

Курсова робота

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

Виконано Цвєтковою А.І. БП КН-3

За наукового керівництва Гороховського К.С.

## Актуальність

Для чого потрібне це дослідження?  
Як використати його результати?



## Успішна інтеграція у ЄС

Зараз ми маємо активно рухатися у бік Європейського Союзу на усіх рівнях, включно з цифровою співпрацею. Покращення якості послуг для громадян України та ЄС. Нашою державою уже з 2022 року запущений такий проект.



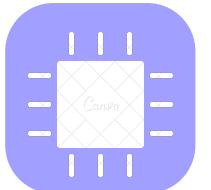
## Підвищення безпеки ДІЇ

Блокчейн технологія ускладнює масові атаки хакерів для отримання даних мільйонів користувачів, захист від російських кібератак.



## Посилена приватність

Користувачі отримують контроль над своїми персональними даними, обирають інформацію для поширення. Важливо для збереження анонімності військових.



## Цифровий розвиток України

Не можна зупинятися у впровадженні нових технологій, сфера розвивається дуже швидко. Професійний зрист наших фахівців.

# Блокчейн

- ✓ **Цілісність даних**  
Прозорі,  
підтвердженні дані
- ✓ **Приватність**  
Контроль над своїми  
даними
- ✓ **Децентралізована,**  
спільна база

асинхронна нереляційна система  
запису інформації в загальну  
децентралізовану базу даних, де  
кожен сервер у мережі має копію  
цифрового журналу транзакцій

- ✓ **Пришвидшений**  
процес верифікації,  
авторизації
- ✓ **Безпека**
- ✓ **Стійкість до**  
втручання

# Елементи Децентралізованої системи ідентичності



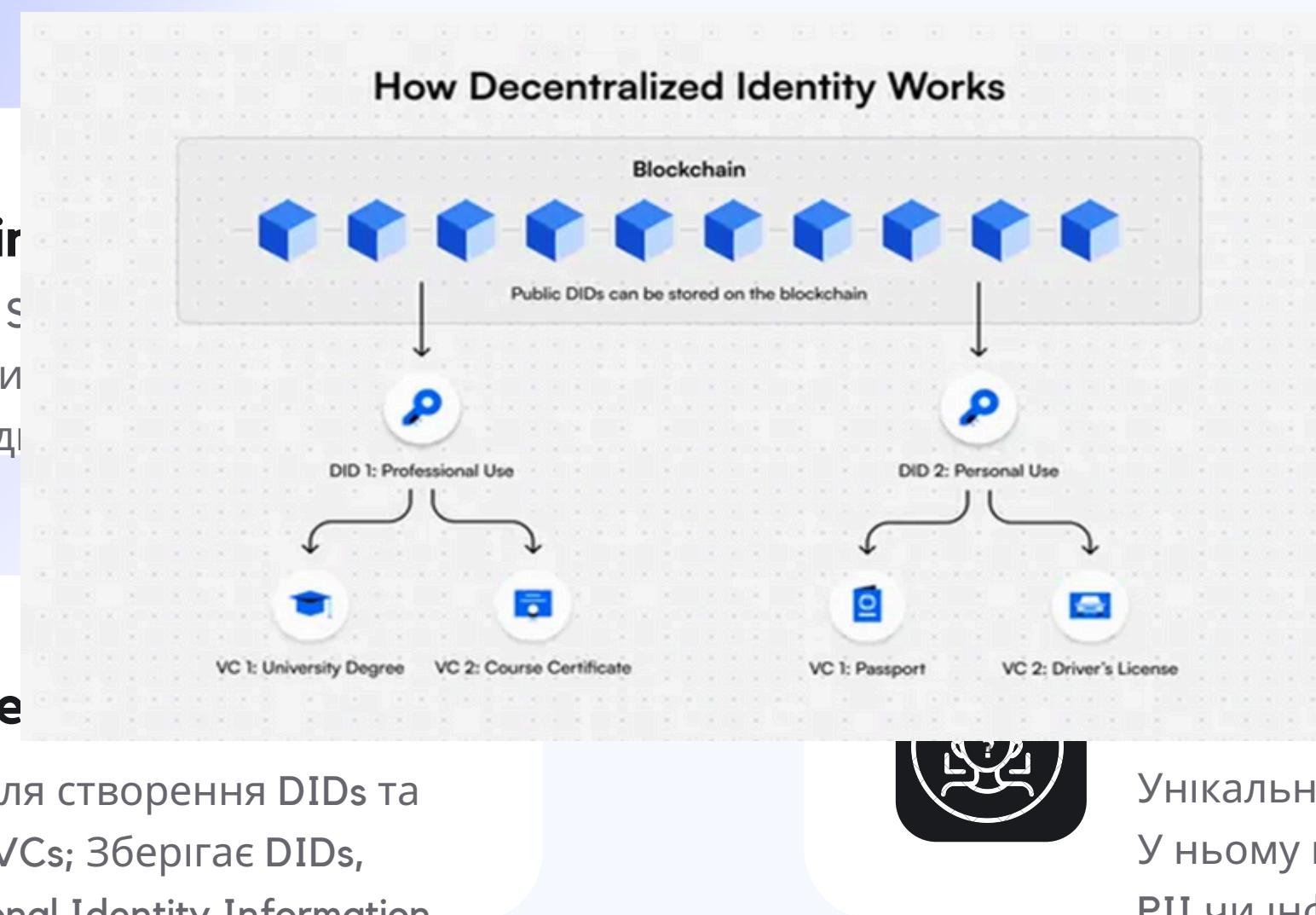
## Blockchair

Забезпечує Decentralized Identity system; Містить відповідальність видавця, відповідальність



