TeleTrusT-Informationstag "Blockchain"

Frankfurt a.M., 13.07.2017

Elektronische Zustellung – Anwendungsmöglichkeiten der Blockchain

Dr. Christian Baumann, AUSTRIAPRO

Agenda

- Elektronische Zustellung
- Blockchain
- Anwendungsmöglichkeiten

Kurzvorstellung AUSTRIAPRO

- Standardisierungs- & Expertenplattform
  - E-Business Themen
  - Zusammenarbeit mit der WKO
- ca. 80 Vereinsmitglieder
  - Unternehmen, Institutionen, Behörden
- Themen der Arbeitskreise
  - E-Billing (ebInterface, E-Rechnung an den Bund)
    - Vgl. ZUGFeRD, RL 2014/55/EU
  - E-Zustellung (im privatwirtschaftlichen Bereich)
  - …
- Neu seit 2016: Blockchain / DLT
  - Zusammenarbeit mit u.a. TeleTrust
  - WKO-FG Versicherungen & Banken …

Elektronische Zustellung in Österreich

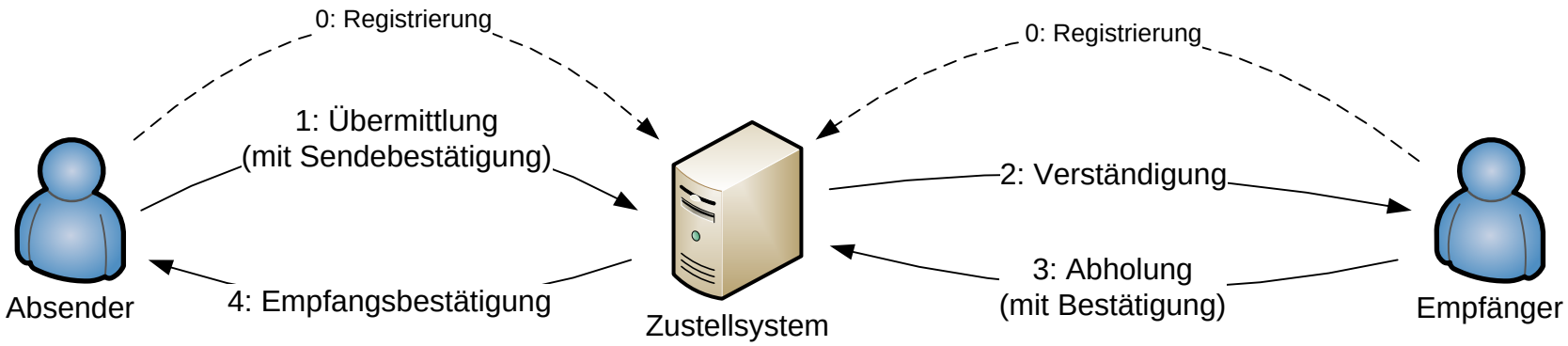
- E-Government => "behördliche e-Zustellung"
  - Behördliche Dokumente an Bürger & Unternehmen
  - Behördliche Zustelldienste
  - Nutzung der "Bürgerkarte" zwingend
    - Qualifizierte Signatur & Personenbindung
    - Chipkarte oder Handysignatur
- "Privatwirtschaftliche e-Zustellung"
  - Firmen/Personen an Firmen/Personen
    - Erweiterung für Anwälte und Notare
  - Bürgerkarte optional

