Smart Contracts

Telemedicus Sommerkonferenz Berlin 2017

Jörn Erbguth, Law & IT Consultant

joern@erbguth.net +41 787256027

Die Blockchain

- Speicherung von Daten
- Unveränderlich
  - Bestehende Blöcke werden nie verändert oder gelöscht

Was ist eine Blockchain?

Eine Blockchain sind aneinander gereihte Datenblöcke. Ähnlich einer Datenbank werden diese Datenblöcke für viele zugreifbar abgelegt. Im Gegensatz zu Datenbanken geht es hier jedoch um pro Transaktion vergleichbar kleine Datenmengen und es fehlen zudem effiziente Zugriffsstrukturen wie z.B. Indizes. Im Gegensatz zu Datenbanken werden die Daten auch nie gelöscht sondern werden immer nur ergänzt.

Die Blockchain

- Speicherung von Daten
- Unveränderlich
  - Bestehende Blöcke werden nie verändert oder gelöscht

Was ist eine Blockchain?

Eine Blockchain sind aneinander gereihte Datenblöcke. Ähnlich einer Datenbank werden diese Datenblöcke für viele zugreifbar abgelegt. Im Gegensatz zu Datenbanken geht es hier jedoch um pro Transaktion vergleichbar kleine Datenmengen und es fehlen zudem effiziente Zugriffsstrukturen wie z.B. Indizes. Im Gegensatz zu Datenbanken werden die Daten auch nie gelöscht sondern werden immer nur ergänzt.

Die Blockchain

- Speicherung von Daten
- Unveränderlich
- Weltweit verteilt
  - Dezentral
    Jeder Knoten hat vollständige Kopie
    Spezielles Abstimmungsverfahren

Dezentral und weltweit verteilt

Eine Blockchain kennt keinen zentralen Server sondern ist auf sehr viele Server verteilt. Dabei hat jeder Rechner eine vollständige Kopie. Um sicher zu stellen, dass alle Kopien identisch sind, gibt es ein spezielles Abstimmungsverfahren. Dieses Verfahren stellt dabei ebenfalls sicher, dass Server mit einer manipulierten Version der Blockchain ausgeschlossen werden.

Die Blockchain

- Speicherung von Daten
- Unveränderlich
- Weltweit verteilt
- Regeln im Programmcode

  - Regeln bestimmen, welche Transaktionen in einen neuen Block aufgenommen werden dürfen.

Sicherheit durch transparente Regeln im offenen Quellcode

Die Regeln, wer was auf die Blockchain schreiben kann, stehen im Programmcode der Blockchain. Neuere Varianten von Blockchains schreiben ein Teil dieser Regeln sogar selbst auf die Blockchain. Diese Regeln werden dann auch „Smart Contracts“ genannt.

Smart Contracts ≠ intelligente Verträge

Was sind eigentlich „Smart Contracts“?
Smart Contracts sind nicht „intelligente Verträge“. Sie sind genau genommen weder besonders intelligent noch sind es juristische Verträge.

Aber was ist eigentlich ein juristischer Vertrag?
Ein juristischer Vertrag ist ja auch nicht das Stück Papier auf dem die Vertragsbedingungen geschrieben sind. Ein Vertrag ist ein abstraktes juristisches Konstrukt. Es ist ein Rechtsgeschäft, begründet durch inhaltlich übereinstimmende in Bezug zu einander stehende Willenserklärungen von zwei oder mehr Personen.

Smart Contracts - technisch

- Kleine Programme
- Erhalten Nachrichten
- Kontrollieren das Ergebnis der Transaktionen

Was sind Smart Contracts technisch?

Das sind kleine Programme. Sie erhalten Nachrichten und führen abhängig von den Nachrichten und den intern gespeicherten Regeln Transaktionen aus.

Damit wird klar, wie die Smart Contracts zu ihrem Namen kamen. Sie können feststellen, dass zwei (oder mehr) Willenserklärungen zusammen passen und führen dann die Vertragstransaktion aus.

Ein Smart Contract ist daher auch nicht ein Vertrag sondern eher eine Klasse von gleichartigen Verträgen

Smart Contracts - auf der Blockchain

- auf der Blockchain gespeichert
- auf der Blockchain ausgeführt
- transparent
- manuell nicht beeinflussbar

Was haben Smart Contracts mit der Blockchain zu tun?

Jeder kann sein vertragliches Handeln automatisieren. Automaten drucken Tickets oder geben uns nach Münzeinwurf eine Ware. Hier ist die Automatisierung nicht transparent und liegt klar in der Hand eines Vertragspartners.

