електронного, так і паперового документообігу [20, с. 74].

Вивчивши питання впровадження електронного архіву на підприємстві, зазначимо, що його основними перевагами є: економічна доцільність, безпека

та конфіденційність, ефективність роботи з документами та надійність. Отже, кілька користувачів можуть одночасно працювати з одними і тими ж документами для будь-якої структури та типу локальної мережі підприємства, це абсолютно недоступно при використанні звичайного архіву, в якому на певний час кожен документ доступний лише для одного працівника.

З вищесказаного можна зробити висновок, що електронний документообіг та електронні документообіги є важливими складовими роботи з документами. За допомогою електронних документообігу можна оптимізувати роботу з документами, скоротити час передачі та отримання інформації.

Вже сьогодні можна говорити про глобальне застосування технології електронного безпаперового документообігу, яка об'єднує користувачів в єдину мережу, здатна забезпечити швидкий, цілісний обмін документами, здійснюється за єдиними оптимальними правилами та правилами.

РОЗДІЛ 2. АНАЛІЗ МОЖЛИВОСТЕЙ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПОБУДОВИ СИСТЕМ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

2.1 Використання блокчейн у побудові програмних продуктів

Нова парадигма інформаційного простору блокчейнів набула широкого поширення у всьому світі, зокрема в Україні. Інтернет вступає в наступну стадію розвитку. Всесвітня павутина дозволила швидко обмінюватися інформацією. Це можна назвати "Всесвітньою павутиною інформації". Другий етап - впровадження технології блокчейну, яка дає можливість обмінюватися цінностями, створюючи Всесвітню книгу. Тепер ви можете практично обробити все, що важливо для людини і може бути представлене в цифровому форматі: гроші, сертифікати, контракти, майнові права, дипломи та вчені звання, фінансові рахунки, медичні процедури, страхові претензії, результати голосування, походження продуктів харчування. Почалася нова ера цифрової економіки.

Попередній етап ознаменувався поєднанням обчислювальних та комунікаційних технологій. Новий етап базується на розробці комп’ютерних систем, математиці, криптографії та поведінковій економіці [21, с. 83].

«Блокчейн» (блок - блок, ланцюжок - ланцюжок) - це спосіб зберігання даних, який ще називають цифровим регістром будь-яких операцій, упорядкованих у блоки за ланцюговим принципом. Ефективні рішення на основі блокчейну вже існують і успішно працюють у світі, такі як, наприклад, Біткойн - інноваційна платіжна мережа та цифрова валюта, Хоробрий - браузер, який має можливість здійснювати анонімні платежі власникам веб-сайтів та багато інших успішних реалізації.

Ринок стартапів, заснованих на використанні технології блокчейн, за оцінками експертів, залучить інвестиції на суму $ 3 млрд у 2018 р. Використання технології блокчейн викликає інтерес в Україні. Україна уклала угоду з міжнародною технологічною компанією Bitfury Group про передачу всіх електронних державних даних у блокчейн [22, с. 93].

Bitfury розпочне з пілотного проекту, який переведе державні реєстри, соціальне забезпечення, державні служби та охорону здоров'я на блокчейн.

Після завершення пілотного етапу всі сфери, включаючи кібербезпеку, будуть передані до розподіленої книги.

У зв'язку із швидким розвитком блокчейн-сервісів, API для розробників блокчейн-систем, статистики та моніторингу блокчейн-мереж, існує необхідність проаналізувати переваги та недоліки існуючих підходів та реалізацій для використання в різних секторах економіки, і соціальна сфера. Існує необхідність визначити напрямки розвитку безпечних додатків корпоративного блокчейну та вирішити такі проблеми, як безпека, висока доступність та швидкість транзакцій. У галузі блокчейн-процесів процес формування загальновизнаного багаторівневого опису технологій ще не завершений, тому існує необхідність проаналізувати та однозначно визначити три частини концепції: основну технологію блокчейну, протокол передачі даних та цифровий ресурс для корпоративного блокчейну.

Концепція першого блокчейну була розроблена в 2008 році людиною (або групою людей), відомою як Сатоші Накамото. У 2008 році був описаний електронний протокол оплати однорангової мережі (P2P). Це математичний алгоритм, який дозволяє безпечно та приватно обмінювати цінності через однорангові мережі. Протокол, створений Накамото, називається «протоколом довіри» [23, с. 83].

Це заклало основу технології блокчейн. У 2009 році ця технологія була впроваджена в рамках цифрової валюти - біткойн. Таким чином, мережа біткойнів стала першим успішним практичним впровадженням технології блокчейн. У 2015 році журнал The Economist опублікував статтю "Довірча машина", в якій зазначено, що технологія мережі біткойн може повністю змінити економіку. Саме ця технологія стала першою, яка змогла вирішити інформаційну проблему, наприклад, забезпечити довіру між сторонами до отриманої інформації без залучення зовнішніх гарантів - банків, посередників тощо. Автори багатьох публікацій про блокчейни Дон Тапскотт та Алекс Тапскотт проаналізували програми, послуги, бізнес-моделі, ринки, організації та навіть уряди, що працюють з блокчейном. Визначив закономірності та

сформулював 7 принципів, на які спираються послідовники технологій [24, с. 51].

Блокчейн у найпростішому розумінні - це розподілена база даних, в якій кожен може безпечно приєднатися та виконувати код транзакції. Інформація про транзакції знаходиться у загальнодоступній загальнодоступній базі даних блокчейнів. Він підтверджує та приймає операції мережі P2P. Ієрархія таких систем повністю горизонтальна [4, с. 43]. Всі учасники рівні, будь-який учасник системи є контрольним пунктом.

Рівна мережа. Щоб використовувати блокчейн для запису транзакцій, вам потрібно мати можливість перевірити блокчейн. Поточний стан блокчейну завантажується, синхронізується та передається багатьом комп'ютерам з усього світу. Ці комп'ютери називаються «вузлами» або «вузлами», і вони працюють разом у одноранговій мережі, щоб забезпечити безпеку та оновлення блокчейну. Кожен із цих вузлів підтримує повну, оновлену (поточну) версію блокчейну. Щоразу, коли додається новий блок, усі вузли оновлюють свій блокчейн.

Використання однорангової мережі має певні переваги:

• Ви завжди можете перевірити стан блокчейну за допомогою провідника блокчейнів

• не потрібно покладатися лише на одну сторону, щоб знати справжнє положення блокчейну;

• не потрібно покладатися на безпеку одного сервера, щоб знати, що блокчейн захищений;

• зловмисникові доведеться одночасно зламати тисячі комп'ютерів, а не одного сервера;

• завжди є впевненість, що блокчейн ніколи не зникне, оскільки для цього його доведеться знищити на всіх вузлах [26, с. 76].

Усі транзакції зберігаються в блоках даних, які створені таким чином, що ними досить важко маніпулювати після того, як вони вже увійшли в систему блокчейну. Для того, щоб блок потрапив у блокчейн, необхідно перевірити цей

блок і додати його в систему. Транзакції шифруються двома ключами, відкритим та приватним, що гарантує безпеку. Блоки - це дані про транзакції, угоди та контракти всередині системи, представлені в криптографічній формі.

У ланцюжку існує сувора послідовність. Кожен із блоків містить масив конкретних даних. Всі блоки взаємопов'язані. Для написання нового блоку необхідно послідовно читати інформацію про старі блоки. Кожна ланка ланцюга містить певний ключ. Поки його не розшифрують, блок не закриється.

Послідовність дій така:

• користувач А хоче укласти угоду (транзакцію) з користувачем В;

• маючи відкритий ключ для виконання операції, користувач А встановлює інформацію про операцію, щоб сформувати блок, і передає її в мережу;

• роботу перевіряють усі учасники мережі. Якщо помилок немає, тоді кожен учасник додає блок до свого розподіленого екземпляра бази даних. Блок додається до блокчейну і транзакція підтверджується;

• відповідь на підтвердження транзакції разом із закритим ключем для отримання ресурсу надходить до користувача В [27, с. 76].

Всі ланцюжки блоків розподіляються, це обробляється комп'ютерами по всьому світу. Немає центрального сервера, який би вийшов з ладу. Блокчейн є загальнодоступним і одночасно дуже надійним, оскільки використовує зашифровані дані.

Неможливо щось видалити з цієї бази даних або замінити / замінити блок. І це "безмежно" - ви можете записати в нього нескінченну кількість транзакцій. Це одна з головних особливостей блокчейну. Всі операції проводяться безпосередньо між випробовуваними. І проводяться вони завдяки тому, що всі учасники підключені до однієї мережі. Блокчейн має можливість вирішувати такі проблеми, як безпека, висока доступність та швидкість транзакцій. Механізм консенсусу. Сатоші Накамото, засновник біткойнів, поєднав блокчейн із механізмом консенсусу на основі криптографії.

Механізм консенсусу дозволяє вузлам однорангової мережі працювати разом, не знаючи і не довіряючи один одному. Метою консенсусного алгоритму є безпечне оновлення стану згідно з деякими конкретними правилами, з правом вносити зміни стану, розподіленими між користувачами, яким надано право колективно вносити ці зміни за допомогою алгоритму. Механізм консенсусу - це просто набір правил, які узгоджуються вузлами в мережі під час запуску програмного забезпечення в мережі.

Ці правила дозволяють мережі працювати за призначенням та залишатися в синхронізації. Протокол консенсусу встановлює правила:

• як слід додавати блоки до блокчейну;

• коли блоки вважаються дійсними;

• як вирішуються конфлікти.

Найвідоміший механізм консенсусу - це доказ роботи (PoW), який використовується в мережі біткойнів, доказ стану (PoS), який використовується в Coin [28, с. 94], Доказ минулого часу - Доказ минулого часу (PoeT), який використовується в проектах Гіперледжера. Основним недоліком алгоритмів є те, що вони вимагають великої обчислювальної потужності. Триває широке обговорення того, які механізми консенсусу є найкращими, і створюються нові алгоритми.

Структура даних блокчейну - це впорядкований "назад" пов'язаний список блоків транзакцій (рис. 3). Блокчейн можна зберігати в будь-якому файлі або просто в базі даних. Клієнт Bitcoin Core зберігає метадані блокчейну, використовуючи базу даних LevelDB від Google [29, с. 73].

Кожен блок у блокчейні ідентифікується хешем, який генерується за допомогою криптографічного алгоритму SHA256, застосованого до заголовка блоку. Кожен блок також посилається на попередній блок, відомий як батьківський блок, через поле "хеш попереднього блоку" в заголовку блоку. Іншими словами, кожен блок містить власний хеш батька у своєму власному заголовку.

