Blockchain als Grundlage für digitale Identität

Stefanie Roos

TU Delft/Delft Blockchain Lab

~~Was ist Identität?~~

Was ist Identifierung und Authentifizierung?

Identifierung: Aussage, wer man ist

- z.B. “Ich bin Wonder Woman”

Authentifizierung: “Beweis”, dass Person tatsächlich ist, wer sie behauptet zu sein

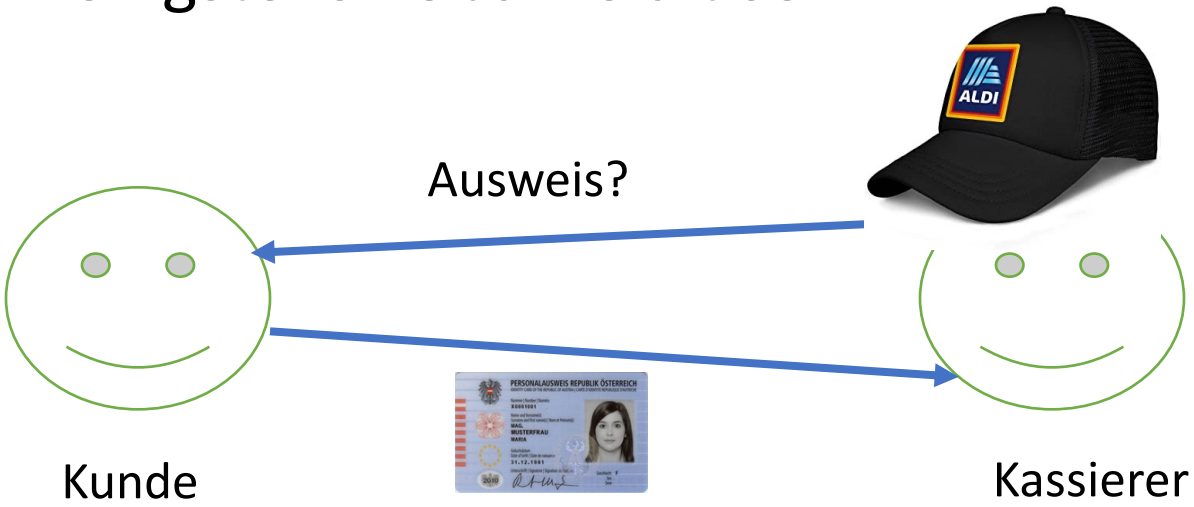
- z.B. Ausweis

Source: https://www.bmeia.gv.at

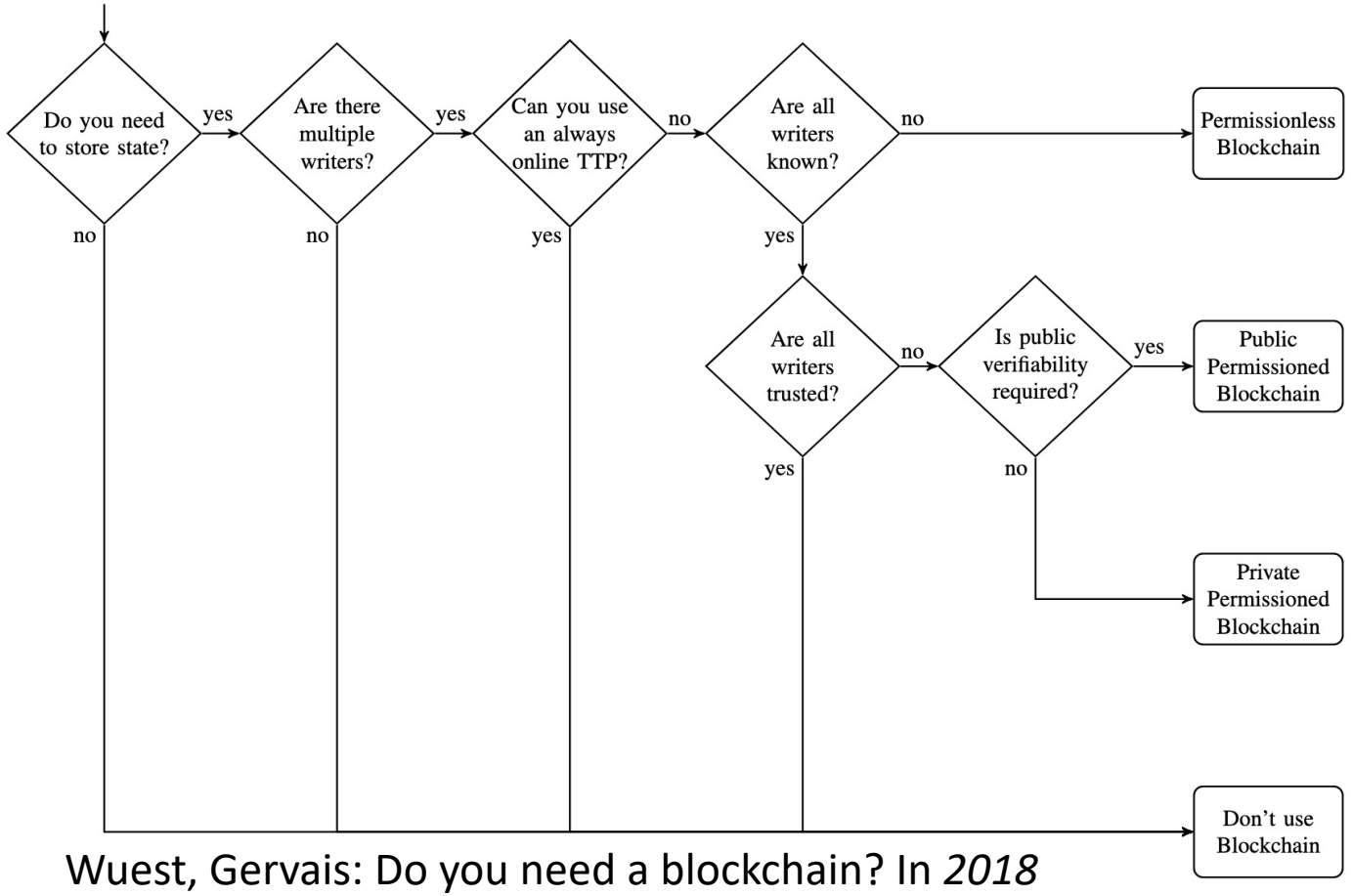
Attribute

Zeigen, dass man ein bestimmtes Attribut hat

Beispiel: wenigstens 18 Jahre alt sein



Wollen/Brauchen wir eine Blockchain?



Wuest, Gervais: Do you need a blockchain? In *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)* (pp. 45-54). IEEE.

Permissionless Blockchain

Öffentliche Permissioned Blockchain

Private Permissioned Blockchain

Keine Blockchain

Blockchain Wahl Digitale Identität

Muss Zustand gespeichert werden? -> Ja

Tragen mehrere (unabhängige) Parteien Daten ein?

-> Vermutlich? Nehmen wir mal an, ja

Kann eine trusted third party, die konstant verfügbar ist, genutzt werden?

-> Nein?

Blockchain Wahl Digitale Identität 2

Sind alle Parteien, die Daten eintragen, im Voraus bekannt?

-> Falls nicht: **permissionless blockchain**

-> Aber wahrscheinlich ja

Sind alle Parteien, die Daten eintragen, vertrauenswürdig?

-> Falls ja: **keine blockchain**

Falls nein: Ist es notwendig, dass die Information von jedem verifiert werden können?

Ja -> **Öffentliche Permissioned Blockchain**