МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

_____ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК І ТЕХНОЛОГІЙ____
(повне найменування факультету)

КАФЕДРА СИСТЕМНОГО АНАЛІЗУ ТА ОБЧИСЛЮВАЛЬНОЇ МАТЕМАТИКИ
(повне найменування кафедри)

Пояснювальна записка

до дипломного проєкту (роботи)
_____магістра_____
(ступінь вищої освіти)

на тему **Застосування блокчейну в управлінні цифровою ідентичністю: Приклад UkraineDAO**

Виконав(ла): студент(ка) 2 курсу, групи_КНТ-812м_

Спеціальності __124 – Системний аналіз_____
(код і найменування спеціальності)

Освітня програма (спеціалізація)
_«Інтелектуальні технології та прийняття___
_рішень в складних системах»_____

_____ТЕРНИЦЬКИЙ Владислав_____
(ПРІЗВИЩЕ та ініціали)

Керівник _____БАХРУШИН Володимир_____
(ПРІЗВИЩЕ та ініціали)

Рецензент_____
(ПРІЗВИЩЕ та ініціали)

2024

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет____комп'ютерних наук і технологій_____
Кафедра_____Системного аналізу та обчислювальної математики_____
Ступінь вищої освіти _____магістр_____
Спеціальність _____124 – Системний аналіз_____
(код і найменування)
Освітня програма (спеціалізація)___«Інтелектуальні технології та прийняття рішень в складних системах»_____
(назва освітньої програми (спеціалізації)

ЗАТВЕРДЖУЮ
В.о. завідувача кафедри _____
___Еліна ТЕРЕЩЕНКО_____
«_____» _____20___року

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

_____ТЕРНИЦЬКОГО Владислава Миколайовича_____
(ПРІЗВИЩЕ, ім'я, по батькові)

1. Тема проєкту (роботи)__Застосування блокчейну в управлінні цифровою ідентичністю: Приклад UkraineDAO_____
керівник проєкту (роботи)_д.ф.-м.н., проф. БАХРУШИН Володимир Євгенович____,
(науковий ступінь, вчене звання, ПРІЗВИЩЕ, ім'я, по батькові)
затверджені наказом закладу вищої освіти від «06»__грудня__2023_року №_492
2. Строк подання студентом проєкту (роботи)__«30» січня 2024 року_____
3. Вихідні дані до проєкту (роботи)__літературні джерела за темою дослідження: наукові статті, публікації, дослідження, публікації в журналах, звіти наукових конференцій._____
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_1. Аналіз публікацій та досліджень на теми технології блокчейн, децентралізованої ідентифікації та цифрової ідентичності; 2. Порівняльний аналіз методів децентралізованої ідентифікації та порівняльну характеристику провайдерів управління цифровою ідентичністю. Виявлено проблему та наведено постановку задачі. Проаналізовано об'єкт дослідження - спільноту UkraineDAO; 3. Вирішення проблеми - попередньої верифікації нових користувачів шляхом інтеграції децентралізованого ідентифікатора (DID) від провайдера BrightID в систему онбордингу через Discord. Проведено аналіз результатів. Зроблено висновок, що застосування запропонованого рішення не лише зміцнює цілісність цифрових ідентичностей, але й активно залучає користувачів до процесу верифікації, сприяючи створенню відчуття колективної відповідальності та довіри в децентралізованих спільнотах._____
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількість слайдів, плакатів)
_____
_____

6. Консультанти розділів проєкту (роботи)

Розділ	ПРІЗВИЩЕ, ініціали та посада консультанта	Підпис, дата	
		завдання видав	прийняв виконане завдання
1	БАХРУШИН В.Є., д.ф.-м.н., проф.		
2	БАХРУШИН В.Є., д.ф.-м.н., проф.		
3	БАХРУШИН В.Є., д.ф.-м.н., проф.		
Нормоконтроль	ШИРОКОРАД Д.В., к.ф.-м.н., доц.		

7. Дата видачі завдання «_08_» __вересня__2023_ року.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проєкту (роботи)	Строк виконання етапів проєкту (роботи)	Примітка
1	Вибір і затвердження теми дипломної роботи	08.09.2023 – 13.09.2023	
2	Формулювання мети та завдання роботи	14.09.2023 – 22.09.2023	
3	Розробка плану та структури роботи	23.09.2023 – 06.10.2023	
4	Підбір та вивчення літературних джерел	07.10.2023 - 29.10.2023	
5	Опрацювання й аналіз матеріалу згідно з темою роботи	30.10.2023 – 01.12.2023	
6	Оформлення пояснювальної записки	02.12.2023 - 13.12.2023	
7	Попередній захист дипломної роботи та отримання рецензій	14.12.2023 – 29.01.2024	
8	Захист дипломної роботи	30.01.2024	

Студент(ка) _____ __Владислав ТЕРНИЦЬКИЙ__
(підпис) (Ім’я ПРІЗВИЩЕ)

Керівник проєкту (роботи) _____ __Володимир БАХРУШИН__
(підпис) (Ім’я ПРІЗВИЩЕ)

РЕФЕРАТ

ПЗ: 69 с., 21 рис., 89 джерел.

Об'єкт дослідження: управління цифровою ідентичністю в децентралізованих спільнотах на прикладі UkraineDAO.

Мета дослідження: імплементація інструменту верифікації нових користувачів в Discord при процедурі онбордингу в децентралізованих спільнотах на прикладі UkraineDAO.

Предмет дослідження: процеси, протоколи та технології, що застосовуються в спільноті UkraineDAO.

Методи дослідження: аналіз джерел, досліджень і публікацій, порівняльний аналіз, порівняльна характеристика.

Діджиталізація кардинально змінила спосіб життя людей у 21 столітті. Від спілкування та розваг до покупок і фінансів. Значних змін зазнали те, як ми живемо, працюємо та взаємодіємо один з одним. Як наслідок, наша концепція ідентичності також еволюціонувала в цифрову епоху. Розвиток інтернету та все більш широке використання цифрових технологій трансформували нашу ідентичність у цифрову форму, так звану цифрову ідентичність. В той же час поява технології блокчейн зробила революцію в різних галузях, пропонуючи безпечні, прозорі та децентралізовані рішення. У сфері управління цифровою ідентичністю блокчейн має величезний потенціал для трансформації традиційних підходів.

В роботі було розглянуто проблеми, пов'язані з традиційними централізованими системами управління цифровою ідентичністю, підкреслено необхідність більш безпечних, прозорих і орієнтованих на користувача рішень. Проаналізовано, як технологія блокчейн може вирішити ці проблеми, пропонуючи децентралізовані та незалежні системи управління цифровою ідентичністю. Проаналізовано децентралізовану спільноту UkraineDAO, а саме її операційну діяльність. Було виявлено потенційні труднощі в координації,

верифікації та залученні нових членів. Було запропоновано рішення для верифікації членів децентралізованих спільнот в системі Discord за допомогою провайдера BrightID - соціальної мережа ідентифікації. Як результат, впровадження надає перевірку особистості та забезпечує унікальність нових членів спільноти.

БЛОКЧЕЙН, ІДЕНТИФІКАЦІЯ, ЦИФРОВА ІДЕНТИЧНІСТЬ (DIGITAL IDENTITY), САМОСУВЕРЕННА ІДЕНТИЧНІСТЬ (SELF-SOVEREIGN IDENTITY), УПРАВЛІННЯ ЦИФРОВОЮ ІДЕНТИФІКАЦІЄЮ (IDENTITY MANAGEMENT, IdM, IAM, IDENTITY GOVERNANCE), ОБЛІКОВІ ДАНІ, СИСТЕМА УПРАВЛІННЯ ОБЛІКОВИМИ ДАНИМИ, ДЕЦЕНТРАЛІЗОВАНИЙ, ПРИВАТНІСТЬ, КОНФІДЕНЦІЙНІСТЬ, КРИПТОВАЛЮТА

ЗМІСТ

ВСТУП

Поява технології блокчейн зробила революцію в різних галузях, пропонуючи безпечні, прозорі та децентралізовані рішення. У сфері систем підтримки прийняття рішень блокчейн має величезний потенціал для трансформації традиційних підходів. У цій роботі досліджується технологія блокчейн, управління цифровою ідентичністю та їх застосування для побудови безпечних і прозорих децентралізованих систем. Проводиться тематичне дослідження UkraineDAO - децентралізована автономна організація [49], яка була створена на початку повномасштабного вторгнення рф в Україну, щоб використовувати “силу технологій web3 і спільноти для захисту України” [56].

Традиційні централізовані системи управління цифровою ідентичністю стикаються з такими проблемами, як конфіденційність і єдині точки відмови [2]. Ці обмеження підкреслили потребу в більш безпечних і орієнтованих на користувача рішеннях для цифрової ідентифікації. Блокчейн з його децентралізованою архітектурою, незмінністю та механізмами консенсусу є перспективним способом вирішення цих проблем.

Дослідження UkraineDAO, представлене в даній роботі, було націлене на вивчення операційної діяльності спільноти. Було виявлено потенційні труднощі в координації, верифікації та залученні нових членів. Тому метою дослідження є імплементація інструменту верифікації нових користувачів в Discord при процедурі онбордингу в децентралізованих спільнотах на прикладі UkraineDAO.

1 ОГЛЯД ЛІТЕРАТУРНИХ ДЖЕРЕЛ

Люди використовують термін "блокчейн" для позначення різних речей, і це може заплутати. Іноді говорять про блокчейн біткойну [3], іноді про інші віртуальні валюти, іноді про смарт-контракти. Але найчастіше говорять про розподілені реєстри [5]. Останніми роками технологія блокчейн привертає до себе значну увагу, оскільки вона має потенціал для революції в різних галузях, від фінансів до охорони здоров'я і не тільки. Але що таке технологія блокчейн і які її основні принципи?

1.1 Огляд технології блокчейн

Робота Накамото про біткойн [3] встановлює основоположні принципи децентралізованих розподілених реєстрів та пропонує вирішення проблеми подвійних витрат за допомогою однорангової мережі - P2P (в яких окремі вузли обмінюються між собою файлами і зберігають один і той же набір даних). Мережа фіксує час транзакцій, хешуючи їх у безперервний ланцюжок підтверджень виконання робіт, формуючи запис, який неможливо змінити без повторного підтвердження виконання робіт.

Блокчейн - це децентралізований і розподілений цифровий реєстр, який записує транзакції через мережу комп'ютерів. По суті, це ланцюжок блоків, кожен з яких містить певну кількість транзакцій [6]. Транзакції обробляються та перевіряються механізмом консенсусу (механізм координації дій в розподіленій мережі) більшістю учасників мережі, що усуває необхідність у посереднику. Транзакції упаковуються в блоки, а блоки з'єднуються між собою за допомогою криптографічного хешу, щоб забезпечити незмінність - як тільки блок додається до ланцюжка, інформація, що міститься в ньому, стає постійною і не може бути змінена [7].

Фундаментальне розуміння технології блокчейн має вирішальне значення для визначення її застосування. Систематичний огляд Yli-Huumo та ін. [1] містить всебічний огляд, який ґрунтує дискусію на сучасному ландшафті технології блокчейн.

Дослідження зосереджене на виявленні та вдосконаленні обмежень блокчейну з точки зору конфіденційності та безпеки, наголошено, що багатьом із запропонованих рішень бракує конкретної оцінки ефективності. Підкреслено інші проблеми, пов'язані з масштабуванням, включаючи пропускну здатність і затримку. Надаються рекомендації щодо майбутніх напрямків досліджень.

У книзі Свон [15] досліджується потенціал технології блокчейн, яка лежить в основі системи біткойну та інших криптовалют, для трансформації різних аспектів суспільства, таких як фінанси, управління, охорона здоров'я, наука тощо. Автор пояснює, що блокчейн - це, по суті, публічна книга, яка може стати всесвітнім децентралізованим реєстром для реєстрації, інвентаризації та передачі всіх активів - не лише фінансів, але й власності та нематеріальних активів, таких як голоси, програмне забезпечення, медичні дані та ідеї [14].

У дослідженні Zheng та ін. [6] критично розглядаються виклики та можливості технології блокчейн, що допомагає зрозуміти ширший ландшафт блокчейну, розглядаються потенційні перешкоди та шляхи для зростання.

1.2 Архітектура та консенсус

Огляд Ісмаїла та Матервали [7] заглиблюється в архітектуру блокчейну та протоколи консенсусу, пропонуючи детальне розуміння технічних тонкощів блокчейн-систем. У статті обговорено еволюцію архітектури блокчейну та його протоколів консенсусу, проводячи ретроспективний аналіз і обговорюючи обґрунтування еволюції різних архітектур і протоколів, а також фіксуючи припущення, що призвели до їх розвитку і внеску в створення додатків. Обговорюється, що поточні консенсусні протоколи, хоча і вирішують деякі

проблеми, критикуються за енергоємність. Запропоновані рішення, такі як протоколи, засновані на можливостях або голосуванні, поєднують енергоефективність з масштабованістю і децентралізацією. Висловлюється думка про необхідність створення обчислювально-інтенсивного протоколу консенсусу, який би збалансовував складність і енергоефективність. Крім того, в тексті наголошується на розвитку гнучкості поточних архітектур, що перешкоджає адаптації до екосистем співпраці. Підкреслюється важливість модульних і гнучких архітектур для задоволення динамічних потреб додатків. Проблеми конфіденційності та безпеки визначені як вирішальні, застерігаючи, що енергоефективний блокчейн може скомпрометувати децентралізацію і сприяти зловмисним атакам. Стаття має на меті заохотити подальші дослідження блокчейну в контексті розумних міст, виступаючи за структуру, яка надає пріоритет співпраці, гнучкості, масштабованості та енергоефективності, що відповідає цілям "зелених" та економічно ефективних обчислень для покращення обслуговування клієнтів.

Дослідження Яо та ін. (2021) [8] про механізми консенсусу в блокчейні консорціуму (об'єднання публічного та приватного блокчейнів, яке частково децентралізоване) сприяє розумінню того, як досягається консенсус у різних конфігураціях блокчейну, з наслідками для децентралізованого прийняття рішень. В статті надано фундаментальну інформацію про поточний стан методологій та технологій консенсусу, а також про існуючі проблеми. Підкреслено значний вплив алгоритмів консенсусу на продуктивність блокчейн-додатків, висвітлено ключові дослідницькі виклики для консорціумних блокчейнів. Ці виклики включають підвищення масштабованості для вирішення критичної проблеми обмеженого членства, алгоритмічне злиття для адаптації алгоритмів консенсусу до умов, що змінюються, збереження конфіденційності, підвищення продуктивності з акцентом на такі фактори, як пропускна здатність і затримка, а також оптимізація пошуку і зберігання в контексті зростаючих очікувань щодо мереж блокчейн. У документі відзначається постійний розвиток консорціумних блокчейн-алгоритмів та їхніх застосувань, визнаючи, що виклики

зберігатимуться, оскільки технологія та її застосування продовжуватимуть розвиватися.

Базова архітектура блокчейну показана на рис. 1.1 та складається з п’ятьох рівнів: інфраструктурного рівня, мережевого рівня, рівня даних, рівня консенсусу і прикладного рівня. У базовій структурі рівень даних включає блоки даних, структуру ланцюжка і криптографічні механізми, які є основними компонентами блокчейну.

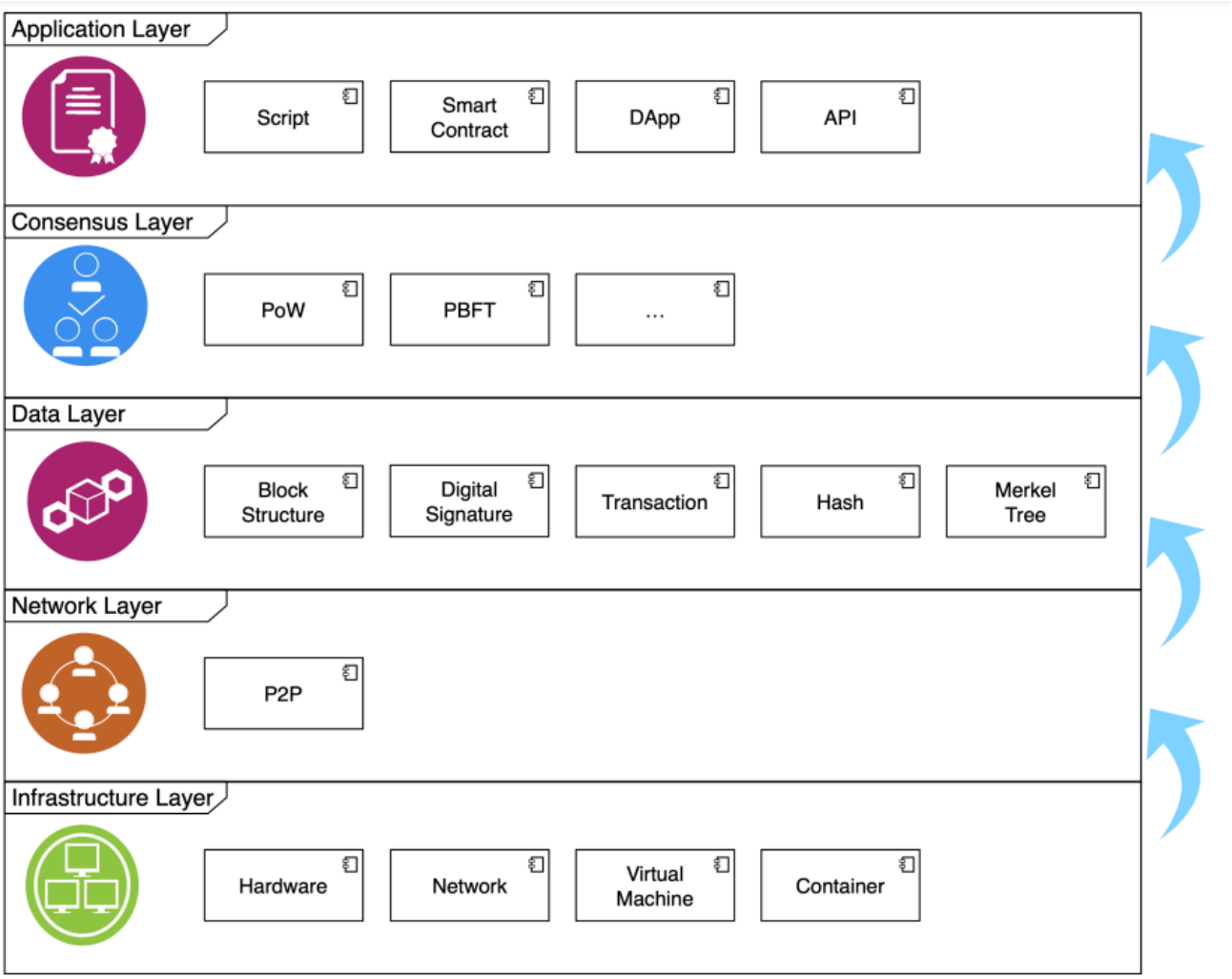

Рис. 1.1 - Архітектура блокчейну [8]

Рівень даних відповідає за транзакції та механізми реалізації блокчейну, а також за пов'язані з ними технології перевірки розповсюдження блоків. Рівень консенсусу - це переважно механізм консенсусу, представлений такими алгоритмами, як Proof of Work (PoW) - форма криптографічного доказу, в якій

одна сторона (той, хто доводить) доводить іншим (тим, хто перевіряє), що певна кількість конкретних обчислювальних зусиль була витрачена, використовується в Bitcoin, а також Proof of Stake (PoS), що використовується в Ethereum - працює шляхом вибору валідаторів пропорційно до кількості їхніх активів у відповідній криптовалюті. У прикладному рівні інкапсулюються різні прикладні сценарії і випадки, представлені програмованими активами, такими як валюти і фінансові інструменти, різні коди сценаріїв і смарт-контракти [8].

