DATA MARKET
AUSTRIA

SMART CONTRACTS AUS TECHNISCHER UND RECHTLICHER PERSPEKTIVE

Dr. Sven Schlarb, Austrian Institute of Technology
Prof. Ing. Dr. Clemens Appl und Mag. Bettina Rinnerbauer, Donau Universität Krems

IT-Rechtstag 2018

Agenda

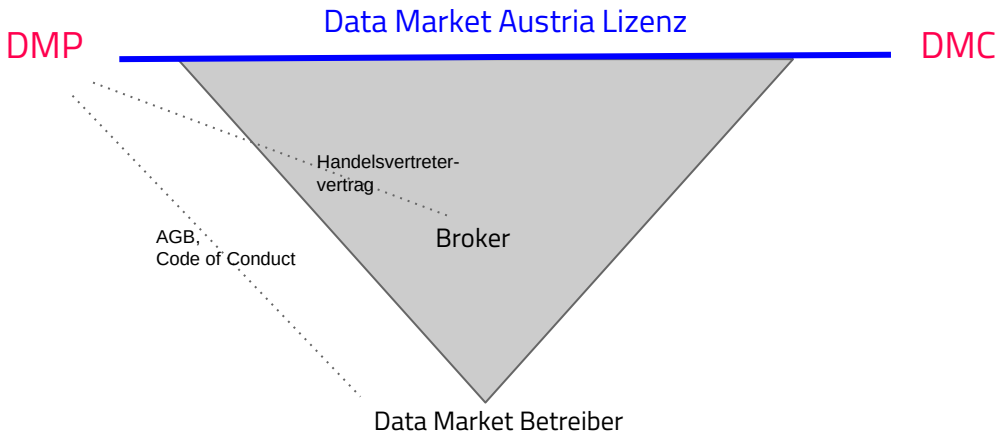
1. Data Market Austria - Einführung
2. Smart Contracts aus technischer Perspektive
   - Blockchain
   - Smart Contracts
   - Smart Contracts im DMA
3. Smart Contracts aus rechtlicher Perspektive
   - Begriffsverständnis
   - Rechtliche Potentiale und Herausforderungen
   - Auswirkungen auf den DMA
4. Zusammenfassung & Diskussion

DATA MARKET
AUSTRIA

1.
Data Market Austria - Einführung

Data Market Austria

Akteure und Vertragsverhältnisse

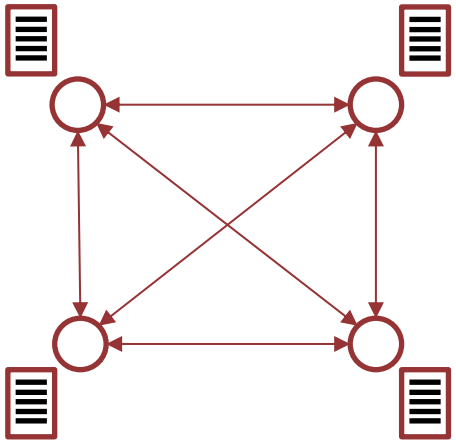


DATA MARKET
AUSTRIA

2.
Smart Contracts aus technischer Perspektive

Was ist eine Blockchain

- Ein **verteiltes Kontobuch**, das eine Transaktionshistorie enthält.
- Eine Technologie, die es **verschiedenen Parteien, die sich nicht notwendigerweise vertrauen**, ermöglicht, eine verteiltes Kontobuch zu verwalten.
- Daten (Transaktionen) sind in einer Struktur gespeichert, die "**Block**" genannt wird.
- Jeder Block referenziert den vorhergehenden Block, dadurch entsteht die **Blockchain**.