E-Zustellung: Einleitung - Definition

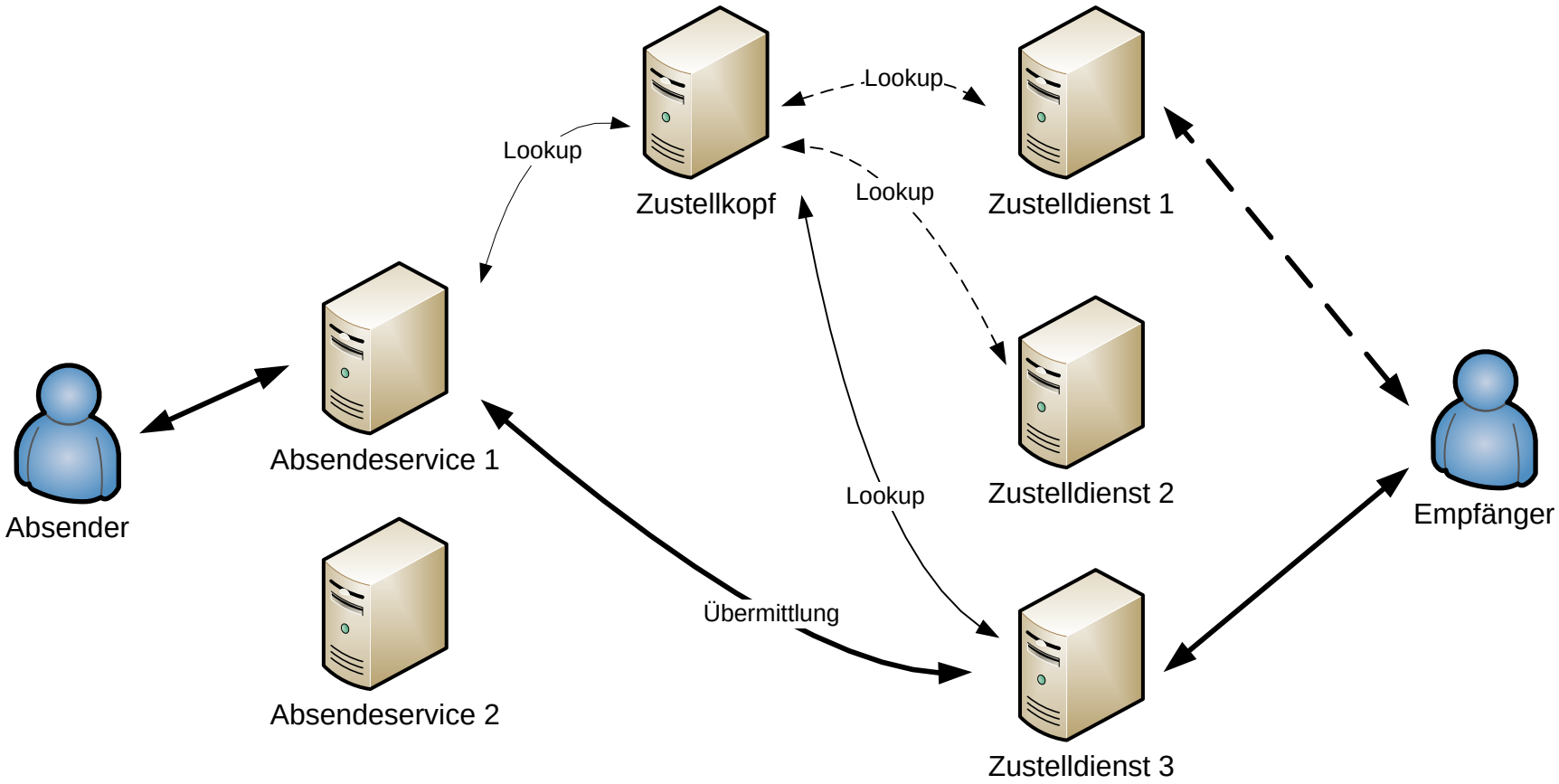
- E-Zustellung ist die sichere Übermittlung von elektronischen Dokumenten.
- Sicherheit
  - Nachvollziehbarkeit
    - Garantierte Übermittlungsbestätigung (digital signiert)
    - Bzw. Mitteilung bei Misserfolg
  - Rechtliche Sicherheit
    - Bei Einsatz einer sicheren Signatur laut SigG ->
    - Gleichstellung mit eigenhändiger Unterschrift
  - Technische Sicherheit
    - Datenübertragung grundsätzlich immer verschlüsselt
    - Dokumente optional digital signiert / verschlüsselt