Послідовність хешів, що пов'язують кожен блок із його батьком, утворює ланцюжок, який тягнеться до самого першого блоку, коли-небудь створеного, відомого як блок генезису. Змінений хеш батьківського блоку вимагає зміни посилання "хеш попереднього блоку" у дочірньому блоці. Цей каскадний ефект гарантує, що якщо блок має багато поколінь, його не можна змінити, не дивлячись на всі попередні блоки. Оскільки такий перерахунок вимагає величезної кількості обчислень, довгий ланцюг блоків робить глибоку історію в блокчейні незмінною, що є запорукою безпеки цифрового ресурсу. Блоки, які вже записані в блокчейні, змінити не можна.

Взагалі, будь-які зміни в інформації про блокчейни (транзакції) заборонені. Ви можете додавати лише нові блоки. Це важлива властивість блокчейну як розподіленої книги транзакцій. Блок складається із заголовка (Head), що містить метадані, а потім довгий список транзакцій (Payload), які займають більшу частину всього обсягу блоку [30, с. 67].

Заголовок блоку містить наступну інформацію: версія блоку, дата та час створення блоку, хеш заголовка блоку, хеш попереднього блоку, хеш усіх транзакцій у блоці, спеціальні параметри nonce та біти. Хеш заголовка блоку з'єднує попередній блок із наступним у ланцюжку блокчейнів. Розмір блоку становить 80 байт, тоді як середня транзакція становить щонайменше 250 байт, а середній блок містить більше 500 угод. Відповідно, блок повністю заповнений транзакціями в 1000 разів більшими за заголовок.

Метафорично, блокчейни (блокчейни) - це кінцеві універсальні комп’ютери. Після запуску вони демонструють неймовірну стабільність, роблячи їх надійними та привабливими для нового покоління децентралізованих послуг та програм [31, с. 93].

Таким чином, основними перевагами блокчейну є:

• децентралізація - у ланцюжку форуму сервера кожен учасник підтримує весь блокчейн;

• прозорість - інформація про транзакції зберігається у відкритому доступі, і ці дані не можуть бути змінені;

• надійність - для запису нових даних необхідний консенсус вузлів блокчейну, що дозволяє фільтрувати операції та реєструвати лише законні транзакції, неможливо замінити хеш;

• теоретичний необмежений - теоретично блокчейн може доповнюватися записами необмежено довго.

Складність практичного впровадження технології блокчейну в бізнес полягає в тому, що вона передбачає зміну парадигми управління та перехід від ієрархічної моделі до плоскої. При цьому рішення приймаються децентралізовано, а весь процес є прозорим для всіх учасників. Очевидно, що це вимагає переосмислення бізнес-процесів, підходів до управління та захисту інформації. Бізнес-блокчейни - це нові технологічні рівні, які перекривають Інтернет і завантажують старі конструктивні рішення та централізовані бізнес-послуги [31, с. 83].

В основному блокчейн вводить довіру в мережу, вилучаючи посередників із виконання цієї функції та творчо порушуючи старі технології. Криптотехнологічна економіка повинна стати економікою, заснованою на децентралізованій довірі [4, с. 87].

Багато галузей децентралізовані надзвичайно неефективно: кожна компанія має власну інфраструктуру, за допомогою якої користувачі взаємодіють, проводять транзакції та обмінюються даними, і яка вимагає координації з іншими компаніями при кожній взаємодії. З появою децентралізованих баз даних, які можуть технологічно відтворювати мережевий ефект, доступний раніше лише для монополій, кожен може приєднатися до них і діяти для свого блага, не створюючи монополії з усіма її негативними сторонами. Ось чому технології блокчейну так затребувані у фінансах, галузі постачання та системах ідентифікації.

Всі вони використовують децентралізовані бази даних, реалізуючи свої цілі на одній платформі, без витрат на переговори про те, хто візьме під контроль цю платформу, а потім миряться з тим, що вони намагатимуться зловживати своїм монопольним становищем. Поширення блокчейну

відбувається поступово, починаючи з розробників стартапів у великих компаніях різних галузей економіки, які виявили величезний потенціал блокчейну. Яскравим прикладом реструктуризації великого бізнесу для нової парадигми є банківський консорціум R3CEV (асоціація понад 70 найбільших фінансових компаній та банків у світі), який був створений для розробки та застосування технологій блокчейн у фінансовому секторі. Окрім R3CEV, існує кілька десятків консорціумів блокчейнів, і постійно з'являються нові асоціації. З 2016 року кількість нових проектів, створених із використанням технології блокчейн, феноменально зросла.

Одним із прикладів українського розвитку є блокчейн-проект електронних аукціонів з оренди та продажу державного майна e-Auction 3.0 [32, с. п'ять].

Послуга була протестована в ряді міст України та отримала підтримку від окремих адміністрацій. ДП "Сетамі" 7 вересня 2017 року провело перший у світі аукціон із використанням технології блокчейн. Для реалізації блокчейну була обрана платформа EXONUM міжнародної компанії BitFury Group. З вересня 2017 року по лютий 2018 року за допомогою блокчейну було проведено 24 202 аукціони, у тому числі 4471 успішний.

Загальна сума продажів склала 692 млн грн. Нові бізнес-моделі блокчейну. Не існує єдиного "офіційного" блокчейну, але існують різні типи блокчейнів, які існують незалежно та взаємодіють між собою. Таким чином, у блокчейні можуть з'являтися конкретні технічні особливості використання в різних додатках. Умовно всі інноваційні бізнес-моделі можна розділити на 4 типи: «розумні» контракти, підприємства з відкритою мережею, автономні агенти, розподілені автоматичні підприємства [33, с. 81].

Вони відрізняються ступенем автоматизації та складністю функціональних можливостей моделі. Автоматизація відображає ступінь необхідності участі людини: низька - необхідна участь людини, висока - модель працює без людей. Складність вказує на кількість функцій у моделі: низька - одна функція, висока - різноманітність функцій.

Розумні контракти - це основна форма компанії, що базується на блокчейні. Це спеціальний код, який містить набір інструкцій для блокчейну. Звичайний контракт - це угода між сторонами угоди, записана на папері. Переговори про умови угоди, врегулювання суперечок, якщо є розбіжності, вимагає зусиль. Розумні контракти усувають усі підготовчі кроки до підписання контракту та виконання його умов. Ведення бізнесу спрощується.

Підприємства з відкритою мережею є об'єднанням «розумних» контрактів, наступним кроком до збільшення складності їх функціональних можливостей. Компанії стають частиною мережі. Як результат, зменшуються витрати на координацію діяльності, і постачальники та партнери з'являються, що раніше було неможливо. Автономний агент - це пристрій або програма, яка збирає інформацію та може робити самостійний вибір.

Можливість визначити спосіб досягнення мети відрізняє агента від звичайного застосування. Агент реагує на зміни в навколишньому середовищі. Ця категорія включає цікаві програми, які можуть здійснювати транзакції, купувати ресурси, здійснювати платежі, тобто створювати цінність для користувачів як творця - агента. Прикладом автономного агента є послуга хмарних обчислень або самокерований автомобіль.

Автомобіль належить людині або групі людей, і, можливо, пересувається містом самостійно, передбачений трансфер, сажа пасажирів сама бере, бере, бере оплату. Розподілені автоматизовані підприємства - це об'єднання відкритих мережевих підприємств та автономних агентів. Система приймає рішення та функції без втручання людини - більшість щоденних процедур можна програмувати. Всі діють відповідно до процедур «розумних» контрактів [32, с. 87].

Завдання персоналу, показники ефективності його роботи стануть простими та зрозумілими. В результаті корпоративна бюрократія зменшиться, а заробітна плата керівників стане прозорою. Клієнти мають відгуки. Компанія постійно враховує їх думку, вдосконалюючи послуги та продукцію. Акціонери

отримують дивіденди частіше, ніж раз на рік, оскільки фінансовий облік компанії відбувається в режимі реального часу.

Програмні засоби для створення та обслуговування блокчейн-додатків. Blockchain базується на реальній технологічній платформі та її різних версіях. Є багато проектів, які пропонують платформи для створення блокчейн-додатків, і постійно з'являються нові. Додатки блокчейн, що будують інфраструктуру криптоекономіки, вимагають величезної кількості програмістів. В основному це розробники блокчейнів зі знанням основних мов програмування: C ++, Golang, Scala, Java та Python. Останнім часом особлива увага приділяється мові Solidity, яка використовується для написання розумних контрактів для мережі Ethereum. Ефіріум (Ethereum) - конструктор для створення рішень на блокчейні [17, с. 98].

Дозволяє створювати будь-які програми з верифікацією блокчейну. Основною ідеєю Ethereum є використання розумних контрактів - записів, що містять умови для виконання певних дій. Будь-яка дія, наприклад, передача товару замовнику, може стати умовою. Розробник, що використовує блокчейн Ethereum, може програмувати необхідні тригери та дії, використовуючи вбудовану мову сценаріїв.

У той же час кожен запис може бути перевірений усіма зацікавленими сторонами: реєстр даних залишається відкритим та децентралізованим. Завдяки високій гнучкості смарт-контрактів, Ethereum став однією з найпопулярніших платформ для створення нових блокчейн-проектів з використанням мови Solidity. Розробникам більше не потрібно придумувати власну реалізацію блокчейну: досить створити бажаний надбудову над існуючою системою.

На сьогоднішній день однією з найпопулярніших відкритих платформ для створення блокчейн-проектів є Hyperledger від Linux Foundation, Intel, IBM та інших (понад 100 великих фірм). Платформа пропонує набір інструментів для розробки: Fabric, Iroha, Sawtooth lake, blockchain explorer, Fabric chaintool (Caliper, Cello, Composer, Quilt), Fabric SDK Py, Corda. Сьогодні одним з найпопулярніших інструментів є Hyperledger Fabric, блокчейн-фреймворк, який призначений створити основу для розробки блокчейн-рішень і базується на

модульній архітектурі. Fabric - це модуль для розробки масштабованих додатків блокчейну з гнучким рівнем дозволу, до якого при необхідності можуть бути приєднані різні компоненти, наприклад, консенсусні алгоритми [18, с. 98].

Основна вимога Hyperledger - це модульна конструкція. Потрібно підключати та відтворювати різні послуги; користувачі повинні мати можливість легко видалити та додати модуль відповідно до особливостей свого бізнесу. Консорціум R3CEV підтримує створення та тестування платформи блокчейну Corda. Corda - це блокчейн-платформа для банківського сектору. Проект NEM, створений великою командою розробників з Японії, дуже схожий на Ethereum і є платформою для розвитку різних блокчейнових проектів.

