Smart Contracts

Arbeitskreis Legal Tech – Automatisierung von Verträgen

EDV-Gerichtstag Saarbrücken, 22. 9. 2017

Jörn Erbguth, IT & Law Consultant

joern@erbguth.ch +41 787256027

AXA nutzt Ethereum-Blockchain für Flugversicherung

14. September 2017 | Danny de Boer ETHEREUM

Der französische Versicherungsriese AXA nutzt aktuell die Ethereum-Blockchain, um Fluggästen eine Versicherung anzubieten. Die Blockchain speichert die Daten und wickelt im Falle eines Versicherungsfalles automatisch die Zahlung ab.

Letzte Woche hat die AXA-Versicherung angekündigt, dass sie Flugverspätungsversicherungen anbieten auf Basis von Ethereum Smart Contracts anbieten möchte.
Ich finde das ein sehr schönes Beispiel:

Auf der einen Seite für die technischen Möglichkeiten

Auf der anderen Seite aber auch für den Bereich Blockchain. Da werden Versicherungen angeboten, die niemand braucht – es gibt ja die EU-Fluggastrechte. Zudem muss man darauf vertrauen, dass die Flugverspätungsdaten korrekt eingetragen werden. Die Blockchain nimmt mir also nicht ab, dass ich da auf der anderen Seite einer Partei vertrauen muss. Dafür entlastet mich der Smart Contract von dem nicht wirklich vorhandenen Insolvenzrisiko der Axa-Versicherung.

Da wird also eine Versicherung verkauft, die niemand braucht. Die Technologie bietet zudem eine Absicherung für ein Insolvenzrisiko, welches ich sowieso als vernachlässigbar einstufen würde. Aber Hauptsache wir haben als erstes ein Smart Contract basiertes Produkt auf dem Markt.

https://www.btc-echo.de/axa-nutzt-ethereum-blockchain-fuer-flugversicherung/

Aspekte der Smart Contracts

1. Formulierung der Vertragsbedingungen als Computerprogramm

2. Automatische Vertragsausführung

Smart Contracts haben zwei Aspekte.

Das erste ist die Formulierung des Vertrags in algorithmischer Form. Damit kann der Vertrag mit Hilfe eines Computers eindeutig interpretiert werden.

Der zweite Aspekt ist die Vertragsausführung auf einem automatisierten System – wie z.B. bei einem Verkaufsautomaten.

Erst wenn beides zusammen kommt, möchte ich von einem « Smart Contract » sprechen.

... Zum ersten Aspekt

Formulierung eines Vertrages als Computerprogramm (1)

- ✓ Berechnungen
- ✓ Abläufe
- ✓ Fristen
- ✓ Rechtsfolgen
- ✗ Unbestimmte Rechtsbegriffe (z.B. *Fahrlässigkeit)*

Kann man denn einen Vertrag effektiv als Computerprogramm formulieren?

Berechnungen lassen sich leicht in Algorithmen fassen
Abläufe, **Fristen**, **Rechtsfolgen** können gut programmiert werden
Unbestimmte Rechtsbegriffe wie z.B. *Fahrlässigkeit* müssen jedoch vermieden oder außerhalb des Computerprogramms entschieden werden

... welche Vorteile bietet das nun?

Formulierung eines Vertrages als Computerprogramm (2)

Vorteile

- Einsatz von Software-Entwicklungstools
- Automatisches Evaluieren einer grossen Anzahl von Verträgen
  - Unternehmensübernahmen / Due Diligence
  - Evaluierung der Auswirkungen von Urteilen oder Gesetzesvorhaben
  - Simulation von Handlungsoptionen

Wenn man Vertragsbedingungen als Computer Code festhält, so können Techniken der Softwareentwicklung eingesetzt werden.
Man kann Testfälle definieren, die automatisiert für jede neue Vertragsversion berechnet werden. Damit können unbeabsichtigte Nebenwirkungen von Vertragsänderungen entdeckt werden.

