Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Факультет інформатики

Кафедра мультимедійних систем

ДОСЛІДЖЕННЯ МОЖЛИВИХ МЕТОДІВ ПІДКЛЮЧЕННЯ ДОДАТКУ "ДІЯ" ДО EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE

Текстова частина до курсової роботи

за спеціальністю 122 «Комп’ютерні науки»

Керівник курсової роботи

Гороховський К. С.

_____

(підпис)

“____” _____ 2024 р.

Виконала студентка

Цвєткова А. І.

“____” _____ 2024 р.

Київ 2024

Міністерство освіти і науки України

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «КИЄВО-МОГИЛЯНСЬКА АКАДЕМІЯ»

Факультет інформатики

Кафедра мультимедійних систем

Зав.кафедри мультимедійних систем,

Жежерун О.П.

_____ (підпис)

„____”_____2024 р.

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ

на курсову роботу

студентці Цвєктовій Анні Іллівні факультету інформатики 3-го курсу

ТЕМА Дослідження можливих методів підключення додатку "Дія" до European Blockchain Services Infrastructure

Зміст теоретичної частини до курсової роботи:

Анотація

Вступ

Розділ 1. ХАРАКТЕРИСТИКИ ТА ПРИНЦИПИ РОБОТИ ЦИФРОВИХ ГАМАНЦІВ «ДІЯ» ТА DIGITAL IDENTITY WALLET.

Розділ 2. КРОКИ ПІДКЛЮЧЕННЯ ДОДАТКУ «ДІЯ» ДО EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE. ЕЛЕМЕНТИ БУДОВИ.

Висновки

Список використаних джерел

Додатки (за необхідністю)

Дата видачі „___” _____ 2024 р. Гороховський К. С. _____ (підпис)

Завдання отримав _____ (підпис)

Тема: Дослідження можливих методів підключення додатку "Дія" до European Blockchain Services Infrastructure

Календарний план виконання роботи:

№ п/п	Назва етапу дипломного проекту (роботи)	Термін виконання етапу	Примітка
1.	Отримання завдання на курсову роботу	25.12.2023	
2.	Аналіз матеріалів за темою	11.01.2024	
3.	Розробка та програмування алгоритму	01.04.2024	
4.	Написання текстової частини до курсової роботи	10.05.2024	
5.	Коригування виконаної роботи	12.05.2024	
6.	Створення слайдів для доповіді та написання доповіді.	16.05.2024	

7.	Остаточне оформлення роботи та слайдів	20.05.2024	
8.	Захист курсової роботи	21.05.2024	

Желізняк А. О. _____

Гороховський К. С. _____

“_____”_____

ЗМІСТ

АНОТАЦІЯ

Дана курсова робота присвячена дослідженню відмінностей та подібностей систем та принципів роботи, які впровадила команда українського бренду цифрової держави «Дія» у порівнянні до European Blockchain Services Infrastructure (далі EBSI) мережі та Digital Identity Wallet (далі DIW), що розроблені у партнерстві European Commission та European Blockchain. Також, для прикладу, було розроблено власний застосунок Verifier Wallet за стандартами EBSI з привертанням уваги до особливостей роботи Дії.

Під час розробки було використано такі технології: React, Java, побудовано власний API з використанням Spring Boot та запропоновано альтернативи, Blockchain система Ethereum за допомоги Geth та Prysm, Nimbus JOSE+JWT та OAuth 2.0 SDK з OpenID Connect Extensions бібліотеки на Java, бібліотеки для React застосунку (qr-scanner, dotenv, axios тощо).

ВСТУП

Цифрові технології швидко змінюють ландшафт державних послуг, надаючи можливості для зручної взаємодії між громадянами та державою. Український проєкт "Дія" став яскравим прикладом того, як цифрові технології можуть полегшити доступ громадян до державних послуг та документів, таких як паспорти, посвідчення водія, сертифікати вакцинації тощо. У той час як "Дія" стала прикладом цифрової трансформації в Україні, у Європейському Союзі було розроблено подібні ініціативи в рамках European Blockchain Services Infrastructure (EBSI) ініціативи.

Ця курсова робота досліджує можливі методи підключення додатку "Дія" до EBSI, вивчаючи обидві системи, їх слабкі та сильні сторони. Особливий акцент робиться на інтеграції з European Blockchain, враховуючи досвід "Дії" та стандарти, впроваджені в EBSI.

Зараз Україна активно рухається у напрямку вступу до Європейського Союзу та нам як ніколи потрібні сучасні нові рішення для успішної інтеграції. Щоб заручитися підтримкою європейських партнерів та отримати можливості співпраці важливо мати чіткий план, обґрунтоване бачення ситуації.

Мета дослідження полягає в тому, щоб визначити, як дві системи можуть співпрацювати для покращення послуг наданих як українцям так і громадянам країн Європейського Союзу. Також порівняти український та іноземний продукти за декількома критеріями, дослідити яким чином вони працюють. Очікується, що результати дослідження сприятимуть кращому розумінню інфраструктури цифрових послуг у Європейському Союзі та Україні, а також відкриють нові шляхи для співпраці в галузі цифрової ідентичності та державних послуг.

Об’єктом дослідження є системи цифрових державних послуг "Дія" та European Blockchain Services Infrastructure (EBSI). Обидві системи представляють собою ініціативи з метою полегшення доступу громадян до державних послуг та ідентифікаційних даних, але вони можуть відрізнятися за технологічними аспектами, принципами роботи та стандартами безпеки.

Предметом дослідження є порівняння та аналіз відмінностей та подібностей між системами "Дія" та EBSI. Основний акцент робиться на технічних аспектах обох систем, таких як принципи криптографії, стандарти безпеки, технології блокчейну та ідентифікації. Дослідження також вивчає можливості підключення додатку "Дія" до EBSI з метою забезпечення сумісності та безпеки обміну даними між двома системами.

ОСНОВНА ЧАСТИНА

Розділ 1. ХАРАКТЕРИСТИКИ ТА ПРИНЦИПИ РОБОТИ ЦИФРОВИХ ГАМАНЦІВ «ДІЯ» ТА DIGITAL IDENTITY WALLET

1.1 Цифровий ідентифікаційний гаманець: означення, застосування, переваги та недоліки

Традиційні гаманці стають застарілими. Цифрові ідентифікаційні гаманці з'явилися, щоб революціонізувати спосіб управління нашими персональними даними та інформацією, як фізичними, так і цифровими, а також удосконалити способи здійснення та отримання платежів. Ми можемо визначити це як систему, яка зберігає приватні дані людей, такі як документи, що посвідчують особу, способи оплати, важливі документи, а також дозволяє їм отримати доступ до глобальної економіки.

Цифровий гаманець є унікальним, приватним і непередаваним, отриманим після автентифікації. Такі технології, як NFC або біометрія зі штучним інтелектом, є ключовими для того щоб забезпечити перевірку та верифікацію особи. Цифровий гаманець стає ключовим елементом для забезпечення зручності та безпеки швидкої взаємодії громадянина із сервісами держави та зберігання цифрових ідентифікаторів. [1]

Застосування цифрового гаманця в системі "Дія" та EBSI: [1]

- зберігання та управління цифровими ідентифікаторами, такими як електронний паспорт, ідентифікаційні дані та інша особиста інформація, необхідна для взаємодії з державними сервісами
- аутентифікація та підтвердження особи користувача (громадянина) для отримання державних послуг або взаємодії з іншими онлайн-системами

- безпека та конфіденційність особистих даних користувача шляхом застосування криптографічних методів шифрування та безпеки

Переваги технології:

- зручність та ефективність отримання доступу до державних послуг та виконання різноманітних операції онлайн
- безпека та приватність, криптографічний захист особистих даних користувача від несанкціонованого доступу
- менший ризик втрати або крадіжки документації
- революція управління даними та платежами, розширення можливостей для розвитку та впровадження нових цифрових сервісів та функцій для задоволення потреб користувачів
- суверенна та децентралізована/централізована ідентичність з контролем над своєю інформацією
- спрощений процес автентифікації та верифікації в інших сервісах, де потрібно підтвердити особу

Недоліки технології:

- технічні перешкоди, з якими можуть зіткнутися деякі користувачі під час використання цифрового гаманця через необхідність розуміння мінімальних технічних аспектів
- ризики безпеки, кібератак та онлайн шахрайства
- додаткові витрати на постійну підтримку, оновлення та підвищення рівня безпеки
- неоднозначність законодавства щодо використання цифрових гаманців та їх правового статусу в деяких країнах

1.2 Опис технології Blockchain

Блокчейн — це асинхронна нереляційна система запису інформації в загальну децентралізовану базу даних, де кожен комп'ютер (сервер нод) у мережі блокчейну має копію цифрового журналу транзакцій. Книга обліку — це цифровий запис бухгалтерських одиниць. Блокчейн дуже ускладнює для когось зміну, злам або обман системи, оскільки записи не можна змінити заднім числом без зміни наступних блоків інформації. [2]

