

Dokumenten-Signierung mit Blockchain

Forschungsseminar Informatik

Nico Peuser & Julian Fleischmann

Problemstellung

The background of the slide features a series of soft, flowing, wavy lines in shades of pink, purple, and light blue. These lines create a sense of movement and depth, with some areas appearing more saturated than others, giving the background a layered, ethereal quality.

Relevanz in der Cyber Security



**Schutz der
Datenintegrität**



**Identitäts-
management**



**Dezentrale
Sicherheit**



**Fälschungs-
sicher**

Use Cases

Wo könnte unsere Lösung eingesetzt werden?



Behörden & öffentliche Verwaltung

- Digitale Urkunden und Bescheinigungen
- Grundbuch- und Registerauszüge
- Wahlverifikationen



Finanzbranche

- Integrität von Finanzdokumenten
- Transparenz
- Compliance



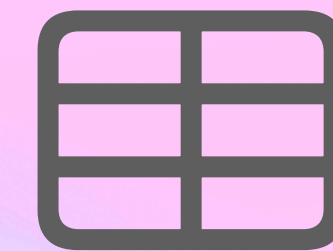
Unternehmen

- Digitale Urkunden und Bescheinigungen
- Grundbuch- und Registerauszüge
- Wahlverifikationen

Blockchain

Grundlagen

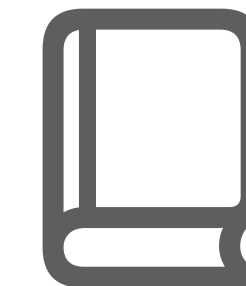
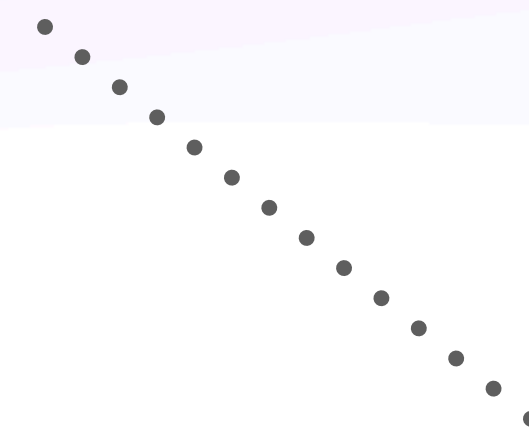
- Gemeinsam genutztes Hauptbuch (unveränderlich)
- Aufzeichnung von Transaktionen
- Verfolgung von Assets
- Verfolgung und Handeln von Wert