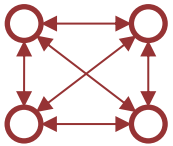


Grundlegende Technologien

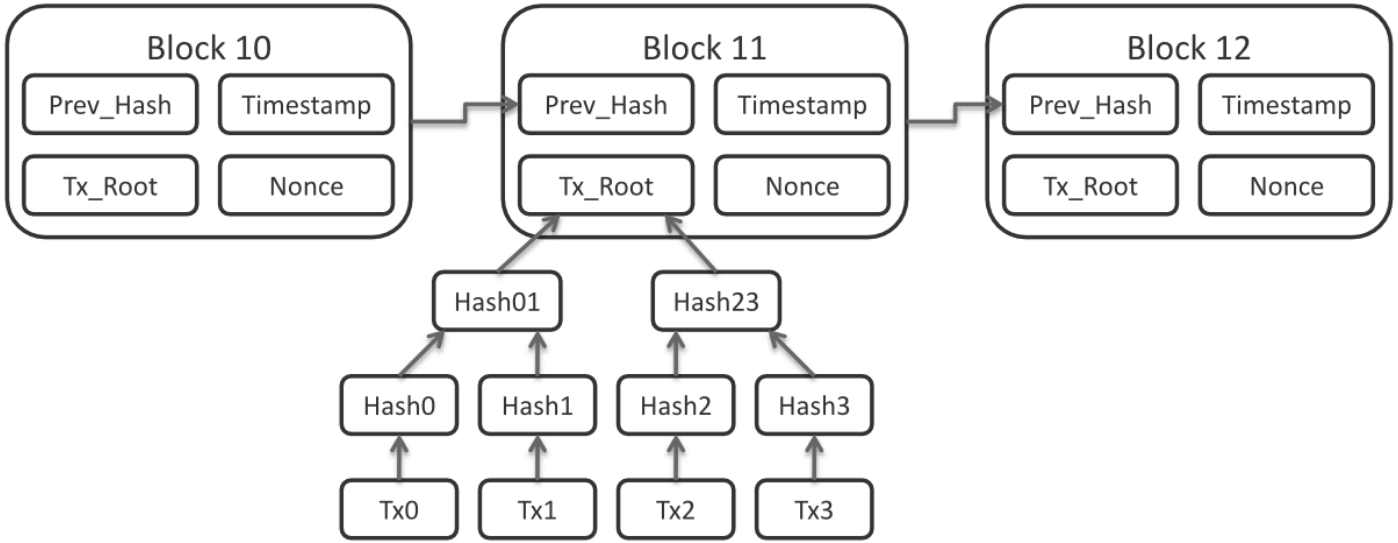
- Hash Funktionen

- Asymmetrische Verschlüsselung

- Peer-to-Peer Netzwerke



Das Blockchain-Grundprinzip

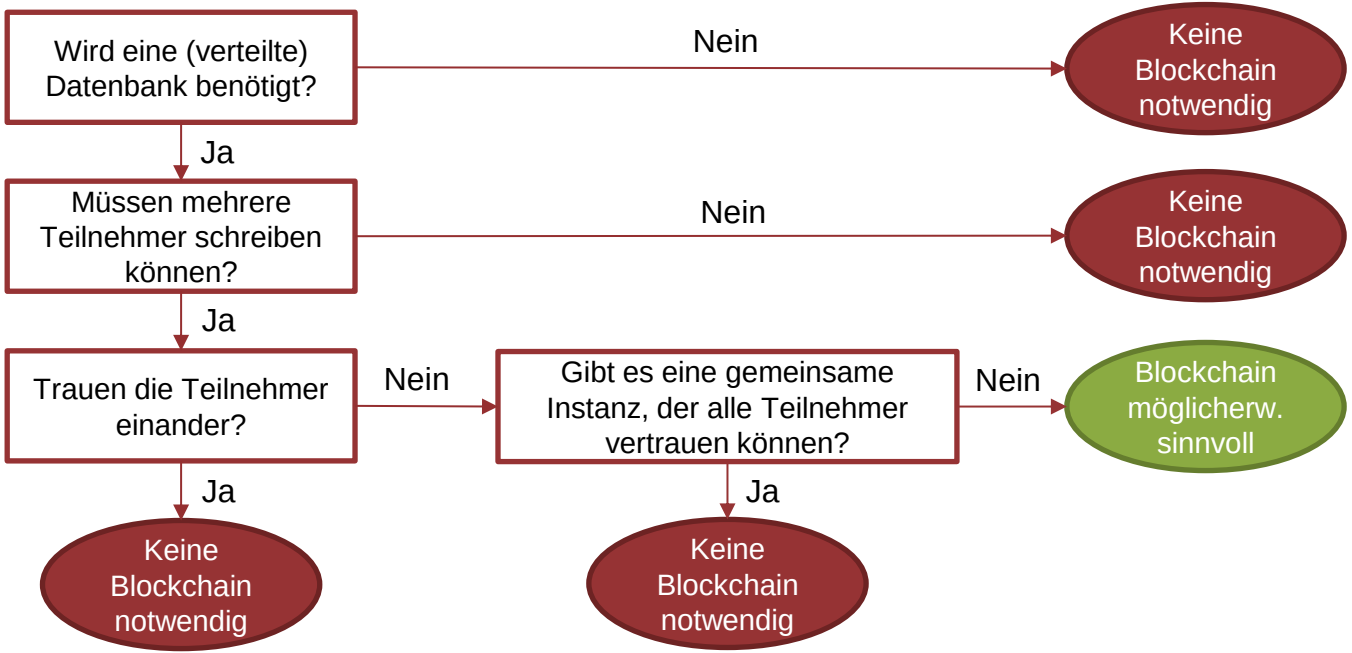


Matthäus Wander (https://commons.wikimedia.org/wiki/File:Bitcoin_Block_Data.png), „Bitcoin Block Data“, https://creativecommons.org/licenses/by-sa/3.0/legalcode

Was bietet die Blockchain?

- **Keine zentrale Vertrauensinstanz notwendig (Konsens-Mechanismus), aber Ehrlichkeit** der Mehrheit der Knoten erforderlich (nicht exklusiv: Paxos)
- Mechanismen der **manipulationssicheren Nachvollziehbarkeit und Rückverfolgbarkeit** (mit Einschränkungen!, nicht exklusiv: manipulationssicherer Datenspeicher)
- **Wirklich dezentrales Lesen und Schreiben**
- **Verteilung der Betriebskosten** (Anreize, Mining)
- **Widerstandsfähigkeit** gegen Angriffe

Wann brauche ich eine Blockchain?



Basierend auf: http://blockchain.mazeus.eu/blog/when-to-use-a-blockchain

Nick Szabo: “Smart Contracts” (1996)

- **Einsehbarkeit**
  - Vertragsparteien müssen in der Lage sein, die Erfüllung des Vertrages der jeweils anderen Vertragsparteien zu beobachten.
- **Überprüfbarkeit**
  - Es muss der Nachweis möglich sein, dass ein Vertrag erfüllt oder verletzt wurde (besonders wichtig im Falle einer Untersuchung oder eines Rechtsstreits)
- **Privatheit**
  - Wissen sollte nur soweit nötig mit den verschiedenen Vertragsparteien geteilt werden.
- **Durchsetzbarkeit**
  - Bestehen auf Vertragserfüllung oder gegebenenfalls Maßnahmen bei Nichterfüllung.