Однак, на відміну від Ethereum, цей проект зосереджений на швидкості обробки транзакцій: підтвердження дії в системі займає секунди. Проект Арагон реалізує концепцію децентралізованих організацій, які існують виключно в рамках блокчейну: відсутність паперів та бюрократичних процедур, лише цифрові дані.

Альфа-версія програмного забезпечення вже доступна на веб-сайті Арагону, який успішно справляється із завданнями, що виникають при створенні стартапів та інших приватних онлайн-проектів. Sia - це децентралізований хмарний проект зберігання даних. На відміну від традиційних сервісів, таких як Google Drive або Amazon S3, які зберігають дані користувачів на власних серверах, Sia пропонує механізм розповсюдження зашифрованої інформації на багатьох незалежних комп’ютерах [35, с. 76].

Перевага Sia перед традиційними хмарними сервісами полягає у вартості передплати: вартість зберігання файлів у децентралізованому сховищі в 10-15 разів нижча, ніж у традиційного хостингу файлів. Крім того, зашифровані файли не можна розголошувати на запит поліції та інших державних установ. Ще одним проектом, майже ідентичним Sia, є розподілене сховище Storj. Захист додатків блокчейн. Технологія блокчейн побудована з нуля, щоб бути безпечною на рівні бази даних. Безпека в технології блокчейн забезпечується за

допомогою децентралізованого сервера, часових та однорангових мережевих з'єднань.

В результаті формується база даних, вона керується автономно, без єдиного центру. Це робить блокчейни дуже корисними для реєстрації подій та операцій з даними, управління ідентифікацією та перевірки походження. Блокчейн - це механізм, який забезпечує високий ступінь обліку та ідентифікації. Більше не буде пропущених транзакцій, людських або машинних помилок або навіть змін, зроблених без згоди залучених сторін. Блокчейн гарантує легітимність транзакції, записуючи її не лише в головній книзі, але і в розподіленій системі книг, пов’язаних через захищений механізм перевірки. Через сам принцип мережі зробити підробку блоку неймовірно складно.

Щоб блок вважався реальним, 51% усіх існуючих вузлів повинен з ним погодитися. Тож існує загроза «51% атаки» - якщо 51% обчислювальної потужності в мережі блокчейн належить одному пристрою, то цілісність буде порушена. Блокове шифрування гарантує, що користувачі можуть використовувати лише ті частини блокчейну, для яких у них є приватні ключі, без яких неможливо змінити зчитування запису. Шифрування забезпечує синхронізацію копій розподіленого блокчейну для всіх користувачів.

Кожен учасник мережі повинен використовувати шифрування. Заходи безпеки вбудовані в мережу. Вони забезпечують конфіденційність та достовірність. Замість того, щоб контактувати з третіми сторонами, вузли мережі блокчейнів використовують спеціальний консенсус-протокол для узгодження вмісту книги, а також криптографічні хешування та алгоритми цифрового підпису для забезпечення цілісності транзакції та передачі її параметрів.

Механізм консенсусу гарантує, що розподілені книги є точними копіями, зменшуючи ризик шахрайських транзакцій, оскільки втручання ззовні може відбуватися в багатьох місцях одночасно. Криптографічні алгоритми хешування, такі як алгоритм обчислення SHA256, гарантують, що будь-яка зміна вхідних даних транзакції, навіть найменша, призведе до різного хеш-

значення в результатах обчислення, що вказує на те, що вхідні дані транзакції можуть бути скомпрометовані. Цифрові підписи гарантують, що транзакції здійснюються законними відправниками (підписаними приватними ключами), а не зловмисниками. Сучасні платформи розробки, такі як Hyperledger, забезпечують широкий спектр криптографічних протоколів та алгоритмів.

Також пропонується гнучка модель PKI (інфраструктура відкритих ключів), яка може використовуватися для управління функціями контролю доступу [35, с. 51].

Таким чином, сила та тип криптографічних механізмів будуть відрізнятися залежно від потреб користувачів. В даний час існує вже низка бізнес-сервісів блокчейну, які надають:

• безпечне адміністрування мереж, запобігання хакерським атакам і усуває проблему "єдиного адміністратора";

• зберігання цифрових сертифікатів, що робить доступ користувачів до сайтів повністю безпечним (зокрема, за винятком перехоплення паролів)

• забезпечити двосторонні угоди без залучення третьої сторони, що гарантує (юридична фірма, нотаріус, банк тощо)

• фіксація часу розміщення документів, дозволяє вирішити питання патентування, авторських прав тощо;

• підтвердження справжності товару (товару) за допомогою надійно захищеного сертифіката;

• підтвердження прав на будь-яке майно;

• створення публічних електронних реєстрів, інформація про які автоматично оновлюється навіть після "розповсюдження" на Інтернет-ресурсах;

• Система DNS невразлива до DDOS-атак [36, с. 87].

Як приклад ми наведемо BAASIS ID та Civic - платформи управління ідентифікацією на основі блокчейну, послуги яких спрямовані на вирішення проблеми крадіжки особистої інформації клієнтів. Послуга дозволяє користувачам реєструватися, перевіряти особисту інформацію та захищати свою кредитну історію від шахраїв.

UniquID Wallet забезпечує безпечне рішення для управління ідентифікацією, інтегроване зі сканерами відбитків пальців та іншими біометричними персональними пристроями. Ви можете працювати з додатком UniquID Wallet на нестандартних пристроях, серверах, персональних комп'ютерах або смартфонах, планшетах та інших пристроях з обмеженим часом роботи без підзарядки.

Серед заявлених можливостей можна виділити індивідуальне сховище блокчейнів для інформації про використовувані «пристрої» без паролів, які замінені алгоритмами розпізнавання користувача особистими об'єктами, підключеними до системи. Це забезпечує максимально можливий рівень цілісності та сумісності в будь-якій інфраструктурі. Ідентифікатор поєднує всі профілі персональної мережі та персональні дані в єдиний інструмент ідентифікації. Блокчейн може записувати дати народження людей, відбитки пальців, зберігати інформацію про дипломи, паспорти, водійські права. Надалі це може допомогти у боротьбі з усіма видами шахрайства [37, с. 98].

Проблеми розробки блокчейн-додатків. Впровадженню технології блокчейну заважає багато факторів. Перелічимо основні з них. Інертність учасників ринку та необхідність досягнення консенсусу між великою кількістю учасників, відсутність законодавчої бази суттєво заважає розвитку ринку. Відсутність законодавчої бази призводить до невизначеності багатьох питань. Щоб технологія здобула авторитет, вона повинна відповідати стандартам (наприклад, уряду).

Ні стандартів, ні відповідності. На технологічному форумі керівний орган і невідомо, хто визначатиме шлях його розвитку. Складність існуючих прототипів блокчейн-рішень для розуміння споживача масового бізнесу.

Сьогодні бізнес, який зацікавлений у практичному застосуванні технологій, задається питанням, які капіталовкладення потрібні для реалізації блокчейн-проекту в корпоративному секторі. У цьому випадку однозначної відповіді немає. Порядок чисел сильно залежить від програми; складність бізнес-логіки, яку потрібно створити для конкретного проекту; кількість

зв'язків зі сторонніми послугами; використана інфраструктура зберігання ключів; кількість ролей та користувачів у системі тощо.

Компанії також знадобиться штатний спеціаліст з безпеки, який керуватиме проектом, навіть якщо спеціалізований розробник блокчейну береться за всю конструкцію системи. У середньому вартість побудови бухгалтерської системи на підприємстві може оцінюватися в десятки і сотні тисяч доларів. Однією з головних проблем є “масштабованість”.

На даний момент усі блокчейнові протоколи побудовані таким чином, що кожен комп'ютер у мережі повинен обробляти кожну транзакцію - ця властивість забезпечує максимальну стійкість до відмов і безпеку ціною того, що обчислювальна потужність мережі насправді обмежена обчислювальними можливостями один комп’ютер. Необхідно подолати ці обмеження і досягти рівня, достатнього для його масового розподілу [38, с. 76].

Існує також проблема інтеграції нових та існуючих приватних систем з відкритим блокчейном.

Одним із рішень цієї проблеми є створення служби автентифікації на основі блокчейну для реалізації глобального рівня безпеки. Така послуга може стати стандартною інфраструктурою безпеки для нових моделей змішаних приватних та державних систем, що принесе користь усім зацікавленим сторонам у різних секторах економіки. Прикладом такого підходу є блокчейн Hydro Raindrop).

2.2 Архітектура та принцип побудови роботи технології блокчейн

Технологія блокчейн стала справді винахідливим творінням розуму людини або групи людей, які працювали під псевдонімом Сатоші Накамото. З часу винаходу та формулювання принципів роботи мережі ця технологія зазнала значних змін та популярності у світі. Що нового принесла ця технологія?

Можливість розповсюдження інформації по мережі без її копіювання між учасниками мережі - ось як Blockchain створив нову основу для нового типу

глобального Інтернету. Оригінальна розробка технології була спрямована на винайдення нового слова в галузі цифрових валют - таких криптовалют, як Біткойн (російський (буквально) Цифровий біткойн), ETH (Ефіріум) та ін. Але з часом спеціалісти в галузі техніки почали винайти нові варіанти та потенціал цього методу.

Blockchain - це незнищенний цифровий кластер для запису змін у мережі; він може бути запрограмований не тільки для запису фінансових операцій, але й будь-яких інших існуючих цінностей - будь-якої інформації у світі. (Дон та Алекс Тапскотт, автори "Blockchain Revolution" ("Blockchain Revolution", 2016)) [39, с. 87].

Технологія блокчейн заснована на роботі всіх механізмів, заснованих на використанні таких технологій і методів роботи та шифрування даних:

• Асиметричні алгоритми шифрування або "асиметричні криптосистеми" (пари "приватних" і "відкритих" ключів)

• Хеш-функції або "хеші" даних (функції MD і SHA)

• Хеш-таблиці для запису хеш-результатів - операції в блоках транзакцій (з використанням хеш-дерева типу "дерево Мерклі")

• Розумні контракти (англ. Smart Contracts) - метод передачі даних (цифрових значень) від однієї особи до іншої;

• Токени та реалізація механізму доказу концепції (POC) - доказ концепції як методу перевірки події (затвердження угоди) в системі. Давайте визначимо поняття кожного із зазначених термінів зі списку [39, с. 54].