Bei Gesetzesänderungen, Urteilen oder dem Verkauf von Unternehmen müssen häufig die Auswirkungen auf eine Vielzahl auf Verträgen evaluiert werden. Liegen die Verträge als Computer Code vor, so kann diese Analyse automatisiert erfolgen.

Viele dieser Vorteile lassen sich bei herkömmlichen Schriftverträgen auch durch eine nachträgliche Analyse und Strukturierung von herkömmlichen Schriftverträgen erreichen. Die Automatisierung dieser Analyse ist sehr aufwändig.

... Und wie ist das dann rechtlich einzuordnen?

Formulierung eines Vertrages als Computerprogramm (3)

Rechtswirksamkeit ?

- B2B
- B2C
- Formerfordernisse (z.B. Schriftform)

Ist das Computerprogramm ein juristischer Vertrag?
Diese Frage ist so, falsch gestellt. Auch bei der Formulierung in deutscher Sprache ist der juristische Vertrag 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. Die ggf. schriftlich festgehaltenen Vertragsklauseln erleichtern nur den Beweis über das Zustandekommen und die Details des vereinbarten Vertrags.

Also daher anders - kann es eine rechtswirksame Einigung über die im Computerprogramm festgelegten Vertragsbedingungen geben?

B2B insbesondere bei einem konventionellen Vorvertrag eher ja.
B2C eher nein – Ausnahmen sind vorstellbar
Formerfordernisse – wohl ebenfalls nicht

... nun zum zweiten Aspekt

Aspekte der Smart Contracts

1. Formulierung der Vertragsbedingungen als Computerprogramm

2. **Automatische Vertragsausführung**

Die automatische Vertragsausführung

... Automatisierte Vertragsausführung kennen wir aus dem Alltag

Automatische Vertragsausführung

- Jeder Verkaufsautomat führt automatisiert Verträge aus
- Programmierung verborgen
- Verkäufer kann Programm unbemerkt manipulieren
- Keine sichere Protokollierung der Transaktion

Ob iTunes oder ein Verkaufsautomat. Hier werden Verträge automatisiert ausgeführt. Doch auch das allein würde ich nicht « Smart Contract » nennen. Bei einem Verkaufsautomaten ist der Programmcode des Automaten verborgen. Daher ist er sicher nicht geeignet, die Vertragsbedingungen festzulegen.

Ich bin auch z.B. nicht davor gefeilt, dass der Verkäufer die einprogrammierten Preise erhöht, dies aber nicht anzeigt. Ich kann mich nicht einmal darauf verlassen, dass meine Transaktion korrekt protokolliert wird.

Kurz – ich brauche Vertrauen in den Automatenhersteller und den Automatenaufsteller.

... Wie sieht das auf der Blockchain aus?

Smart Contracts auf der Blockchain

- Kleine Programme
- Erhalten Nachrichten
- Wenn die Bedingungen erfüllt sind, werden Transaktionen durchgeführt

Smart Contracts auf der Blockchain scheinen dem Verkaufsautomat zunächst recht ähnlich:

Es sind kleine Programme. Sie erhalten Nachrichten, stellen fest, das ein Vertragsschluss stattgefunden hat und führen abhängig davon die Transaktion nach den intern gespeicherten Regeln aus.

Was bedeutet nun, dass Smart Contracts auf der Blockchain sind?

Smart Contracts – kleine Programme auf der Blockchain

- Nicht jedes Smart Contract Programm auf der Blockchain hat etwas mit juristischen Verträgen zu tun
- Der Autor eines Smart Contract Programms ist häufig nicht Vertragspartner
- Ein Smart Contract Programm kann viele Verträge zwischen zwei oder mehr Parteien vermitteln

Dass jedes auf der Ethereum-Blockchain ausführbare Programm „Smart Contract“ genannt wird, verwirrt manchmal:

Viele dieser Programme haben keinen Bezug zu juristischen Verträgen

Ein Smart Contract Programm kann viele juristische Verträge vermitteln und abwickeln. Es gibt also nicht etwa ein Smart Contract pro juristischem Vertrag.