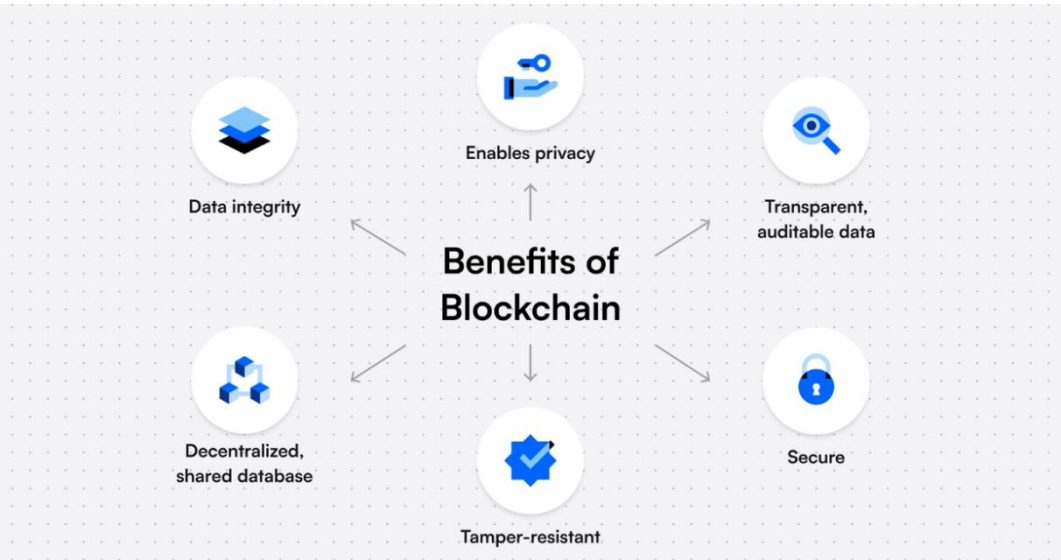


Рис. 1.1 Ключові переваги технології блокчейн

Рішення для ідентифікації на основі блокчейну стають дедалі популярнішими, оскільки вони пропонують безпечний та економічно ефективний спосіб управління цифровими ідентифікаційними даними. Користувачі зберігають свої ідентифікаційні дані та облікові дані в децентралізованому додатку гаманця, а блокчейн дозволяє миттєво перевіряти ці дані без необхідності звертатися до емітента. ID-гаманці надають користувачам більше контролю над своєю особистою інформацією. [2]

Цифрова ідентичність — це повна інформація про особу чи організацію, яка існує в Інтернеті. Дані, які формують цифрову

ідентичність, включають імена користувачів, історію покупок, ідентифікаційний номер та історію пошуку. Майже всі наші цифрові ідентичності підключаються через пристрої, служби та програми, які переважно використовують централізовані та об’єднані системи ідентифікації. Багато з поточних систем управління цифровою ідентичністю мають недоліки, зокрема ризик витоку даних (через який European Union (далі EU) запровадив нову низку правил щодо організацій поза EU, які зберігають дані про громадян країн EU - General Data Protection Regulation (GDPR)), поганий користувальницький досвід, особам доводиться керувати великою кількістю облікових записів, а також відсутній контроль користувачів над своїми даними. Згідно з Рис. 1.1, блокчейн дозволяє прискорити процеси верифікації, знизити витрати на верифікацію, підвищити рівень конфіденційності та безпеки даних. У блокчейні не зберігається персональна ідентифікаційна інформація користувача. [2]

1.3 Складові децентралізованої системи ідентифікації

Шахрайство із сертифікатами, підроблені облікові дані, повільні процеси перевірки та витоки даних – це лише деякі проблеми, пов’язані з нашими поточними централізованими системами цифрової ідентифікації, які може вирішити технологія децентралізованої ідентифікації. Децентралізована ідентифікація — це тип керування ідентифікацією, який допомагає організаціям-видавцям створювати облікові дані, захищені від шахрайства, і дає можливість перевірочним організаціям миттєво підтверджувати автентичність цих облікових даних, як показано на Рис. 1.2. Термін «децентралізована ідентичність» використовується як взаємозамінний із самосуверенною ідентифікацією (далі SSI, Self-Sovereign Identity), що є підходом до цифрової ідентичності, який дає людям можливість контролювати свої цифрові ідентифікаційні та облікові дані

самостійно, не покладаючись на будь-яку третю сторону для підтвердження своїх запитів (дивитися на Рис. 1.3).

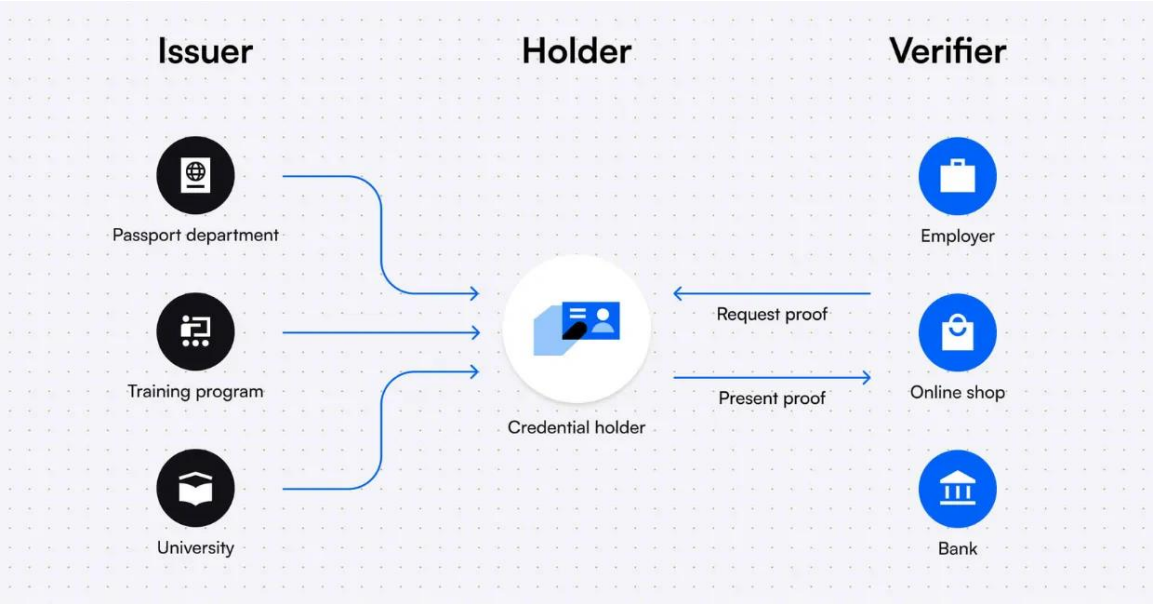


Рис. 1.2 Діаграма роботи Децентралізованої системи ідентифікації

Технологію децентралізованої ідентифікації можна застосовувати до дедалі більшої кількості кейсів, включаючи багаторазову цифрову ідентифікацію, відстеження ланцюга поставок, видачу захищених від шахрайства сертифікатів і керування ідентифікаторами працівників.

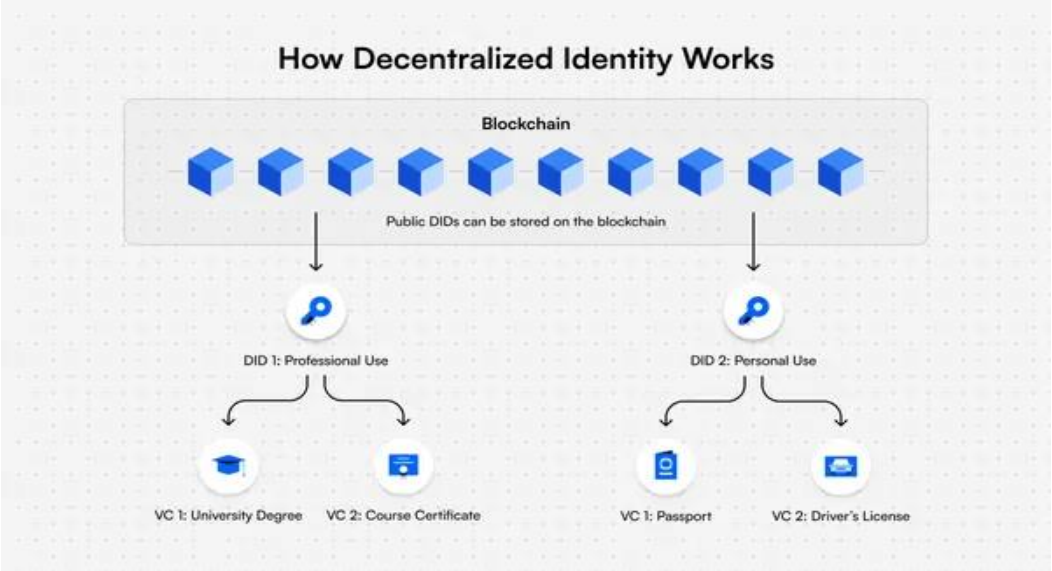


Рис. 1.3 Основна структура видачі VC та зберігання DID у Децентралізованій системі ідентифікації