Smart Contract - Definitionen (J. Stark)

- **"Smart Legal Contract"**
  - Ergänzung oder Ersatz eines Vertrags.
  - Software-Beispiele:
    - Erstellung:
      ContractExpress, HotDocs, Exari
    - Veröffentlichung: LegalZoom, LawDepot, RocketLawyer
    - Analyse: Luminance, LawGeex, Kira, LexPredict
- **“Smart Contract Code”**
  - Code ausgeführt auf der Blockchain.
  - Software-Beispiele:
    - Ethereum, Bitcoin, ICOs (anarchy)
    - Tezos, Allegro, Hyperledger Cicero, InternetOfAgreements, Matterum, Legalese

Smart Contract Plattformen

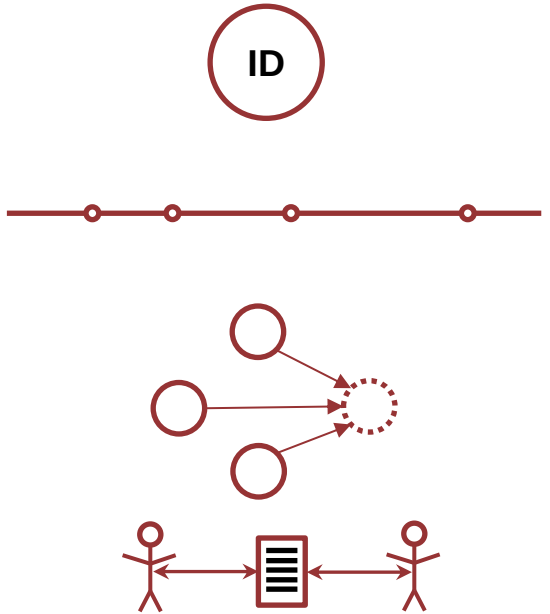
Plattform	Kontrolle	Währung	Konsens	Lizenz	Jahr	Sprache
Bitcoin	Öffentlich	Bitcoin (BTC)	„Schürfen“ Proof-of-Work	MIT	2009	Bitcoin Script
Ethereum	Öffentlich	Ether (ETH)	„Schürfen“ Proof-of-Work	LGPL 3.0	2015	Solidity
Hyperledger Fabric	Privat	Tokens	Solo/Kafka	Apache 2.0	2017	Chaincode, Go
Ripple	Privat	Ripple	Ripple-Konsens	--	2015	Kotlin, Java

Platform name	Contract language	Live?	Origin	Inc. in	Est.	Pub. rel.
Bitcoin	Ivy-lang	Yes	USA	USA	2017.12	2017.12
BitShares	?	Yes				
Cardano	Plutus (Haskell inspired)	no	HK	Switzerland	2015	
Counterparty	?	Yes				
Corda						
DFINITY	Ethereum compatible (aka Solidity, Serpent, etc.)	No				
EOS	C/C++ (compiles to WASM)	no				
Ethereum	Solidity	Yes	CA	Switzerland	2014.04	2015.07
Ethereum Classic	Solidity	Yes	^^^	no	^^^	^^^
Exonum	Rust. Java bindings TBD	No	UA	Netherlands		2017.07
hyperledger	?	?				
Lisk	Javascript					
Nem	?	?				
Neo	1st batch: dotNet; 2nd: Java,Kotlin; 3rd: C,C++,GO,Py,JS (TBD)	Yes	China	China	2014.06	2016.10
Neblio	REST-API, Python,JS, .NET(C# & VB.NET), Objective-C, Java, Node.js, GO, PHP	Yes	USA	USA	2017.01	2017.07
NXT	?	Yes				
OmniLayer						
Qtum	Solidity	Yes	Singapore	Singapore	2016	2017.09
quorum	?	?				
Radix	Scrypto (Based on JavaScript/TypeScript)	Yes	UK	UK	2018	
Rootstock	Solidity	no	Argentina	Argentina	2015.11	
Tezos	Michelson	no				
Ubiq	Solidity	Yes	CA	CA ?		2017.01
Universa						
Urbit	Hoon	Yes				
Waves	*NA*	Yes	RU	?	2016	2016.11

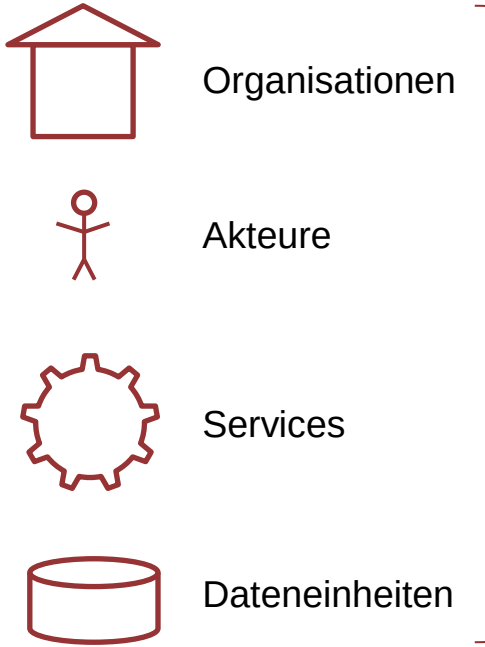
https://github.com/Overtorment/awesome-smart-contracts