E-Zustellung: Funktionsprinzip vereinfacht

Sichere und nachvollziehbare Übermittlung von elektronischen Dokumenten



E-Zustellung: Funktionsprinzip detailliert



E-Zustellung – Details 1/3

- Mehrere Postfächer möglich
  - Bei unterschiedlichen Providern
- Dokumentenklassen
  - Z.B.: Rechnungslegung, Auftragswesen, Ausschreibungen, Verträge, Bankwesen
  - Konfiguration möglich (Empfang ja/nein)
  - Automatisierte Weiterleitung/Verteilung

E-Zustellung – Details 2/3

- Vertrauensstufen
  - "Einfach"
    - Prüfung der e-Mailadresse bei Registrierung
    - Login mit Username, Passwort, SMS-PIN …
  - "Mittel" (§40 BWG)
    - Zusätzlich organisatorischer Prozess (Ausweisvorlage)
    - Koppelung mit Online-Banking
  - "Hoch"
    - Digitale Signatur – Handysignatur (Bürgerkarte)
    - Eindeutige Identität (eGovG §2)

E-Zustellung – Details 3/3

- Zustell-Typen ("Qualitäten")
  - "Standard"
    - Garantierte Übermittlungsbestätigung vom ZD
    - Qualität >>> e-Mail
  - "Eingeschrieben"
    - Zusätzlich vom ZD digital signiert
  - "Identübermittlung"
    - Von ZD und Empfänger digital signiert

		Identifikation/Authentifizierung		
		Einfach	Mittel	Hoch
Zustell-typen	Standard	x	x	x
	Eingeschrieben		x	x
	Ident			x

E-Zustellung – mögliche Verbesserungen

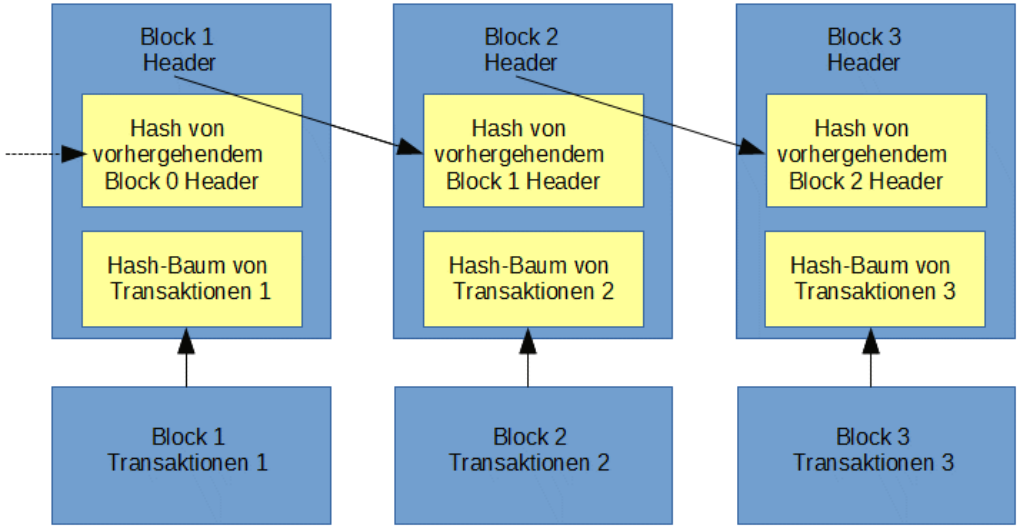
- Teilnehmerverzeichnis
  - Zentraler Meta-Verzeichnisdienst
  - Ausfall von Teilen möglich
- Billing/Clearing komplex
  - Absende- an Zustelldienste, Teil an Zustellkopf
  - "Billing-Token", Verrechnung nur bei Verwendung
- Wegfall eines Anbieters
  - Insolvenz, strategische Gründe …
  - Weitere Speicherung der Metadaten (Beweis der Übermittlung)?