Auf der Blockchain ist das anders: Die Verträge sind transparent, der sehr kompakte Programmcode ist transparent, ohne unbestimmte Rechtsbegriffe und für viele verständlicher als hundert Seiten lange allgemeine Geschäftsbedingungen.
Die Smart Contracts werden aber auf der Blockchain ausgeführt. Dies ist eine neutrale kaum manipulierbare Plattform. Das bedeutet, dass damit sicher gestellt ist, dass auch nur diese Programmversion ausgeführt wird.

Im Vergleich mit einem Verkaufsautomaten hat dies den Vorteil, dass wir sicher gehen können, dass der Automat genau das tut, was im Code geschrieben ist. Wir müssen nicht dem Automatenhersteller oder Automatenaufsteller vertrauen.

Wie insgesamt auf der Blockchain bedeutet dies, dass auch bei Smart Contracts Vertrauen durch Transparenz und Algorithmen hergestellt wird.

Smart Contracts und Krypto-Währungen

Smart Contracts können

- Krypto-Geld erhalten
- Krypto-Geld halten
- Krypto-Geld transferieren

Ein weiterere Besonderheit von Smart Contracts auf der Blockchain ist der Zugriff von Smart Contracts auf Krypto-Währungen.
Smart Contracts können Krypto-Geld (ihrer Blockchain) erhalten, verwalten und transferieren. Damit können sie z.B. als Treuhänder agieren, der das Geld nur nach den transparent und unveränderbar festgelegten Regeln weitergibt.

Smart Contract

- Beispiel
- Blockchain basierte Verkaufsplattform
- Transparente Regeln
- Komplett automatisiert
- Ohne manuelle Eingriffsmöglichkeit

Um das Funktionieren eines „Smart Contracts“ zu illustrieren, möchte ich das Beispiel einer Blockchain basierten Verkaufsplattform vorstellen.
Sie ist komplett automatisiert und funktioniert nach transparenten Regeln.

Smart Contract - Beispiel Handelsplattform

Blockchain

Verkäufer

Ein Verkäufer bietet ein Fahrrad zum Verkauf an. Dazu bedient er sich eines Smart Contracts auf der Blockchain.

Smart Contract - Beispiel Handelsplattform

Smart Contract
Entwickler

Verkäufer

Ein Smart Contract Entwickler hat einen Smart Contract entwickelt, damit Dritte miteinander Handel treiben können.

Smart Contract - Beispiel Handelsplattform

Smart Contract
Entwickler

Verkäufer

Käufer

Der Verkäufer sendet eine Nachricht mit seinem
Verkaufsangebot an den Smart Contract auf der Blockchain.

Dies sieht ein Interessent.

Smart Contract - Beispiel Handelsplattform

Smart Contract
Entwickler

Verkäufer

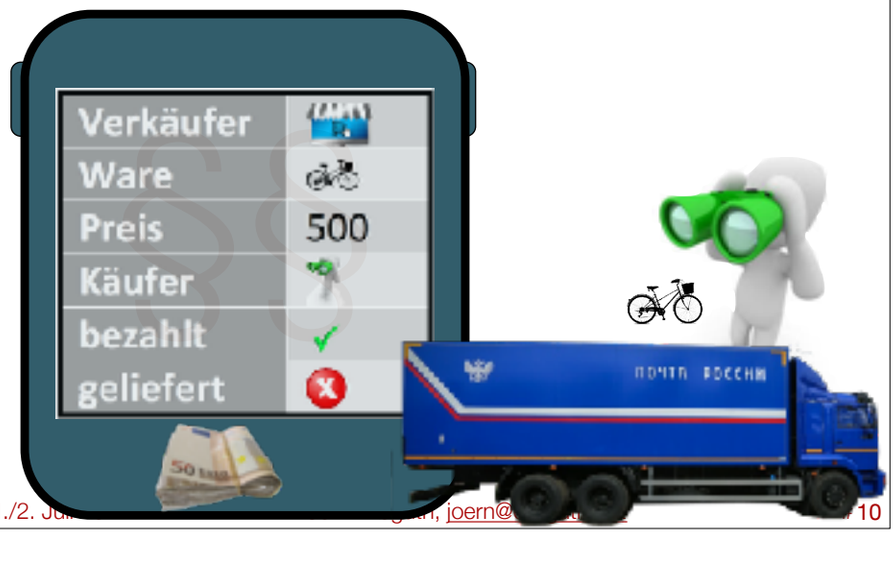
Käufer

Der Interessent nimmt dieses Angebot an und transferiert mit seinem Angebot den Kaufpreis (in der Kryptowährung der Blockchain). Der Kaufpreis wird bis zur erfolgten Lieferung vom Smart Contract gehalten.