Децентралізована система ідентифікації має декілька головних елементів: [4]

- **блокчейн –** децентралізована база даних, що синхронізується між усіма серверами в мережі, містить публічний DID користувачів та публічний DID + відповідний публічний криптографічний ключ видавців [3], реєстри відкликань виданих документів, підтвердження видачі облікових даних (тільки якщо користувач спеціально погодився на цю функцію).
- **децентралізований гаманець особи (далі DIW, Decentralized Identity Wallet)** – програма, за допомогою якої користувач може створити свій DID та керувати своїми VC; також зберігає VC, DID та Personal Identity Information користувача.
- **децентралізовані ідентифікатори (далі DID, Decentralized Identifiers)** – унікальний ідентифікатор особи, рядок що складається з літер та цифр та містить в собі публічний ключ та перевірочну інформацію для блокчейну; не містить особистих даних (далі PII, Personal Identifiable Information) чи інформацію з гаманця. Користувач може мати декілька DID для різних інтеракцій в інтернеті (окремі для онлайн ігор, навчання, роботи та онлайн покупок).
- **верифіковані облікові дані (далі VC, Verifiable Credentials) –** цифрова, криптографічно зашифрована версія паперових та цифрових облікових даних (наприклад паспорт, професійні сертифікати, статус робітника, права на водіння), за якою їх можуть верифікувати сторонні особи. Щоб називатися VC, цифрові облікові дані мають відповідати Verifiable Credentials Data Model 1.0, визначеному World Wide Web Consortium (W3C).

Три основні залучені сторони даної системи (дивитися Рис. 1.4): [4]

- **Holder –** користувач, який створює DID за допомогою застосунку цифрового гаманця та отримує VC
- **Issuer –** організація, яка підписує VC своїм приватним ключем та видає його власнику
- **Verifier –** особа, що перевіряє дані та має доступ до публічного ключа Issuer (Issuer's DID) у блокчейні, щоб верифікувати підпис Issuer на спільному Holder VC

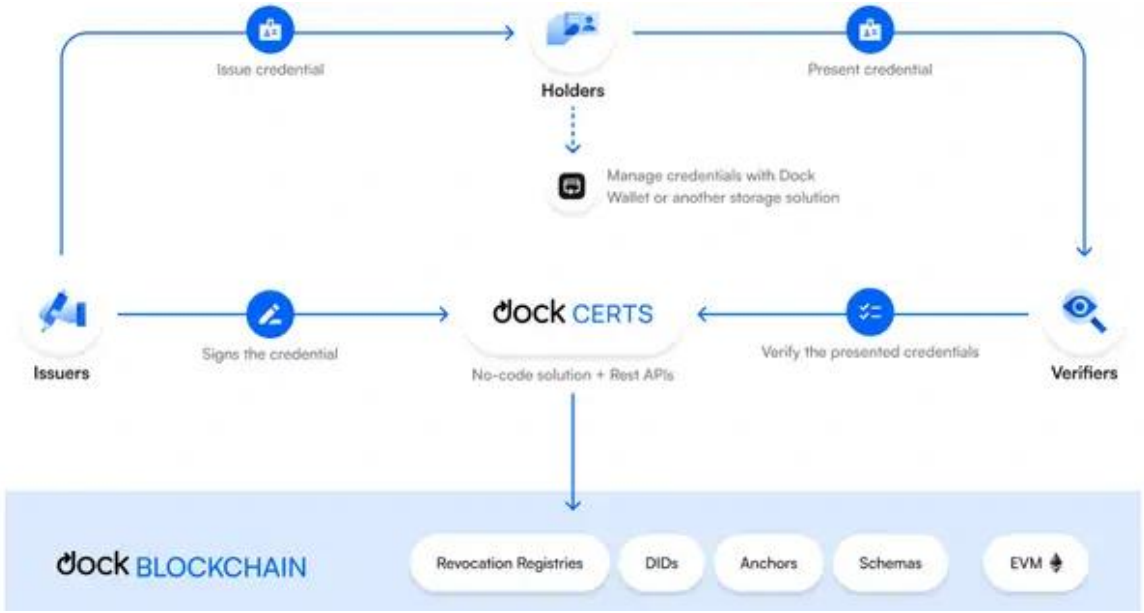


Рис. 1.4 Детальний огляд системи децентралізованої ідентифікація особи

Centralized Identity Management	**Decentralized Identity Management**
Increased risk of data breaches from storing data in a centralized system	Data is decentralized and stored by users in their wallets, which reduces the risk of large scale data breaches
Data may be collected, stored, and shared with other parties without your knowledge	Data is only shared when you give authorization
Data is owned and controlled by organizations, apps, and services	Data is fully owned and controlled by the user

Таб. 1.1 Порівняння централізованої та децентралізованої систем ідентифікації

У Таб. 1.1 показано, що технологія децентралізованої ідентифікації вирішує багато проблем, пов’язаних із централізованими та об’єднаними системами керування ідентифікацією, включаючи широко поширене шахрайство із сертифікатами, повільні та дорогі процеси перевірки та ризики витоку даних. [4]

Також варто зауважити, що у цій сфері дуже жорсткі стандарти, які посилюються кожного року, адже держави починають все більше турбуватися про безпеку особистих даних своїх громадян через підвищення ризику (General Data Protection Regulation + eIDAS 2.0 regulation впроваджені EU). Основні організації, які працюють над забезпеченням цих вимог по всьому світу: [4]

- Decentralized Identity Foundation (DIF)
- World Wide Web Consortium (W3C)
- Internet Engineering Task Force (IETF)

1.4 Огляд українського застосунку «Дія»

Коли внутрішні процеси управління в державі здійснюються за допомогою інформаційних технологій, вони стають ефективними й прозорими, а кожен громадянин має доступ до публічної інформації про державу. Державні послуги стають зрозумілішими й доступними в електронній формі, а органи влади завжди мають правдиві дані для ухвалення ефективних рішень. Дія — це взаємодія «Держава і я”. Дія — це застосунок в якому усі потрібні документи в одному місці, у вашому смартфоні. [6] Дія (див. Рис. 1.5) - це ключовий елемент проєкту «Цифрова держава», що має за мету об’єднати всі відомства в одну єдину зручну й дієву онлайн-систему. На разі на сайті Дії перелічено 94 різних проєктів з цифрової трансформації України. [5] Продукт розвивається під керівництвом Міністерства цифрової трансформації України та за

спонсорства/підтримки багатьох європейських агенцій, фондів, проєктів; не фінансується за рахунок державних коштів України. Також нещодавно Дія стала Open Source, надавши доступ до всього свого коду на GitHub з ліцензіюванням. [6]

Дія поєднує в собі:

- онлайн-сервіс державних послуг
- мобільний застосунок з електронними документами та даними про людину з реєстрів
- портал з онлайн-курсами
- портал з допомоги малому та середньому бізнесу
- центри надання адміністративних послуг (Центри Дії)
- спеціальний правовий режим для IT-індустрії

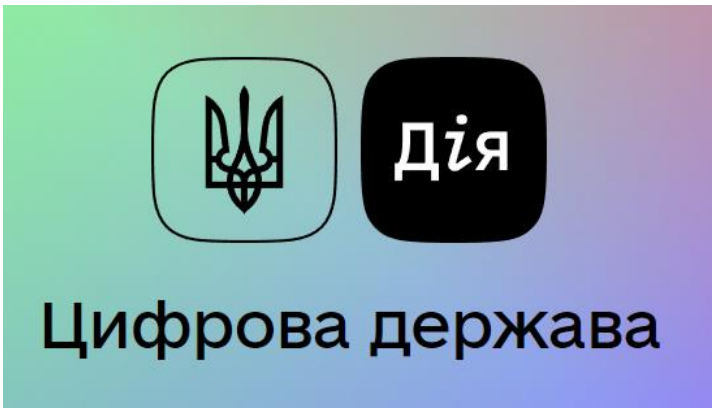


Рис. 1.5 Логотип проєкту «Цифрова держава» та Дії

Також Дія дозволяє інтеграцію для валідації та шерингу копії цифрових документів у форматі pdf-файлів.