Асиметричні криптосистеми - це ефективні системи захисту криптографічних даних, які також називаються криптосистемами з відкритим ключем. У таких системах один ключ використовується для шифрування даних, а інший - для дешифрування (звідси і назва - асиметричний). Перший ключ є загальнодоступним і може бути опублікований для використання всіма користувачами системи, зашифрувавши дані.

Розшифрувати дані за допомогою відкритого ключа неможливо. Для розшифровки даних одержувач зашифрованої інформації використовує другий

ключ, який є секретним (приватним). Ключ розшифровки не можна визначити за ключем шифрування.

Щоб гарантувати надійний захист інформації, системи відкритих ключів (SPK) повинні відповідати двом очевидним і важливим правилам:

1. Трансформація оригінального тексту повинна бути незворотною і виключати можливість відтворення зашифрованої інформації за допомогою відкритого ключа;

2. Визначення приватного ключа на основі відкритого ключа повинно бути неможливим з урахуванням сучасних досягнень та можливостей обчислювальної техніки [40, с. 54].

У той же час точна оцінка складності (кількості операцій та часу) для розбивання шифру є обов’язковою. Ідея криптографії відкритого ключа тісно пов'язана з ідеєю односторонніх функцій, або таких функцій f (x), що, знаючи значення аргументу "x", досить легко знайти значення функція, тоді як визначення аргументу з функції є досить складним у сенсі теорії. Отже, насправді, щоб знайти аргумент із функції, користувач повинен мати додатковий спосіб полегшити декодування та мати спосіб легкого відтворення вихідного значення. Таким чином, ключ користувача діє, а в цьому прикладі діє як значення функції, так що f (x) = y, де 'y' є закритим ключем у системі SPK.

Загалом усі сучасні криптосистеми з відкритим ключем використовують один із таких типів незворотних перетворень:

1. Розбиття великих чисел на прості множники;

2. Розрахунок логарифмічної функції в скінченному просторі; 3. Обчислення коренів алгебраїчних рівнянь.

Також, говорячи про практичну цінність SPK, слід зазначити можливі застосування таких алгоритмів:

1. Як самостійний засіб захисту передачі та зберігання даних;

2. Як засіб для розподілу ключів. Алгоритми SPK досить складні в порівнянні з іншими традиційними криптосистемами, і на практиці, використовуючи SPK, зручно розподіляти ключі, обсяг інформації яких

незначний. А потім, використовуючи хмарні технології, обмінюйтесь великими потоками інформації.

3. Як засіб аутентифікації користувачів. Системи відкритих ключів можуть використовувати широкий спектр методів шифрування [38, с. 90].

Одними з найпопулярніших криптосистем є криптосистеми RSA, El-Gamal або Diffie-Gellman та криптосистеми, засновані на еліптичних рівняннях. Насправді вибір алгоритму визначає лише метод і складність шифрування ключів, а не принципову різницю між способом передачі інформаційних потоків. Цифровий підпис або електронний підпис.

Щоб перевірити, чи повідомлення чи інформація дійсно належить тому чи іншому учаснику мережі, повідомленням слід призначити так звані цифрові підписи.

Жоден учасник мережі, крім користувача А (відправник), не може визначити формат підпису для кожного конкретного повідомлення. Ніхто, включаючи самого користувача, не може змінити зміст повідомлення, щоб підпис залишався незмінним. Хоча одержувач повідомлення повинен мати можливість перевірити підпис на належність відправника. Для перевірки дійсності цифрового підпису користувач В (одержувач) повинен надати сторонній С інформацію (мережу або сервер перевірки підпису) інформацію про те, які дані були використані для перевірки підпису. Якщо повідомлення передається безпосередньо від відправника адресату, за винятком третьої сторони, то в даному випадку мова йде про «оригінальний цифровий підпис» [39, с. 51].

Кілька недоліків вищевказаної моделі:

● Мережа передбачає присутність третьої сторони - клієнта, якому однаково довіряють як відправник, так і одержувач;

● Відправник, одержувач та клієнт підтвердження повинні обмінятися значним обсягом службової інформації перед передачею самого повідомлення;

● Передача такої інформації повинна бути закрита, її використання в цьому випадку неефективне.

Тим не менше, навіть така схема цифрового підпису успішно використовується в цифрових системах, де потрібно дотримуватися двох простих правил: необхідність автентифікації / ідентифікації інформації та обов'язкове шифрування переданих у мережі.

РОЗДІЛ 3. РОЗРОБЛЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ЦІЛІСНОСТІ ЕЛЕКТРОННИХ ДОКУМЕНТІВ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН

3.1 Постановка завдання

Необхідно розробити універсальну електронну систему документообігу, яка полегшить та пришвидшить роботу з документами.

Система електронного документообігу повинна відповідати таким вимогам:

1) диференціація прав доступу користувачів повинна бути реалізована в системі, необхідно реалізувати дві ролі: адміністратора та користувача;

2) доступ до системи повинні мати лише користувачі, зареєстровані системним адміністратором;

3) необхідно забезпечити міжплатформене застосування;

4) заявка не повинна бути орієнтована на конкретну спеціалізацію підприємства; необхідно передбачити можливість адміністратора налаштовувати систему під конкретну організацію;

5) адміністратор повинен мати можливість використовувати такі функції: додавання / видалення / редагування користувачів, додавання / видалення / редагування груп, додавання / видалення каталогів, видалення файлів;

6) метадані повинні зберігатися для кожного документа;

7) користувачі повинні мати такі можливості для роботи з файлами: додавати / видаляти файл, встановлювати термін зберігання файлу в системі, писати коментар до файлу, надсилати повідомлення користувачам електронною поштою;

8) конструкція системи повинна бути ненав’язливою;

9) система повинна бути простою у використанні, мати інтуїтивно зрозумілий інтерфейс.

3.2. Функціональний опис системи

Модель користувача - уявлення про те, які функції буде виконувати система, як вона буде взаємодіяти з користувачем. Це погляд на систему з точки зору користувача. Відповідно до технології Microsoft Solution Framework, процес проектування починається з методологічного аналізу потенційних користувачів, за допомогою якого визначаються різні типи користувачів системи та їх робочі функції.

Потім формується набір випадків використання, кожен з яких розбивається на послідовність конкретних дій, які називаються випадками використання.

Веб-додаток "BlockDoc" передбачає два типи користувачів системи електронного документообігу:

1) користувач - кожен працівник підприємства;

2) адміністратор - обирається особа, наділена особливими повноваженнями (правами) в системі [40, с. 6].

Наступні функції є спільними для обох типів користувачів: Авторизація користувача: після введення правильного логіна та пароля користувач має авторизацію в системі і може виконувати певні дії відповідно до своїх прав у системі. Електронна пошта вважається іменем користувача, оскільки вона зручна у використанні та не бентежить користувача. Перегляд інформації про файл: користувач може переглянути наступну інформацію про файл - його ім'я, дату створення, який користувач його створив, його розмір, термін зберігання.

Видалити файл: під час перегляду файлу користувач має можливість його видалити. Усі попередні версії файлу видаляються разом із файлом. Видалити файл може лише його власник або адміністратор. Завантаження файлу: користувач може завантажити файл, доступний для перегляду. Для цього він повинен вибрати місце (папку) для завантаження файлу.

Перегляд доступу до файлу: Адміністратор та користувачі, які мають доступ до файлу, можуть переглядати списки користувачів та груп, для яких

файл доступний. Перегляд завдань для файлу: коли вибрано конкретний файл, користувач може переглянути всі завдання, пов’язані з цим файлом (текст завдання, хто його додав, виконавець, відмітка про виконання завдання). Завантажити версію файлу: користувач може завантажити версію файлу, яка йому доступна для перегляду, вибравши місце для збереження. Версії файлу можуть бути видалені адміністратором або будь-яким користувачем системи, який має права доступу до файлу із зазначеними версіями [41, с. 76].

Перегляд користувачів певної групи: Користувач може переглядати списки користувачів, що належать до поточної групи. Перегляд списку користувачів: ви можете побачити список усіх користувачів системи з їх повним ім'ям, назвою та адресою електронної пошти.

Переглянути список груп: користувач може переглянути список груп, які існують у системі. Для користувачів, уповноважених на роль адміністратора, надаються такі сценарії використання: Додати користувача Адміністратор може додати користувача, ввести його прізвище, ім’я, по батькові, посаду, адресу електронної пошти, логін та пароль. Видалити користувача Адміністратор може позначити, що користувача видалено.

У цьому випадку користувач не відображається у списках. Відновити користувача Адміністратор може відновити користувача, раніше зареєстрованого в системі. Для редагування інформації про користувача адміністратор може змінити таку інформацію про користувача - ім'я, посаду, адресу електронної пошти, логін та пароль. Перегляд груп користувачів Адміністратор може переглядати групи користувачів. Додати завдання: адміністратор може додати нове завдання, яке буде використовуватися, коли користувачі визначають завдання до файлу для виконання іншими користувачами.

Видалення завдань: адміністратор може видалити завдання зі списку запланованих завдань через те, що воно втратило свою актуальність. У цьому випадку це завдання зберігатиметься лише для файлів, збережених у системі. Перегляд списку завдань Адміністратор може переглянути список доданих ним

завдань, який буде використаний пізніше, коли користувачі створюватимуть завдання для файлу.

Створення групи Адміністратор має можливість створити групу користувачів, вказавши її назву. Видалення групи Адміністратор має можливість видалити групу. Щоб додати користувача до групи, адміністратор може додати до групи користувачів, зареєстрованих у системі. Видалення користувача з групи Адміністратор може видалити користувача з певної групи. Для користувачів, уповноважених постійними працівниками установи, випадки використання, крім адміністратора, такі:

Додати файл: щоб додати файл, користувач повинен ввести ім’я, коментар, період зберігання та вибрати файл для завантаження. Дата додавання, розмір файлу, поля власника генеруються автоматично. За замовчуванням файл доступний для всіх користувачів системи [42, с. 87].

Перегляд доданих файлів: користувач може переглянути файли, які він додав, і відобразиться табличний список із зазначенням імені, дати додавання, розміру, коментарів та періоду зберігання кожного файлу з можливістю перегляду інформації про них. Призначення завдання файлу: користувач може встановлювати завдання файлу, вибираючи тип завдання та виконавця. Поля користувача, який додав завдання, порядок виконання та статус виконання завдання автоматично генеруються системою. За замовчуванням завдання вважається невиконаним.