Smart Contract - Beispiel Handelsplattform

Smart Contract
Entwickler

Verkäufer



Das Fahrrad wird geliefert und die Lieferungsbestätigung vom Spediteur (z.B. die russische Post) auf der Blockchain bestätigt.

Smart Contract - Beispiel Handelsplattform

Smart Contract
Entwickler

Verkäufer

Käufer

Mit der Lieferbestätigung transferiert der Smart Contract automatisch den Kaufpreis an den Verkäufer.

Smart Contract - Beispiel Code

```
1  pragma solidity ^0.4.2;
2
3  contract Handel {
4      string public Ware;
5      uint public Preis;
6      address public Verkaeufer;
7      address public Kaeufer;
8      bool public bezahlt;
9      bool public geliefert;
10     bool public angenommen;
11     address constant post=0x1234567890abcdef;
12
13 function Angebot(string iWare, uint iPreis)
14 {
15     Verkaeufer=msg.sender;
16     Ware=iWare;
17     Preis=iPreis;
18 }
19
20 function Annahme() payable
21 {
22     if(msg.value==Preis)
23     {
24         Kaeufer=msg.sender;
25         bezahlt=true;
26     }
27 }
28
29 function Lieferung()
30 {
31     if(msg.sender==post && geliefert==false)
32     {
33         geliefert=true;
34         abgesendet=Verkaeufer.send(Preis);
35     }
36 }
37 }
```

Hier der beispielhafte Programmcode. Dieser ist sehr kompakt. Klar erkennbar sind oben die Variablen und darunter die Funktionen zur Entgegennahme der drei Arten von Nachrichten, die dieser Smart Contract verarbeiten soll.

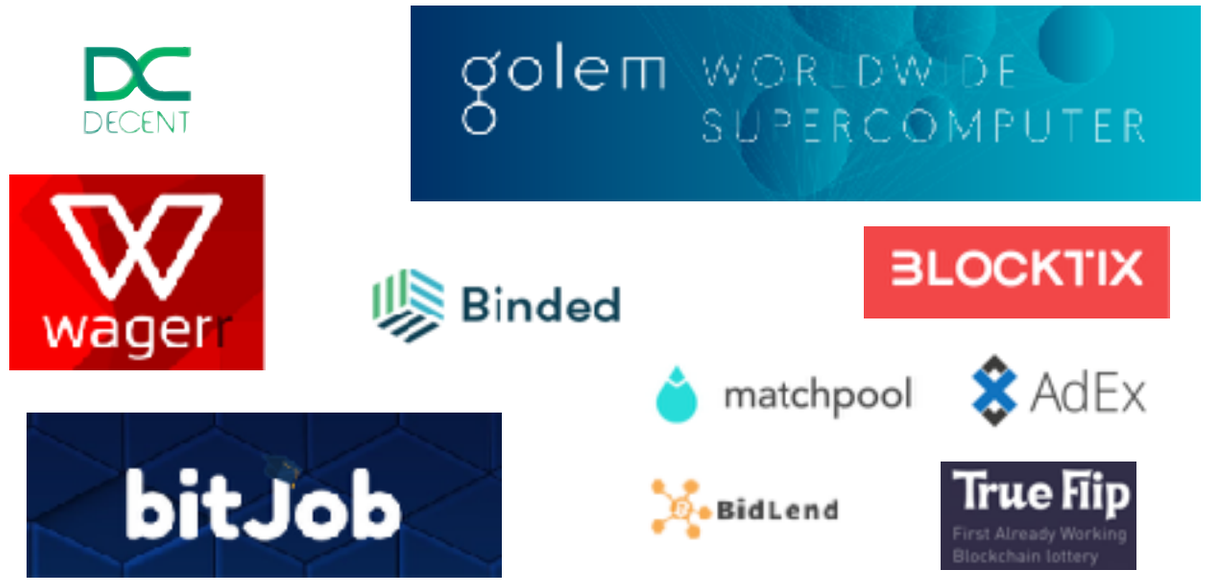
Auswirkungen (1)

Disintermediation

Die „Share Economy“ hat uns viele neue Intermediäre gebracht, die die neuen direkten Geschäfte verwalten und daran verdienen. Blockchain und insbesondere Smart Contracts versprechen nun diese Intermediäre überflüssig zu machen.