Авторизація користувача відбувається за допомогою BankID (через Приватбанк або один з 12 банків системи Національного банку україни), користувач надає доступ лише до Personal Identifiable Information (далі PII). Отримана інформація передається на смартфон користувача у вигляді зашифрованого і підписаного криптопримітива. [7] Він не

розшифровується на пристрої, а лише слугує ключем, за яким застосунок отримує доступ до документів. Електронні документи користувача з’являються у застосунку автоматично, за наявності повних даних у центральному реєстрі. Для захисту персональних даних використовується підхід «глибокого захисту» (defense-in-depth), також було проведено відповідні пен-тести, тобто тестування безпеки застосунку компанією EPAM.

Архітектура застосунку Дія побудована таким чином, що на серверній частині не здійснюється зберігання персональних даних користувачів, а лише в разовий запит ідентифікованого громадянина відображає інформацію з центральних реєстрів отриману через API запит. [7] При цьому інформація в каналах передачі даних передається у зашифрованому вигляді, а на деяких етапах – використовується подвійне шифрування. Усі сервери мобільного застосунку Дія розташовані в Україні. Серверна частина системи розгорнута в хмарній інфраструктурі компанії-партнера De Novo, яка має необхідні сертифікати безпеки (КСЗІ). Також Дія використовує послуги одної зарубіжної компанії для захисту від атак розподіленого доступу (DDOS-атак) – інфраструктуру компанії Amazon у Німеччині. Застосунок Дія пройшов низку позитивних аудитів – як приватних, так і державних (ДССЗЗІ). [8]

Для того щоб перевірити достовірність документів у Дії, використовується QR-код. У QR-коді зашифрований одноразовий пароль, який дозволяє верифікувати документ. Він дійсний лише три хвилини.

Також, у 2023 році була розроблена нова децентралізована система електронної взаємодії державних електронних інформаційних ресурсів «Трембіта». Вона створює зв'язок між реєстрами та їх інформаційними системами, та реалізує механізми захищеного обміну даними. [9] Каталог системи Трембіта призначений для накопичення, обліку та відображення

інформації про суб’єктів системи Трембіта, електронні інформаційні ресурси, підсистеми, програмні інтерфейси електронних інформаційних ресурсів, сервіси та електронні інформаційні взаємодії, а також для спрощення подачі всіх видів заявок згідно Регламенту роботи системи Трембіта. Система "Трембіта" є одним із ключових елементів інфраструктури надання електронних послуг громадянам та бізнесу, який забезпечує зручний уніфікований доступ до даних державних реєстрів.

Основу системи "Трембіта" становить удосконалена естонська платформа обміну даними X-ROAD, яка є фундаментом естонського цифрового суспільства. [10]

Функціонування та експлуатація системи “Трембіта” визначається регламентом [11], що визначає організаційні та технічні умови забезпечення електронної інформаційної взаємодії. Учасниками системи "Трембіта" є органи державної влади, органи місцевого самоврядування та суб’єкти господарювання

1.5 Огляд Digital Identity Wallet Європейського Союзу та можливостей European Blockchain Services Infrastructure

Європейська інфраструктура блокчейн-сервісів (EBSI) — це передова блокчейн-мережа, розроблена для публічних послуг. Вона об’єднує майже 40 державних органів з усіх європейських країн через уніфіковану мережу блокчейн, безперебійно обмінюючись даними через спільну журнал транзакцій. EBSI — це мережа, яка охоплює всі 27 держав-членів ЄС у рівних умовах, а також Норвегію та Ліхтенштейн, об’єднуючи різні державні установи з метою покращення доступу до закордонних державних послуг. EBSI розвинувся з єдиного середовища до шести різних середовищ, кожне з яких розгорнуто в певному масштабі. Розробляється у партнерстві European Commission та European Blockchain (далі EBP), до якого Україна

приєдналася в статусі спостерігача в червні 2022 року. Також у вересні 2022 року Blockchain4Ukraine увійшло до консультативної ради міжнародної асоціації International Association for Trusted Blockchain Applications (INATBA). Також Україна входить у консорціум Potential. [12]

EBSI — це загальнодоступна блокчейн-мережа з дозволами, пропонує загальнодоступні API для взаємодії з обліковою журналом. Вона має сувору процедуру отримання дозволу для приєднання до мережі як звичайним вузлам (нодам, серверам), так і вузлам перевірки. [13]

Digital Identity Wallet (DIW), розроблений Європейською Комісією в рамках European Blockchain Services Infrastructure (EBSI), представляє собою передовий інструмент для керування та захисту цифрової ідентичності громадян. Цей гаманець використовує низку технічних інновацій та протоколів безпеки для забезпечення надійного зберігання та обміну особистих даних. Декількома хорошими прикладами таких вже розроблених гаманців є Altme [14], walt.id [15] та Gataca [16].

На відміну від традиційних ідентифікаторів, які часто зберігаються централізовано, DIW використовує блокчейн-технологію для розподіленого зберігання даних. Це забезпечує високий рівень безпеки, оскільки інформація розподіляється по всій мережі і кожен блок має підпис, що гарантує його непорушеність.

Протоколи безпеки, такі як JSON Web Tokens (JWT) та OAuth 2.0, використовуються для забезпечення автентифікації та авторизації користувачів. JWT використовується для створення токенів доступу, які надають можливість користувачам автентифікуватися без необхідності надання свого пароля кожного разу. OAuth 2.0 використовується для керування доступом до ресурсів, що дозволяє користувачам контролювати, як їхні дані використовуються.

Крім того, DIW підтримує стандарти децентралізованих ідентифікаторів, таких як Decentralized Identifiers (DIDs) та Verifiable Credentials (VCs), що дозволяє користувачам контролювати свою ідентичність та обмінюватися даними безпосередньо з іншими користувачами чи сервісами.

1.6 Порівняння технологічних аспектів роботи Дії та Digital Identity Wallet

Отже, для підсумування пунктів 1.4 та 1.5 цього розділу я створила табличку з порівнянням певних технічних аспектів Дії та EUDI Wallet, дивитися Таб. 1.2.

	Дія	**EUDI Wallet**
Масштаб програми	Україна, одна країна	EU+
Зберігання облікових даних користувачів	Централізоване	Децентралізоване
Основна база даних для подальшої перевірки документів	Центральний реєстр	Блокчейн, EBSI
Інформація, що зберігається про користувача в організації	PII, інформація з гаманця, документи	DID, публічні ключі
Спосіб авторизації користувача в застосунку	BankID	OAuth 2.0; certain DID; certain VC

Таб. 1.2 Порівняння технологічних аспектів Дії та EUDI Wallet

Розділ 2. КРОКИ ПІДКЛЮЧЕННЯ ДОДАТКУ «ДІЯ» ДО EUROPEAN BLOCKCHAIN SERVICES INFRASTRUCTURE. ЕЛЕМЕНТИ АРХІТЕКТУРИ

2.1 Зберігання даних про користувачів та їх Verifiable Credentials. Налаштування Blockchain

2.1.1 Підключення до EBSI мережі серверів

EBSI — це однорангова мережа розподілених вузлів по всій Європі, яка підтримує програми, орієнтовані на вибрані варіанти використання. Кожен учасник мережі, уповноважений членом ЕВР, розміщує вузли EBSI на національному рівні. Усі вузли можуть створювати та транслювати транзакції, які оновлюватимуть реєстр. Кожен вузол зберігає ідентичну копію цієї книги. [17]

Для того щоб підключитися до EBSI мережі серверів, початковою ідеєю було розгорнути одну або дві ноди EBSI блокчейну на персональному девайсі, синхронізувати їх та отримати доступ до перегляду журналу транзакцій. Кожен вузол EBSI може розгортати одне або кілька середовищ EBSI: пілотне середовище для тестування користувачами або середовище Pre-Production і Production для прийняття та активації мережі EBSI відповідно. Для кожного середовища існують технічні та юридичні: відповідні Загальні умови/Заява про відповідність і додана угода про обробку даних, Відповідні SLA та правила експлуатації, викладені в Операційній книзі оператора вузла (NOOB), Мінімальні технічні вимоги, включені в NOOB. [17] Ноди бувають двох основних типів, а саме звичайні ноди та ноди-валідатори.

Будь-яка організація в одній із країн Європейського блокчейн-партнерства (ЄС 27 + Норвегія та Ліхтенштейн) може розмістити вузол EBSI за умови дотримання певних умов. Існують мінімальні технічні

вимоги та SLA, яких необхідно виконати, і всі вони викладені в Загальних умовах оператора вузла EBSI. Кандидат в оператора вузла також повинен запитати схвалення члена ЕВР у своїй країні у вигляді сертифікату ISO27001. [18] Також потрібно напряму проконтактувати з EBSI та заповнити спеціальну форму на їх вебсайті. [19] Мій куратор Кирило Семенович Гороховський спробував сконтактувати з їх групою підтримки, але комунікація не дійшла позитивного для нас результату. Отже, було вирішено спробувати інший метод.