Agenda

- Elektronische Zustellung
- Blockchain
- Anwendungsmöglichkeiten

Blockchain – Definition 1/2

- Verteilte Datenbank
- Datensätze (Blöcke)
  - beinhalten Transaktionen
  - sind kryptografisch abgesichert verkettet (d.h. können nachträglich nicht mehr verändert werden)



Blockchain – Definition 2/2

- Inhalte von "Transaktionen"
  - Transfer von Werten
    - bei Kryptowährungen
    - vgl. Überweisungen
  - "Skripts"
    - Programmcode
  - Textuelle u.a. Informationen
    - Klartext, Hash
  - …

Blockchain – Wesentliche Eigenschaften

- Verteilte Datenbank
  - Keine zentrale Infrastruktur (weder Datenbank, noch Netzwerk)
    - Kein Single Point of Failure
    - Nicht zerstörbar, zensierbar
  - Peer-to-Peer
    - Teilnehmer haben eine konsistente Kopie
  - Daten "öffentlich" einsehbar
    - Auch "privat" => siehe später
  - Auch "Konsensfindung" ist verteilt
    - "dezentral, gleichzeitig vertrauenswürdig"

Blockchain – Ausprägungen (2 Dimensionen)

		Validierung	
		Permissionless	*Permissioned*
Zugriff	*Public*	Bitcoin Ethereum	Evernym / Sovrin
	Private	{nicht betrachtet}	Corda / R3

- Zugriff
  - "Wer darf zugreifen?" (=lesen)
  - Public: Jeder Client darf (komplette Blockchain) lesen
  - Private: nur bekannte (geprüfte, authentifizierte) Teilnehmer
- Validierung
  - "Wer darf validieren?" (=schreiben)
    - Transaktionen verarbeiten, Blöcke bilden und hinzufügen)
  - Permissionless: Jeder Teilnehmer
  - Permissioned: beschränkte Liste ("Konsortium-Chain")

Agenda

- Elektronische Zustellung
- Blockchain
- Anwendungsmöglichkeiten

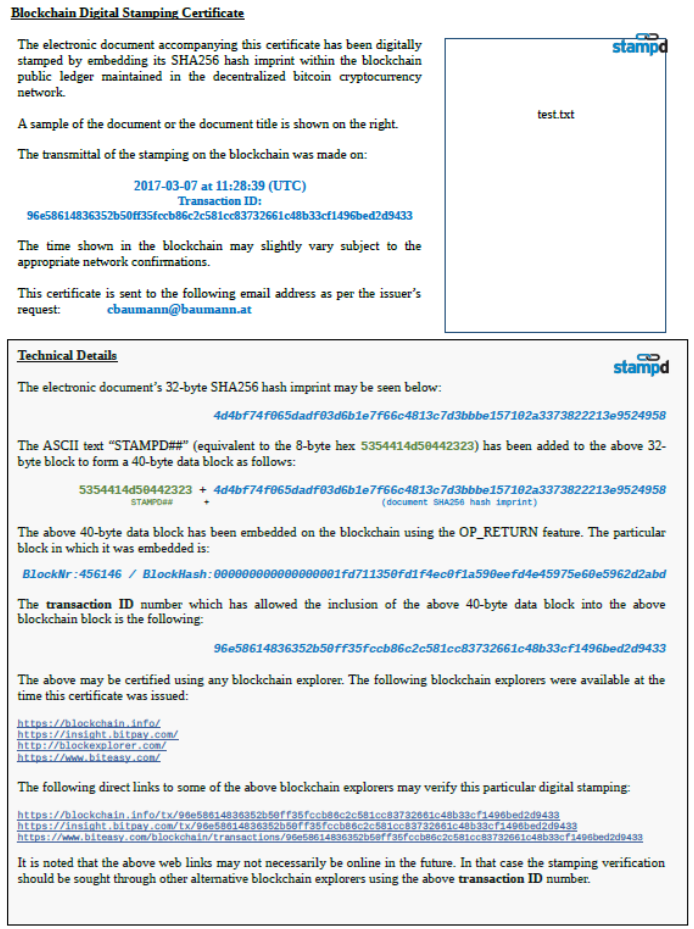
Einsatzszenarien der Blockchain Technologie bei e-Zustellung