Редагувати доступ до файлу: для кожного доданого файлу користувач може змінювати списки доступу до файлів за групами та користувачами, вибираючи зі списку ті групи та користувачів, які бачитимуть файл. За замовчуванням файл доступний для всіх користувачів системи.

Перегляд завдань користувача: відображає всі файлові завдання для цього користувача. Для кожного завдання ви можете бачити таку інформацію: текст завдання, до якого файлу воно було додано, ким воно було додано, та відмітку про виконання завдання.

Переглянути додані завдання: відображає всі завдання для файлів, які користувач призначив іншим. Для кожного завдання ви можете бачити таку інформацію: текст завдання, до якого файл він був доданий, виконавець та відмітка про виконання завдання.

Позначення завершення завдання: користувач, який додав завдання у файл, або той, хто отримав завдання, має можливість позначити завершення завдання в кінці виконаної роботи. У разі позитивної оцінки («завдання виконано») користувач, який призначив поточне завдання, отримує повідомлення електронною поштою про те, що завдання виконано, а піктограма завершення завдання також відображається у списку його завдань для виконання .

Для опису предметної області з урахуванням особливостей подання даних у розробленій системі створено такі основні сутності:

1) користувач;

2) груповий;

3) документ;

4) завдання на документ;

5) категорія документа.

В результаті аналізу архітектури було визначено такі групи завдань (послуг), які необхідні для реалізації всіх функцій, описаних у спеціальній архітектурі:

1) послуга для роботи з базою даних;

2) послуга для роботи з користувачами та групами;

3) сервіс для роботи з файлами та категоріями;

4) послуга для роботи із завданнями [43, с. 98].

Для спрощення взаємодії системних компонентів були створені окремі служби для окремих частин функціоналу. Послуга по роботі з базою даних містить основні функції:

1) створює стійке з'єднання з базою даних;

2) створення таблиць в базі даних - створює таблиці в базі даних, додає до таблиці необхідні вихідні дані (створює адміністратора та кореневий каталог).

Сервіс для роботи з користувачами та групами містить реалізацію наступних функцій:

1) автентифікація користувачів та адміністраторів - перевіряє, чи є в базі даних користувач або адміністратор за введеними іменем користувача та паролем; якщо такий користувач або адміністратор є, надайте їм доступ до системи;

2) отримати інформацію про користувача;

3) отримати список користувачів - для відображення всіх користувачів системи;

4) отримати список груп - для відображення інформації про групи користувачів системи;

5) отримати список груп, якими є користувач;

6) отримати список користувачів групи;

7) додавання / редагування / видалення користувача - функції доступні лише системному адміністратору;

8) відновити користувача - користувач, видалений із системи, може бути відновлений адміністратором;

9) додавання / видалення групи - функції доступні лише системному адміністратору;

10) додати / видалити користувача до / з групи - функції, доступні лише системному адміністратору [44, с. 77].

Окрім основних функцій, служба містить такі сервісні функції:

1) перевірка логіну на відповідність адресі електронної пошти - це дозволяє надсилати повідомлення користувачеві електронною поштою;

2) перевірка наявності логіна - це дозволяє наявність унікального ідентифікатора користувача системи;

3) перевірка існування групи за введеною назвою - дозволяє забезпечити унікальність назви групи;

4) отримання різних атрибутів сутностей.

Послуга по роботі з файлами та каталогами містить такі основні функції:

1) додавання / видалення каталогу - доступний лише адміністратору;

2) відображати вміст каталогу - служить для відображення каталогів і файлів, розташованих у вибраному каталозі, до яких користувач має доступ;

3) усі файли системи доступні адміністратору;

4) додати файл - введення даних, що описують файл, і завантаження файлу в файлову систему сервера;

5) видалити файл - функція доступна адміністратору та користувачеві, який додав файл; файл видаляється з бази даних та з файлової системи; разом із файлом видаляються всі версії файлу;

6) отримати інформацію про файл - необхідно відобразити опис файлу та користувача, який додав цей файл;

7) дозволити / заборонити доступ усіх користувачів до файлу - доступно лише автору файлу;

8) дозволити / заборонити груповий доступ до файлу - доступно лише автору файлу;

9) дозволити / заборонити доступ користувача до файлу - доступно лише автору файлу;

10) отримати списки груп та користувачів, які мають доступ до файлу - доступні системному адміністратору та автору файлу;

11) додати / видалити версію файлу - доступна адміністратору та особам, які мають доступ до файлу;

12) видалити всі версії файлу - всі версії вибраного файлу видаляються, сам файл не видаляється;

13) видалити всі версії файлу, крім однієї - це необхідно у тому випадку, коли потрібно залишити лише одну версію файлу (наприклад, останню, остаточну), а всі інші видалити; сам файл не видаляється;

14) отримати версії файлів - для відображення інформації про версію вибраного файлу [44, с. 76].

Окрім основних функцій, служба містить такі сервісні функції:

1) перевірка наявності імені каталогу - дозволяє зберегти унікальність назв каталогів, розташованих на одному рівні;

2) отримання шляху до файлу у файловій системі - це необхідно для завантаження, видалення файлу, додавання версій до файлу;

3) отримати поточну кількість версій файлів;

4) отримати загальну кількість версій файлів;

5) отримати шлях до версії файлу у файловій системі - це потрібно для завантаження, видалення версій.

Послуга по роботі з завданнями містить такі функції:

1) додавати / видаляти завдання для роботи з файлами - завдання, які будуть додані до файлів, доступні лише системному адміністратору;

2) відображення завдань для роботи з файлами - для вибору завдання для файлу або для перегляду завдань адміністратором;

3) додавання / видалення завдань у файл - коли завдання додається до файлу, повідомлення надсилаються адресату електронною поштою;

4) отримати завдання для файлу - відобразити список усіх завдань для цього файлу;

5) отримати завдання, адресоване користувачеві - користувач системи може переглянути завдання, адресовані йому,

6) отримати завдання, додані користувачем - користувач системи може переглядати інформацію про завдання, які він додав сам;

7) перевірити, чи виконано завдання;

8) повідомити про виконання / невиконання завдання - адресат або автор файлу може підтвердити виконання завдання або повторно призначити завдання повторним відправленням повідомлення на пошту [42, с. 89].

Послуга по роботі з блокчейном містить такі функції:

1) додати запис до блокчейну;

2) переглянути один / кілька записів;

3) створити підпис на документі;

4) перевірити документ / підпис.

При виборі технології розробки системи враховувались такі вимоги: Система повинна бути міжплатформною. Щоб задовольнити цю вимогу, ви повинні використовувати відповідну мову програмування. Ця система була розроблена з використанням мови C # на платформі .Net Core.

Система повинна бути реалізована як веб-додаток. Це забезпечує наступні переваги:

1) реалізація моделі клієнт-сервер дозволяє концентрувати та централізувати інформацію;

2) веб-програми не потребують ручного процесу встановлення, вони запускаються та встановлюються автоматично;

3) користувачам для роботи потрібен лише браузер; можливість віддаленої роботи в мережі. На основі цієї вимоги було обрано технологію ASP.NET Core. як шаблон дизайну була використана модель MVC (Model View Controller). При розробці системи в якості моделі використовувались сутності та служби, описані на етапі логічного проектування. Функції, описані в сервісах, були реалізовані за допомогою запитів до бази даних мовою sql та викликів до файлової системи, вони також містять реалізацію необхідних алгоритмів.

Для реалізації подань використовується технологія Razor - вона дозволяє поєднувати мову розмітки HTML для веб-сторінки з фрагментами коду C #. Коли клієнт робить запит на веб-сторінку, веб-сервер перенаправляє цей запит на відповідний контролер, який викликає служби, що виконують певну ділову логіку, залежно від дій корішувача, після чого контролер генерує відповідь, яка надсилається на клієнт. Були розроблені сторінки CSHTML, кожна з яких відповідає за певну функціональність системи, яка доступна за допомогою браузера.

Оскільки система забезпечує дві ролі користувачів (звичайного користувача та адміністратора) з різними можливостями, для них були створені окремі домашні сторінки. Для зручності користувачів інтерфейс розроблений з

використанням технології AJAX. AJAX - це підхід до побудови користувальницьких інтерфейсів для веб-додатків, що передбачає "фонову" комунікацію між браузером та веб-сервером. Як результат, при оновленні даних веб-сайт НЕ повністю перезавантажується, а веб-програми стають швидшими та зручнішими. Для спілкування з базою даних була використана технологія ODBC - це програмний інтерфейс, що забезпечує можливість підключення системи управління базами даних до великої кількості баз даних SQL та доступу до інших джерел табличних даних, наприклад, електронних таблиць або неструктурованих файлів [10, с. 93].

При розробці системи використовувались новітні підходи до розробки програмних систем із підтримкою масштабованості, простого оновлення та реалізації функціональних можливостей. Процес розробки системи супроводжувався створенням діаграм UML - діаграм компонентів, діаграм ER, діаграм розгортання, класів моделей доменів, випадків використання та функціональних частин.

Для взаємодії з блокчейном було обрано відкриту реалізацію платформи Ethereum, Nethereum, та мову для створення інтелектуальних контрактів, Solidity. Ethereum - це платформа для створення децентралізованих онлайн-сервісів на основі блокчейну на основі смарт-контрактів. Реалізовано як єдину децентралізовану віртуальну машину. Ethereum прагне дозволити людям легко писати децентралізовані програми, використовуючи технологію блокчейну. Децентралізована програма - це програма, яка з точки зору користувача нічим не відрізняється від звичайної програми, але має важливу властивість, оскільки як додаток вона не залежить від будь-якого централізованого посередника [11, с. 93].

Блокчейн Ethereum також можна описати як вбудований блокчейн мови програмування або як глобальну віртуальну машину на основі консенсусу. Віртуальна машина підтримує два типи облікових записів, які можуть взаємодіяти один з одним:

1) особистий рахунок захищений приватним ключем;

2) договір має власний кодекс і регулюється ним.

За замовчуванням середовище Ethereum неактивне, але кожен користувач може виконати дію, надіславши транзакцію з власного облікового запису. Якщо призначення транзакції є контрактом, воно автоматично активується і запускає свій код. Код має можливість читати / писати у власну внутрішню пам’ять (база даних, це відображення 32-байтових ключів у 32-байтові значення), зберігати отримане повідомлення та надсилати повідомлення в інші контракти, починаючи їх виконання по черзі. Після того, як виконання коду контракту зупиниться і всі підвікліки будуть повністю завершені, час виконання перестане працювати, поки його не викликає наступна транзакція.