Blockchain und Smart Contracts im DMA

- (1) Eindeutige Identifikatoren
  - für Daten, Services, und Akteure
- (2) Erfassen ausgewählter Ereignisse
  - z.B. Datenprodukt wird publiziert
- (3) Mitglieder-Abstimmung
  - Ein Kandidat wird vorgeschlagen und existierende Mitglieder können abstimmen
- (4) Vertragsabschlüsse
  - zwischen Daten- bzw. Service-Anbieter und DMA Kunde



DMA (1) Eindeutige Identifikation



Organisationen

Akteure

Services

Dateneinheiten

ID

Externally owned account (EOA)

1. **Privater Schlüssel**
   (64 (hex) characters / 256 bits / 32 bytes)
2. **Privater Schlüssel → Öffentlicher Schlüssel**
   (128 (hex) characters / 512 bits / 64 bytes)
3. **Öffentlicher Schlüssel → Addresse**
   (40 (hex) characters / 160 bits / 20 bytes)
   z.B. cd2a3d9f938e13cd947ec05abc7fe734df8dd826

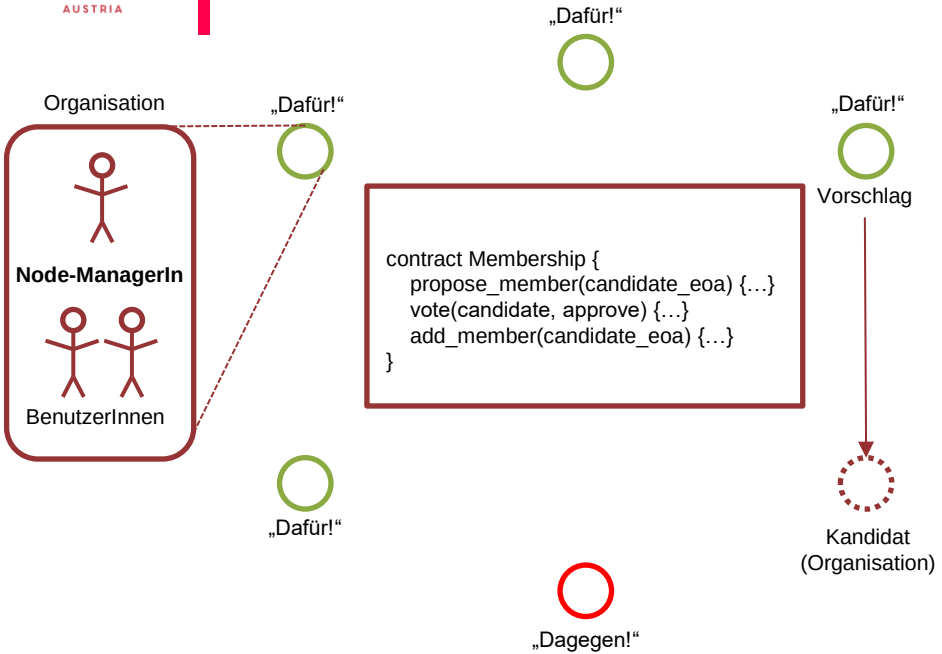
Private

Public

EOA

DMA (2) Erfassen ausgewählter Ereignisse

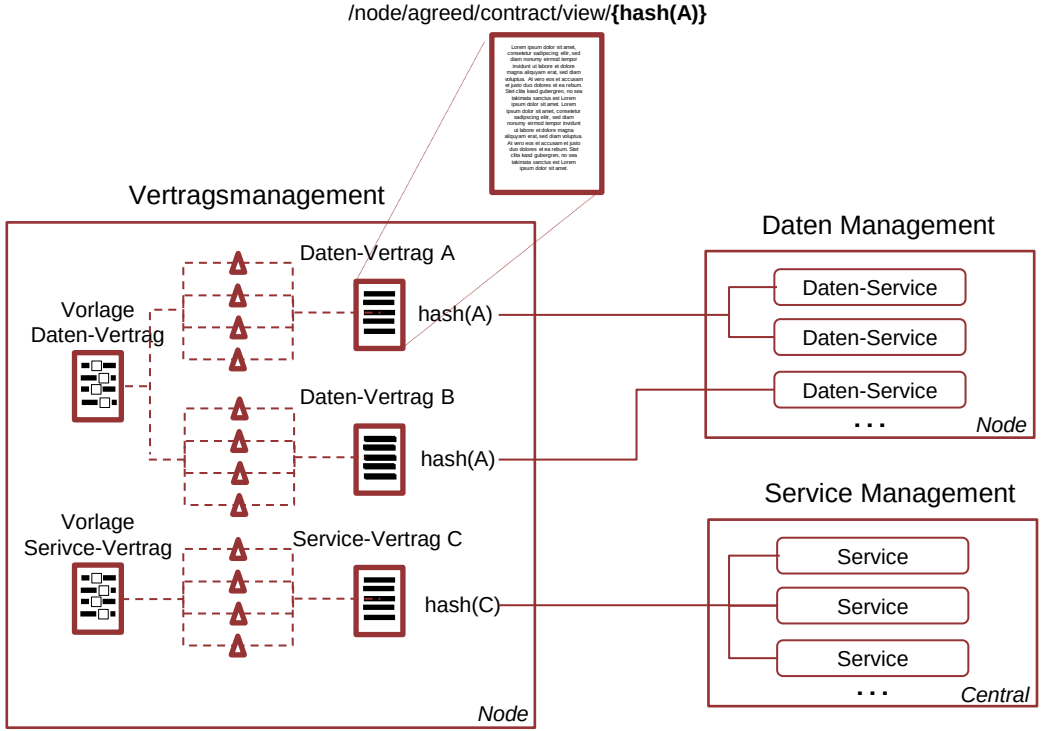
DMA (3) Mitglieder-Abstimmung



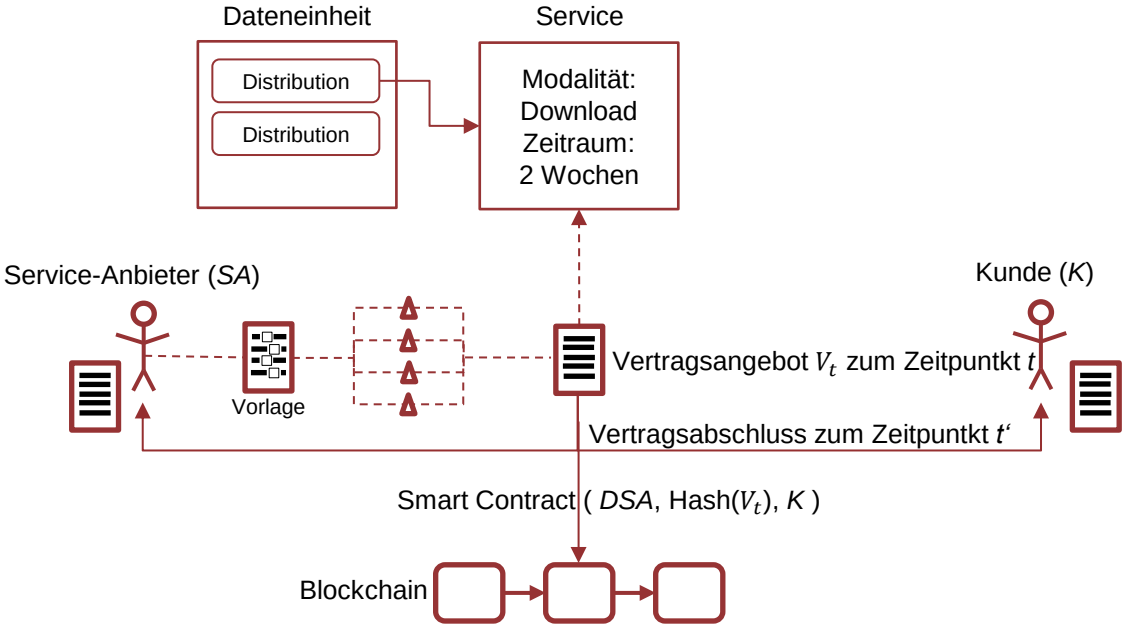

```
Attributes

    members : array of agents represented by Externally Owned Accounts (EOAs) of each DMA member organisation
    votes : map of voting values (0 for "no" or 1 for "yes") associated with
            EOAs e.g. [ait:d327da474bd44679b6cff25be194245f2d178874,1]

Methods

    propose_member (candidate_eoa) : Creates a new entry in the votes map keyed
        to the candidate_eoa. Can be invoked by any DMA member, but only once for
        any given candidate.

        Returns: true (if successful) or false (if failed)

    vote (candidate_eoa, approve) : Registers the value of approve (true or
        false) for a given candidate_eoa and the member organization executing the
        function in the vote map. Can be invoked by any DMA member, but only once
        for any given candidate.

        Returns: true (if successful) or false (if failed)

    add_member (candidate_eoa) : Checks the status of the votes map for a given
        candidate_eoa. If a majority of the existing members have voted in favor
        of the new candidate, the candidate_eoa is added to the members array and
        the vote is removed from the votes map. If a majority of the existing
        members have voted against the new candidate, the vote is removed from the
        votes map (and the proposed membership is rejected). If member votes are
        still pending, the function returns false but no other action is taken. Can
        be invoked by any DMA member.

        Returns: true (if successful) or false (if failed)
```

Bedingung: mindestens 80% dafür
4 von 5 Mitgliedern stimmen positiv
→ Kandidat wird Mitglied