2.1.2 Розвертання власного Ethereum нода з допомогою Geth та Prysm

Цього разу була поставлена задача дослідити, як влаштована нода низькорівнево, які її складові та запустити власну ноду.

Спочатку серед усіх платформ для блокчейну, таких як IBM, Ripple, Microsoft Azure Blockchain, Bitcoin, Blockstream, було обрано Ethereum. Таке рішення було прийняте, бо нещодавно вийшло нове оновлення Ethereum 2.0 з багатьма новими фічами та покращеннями. Також саме з Ethereum почалася ера криптовалют та NFT на ринку.

У 2022 році Ethereum та низка інших платформ перейшли на Proof-of-stake процедуру замість Proof-of-work. Підтвердження частки (PoS) лежить в основі механізму консенсусу Ethereum. Ethereum увімкнув цей механізм, оскільки він є більш безпечним, менш енергоємним і кращим для реалізації нових рішень масштабування порівняно з попередньою архітектурою підтвердження роботи (PoW). [20] Доказ частки — це спосіб довести, що валідатори вклали в мережу щось цінне, що може бути знищено, якщо вони діятимуть нечесно. У доказі частки Ethereum валідатори явно вкладають капітал у формі ETH у смарт-контракт на Ethereum. Тоді валідатор відповідає за перевірку того, що нові блоки, що розповсюджуються через мережу, дійсні, а також час від часу сам створює та розповсюджує нові блоки. Якщо вони намагаються обдурити мережу (наприклад, пропонуючи

кілька блоків, коли вони повинні надіслати один, або надсилаючи суперечливі атестації), частина або весь їхній ETH може бути знищений. [21]

Ethereum — це децентралізована мережа вузлів, які спілкуються через однорангові з'єднання. Ці з'єднання формуються комп'ютерами, на яких працює спеціалізоване клієнтське програмне забезпечення Ethereum, див. Рис. 2.1. [22]

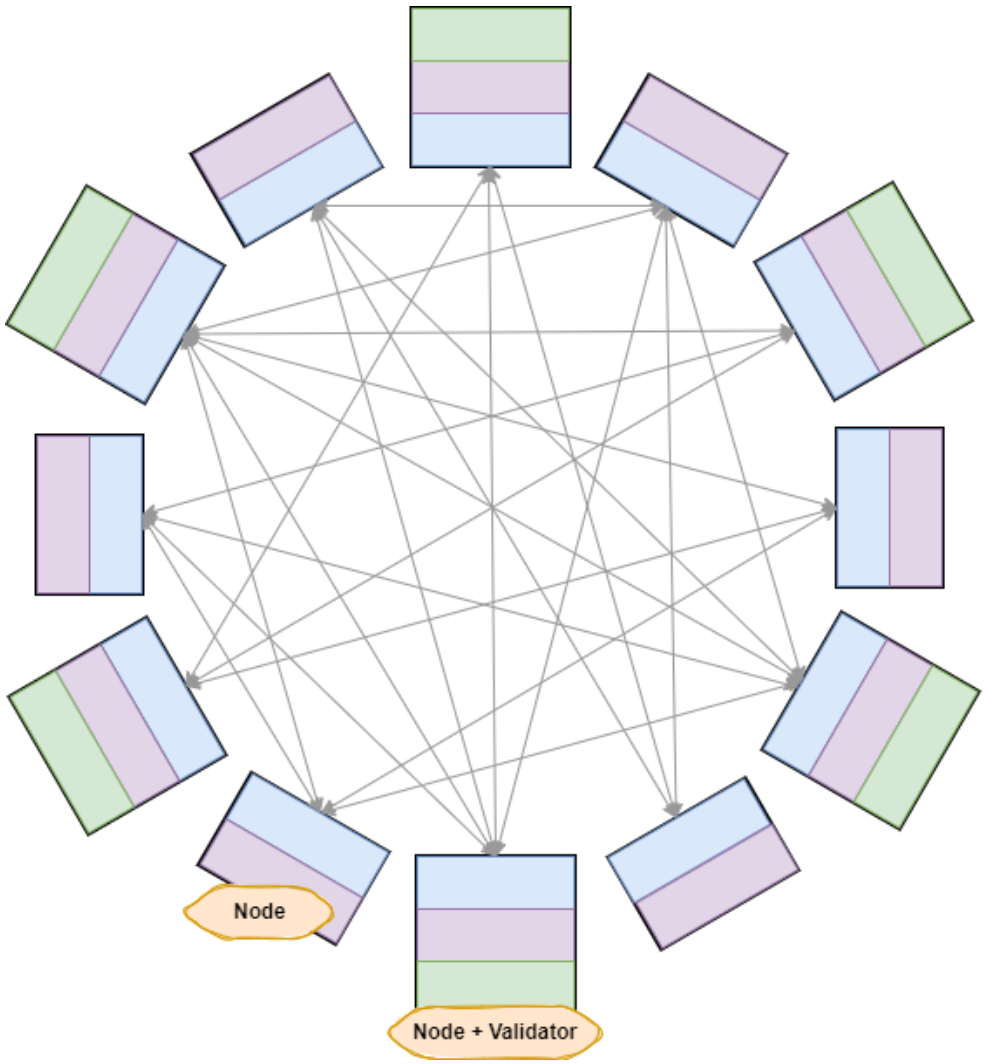


Рис. 2.1 Макет мережі Ethereum з різними серверами

Вузол Ethereum — це запущений екземпляр клієнтського програмного забезпечення Ethereum. Це програмне забезпечення відповідає за роботу блокчейну Ethereum. [22]

Три основні види вузлів, див. Рис. 2.2:

- Execution node – шар виконання
- Beacon node – шар згоди
- Validator client

Повна Ethereum нода складається з execution та beacon нод, що разом виконуються.

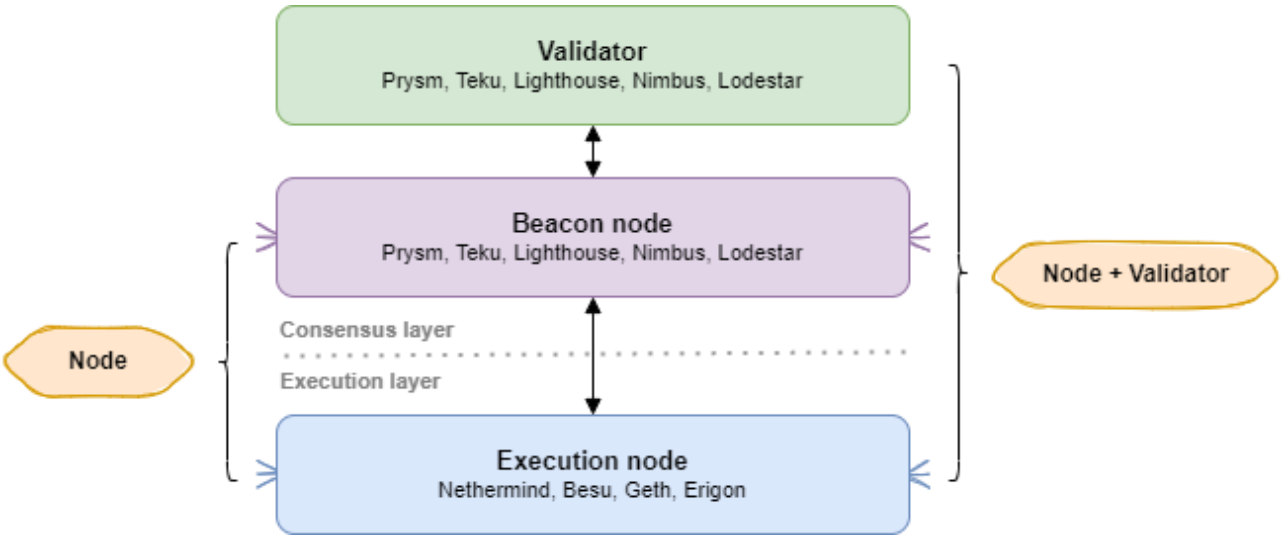


Рис. 2.2 Типи вузлів у мережі Ethereum та взаємодія між ними

Мережа Ethereum, у якій розміщені програми, називається Mainnet Ethereum. Ethereum Mainnet — це активний виробничий екземпляр Ethereum, який карбує та керує реальним Ethereum (ETH) і зберігає реальну грошову вартість.

Існують інші активні тестові екземпляри Ethereum, які карбують і керують тестовим Ethereum. Кожна тестова мережа сумісна (і тільки з) своїм типом тестового ETH. Ці тестові мережі дозволяють розробникам, користувачам вузлів і валідаторам тестувати нові функції перед використанням справжнього ETH у мережі Mainnet.