Auswirkungen (2)

Neue direkte Geschäfte



Unzählige Systeme bieten neue direkte Geschäfte an:

Decent: Für Autoreninhalte
golem: Das Aribnb für Computerleistung
Wagerr: Eine Wettplattform
bitJob: Jobvermittlung
Binded: Für das einfache und direkte Verwerten von Urheberrechten
Blocktix: Für Eventtickets
BidLend: Eine Peer-to-Peer Darlehensplattform
TrueFlip: Eine Blockchain-Lotterie
AdEx: Eine Plattform für das Vermarkten von Online-Werbung
matchpool: Blockchain basiertes Dating

Auswirkungen (3)

eGovernment

- Grundbücher
- umfassend
- virtueller Staat

Grundbücher - Projekte gibt es in Schweden, Ghana, Georgien, Honduras
Ukraine sagt: Public Services, Social Security, Public Health, Energy Sector
virtueller Staat - Bitnation: Umfangreiche Dienstleistungen - kompatibel mit estnischen e-residency

Quellen: https://www.btc-echo.de/schweden-geht-weitere-schritte-richtung-blockchain-grundbucheintraege/
https://bravenewcoin.com/news/ukraine-and-bitfury-launching-first-full-scale-blockchain-egovernment-pilot/

Auswirkungen (3)

eGovernment

- Grundbücher

Grundbücher - Projekte gibt es in Schweden, Ghana, Georgien, Honduras

Auswirkungen (3)

eGovernment

- Grundbücher
- umfassend

Public Services, Social Security, Public Health, Energy Sector

Auswirkungen (3)

eGovernment

- Grundbücher
- umfassend
- virtueller Staat

virtueller Staat - Bitnation: Umfangreiche Dienstleistungen - kompatibel mit estnischen e-residency

Quellen: https://www.btc-echo.de/schweden-geht-weitere-schritte-richtung-blockchain-grundbucheintraege/
https://bravenewcoin.com/news/ukraine-and-bitfury-launching-first-full-scale-blockchain-egovernment-pilot/

Auswirkungen (4)

- Autonome Plattformen
- Regulierung kaum durchsetzbar
- Attraktiv für kriminelle Geschäfte
- Konfliktlösung ?
- Datenschutz ?

Lauter neue autonome Plattformen - naja nicht immer. Inzwischen ist das so ein Hype, dass alle sagen, sie würden die Blockchain einsetzen - obwohl das häufig nicht der Fall ist.
Wenn die Plattform autonom als Smart Contract läuft, ist Regulierung kaum durchsetzbar.
Daher sind diese Plattformen gerade für illegale Geschäfte interessant. Kriminelle vertrauen sich nicht - da kommt Vertrauen durch Algorithmen gerade recht.
Was ist bei Konflikten? Der Rechtsweg ist meistens nicht praktikabel. Konfliktlösung ist aber teilweise eingebaut.
Die Daten auf der Blockchain sind - wenn sie nicht encrypted sind - immer öffentlich auslesbar und können nicht gelöscht oder verändert werden. So ist z.B. das Recht auf Vergessen oder auf Berichtigung nicht durchsetzbar.

Konsequenzen

- Nationale Regulierungen für internationale Plattformen ?
- Effektives Verbot von Peer-to-Peer ?
- Umsetzung einer kontrollierten Privatautonomie
- Internationales „Crypto-Law“

Nationale Regulierungen für internationale Plattformen können nur die großen Plattformen stemmen. Sie schränken in ihrer Summe die Freiheit massiv ein. Also bitte keine nationalen „Netzwerkdurchsetzungsgesetze“ für die Blockchain.

Die Bundesnetzagentur geht gegen XMPP Softwareanbieter vor. Wollen wir wirklich alles regulieren und überall dort wo es keinen zentralen Player gibt, sehr weitgehende Verbote aussprechen? Ist es ein Grundrecht, unreguliert direkt zu kommunizieren oder zu handeln? Oder hat der Staat die Verpflichtung, alle Geschäfte - auch die direkten - zu kontrollieren?

Es gilt Privatautonomie - aber nicht unbegrenzt. Wir müssen Mindeststandards von Governance für Blockchains und Smart Contracts entwickeln.

Vor allem aber brauchen wir ein internationales „Crypto-Law“ und bitte keinen Flickenteppich sich widersprechender nationaler Regelungen.

Vielen Dank !

Fragen, Diskussion