1.3 Класифікація блокчейн-мереж

Дослідження Бутеріна (2015) [9] розрізняє публічні та приватні блокчейни, забезпечуючи фундаментальне розуміння різних типів блокчейнів та їх застосування. У публічних блокчейнах (без дозволів) будь-хто може приєднатися як новий користувач або майнер нод (особа, яка бере участь у процесі перевірки та додавання нових транзакцій до блокчейну), і всі учасники можуть виконувати операції, такі як транзакції або контракти, без обмежень.
У приватних блокчейнах, які підпадають під категорію блокчейнів з дозволами разом з федеративними блокчейнами, зазвичай існує білий список дозволених користувачів з певними характеристиками та дозволами на здійснення мережевих операцій. Приватні блокчейни можуть уникати дорогих механізмів консенсусу, таких як механізм підтвердження роботи (PoW), оскільки ризик атак sybil (в якій зловмисник підриває систему репутації пірингової мережі, створюючи велику кількість псевдонімів і використовуючи їх для отримання непропорційно великого впливу) є низьким. [10]. Замість цього вони можуть використовувати ширший спектр протоколів консенсусу, що базуються на антистимулах.

Федеративний блокчейн - це гібридна комбінація публічного та приватного блокчейнів [9, 6]. Хоча він має схожі з приватними блокчейнами рівні масштабованості та захисту конфіденційності, головна відмінність полягає

в тому, що для перевірки процесів транзакцій обирається набір вузлів, які називаються вузлами-лідерами, а не один суб'єкт. Це дозволяє створити частково децентралізовану структуру, де вузли-лідери можуть надавати дозволи іншим користувачам.

Публічні блокчейни, такі як Bitcoin та Ethereum, є самодостатніми і мають низькі витрати на інфраструктуру, що робить їх придатними для криптовалют. Приватні блокчейни зазвичай використовуються для управління базами даних та аудиту, тоді як федеративні блокчейни знаходять застосування в таких секторах, як банківська справа та промисловість.

Більш детальний огляд класифікації блокчейн мереж можна знайти в роботах таких авторів як Walport [12] та Swanson [10], а також в роботі Casino та ін. [13], де були враховані та проаналізовані такі характеристики, як час схвалення транзакції, аспекти безпеки, та анонімність, та підсумовано основні характеристики кожної блокчейн-мережі щодо ефективності, безпеки та механізмів консенсусу Рис. 1.2.

Property	Public	Private	Federated
Consensus Mechanism	• Costly PoW • All miners	• Light PoW • Centralised organisation	• Light PoW • Leader node set
Identity Anonymity	• (Pseudo) Anonymous • Malicious?	• Identified users • Trusted	• Identified users • Trusted
Protocol Efficiency & Consumption	• Low efficiency • High energy	• High efficiency • Low energy	• High efficiency • Low energy
Immutability	• Almost impossible	• Collusion attacks	• Collusion attacks
Ownership & Management	• Public • Permissionless	• Centralised • Permissioned whitelist	• Semi-Centralised • Permissioned nodes
Transaction Approval	• Order of minutes	• Order of milliseconds	• Order of milliseconds

Рис. 1.2 - Класифікація та основні характеристики блокчейн-мереж [13]

1.4 Застосування блокчейну

Шарплз і Домінге [29], Сінгла та ін. [36], Петерсон та ін. [22] і Liu та ін. [23] досліджують потенціал блокчейну в окремих секторах, а саме освіті та охороні здоров'я, наголошуючи на безпечному веденні записів та управлінні ідентифікацією.

Ліптон [5] представляє блокчейн і розподілені реєстри та описує їхнє потенційне застосування у сфері грошей і банківської справи. В аналізі порівнюються публічні та приватні реєстри та окреслюється придатність різних типів реєстрів для різних цілей. Крім того, представлено кілька історичних прототипів блокчейнів і розподілених реєстрів, а також проілюстровано результати їхнього хардфоркінгу - кардинальної зміни роботи алгоритмів і самого коду. Окреслено деякі потенційні застосування розподілених реєстрів у торгівлі, клірингу та розрахунках, платежах, торговому фінансуванні тощо. Стверджується, що грошові ланцюги є природним застосуванням блокчейнів. Сформульовано роль цифрових валют у сучасному суспільстві та порівняно і протиставлено різні форми цифрових грошей, такі як електронні гроші, емітована центральним банком валюта, банківські гроші, біткойн та P2P-гроші.

Дослідження Кшетрі про блокчейн та інтернет речей [2] розширює перспективу застосування, досліджуючи його потенціал за межами фінансової сфери. В роботі увага акцентується на застосування блокчейну для посилення безпеки інтернету речей - мережі фізичних пристроїв, які підключені до Інтернету і обмінюються даними за допомогою давачів, програмного забезпечення та інших технологій. Наголошується на використанні систем управління ідентифікацією та доступом на основі блокчейну, порівнюються хмарні моделі мереж інтернету речей з моделями на основі блокчейну, а також забезпечення безпеки ланцюга поставок.

Було також проаналізовано роботу Casino та ін. [13] в якій пропонують класифікацію, орієнтовану на застосування. Автори в своєму підході

використовують строгу статистичну методологію, засновану на літературних джерелах, що краще відповідає поточним розробкам блокчейну і з високою точністю ілюструє майбутні тенденції розвитку блокчейну. У тексті також підкреслюється, що, незважаючи на широке розгортання блокчейн-додатків, існує безліч невирішених питань, які потребують уваги для покращення масштабованості, ефективності та довговічності. У звіті зазначається, що хоча окремі функції блокчейнів не є унікальними, їхня комбінація робить їх добре придатними для різних застосувань, що пояснює значний інтерес до них з боку різних галузей. Очікується, що зрілість блокчейнів призведе до їх більш широкого впровадження в різних галузях. Однак у тексті застерігається, що блокчейн не слід розглядати як універсальне рішення або альтернативу традиційним базам даних. Визнається необхідність ретельного вивчення конкретних вимог до застосування і підкреслюється важливість визначення індивідуальних характеристик для кожної сфери застосування. Такий підхід допомагає вибрати відповідний блокчейн і пов'язані з ним механізми, щоб адаптувати технологію до конкретних потреб кожної програми. Класифікація додатків на основі блокчейну графічно представлена на рис. 1.3.

Фінансовий сектор. Технологія блокчейн використовується в різних фінансових сферах, включаючи бізнес-послуги, розрахунки за активами, ринки прогнозування та економічні транзакції. Очікується, що вона принесе користь споживачам, банківській системі та суспільству в цілому. Застосування у фінансовому секторі включає ринки капіталу, операції з цінними паперами та деривативами, цифрові платежі, управління кредитами, банківські послуги, фінансовий аудит, а також платежі та обмін криптовалют [13, 16].

Перевірка цілісності. Перевірка цілісності - це нова сфера застосування блокчейну. Вона передбачає зберігання інформації та транзакцій, пов'язаних зі створенням і життєвим циклом продукту або послуги. Приклади можуть включати відстеження походження (товару) та захист від підробок, страхування та управління інтелектуальною власністю. Такі рішення, як Mediachain [17], Accumulate [18] і Silent Notary [19], використовують блокчейн для передачі прав

власності, зберігання метаданих і підтвердження подій. Технологія блокчейн також досліджується в страховій індустрії для продажу, андеррайтингу, обробки страхових випадків і виплат [13].

Рис. 1.3 - Сфери потенційного застосування блокчейну [13]

Державне управління. Технологія блокчейн має потенціал для трансформації державних операцій на місцевому та державному рівнях шляхом покращення підзвітності, автоматизації та безпеки при роботі з державними документами. Її можна використовувати для безпечного зв'язку, інтеграції "розумного міста", реєстрації, юридичних документів, ідентифікації, шлюбних

контрактів, податків і голосування. Приклади включають децентралізовані паспортні служби, управління державними послугами та системи голосування, які підвищують довіру та рівень залучення [13].

Інтернет речей. Поєднання блокчейну та Інтернету речей (IoT) має величезний потенціал. Блокчейн може вдосконалити IoT, вирішуючи проблеми безпеки та обміну даними. Децентралізовані платформи IoT використовують технологію блокчейн для забезпечення безпечного та контрольованого обміну даними в гетерогенних середовищах (де поєднуються компоненти, які можуть відрізнятися за своїми властивостями, характеристиками чи призначенням) з взаємопов'язаними розумними пристроями. Це дозволяє здійснювати платежі в режимі реального часу, вдосконалювати комерцію та транспортні системи. Як приклад можна навести Filecoin - децентралізований постачальник сховища даних [20]. У майбутньому пристрої Інтернету речей можуть мати банківські рахунки в криптовалюті для мікротранзакцій та обміну послугами [11]. Блокчейн також може бути застосований для ланцюгів поставок і відстеження походження в розподілених мережах [13].

Охорона здоров'я. Технологія блокчейн має значний потенціал в галузі охорони здоров'я, пропонуючи різні застосування в таких сферах, як управління державною охороною здоров'я, лонгітюдні медичні записи, автоматизований розгляд медичних претензій, онлайн-доступ до пацієнтів, обмін медичними даними пацієнтів, орієнтовані на користувача медичні дослідження, боротьба з підробкою ліків, клінічні випробування та точна медицина [21], 22]. Системи на основі блокчейну для управління електронними медичними картами (ЕМК) [23, 24] можуть надавати безпечний і приватний доступ до медичних даних, забезпечуючи їх розподілене зберігання, перевірку і доступність для різних постачальників медичних послуг. Це може вирішити проблеми цілісності даних, безпеки та згоди пацієнтів у клінічних випробуваннях [13, 21].

Конфіденційність і безпека. Технологія блокчейн може посилити аспекти безпеки великих даних, забезпечуючи децентралізовану і стійку до несанкціонованого втручання структуру. Вона пропонує додатки, орієнтовані на

конфіденційність і безпеку, які вирішують проблеми централізованого зберігання і обробки даних. Децентралізовані реалізації DNS, такі як Namecoin [25], можуть підвищити безпеку, стійкість до цензури та конфіденційність. Рішення на основі блокчейну також можуть підвищити безпеку та надійність розподілених мереж, хмарних систем, пристроїв Інтернету речей (IoT) та енергосистем. Такі методи, як змішування сервісів [26] і доведення з нульовим розголошенням [27], можуть покращити конфіденційність транзакцій в блокчейні [13].

Освіта. Технологія блокчейн може вирішити проблеми вразливості, безпеки та конфіденційності у навчальному середовищі [28]. Вона може зберігати записи про освіту і репутаційні винагороди [29], створюючи безпечну і розподілену систему управління освітніми даними. Системи на основі блокчейну можуть покращити управління освітніми сертифікатами, управління кредитами, цифрову акредитацію, а також збір та аналіз даних для прийняття рішень в освітніх системах. Вони також можуть покращити наукові публікації, полегшуючи подання рукописів, рецензування та перевірку [13].

Управління даними. Технологія блокчейн покращує управління даними, пропонуючи ефективні та безпечні рішення з можливістю верифікації [30]. Вона забезпечує міжорганізаційне управління даними, полегшуючи інтероперабельність (можливість створення систем з довільних неоднорідних, розподілених компонентів на базі уніфікованих інтерфейсів або протоколів) [31] між сторонами. Системи на основі блокчейну пропонують смарт-контракти, що зберігають конфіденційність, та орієнтовні на приватність проміжні обчислення. Їх можна застосовувати для безпечного розподілу, управління та обміну даними, забезпечуючи довіру та можливість аудиту. Хмарні децентралізовані рішення з використанням технології блокчейн долають проблеми великих даних і дозволяють аналізувати великі обсяги транзакцій [32]. Механізми контролю доступу та автентифікації можуть ще більше підвищити конфіденційність і безпеку при розподілі даних [13].

1.5 Цифрова ідентичність

Цифрова ідентичність охоплює різні аспекти присутності людини в Інтернеті, включаючи її особисту, професійну та соціальну складову. Зі зростанням інтернету та збільшенням кількості онлайн-транзакцій важливо мати унікальну та безпечну цифрову ідентичність, яка точно відображає те, ким ми є і що робимо в мережі. Як наслідок з'являється потреба в управлінні цифровою ідентичністю [34] - комплекс підходів, практик і технологій для управління обліковими даними користувачів. Він дає змогу особам та організаціям підтверджувати свою особистість в Інтернеті та отримувати доступ до необхідних послуг та ресурсів. Однак сучасні системи управління цифровою ідентичністю мають певні обмеження, зокрема, недостатній рівень безпеки, конфіденційності та портативності. З появою технології блокчейн почали з'являтися рішення для подолання цих обмежень, і зараз досліджуються потенційні можливості застосування блокчейну в управлінні цифровою ідентичністю [48].

Дослідження децентралізованої ідентифікації та цифрових ідентичностей в літературі відображає тонке розуміння того, як технологія блокчейн може змінити традиційні системи управління ідентифікацією.

Історична контекстуалізація Кемп [35] дає уявлення про еволюцію цифрової ідентичності, поміщаючи сучасні дискусії в історичні рамки. У статті обговорюється поняття ідентичності в контексті цифрових мережевих систем, а також те, чим вони відрізняються від традиційних паперових систем ідентифікації. Визначається ідентичність як "набір тверджень, які пов'язані з фізичною або юридичною особою", і пояснює терміни автентифікація, верифікація та доступ. У статті також розглядаються виклики та ризики управління ідентичністю в цифровому світі, такі як крадіжка особистих даних, порушення приватності та соціальні наслідки. Стверджується, що припущення і політика паперових систем ідентифікації не підходять для цифрових мережевих

систем, і що необхідні нові моделі і рішення для вирішення складної і динамічної природи цифрової ідентичності.

Дослідження Singla та ін. [36], Kubach та ін. [45], Stockburger та ін. [38] та Allen [37] заглиблюються в децентралізоване управління ідентичністю, сприяючи розумінню самосуверенної ідентичності та розширенню можливостей користувачів.

Singla [36] досліджує використання децентралізованого управління ідентифікацією (DIdM - Decentralized Identity Management) з використанням блокчейну в глобальних організаціях для підтримки безпечного використання інформаційних ресурсів. У статті пропонується концептуальний куб для аналізу та вивчення різних платформ DIdM, а також обговорюються переваги та виклики DIdM у порівнянні з традиційними, централізованими або федеративними моделями управління ідентифікацією.

Kubach [45] та Allen [37] розглядають самосуверенну ідентичність (SSI) - форма децентралізованої ідентичності, яка дозволяє користувачам створювати власні ідентифікаційні дані та керувати ними, не залежачи від зовнішніх органів влади. У статті викладено принципи та характеристики SSI, описано технічні компоненти та стандарти, які уможливлюють SSI, такі як децентралізовані ідентифікатори (DID), облікові дані, що перевіряються (VC), та децентралізовані системи управління ключами (DKMS), а також проаналізовано виклики та можливості SSI для управління ідентичністю.

У публікації Stockburger [38] представлено тематичне дослідження децентралізованого управління ідентифікацією в громадському транспорті на основі блокчейну з акцентом на рішенні SSI, розробленому в рамках європейського проекту SOFIE. У документі демонструється, як SSI може покращити користувацький досвід, безпеку та конфіденційність користувачів громадського транспорту, а також ефективність та інтероперабельність операторів громадського транспорту, обговорюються технічні та соціальні виклики і можливості впровадження SSI в громадському транспорті. У статті описується робота низькорівневого прототипу, щоб продемонструвати, як

запропонована система працює на практиці. Прототип показує, як пасажири можуть використовувати стандартизовані проїзні документи, які дійсні в різних транспортних мережах Європи, і як вони можуть підтвердити свою особу та оплатити квитки за допомогою технології блокчейн. У документі також обговорюються переваги та виклики впровадження запропонованої системи, такі як посилений контроль користувачів, конфіденційність, безпека та інтероперабельність, а також технічні та соціальні складнощі та бар'єри.

Протокол Sovrin Харджоно та ін. [4] заглиблюється в самосуверенну ідентичність, наголошуючи на розширенні прав і можливостей людей у контролі над власною ідентичністю. У статті стверджується, що сучасні системи цифрової ідентичності є фрагментованими, незахищеними і втручаються в приватне життя, і що існує потреба в новій парадигмі ідентичності, яка ґрунтується на контролі користувача, конфіденційності та інтероперабельності. У статті пропонується мережа Sovrin Network як рішення, що використовує технологію блокчейн для того, щоб дозволити користувачам створювати власні цифрові ідентичності та керувати ними, не залежачи від будь-якого центрального органу або посередника.

