



PROJE RAPORU – BLOCKCHAIN TABANLI SERTİFİKA DOĞRULAMA SİSTEMİ

Ders: Dijital Dönüşüme Giriş

Proje: Docker Üzerinde Blockchain ve Akıllı Kontrat ile Sertifika Doğrulama Sistemi

Öğrenci: Aslı Öz

Numara: 221229012

Bölüm: Yazılım Mühendisliği

Kurum: Konya Teknik Üniversitesi

1. Giriş

Bu projede blockchain tabanlı bir sertifika doğrulama sistemi geliştirilmiştir. Amaç, kişisel veriler zincire yazılmadan hash tabanlı sertifika kaydı, doğrulaması ve iptal işlemlerini gerçekleştiren bir yapı kurmaktır. Sistem akıllı kontrat, istemci (CLI) ve yerel blockchain ağı üzerinde çalışmaktadır.

2. Amaç

Projenin amacı sertifikaların güvenli şekilde doğrulanabildiği, değiştirilemez yapıda saklandığı bir blockchain altyapısı kurmaktır. Hardhat geliştirme ortamı ve Node.js istemcisi ile uçtan uca doğrulama süreci gerçekleştirilmiştir.

3. Sistem Mimarisi

Sistem üç temel bileşenden oluşur:

- Yerel Ethereum ağı (Hardhat Node)
- Akıllı kontratları derleyen ve dağıtan Hardhat ortamı
- Sertifikaları ekleyen ve doğrulayan CLI istemcisi

4. Kullanılan Teknolojiler

Solidity, Hardhat, Node.js/ethers.js, JSON-RPC, VS Code.

5. Akıllı Kontrat Tasarımı

CertificateRegistry.sol dosyası issue, revoke ve verify fonksiyonlarını içerir. Veriler hash tabanlı tutulur ve KVKK uyumludur. onlyOwner kontrolü ile yetkilendirme sağlanır.

6. İstemci Uygulaması

Node.js ile yazılan istemci sertifika hash'i üretir, kontrata gönderir ve verify fonksiyonuyla doğrulama yapar. Örnek çıktı:

- Kontrat deploy edildi
- Sertifika hash üretildi
- Sertifika verildi
- Doğrulama sonucu: Geçerli

7. Çalışma Akışları

Issue, verify ve revoke işlemleri test edilmiştir. Hash eşleşmesi, süresi dolmuş sertifikalar ve iptal kontrolleri başarıyla yapılmıştır.

8. Güvenlik ve KVKK

Zincire kişisel veri yerine yalnızca hash yazılır. Salt kullanımı sözlük saldırılarını engeller. Erişim kontrolü kontrat içinde sağlanmıştır.