Кожна мережа Ethereum ділиться на два рівні: рівень виконання (EL) і рівень консенсусу (CL), див. Рис. 2.3. [21]

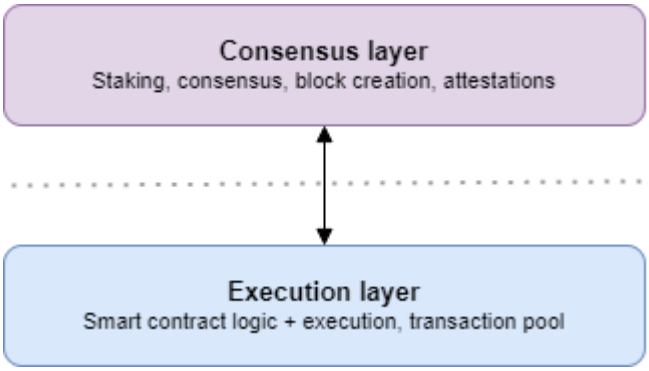


Рис. 2.3 Два рівні мережі Ethereum: CL та EL

Як видно на Рис. 2.2, для того щоб створити одну повну ноду треба запустити execution node за допомогою, наприклад, Geth та запустити beacon node за допомогою, наприклад, Prysm. Prysm (на Go) це клієнт згоди PoS Ethereum, який було згадано раніше. Geth (на Go) був частиною Ethereum з самого початку, найбільш загартований і перевірений клієнт. Geth — це клієнт виконання Ethereum, тобто він обробляє транзакції, розгортання та виконання смарт-контрактів і містить вбудований комп'ютер, відомий як віртуальна машина Ethereum. Запуск виконавчого Geth разом із консенсусним клієнтом Prysm перетворює комп'ютер на вузол Ethereum. [23]

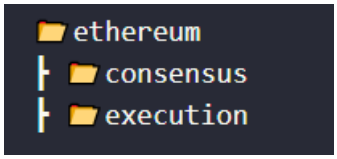


Рис. 2.4 Структура папок на початку створення одного Ethereum вузла

Щоб створити свою ноду було виконано інструкції з детального гайду від Prysm: [24]

- створено файлову структуру як на Рис. 2.4
- у папці consensus через Terminal запущено команди, щоб завантажити Prysm клієнта та дозволити обширне логування

curl https://raw.githubusercontent.com/prysmaticlabs/prysm/master/prysm.bat --output prysm.bat

reg add HKCU\Console /v VirtualTerminalLevel /t REG_DWORD /d 1

- Далі, щоб створити JWT автентифікацію для HTTP Connection між виконавчим та вузлом згоди

prysm.bat beacon-chain generate-auth-secret

- Переносимо jwt.hex файл згенерований минулою командою у папку ethereum
- Завантажте та запустіть останню 64-розрядну стабільну версію Geth для вашої операційної системи зі сторінки завантажень Geth [25]. Перемістіть виконуваний файл geth у папку execution
- У папці execution запустити команду, щоб почати execution node (див. Рис. 2.5)

geth --sepolia --http --http.api eth,net,engine,admin --authrpc.jwtsecret=”..\jwt.hex”

- У папці consensus запускаємо команду, щоб почати consensus node (див. Рис. 2.6)

prysm.bat beacon-chain --execution-endpoint=http://localhost:8551 --sepolia --jwt-secret=”..\jwt.hex” --checkpoint-sync-url=https://sepolia.beaconstate.info --genesis-beacon-api-url=https://sepolia.beaconstate.info

Отже, процедура завершена, тепер у нас запущена повноцінна Ethereum node, один з серверів блокчейну.

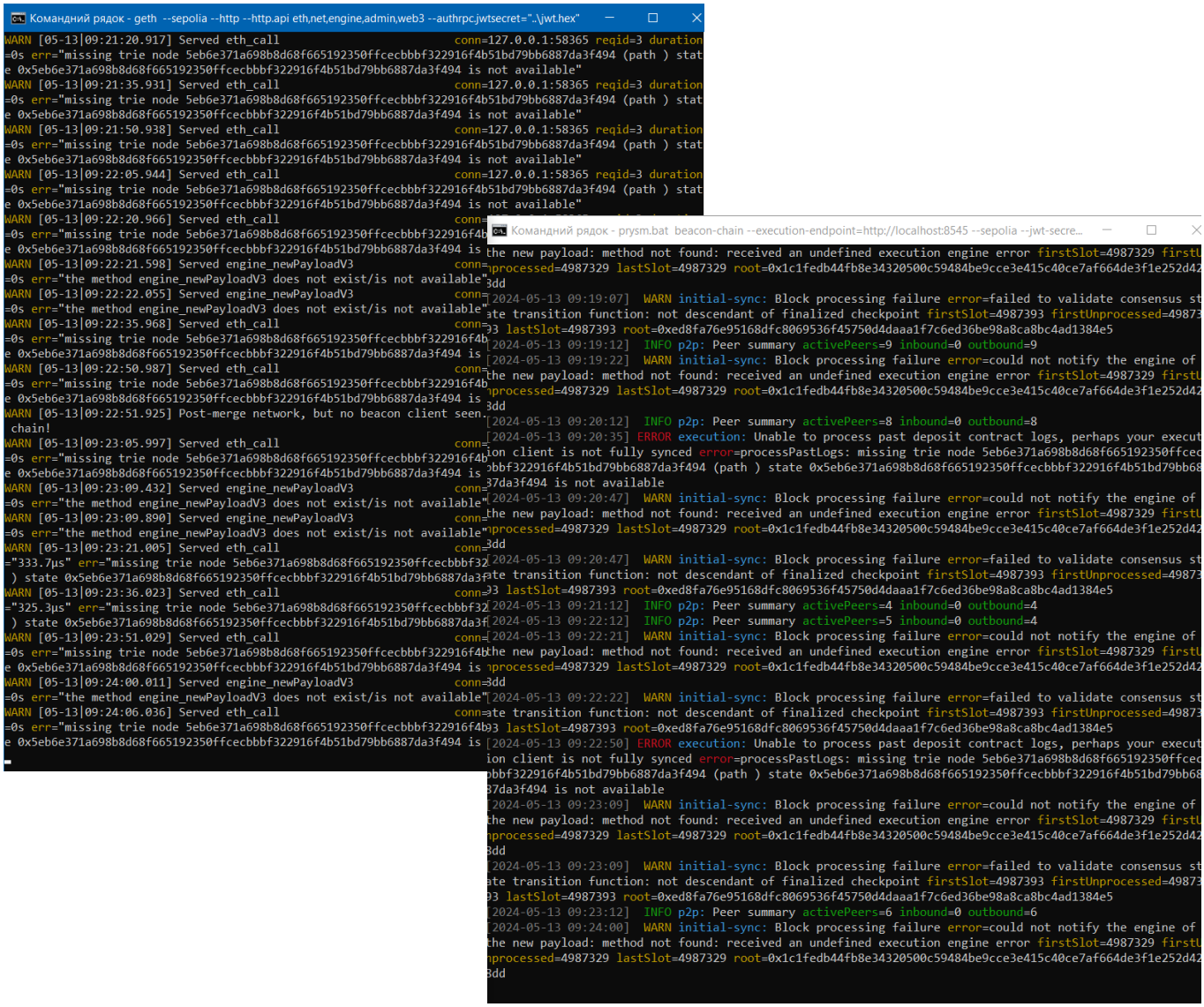


Рис. 2.5, 2.6 Логування процесу запуску та роботи 2.5 – execution node; 2.6 – beacon node. Згори вікон написані відповідні команди.

2.1.3 Наступні кроки для синхронізації декількох нод

Наступним кроком може бути створення декількох таких нод та їх синхронізація, пізніше це дозволить вести деяку комунікацію між ними,

надсилаючи валюту або просто перевірку стану один одному. Функціонуватиме як майже повноцінна приватна мережа (для мереж рекомендують мати непарну кількість нод, тобто 3+). На жаль, це продовження вже не підпадає під масштаб даної роботи, але маю впевненість, що за допомогою попередніх інструкцій з пункту 2.1.2 зробити наступні кроки буде легше (як мінімум деякі етапи).

2.2 Побудова власного API для гаманця Verifier. Демонстрація інших варіантів

2.2.1 Архітектура спрощеного варіанту API для гаманця Verifier

Для прикладу, було обрано створити демо-версію додатку Verifier, який є частиною архітектури EBSI, як було показано в пункті 1.3. Усе теоретичне пояснення про роботу Verifier прошу переглянути в пункті 1.3.

Отже, базуючи свою архітектуру та методи безпеки на The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework виданому в 2023 (стандарт в EU) [26] та на провідних DIW на просторах інтернету [27] [28], я написала свою API використовуючи Java, Spring, Spring Boot, REST Controller. Також для якісної автентифікації під час HTTP Connection я використала Nimbus JOSE+JWT. Додатковою безпековою мірою була автентифікація за допомгою - OAuth 2.0 SDK з OpenID Connect Extensions.