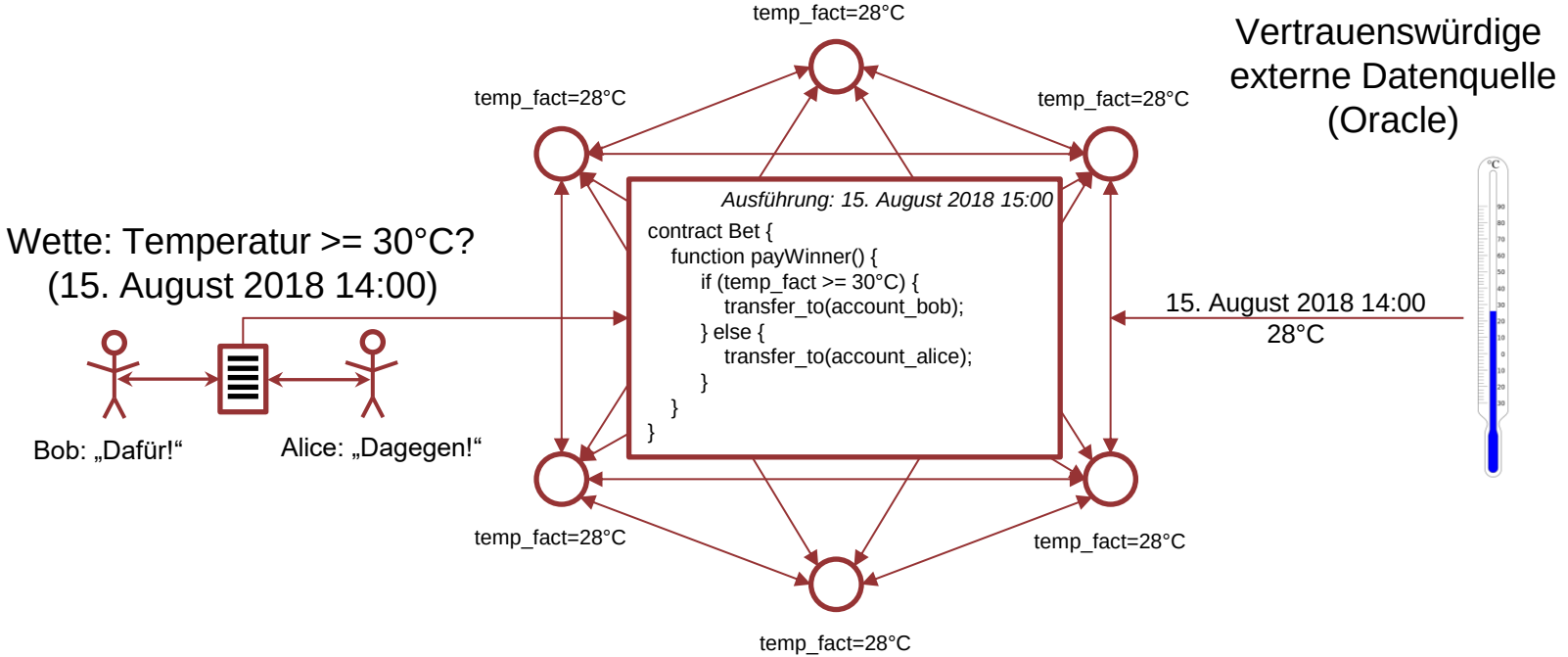
DMA (4) Vertragsmanagement



DMA (4) Vertragsabschluss zwischen Daten- bzw. Service-Anbieter und DMA Kunde



Unabhängige Vertrauensinstanz (*trused third party*)



Zustimmung zum Vertrag

Vertragspartei muss Vertragsinhalt verstehen

- Zugänglicher, verifizierbarer Source-Code

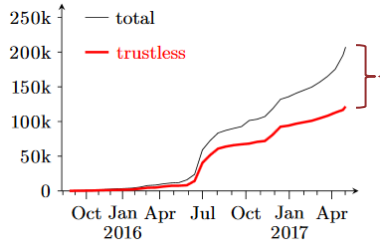
Integrität des Vertrags muss gewährleistet sein

- Unveränderlichkeit des kompilierten Codes

Keine Bedingungen, die sich im Nachhinein einseitig ändern lassen

- Unveränderlichkeit der Ablaufskontrolle

Ethereum Smart Contracts



Fröwis, M. & Böhme 2017, S. 14

Externe Abhängigkeiten

Bibliographie

- Clack, C. D.; Bakshi, V. A. & Braine, L. Smart Contract Templates: foundations, design landscape and research directions CoRR, 2016, abs/1608.00771
- Nick Szabo. Smart contracts: Building blocks for digital markets. Extropy, (16), 1996.
- Fröwis, M. & Böhme, R. In Code We Trust? Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer, 2017, 357-372

DATA MARKET
AUSTRIA

3.
Smart Contracts aus rechtlicher Perspektive

Smart Contract - Begriff

- Keine allgemein anerkannte Definition (Weber, R. H. 2017, 209)
- Auswahl:
  - "**Programme**, die von Maschinen verstanden, kontrolliert (auf das Eintreten der Bedingungen hin untersucht) und ausgeführt werden müssen" (Voshgmir 2016, 26)
  - "Rechtliche Vereinbarungen, die sich IT-Technologien bedienen, um die eigene Durchsetzbarkeit sicherzustellen" (Meitinger 2017, 372)
  - "Programm, das **manipulationssicher** gespeichert ist und bei Eintritt bestimmter Bedingungen vorher festgelegte Maßnahmen **garantiert** ausführt" (Heckelmann 2018, 504 mwN; Hervorhebung hinzugefügt)

Formen

- **Unterscheidung** nach Verwendung (Smets/Kapeller 2018, 296; Buchleitner/Rabl 2017, 7)
  - Erfüllungsinstrument
  - Juristischer Vertrag

- **“Self executing”** (Buchleitner/Rabl 2017, 7)
  - Suche von Vertragspartnern
  - Vertragsabschluss
  - Vertragsabwicklung

