der Bundeswehr
Universität München

Blockchain-basiertes Föderiertes Identity Management am Beispiel von Ethereum Smart Contracts

24. DFN-Konferenz „Sicherheit in vernetzten Systemen“
14.02.2017

Michael Grabatin
Wolfgang Hommel

Gliederung

Entwicklung Computer

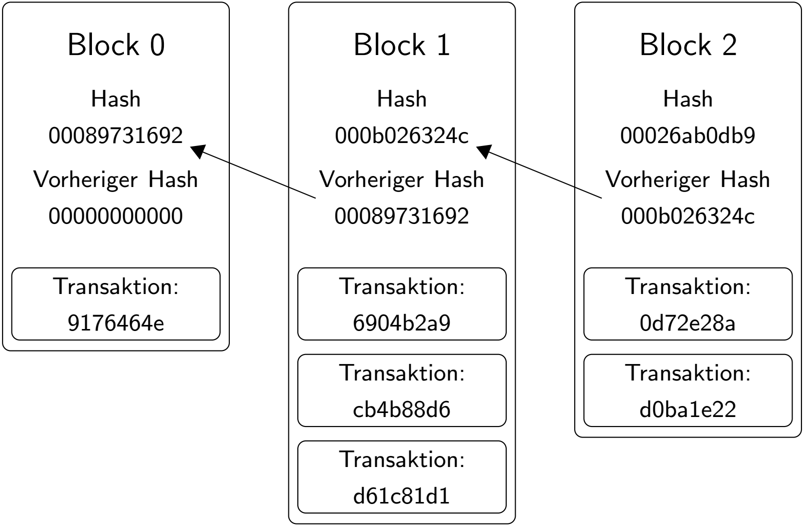
- Lokale Computer
- Mainframe
- Server
- Cloud-Computing
- Blockchain

Zunehmende Verteilung von Ressourcen

Bessere Skalierbarkeit

Höhere Verfügbarkeit

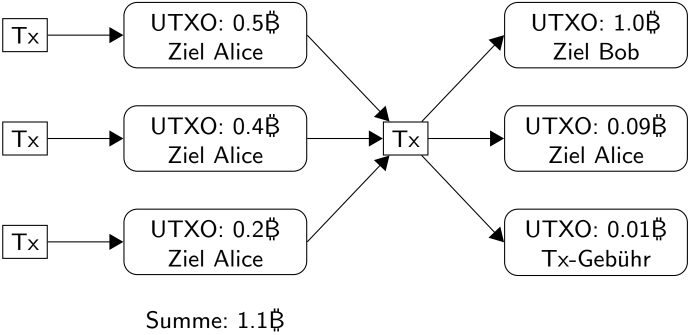
Blockchain



Block 0
Hash
00089731692
Vorheriger Hash
00000000000
Transaktion:
9176464e
Block 1
Hash
000b026324c
Vorheriger Hash
00089731692
Transaktion:
6904b2a9
Transaktion:
cb4b88d6
Transaktion:
d61c81d1
Block 2
Hash
00026ab0db9
Vorheriger Hash
000b026324c
Transaktion:
0d72e28a
Transaktion:
d0ba1e22

bitcoin

Blockchain und P2P-Netz zum Überweisen von digitaler Währung



Tx: Transaktion

UTXO: Unspent Transaction Output

Ethereum

Ethereum = Bitcoin + Smart Contracts

- Erweiterung der Bitcoin-Transaktionen
- Turing-vollständige Skriptsprache
- Langsame Ausführung/Entscheidungsfindung
- Vergleichsweise teuer
- Überprüf- und auditierbar

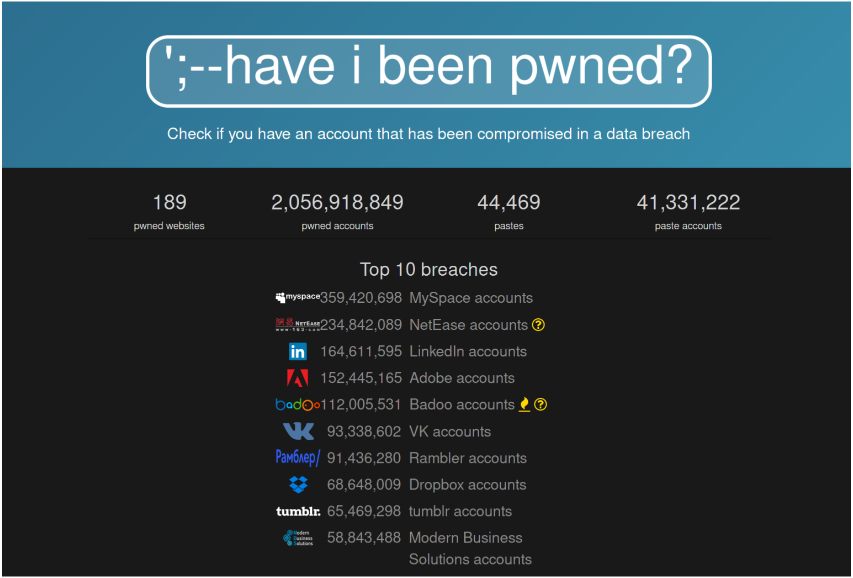
Ethereum

- Globaler Computer
- Kein Ein-/Ausschalter
- Zugreifbar für jeden

„Web3"-Technologien

- Ethereum: Serverloser Computer
- Whisper: Private asynchrone Nachrichten
- IPFS/Swarm: Dezentraler Datenspeicher