## Digital Identity

Програма для створення DIDs та керування VC-s; Зберігає DIDs, VC-s та Personal Identity Information



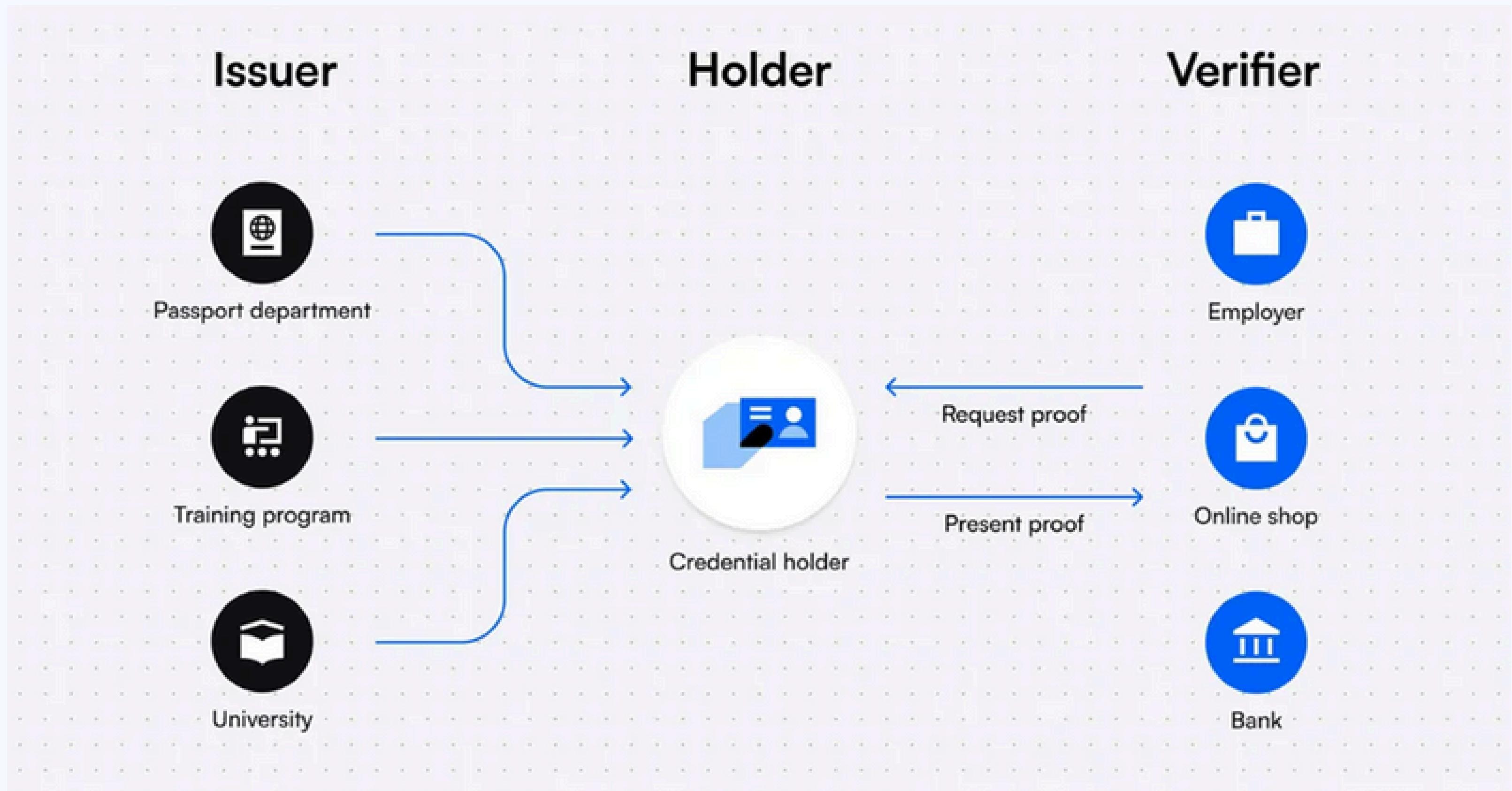
## Digital Credentials

Використовує криптографічно зашифрована інформація про осіб; Відповідає W3C Digital Credentials Data Model 1.0 by W3C



## Decentralized identifiers

Унікальний ідентифікатор особи; У ньому публічний ключ, немає PII чи інформації з DIW. 0+