Контракти зазвичай використовуються для чотирьох цілей:

1) сховище даних невеликого розміру, що може бути корисним при виконанні інших контрактів;

2) служать своєрідним інструментом бухгалтерського обліку зі складною політикою доступу, це також називається експедиторським договором;

3) управління поточним контрактом або відносинами між кількома користувачами. Прикладом може бути фінансовий контракт з кількома посередниками;

4) надання функцій іншим контрактам; по суті служить бібліотекою для програмного забезпечення. Контракти взаємодіють між собою через діяльність, яка називається «дзвінок» або «надсилання повідомлення» [43, с. 31].

Повідомлення - це об'єкт, що містить певну кількість ефіру (внутрішня віртуальна валюта), дані представлені масивом байтів, адресами відправника та одержувача. Коли договір отримує повідомлення, він може додатково повернути деякі дані, які оригінальний відправник може негайно використати. У цьому випадку "надсилання повідомлення" працює так само, як виклик функції. Блокчейн Ethereum (або "книга") - це децентралізована, масштабована копія бази даних, яка зберігає поточний стан усіх облікових записів.

Блокчейн використовує базу даних під назвою дерево Patricia (або «триє») для зберігання всіх облікових записів; це спеціалізований вид дерева Меркле,

який діє як сховище спільних ключів. Як і у випадку зі стандартним деревом Merkle, дерево Patricia має "кореневий хеш", який можна використовувати для посилання на все дерево, і вміст дерева не можна змінити без зміни кореневого хешу.

Для кожного облікового запису дерево зберігає 4 пакети, що містять [account_nonce, ether_balance, code_hash, storage_root], де account_nonce - це кількість транзакцій, надісланих з рахунку (збережених для запобігання повторним атакам), ether_balance - залишок на рахунку, code_hash - хеш код, якщо рахунок є контрактом, а в іншому випадку storage_root є коренем іншого дерева Патриції, що зберігає дані [11, с. 39].

Щохвилини майнер виробляє новий блок (концепція видобутку в Ефіріумі точно така ж, як і в біткойнах), і цей блок містить список транзакцій, що відбулися з моменту створення останнього блоку, і кореневий хеш дерева Патриції, представлення нового стану після застосування цих транзакцій та надання Майнеру винагороди у вигляді ефіру за створення блоку. Оскільки дерево Патриції працює, якщо внесено кілька змін, більшість частин дерева будуть точно такими ж, як і в останньому блоці; тому немає необхідності зберігати дані двічі, оскільки вузли в новому дереві просто зможуть вказувати на ту саму адресу пам'яті, яка зберігає вузли старого дерева в тих місцях, де є нове дерево і старе дерево. те саме [12, с. 92].

Для створення інтелектуальних контрактів була обрана мова Solidity - це об’єктно-орієнтована мова високого рівня. Розумні контракти - це програми, що регулюють поведінку рахунків у блокчейні Ethereum. Під впливом C ++, Python та JavaScript, Solidity орієнтована на віртуальну машину Ethereum (EVM).

Solidity підтримує статичну типізацію, успадкування, бібліотеки та складні визначені користувачем типи. За допомогою Solidity можна створювати смарт-контракти для таких цілей, як голосування, краудфандинг, сліпі аукціони та блокування гаманців.

Створюючи інтелектуальні контракти, для швидкого розвитку мови слід використовувати останню доступну версію Solidity

Приклад договору:

Цілісність: контракт SimpleStorage {uint storedData; набір функцій (uint x) {storedData = x; } Функція get () постійних повертань (uint retVal) {return storedData; }} Uint storedData оголошує змінну стану з назвою storedData типу uint (256-бітове ціле число без знака), позиція зберігання якої автоматично визначається компілятором.

Функції set і get використовуються для зміни та отримання значення змінної. Суцільність - це статично набрана мова, що означає, що тип кожної змінної (глобальної чи локальної) повинен бути вказаний (або хоча відомий із вирахування типу) під час компіляції. Суцільність забезпечує кілька основних типів, які можна об'єднати в складні типи.

Структура хеш в блокчейні зображена на рисунку 3.1:

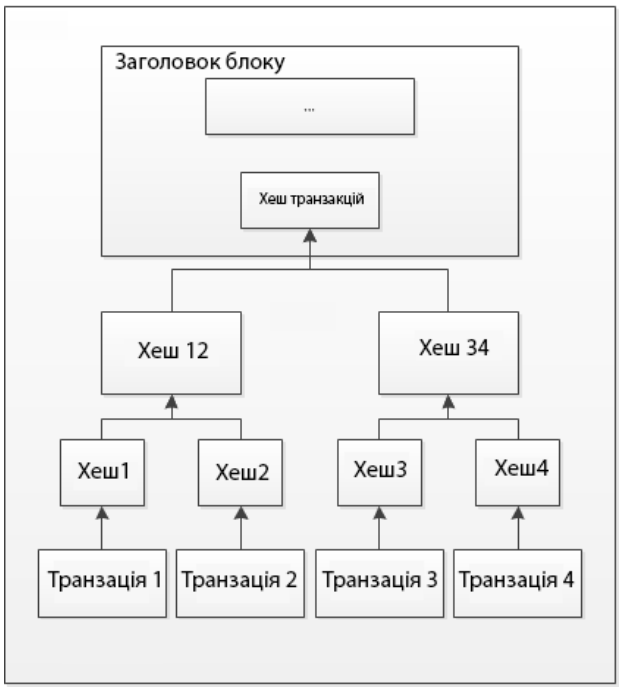


Рис.3.1.Хеш в блокчейні

Хеш - це функція, яка відповідає зашифрованим вимогам, необхідним для обчислення блокчейна.

Хеши мають фіксовану довжину, проте практично неможливо вгадати довжину хеша, якщо зловмисник намагається зламати блокчейн.

Хеш розробляється на основі інформації, що міститься в заголовку блоку. Хешування вимагає обробку даних з блоку через математичну функцію, що і призводить до висновку фіксованої довжини. Використання фіксованої довжини підвищує безпеку, так як будь-який, хто намагається зламати хеш, не зможе визначити довжину, побачивши довжину виведення.

3.3 Аналіз систем забезпечення цілістності інформації

Існує 3 основних системи забезпечення цілісності інформації – це шифрування, хешування та система електронного підпису документа.

У табл.3.1 наведено зв’язок способів забезпечення цілісності інформації можливостями корегування даних.

Таблиця 3.1

Способи забезпечення цілісності інформації

	Гарантія цілісності	Можливість редагування	Втручання та аналіз вхідних данних
Централізоване шифрування	-	+	-
Блокчейн	+	-	-
Електронний підпис	-	+	+

Централізоване шифрування.

Цей метод не може забезпечити повний захист даних від модифікації, через що нарівні з шифруванням застосовують і інші методи забезпечення цілісності даних. При передачі зашифрованих даних може виникнути ситуація, при якій можуть бути видалені деякі біти інформації, змінено порядок їх слідування або зловмисниками додані нові біти даних. Щоб уникнути цього, в криптографії застосовується метод имитовставки, коли до шифрованих даними додається певна кількість надлишкової інформації. Це дозволяє знизити можливість розшифрування даних зловмисниками.

Блокчейн.

Даний метод мається на увазі перетворення даних із застосуванням хеш-функції або певного алгоритму в рядок певної довжини. Особливістю хешування є зміна всього рядка, в разі навіть мінімального зміни вхідних даних.

Електронний підпис.

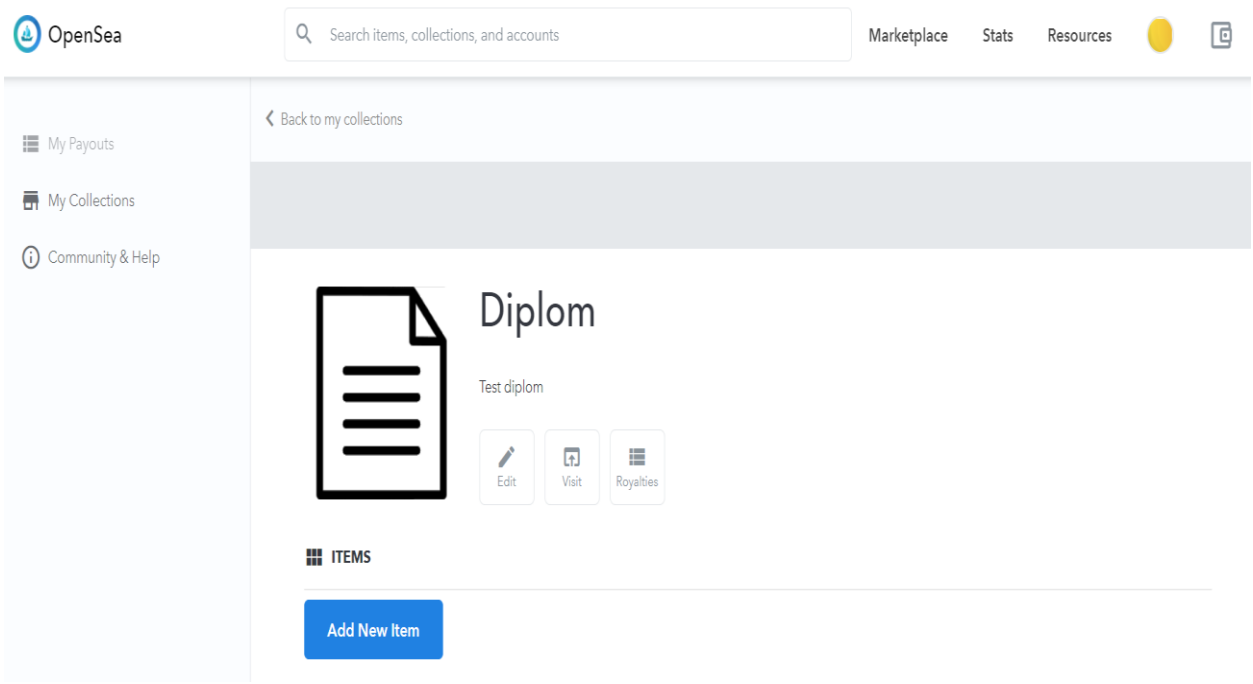
У загальному сенсі електронний підпис відносять до реквізитів електронних документів, при цьому вона забезпечує юридичну значимість документа і його цілісність за рахунок застосування криптографічного перетворення. Щоб підписати документ електронним підписом, необхідно використовувати закритий ключ, який зберігається у власника електронного підпису. При цьому електронний підпис дозволяє перевірити дані на наявність можливих несанкціонованих змін, а також авторство документа і неспростовності.