Anwendungsvoraussetzungen

- 2 Technologische Komponenten:
  - Blockchain
  - Contractware
    - Schreibt die Bedingungen der Vereinbarung in mit der ausführenden Maschine verbundene Software (Raskin 2017, 307)
    - Software zur Abbildung von wenn-dann-Konstellationen (Eschenbruch/Gerstberger 2018, 3 mwN)
- 2 Erfordernisse (Raskin 2017, 314):
  - Leistung der richtigen Ausgabe basierend auf einer faktischen Eingabe
  - Vergegenständlichung der Ausgabe in der realen Welt

Smart Contracts
Anwendungsfälle

- Drei Phasen des Vertragsrechts (Raskin 2017, 322-333):
  - Zustandekommen des Vertrages
  - Leistung
  - Vertragsverletzung
    - Ersatzansprüche für fahrlässiges Programmieren?
    - Ferngesteuerte "Startunterbrechung" eines Autos bei Unterbleiben der Zahlungen

- Beispiel: Photovoltaikanlagen
  - Übernahme von Strom der Nachbarn bei festgelegtem Preis (Smart-Meter, Software etc., siehe Buchleitner/Rabl 2017, 8 über Projekt http://brooklynmicrogrid.com/)

DATA MARKET
AUSTRIA

Smart Contract & Warenautomat

(Vgl Raskin 2017, 306 und Szabo, 2002)

Offertum ad incertas personas
(Buchleitner/Rabl 2017, 9 mwN)

Foto: Jiri Hönes, 2010 (CC-BY-SA 3.0)

Smart Contracts
& Zivilrecht (Heckelmann 2018, 506-508 mwN)

- Abgabe der Willenserklärung
- Zugang der Willenserklärung
- Zurechnung
- Zulässige Vertragssprache
- Anfechtung?

- Signieren der eigenen Erklärung mit privatem Schlüssel
- Anhängen des neuen Blocks an die Blockchain
- “Je autonomer ein System ist, desto weniger sind seine Handlungen dem Nutzer und desto mehr dem Programmierer zuzurechnen”
- Programmiersprache ist zulässig
- Anfechtungserklärung als eigener Block, aber gesetzlicher Unwirksamkeitsgrund nicht dokumentiert - (Un-)Wirksamkeit kann uU nicht aus Blockchain ersichtlich sein

Was bieten Smart Contracts nicht?
Die Grenzen

- Nicht alle Smart Contracts sind Verträge im zivilrechtlichen Sinn (Heckelmann 2018, 506 z.B. wetterabhängige Steuerung von Jalousien: es fehlen 2 Vertragspartner)
- Wahrnehmung von Ermessensspielraum wie ein Mensch - z.B. persönliche Zufriedenheit des Käufers mit einem Gemälde (Raskin 2017, 326)
- Garantie der Erfüllung in Übereinstimmung mit dem Vertrag
- Ausschluss der Geltendmachung von Ansprüchen auf Aufhebung oder Anpassung

Herausforderungen

- **Haftung** der beteiligten Akteure (Buchleitner/Rabl 2017, 7-8)
  - Programmierer der Blockchain
    - (Un-)Entgeltlichkeit maßgeblich für Leistungsstörungen und Schadenersatz
  - Mitglieder des Netzwerks
    - Bilaterale Verträge oder gesellschaftsrechtliche Elemente?
  - Smart-Contract Programmierer (zusätzlich bei Smets/Kapeller 2018, 298)
    - Werkvertrag, Warnpflichten

- **Identifizierbarkeit** der Teilnehmer:
  - Höhere Transparenz und Sicherheit der Transaktionen
  - Wie soll datenschutzrechtliche Löschung der in der Kopie der Blockchain enthaltenen Daten bei allen Teilnehmern erfolgen? (zur Thematik Martini/Weinzierl 2017)

- **Unsicherheit** als Barriere für Anwendung neuer Technologien (Raskin 2017, 340)

Smart Contracts im DMA

Überlegungen: Zustandekommen des Vertrages, Erfüllung bei Unentgeltlichkeit, Beendigung

1. Smart contract wird generiert mit **Angebotslegung** des DMP

2. Hash über das Angebot wird in Bezug auf eine Distribution in Blockchain gespeichert

3. DMC nimmt Angebot an

3. DMC legt Gegenanbot

4. Dokumentation in Blockchain:
   - Alle Angebote
   - Finaler Vertrag

Smart Contracts - Ausgewählte Potentiale

1. Weniger staatliche Rechtsdienstleistungen erforderlich?
2. Fälschungssicherheit?
3. Sichere Erfüllung?
4. Vereinfachung bei wiederkehrenden Leistungen?

