Übung BC: Blockchain

Gruppe 8: Lukas Arnold, Patrick Bucher, Christopher James Christensen, Jonas Kaiser, Melvin Werthmüller

1. Macht der Einsatz einer Blockchain immer Sinn?

Der Einsatz einer Blockchain macht dann Sinn, wenn:

- die Abwicklung in einem nicht-hierarchischem Netzwerk (Peer-to-Peer) erfolgen soll
- die Teilnehmer grundsätzlich anonym sein aber ihre Identität bei Bedarf nachweisen können sollen
- die festzuhaltenden Informationen nicht modifizierbar sein dürfen

2. Welche Blockchain-Typen gibt es?

- Permissionless Blockchain
- Permissioned Blockchain

3. Für welche Anwendungsfälle ist die Blockchain primär gedacht?

Grundsätzlich für alle Anwendungsfälle, wo eine zentrale vertrauenswürdige Instanz eliminiert werden soll. Zum Beispiel:

- Nachweis vom Besitz einer Sache (Geld, Dokument)
- Nachweis von Transaktionen (Handel, Geldtransfer)
- Nachweis von Identität bei gewahrter Anonymität (E-Voting)

4. Überlegen Sie sich einen möglichen Anwendungsfall und beschreiben Sie diesen kurz mit einem passenden Use Case.

Anwendungsfall: Nachrichtensystem

- Alice möchte Bob eine Mitteilung machen.
- Die Mitteilung soll privat sein, also für aussenstehende nicht lesbar sein.
  - Es wird nur der Hash in der Blockchain gespeichert, die Mitteilung kann somit nicht entziffert werden.
- Alice möchte aber nachweisen können, dass Bob eine bestimmte Nachricht erhalten hat.
  - Bob signiert die Nachricht zur Bestätigung, nachdem er sie gelesen hat.
  - Die Nachricht wird in der Blockchain von anderen Teilnehmern bestätigt.

- Alice möchte im Zweifelsfall nachweisen können, dass die übermittelte und von Bob empfangene Nachricht genau so lautet, wie sie das behauptet.
  - Dazu kann sie die von ihr gespeicherte Originalnachricht wieder hashen.
  - Ist die Originalnachricht verloren, ist dies nicht mehr möglich.