Тематичне дослідження Kruk та ін. [41] та метааналіз Mulaji та Roodt [47] пропонують практичне розуміння впровадження та викликів управління ідентичністю на основі блокчейну, встановлюючи міст між теорією та реальними застосуваннями.

У роботі Kruk та ін. [41] представлено D-FOAF, розподілену систему управління ідентифікацією, яка використовує соціальні мережі для делегування прав доступу. У статті показано, як інформація з соціальних мереж може бути використана для авторизації довірених друзів для доступу до послуг, а також як керувати розподіленою ідентичністю, авторизацією та перевіркою прав доступу.

В метааналізі Mulaji та Roodt [47] зроблено огляд літератури про розподілене управління ідентифікаційними даними на основі блокчейну та синтезовано висновки в мета фреймворк - набір керівних принципів для створення інших фреймворків. У статті оцінюється практичність впровадження

розподіленого управління ідентичностями на основі блокчейну в організаціях, а також визначаються переваги, бар'єри та найкращі практики. У статті використано методологію мета синтезу, яка є якісним методом дослідження, що поєднує та інтерпретує результати кількох досліджень на одну тему. У статті відібрано 69 робіт з авторитетних академічних джерел і проаналізовано їх за допомогою підходу тематичного аналізу. Висновки згруповані за трьома темами:

- поточний стан розподіленого управління ідентифікацією на основі блокчейну: виявлено, що більшість літератури про розподілене управління ідентифікацією на основі блокчейну є теоретичною та концептуальною, а не емпіричною та практичною. У документі також йдеться про відсутність консенсусу щодо визначень, концепцій та стандартів розподіленого управління ідентифікацією на основі блокчейну, а також про розмаїття підходів та платформ для його реалізації;
- переваги розподіленого управління ідентифікацією на основі блокчейну, такі як посилений контроль над користувачами, конфіденційність, безпеку та інтероперабельність. У документі також зазначається, що розподілене управління ідентифікацією може уможливити нові додатки та послуги, такі як самоуверенна ідентичність (SSI), облікові дані, які можна перевірити (VC), та докази з нульовим рівнем розголошення (ZKP);
- бар'єри на шляху до розподіленого управління ідентичністю: зазначається низка технічних і соціальних проблем, які перешкоджають його прийняттю та впровадженню, таких як масштабованість, продуктивність, зручність використання, сумісність, регулювання, управління та довіра. У документі також підкреслюється вимога до зміни парадигми та культурних змін у тому, як люди та організації сприймають та управляють своїми цифровими ідентичностями.

В цілому у статті розкривається багатообіцяючий, але незрілий стан розподіленого управління ідентифікацією на основі блокчейну і ставиться під сумнів його практичність в організаційному контексті. Пропонується також

дослідницька модель для подальшого вивчення та оцінки потенціалу децентралізованого управління ідентичностями в організаціях.

В сучасному цифровому ландшафті можна виділити наступні типи цифрової ідентичності.

Централізована ідентичність. Централізована ідентичність видається та підтверджується централізованим органом або стороннім постачальником послуг, таким як, до прикладу, Amazon, з певною метою [36, 37, 38]. Централізована ідентичність надає більше повноважень органу, який її видає, ніж особам, пов'язаним з цією ідентичністю. Центральний орган може заперечити ідентичність особи або підтвердити фальшиву ідентичність. Крім того, централізована ідентичність тягне за собою балканізацію (ділення) ідентичності, оскільки користувачі змушені створювати окремі ідентичності для різних веб-сайтів та онлайн-сервісів. Централізована ідентичність поширюється в сучасному Інтернеті. Це призвело до того, що користувачі змушені підтримувати кілька облікових даних, не маючи повного контролю над ними.

Федеративна ідентичність. Федеративна ідентичність - це централізована ідентичність, яка дозволяє користувачам використовувати одні й ті самі облікові дані для доступу до кількох цифрових сервісів у межах федерації за допомогою служб єдиного входу. Наприклад, дані облікового запису Google можна використовувати для входу в інші сервіси, такі як YouTube, Gmail і Google Docs, Facebook та ін., а також при реєстрації на різних сайтах. Федеративна ідентичність зменшує проблему балканізації ідентичності; однак контроль над ідентичністю залишається за федерацією, а не за окремою особою.

Ідентичність, орієнтована на користувача. Інший тип централізованої ідентичності, орієнтованої на користувача, делегує більший контроль над цифровою ідентичністю окремим користувачам. Користувацька ідентичність видається службою цифрової ідентичності, такою як OpenID [39] або OAuth [40]. Вона дозволяє користувачам самостійно керувати та підтримувати свою ідентичність. Користувачі можуть уповноважити ці сервіси підтверджувати їхню особу іншим третім особам без розкриття конфіденційної інформації

користувачів. Орієнтована на користувача ідентичність забезпечує більшу мобільність. Проте, вона не надає користувачеві повного контролю, оскільки право власності та контроль над цифровою ідентичністю користувача залишається за централізованим постачальником послуг.

Розподілена ідентичність. Розподілена ідентичність - це цифрова ідентичність, яка управляється через мережу рівноправних вузлів [41]. У цьому випадку ідентифікація, авторизація та права доступу делегуються через спільноту осіб або вузлів (наприклад, соціальну мережу або федерацію організацій). Учасники розподіленої системи ідентифікації вважаються рівними, при цьому будь-який з них виступає емітентом цифрової ідентичності, яка може бути використана для доступу до послуг, що пропонуються іншими учасниками [42]. Крім того, верифікація є локальною (між двома вузлами). Третя сторона не може відстежити використання цифрової ідентичності [43].

Децентралізована ідентичність. Децентралізована ідентичність дає користувачеві повний контроль над своєю цифровою ідентичністю. Вона є повністю автономною і відокремленою від будь-якого централізованого органу, що видає цифрову ідентичність або керує нею. Централізований орган часто несе відповідальність за те, що наражає користувачів на ризик витоку даних, зловживання ідентифікаційними даними та крадіжки ідентичностей. Без цього користувачі можуть отримати суверенітет над своєю цифровою ідентичністю [38].

Самосуверенна ідентичність. Децентралізована ідентичність на блокчейні називається самосуверенною ідентичністю [44] (self-sovereign identity) або ССІ (SSI) [45]. ССІ використовує децентралізовані, розподілені системи управління ідентифікацією, щоб дозволити користувачеві існувати незалежно від сервісу [46]. Тут децентралізація означає усунення центрального органу управління ідентифікацією. Розподіл означає дублювання або використання точної копії ідентичності користувача у всіх компонентах системи управління ідентифікацією [47]. У цьому випадку користувач зберігає свою цифрову

ідентичність у захищеному сховищі даних, наприклад, у цифровому гаманці. Його використовують для підтвердження особи легітимним верифікатором.

Керівні принципи CCI, запропоновані Алленом [37], можна класифікувати за такими аспектами, як безпека, контрольованість і портативність. Вимір безпеки вимагає, щоб система управління CCI забезпечувала постійну цифрову ідентичність користувача, оскільки вона мінімізує витік даних і захищає права користувача. Будь-які дані цього користувача повинні поширюватися за його згодою. Вимір портативності означає, що цифрову ідентичність можна перенести в іншу систему. Це гарантує, що користувач зберігає доступ і контроль над своєю ідентичністю та даними. Крім того, система повинна працювати та керувати ідентифікацією у повністю прозорий спосіб.

Можемо виділити основні задачі, які вирішують децентралізовані системі на основі блокчейну в контексті цифрової ідентифікації:

Підвищення цілісності та прозорості даних. Незмінна природа блокчейну забезпечує цілісність даних, що зберігаються в реєстрі. Як тільки транзакція записана, вона стає практично захищеною від несанкціонованого втручання, забезпечуючи перевірку та аудит історії подій. У системах підтримки прийняття рішень ця властивість може підвищити цілісність і прозорість даних, дозволяючи зацікавленим сторонам відстежувати походження і достовірність інформації. Незмінні записи також знижують ризик маніпуляцій з даними або шахрайства, сприяючи зміцненню довіри між учасниками [15].

Децентралізація та розподілений консенсус. Блокчейн працює в децентралізованій мережі, що усуває потребу в центральному органі або посереднику. Перевагою систем підтримки прийняття рішень, заснованих на блокчейні, від традиційних, буде забезпечення рівноправної (peer-to-peer) взаємодії та усунення єдиних точок відмови. Завдяки алгоритмам розподіленого консенсусу, таким як доказ виконання роботи (PoW) або доказ частки (PoS), блокчейн забезпечує згоду щодо стану реєстру, сприяючи довірі та зменшуючи залежність від централізованих органів, що приймають рішення [1].

Підвищення безпеки та захисту даних. Технологія блокчейн використовує криптографічні методи для захисту даних і транзакцій. Кожна транзакція криптографічно пов'язана з попередньою, утворюючи ланцюжок блоків [1]. Така структура в поєднанні з механізмами консенсусу надзвичайно ускладнює зловмисникам будь-яку зміну або маніпуляції з даними. Крім того, контрольовані користувачем цифрові підписи та приватні ключі забезпечують надійну автентифікацію, захищаючи конфіденційну інформацію від несанкціонованого доступу. Такі функції блокчейну можуть посилити безпеку і конфіденційність в системах.

Ефективність та автоматизація. Усуваючи посередників і оптимізуючи процеси, системи на основі блокчейну можуть підвищити ефективність і знизити операційні витрати. Смарт-контракти - програмовані угоди, що виконуються на блокчейні - автоматизують і забезпечують виконання заздалегідь визначених правил і умов, усуваючи необхідність ручного втручання. Така автоматизація може прискорити процеси прийняття рішень, зменшити паперовий документообіг і мінімізувати помилки або затримки, спричинені людським фактором [33].

1.6 Висновок до розділу 1

Таким чином, огляд літератури охоплює широкий спектр досліджень, які в сукупності висвітлюють багатогранний ландшафт технології блокчейн, децентралізованої ідентифікації та цифрових ідентичностей. Від теоретичних засад суверенної ідентичності до реальних застосувань і викликів - література відображає всебічне дослідження трансформаційного потенціалу блокчейну в зміні нашого сприйняття та управління цифровими ідентичностями.

У розділі було представлено огляд технології блокчейн, її класифікації, висвітлено фундаментальні концепції та характеристики, а саме децентралізація, незмінність, простежуваність, прозорість та механізм консенсусу. Було

досліджено варіанти використання та сфери застосування, до яких увійшли фінансовий сектор, перевірка цілісності, державне управління, інтернет речей, охорона здоров'я, конфіденційність і безпека, освіта, управління даними.

Було проаналізовано потенційні переваги блокчейну в системах підтримки прийняття рішень та акцентовано увагу на таких аспектах як підвищення цілісності та прозорості даних, децентралізація, безпека та захист даних, підвищення ефективності та автоматизація процесів. Було розглянуто концепт цифрової ідентичності да методи управління цифровою ідентичністю, виділено та проаналізовано типи цифрової ідентичності, такі як централізована, федеративна, децентралізована, розподілена та самосуверенна. Було досліджено, як технологія блокчейн може змінити традиційні системи управління ідентифікацією, підкреслено переваги розподіленого управління ідентифікацією на основі блокчейну, такі як посилений контроль над користувачами, конфіденційність, безпеку та інтероперабельність. Було окреслено основні задачі, які вирішують децентралізовані системі на основі блокчейну в контексті цифрової ідентифікації, такі як підвищення цілісності та прозорості даних, децентралізація та розподілений консенсус, підвищення безпеки та захисту даних, ефективність та автоматизація. Також було проаналізовано виклики на шляху до впровадження розподіленого управління ідентифікацією, підкреслено низку технічних і соціальних проблем, які перешкоджають його прийняттю та впровадженню, такі як масштабованість, продуктивність, зручність використання, сумісність, регулювання, управління та довіра.

Загалом, вивчення технології блокчейн та її застосування відкриває нові можливості для безпечного та прозорого прийняття рішень, прокладаючи шлях до реформування та створення більш ефективних та надійних систем у широкому спектрі галузей.

2 МЕТОДИ ДОСЛІДЖЕННЯ ТА ВИРІШЕННЯ ПРОБЛЕМИ

Система управління цифровою ідентифікацією в децентралізованих спільнотах наразі стикається зі значними викликами, починаючи від потенційних вразливостей у процесах верифікації особи і закінчуючи питаннями, пов'язаними з конфіденційністю користувачів та безпекою даних. В існуючих системах може бракувати надійності, щоб протистояти загрозам у цифровому середовищі, що постійно змінюються. Крім того, централізований характер систем управління ідентифікацією може створювати обмеження з точки зору масштабованості та контролю над користувачами. Вирішення цих проблем має вирішальне значення для забезпечення цілісності та надійності цифрової ідентичності [47]. Робота має на меті дослідити проблему верифікації осіб в децентралізованих спільнотах, та запропонувати децентралізоване рішення, яке не лише пом'якшить існуючі виклики, але й відповідатиме принципам безпеки та прозорості.

2.1 Порівняльний аналіз методів децентралізованої ідентифікації

Діапазон децентралізованих методів перевірки особи є різноманітним і швидко розвивається, представляючи спектр інноваційних рішень для вирішення проблем, пов'язаних з традиційним управлінням ідентифікаційними даними. У цьому підрозділі буде зроблений порівняльний аналіз різних децентралізованих методів ідентифікації. Вивчаючи сильні та слабкі сторони, а також унікальні особливості різних підходів, я прагну виявити ідеї, які сприятимуть розробці оптимізованої системи верифікації для децентралізованих спільнот.

У сфері децентралізованої перевірки ідентичності з'явилися різні інноваційні методи для захисту та автентифікації ідентичності користувачів у цифрових екосистемах. Один із найпоширеніших підходів передбачає

використання невзаємозамінних токенів (NFT) [50], де володіння певним NFT слугує унікальним ідентифікатором, що прив'язує особу до її цифрової ідентичності. Цей метод забезпечує стійкий до підробок і перевірений спосіб встановлення права власності та контролю над ідентифікацією особи.

Інший шлях - використання токенів ERC20 [51], де володіння визначеним токеном стає критерієм валідації. Цей підхід, орієнтований на токени, пропонує гнучкість і може бути адаптований до конкретних вимог, пов'язуючи ідентифікацію з володінням заздалегідь визначеним цифровим активом.

Soulbound токени (SBT) [52] - різновид NFT-активу, який випускається в єдиному екземплярі і назавжди прив'язується до однієї блокчейн-адреси, представляють нову концепцію, створюючи нерозривний зв'язок між токеном і його власником, підвищуючи безпеку і забезпечуючи міцний зв'язок між цифровою ідентичністю і пов'язаним з нею токеном.

Крім того, метод "членства в контрактах", прикладом якого є попередньо дозволені (у білому списку) адреси, встановлює особу через членство в конкретному смарт-контракті [53], пропонуючи універсальний засіб для контролю доступу та перевірки особи на основі попередньо визначених критеріїв.

Отримання децентралізованого ідентифікатору (DID) [54] від надійного провайдера є окремим методом перевірки в умовах децентралізованої ідентифікації. За такого підходу особи отримують свої унікальні DID - цифрові ідентифікатори, засновані на технологіях децентралізованих і розподілених реєстрів. Ці провайдери використовують блокчейн або інші децентралізовані протоколи для безпечного створення та управління DID. Користувачі можуть надавати ці DID як доказ своєї ідентичності на різних платформах і в різних додатках, який можна перевірити. Цей метод пропонує зручний і стандартизований спосіб взаємодії з ідентичністю, що дозволяє людям покладатися на довірені організації для видачі та управління своїми DID.

Кожен з цих підходів пропонує унікальні переваги, що підкреслює важливість детального розуміння їхніх індивідуальних особливостей. Таке

розуміння відіграє ключову роль у створенні децентралізованої системи підтвердження особи, яка буде не лише стійкою та адаптивною, але й відповідатиме специфічним потребам децентралізованих громад.

2.2 Порівняльний аналіз провайдерів децентралізованої верифікації

Даний аналіз заглиблюється в технологічні нюанси, протоколи безпеки та аспекти використання та впровадження різних рішень [55]. Мета полягає в тому, щоб отримати інформацію, яка може бути використана при виборі та потенційній інтеграції інструменту з верифікації в децентралізованих спільнотах та UkraineDAO.

1. Sovrin - глобальна утиліта для самосуверенної ідентичності, яка дозволяє користувачам створювати та керувати власними цифровими ідентифікаторами та обліковими даними, не залежачи від будь-якого центрального органу влади чи посередника. Sovrin використовує мережу блокчейн, засновану на Hyperledger Indy, для зберігання і перевірки децентралізованих ідентифікаторів (DID) і верифікованих облікових даних (VC). Sovrin також має власний токен, який забезпечує економічні стимули для учасників мережі та дозволяє здійснювати обмін цінностями та мікроплатежі із збереженням конфіденційності [4].
2. Civic - децентралізована екосистема ідентифікації, яка об'єднує власників ідентифікаційних даних, валідаторів та постачальників послуг і забезпечує безпечну та конфіденційну перевірку ідентичності. Civic використовує блокчейн Ethereum для зберігання та управління DID та VC, а також використовує біометричну автентифікацію та ZKP для підвищення безпеки та конфіденційності. Civic також має власний токен CVC, який використовується для стимулювання перевірки особи та доступу до послуг, пов'язаних з ідентифікацією [60].