Datensätze



Smart Contracts




Distributed Ledger



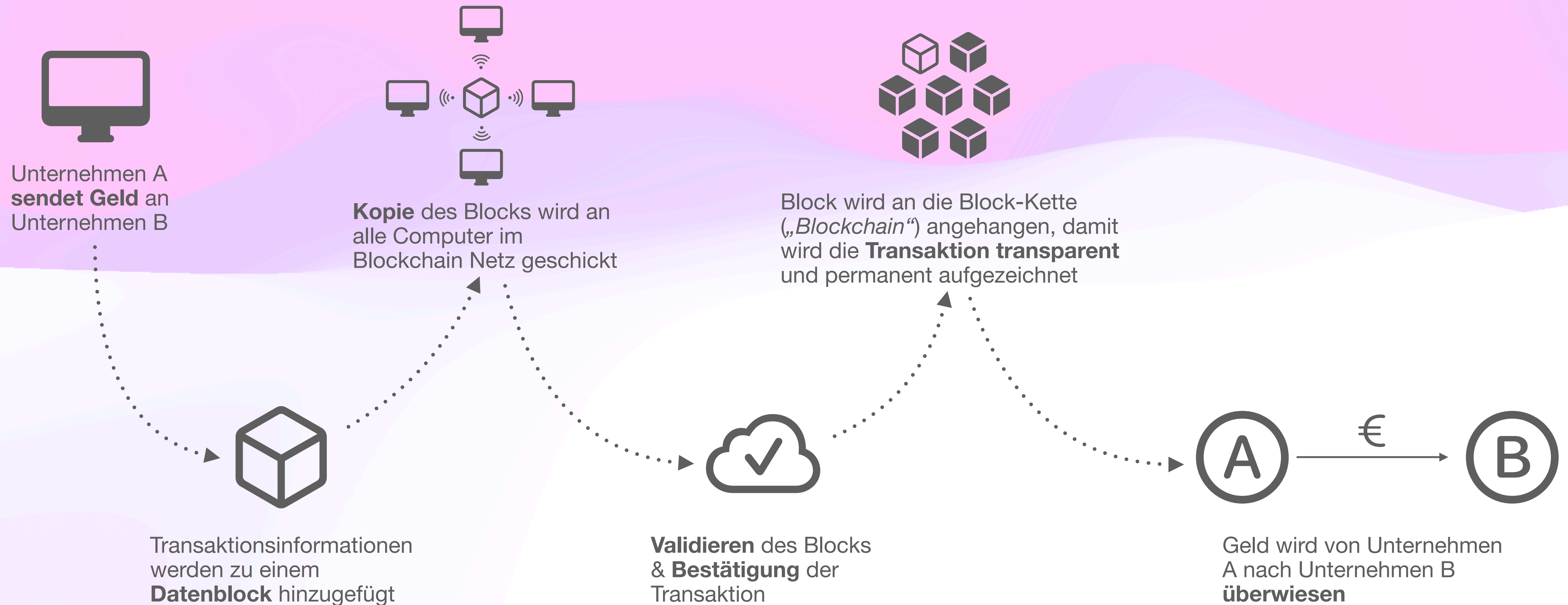
Blockchain

Hauptbestandteile

 Smart Contracts	 Distributed Ledger	 Datensätze
<ul style="list-style-type: none">• Reihe von Regeln• Automatisieren Transaktionen und Geschäftslogik• Selbst ausführende Programme mit Bedingungen in Codeform	<ul style="list-style-type: none">• „Hauptbuch“• Dezentrale Datenbank, die auf viele Knoten verteilt ist• Alle Netzwerkteilnehmer haben Zugriff• Unveränderliche Aufzeichnung aller Transaktionen	<ul style="list-style-type: none">• Unveränderliche Datensätze• Speicherung jeder Transaktion in einem Block• Kryptografische Verknüpfung der Blöcke

Blockchain

Funktionsweise (am Beispiel von Finanztransaktionen)



Blockchain

Welche Vorteile bringt die Technologie mit?



Unveränderbarkeit

Hash-Werte in der Blockchain sind nicht mehr änderbar



Nachvollziehbarkeit

Jede Notarisierung wird protokolliert als Transaktion



Dezentralisierung

Kein Single-Point-of-Failure (Ausfallsicherheit)



Vertrauensfreiheit

Nutzer müssen keiner zentralen Instanz trauen



Zeit-Beweis

Zeitstempel beweisen, dass Dokumente existiert haben



Manipulationssicherheit

Nur gültige Transaktionen werden in die Blockchain übernommen.

Projekt Setup

Welche Technologien haben wir verwendet?

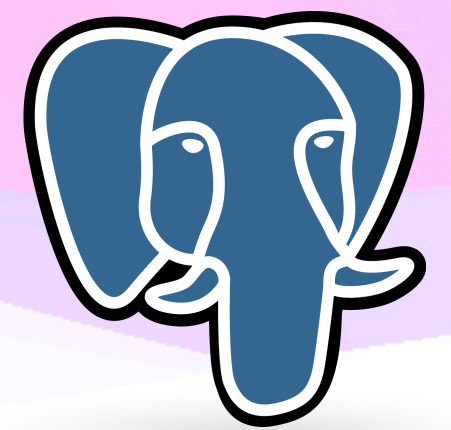
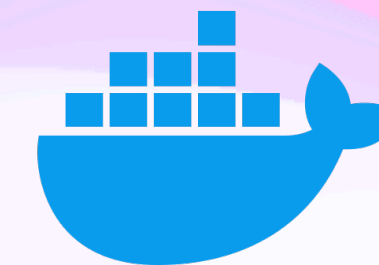