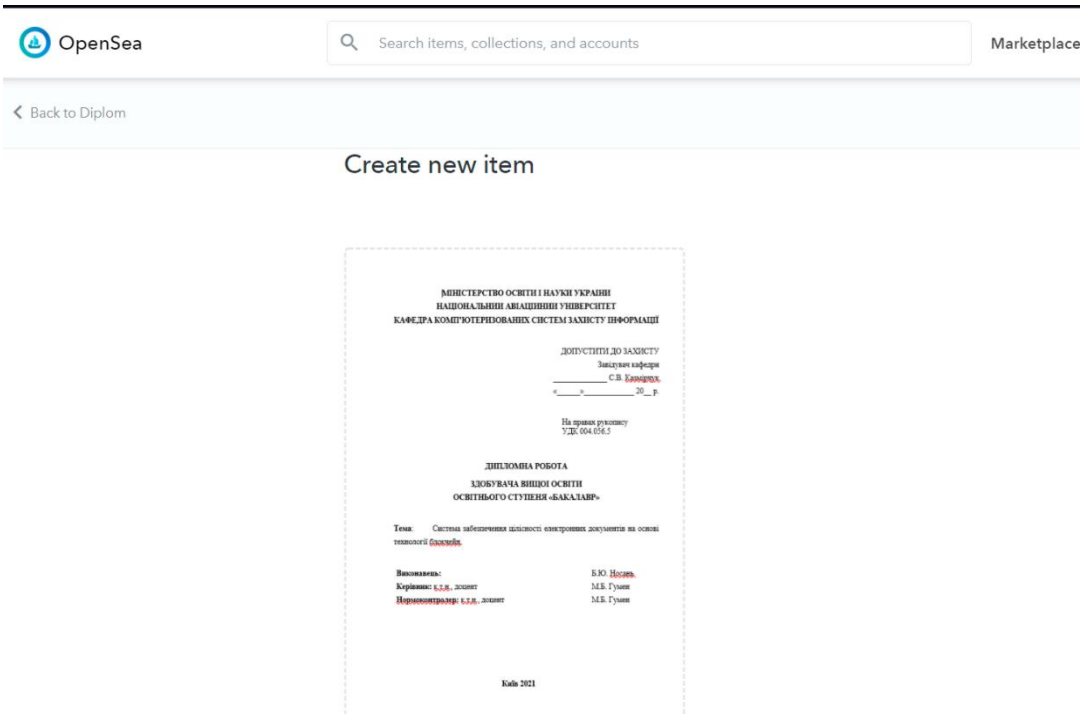
Забезпечення цілісності даних також є однією з функцій засобів захисту інформації від несанкціонованого доступу. Ці засоби захисту виробляють відстеження незмінності даних в автоматичному режимі за заздалегідь налаштованому розкладом. При цьому крім незмінності самих файлів, засоби захисту можуть перевіряти незмінність прав доступу до об'єктів і їх атрибутів. У разі виявлення помилок при проходженні процедури контролю цілісності, засоби захисту від несанкціонованого доступу можуть сигналізувати про це адміністраторам безпеки, забороняти доступ до системи, зберігати зміни в файлах або відкочувати ресурси до початкового стану. При цьому засоби захисту від несанкціонованого доступу надають такі алгоритми перевірки цілісності даних: електронно-цифровий підпис (перевіряється вбудована цифровий підпис даних), CRC32 (або розрахунок контрольних сум файлів), хеш, имитовставка, повний збіг.

3.4 Практична реалізація на базі NFT токену

Для реалізації цього потрібно створити nft токен документу за допомогою сервісу OpenSea. Для прикладу я буду шифрувати титульну сторінку диплому.

Для цього я створію NFT токен документу(див. рис.3.2).





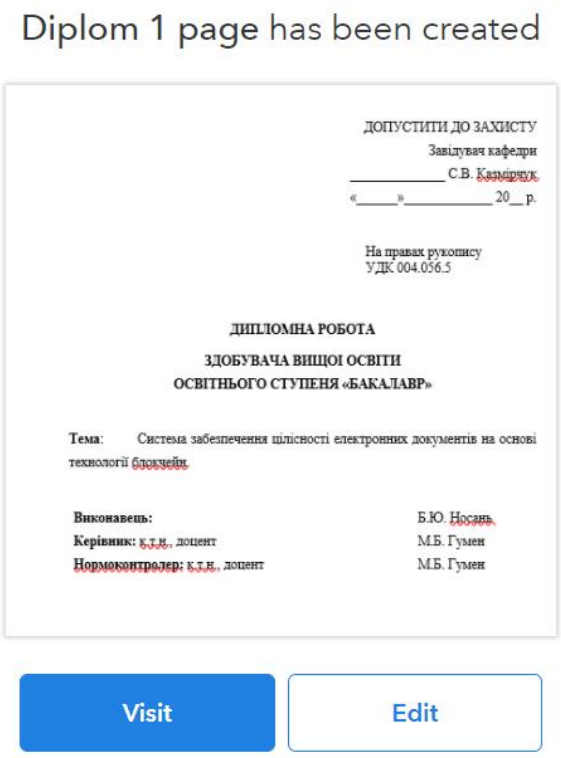


Рис.3.2. NTF токен документа

Підтверджуємо створення NFT токену на базі технології блокчейн(див. рис.3.3).

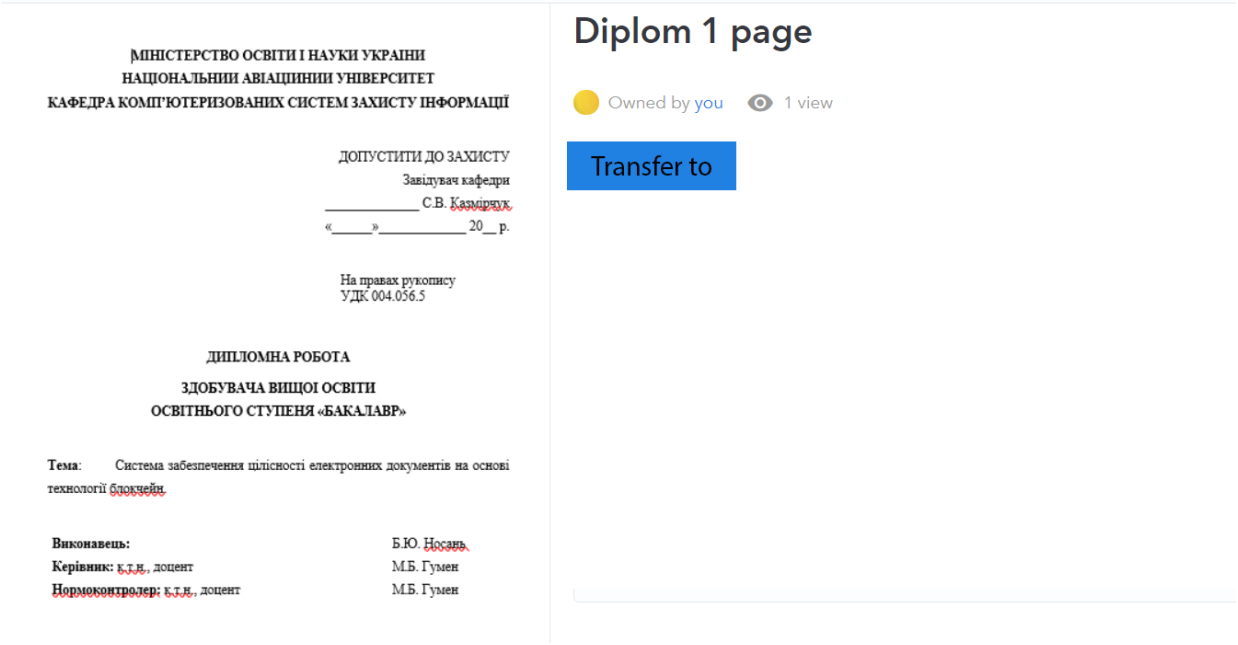
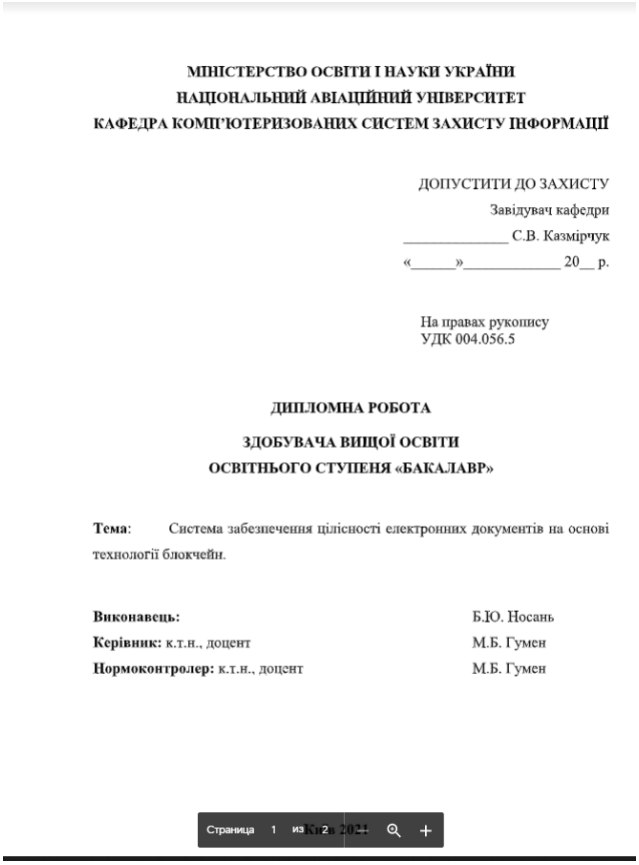


Рис.3.3.Підтвердження створення NTF токену на базі технології блокчейн

Надсилаю для перевірки(див. рис.3.4).



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.056.5

ДИПЛОМНА РОБОТА
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: Система забезпечення цілісності електронних документів на основі технології блокчейн.

Виконавець: Б.Ю. Носань
Керівник: к.т.н., доцент М.Б. Гумен
Нормоконтролер: к.т.н., доцент М.Б. Гумен

Страница 1 из 2

Рис.3.4.Результат перевірки

Можемо спостерігати, що файл який надійшов через NFT токен залишився таким самим, який при відправці. Тобто цілісність файла була збережена.