3. Stripe Identity - децентралізований інструмент ідентифікації, який дозволяє перевірити справжність ідентифікаційних документів. Це один з популярних децентралізованих інструментів ідентифікації, який допомагає в програмному підтвердженні ідентичності користувачів для запобігання шахрайству. Рішення Stripe Identity допомагає розробникам підтримувати правила KYC та виявляти підроблені ідентифікатори за допомогою машинного навчання [61].
4. Jolocom - децентралізований протокол ідентифікації, який дозволяє користувачам створювати і контролювати власну цифрову ідентичність, а також використовувати її для взаємодії з різними додатками і платформами [62]. Jolocom використовує DID та VC для представлення та обміну ідентифікаційними даними, а також підтримує ZKP та шифрування для забезпечення конфіденційності та безпеки. Jolocom може працювати з будь-яким блокчейном, який підтримує DID, наприклад, Ethereum, Bitcoin або Hyperledger, блокчейн мережі другого рівня [63].
5. Nametag. - інструмент ідентифікації, який підходить для децентралізованих соціальних мереж. Він може слугувати децентралізованим профілем у соціальних мережах для користувачів, що може допомогти у з'єднанні облікових записів сервісів web3 та web2. Профіль Nametag може допомогти з'єднати кілька гаманців у різних мережах і створити власну галерею. В подальшому користувач може перенести профіль у популярні додатки, такі як YouTube, Discord і Twitter. Крім того, користувач також може перенести свій профіль у web3-ігри, метаплатформи та додатки на основі блокчейну. Nametag використовує блокчейн Ethereum для зберігання і перевірки DID і VC, а також використовує IPFS і OrbitDB для зберігання ідентифікаційних даних поза ланцюжком [64].
6. SelfKey - децентралізована мережа ідентифікації, яка дозволяє користувачам володіти, контролювати і управляти своєю цифровою ідентичністю, а також отримувати доступ до різних послуг і продуктів,

таких як фінансові, імміграційні та криптовалютні сервіси. SelfKey використовує блокчейн Ethereum для зберігання і перевірки DID і VC, а також надає цифровий гаманець і ринок для послуг, пов'язаних з ідентифікацією. SelfKey також має власний токен KEY, який використовується для доступу до мережі та оплати послуг [65].

7. Fractal ID. Fractal є популярним інструментом DID, який слугує постачальником криптографічних ідентифікаторів. Він має майже 1 мільйон багаторазових підтверджених ідентичностей, а також понад 160 додатків, що використовують цей інструмент. Платформа пропонує можливість підключення для різних випадків використання, пов'язаних з комплаєнсом, таких як KYC-перевірки або KYB-верифікація. Крім того, рішення Fractal допомагає перевіряти відповідність користувачів вимогам для участі в певних заходах, таких як участь у криптовалютних іграх або роздачі токенів спільноті проектів (crypto airdrop). Fractal використовує блокчейн Polkadot для зберігання і перевірки DID і VC, а також надає токен FCL для обміну активами і стимулювання участі на платформі [66].
8. Blockstack - децентралізована обчислювальна мережа і екосистема додатків, яка дозволяє користувачам створювати і контролювати власну цифрову ідентичність і використовувати її для доступу до різних децентралізованих додатків (dApps). Blockstack використовує блокчейн Bitcoin для зберігання та захисту DID та VC, а також інтегрується з Gaia, децентралізованою системою зберігання даних, щоб зберігати ідентифікаційні дані поза ланцюжком. Blockstack також має власний токен STX, який використовується для реєстрації DID та виконання смарт-контрактів у мережі [67].
9. Polygon ID. Створений командою, що стоїть за блокчейном Polygon, Polygon ID є децентралізованим інструментом ідентифікації з перевагами програмованої конфіденційності. В результаті користувачі можуть взаємодіяти з різними web3-сервісами на свій вибір у децентралізований спосіб, орієнтований на конфіденційність. Polygon ID також використовує

технологію zk-SNARK для полегшення криптографічного захисту, а також використовує IPFS і OrbitDB для зберігання ідентифікаційних даних поза ланцюжком [68].

10. Veres One - децентралізована мережа ідентифікації, яка дозволяє користувачам створювати та керувати власною цифровою ідентичністю, а також використовувати її для доступу до різних послуг та платформ. Veres One використовує DID та VC для представлення та обміну ідентифікаційними даними, а також підтримує ZKP та шифрування для забезпечення конфіденційності та безпеки. Veres One використовує консорціумний блокчейн, заснований на протоколі Sidetree, для зберігання і перевірки DID і VC, а також використовує протокол Interledger для забезпечення міжмережевої взаємодії [69].
11. KYCDAO. - інструмент для впровадження комплаєнс-сервісів на базі web3. Він працює як багатоланцюгова платформа для видачі багаторазових та внутрішньоланцюгових KYC-перевірок. KYC NFT на DAO можуть запропонувати надійний підхід для перевірки особи в різних сценаріях використання, таких як перевірка засновників, збір коштів, інвестиції та управління. Користувачі також можуть карбувати KYC NFT для декількох гаманців, підтверджуючи право власності на різні гаманці. KYCDAO використовує блокчейн Ethereum для зберігання і перевірки DID і VC, а також надає токен KYC для обміну цінностями і стимулювання участі на платформі [70].
12. Ontology ID. Ontology - це високопродуктивний публічний блокчейн і розподілена платформа для спільної роботи, яка підтримує різні децентралізовані рішення для ідентифікації, такі як ONT ID, ONT Pass і ONT Auth. Ontology використовує DID і VC для створення та обміну ідентифікаційними даними, а також підтримує ZKP і шифрування для забезпечення конфіденційності та безпеки. Ontology має власний токен ONT, який використовується для доступу до мережі та оплати послуг [71].

13. Disco. Disco пропонує інструмент децентралізованої ідентифікації з діагностикою ланцюгів і використовує децентралізовані ідентифікатори (DID) разом з VC (verifiable credentials), для володіння даними. Платформа працює шляхом групування персоналізованих даних користувачів, якими користувачі можуть поділитися з верифікаторами. Disco використовує блокчейн Ethereum для зберігання і перевірки DID і VC, а також використовує IPFS і OrbitDB для зберігання ідентифікаційних даних поза ланцюжком [72].
14. Evernym - децентралізована платформа ідентифікації, яка дозволяє користувачам створювати та керувати власною цифровою ідентичністю, а також використовувати її для доступу до різних сервісів та платформ. Evernym використовує мережу та протокол Sovrin для зберігання та перевірки DID та VC, а також використовує ZKP та шифрування для забезпечення конфіденційності та безпеки. Evernym також надає набір інструментів і сервісів, таких як Connect.Me, Verity і Accelerator, які допомагають користувачам і організаціям впроваджувати децентралізовані ідентифікаційні рішення [73].
15. Spruce. Spruce ID - один з найвідоміших провайдер DID, який пропонує колекцію інструментів з відкритим вихідним кодом. Репутація Spruce як одного з популярних провайдерів децентралізованої ідентифікації підтверджується наявністю багатьох інструментів децентралізованої ідентифікації в екосистемі. Деякі з відомих інструментів, доступних на Spruce, включають криптографічні облікові дані для соціальних мереж і гаманці на основі облікових даних. Платформа має на меті надати користувачам можливість контролювати свої дані за допомогою децентралізованих ідентифікаторів, таких як адреси гаманців Ethereum. Spruce є блокчейн-агностичним, тобто може працювати з будь-яким блокчейном, що підтримує DID, таким як Ethereum, Tezos або Bitcoin [74].
16. Microsoft ION - децентралізована мережа ідентичності, яка дозволяє користувачам створювати та керувати власною цифровою ідентичністю, а

також використовувати її для доступу до різних сервісів та платформ. Microsoft ION використовує DID та VC для представлення та обміну ідентифікаційними даними, а також підтримує ZKP та шифрування для забезпечення конфіденційності та безпеки. Microsoft ION використовує рішення другого рівня, засноване на протоколі Sidetree, для зберігання і перевірки DID і VC в блокчейні Bitcoin, а також використовує протокол Interledger для забезпечення сумісності між різними блокчейнами [75].

17. Galxe ID. Galxe пропонує доступну інфраструктуру облікових даних побудовану на Ethereum для web3 розробників. Платформа створює мережу облікових даних, яка може задовольнити вимоги як онлайн, так і офлайн спільнот. Мережеві облікові дані Galxe використовують статичні знімки або запити до підграфів. З іншого боку, Galxe використовує джерела даних з різних організацій, таких як Github, Snapshot і Twitter [76].
18. Shyft Network - це децентралізована платформа ідентичності та даних, яка дозволяє користувачам створювати та керувати власною цифровою ідентичністю, а також використовувати її для доступу до різних сервісів та платформ, особливо у фінансовому секторі. Shyft Network використовує DID та VC для створення та обміну ідентифікаційними даними, а також підтримує ZKP та шифрування для забезпечення конфіденційності та безпеки. Shyft Network використовує блокчейн, заснований на Parity Substrate, для зберігання і перевірки DID і VC, а також надає токен SHFT для обміну цінностями і стимулювання участі в мережі [77].
19. Bright ID. Bright ID є багатообіцяючим прикладом інструментів DID, спрямованих на майбутнє web3. Це соціальна мережа ідентифікації, яка намагається застосувати нові підходи до верифікації особистості в соціальних мережах. Bright ID використовує децентралізовану технологію з відкритим вихідним кодом, допомагаючи користувачам довести, що вони не використовують кілька акаунтів у соціальних мережах. Bright ID створює доказ унікальної ідентичності, розробляючи та аналізуючи соціальний граф використовуючи технологію доказу з нульовим

розголошенням (ZKP) для забезпечення конфіденційності та безпеки. BrightID також надає набір інструментів і послуг, таких як BrightID Node, BrightID App і BrightID Sponsorship, щоб допомогти користувачам і організаціям прийняти і впровадити децентралізовані рішення для ідентифікації [78].

20. Dfinity Internet Identity. Децентралізована служба ідентифікації, яка дозволяє користувачам створювати та керувати власною цифровою ідентичністю, а також використовувати її для доступу до різних додатків і платформ, децентралізованій мережі хмарних обчислень [79]. Dfinity Internet Identity використовує DID та VC для створення та обміну ідентифікаційними даними, а також підтримує шифрування та біометричну автентифікацію для забезпечення конфіденційності та безпеки. Dfinity Internet Identity використовує блокчейн Internet Computer [80] для зберігання та перевірки DID та VC, а також використовує API веб-аутентифікації для забезпечення безперешкодного входу та доступу.
21. HashKey DID. Мультичейн (підтримує декілька блокчейнів) децентралізований агрегатор ідентифікаційних даних, що працює на основі смарт-контрактів, NFT і децентралізованого протоколу захисту конфіденційності для надання ідентифікаційних послуг користувачам Web3. Стек технологій, що лежить в основі HashKey DID, інтегрує надійні децентралізовані протоколи, надаючи користувачам підвищений контроль над своїми ідентифікаційними даними та зменшуючи залежність від централізованих організацій. HashKey DID використовує криптографічні методи для забезпечення конфіденційної обробки особистої інформації, що дозволяє безперешкодно перевіряти особу [81].
22. Spherity - децентралізована платформа ідентичності та даних, яка дозволяє користувачам та організаціям створювати та керувати власною цифровою ідентичністю, а також використовувати її для доступу до сервісів та платформ. Spherity використовує DID та VC для створення та обміну ідентифікаційними даними, а також підтримує шифрування та контроль

доступу для забезпечення конфіденційності та безпеки. Spherity є блокчейн-агностичним, тобто може працювати з будь-яким блокчейном, що підтримує DID, наприклад, Ethereum, Hyperledger або EOS [82].

23. xHashtag - протокол для репутації в web3. У світі web3 репутація в мережі є життєво важливою, і її потрібно підтверджувати за допомогою облікових даних. xHashtag слугує ефективним рішенням для накопичення та отримання облікових даних в мережі. Доменне ім'я ".soul" допомагає представляти докази діяльності користувачів в мережі за допомогою soulbound NFT. Використовуючи репутаційні облікові дані, особи можуть динамічно збирати кваліфіковані ліквідні команди, а користувачі можуть будувати свою репутацію в Web3 і заробляти в обмін на створення цінності [83].
24. zCloak Network. Мережа zCloak пропонує інструмент zkID Login, щоб допомогти користувачам отримати більш чіткий, швидкий і приватний механізм для входу в сервіси. zCloak Network - це DID-інфраструктура, орієнтована на конфіденційність і перевірену обчислювальну інфраструктуру. Вона спрямована на реалізацію цілей Web3 про самосуверенність шляхом переносу зберігання та обчислення даних користувача з централізованих серверів на пристрої користувача [84].
25. Violet - комплексна платформа для управління ідентифікацією та відповідністю нормативним вимогам. Violet використовує технологію доведення з нульовим розголошенням для забезпечення конфіденційності для користувачів. У той же час, безперебійні системи зберігання даних офчейн гарантують безпеку даних користувачів [85].
26. Iden3 - це система контролю доступу нового покоління, заснована на самосуверенній ідентичності (SSI) та розроблена для децентралізованих середовищ з низьким рівнем довіри. Основна ідея протоколу полягає в тому, що кожна SSI ідентичність може висувати запити до іншої ідентичності (яка може стосуватися особи, організації або системи/машини) [86]. Проста і унікальна характеристика може призвести

до створення складних адаптивних систем та різноманітних варіантів використання: децентралізовані моделі довіри, підтвердження особи, системи голосування, автентифікація та авторизація, приватний контроль доступу та ін.

Завершуючи порівняльний аналіз інструментів ідентифікації, оцінка охоплює спектр рішень, кожне з яких має свої унікальні особливості та можливості. Від відомих платформ, таких як Stripe Identity і Nametag, до нових гравців, таких як Disco. Помітні інновації, такі як соціальний підхід в Bright ID, та рішення на основі блокчейну, такі як HashKey DID і Polygon ID, Fractal ID, підкреслюють динамічний характер екосистеми децентралізованої ідентичності. Цей аналіз проливає світло на сильні сторони та потенційні міркування, пов'язані з кожним інструментом, надаючи інформацію для подальшого впровадження децентралізованої системи верифікації для спільнот. Розмаїття розглянутих інструментів свідчить про постійний розвиток та експерименти у сфері децентралізованої ідентичності, підкреслюючи важливість вибору, узгодженого з конкретними випадками використання та вимогами.

2.3 Об’єкт дослідження - UkraineDAO

UkraineDAO - це онлайн-спільнота, створена Альоною Шевченко, Trippy Labs та учасниками PleasrDAO за кілька днів до повномасштабного вторгнення Росії в Україну, для фінансування військових потреб в Україні. Оскільки конфлікт триває вже другий рік, криптовалюта продовжує залишатися важливим джерелом допомоги. За даними аналітичної компанії Elliptic, що займається блокчейн-аналітикою, станом на березень 2023 року на проукраїнські військові цілі було пожертвувано криптовалюти на суму понад 212 мільйонів доларів США, з яких близько 80 мільйонів доларів США було виділено уряду України. Як повідомляється, кошти, пожертвувані в криптовалюті, були використані для придбання широкого спектру товарів - від бронежилетів і шоломів до медичних засобів і радіостанцій. [56]

UkraineDAO - що використовує асоціативну модель (концепція, коли елементи чи об'єкти пов'язані між собою на основі асоціацій, зв'язків або спільних характеристик), засновану на спільноті, спрямовану на збір і подальшу передачу коштів на проукраїнські цілі з конкретною метою. На сьогоднішній день UkraineDAO, яка була створена, за словами Альони Шевченко, для використання "потужності технологій і спільноти Web3 для захисту України", пожертвувала близько 7 мільйонів доларів США в криптовалюті [56]. Окрім надання коштів, UkraineDAO повідомляє, що також працює над підвищенням медіаграмотності як засобом боротьби з дезінформаційними кампаніями. Крім того, у партнерстві зі Starling Labs, UkraineDAO запустила проект "Доказ" для документування російських воєнних злочинів в Україні та передачі зібраних доказів до Міжнародного кримінального суду [57].

Управління та структура UkraineDAO ґрунтуються на принципах децентралізації, прозорості та участі. Сама структура складається з трьох основних компонентів: смарт-контракту, веб-сайту та спільноти. В спільноті використовується блокчейн Ethereum та смарт-контракти для зберігання та

управління своїми коштами та операціями, а також для забезпечення демократичного прийняття рішень своїми членами. DAO використовує мультипідписний гаманець з трьома з п'яти підписантів, необхідних для схвалення будь-якої транзакції. До підписантів належать [87]:

1. Альона Шевченко - співзасновниця та лідерка спільноти в Україні, співорганізаторка Kyiv Tech Summit.
2. Діма Бутерін - філософ, програміст, підприємець. Батько Віталіка Бутеріна - засновника проєкту Ethereum.
3. Естебан Хопенгайн (Стів) - співзасновник UkraineDAO та фінансовий директор PleasrDAO.
4. Метью Бандей - співзасновник та старший інженер PleasrDAO, оператор валідатора OG ETH, двічі технічний директор стартапу Xoogler. Допомагав заснувати і запустити FreeRossDAO.
5. Ітцель Ярд - співзасновниця Creative Code Art та найбільш продавана художниця NFT.

Веб-сайт DAO - це інтерфейс організації, де члени та прихильники можуть отримати доступ до інформації, робити пожертви, купувати NFT, а також взаємодіяти один з одним. Спільнота DAO - це дух організації, де члени та прихильники можуть спілкуватися, співпрацювати та координувати свої дії та ініціативи, використовуючи різні платформи, такі як Discord, Twitter та Telegram.

DAO організована в кілька робочих груп, які зосереджені на різних напрямках, таких як перевірка фактів і медіаграмотність, правові ресурси та психічне здоров'я [58]. Організація продовжує балансувати між потребою бути прозорою, пропонуючи метрики підзвітності, та необхідністю захистити своїх донорів від "доксингу". Спільнота є відкритою, але її члени потребують перевірки з огляду на чутливість операцій з надання допомоги постраждалим від війни.

UkraineDAO як і більшість децентралізованих спільнот використовує Discord для комунікації та координації. На сервері Discord людям призначаються ролі на основі їхньої кваліфікації. Ці ролі по суті дають дозвіл на виконання

певних дій на сервері (наприклад, запрошення, переміщення, видалення, заборона або зміна ролей учасників; створення нових каналів, розміщення повідомлень в каналах з обмеженим доступом) і надання доступу до відповідних матеріалів відповідно до призначеної функції. Це робиться за допомогою функції "тегів" в Discord. Власник сервера може вирішувати, які мітки повинні існувати, і що їх наявність має розблокувати користувачів, які ними володіють. Так, наприклад, якщо користувач є членом, наприклад, групи зі збору коштів або перекладу в UkraineDAO, він отримає відповідний тег, який надасть доступ до каналів та інформації, що стосуються саме цих напрямів. Це гарантує, що люди мають все необхідне для виконання своїх функцій, не перевантажуючи їх усією доступною інформацією. Крім того, ролі забезпечують візуальну та побудовану ієрархію, що полегшує залучення нових людей та допомагає їм зрозуміти, наприклад, до кого звертатися щодо інтерв'ю, блокчейну чи перекладу українських текстів [59].