A X I O S

Frontend



Flask



Backend



Blockchain & Smart Contracts

Projekt

Planung

Entwurf

Technologie Stack



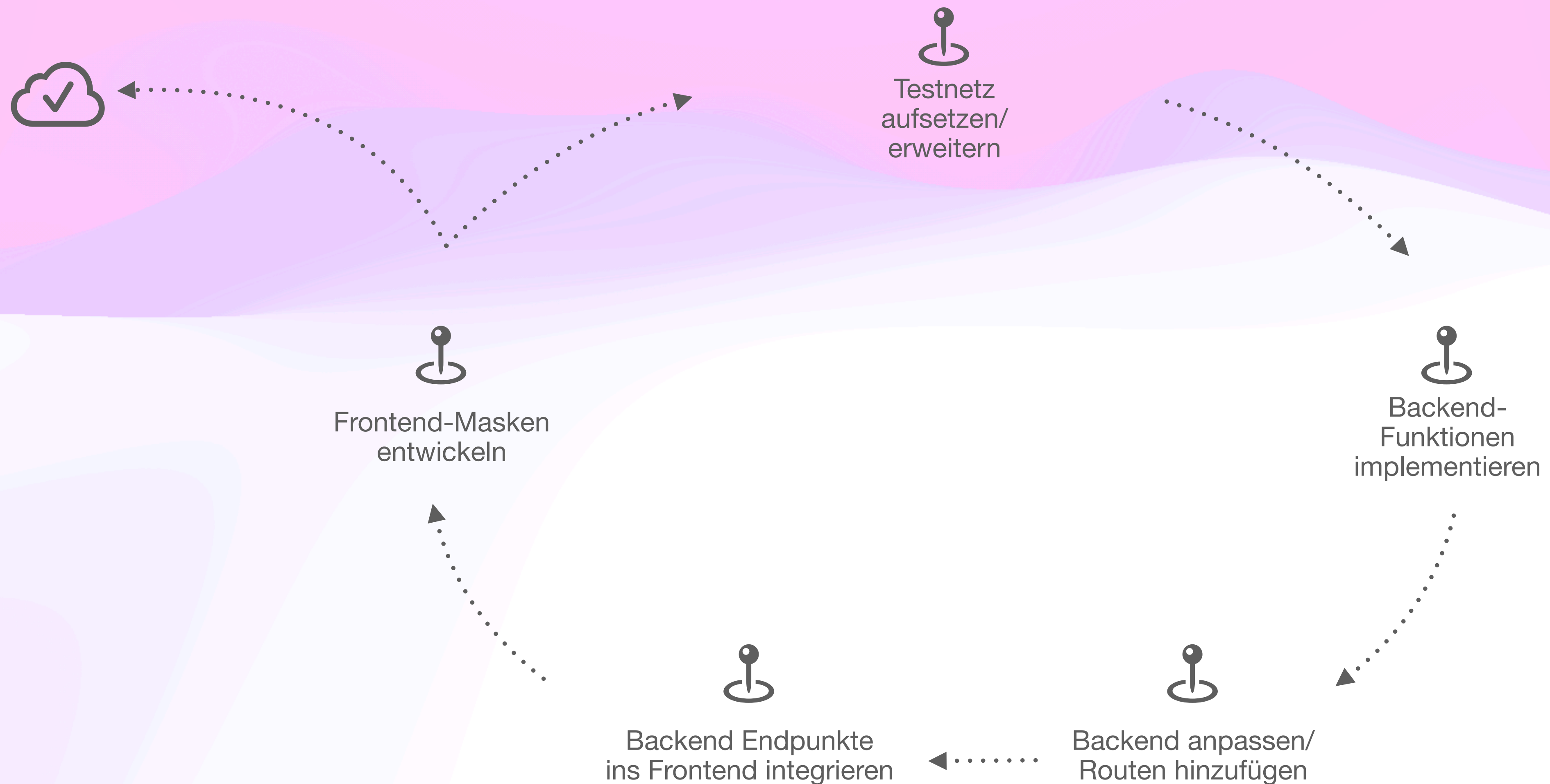
Languages



● Vue 44.2%	● Python 35.3%
● JavaScript 13.7%	● Solidity 5.3%
● Mako 0.7%	● HTML 0.4%
● CSS 0.4%	