3.5 Практична реалізація блокчейну

Створення хеш блоку який використовується в блокчейні: Хеш попереднього блоку необхідно знайти в блоці для збереження цілісності ланцюга:

```
class Block {
constructor(index, previousHash, timestamp, data, hash) {
this.index = index;
this.previousHash = previousHash.toString();
```

```
this.timestamp = timestamp; this.data = data; this.hash = hash.toString();
}
}
```

Генерація блоку (хеша) блокчейну:

Для створення блоку потрібно знати хеш попереднього блоку, а решта необхідно створювати з такого змісту (= index, hash, data і timestamp). Блок-дата - це якась інформація, яка передається кінцевому користувачеві.

```
var generateNextBlock = (blockData) => {
var previousBlock = getLatestBlock();
var nextIndex = previousBlock.index + 1;
var nextTimestamp = new Date().getTime() / 1000;
var nextHash = calculateHash(nextIndex, previousBlock.hash, nextTimestamp, blockData);
return new Block(nextIndex, previousBlock.hash, nextTimestamp, blockData, nextHash);
};
```

Перевірка цілісності блоків

Дуже важливо, щоб зберігалась цілісність документу, тому для цього потрібна перевірка цілісності блоків, через які проходить документ:

```
var isValidNewBlock = (newBlock, previousBlock) => {
if (previousBlock.index + 1 !== newBlock.index) {
console.log('invalid index');
return false;
} else if (previousBlock.hash !== newBlock.previousHash) {
 console.log('invalid previoushash');
return false; }
```

```
        else if (calculateHashForBlock(newBlock) !== newBlock.hash) {
console.log('invalid hash: ' + calculateHashForBlock(newBlock) + ' ' +
newBlock.hash);
        return false; }
        return true;
        };
```

ВИСНОВКИ

Документообіг є сферою практичної діяльності, що документально забезпечує функціонування кожного органу державної влади, органів місцевого самоврядування, підприємств, установ, організацій та їх об’єднань усіх форм власності.

Для підвищення ефективності організації роботи з документами необхідно володіти процесами створення управлінських документів та їх керуванням тощо.

Важливе значення для організації роботи з документами щодо практичного застосування набутих знань є дотримання єдиних вимог та правил оформлення службових документів, які закріплені національними стандартами; дотримання вимог та правил організації роботи зі службовими документами, які зафіксовані у законодавчих і нормативно-правових актах України, що регламентують роботу з інформацією та документацією; впровадження комп’ютерних технологій на всіх етапах документування управлінської інформації для автоматизованого опрацювання задокументованої інформації.

Основною метою при розробці технологій електронного документообігу було досягнення максимальної наступності правил і прийомів паперового документообігу і журнально-картотечного діловодства, що дозволяє забезпечити безболісний перехід від традиційних технологій до сучасних.

Наскрізний автоматичний контроль виконання на всіх етапах роботи з документами кардинально підвищує якість роботи виконавців, робить терміни підготовки документів більш прогнозованими і керованими.

На відміну від документів на паперових носіях зі своїми жорсткими рамками, статичною формою й обмеженими можливостями, перехід до динамічних цифрових електронних документів забезпечує особливі переваги у створенні, спільному використанні, поширенні та збереженні інформації.

Можна зробити висновки, що блокчейн, насамперед, це інструмент для вирішення питань безпеки, надійності та прозорості трансакцій, тому

використання його у різних сферах ділової активності набирає обертів. Зважаючи на проблеми розвитку блокчейн додатків, необхідно продовжувати розвиток технології в напрямку стандартизації, безпеки додатків та інтеграції блокчейн систем з іншими сучасними технологіями.

Також, необхідно системно підходити до питання безпеки блокчейн додатків. В цьому напрямку необхідно проводити серйозні дослідження. На сьогодні немає великого практичного досвіду використання блокчейн систем. Єдиною мережею, яка довгий час працює без істотних збоїв є блокчейн біткойн. Проблеми, що пов’язані з мережею біткойну, були через злам сервісів, побудованих поверх блокчейну. Також, була успішно виконана атака у мережі Ethereum.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Велика радянська енциклопедія. 3-є вид. М. : Сов. энциклопедия, 1972. Т. 8. 1996 с.

2. Видання. Основні види. Терміни та визначення. ДСТУ 3017–95. Чинний від 01.01.96. К. : Держстандарт України, 1996. 347 с.

3. Діловодство й архівна справа. Терміни та визначення. ДСТУ 2732– 94. Чинний від 01.07.95. К. : Держстандарт України, 1994. 553 с.

4. Інформація та документація. Базові поняття. Терміни та визначення. ДСТУ 2392–94. Чинний від 01.01.95. К. : Держстандарт України, 1994. 153 с.

5. Інформація та документація. Комплектування фонду, бібліографічний опис, аналіз документів. Терміни та визначення. ДСТУ 2394 – 94. К. : Держстандарт України, 1994. 89 с.

6. Коршунов О. П. Библиографоведение. Общий курс : учеб. для библ. фак. ин-тов культуры, ун-тов и пед. Вузов. М. : Кн. палата, 1990. 232 с.

7. Кушнаренко Н. М. Документознавство: підручник для вузів. 4-е вид. К. : Знання, 2003. 467 с.

8. Кушнаренко Н. М. Складові спеціальності „Документознавство та інформаційна діяльність”: питання методології. Бібліотекознавство. Документознавство. Інформологія. 2004. № 1. 156 с.

9. Михайлов А. И. Основы інформатики. 2-е изд., перераб. и доп. М. : Наука, 1968. 756 с.

10. Столяров Ю. М. Соціальні комунікації: розвиток в інформаційному просторі. Вісн. Харків. Держ. акад. к-ри : зб. наук. пр. Вип. № 2. Х., 2000. 538 с.

11. Терминологический словарь по библиотечному делу и смежным отраслям знания / Сост. З.Г. Высоцкая (отв. ред.), В.А. Врубель, А.Б. Маслов; РАН. Б-ка по естественным наукам. М. : [б. и.], 1995. 268 с.

12. Терминологический словарь по информатике. М. : МЦНТИ, 1975. 752 с.

13. Терминологический словарь по теории и практике научной информации. М., 1964. 567 с.

14. Швецова-Водка Г. М. Типологія книги : навч. посібник для студ. вузів культури і мистецтв. Рівнен. держ. ін-т культури. К. : Кн. палата України, 1999. 668 с.

15. Глущик С. В. Сучасні ділові папери : навч. посібник. 4-те вид., перероб. і доп. К., 2003. 400 с.

16. Діденко А. Н. Сучасне діловодство : навч. посібник. 4-те вид. К. : Либідь, 2004. 384 с

17. Швецова-ВодкаГ. Н. Про обсяг поняття «книга» в документознавстві. Бібл. вісн. 2008. № 4. 273 с.

18. Швецова-ВодкаГ.М. Типологія документа: Навч.посібник для студентів ін-тів культури. Рівн.держ. ін-т культури. К.: Кн.палата України, 2008. 267 с.

19. К.Г. Мітяєв і становлення документознавства. Бібліотекознавство. Документознавство. Інформологія. 2008. № 1. 674 с.

20. Сучасне документознавство в Україні : концепції, перспективи розвитку. Укр. іст. журн. 2008. № 6. 473 с.

21. Барановський В.П. Документаційне забезпечення діяльності організації. // Навчальний посібник. М.: Асоціація авторів і видавців «Тандем». Вид.-во ЕКМОС, 1999. 433 с.

22. Печнікова Т. В. Практика роботи з документами в організації. Вид."Тандем". М.: ЕМОС, 1999. 208 с.

23. Алексєєва Т., Потапенко М. Системи електронного документообігу: від усвідомлення потреби до оцінки та імплементації. ІТ- спец. 2008. № 12. 578 с.

24. Матвієнко О.В. Основи організації електронного документообігу. 2008. 112 с.

25. Брускіна Т., Дроздов Д. Спецобзор: програмні рішення в сфері електронного документообігу. ІТСпец. 2008. № 12. 580 с.

26. Леонов И.В. Введення в методологію розробки програмного забезпечення // Ескейп, 2004. 301 с.

27. Електронний документообіг та захист інформації: навч. посіб. За заг. ред. д.держ.упр., професора Н.В. Грицяк. К.: НАДУ, 2015. 84 с.

28. Клименко І.В., Линьов К.О. Система електронного документообігу в державному управлінні. Київ, 2006. 32 с.

29. Генкин А., Михеев А. Блокчейн: как это работает и что ждет нас завтра. Москва, 2018. 592 с.

30. Данильченко О. Блокчейн: юрист из машины // ЮРИСТ&ЗАКОН. 2017. № 21. июнь. 2012. 349 с.

31. Уолпорт М. Технология распределения реестра: за рамками блокчейн. 2019. 589 с.

32. Потій О.В., Лєншин А.В. Основні положення математичного апарату суб'єктивної логіки та його застосування для оцінки зрілості систем забезпечення безпеки інформації. Радіотехніка. Тематичний випуск "Інформаційна безпека". Вип. 141. Х.: Радіотехніка. 2015. 763 с.

33. Смірнов А.О., До́ренський О.П. Оцінювання загального показника якості системи забезпечення безпеки інформації автоматизованої системи. Системи обробки інформації. – Х. ХУПС, 2017. №7 (65). 890 с.

34. Домарев В.В. Безопасность информационных технологий. Системный подход. К. ООО "Тид "ДС". 2004. 992 с.

35. Галатенко В.А. Стандарты и рекомендации в области информационной безопасности. Информационный бюлетень "Jet Informations". №1-3 (8-10). 1996. 895 с.

36. Егоров Ф.И., Чирков Д.В. Модель угроз безопасности корпоративных сетей. Матеріали III Міжнародної науково-технічної конференції "Сучасні інформаційно-комунікаційні технології COMINFO'2007". К.: ДУІКТ. 2007. 564 с.

37. Доренський О.П. Дослідження потенційних загроз безпеці інформації інформаційної системи та аналіз їх класифікаційного поділу. Збірник наукових

праць Кіровоградського національного технічного університету. Вип. 19. Кіровоград: КНТУ. 2007. 789 с.

38. Ротштейн А.П. Интелектуальные технологии идентификации. Вінниця: Вид-во “Універсум Вінниця”. 2009. 320 с.

39. Галатенко В.А. Основы информационной безопасности. 3-е изд. М.: “ИУИТ”. 2015. 208 с.

40. Локазюк В.М., Савченко Ю.Г. Надійність, контроль, діагностика. К.: Видавничий центр “Академія”. 2010. 376 с.