Проте, процес приєднання нових користувачів до децентралізованих спільнот, включно з такими організаціями, як UkraineDAO, створює значну проблему, а саме - попередню верифікацію користувачів. У децентралізованих екосистемах, де взаємодія користувачів регулюється принципами автономії та розширення прав і можливостей користувачів, створення надійних і безпечних засобів перевірки особистих даних перед наданням доступу стає ключовим питанням. Відсутність централізованого органу, який би контролював цей процес, вимагає рішень, які б гарантували, що нові користувачі, які приєднуються до цих спільнот, є легітимними та реальними людьми і відповідають визначеним критеріям. Тонкощі попередньої верифікації є критичним моментом у розробці децентралізованих систем управління ідентичністю, що вимагає розгляду і стратегічних рішень для підтримки цілісності таких спільнот при дотриманні принципів децентралізації.

2.4 Висновок до розділу 2

У розділі було представлено порівняльний аналіз методів децентралізованої ідентифікації. Були розглянуті особливості методів перевірки особи, від NFT і токенів ERC20 до отримання DID від провайдерів, розкриваючи тонкощі і потенційні можливості кожного з них. Також було зроблено порівняльну характеристику провайдерів управління цифровою ідентичністю, продемонструвавши різноманітність існуючих інструментів, таких як Stripe Identity, BrightID, Polygon ID, Nametag та інші.

Однією з проблем, яка була виявлена, є верифікація нових користувачів у децентралізованих спільнотах на прикладі UkraineDAO. Це складний баланс між тим, щоб переконатися, що люди є тими, за кого себе видають, і водночас поважати конфіденційність та децентралізований дух.

У наступному розділі буде представлене рішення для децентралізованої системи верифікації, яка відповідатиме потребам децентралізованих спільнот - безпечної, зручної для користувачів і такої, що відповідає безпосередньо принципам децентралізації.

3 ВИРІШЕННЯ ПРОБЛЕМИ

Для вирішення проблеми попередньої верифікації нових користувачів було обрано рішення інтегрувати процедуру отримання децентралізованого ідентифікатору (DID) від провайдера BrightID в систему онбордингу через Discord. BrightID, децентралізоване рішення для ідентифікації особи, вирізняється парадигмою соціальної верифікації, що робить його особливо придатним для попередньої верифікації нових користувачів у децентралізованих спільнотах. Його підхід полягає в аналізі соціальних графів, що спирається на зв'язки і свідчення існуючих членів для встановлення надійності нових учасників [78]. Цей механізм узгоджується з етикою децентралізованих екосистем, наголошуючи на перевірці користувачами, а не на централізованому органі. Використовуючи механізм консенсусу, сформований всередині спільноти, BrightID вирішує проблему приєднання нових членів, зосереджуючись на інклюзивності та довірі користувачів. Його впровадження не лише зміцнює цілісність цифрових ідентичностей, але й активно залучає спільноту до процесу валідації, сприяючи формуванню почуття колективної відповідальності та довіри в рамках децентралізованих платформ.

Демонстрація імплементації складатиметься з наступних етапів:

1. Створення тестового серверу спільноти в Discord.
2. Додавання каналу “verify” на сервері, в якому будуть верифікуватися користувачі.
3. Додавання Bright ID Discord Bot до серверу.
4. Приєднання нового користувача до спільноти в Discord.
5. Реєстрація користувача в екосистемі BrightID.
6. Верифікація користувача в екосистемі BrightID.
7. Верифікація користувача в спільноті Discord через Bright ID Discord Bot.

3.1 Створення тестового серверу спільноти в Discord.

Discord - це онлайн-платформа, яка пропонує послуги голосового, відео та текстового зв'язку для різних спільнот, таких як ігрові, освітні та соціальні групи. Discord дозволяє користувачам створювати або приєднуватися до серверів, які по суті є приватними або публічними чатами з різними каналами та функціями [88].

Для створення тестового серверу потрібно спочатку створити обліковий запис в системі шляхом завантаження додатку на комп'ютер, мобільний пристрій на операційній системі Android або iOS, або через браузер, та пройти реєстрацію.

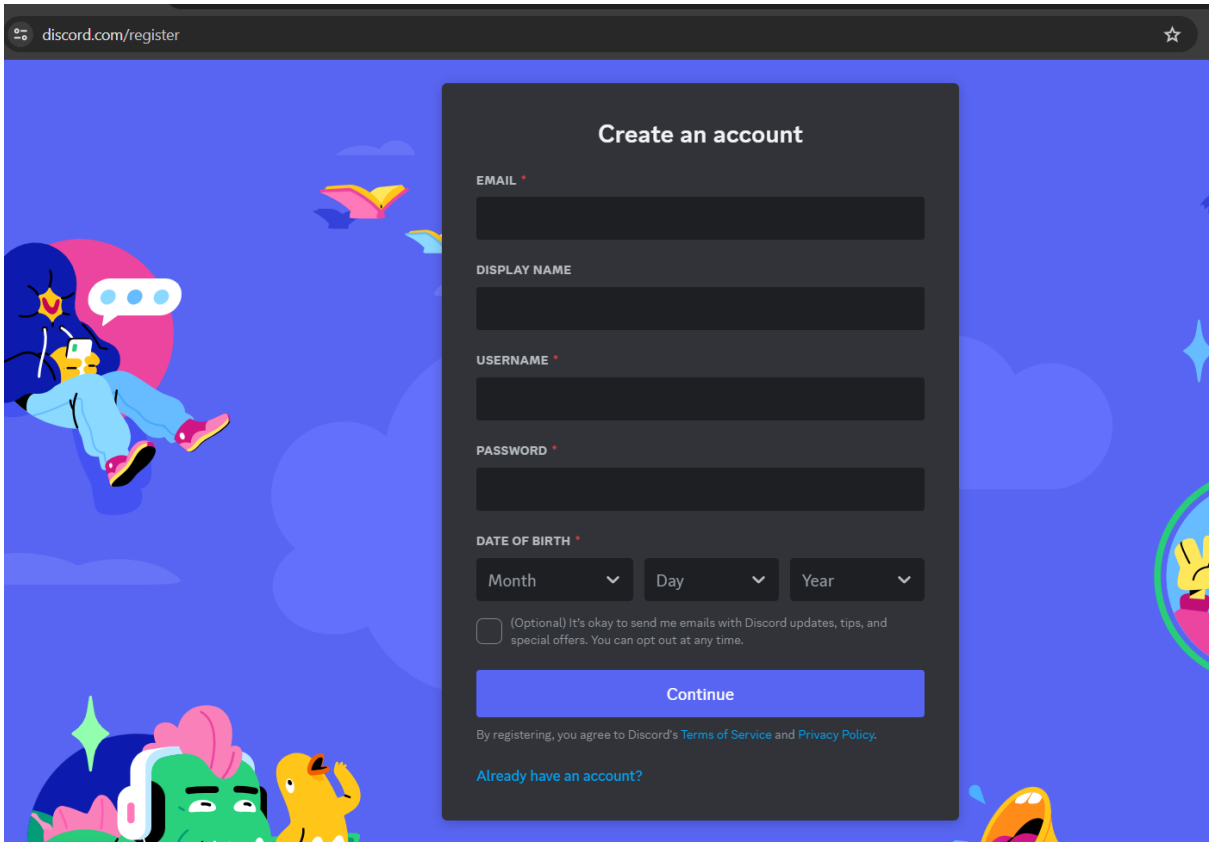

Рис. 3.1 - Вікно реєстрації в системі Discord

Після чого з’являється можливість долучатися до спільнот та створювати власні канали та групи. Створюємо тестовий сервер.

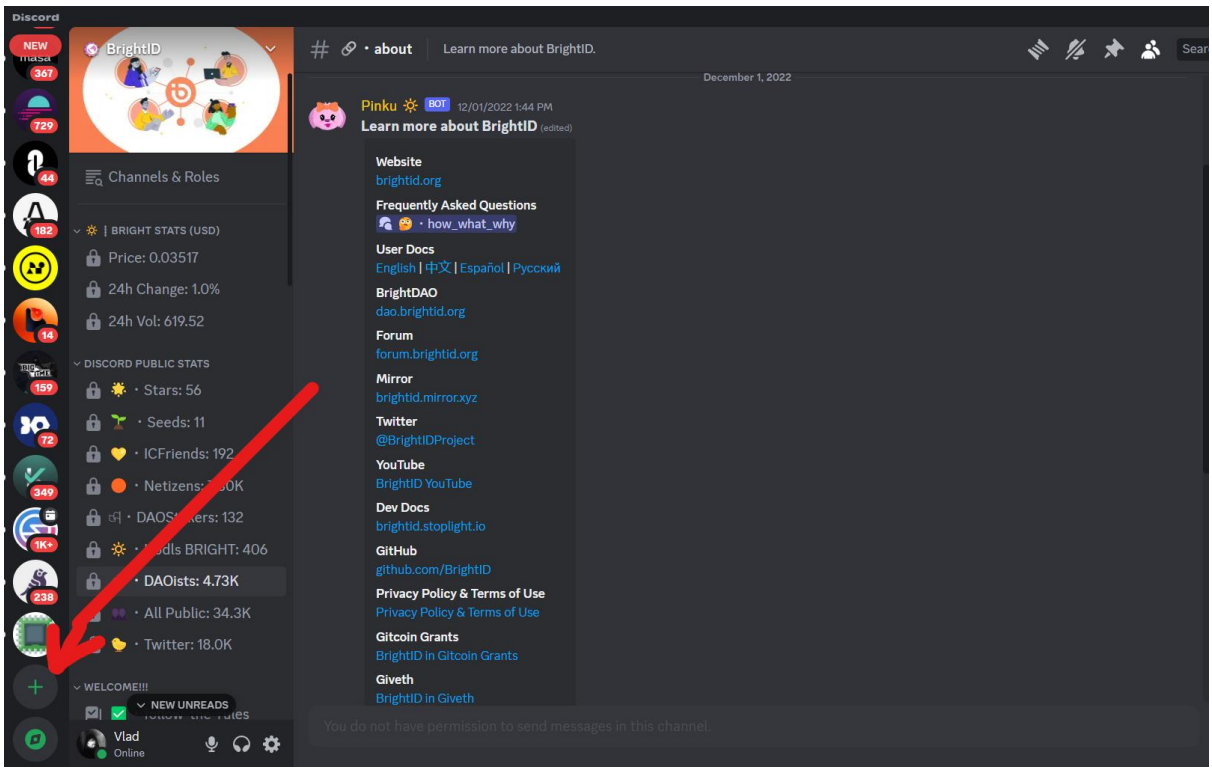

Рис. 3.2 - Вікно в системі Discord: створення сервера

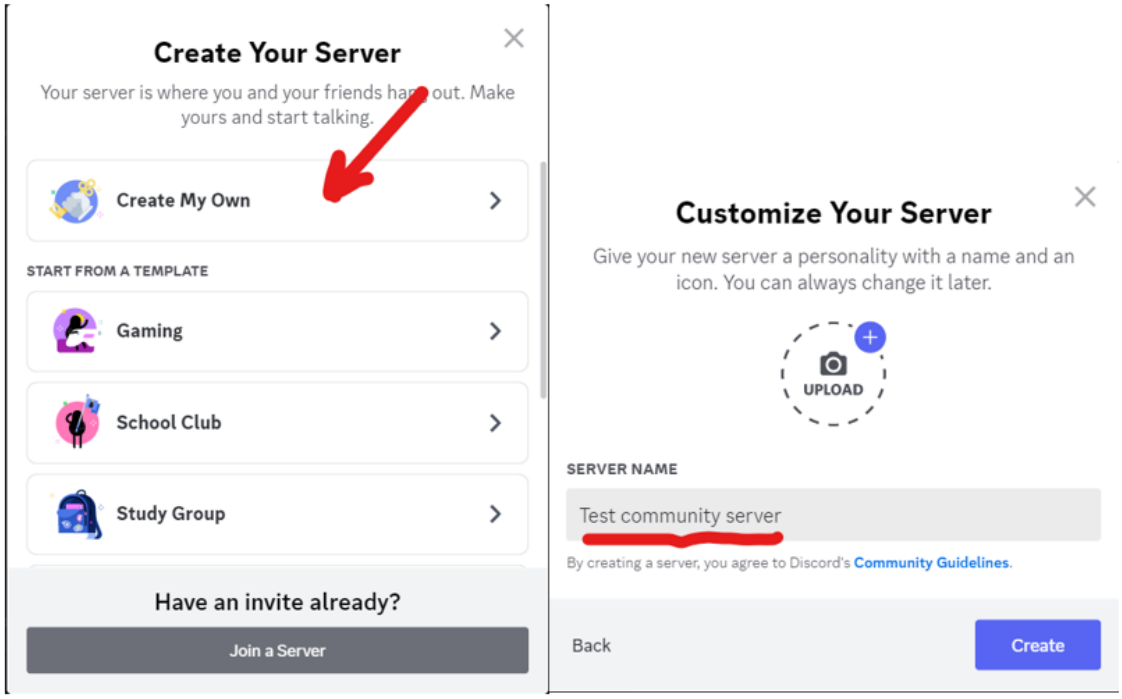

Рис. 3.3 - Вікно в системі Discord: створення сервера

Назвемо його “Test community server”. Новостворений канал буде виглядати наступним чином.

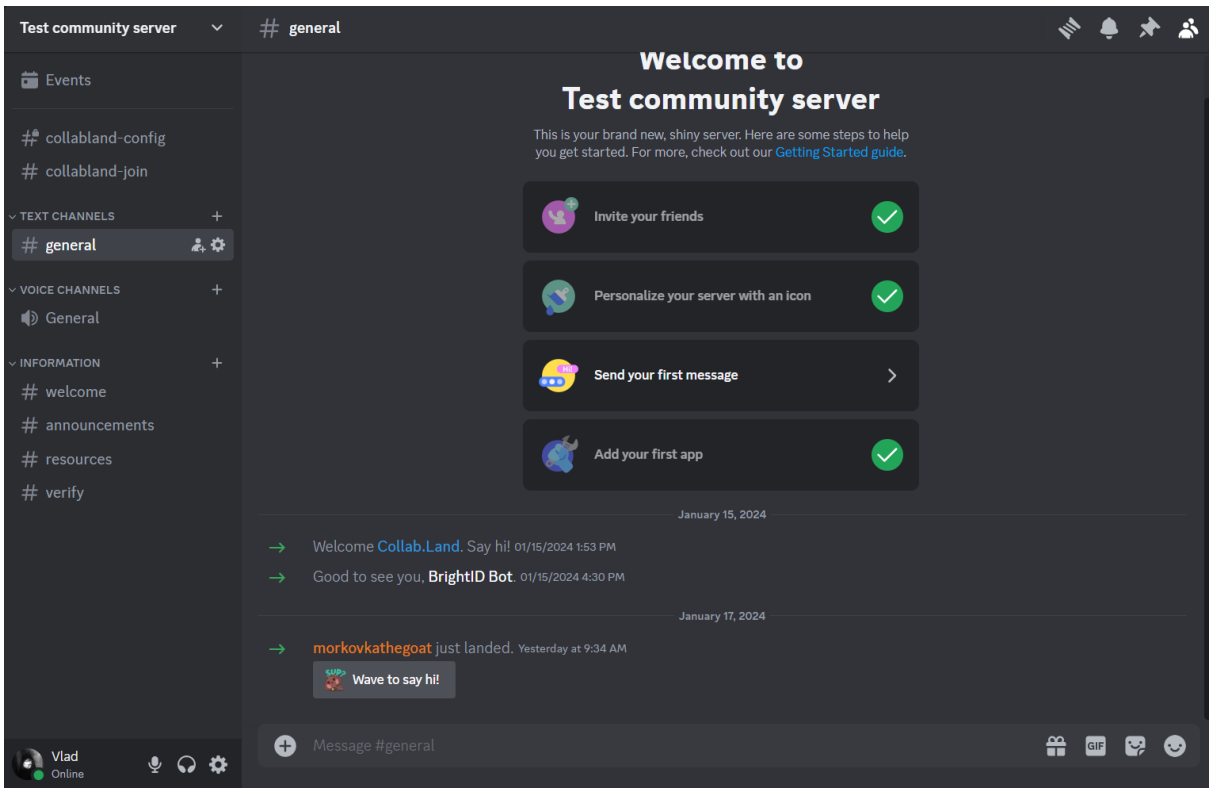

Рис. 3.4 - Створений канал “Test community server” в Discord

3.2 Додавання каналу “verify” на сервері, в якому будуть верифікуватися користувачі.

На панелі управління сервером біля вкладки “Information” тиснемо “+”, вказуємо назву каналу “verify” та тиснемо “Create Channel”.