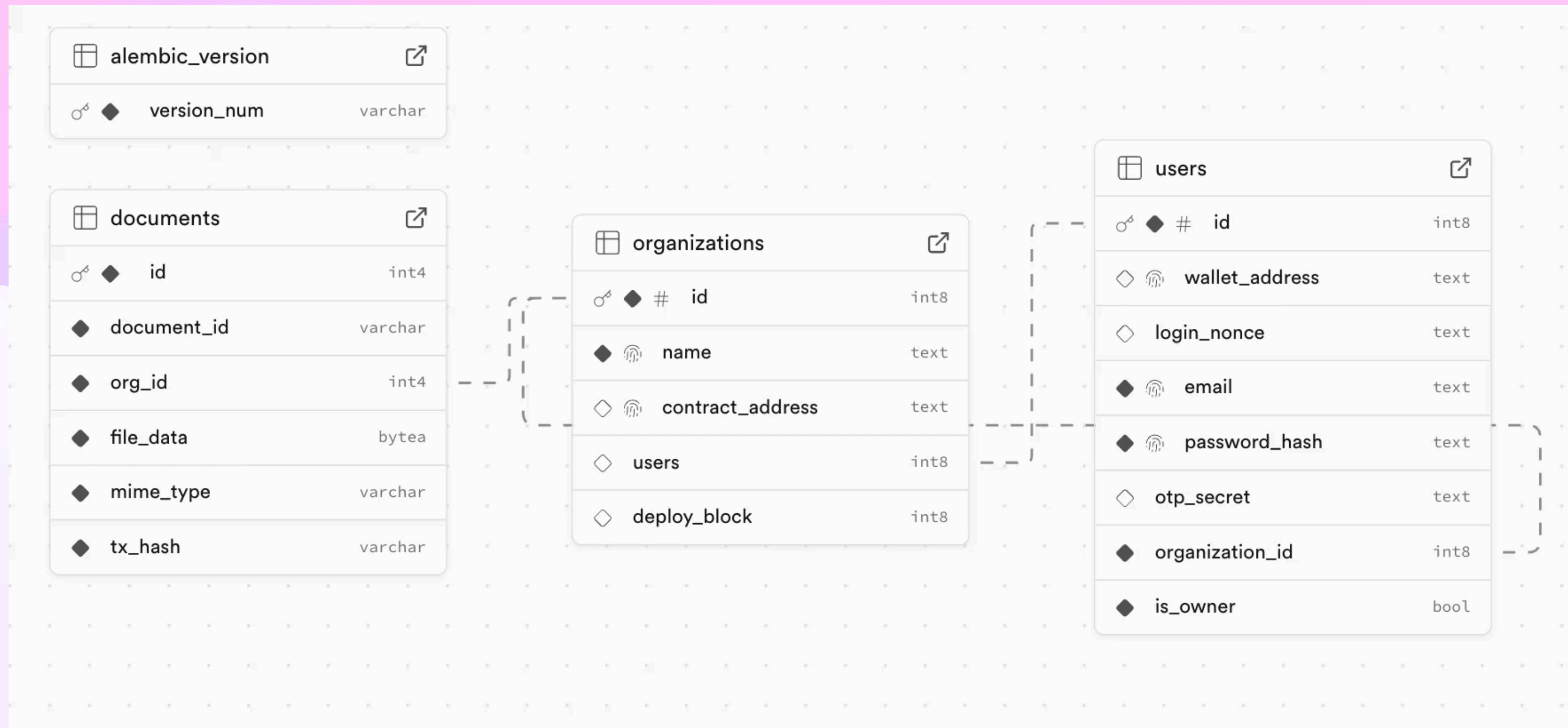
Entwurf

Wie lief unsere Entwicklung ab?



Entwurf

Datengrundlage



Entwurf

Umsetzung

- Ausschnitte aus Notary.sol / Routen (/notarize) zeigen + erklären anhand von Screenshots in der Präsi (immer wieder Bogen schlafen zu den Keypoints (Warum wichtig für Cybersecurity?))
- Info Nico

Entwurf

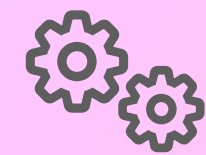
Was läuft bei der Signierung im Hintergrund alles ab?

Schaubild Nico

Live-Demo

Entwurf

Herausforderungen



Neue Technologie

> Dokumentation u.a nicht vollständig ausgereift



Public Testnetz

> Schritt von lokalem Testnetz zu öffentlichem Testnetz groß



Wallet Integration

> Eigene Wallets, die Transaktionen signieren



(De-)Zentralisierung

> Balance zwischen Transaktionen (dezentral) und Dateien lokal(Datenbank)



Komplexität

> Backend - Contracts / Backend - Frontend

Rückblick

Was haben wir erreicht?

X Datenbanktabellen

10 Frontend-Masken

36 Trello-Tasks

86 Commits

10 API-Endpunkt

Ausblick

Wie könnte es weitergehen?

①

Eigene Wallet-Signierung



Jeder User signiert mit seinem eigenen Wallet.

②

Admin Panel



Prüfung der Berechtigungen



Verwaltung der User einer Organisation

③

Transparenz schaffen



Coding der Smart Contracts anzeigen

④

Insights schaffen



Mehr Daten anzeigen mit etherscan.io

⑤

Offizielles Deployment



Was sagt die Gesetzeslage in Deutschland zu unserer Idee?

Ausblick

Gesetzeslage in Deutschland

„Die Rechtslage in Deutschland sieht bislang nicht vor, dass zivilrechtliche Wertpapiere auf einer Blockchain begeben werden können. Zu ihrer Entstehung bedarf es der Verkörperung eines Rechts in einer (Papier-)Urkunde.“

~ Bundesministerien der Wirtschaft & Finanzen
(aus Blockchain-Strategie der Bundesregierung)

Dankeschön!

Quellen & Abbildungsverzeichnis

- <https://www.ahd.de/was-ist-eine-blockchain-die-erklaerung-fuer-einsteiger/>
- <https://www.bmwk.de/Redaktion/DE/Publikationen/Digitale-Welt/blockchain-strategie.pdf>
- <https://github.com/picooo0001/doc-verification-blockchain/tree/feature/dynamic-auth>
-