GaslessCert

Blockchain HS25

Sven Elvedi, Timo Strolz, Davide Ferrara

Inhalt

- Idee
- Use Case
- Technische Umsetzung
- Certificate contract
- Architektur
- Weitere Möglichkeiten

Idee

- Zertifikate gasless auf Blockchain persistieren
- Vorteile
  - Zentralisiertes Zertifikatstool
  - Einfachere Handhabung
  - Einfachere Verifizierung

Use Case

- Instructor erstellt ein Zertifikat
- Instructor sendet Zertifikat an Recipient
- Recipient kann Zertifikat claimen (wird auf Blockchain persisitiert)
- Recipient sendet Zertifikat an Verifier
- Verifier kann Zertifikat verifizieren

Technische Umsetzung

Issue Certificate, Claim Certificate und Verify Certificate

Issue Certificate

- Instuctor verbindet MetaMask Account
- Instructor erstellt Zertifikat (nur Meta Data)
- Zertifikat (Meta Data) wird gehashed
- Instructor signiert Hash mit Wallet Key
- Hash + Meta Data = Zertifikat

Claim Certificate

- Recipient verbindet MetaMask Account
- Recipient ladet Zertifikat hoch
- App verifiziert Signatur local
- Smart Account wird erstellt
- User Operation wird erstellt
- Pimlico als Bundler und Paymaster führt Transaktion durch
- Zertifikat ist auf Chain

Verify Certificate

- Verifier ladet Zertifikat hoch
- Signatur wird local verifiziert
- On Chain Status des Zertifikats wird überprüft

Certificate Contract

Tech-Stack

- HTML, CSS, JS
- Vite als build tool (wegen SES lockdown Problemen)
- Pimlico als Bundler und Paymaster

Verwendete Libraries

	Vite	Ethers	Ox	Permissionless	Viem
Version	5.4.11	6.15.0	0.8.0	0.2.15	2.21.54
Zweck	- Build Tool	- MetaMask einbindung	- Wird von Viem benötigt	- Pimlico integration	- Interface für Ethereum

Weitere Dependencies

- OpenZeppelin
  - ECDSA.sol (für signing)
  - MessageHashUtils.sol (für hashing)
- Pimlico
  - Bundler
  - Paymaster

Weitere Möglichkeiten

- Support für andere Dateiformate (nicht nur JSON Zertifikate)
- Besseres File-Handling
- Wallet-Ownership Check bei Zertifikats-Verifizierung
- Erweiterung zu einer Full Stack App
  - Mehrere Zertifikate gleichzeitig handhaben
  - Zertifikatsaustausch zwischen Instructor, Recipient und Verifier

Demo

Q&A