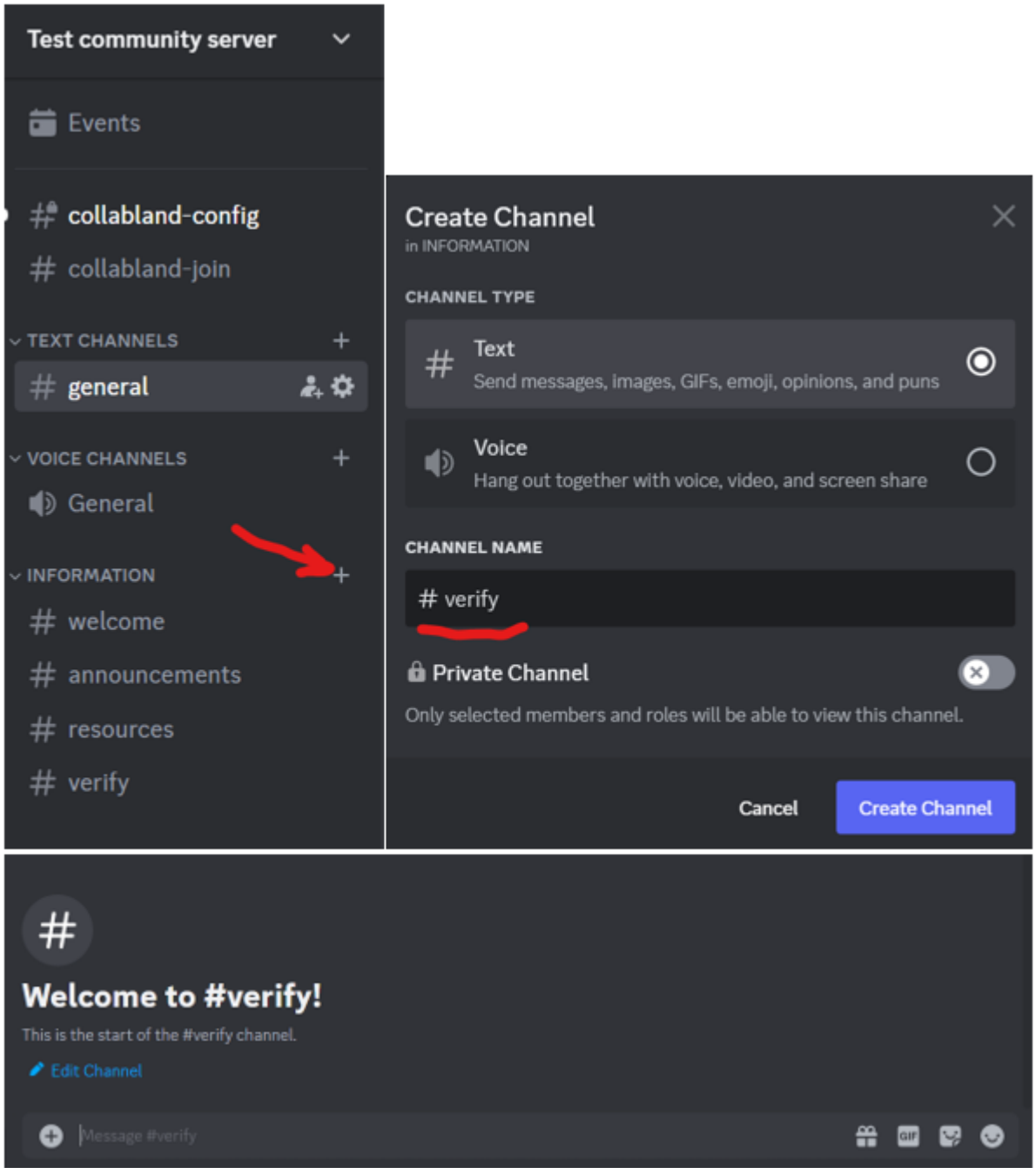

Рис. 3.5 - Створення каналу на сервері Discord

3.3 Додавання Bright ID Discord Bot до серверу.

Bright ID Discord Bot - інструмент, який дозволяє серверам Discord верифікувати своїх користувачів як унікальних людей за допомогою BrightID. Перейшовши за посиланням “https://bot.brightid.org/” додаємо його до тестового серверу в Discord.

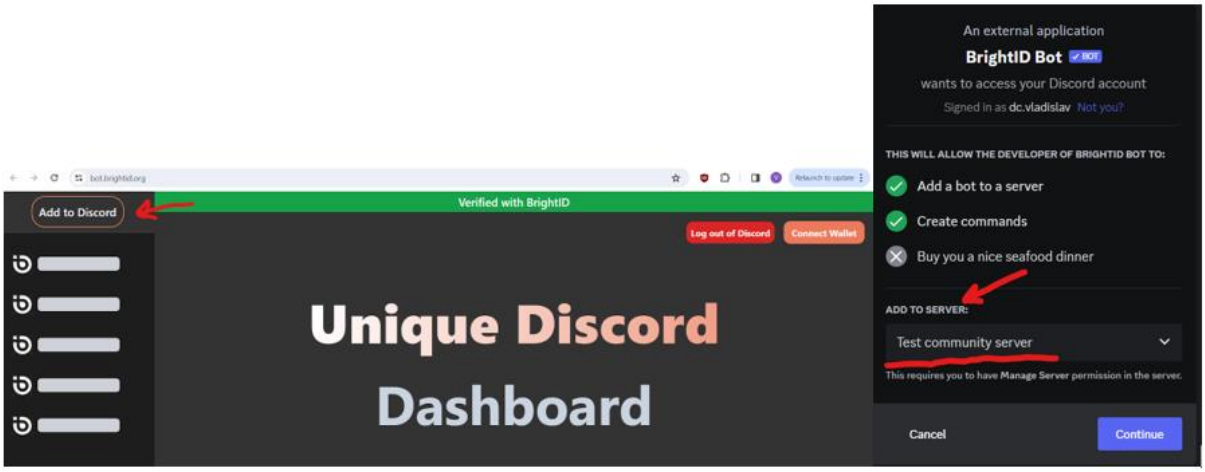

Рис. 3.6 - Додавання Bright ID Discord Bot до серверу

Після чого на сервері з'являється користувач BrightID Bot з окремою роллю “BrightID Bot”, а також створюється роль “Verified”, яка буде надаватися користувачам після верифікації.

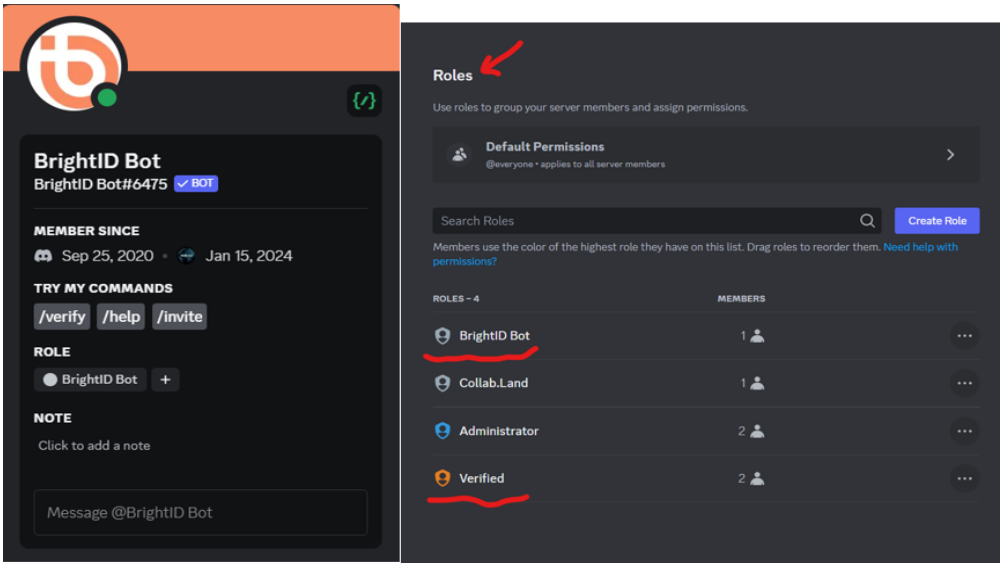

Рис. 3.7 - Вікно користувача BrightID Bot та ролі в Discord

3.4 Приєднання нового користувача до спільноти в Discord.

Створюємо посилання, за яким користувачі зможуть долучитися до спільноти.

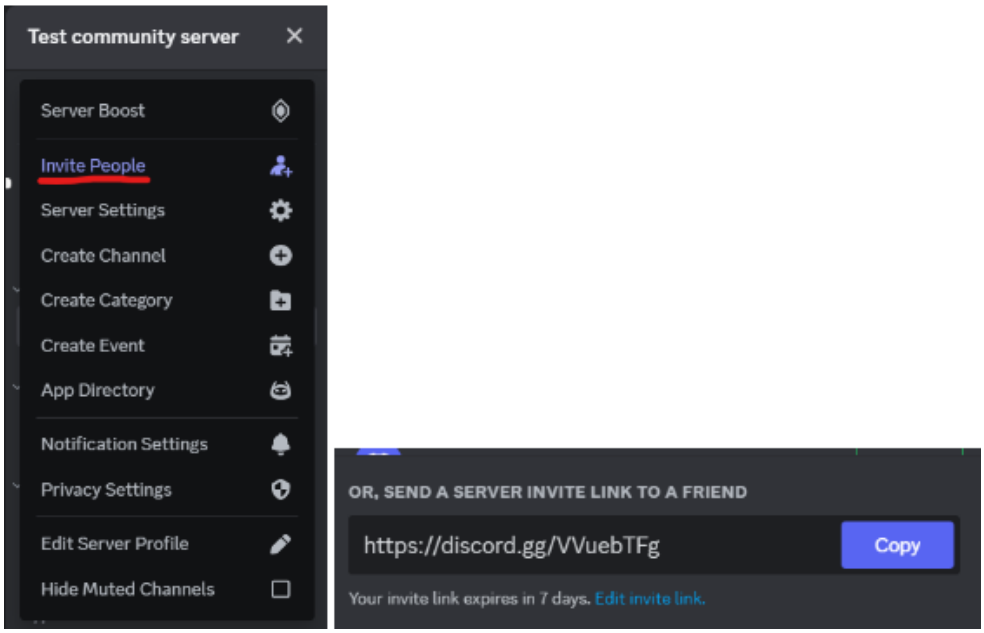

Рис. 3.8 - Створення посилання для приєднання до серверу в Discord

За даним посиланням користувач доєднується серверу та з'являється в списку учасників групи.

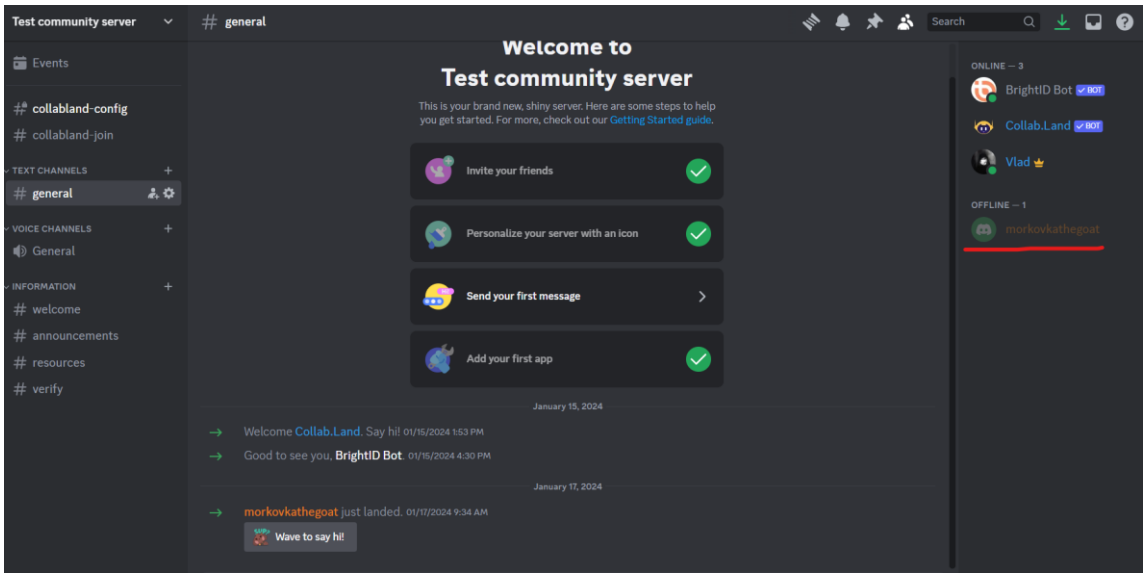

Рис. 3.9 - Новий користувач в списку членів спільноти

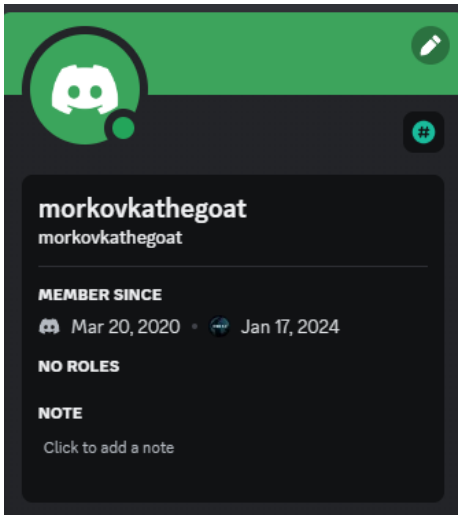

Рис. 3.10 - Профіль нового користувача в тестовій спільноті Discord (без ролей)

3.5 Реєстрація користувача в екосистемі BrightID.

Використовуючи мобільний пристрій на операційній системі iOS завантажуйте додаток BrightID.

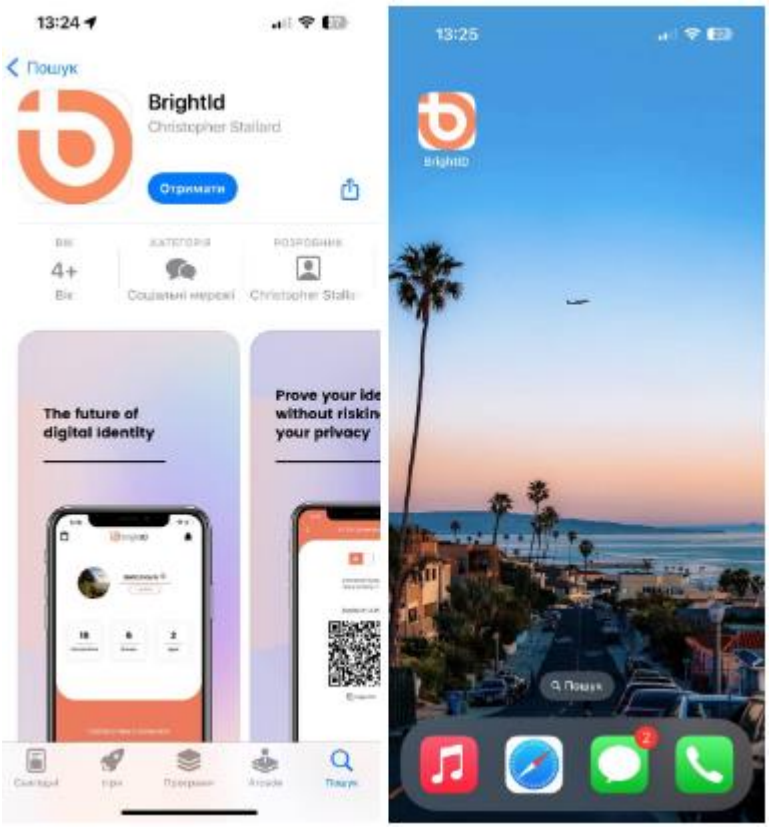

Рис. 3.11 - Завантаження додатку BrightID на мобільний пристрій

Далі створюємо обліковий запис в системі BrightID, вказуємо ім’я та додаємо фото.

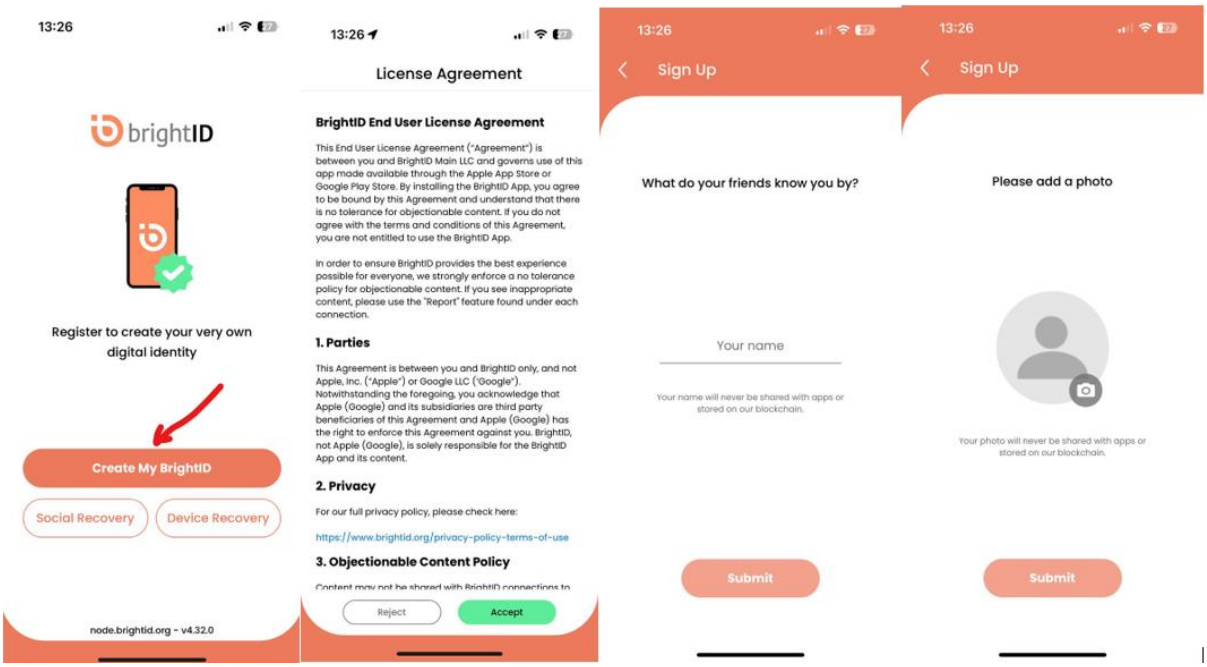

Рис. 3.12 - Процес створення облікового запису в системі BrightID

В результаті отримуємо неверифікований “Verification: none” обліковий запис.

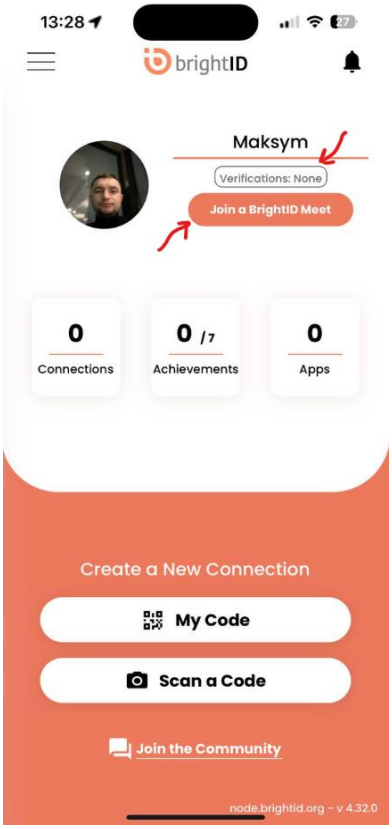

Рис. 3.13 - Профіль новоствореного користувача в системі BrightID (неверифікований)

3.6 Верифікація користувача в екосистемі BrightID.