... Was sind nun die Vorteile, dass die Smart Contracts auf der Blockchain laufen?

Smart Contracts – warum auf der Blockchain?

- Auf der Blockchain gespeichert
- Auf der Blockchain ausgeführt
- Transparent
- Manuell nicht beeinflussbar

Dadurch dass die Smart Contracts auf der Blockchain gespeichert sind, sind sie transparent - jeder kann den Code einsehen.
Sie werden aber auch auf der Blockchain ausgeführt. Das bedeutet, dass damit sicher gestellt ist, dass auch nur diese Programmversion ausgeführt wird.
Jeder Knoten führt den Smart Contract separat aus und vergleicht das eigene Ergebnis mit dem Ergebnis im übermittelten Block

Im Vergleich mit einem Verkaufsautomaten hat dies den Vorteil, dass wir sicher gehen können, dass der Automat genau das tut, was er soll. 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.

... Daneben gibt es noch einen wichtigen weiteren Vorteil

Smart Contracts und Krypto-Währungen

Smart Contracts können

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

Dies ist der Zugriff von Smart Contracts auf Krypto-Währungen.
Smart Contracts können Krypto-Geld (ihrer Blockchain) erhalten, verwalten und transferieren.
Damit kann eine wichtige Pflicht in juristischen Verträgen automatisiert ausgeführt werden.
Smart Contracts können z.B. als Treuhänder agieren, der das Geld nur nach den transparent und unveränderbar festgelegten Regeln weitergibt.

... Dies sehen wir uns in einem Beispiel an

Smart Contract – Beispiel

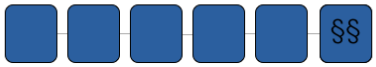
Blockchain basierte Handelsplattform

- Transparente Regeln
- Komplett automatisiert
- Ohne manuelle Eingriffsmöglichkeit

Zur Illustration der Funktionsweise eines „Smart Contracts“ möchte ich das Beispiel einer Blockchain basierten Handelsplattform vorstellen.
Sie ist komplett automatisiert und funktioniert nach transparenten Regeln.

Smart Contract - Beispiel Handelsplattform

Smart Contract
Entwickler



Blockchain

Verkäufer

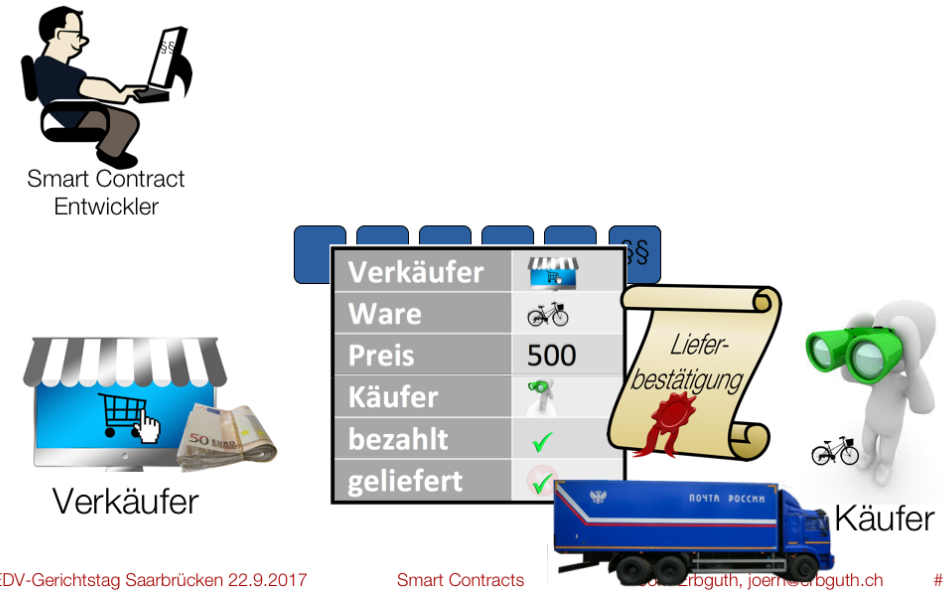
Käufer

Ein Smart Contract Entwickler schreibt ein Smart Contract Computerprogramm zur Abwicklung von Verkäufen auf einer Verkaufsplattform.