1. Weniger staatliche Rechtsdienstleistungen?

- Reduktion der Erforderlichkeit staatlicher Rechtsdienstleistungen?
  (Raskin 2017, 308 mwN; 309;312;325)
  - Senkung von Transaktionskosten durch Wegfall von Intermediären
  - Sicherstellen der Leistung ex ante, kein ressourcen-intensives Gerichtsverfahren
  - Weniger Zweideutigkeit/Unklarheit

Auswirkungen auf den DMA

- **Ersatz vertrauenswürdiger Dritter:** grds möglich
  - Treuhand: Bestellung, Hinterlegung des Kaufpreises
    → Zustellung führt zur Übermittlung des Preises (Heckelmann 2018, 504)
  - Keine Hinterlegung beim Notar
    (Eschenbruch/Gerstberger 2018, 6 im Kontext von Bauverträgen)
- **Entfall von Rechtsstreitigkeiten:** aktuell kaum denkbar
  - Keine Streitigkeiten über Mängel, Irrtümer etc. und keine staatlichen Streitbeilegungsmechanismen = Illusion
    (Buchleitner/Rabl 2017, 6, 13)
- **Hilfe für Vertragsauslegung:** möglich
  - Abspeicherung in Blockchain lässt erkennen, von wem eine Klausel stammt (z.B. relevant für Auslegung nach § 915 ABGB)

DATA MARKET AUSTRIA

2. Fälschungssicherheit ?

- Vermeidung von
  (Eschenbruch/Gerstberger 2018, 4)
  - Manipulation
  - Vertragsbrüchigkeit
  - Zahlungsunwilligkeit
  - Zahlungsunfähigkeit

Auswirkungen auf den DMA

- Fälschungssicherheit der Blockchain zweifelhaft?
  (dagegen Buchleitner/Rabl 2017, 6; dafür Martini/Weinzierl 2017, 1252)
- Ablegen verschieder Angebotsversionen in Blockchain:
  - Beweiserleichterung im Fall eines Gerichtsverfahrens

3. Sichere Erfüllung?

- "Vertragsmanagement"
  (Heckelmann 2018, 505)
  - Bezahlung
    → Hotelzimmertür öffnet
  - Ausbleiben der Leasingraten
    → Sperrung des Kfz

- z.B. bei Bauverträgen
  (Eschenbruch/Gerstberger 2018, 5-6):
  - Vertragsversion mit elektronischer Signatur unveränderbar gespeichert
  - Prüfung auf Mängel durch Objektüberwacher, Abnahme
    → Automatisierte Zahlung/Einbehaltung
  - Gesteigerte Erfüllungs- u. Gewährleistungssicherheit

Auswirkungen auf den DMA

- Automatisierung kann Leistungsstörungen mitunter vorbeugen, aber in vielen Fällen nicht völlig ausschließen
  - Problem: Automatisierte Prüfung der Datenqualität hat Grenzen
    (z.B. sole source data)

4. Vereinfachung bei wiederkehrenden Leistungen

- Ausführung gesetzlicher Regelungen
  - Bezahlung von jährlichen Gebühren
    (Meitinger 2017, 372, 374)

Auswirkungen auf den DMA

- Mögliche Vereinfachung beim Bezug von Daten im Dauerschuldverhältnis

DATA MARKET
AUSTRIA

4. Zusammenfassung, Diskussion

Zusammenfassung

1. **“Smart Contract” ≠ “Vertrag im rechtlichen Sinn“**
   - Häufig nur “smarte“ Vertragsdurchführung
   - Wurzelmängel und Leistungsstörungen sind nicht immer “smart” erfassbar
   - Authentizität?

2. **„Smart Negotiating“**
   - Automatisierte Aushandlungsmechanismen komplexer Vertragswerke durch „smart contracts“
   - Vereinfachung in Dauerschuldbeziehungen
   - Blockchain: Lückenlose Dokumentation der Vertragsaushandlung; Sicherung der Datenintegrität

3. **Systemische Grenze:** Smart Contracts können nur in vollständig determinierten Umgebungen ihren vollen Nutzen entfalten; Schnittstellen in die reale Welt bilden vielfach die Schwachstelle.
   - Trustless trust & Oracles – ein Widerspruch?

Herzlichen Dank für Ihre Aufmerksamkeit!

sven.schlarb@ait.ac.at
clemens.appl@donau-uni.ac.at
bettina.rinnerbauer@donau-uni.ac.at

Siehe auch https://datamarket.at/events/kategorie/webinar-reihe/

Quellen

- *Buchleitner, C./Rabl, T.* (2017), Blockchain und Smart Contracts: Revolution oder alter Wein im digitalen Schlauch?, ecolex 2017, 4
- *Eschenbruch, K./Gerstberger, R.* (2018), Smart Contracts: Planungs-, Bau- und Immobilienverträge als Programm?, NZBau 2018, 3
- *Heckelmann, M.* (2018), Zulässigkeit und Handhabung von Smart Contracts, NJW 2018, 504.
- *Martini, M./Weinzierl, Q.* (2017), Die Blockchain-Technologie und das Recht auf Vergessenwerden: Zum Dilemma zwischen Nicht-Vergessen-Können und Vergessen-Müssen, NVwZ 2017, 1251
- *Meitinger, T.H.* (2017), Smart Contracts, Informatik Spektrum 40_4_2017, 371
- *Raskin, M.* (2017), The Law and Legality of Smart Contracts, Georgetown Law Technology Review, 305
- *Smets, S./Kapeller, S.* (2018), Smart Contracts: Vertragsabschluss und Haftung, ÖJZ 2018, 39
- *Szabo, N.* (2002), A Formal Language for Analyzing Contracts, accessible via http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/contractlanguage.html
- *Voshgmir, S.* in Hammel, C. (Hrsg.) (2016), Blockchains, Smart Contracts und das Dezentrale Web, Technologiestiftung Berlin
- *Weber, R. H.* (2017), Liability in the Internet of Things, EuCML 2017, 207

Special thanks to all the people who made and released these template resources for free:

- Presentation template by SlidesCarnival
- Photographs by Unsplash