9. Test Çıktıları

Şekil 1. Hardhat Node'un Başlatılması

```
C:\Users\Aslı Öz\Desktop\cert-project\dapp>npx hardhat node
Started HTTP and WebSocket JSON-RPC server at http://127.0.0.1:8545/

Accounts
=====

WARNING: These accounts, and their private keys, are publicly known.
Any funds sent to them on Mainnet or any other live network WILL BE LOST.

Account #0: 0xf39Fd6e51aad88F6F4ce6aB8827279cFfFb92266 (10000 ETH)
Private Key: 0xac0974bec39a17e36ba4a6b4d238ff944bacb478cbed5efcae784d7bf4f2ff80

Account #1: 0x70997970C51812dc3A010C7d01b50e0d17dc79C8 (10000 ETH)
Private Key: 0x59c6995e998f97a5a0044966f0945389dc9e86dae88c7a8412f4603b6b78690d

Account #2: 0x3C44CdDdB6a900fa2b585dd299e03d12FA4293BC (10000 ETH)
Private Key: 0x5de4111afa1a4b94908f83103eb1f1706367c2e68ca870fc3fb9a804cdab365a

Account #3: 0x90F79b6f6EB2c4f870365E785982E1f101E93b906 (10000 ETH)
Private Key: 0x7c852118294e51e653712a81e05800f419141751be58f605c371e15141b007a6

Account #4: 0x15d34AAf54267DB7D7c367839AAf71A00a2C6A65 (10000 ETH)
Private Key: 0x47e179ec197488593b187f80a00eb0da91f1b9d0b13f8733639f19c30a34926a

Account #5: 0x9965507D1a55bcC2695C58ba16FB37d819B0A4dc (10000 ETH)
Private Key: 0x8b3a350cf5c34c9194ca85829a2df0ec3153be0318b5e2d3348e872092edffba

Account #6: 0x976EA74026E726554dB657fA54763abd0C3a0aa9 (10000 ETH)
Private Key: 0x92db14e403b83dfe3df233f83dfa3a0d7096f21ca9b0d6d6b8d88b2b4ec1564e

Account #7: 0x14dC79964da2C08b23698B3D3cc7Ca32193d9955 (10000 ETH)
Private Key: 0x4bbbf85ce3377467afe5d46f804f221813b2bb87f24d81f60f1fcd6bf7cbf4356

Account #8: 0x23618e81E3f5cdF7f54C3d65f7FbC0aBf5B21E8f (10000 ETH)
Private Key: 0xdbda1821b80551c9d65939329250298aa3472ba22feea921c0cf5d620ea67b97

Account #9: 0xa0Ee7A142d267C1f36714E4a8F75612F20a79720 (10000 ETH)
Private Key: 0x2a871d0798f97d79848a013d4936a73bf4cc922c825d33c1cf7073dff6d409c6

Account #10: 0xBcd4042DE499D14e55001CcbB24a551F3b954096 (10000 ETH)
Private Key: 0xf214f2b2cd398c806f84e317254e0fb801d0643303237d97a22a48e01628897

Account #11: 0x71bE63f3384f5fb98995898A86B02Fb2426c5788 (10000 ETH)
Private Key: 0x701b615bbdfb9de65240bc28bd21bbc0d996645a3dd57e7b12bc2bdf6f192c82
```

Şekil 2. Akıllı Kontratın Deploy Edilmesi

```
C:\Users\Aslı Öz\Desktop\cert-project\dapp>npx hardhat run scripts/deploy.js --network localhost
🚀 DEPLOY BAŞLIYOR...
🎉 Kontrat başarıyla deploy edildi!
📌 Adres: 0x5FbDB2315678afecb367f032d93F642f64180aa3

C:\Users\Aslı Öz\Desktop\cert-project\dapp>

C:\Users\Aslı Öz\Desktop\cert-project\dapp>npx hardhat run scripts/interact.js --network localhost
Üretilen hash: 0x0b018fee6045cebae3ce179da0308f428d3259d8f5cb6ffe0e2474c325119508
📌 Sertifika eklendi!
🔵 Doğrulama sonucu: GEÇERLİ

C:\Users\Aslı Öz\Desktop\cert-project\dapp>
```

Şekil 3. Sertifika Ekleme ve Doğrulama

```
C:\Users\Aslı Öz\Desktop\cert-project\dapp>npx hardhat run scripts/interact.js --network localhost
Üretilen hash: 0x0b018fee6045cebae3ce179da0308f428d3259d8f5cb6ffe0e2474c325119508
📌 Sertifika eklendi!
🔵 Doğrulama sonucu: GEÇERLİ

C:\Users\Aslı Öz\Desktop\cert-project\dapp>
```

10. Docker Mimarisinin Değerlendirilmesi

Docker ortamı hazırlanmış ancak teknik engeller nedeniyle çalışma Hardhat Node üzerinde tamamlanmıştır. Docker ileride kolayca entegre edilebilir.

11. Sonuç

Projede blockchain üzerinde değiştirilemez bir sertifika sistemi kurulmuş, akıllı kontrat mantığı uygulanmış, istemci ile uçtan uca çalışma gösterilmiştir.

12. Kaynakça

1. Hardhat Documentation. (2024). *Ethereum development environment*.
<https://hardhat.org>
2. Ethers.js Documentation. (2024). *JavaScript library for Ethereum*.
<https://docs.ethers.org/>
3. Docker Documentation. (2024). *Containerization platform*.
<https://docs.docker.com/>
4. Ganache Documentation. (2024). *Personal blockchain for Ethereum development*.
<https://trufflesuite.com/ganache/>
5. Solidity Documentation. (2024). *Smart contract programming language*.
<https://docs.soliditylang.org/>
6. Node.js Documentation. (2024). *JavaScript runtime*.
<https://nodejs.org/>