Status Quo



Quelle: https://haveibeenpwned.com (Stand 06.02.2017)

Facebook

Facebook will Passwort-Zentrale des Internet werden

01.02.2017 10:30 Uhr – Jürgen Schmidt, Daniel AJ Sokolov

Mit dem Konzept der Delegated Recovery will Facebook den traditionellen Passwort-Reset via E-Mail ablösen – und sich selbst als unersetzlichen Mittelpunkt des Internet verankern.

Quelle: https://heise.de/-3613518

Authentifizierung

- Keine Authentifizierung
- Lokale Authentifizierung
- Organisationsinterne Authentifizierung (LDAP)
- Föderiertes Identity Management (SAML, Shibboleth, OpenID Connect)
- Blockchain

Zunehmende Verteilung von Ressourcen

Bessere Skalierbarkeit

Höhere Verfügbarkeit

Identity Management

- Authentifizierung
- Verwaltung von Attributen/Rollen/Rechten
- Definition von Geltungsbereichen/zeiträumen
- Autorisierung
- Delegation
- Austausch von Informationen

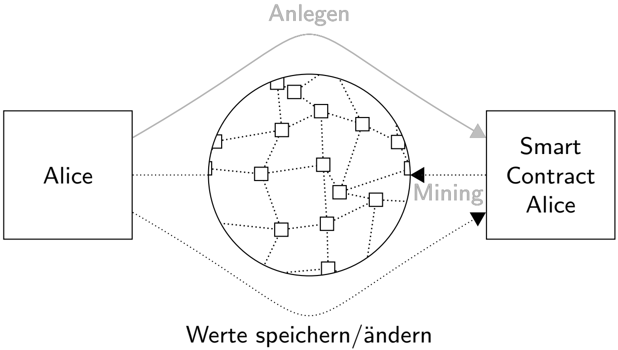
Identity Management auf öffentlichen Blockchains

- Niemand gehört/kontrolliert die Blockchain
- Teilnehmer müssen sich an Vereinbarungen halten
- Jeder kann Vereinbarungen überprüfen
- Nutzer entscheidet über Verwendung seiner Identitäten

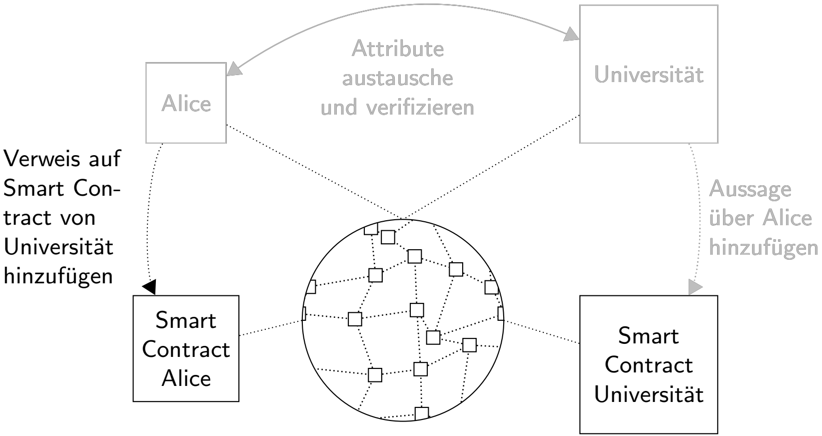
Konzept

- Identität = Adresse = Smart Contract
- Öffentliche Attribute können in dem Smart Contract gespeichert werden
- Kontrolliert wird der Smart Contract über einen *PrivateKey*

