Identity & Access managen über die Blockchain

Anwendungsszenarien, verfügbare Lösungen und eine kritische Analyse

NET-WORK #13 von WKÖ und AUSTRIAPRO, 6. Dezember 2016

Die nächste große Sache nach dem Internet?

esatus AG
The CISO Consulting Company

- Digitalisierung
- Industrie 4.0
- Internet of Things

Blockchain

Was ist dran an den aneinandergeketteten Datenblöcken?

Eine Beschäftigung mit dem Thema ist unumgänglich, wenn man die nächste digitale Revolution nicht verschlafen will!

esatus AG
The CISO Consulting Company

Bitcoin

- „Satoshi Nakamoto“
- Whitepaper 2008
- Währung ohne Vertrauen in Banken
- Erste Bitcoins in 2009

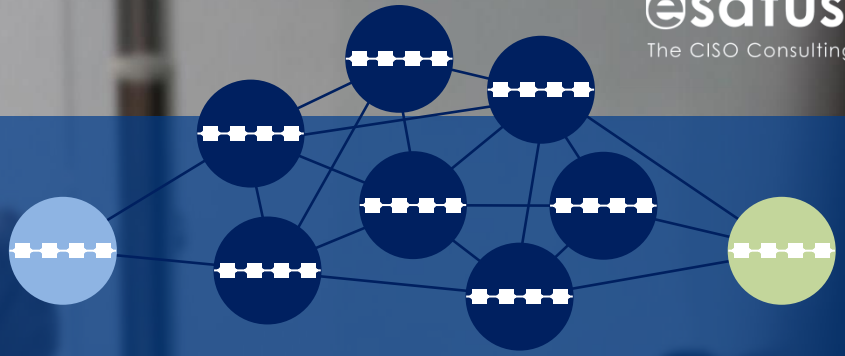
Was ist Bitcoin?

Eine elektronische Währung, die auf einem kryptografischen Beweis der Transaktionen beruht und ohne Vertrauen in Mittelsmänner auskommt.

Globalität und Dezentralität

esatus AG
The CISO Consulting Company

- Blockchain speichert alle Bitcoin-Transaktionen ab
- Global verteilte dezentrale Clients, ca. 5.100 aktive derzeit
- Jeder mit Blockchain-Kopie, ca. 110 GB an Speicherbedarf
- Peer-to-Peer-Netzwerk ohne zentrale steuernde Instanz



Der Zusammenhang von Bitcoin und Blockchain

Die Blockchain ist die verteilte Datenbank hinter der Krypto-Währung Bitcoin.

Unanfechtbarkeit und Konsens

esatus AG
The CISO Consulting Company

- Konsensbildender Mechanismus ist ein aufwändiges Hashverfahren

Proof-of-Work

- Miner erhalten für erfolgreiche Blockerstellung eine Belohnung
- Neuer Block alle 10 Minuten

Konsensbildung als elementarer Blockchain-Bestandteil

Alle Clients des Netzwerkes vertrauen den Rechenergebnissen des Clients, der den letzten Datenblock manifestiert hat.

Alternativen zum Proof-of-Work

esatus AG
The CISO Consulting Company

- Proof-of-Stake
- Proof-of-Capacity
- Proof-of-Activity
- Proof-of-Burn
- Proof-of-Storage
- …

Ausblick

Es gibt eine Vielfalt an Beweismethoden – die Anzahl steigt kontinuierlich.

Blockchain IDs, Profile und Attestierung

esatus AG
The CISO Consulting Company

- Blockchain-Erweiterungen für Identity & Access
- IDs mit Attributen werden zum Profil
- IDs auch für Unternehmen, Webseiten oder Applikationen
- Bestätigung der Attribute durch andere IDs

Attestierung

Anwendungsfall Authentifizierung und Autorisierung

Die ID einer Applikation kann der ID einer Person attestieren, dass sie diese kennt und als legitimen Nutzer betrachtet.

Vorteile der Blockchain ID sind offenkundig

esatus AG
The CISO Consulting Company

- Digitale Identitäten werden nur noch einmal verwaltet
- Der Eigentümer einer digitalen Identität ist wirklich Herr über diese

Souveräne Identität

- Eine Applikation muss selbst keine Berechtigungen verwalten
- Administration nur an einer Stelle

Schlüsselfaktor bleibt erhalten

Vertrauen in eine zentrale Instanz ist nicht erforderlich – weder für Identitäten noch für Berechtigungen.

Kaum Anwendung des Verfahrens in der Praxis

esatus AG
The CISO Consulting Company

- Alle Clients können in die Blockchain schauen und Transaktionen einsehen
- Distributed Public Ledger – jeder kann sich beteiligen

Permissionless

- Energieintensives Proof-of-Work

Mangel an Systemvertrauen hindert Adaption

Aufgrund des öffentlichen Charakters können Langzeitverlässlichkeit und -stabilität des Systems nicht garantiert werden.

Vertrauensbildung im Konsortium

esatus AG
The CISO Consulting Company

- Consortium Chain – nur bekannte & genehmigte Teilnehmer mit Clients

Permissioned

- Alternative Konsensbildung möglich
- Nach wie vor keine zentrale Kontrollinstanz erforderlich

Resümee Consortium Chains

Größere Transparenz, die besseres Gefühl für Kontrollierbarkeit und Verlässlichkeit schafft. Für manche Anwendungsbereiche, gar ganze Industrien unerlässlich.

Abgrenzung der relevanten Dimensionen: Validierung und Zugriff

esatus AG
The CISO Consulting Company

		Validierung	
		Permissionless	*Permissioned*
Zugriff	*Public*	„Jeder darf lesen und rechnen“	„Jeder darf lesen, nur erlaubte dürfen rechnen“
	Private	„Nur erlaubte dürfen lesen, jeder darf rechnen“	„Nur erlaubte dürfen lesen und rechnen“

Identity & Access als Schlüsselapplikation

esatus AG
The CISO Consulting Company

- Vertrauen im Konsortium hergestellt
- Implikationen für Unternehmen und im öffentlichen Sektor
- Nutzer bringen eigene digitale Identität einfach mit

Bring Your Own Identity

Identity & Access simplifiziert

Ein Unternehmen muss dem Mitarbeiter lediglich die Organisationszugehörigkeit bestätigen und die erforderlichen Zugriffsberechtigungen gewähren.

Blockchain Identity & Access auf dem Prüfstand

esatus AG
The CISO Consulting Company

- Permissioned Distributed Ledger bietet notwendige Prämissen
- Kritische Masse erforderlich, aber bei weitem nicht erreicht
- Finanzindustrie und öffentlicher Sektor als Treiber und unmittelbare Profiteure

Web of Trust

Ansätze für eine disruptive Innovation

Geduld ist für wertschöpfende Anwendungsszenarien erforderlich. Aber Identity & Access – auf Basis eines Permissioned Distributed Ledgers – könnte ein solches sein.

Lösungen, die sich noch in der Praxis behaupten müssen

esatus AG
The CISO Consulting Company

		Validierung	
		Permissionless	*Permissioned*
Zugriff	*Public*	**Blockstack**	**Evernym / Sovrin**
	Private	**-**	**Corda / R3**

Herausgeber: esatus AG
Copyright Fotos: kuegi/Fotolia.com; esatus AG