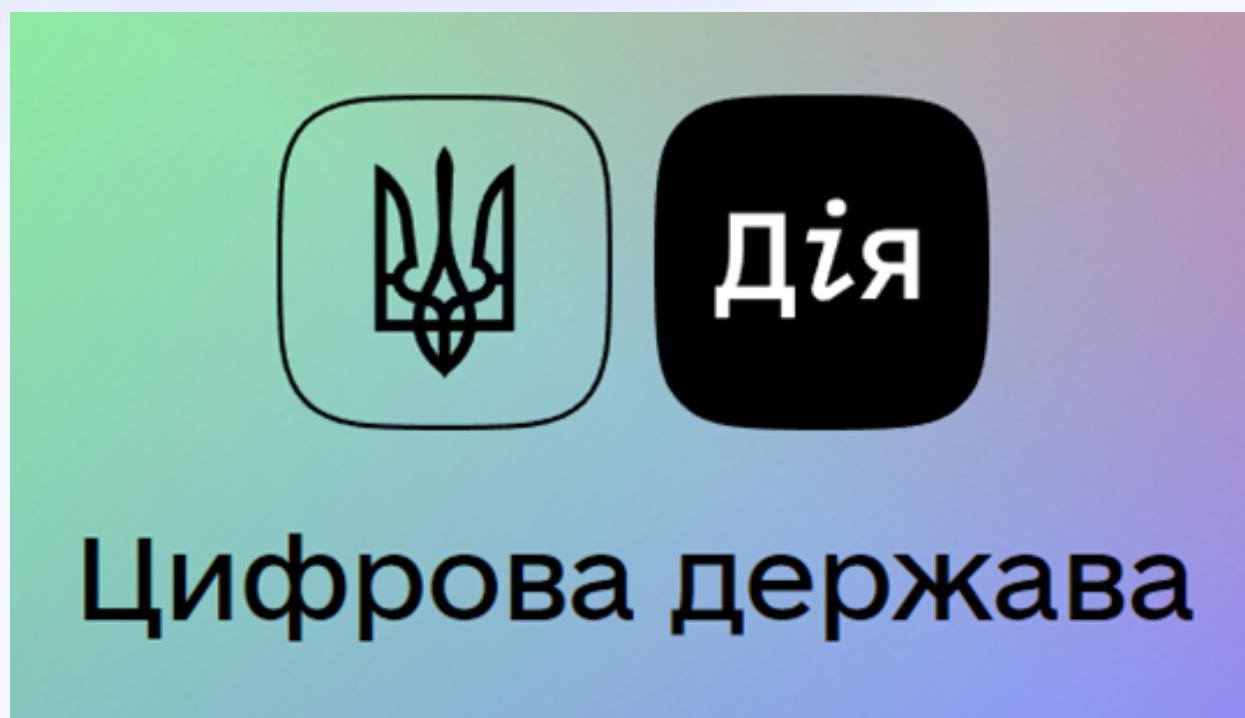
# ДІЯ vs DIW (EBSI)

Порівняння цих двох стандартів додатку електронної  
держави

# Дія

- ключовий елемент проекту «Цифрова держава» в Україні, що має за мету об'єднати всі відомства в одну єдину зручну й дієву онлайн-систему
- поєднує в собі онлайн-сервіс державних послуг та мобільний застосунок з електронними документами та даними про людину з реєстрів

- ✓ **Поширюється на Україну**
- ✓ **Дані користувачів у центральному реєстрі**
- ✓ **Авторизація користувача через BankID**
- ✓ **Defense-in-depth для захисту РІ**
- ✓ **Шифрування/подвійне каналів передачі**



# DIW

- EBSI – це передова блокчейн-мережа, розроблена для публічних послуг у партнерстві European Commission та European Blockchain. Пропонує загальнодоступний API для взаємодії з журналом транзакцій блокчейну.
- Digital Identity Wallet представляє собою передовий інструмент для керування та захисту цифрової ідентичності громадян, забезпечує надійне зберігання та обмін осбистих даних

✓ **Поширюється на EU+**

✓ **Дані користувачів у них на пристрой**

✓ **DID та Public Keys децентралізовано у блокчейні**

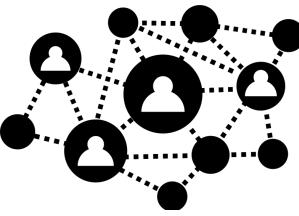
✓ **Авторизація через свій DID або певний VC**  
Далі JWT та OAuth 2.0