Для підтвердження особистості потрібно пройти соціальну верифікацію (Meets Verification) в екосистемі BrightID. Верифікація Meets Verification - це перший і найпростіший протокол/механізм верифікації проекту BrightID. Механізм протоколу полягає в тому, що користувач встановлює зв'язок з одним із спеціального набору людей, які називаються Хостами. Усередині протоколу вони називаються “Seeds”. "Seed" насправді відображається у вигляді спеціального значка в BrightID Хоста. Кожен, хто встановлює з'єднання з Хостом, а Хост відповідає йому взаємністю, отримує верифікацію Meets. Для верифікації достатньо лише одного з'єднання. На практиці, хости проводять “вечірки знайомств” в режимі реального часу, щоб нові члени могли познайомитися з хостом і встановити з ним зв'язок.

Протокол вимагає, щоб нова особа чітко показала себе на відео. Вона також повинна уважно слухати і розумно реагувати, якщо ведучий просить її відповісти. Якщо відповіді немає, або вона не є обґрунтованою, як це може статися, якщо учасник не розуміє мови зустрічі, то ведучий відмовляється встановлювати з ним зв'язок. Тому важливо, щоб новий член або приходив на зустріч, яка проводиться тією мовою, яку він розуміє і добре розмовляє, або щоб він взяв із собою перекладача, який допоможе йому слухати і реагувати належним чином під час зустрічі [89].

В додатку BrightID тиснемо на “Join a BrightID Meet” і переходимо на календар запланованих зустрічей для верифікації Хостом. Зустрічі проходять в платформі для відеоконференцій Zoom.

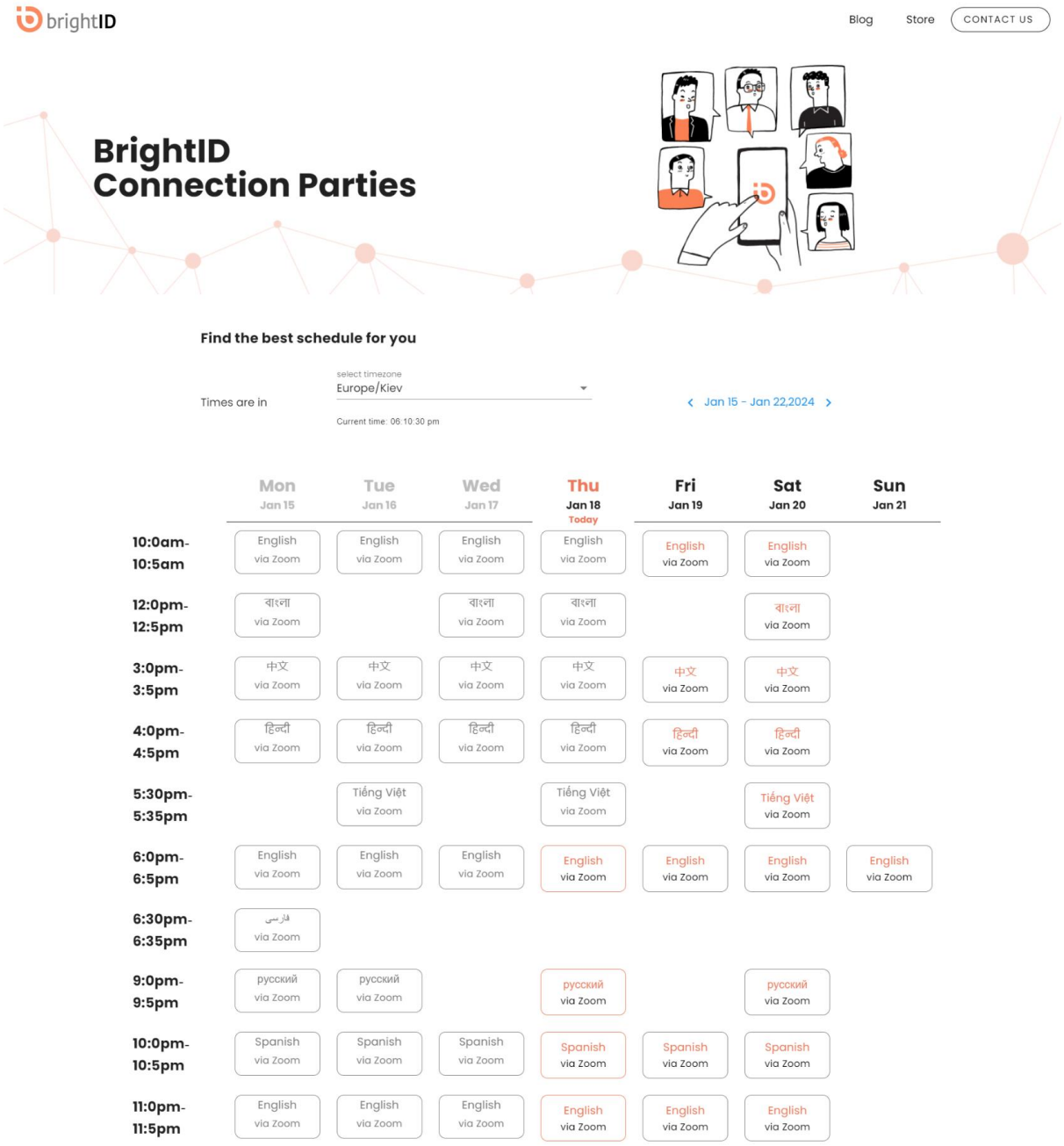

Рис. 3.14 - Календар верифікації Meets

Після верифікації Meets на платформі Zoom особа отримує статус “Meets” в профілі BrightID.

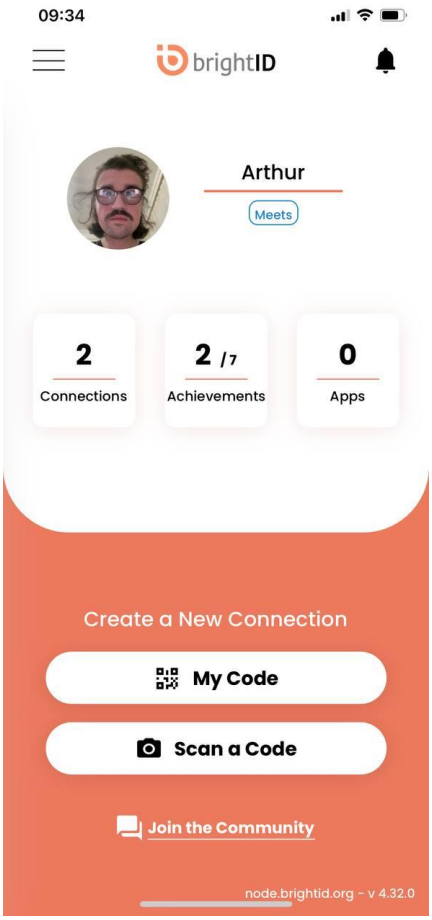

Рис. 3.15 - Верифікований профіль BrightID

3.7 Верифікація користувача в спільноті Discord через Bright ID Discord Bot.

В каналі “verify” тестового серверу відправляємо команду “/verify” та викликаємо процедуру початку верифікації через Bright ID Discord Bot шляхом генерування QR коду. На мобільному пристрої, де було встановлено додаток BrightID, створено обліковий запис в екосистемі BrightID та пройдено соціальну верифікацію “Meets Verification”, скануємо QR код. Після сканування автоматично відкриється додаток BrightID та почнеться зв'язування облікового запису BrightID з обліковим записом в Discord.

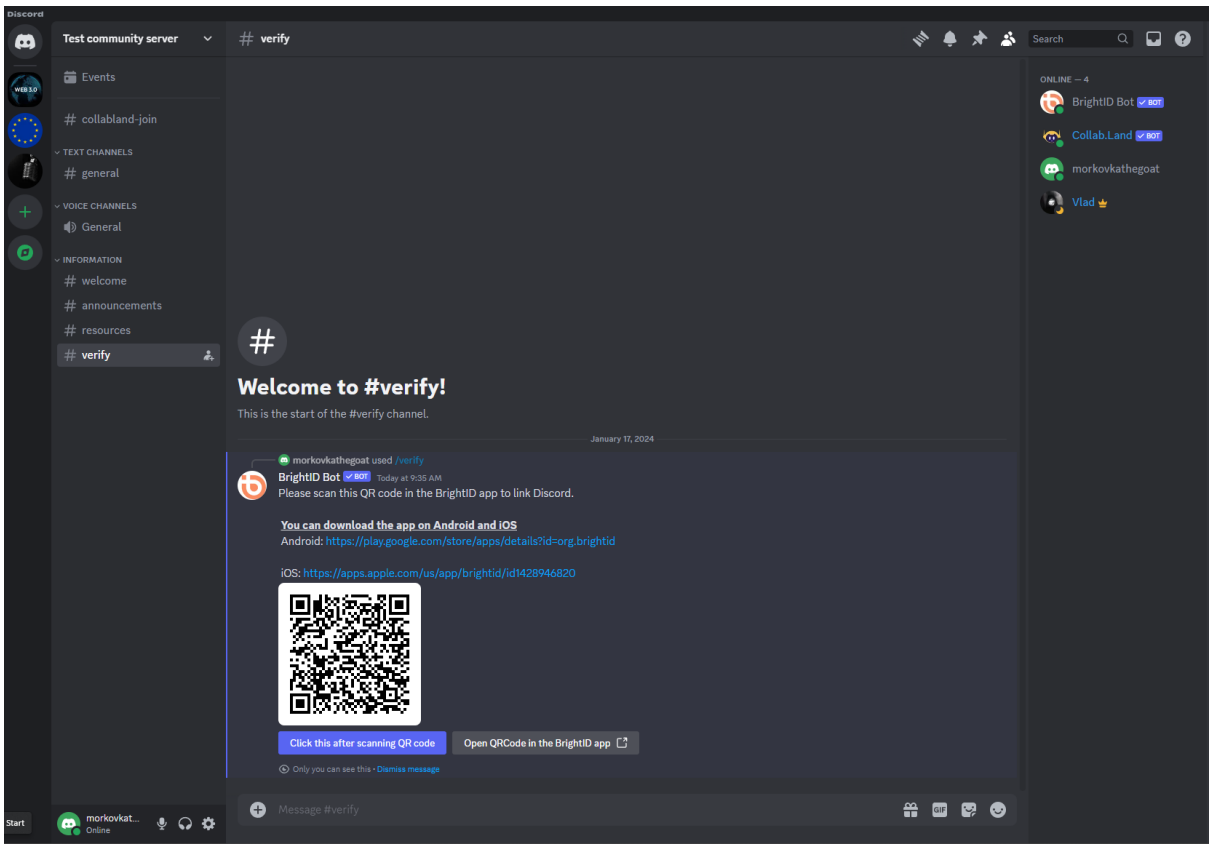

Рис. 3.16 - Генерування QR коду в каналі “verify”

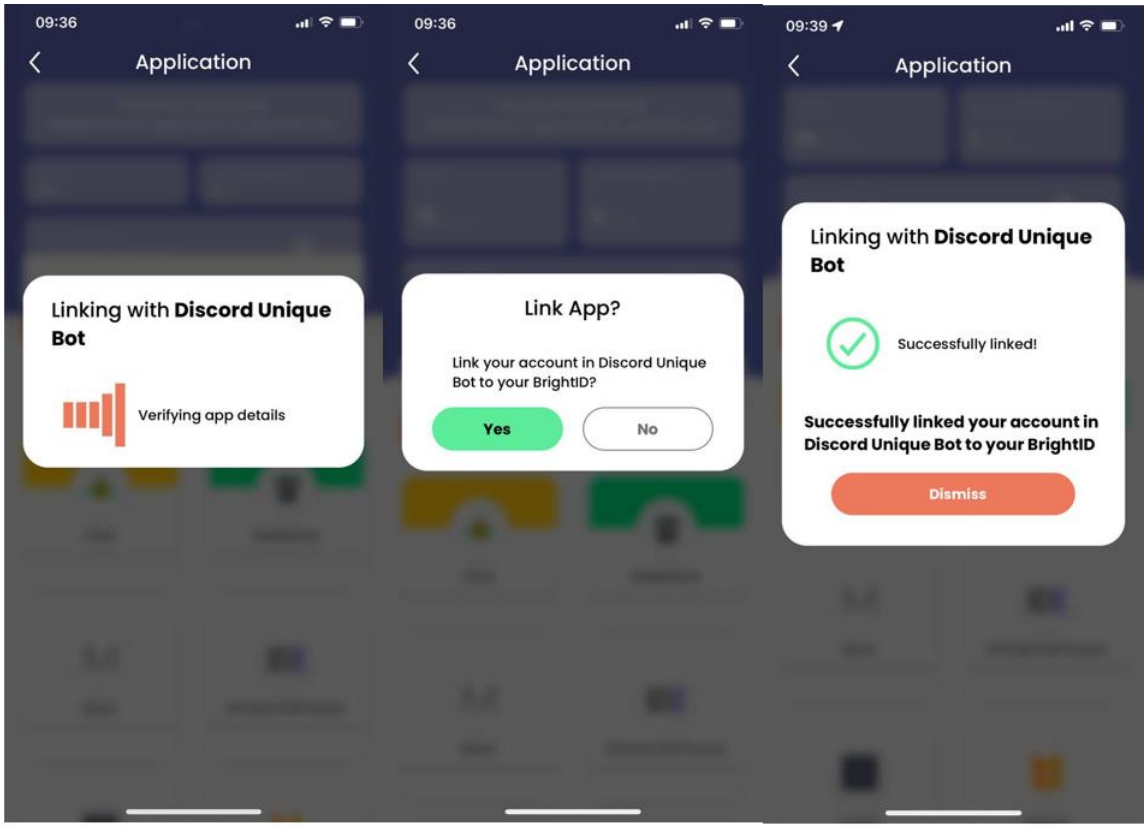

Рис. 3.17 - Зв'язування облікового запису BrightID з обліковим записом в Discord

Після процедури верифікації в Discord новий член спільноти отримує тег “verified” в профілі, таким чином підтверджуючи свою особистість.

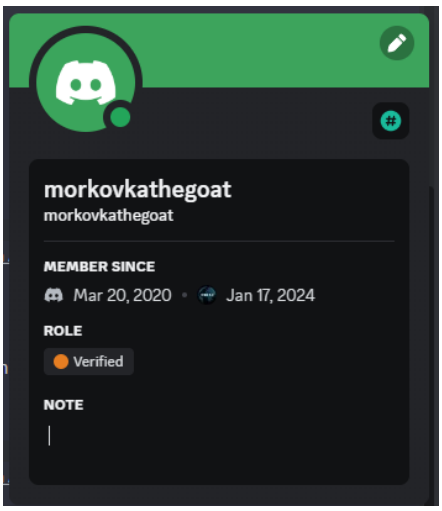

Рис. 3.18 - Профіль верифікованого через екосистему BrightID користувача в тестовій спільноті Discord

3.8 Висновок до розділу 3

У розділі було розглянуто вирішення проблеми попередньої верифікації нових користувачів шляхом інтеграції децентралізованого ідентифікатора (DID) від провайдера BrightID в систему онбордингу через Discord. BrightID, заснований на соціальній верифікації, став ключовим елементом для підтвердження особистості нових учасників у децентралізованих спільнотах. Використовуючи соціальні графи BrightID активно включає спільноту в процес верифікації, сприяючи формуванню відчуття довіри та відповідальності.

Демонстрація імплементації включала створення тестового серверу у Discord, додавання спеціального каналу для верифікації, та інтеграцію Bright ID Discord Bot. Крок за кроком було показано, як новий користувач може приєднатися до спільноти, зареєструватися та пройти верифікацію в екосистемі

BrightID, а потім пройти верифікацію на сервері Discord за допомогою Bright ID Discord Bot.

Застосування цього рішення не лише зміцнює цілісність цифрових ідентичностей, але й активно залучає користувачів до процесу верифікації, сприяючи створенню відчуття колективної відповідальності та довіри в децентралізованих спільнотах.

ВИСНОВКИ

Дослідження різноманітних аспектів технології блокчейн та її застосувань в контексті децентралізованої ідентифікації та цифрових ідентичностей вказує на значущий внесок цих інновацій у різні галузі. Огляд літератури виявив багатогранність досліджень, від теоретичних концепцій до практичних застосувань, аналізуючи переваги та виклики використання блокчейну в різних сферах. Аналіз технології, її концепцій та застосувань, підкреслили потенційні переваги у системах підтримки прийняття рішень, також було акцентовано увагу на таких аспектах як підвищення цілісності та прозорості даних, децентралізація, безпека та захист даних, підвищення ефективності та автоматизація процесів.

Було проаналізовано концепт цифрової ідентичності да методи управління цифровою ідентичністю, виділено та проаналізовано типи цифрової ідентичності. Було досліджено, як технологія блокчейн може змінити традиційні системи управління ідентифікацією, підкреслено переваги систем розподіленого управління ідентифікацією, такі як посилений контроль користувачів над своєю ідентичністю, конфіденційність, безпеку та інтероперабельність.

Було зроблено порівняльний аналіз методів децентралізованої ідентифікації та провайдерів, виявивши складнощі та можливості кожного з підходів, а також аналіз децентралізованої спільноти UkraineDAO. Однією з проблем, яка була виявлена, є верифікація нових користувачів у децентралізованих спільнотах

В практичній частині було розроблено рішення для проблеми попередньої верифікації користувачів, шляхом інтеграції децентралізованого ідентифікатора (DID) від провайдера BrightID в систему онбордингу через Discord. Імплементація цього рішення не лише посилює цілісність цифрових ідентичностей, але й включає спільноту у процес верифікації, сприяючи довірі та колективній відповідальності.