Smart Contract - Beispiel Handelsplattform

Der Verkäufer schickt ein Angebot an den Smart Contract. Ein Interessent findet dieses Angebot und sendet eine Annahmeerklärung. Zusammen mit der Annahmeerklärung sendet er den Kaufpreis. Der Kaufpreis wird dann vom Smart Contract bis zur Lieferung der Ware treuhänderisch verwahrt.

Smart Contract - Beispiel Handelsplattform



Der Verkäufer sieht die Annahme seines Angebots und versendet die Ware. Sobald die Lieferung erfolgt und vom Spediteur auf der Blockchain bestätigt wurde, transferiert der Smart Contract automatisch den Kaufpreis an den Verkäufer. Sollte innerhalb einer festgelegten Frist keine Lieferung erfolgen wird der Kaufpreis an den Käufer zurück transferiert.

Hier ist die russische Post als Spediteur aufgeführt, da sie angekündigt hat, ihre Sendungsverfolgung auf die Blockchain zu stellen.

Smart Contract - Beispiel Code

```
pragma solidity ^0.4.2;

contract Handel {
    string public Ware;
    uint public Preis;
    address public Verkaeufer;
    address public Kaeufer;
    bool public bezahlt;
    bool public geliefert;
    bool public abgewickelt;
    address constant post=0x123456789abcdef;

function Angebot(string iWare, uint iPreis)
{
    Verkaeufer=msg.sender;
    Ware=iWare;
    Preis=iPreis;
}

function Annahme() payable
{
    if(msg.value>=Preis)
    {
        Kaeufer=msg.sender;
        bezahlt=true;
    }
}

function Lieferung()
{
    if(msg.sender==post && geliefert==false)
    {
        geliefert=true;
        abgewickelt=Verkaeufer.send(Preis);
    }
}
}
```

Der Smart Contract ist recht übersichtlich. Selbst ohne Programmierkenntnisse sieht man am Anfang die Deklaration der Variablen und danach die 3 Funktionen für den Empfang der Nachrichten über Angebot, Annahme und Lieferbestätigung.

… wo können solche Smart Contracts eingesetzt werden?

Auswirkungen (1)

Disintermediation

Smart Contracts können die Intermediäre der Share Economy überflüssig machen – so zumindest die positiven Zukunftsvisionen.

… viele Startups stehen dazu in den Startlöchern

Auswirkungen (2)

Neue direkte Geschäfte

Um nur ein paar zu nennen:

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

... Doch auch über den Bereich des eGovernment gibt es Anwendungen

Auswirkungen (3)

eGovernment

- Grundbücher

Grundbücher - Projekte gibt es in Schweden, Ghana, Georgien, Honduras – wobei Schweden bereits ein Grundbuch im Echtbetrieb auf einer Blockchain betrieben wird.