✓ **Слідування стандартам ARF та API EBSI**

✓ **Користувачі мають підвищений контроль над своїми даними (за GDPR)**

# Запропоновані практичні кроки

# Налаштування Blockchain



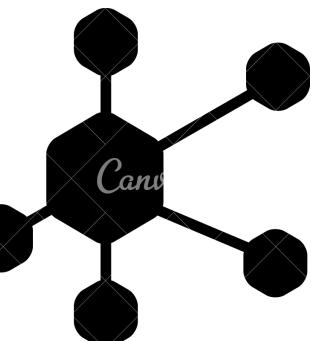
## Підключення до ЕБСІ

Має відбуватися на рівні державної інституції + вимагають ISO27001



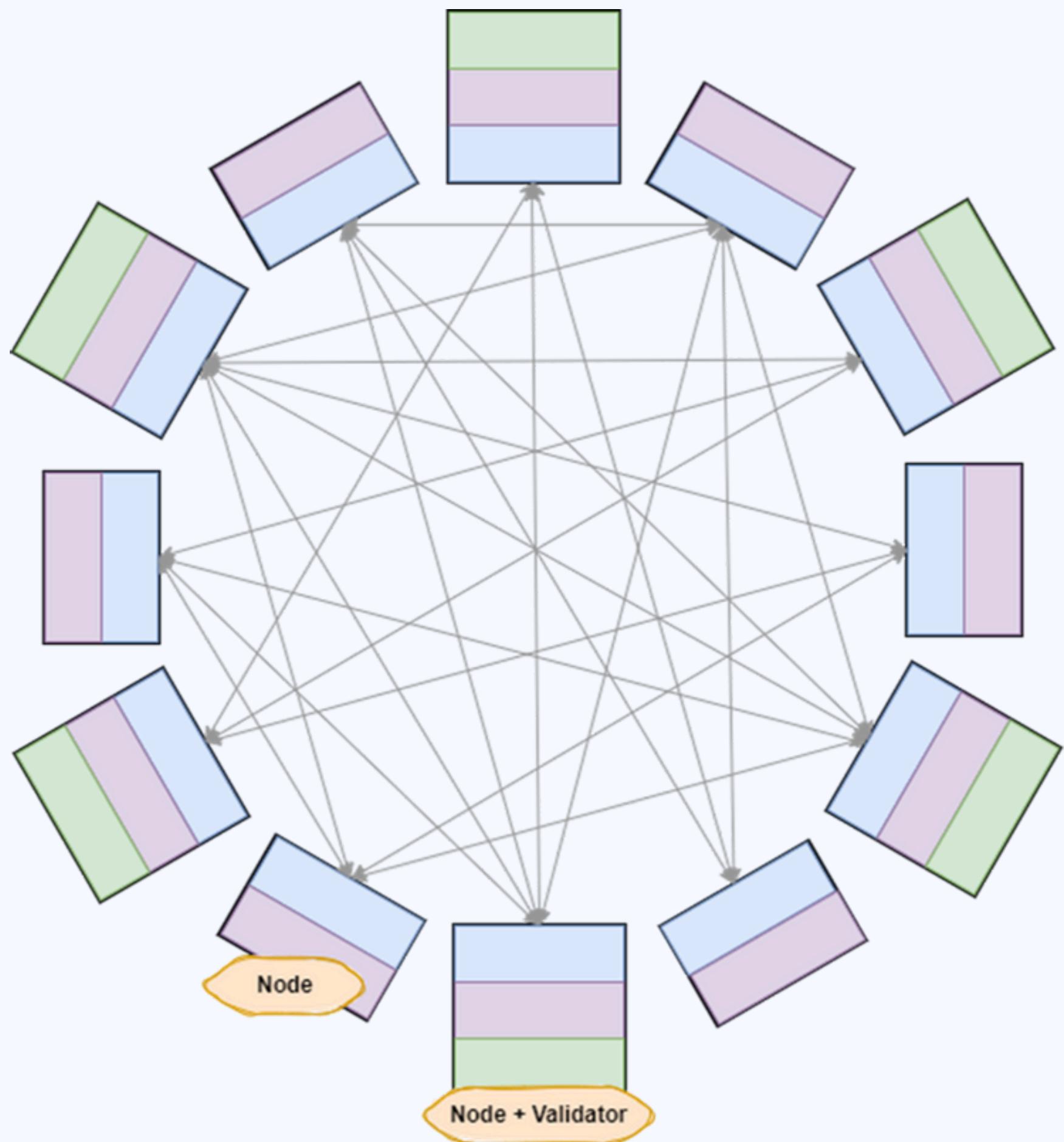
## Розгортання власної Ethereum ноди

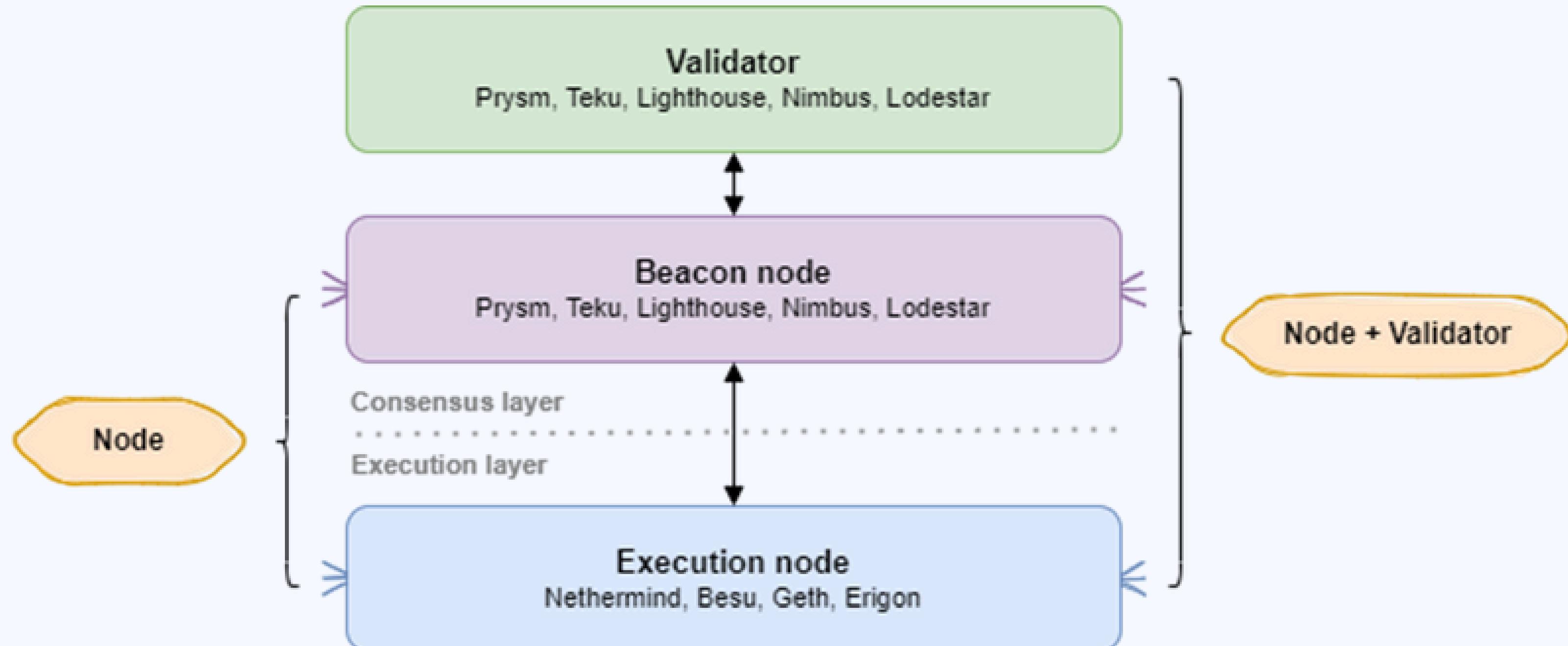
Встановлення та запуск клієнтського програмного забезпечення Ethereum