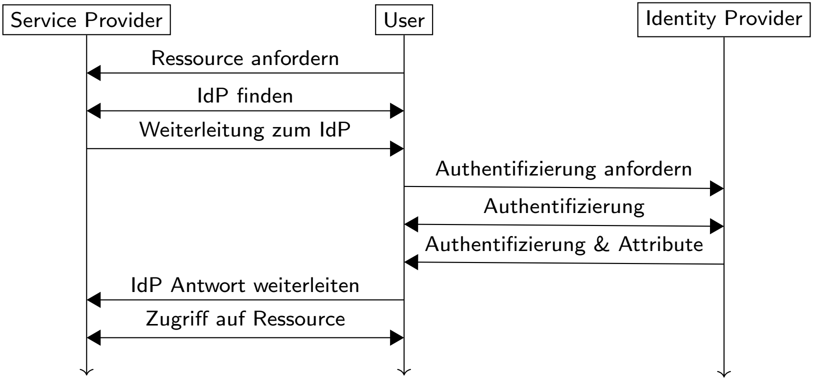
Attribute speichern



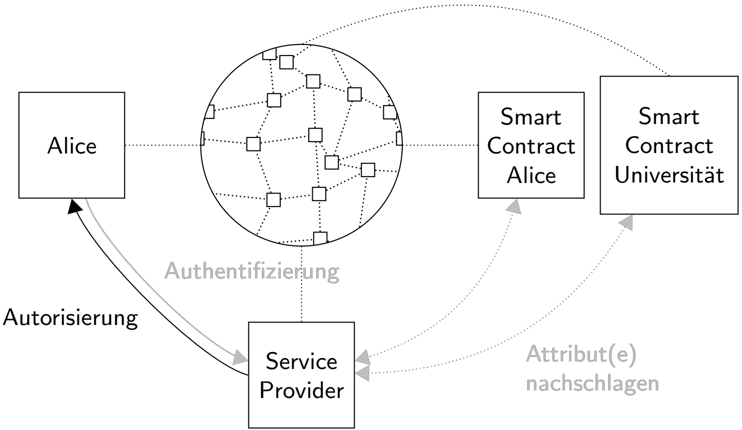
Attribute attestieren

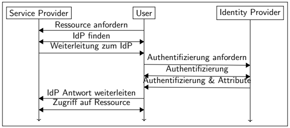


Generisches Föderiertes Identity Management



Authentifizierung & Autorisierung





Implementierungsbeispiel

Persönlicher Smart Contract (Attribute Authority): 35 LoC

Ermöglicht das Hinterlegen von beliebigen öffentlichen Attributen zu einer Identität

Service Provider: 50 LoC

Überprüft ob eine Liste von Attributen vorhanden bzw. mit dem richtigen Wert vorliegen

Kosten

$1ETH = 10.73\$$

Anfallende Kosten = Wert aller Operationen * $0.2\mu ETH$

Wert pro Operation:

- Erstellen eines Smart Contracts: 32.000
- Löschen eines Smart Contracts: -24.000
- Speichern von Werten: 20.000
- Löschen von Werten: -5.000
- Addition: 3
- Multiplikation: 5

Erstellen und Speichern von Wert:
$(32.000 + 20.000) * 0.2\mu ETH = 0.0104ETH \approx 0.11\$$

Vorteile & Herausforderungen

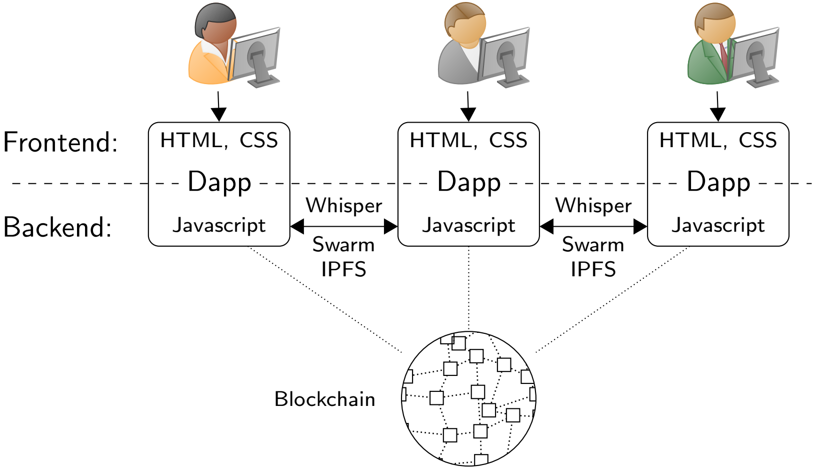
Vorteile

- Erstaunlich einfach zu Implementieren
- User unter voller Kontrolle seiner Identitäten
- Sehr verlässlich

Herausforderungen

- User unter voller Kontrolle seiner Identitäten
- Datenschutz
- Betrachtet nur technische Vertrauensbeziehungen

Erweiterung decentralized App (Dapp)



Ausblick

Private Attribute geschützt speichern

Unabdingbar für Identity Management außerhalb von Namen und E-Mail-Adressen

Zero-Knowlege-Beweise

Ermöglichen es, Aussagen zu beweisen ohne Informationen über die Aussage preiszugeben

Homomorphe Verschlüsselung

Rechnen auf verschlüsselten Daten

Fragen

Föderiertes Identity Management
auf einem globalen Computer

Kontakt:
Michael Grabatin
michael.grabatin@unibw.de

Universität der Bundeswehr München