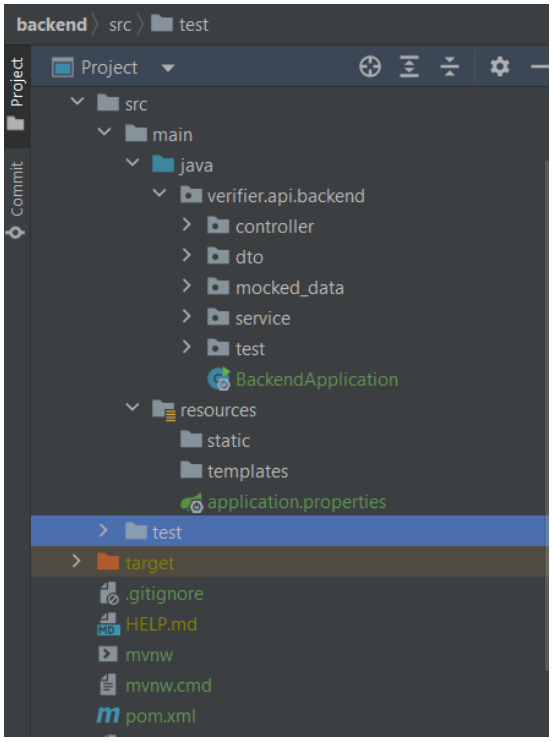


Рис. 2.7 Структура папок проєкту Verifier API на Spring Boot

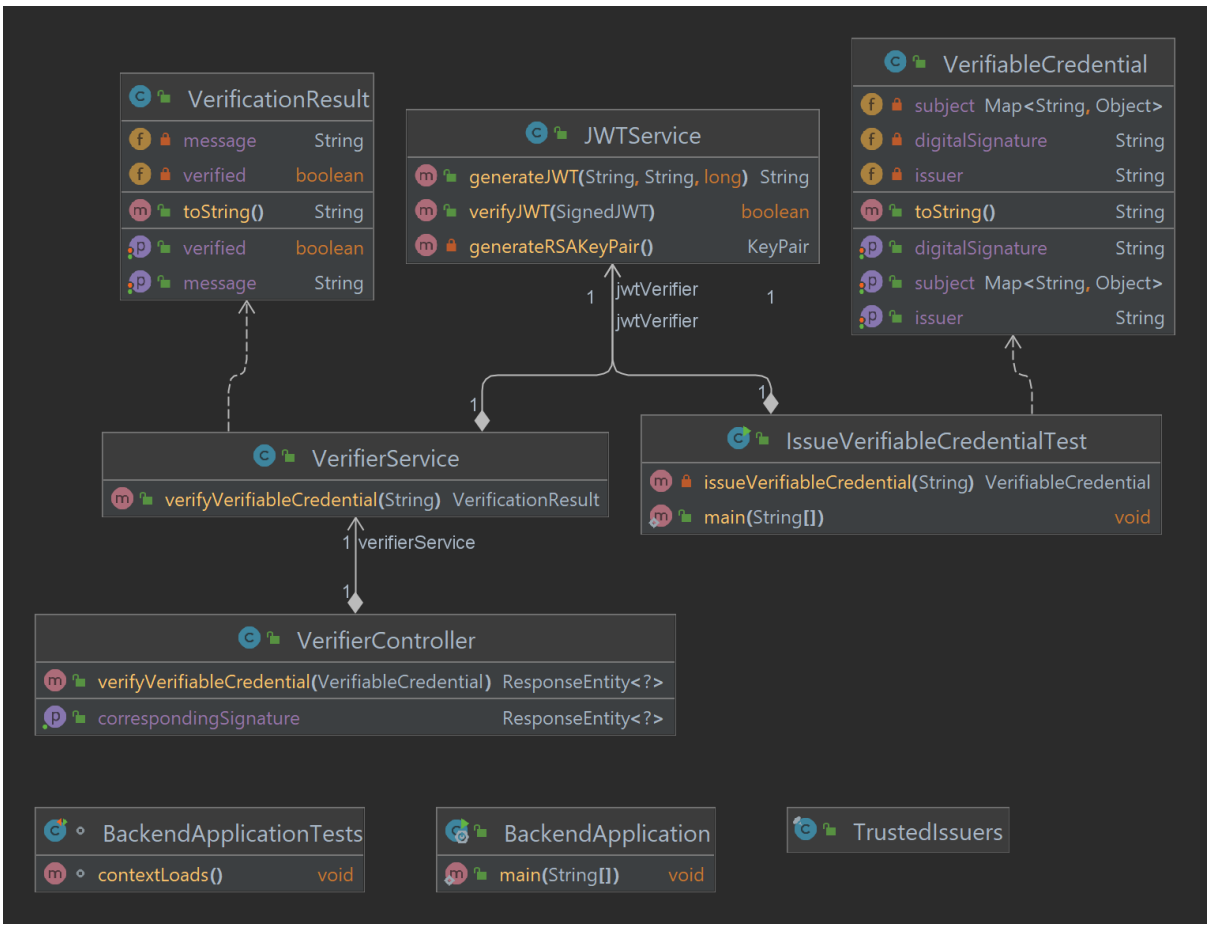


Рис. 2.8 Діаграма Java класів проєкту Verifier API на Spring Boot. Разом зі зв’язками, полями та методами. Згенерована автоматично в IntellliJ IDEA.

На Рис. 2.7 можна побачити структуру папок мого проєкту, стандарт MVC та Spring Boot. У мене реалізовані два запити один з них, для того щоб симулювати видання VC (GET /api/{id}/signature без додаткових параметрів), а інший повноцінний для того щоб верифікувати VC за запитом без видавця (POST /api/verify-vc на вхід json з полями issuer, subject, digitalSignature).

Під час верифікації перевіряється чи публічний DID видавця цього VC є в реєстрі (у майбутньому, децентралізованому блокчейні), чи валідний signed JWT (за допомогою шифрування RS256, пари публічного та приватного RSA ключів), та чи ще не минув термін роботи JWT.

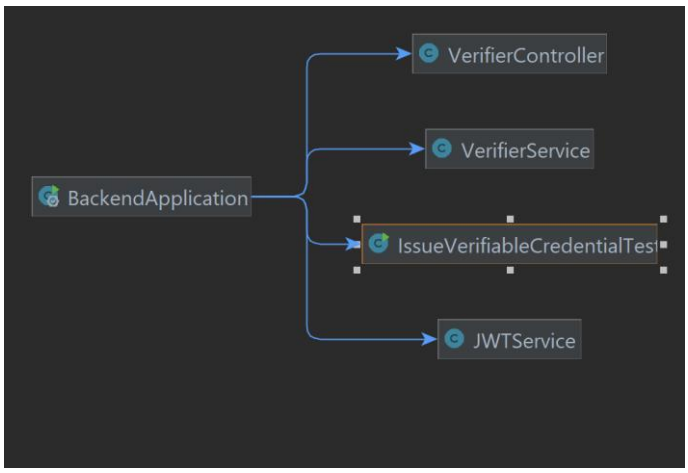


Рис. 2.9 Діаграма залежностей Spring Model проєкту Verifier API на Spring Boot. Згенерована автоматично в IntellliJ IDEA.

На Рис. 2.8 продемонстровано діаграму Java класів моєї програми з усіма зв’язками, полями та методами. Рис. 2.9 доповнює попередню діаграму, але тепер зв’язками/залежностями компонентів Spring Model.

2.2.2 Альтернативні готові до використання рішення

На мою думку, кожному хто зараз знаходиться на стадії дизайну/розробки свого Verifier Wallet або ж будь-якого DIW корисно буде переглянути наступні вже готові рішення (почерпнути ідеї, надихнутися або просто використати вже готове рішення):

- Altma
- walt.id
- Gataca

2.3 Оформлення User Interface у вигляді веб-застосунку для взаємодії з Verifier API

Для того щоб завершити веб-застосунок/плагін Verifier та продемонструвати його роботу, також було створено фронт на React. Були використані наступні бібліотеки: qr-scanner для сканування QR-коду з камери, dotenv для використання змінних середовища, axios для запитів на бек, tailwindcss для легшого дизайну окремих елементів. На Рис. 2.10 можна побачити структуру папок даного проєкту.