## Наступні кроки - розгортання мережі з 3+ нод

Синхронізація, комунікація між нодами





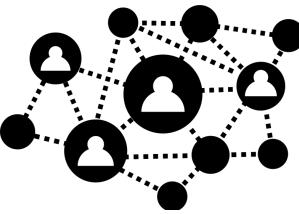
```
Командний рядок - geth --sepolia --http --http.api eth,net,engine,admin,web3 --authrpc.jwtsecret=".\\jwt.hex" - 

WARN [05-13|09:21:20.917] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:21:35.931] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:21:50.938] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:22:05.944] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:22:20.966] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:22:21.598] Served engine_newPayloadV3 conn=127.0.0.1:58365 reqid=4 duration=0s err="the method engine_newPayloadV3 does not exist/is not available"
WARN [05-13|09:22:22.055] Served engine_newPayloadV3 conn=127.0.0.1:58365 reqid=5 duration=0s err="the method engine_newPayloadV3 does not exist/is not available"
WARN [05-13|09:22:35.968] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:22:50.987] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:22:51.925] Post-merge network, but no beacon client seen. Please launch one to follow the chain!
WARN [05-13|09:23:05.997] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:23:09.432] Served engine_newPayloadV3 conn=127.0.0.1:58365 reqid=4 duration=0s err="the method engine_newPayloadV3 does not exist/is not available"
WARN [05-13|09:23:09.890] Served engine_newPayloadV3 conn=127.0.0.1:58365 reqid=5 duration=0s err="the method engine_newPayloadV3 does not exist/is not available"
WARN [05-13|09:23:21.005] Served eth_call conn=127.0.0.1:58365 reqid=3 duration="333.7μs" err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:23:36.023] Served eth_call conn=127.0.0.1:58365 reqid=3 duration="325.3μs" err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:23:51.029] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
WARN [05-13|09:24:00.011] Served engine_newPayloadV3 conn=127.0.0.1:58365 reqid=4 duration=0s err="the method engine_newPayloadV3 does not exist/is not available"
WARN [05-13|09:24:06.036] Served eth_call conn=127.0.0.1:58365 reqid=3 duration=0s err="missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available"
-
```

```
Командний рядок - prysm.bat beacon-chain --execution-endpoint=http://localhost:8545 --sepolia --jwt-secre... - 

the new payload: method not found: received an undefined execution engine error firstSlot=4987329 firstUnprocessed=4987329 lastSlot=4987329 root=0x1c1fedb44fb8e34320500c59484be9cce3e415c40ce7af664de3f1e252d423dd
[2024-05-13 09:19:07] WARN initial-sync: Block processing failure error=failed to validate consensus state transition function: not descendant of finalized checkpoint firstSlot=4987393 firstUnprocessed=4987393 lastSlot=4987393 root=0xed8fa76e95168dfc8069536f45750d4daaa1f7c6ed36be98a8ca8bc4ad1384e5
[2024-05-13 09:19:12] INFO p2p: Peer summary activePeers=9 inbound=0 outbound=9
[2024-05-13 09:19:22] WARN initial-sync: Block processing failure error=could not notify the engine of the new payload: method not found: received an undefined execution engine error firstSlot=4987329 firstUnprocessed=4987329 lastSlot=4987329 root=0x1c1fedb44fb8e34320500c59484be9cce3e415c40ce7af664de3f1e252d423dd
[2024-05-13 09:20:12] INFO p2p: Peer summary activePeers=8 inbound=0 outbound=8
[2024-05-13 09:20:35] ERROR execution: Unable to process past deposit contract logs, perhaps your execution client is not fully synced error=processPastLogs: missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available
[2024-05-13 09:20:47] WARN initial-sync: Block processing failure error=could not notify the engine of the new payload: method not found: received an undefined execution engine error firstSlot=4987329 firstUnprocessed=4987329 lastSlot=4987329 root=0x1c1fedb44fb8e34320500c59484be9cce3e415c40ce7af664de3f1e252d423dd
[2024-05-13 09:20:55] INFO p2p: Peer summary activePeers=8 inbound=0 outbound=8
[2024-05-13 09:21:02] WARN initial-sync: Block processing failure error=could not validate consensus state transition function: not descendant of finalized checkpoint firstSlot=4987393 firstUnprocessed=4987393 lastSlot=4987393 root=0xed8fa76e95168dfc8069536f45750d4daaa1f7c6ed36be98a8ca8bc4ad1384e5
[2024-05-13 09:21:12] INFO p2p: Peer summary activePeers=4 inbound=0 outbound=4
[2024-05-13 09:22:12] INFO p2p: Peer summary activePeers=5 inbound=0 outbound=4
[2024-05-13 09:22:21] WARN initial-sync: Block processing failure error=could not notify the engine of the new payload: method not found: received an undefined execution engine error firstSlot=4987329 firstUnprocessed=4987329 lastSlot=4987329 root=0x1c1fedb44fb8e34320500c59484be9cce3e415c40ce7af664de3f1e252d423dd
[2024-05-13 09:22:22] WARN initial-sync: Block processing failure error=failed to validate consensus state transition function: not descendant of finalized checkpoint firstSlot=4987393 firstUnprocessed=4987393 lastSlot=4987393 root=0xed8fa76e95168dfc8069536f45750d4daaa1f7c6ed36be98a8ca8bc4ad1384e5
[2024-05-13 09:22:50] ERROR execution: Unable to process past deposit contract logs, perhaps your execution client is not fully synced error=processPastLogs: missing trie node 5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 (path ) state 0x5eb6e371a698b8d68f665192350ffceccbbbf322916f4b51bd79bb6887da3f494 is not available
[2024-05-13 09:23:09] WARN initial-sync: Block processing failure error=could not notify the engine of the new payload: method not found: received an undefined execution engine error firstSlot=4987329 firstUnprocessed=4987329 lastSlot=4987329 root=0x1c1fedb44fb8e34320500c59484be9cce3e415c40ce7af664de3f1e252d423dd
[2024-05-13 09:23:09] INFO p2p: Peer summary activePeers=6 inbound=0 outbound=6
[2024-05-13 09:23:12] INFO p2p: Peer summary activePeers=6 inbound=0 outbound=6
[2024-05-13 09:24:00] WARN initial-sync: Block processing failure error=could not notify the engine of the new payload: method not found: received an undefined execution engine error firstSlot=4987329 firstUnprocessed=4987329 lastSlot=4987329 root=0x1c1fedb44fb8e34320500c59484be9cce3e415c40ce7af664de3f1e252d423dd
[2024-05-13 09:24:00] INFO p2p: Peer summary activePeers=6 inbound=0 outbound=6
```