- "Notarization"
  - Proof of Existence
  - Proof of Delivery
- Metadaten
  - Kopie in Blockchain
- Zentraler Meta-Verzeichnisdienst
  - Ersatz durch Identity & Access

Notarization 1/2

- "Proof of Existence"
  - Ein Dokument existiert …
    - zu einem bestimmten Zeitpunkt …
    - in einer bestimmten Form / Inhalt (Hashwert)
  - Bestehende Systeme
    - Bitproof, BlockSign, ProveBit, Stampd, Stampery …
    - Hashwert wird in bestehender Blockchain gespeichert (z.B. Bitcoin, Ethereum)
    - manueller Prozess

Beispiel: Proof of Existence



Blockchain Digital Stamping Certificate

The electronic document accompanying this certificate has been digitally stamped by embedding its SHA256 hash imprint within the blockchain public ledger maintained in the decentralized bitcoin cryptocurrency network.

A sample of the document or the document title is shown on the right.

The transmittal of the stamping on the blockchain was made on:

2017-03-07 at 11:28:39 (UTC)
Transaction ID:
96e58614836352b50ff35fccb86c2c581cc83732661c48b33cf1496bed2d9433

The time shown in the blockchain may slightly vary subject to the appropriate network confirmations.

This certificate is sent to the following email address as per the issuer's request: cbaumann@baumann.at

stampd

test.txt

Technical Details

stampd

The electronic document's 32-byte SHA256 hash imprint may be seen below:

4d4bf74f065dadf03d6b1e7f66c4813c7d3bbbe157102a3373822213e9524958

The ASCII text "STAMPD##" (equivalent to the 8-byte hex 5354414d50442323) has been added to the above 32-byte block to form a 40-byte data block as follows:

5354414d50442323 + 4d4bf74f065dadf03d6b1e7f66c4813c7d3bbbe157102a3373822213e9524958
STAMPD## + (document SHA256 hash imprint)

The above 40-byte data block has been embedded on the blockchain using the OP_RETURN feature. The particular block in which it was embedded is:

BlockNr:456146 / BlockHash:00000000000000001fd711350fd1f4ec0f1a590eefd4e45975e60e5962d2abd

The **transaction ID** number which has allowed the inclusion of the above 40-byte data block into the above blockchain block is the following:

96e58614836352b50ff35fccb86c2c581cc83732661c48b33cf1496bed2d9433

The above may be certified using any blockchain explorer. The following blockchain explorers were available at the time this certificate was issued:

https://blockchain.info/
https://insight.bitpay.com/
http://blockexplorer.com/
https://www.biteasy.com/

The following direct links to some of the above blockchain explorers may verify this particular digital stamping:

https://blockchain.info/tx/96e58614836352b50ff35fccb86c2c581cc83732661c48b33cf1496bed2d9433
https://insight.bitpay.com/tx/96e58614836352b50ff35fccb86c2c581cc83732661c48b33cf1496bed2d9433
https://www.biteasy.com/blockchain/transactions/96e58614836352b50ff35fccb86c2c581cc83732661c48b33cf1496bed2d9433

It is noted that the above web links may not necessarily be online in the future. In that case the stamping verification should be sought through other alternative blockchain explorers using the above **transaction ID** number.

