



Vehicle Identification Number Index

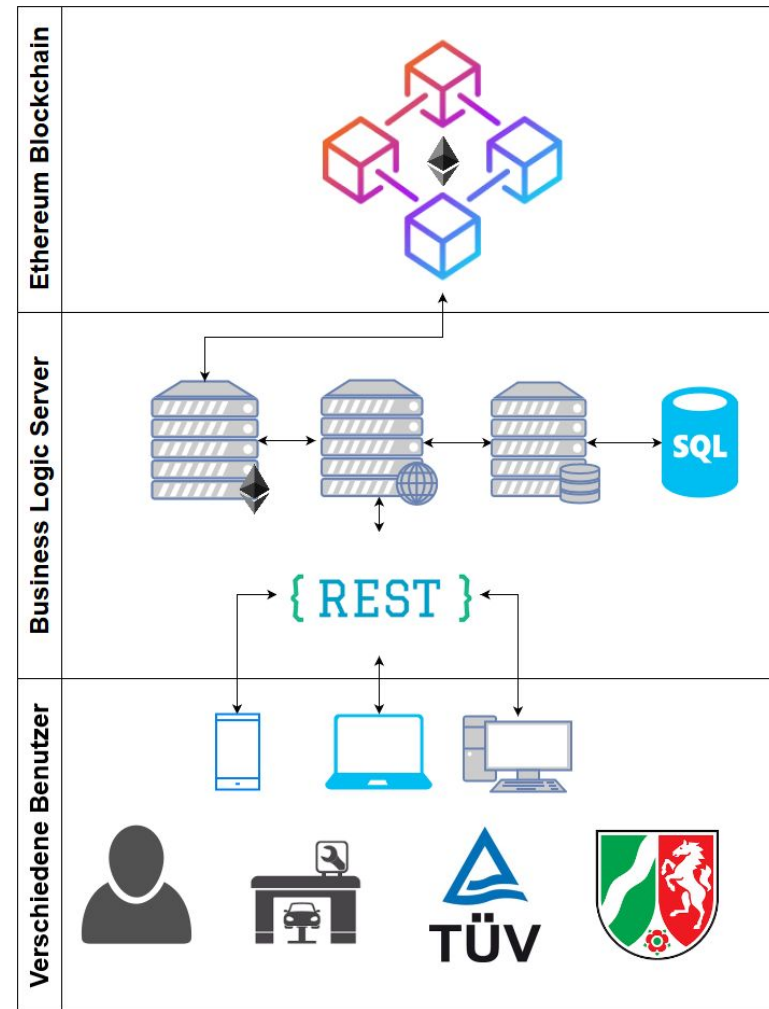
Agenda



- Was ist VINI?
- Vorführung der Demo
- Source-Code Review
- Lessons-Learned: Technologie
- Lessons-Learned: Blockchain
- Fragen und Feedback

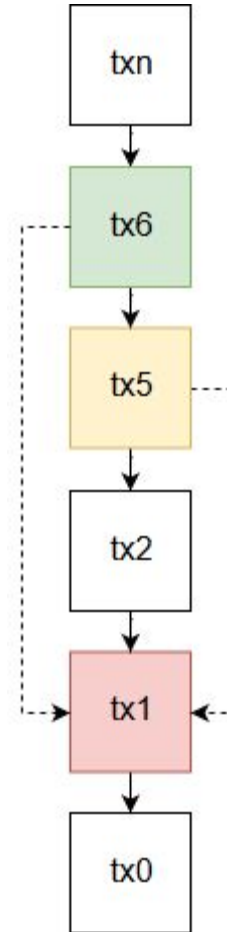
Was ist VINI?

- Deutschlandweites digitales Kfz-Scheckheft
- Open/Stakeholder: STVA, TÜV, Werkstätten
- Nutzung von Blockchain Eigenschaften
 - Manipulation verhindern
 - Abstreitbarkeit verhindern
 - Nachvollziehbarkeit
- Webbasiert (keine BC Kenntnisse benötigt)
- Wallets/Keys werden automatisch generiert
- Andere BC über Schnittstelle möglich
- Rest-API in Fremdsoftware integrierbar
- Transparente Korrektur für Benutzerfehler



Was ist VINI?

- Deutschlandweites digitales Kfz-Scheckheft
- Open/Stakeholder: STVA, TÜV, Werkstätten
- Nutzung von Blockchain Eigenschaften
 - Manipulation verhindern
 - Abstreitbarkeit verhindern
 - Nachvollziehbarkeit
- Webbasiert (keine BC Kenntnisse benötigt)
- Wallets/Keys werden automatisch generiert
- Andere BC über Schnittstelle möglich
- Rest-API in Fremdsoftware integrierbar
- Transparente Korrektur für Benutzerfehler



Demo

Source-Code

Lessons-Learned: Technologie

- async/await (ES2017) vielseitiger als Callbacks
- https einrichten und SSL Zertifikate generieren
- OAuth keine unterschiedlichen Autorisierungs-Level
- Gute Strategie für das State Management wichtig (Frontend-Komponenten)
- Dynamische Typisierung und Callbacks erschweren Einarbeitung in Code/Bibliotheken
- NPM kann bei komplexen Abhängigkeiten Probleme machen => YARN
- MS Azure schnell und einfach, aber limitiert
 - max. 5 User pro Ressource
 - kein Web3.js/Geth in Node.js Azure WebApp-Server

Lessons-Learned: Blockchain

- Warum Blockchain für VINI?
 - Datenredundanz, Unveränderlichkeit und dezentralisierbar
 - Proof of Authority begrenzt Manipulation durch Rogue-Node $\left\lceil \frac{\text{Schreiberanzahl}}{2} + 1 \right\rceil$
 - mit 4 Nodes max. 3 Blöcke in Folge manipulierbar anstelle von “DROP DATABASE”
- web3.js in Beta
 - getAllTransactionsToOrFromAccount nicht existent
 - Hilfreiche Filter wurden wieder entfernt
 - batchRequest hat kein Promise
 - Ohne DB praktisch nicht effizient nutzbar (Timeouts)
 - Mining von Blöcken nicht pausierbar
 - Transaktionskosten nicht abschaltbar
- Bot entwendete 9^{74} *Ether* von pre-funded Node
- Schwer testbar und Unveränderlichkeit bei Entwicklung hinderlich

Vielen Dank für Ihre Aufmerksamkeit!

Fragen und Feedback