# Налаштування Blockchain



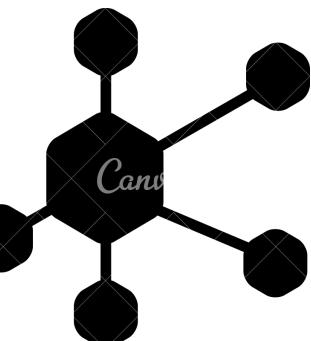
## Підключення до ЕБСІ

Має відбуватися на рівні державної інституції + вимагають ISO27001



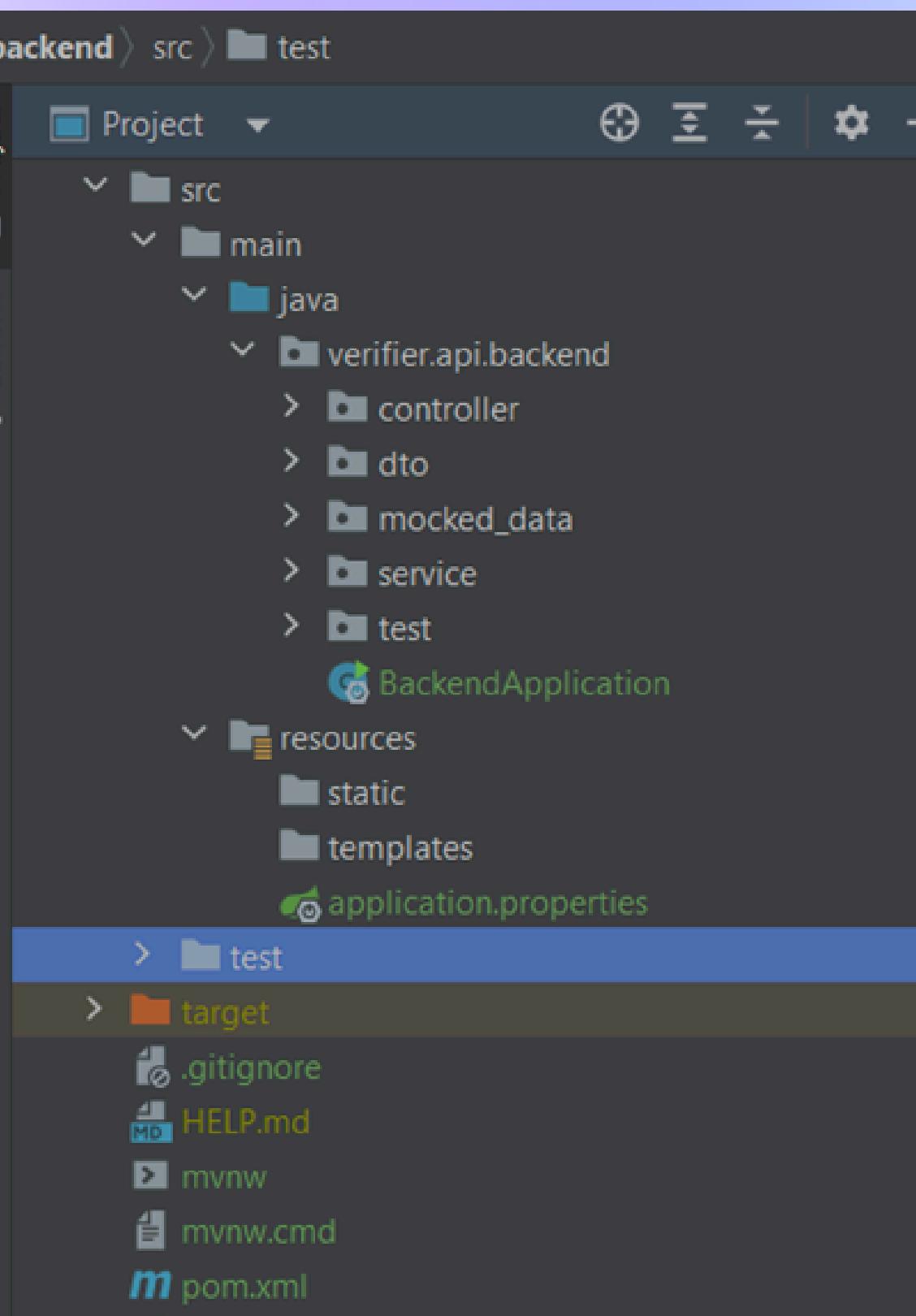
## Розгортання власної Ethereum ноди

Встановлення та запуск клієнтського програмного забезпечення Ethereum