Quelle: https://www.btc-echo.de/schweden-geht-weitere-schritte-richtung-blockchain-grundbucheintraege/

Auswirkungen (3)

eGovernment

- Grundbücher
- Handelsregister

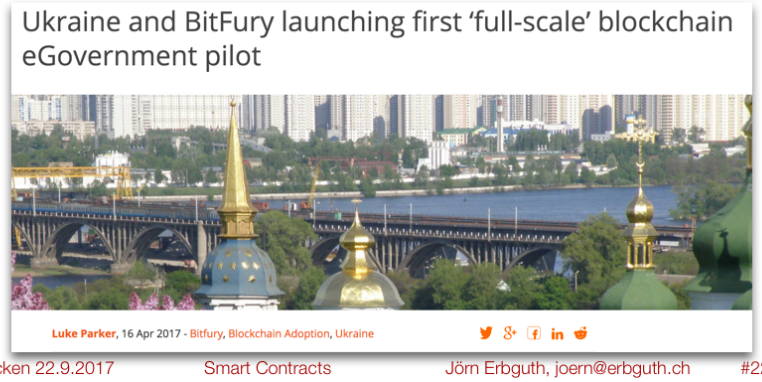
Kanton Genf hat ein Projekt gestartet das Handelsregister auf die Blockchain zu bringen

Quelle: https://www.letemps.ch/economie/2017/08/24/geneve-reve-convertir-suisse-blockchain

Auswirkungen (3)

eGovernment

- Grundbücher
- Handelsregister
- umfassend



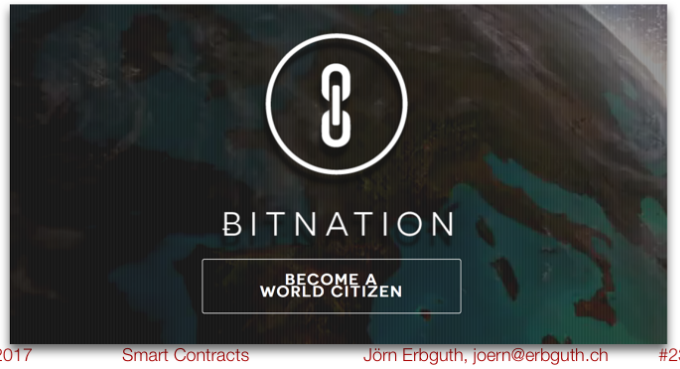
Die Ukraine hat eine umfassende Nutzung der Blockchain für Public Services, Social Security, Public Health und Energy Sector angekündigt

Quelle: https://bravenewcoin.com/news/ukraine-and-bitfury-launching-first-full-scale-blockchain-egovernment-pilot/

Auswirkungen (3)

eGovernment

- Grundbücher
- Handelsregister
- umfassend
- virtueller Staat



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

... Was bedeutet das?

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 viele Blockchain wie eine Datenbank einsetzen. Für tatsächlich autonom als Smart Contract auf einer öffentlichen Blockchain laufenden Plattformen gilt:

Regulierung ist schwer durchsetzbar.
Das macht 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. Mechanismen zur Konfliktlösung sind nur selten eingebaut.

Die Daten auf der Blockchain sind - wenn sie nicht verschlüsselt sind - immer öffentlich auslesbar und können nicht gelöscht oder verändert werden. So ist z.B. das Recht auf Vergessen oder auf Berichtigung nicht durchsetzbar.

... Dies führt zu verschiedenen Reaktionen

Reaktionen und Konsequenzen

- Umsetzung einer kontrollierten Privatautonomie
- Sandbox-Ausnahmen für Startups mit begrenztem Finanzvolumen
- Nationale Regulierungen für internationale Plattformen ?
- Internationales „Crypto-Law“

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

Ein Weg ist die Einführung der „Sandbox“ im Schweizer Recht. Damit werden kleine Startups nicht gleich mit der vollen Last der Regulierung konfrontiert.

Smart Contracts auf der Blockchain kennen aber keine Grenzen. Selbst an sich positive nationale Regulierungen können da in der Summe schnell zur Überregulierung führen.

Wir brauchen daher vor allem ein internationales „Crypto-Law“ welches Mindestanforderungen aber auch ein Minimum an garantierten Freiheiten gewährt. Wir sollten damit einen Flickenteppich sich widersprechender nationaler Regelungen vermeiden.

Vielen Dank für Ihre Aufmerksamkeit!

Fragen, Diskussion