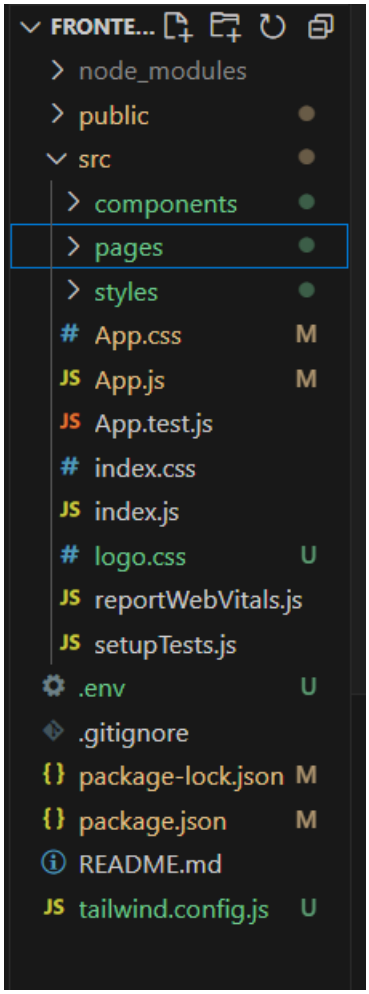


Рис. 2.10 Структура папок у фронті на React для Verifier

Коли користувач тільки заходить у застосунок, на першому екрані він бачить камеру та логотип, як на Рис. 2.11 а), б):

Рис. 2.11 а), б) Початковий екран з камерою та логотипом зі спецефектами

Далі потрібно піднести QR-код до камери, вона спробує його розпізнати (див. Рис. 2.12 а), б)) Якщо камері вдається успішно розпізнати QR-код вона надсилає запит на отримання JWToken за адресою з QR-коду.

Рис. 2.12 а), б) QR-код піднесений до камери для сканування та фокусу

Далі програма обробляє відповідь на свій запит. Якщо документ VC підтверджений див. Рис. 2.13:

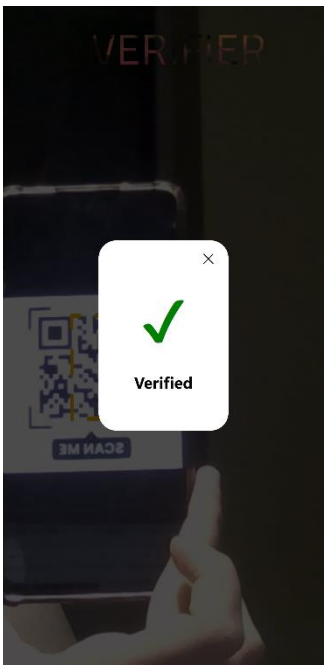
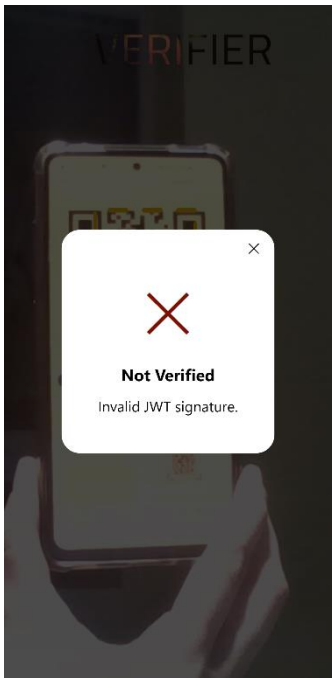
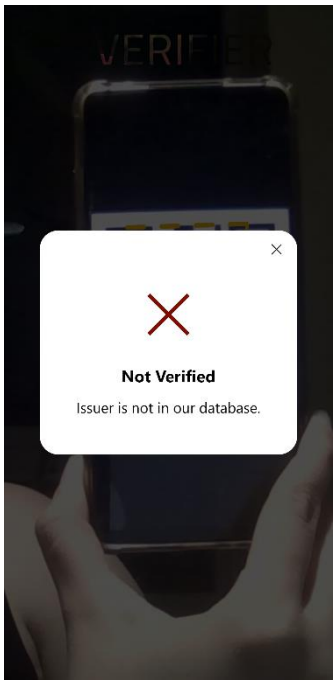


Рис. 2.13 Документ було верифіковано

Якщо документ не був підтверджений програма показує це і додає конкретну помилку знизу, див Рис. 2.14 а), б), в):





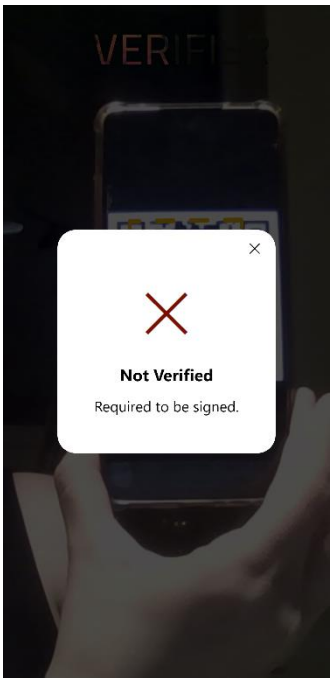


Рис. 2.14 Документ не було верифіковано. Конкретна помилка написала під червоним хрестом

ВИСНОВКИ

У результаті виконання курсової роботи було досліджено відмінності та схожості українського додатку Дія та DIW EU, їх особливості та цікавинки. Також було проведено детальний огляд таких понять як Blockchain, Decentralized Digital Identity System, Digital Identity Wallet. Розглянуто яким чином можливо запустити свої вузли блокчейну на локальному пристрої, та які критерії мають бути виконані, щоб отримати доступ до EBSI Node Operator.

Головним досягненням цієї роботи є step-by-step guide про потенційне підключення Дії до European Blockchain Services Insrustructure. Починаючи від взаємодії з блокчейном, вивчення його сутності, структури. Продовжуючи створенням свого API на Java для використання блокчейну та огляду ключових елементів децентралізованої системи ідентичності. Закінчуючи демонстрацією виконання програми у веб-застосунку на React.

Наступним кроком, продовженням цієї роботи, могла би бути співпраця з програмістами Дії заради швидшого залучення нашої країни до цифрової системи Європейського Союзу.

СПИСОК ПРИЙНЯТИХ СКОРОЧЕНЬ

EBSI – European Blockchain Services Infrastructure

EUDI – European Union Digital Identity

DIW – Digital Identity Wallet

PII – Personal Identifiable Information

DID - Decentralized Identifier

VC - Verifiable Credential

EU – European Union

JWT – JSON Web Token

W3C - World Wide Web Consortium

SSI - Self-Sovereign Identity

API – Application Programming Interface

NFC - Near Field Communication

NOOB - Node Operator Operational Book

SLA - Service-level agreement

PoS – Proof-of-stake

PoW – Proof-of-work

ETH – Ethereum

EL – Execution Layer

CL - Consensus Layer

HTTP - HyperText Transfer Protocol

RSA – Rivest, Shamir and Adleman

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] https://didit.me/blog/what-are-identity-wallets-discover-the-future-of-identity

[2] https://www.dock.io/post/blockchain-identity-management

[3] https://cqr.company/ua/web-vulnerabilities/zlovzhyvannya-kryptografiyeyu/

[4] https://www.dock.io/post/decentralized-identity

[5] https://plan2.diia.gov.ua/

[6] https://github.com/diia-open-source

[7] https://diia.gov.ua/policy

[8] https://thedigital.gov.ua/news/bezpeka-mobilnogo-zastosunku-diya

[9] https://trembita.gov.ua/

[10] https://se.diia.gov.ua/trembita

[11] Trembita Government Portal. (2023). Регламент роботи системи електронної взаємодії державних електронних інформаційних ресурсів «Трембіта» [PDF]. Retrieved from https://portal.trembita.gov.ua/media/website-media/Reglament.pdf

[12] https://www.digital-identity-wallet.eu/

[13] https://hub.ebsi.eu/blockchain

[14] https://altme.io/

[15] https://docs.oss.walt.id/home

[16] https://gataca.io/

[17] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Node+Operators

[18] https://www.ebsi-ne.com/faqs

[19] Robby Goetinck & Deconinck Shane. (2023, December 7). Deploying and Hosting EBSI Nodes Based on Hyperledger BESU [Video]. YouTube. Retrieved from https://www.youtube.com/watch?v=HClN-UI_Muw?t=24m33s

[20] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

[21] https://docs.prylabs.network/docs/install/install-with-script

[22] https://docs.prylabs.network/docs/concepts/nodes-networks

[23] https://geth.ethereum.org/

[24] https://docs.prylabs.network/docs/monitoring/checking-status

[25] https://geth.ethereum.org/downloads

[26] "The Common Union Toolbox for a Coordinated Approach Towards a European Digital Identity Framework: The European Digital Identity Wallet Architecture and Reference Framework" (January 2023), Version 1.0.0.

[27] https://verifier.portal.walt.id/swagger/index.html#/

[28] https://docs.oss.walt.id/verifier/api/vc-oid4vc

ДОДАТКИ

https://github.com/CatsenjoyobservingClouds/project-verifier-ebsi.git

Додаток 1. Посилання на репозиторій проєкту Verifier у GitHub