## Наступні кроки - розгортання мережі з 3+ нод

Синхронізація, комунікація між нодами



# Verifier API для Блокчейну

Java, Spring Boot, REST, MVC

## Стандарт:

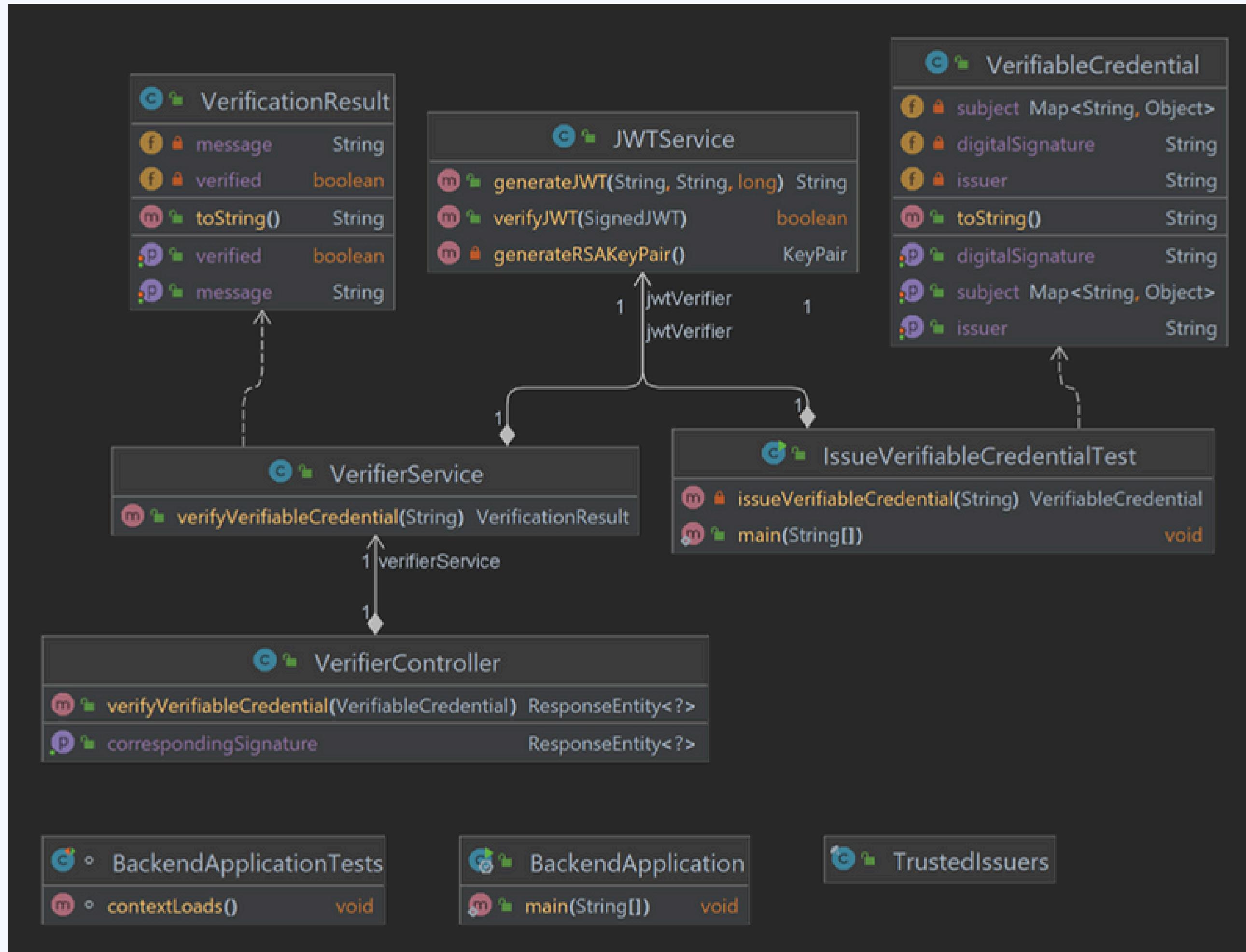
The European Digital Identity Wallet  
Architecture and Reference Framework