- stampd.io
- File => Upload => Hash => Bitcoin-Blockchain
- Kosten: 0,09 €
- Certificate
  - Timestamp & Hash
  - Details zur Verifizierung
- => Certificate + Document = Proof

Notarization 2/2

- "Proof of Delivery"
  - Proof Of Existence
  - Plus "Beweis der Übermittlung"
  - D.h. zusätzliche Metadaten
    - …

Metadaten von Zustellungen 1/2

- Speicherung von Metadaten für Nachweis der Übermittlung
  - derzeit providerintern
  - vertraglich geregelt
- Metadaten
  - Sender, Empfänger: ID, RealName,
  - Zeitstempel: Versand, Übermittlung (an Zielsystem), Empfang, (ggf. Notifies)
  - Zustelldaten: Dokumententyp, Qualität
  - Dokumente
    - Hashwert des Files
    - Ggf. Zusatzinfos (MIME-Type, Filename, Filedatum, Größe)
    - Dokument abgelegt in Cloud: Link (ev. Gültigkeitsdatum)
  - Empfangsbestätigungen (signiert)

Metadaten von Zustellungen 2/2

- Derzeitiger Nachteil
  - Ausfall eines Providers (Insolvenz …)
  - Metadaten verloren => Übermittlungsnachweise nicht mehr möglich
- Lösungsansatz
  - Zusätzliche Verspeicherung der Metadaten in einer Blockchain
    - Optional, Kundenwunsch …
  - Verschlüsselung – je nach Anwendungsfall
    - Verschlüsselt (Kunde hält Key)
    - Verschlüsselt (Key wird hinterlegt)
    - Hashwert (=> POE/POD)
    - Unverschlüsselt: jeder BC-Teilnehmer kann lesen (Veröffentlichungspflicht, Ausschreibungen …)

E-Zustellung – Verzeichnisdienst 1/2

- Derzeit: Zentraler Meta-Verzeichnisdienst
  - sucht in den Daten der einzelnen Anbieter
  - konzentriert die Ergebnisse
- Nachteile
  - (Temporärer technischer) Ausfall eines Anbieters
    - => Teile der Suchergebnisse fehlen
  - Ausfall des zentralen Dienstes

E-Zustellung – Verzeichnisdienst 2/2

- Lösungsansatz
  - Identity & Access mit Blockchain
  - Teilnehmer verwaltet eigene digitale Identität
    - In dezentralem System
    - Für viele Anwendungen
  - Koppelung der Identität mit jeweiligem Serviceprovider
  - Provider haben dieselbe Sicht auf die Teilnehmer
  - => kein zentraler Verzeichnisdienst mehr nötig
- Vgl. u.a. Positionspapier TeleTrusT

Weitere Themen, Ausblick

- Sidechains
  - BCs, die andere Anforderungen abdecken (Geschwindigkeit und/oder Datenmenge)
  - periodisch durch andere BC bestätigt
- Smart Contracts
  - Automatisierte Abwicklung von Verträgen (Ethereum)
  - DAOs (dezentrale autonome Organisationen)
- Konsortien (Standardisierung)
  - B3i (Versicherungen), R3 Corda (Banken)
  - Hyperledger (Linux foundation, industrieübergreifend)

Zusammenfassung, Ausblick

- BC Technologie
  - Mehrere Jahre erprobt (Kryptowährungen)
- Auch in anderen Anwendungsbereichen (sinnvoll) einsetzbar
  - Dokumentenübermittlung, Notarization …
  - Identity & Access, Supply Chain, Fertigung, Energiewirtschaft …

- "Hausaufgaben"
  - Technologische Aspekte
  - Standardisierung
  - Rechtliche Rahmenbedingungen

Kontakt

AUSTRIAPRO

http://www.austriapro.at
austriapro@wko.at

DI Dr. Christian Baumann
c.baumann@baumann.at
+43 664 43 24 243