Робота вказує на перспективи та важливість використання технології блокчейн у розбудові децентралізованих та надійних систем управління цифровими ідентичностями, відкриваючи нові можливості для розвитку та ефективного впровадження інновацій.

ПЕРЕЛІК ПОСИЛАНЬ

1. Yli-Huumo, J. Where is current research on blockchain Technology? A systematic review [Electronic resource] / J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander // PLOS ON. — 2016. — 11(10). — e0163477. — Mode of access: https://doi.org/10.1371/journal.pone.0163477.

2. Kshetri, N. Can blockchain strengthen the internet of things? / N. Kshetri // IEEE IT Professional. — 2017. — 19(4), — P. 68-72.

3. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system [Electronic resource] / S. Nakamoto // — 2008. — Mode of access: https://bitcoin.org/bitcoin.pdf.

4. Hardjono, T., Sovrin: A protocol and token for self-sovereign identity and decentralized trust [Electronic resource] / T. Hardjono, D. Smith, R. Lipton — 2016. — 42 p. — Mode of access: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

5. Lipton, A. Blockchains and Distributed Ledgers In Retrospective And Perspective [Electronic resource] / A. Lipton // The Journal of Risk Finance. — 1(19), — P. 4-25. — Mode of access: https://doi.org/10.1108/jrf-02-2017-0035.

6. Zheng, Z. Blockchain challenges and opportunities: A survey / Z. Zheng, S Xie, H.N. Dai, X. Chen, H. Wang // Int. J. Web and Grid Services. — 2018. — Vol. 14, No. 4,. — P. 352-375.

7. Ismail, L.C. A Review Of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, And Solutions [Electronic resource] / L.C. Ismail, H. Materwala // Symmetry. — 2019. — 11(10). — 1198. — Mode of access: https://doi.org/10.3390/sym11101198.

8. Yao, W. SOK: A Taxonomy for Critical Analysis of Consensus Mechanisms in Consortium Blockchain [Electronic resource] / W. Yao, F. P. Deek, R. Murimi, G. Wang // IEEE Access. — 2023. — 11. — P. 79572-79587. — Mode of access: https://doi.org/10.1109/access.2023.3298675.

9. On Public and private blockchains | Ethereum Foundation blog. Ethereum Foundation Blog [Electronic resource]. — Mode of access:: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains.

10. Swanson, T. Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems [Electronic resource] / T. Swanson. — 2015. — 66 p. — Mode of access: https://allquantor.at/blockchainbib/pdf/swanson2015consensus.pdf

11. Christidis, K. Blockchains and smart contracts for the internet of things [Electronic resource] / K. Christidis, M. Devetsikiotis // IEEE Access. — 2016. — 4. — P. 2292–2303. — Mode of access: https://doi.org/10.1109/access.2016.2566339

12. Walport, M. Distributed ledger technology: beyond block chain / M. Walport // Government Office for Science. — 2016. — 88 p.

13. Casino, F. A systematic literature review of blockchain-based applications: Current status, classification and open issues [Electronic resource] / F. Casino, T. K. Dasaklis, C. Patsakis // Telematics and Informatics. — 2019. — I. 36, 55–81. — Mode of access: https://doi.org/10.1016/j.tele.2018.11.006.

14. Crosby, M. Blockchain technology: beyond bitcoin / M. Crosby, P. Pattanayak, S. Verma, V. Kalyanaraman // Appl. Innovation. — 2016. — I. 2. — P. 6–10.

15. Swan, M. Blockchain Blueprint for a New Economy / M. Swan. — O'Reilly Media Inc. — 2015. — 129 p.

16. Zhao, J.L. Overview of business innovations and research opportunities in blockchain and introduction to the special issue / J.L Zhao, S. Fan, J. Yan // Financial Innovation. — 2016. — 2 (1). — 28.

17. Labs, M. Building a more connected world for creators and audiences [Electronic resource] / M. Labs. — 2016. — Mode of access: http://www.mediachain.io/

18. Accumulate: An identity-based blockchain protocol with cross-chain support, human-readable addresses, and key management capabilities. [Electronic resource]. — Mode of access: https://accumulatenetwork.io/.

19. Silent Notary - Blockchain Notary Service. [Electronic resource]. — Mode of access: https://silentnotary.com/files/wp.pdf

20. Filecoin: A Decentralized Storage Network. [Electronic resource]. — Mode of access: https://filecoin.io/filecoin.pdf

21. Mettler, M. Blockchain technology in healthcare: The revolution starts here / M. Mettler // 18th International Conference on e-Health Networking, Applications and Services (Healthcom) IEEE. — 2016. — P. 1-3.

22. Peterson, K. A blockchain-based approach to health information exchange networks / K. Peterson, R. Deeduvanu, P. Kanjamala, K. Boles // Proc. NIST Workshop Blockchain Healthcare. — 2016. — Vol. 1. — P. 1–10.

23. Liu, P.T.S. Medical record system using blockchain, big data and tokenization / P.T.S Liu // Lecture Notes in Computer Science. LNCS. — 2016. — 9977. — P. 254–261.

24. Angraal S. Blockchain Technology: Applications in Health Care [Electronic resource] / S. Angraal, H.M. Krumholz, W.L. Schulz // Circ Cardiovasc Qual Outcomes. — 2017. — 10(9). — e003800. — Mode of access: https://doi.org/10.1161/CIRCOUTCOMES.117.003800. — PMID: 28912202.

25. Haferkorn, M. Seasonality and Interconnectivity Within Cryptocurrencies – An Analysis on the Basis of Bitcoin, Litecoin and Namecoin / M. Haferkorn, J.M. Quintana Diaz // Springer International Publishing, Cham. — 2015. — P. 106–120.

26. Möser, M. Anonymity of bitcoin transactions: an analysis of mixing services / M. Möser // Münster bitcoin conference. — Münster, Germany. — 2013.

27. Кулага А. А. Протокол доведення знання розв'язку задачі Діффі–Хеллмана з нульовим розголошенням / А. А. Кулага // НАУКОВІ ЗАПИСКИ НаУКМА. — 2011. — Т. 138. — С. 19—24.

28. Bdiwi, R. Towards a New Ubiquitous Learning Environment Based on Blockchain Technology / R. Bdiwi, C. De Runz, S. Faiz, A.A. Cherif // Proceedings – IEEE 17th International Conference on Advanced Learning Technologies, ICALT. — 2017. — P. 101–102.

29. Sharples, M. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward [Electronic resource] / M. Sharples, J. Domingue // Adaptive and Adaptable Learning. EC-TEL 2016. Lecture Notes in Computer Science. — 2016. — 9891. — P. 490-496. — Mode of access: https://doi.org/10.1007/978-3-319-45153-4_48.

30. Zhang, J. Walks trajectory tracking of shared information based on consortium blockchain / J. Zhang // Revista de la Facultad de Ingenieria. — 2016. — 31 (12) . — P. 8–17.

31. Брюхов Д. О. Интероперабельные информационные системы: архитектуры и технологии / Д.О. Брюхов, В.И. Задорожный, Л.А. Калиниченко, М.Ю. Курошев, С.С. Шумилов // СУБД. — 1995. — С. 86–113.

32. Abdullah, N. Blockchain based approach to enhance big data authentication in distributed environment / N. Abdullah, A. Håkansson, E. Moradian // International Conference on Ubiquitous and Future Networks. ICUFN. — 2017. — P. 887–892.

33. Hasan, M.R. Operational Efficiency Effects Of Blockchain Technology Implementation In Firms [Electronic resource] / M.R. Hasan, D. Shiming, M.A. Islam, M.Z. Hossain // RIBS. — 2020. — 2(30). — P. 163-181. — Mode of access: https://doi.org/10.1108/ribs-05-2019-0069.

34. Rosencrance, L. Identity management (ID management). Security [Electronic resource] / L. Rosencrance, C. Mathias. — 2021. — Mode of access: https://www.techtarget.com/searchsecurity/definition/identity-management-ID-management.

35. Camp, L. Digital identity [Electronic resource] / L. Camp // Technology and Society Magazine, IEEE. — Vol 23. — P. 34-41. — Mode of access: https://doi.org/10.1109/MTAS.2004.1337889.

36. Singla, A. Decentralized identity management using blockchain [Electronic resource] / A. Singla, N. Gupta, P. Aeron, A. Jain, D. Sharma, S.S. Bharadwaj // Journal of Global Information Management. — 2022. — Vol 31(2). — P 1-24. — Mode of access: https://doi.org/10.4018/jgim.315283.

37. Allen, C. The path to self-sovereign identity [Electronic resource] / C. Allen // Life with Alacrity. — 2016. — Mode of access: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

38. Stockburger, L. Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation [Electronic resource] / L. Stockburger, G. Kokosioulis, A. Mukkamala, R.R. Mukkamala, M. Avital // Blockchain: Research and Applications. — 2021. — 2(2). — 100014. — Mode of access: https://doi.org/10.1016/j.bcra.2021.100014.

39. OpenID - OpenID Foundation. OpenID Foundation - Helping People Assert Their Identity Wherever They Choose [Electronic resource]. — Mode of access: https://www.openid.net/.

40. Hardt, D. RFC6749 - The OAuth 2.0 Authorization Framework [Electronic resource] / D. Hardt // Internet Engineering Task Force. — 2012. — Mode of access: https://doi.org/10.17487/RFC6749.

41. Kruk, S.R. D-FOAF: Distributed identity management with access rights delegation [Electronic resource] / S.R. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki, H.C. Choi // LNISA. — 2006. — 4185. — P. 140-154. — Mode of access: https://doi.org/10.1007/11836025_15.

42. Koshutanski, H. Distributed identity management model for digital ecosystems [Electronic resource] / H. Koshutanski, M. Ion, L. Telesca // In The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007). — 2007. — P. 132-138. — Mode of access: https://doi.org/10.1109/SECUREWARE.2007.4385323.

43. Höller, T. Evaluating dynamic tor onion services for privacy preserving distributed digital identity systems / T. Höller, M. Roland, R. Mayrhofer // Journal of Cyber Security and Mobility. — 2022. — P. 141–164.

44. Ferdous, M. S. In Search of Self-Sovereign Identity Leveraging Blockchain Technology [Electronic resource] / M.S. Ferdous, F. Chowdhury, M.O. Alassafi // IEEE Access. — 2019. — Vol. 7. — P. 103059–103079. — ISSN 2169-3536. — Mode of access: https://doi.org/10.1109/ACCESS.2019.2931173.

45. Kubach, M. Self-sovereign and decentralized identity as the future of identity management? / M. Kubach, C.H. Schunck, R. Sellung, H. Roßnagel // Open Identity Summit. — 2020.

46. Mühle, A.G. A survey on essential components of a self-sovereign identity [Electronic resource] / A.G. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel // Computer Science Review. — 2018. — Vol. 30. — P. 80–86. — Mode of access: https://doi.org/10.1016/j.cosrev.2018.10.002.

47. Mulaji, S.S. The practicality of adopting blockchain-based distributed identity management in organizations: A meta-synthesis [Electronic resource] / S.S. Mulaji, S.S. Roodt // Security and Communication Networks. — 2021. — P. 1-19. — Mode of access: https://doi.org/10.1155/2021/9910078.

48. Chango, M. Building a credential exchange infrastructure for digital identity: A sociohistorical perspective and policy guidelines [Electronic resource] / M. Chango // Frontiers in Blockchain. — 2022. — Vol. 4. — 629790. — Mode of access: https://doi.org/10.3389/fbloc.2021.629790.

49. Hassan, S. Decentralized Autonomous Organization [Electronic resource] / S. Hassan, P. De Filippi // Internet Policy Review. — 2021. — 10(2). — Mode of access: https://doi.org/10.14763/2021.2.1556.

50. Ghelani, D. What is Non-fungible token (NFT)? A short discussion about NFT Terms used in NFT [Electronic resource] / D. Ghelani // Authorea (Authorea). — 2022. — Mode of access: https://doi.org/10.22541/au.166490992.24247550/v1.

51. Vogelsteller, F. ERC-20 token standard [Electronic resource] / F. Vogelsteller, V. Buterin // Ethereum Improvement Proposals. — No. 20. — 2015. — Mode of access: https://eips.ethereum.org/EIPS/eip-20.

52. Weyl, E.G. Decentralized Society: Finding Web3’s soul [Electronic resource] / E.G. Weyl, P. Ohlhaver, V. Buterin // Social Science Research Network. — 2022. — Mode of access: https://doi.org/10.2139/ssrn.4105763.

53. Angelo, M. Identification of token contracts on ethereum: standard compliance and beyond [Electronic resource] / M. Angelo, G. Salzer // International

Journal of Data Science and Analytics. — 2021. — 16(3). — P. 333-352. — Mode of access: https://doi.org/10.1007/s41060-021-00281-1.

54. Avellaneda, O. Decentralized identity: Where did it come from and where is it going? [Electronic resource] / O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K.H. Duffy, E. Maler, D. Reed, M. Sporny // IEEE Communications Standards Magazine. — 2019. — 3(4). — P. 10–13. — Mode of access: https://doi.org/10.1109/mcomstd.2019.9031542.

55. List of Top 20 Decentralized Identity Tools [Electronic resource]. — Mode of access: https://101blockchains.com/top-decentralized-identity-tools/.

56. DAOs for impact. World Economic Forum [Electronic resource]. — 2023. — Mode of access: https://www.weforum.org/publications/daos-for-impact/.

57. USC Dornsife, Center for Advanced Genocide Research, Starling Lab and Hala Systems File Cryptographic Submission of Evidence of War Crimes in Ukraine to the International Criminal Court [Electronic resource]. — 2022. — Mode of access: https://dornsife.usc.edu/cagrnews/news/2022/06/33571-starling-lab-and-hala-systems-file-cryptographic-submission-evidence-war-crimes.

58. Hubbard, S. Case profiles of decentralized autonomous organizations [Electronic resource] / S. Hubbard, A. Trivedi, M. Sharma // Belfer Center for Science and International Affairs. — 2023. — Mode of access: https://www.belfercenter.org/publication/case-profiles-decentralized-autonomous-organizations.

59. Sehested Lund, F.A. Leveraging Blockchain Technology in Crisis Situations — a Network Analysis of The Blockchain-related Intricacies in the 2022 Ukraine War / F.A. Sehested Lund // IT University of Copenhagen. Digital Innovation & Management, M.Sc. — 2022. P. 39-40.

60. Civic Pass | trust, control and safety for digital identity [Electronic resource]. — Mode of access: Civic Technologies, Inc. https://www.civic.com/

61. Stripe Identity: Verify identities with confidence [Electronic resource]. — Mode of access: https://stripe.com/identity.

62. The Jolocom Protocol - Own Your Digital Self — Jolocom-Lib documentation [Electronic resource]. — Mode of access: https://jolocom-lib.readthedocs.io/en/latest/.

63. MLizzbert. Layer 2 - Cryptocurrencies. IQ.wiki [Electronic resource]. — Mode of access: https://iq.wiki/wiki/layer-2.

64. Nametag | The username of the future [Electronic resource]. — Mode of access: https://nametag.org/.

65. SelfKey. Self-Sovereign Identity for more Freedom and Privacy - SelfKey [Electronic resource]. — Mode of access: https://selfkey.org/.

66. Fractal. Fractal ID - Web3 Identity Solution Provider [Electronic resource]. — Mode of access: https://web.fractal.id/.

67. Introducing the Blockstack Identity System [Electronic resource]. — Mode of access: https://blog.blockstack.org/introducing-the-blockstack-identity-system.

68. Polygon ID | Trusted digital identity for your next big idea [Electronic resource]. — Mode of access: https://polygonid.com/.

69. The Veres One Project. VERes One - a globally interoperable network for identity [Electronic resource]. — Mode of access: https://veres.one/.

70. KycDAO - web3 framework for compliant smart contracts [Electronic resource]. — Mode of access: https://kycdao.xyz/.

71. ONT ID - Ontology Developer Center [Electronic resource]. — Mode of access: https://docs.ont.io/decentralized-identity-and-data/ontid.

72. Disco - Bring all your selves [Electronic resource]. — Mode of access: https://www.disco.xyz/.

73. Evernym. The solution: Self-Sovereign Identity - Evernym [Electronic resource]. — Mode of access: https://www.evernym.com/solution/.

74. SpruceID. Digital IDs [Electronic resource]. — Mode of access: https://spruceid.com/digital-ids.

75. ION - an open, public, permissionless decentralized identifier network [Electronic resource]. — Mode of access: https://identity.foundation/ion/.

76. Galxe ID - Profile | Galxe [Electronic resource]. — Mode of access: https://galxe.com/id.

77. Shyft Network | Trusted Blockchain Compliance [Electronic resource]. — Mode of access: https://www.shyft.network/.

78. BrightID - BrightID [Electronic resource]. — Mode of access: https://brightid.gitbook.io/brightid/.

79. Internet Identity | Internet Computer [Electronic resource]. — Mode of access: https://internetcomputer.org/docs/current/developer-docs/integrations/internet-identity/overview.

80. Home | Internet Computer [Electronic resource]. — Mode of access: https://internetcomputer.org/.

81. HashKey DID [Electronic resource]. — Mode of access: https://www.hashkey.id/.

82. Home - Spherity [Electronic resource]. — Mode of access: https://www.spherity.com/.

83. XHashtag - Web3 Credentials for Future of Work [Electronic resource]. — Mode of access: https://www.xhashtag.io/.

84. ZCloak Network - Real-World Identity for Web3 [Electronic resource]. — Mode of access: https://zcloak.network/.

85. Violet - Compliance & Identity Infrastructure for DEFI [Electronic resource]. — Mode of access: https://www.violet.co/.

86. iden3 [Electronic resource]. — Mode of access: https://iden3.io/.

87. Ukraine DAO [Electronic resource]. — Mode of access: https://ukraine-dao.notion.site/.

88. What is Discord: A Guide for Parents and Educators [Electronic resource]. — Mode of access: https://discord.com/safety/360044149331-what-is-discord.

89. Meets Verification - BrightID [Electronic resource]. — Mode of access: https://brightid.gitbook.io/brightid/verifications/meets-verification.