## Бібліотеки:

Nimbus JOSE+JWT для авторизації та signed JWT (RS256)

## API Endpoints:

GET /api/{id}/signature  
POST /api/verify-vc (issuer, subject, digitalSignature)



# Verifier веб-застосунок на React

13-20

Застосунок/плагін сканує qr-code з посиланням на підпис видавця документу та перевіряє чи є цей видавець у блокчейні.

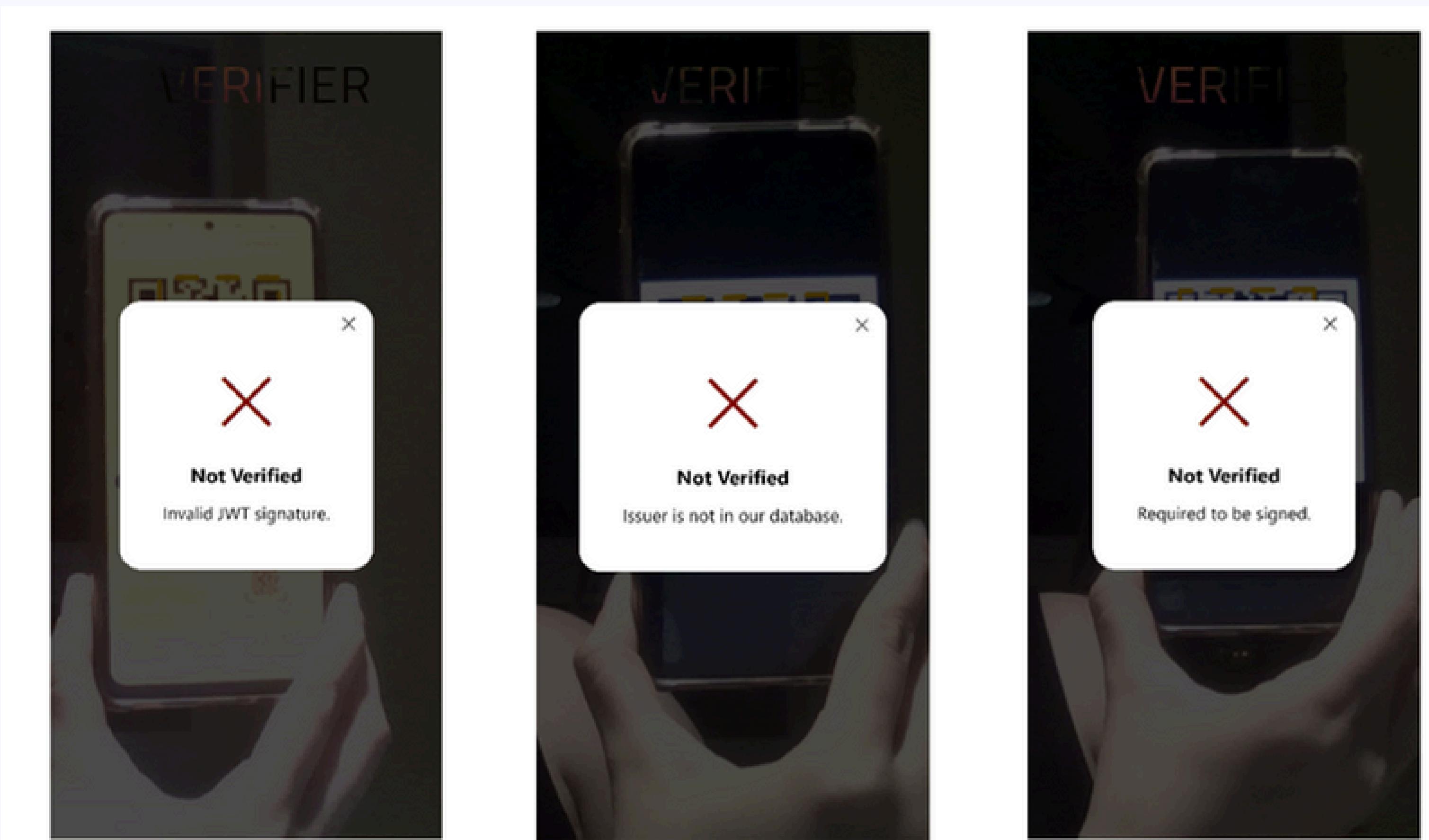


Verifier



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



# Висновки

- проведено грунтовне дослідження процесу який зараз відбувається у нашій державі на шляху до диджиталізації та інтеграції з ЄС
- порівняні переваги та недоліки теперішніх рішень України та ЄС
- розроблена інструкція з кроками для продовження інтеграції на прикладі Verifier

Дякую за увагу