Smart Contracts auf der Blockchain

Weblaw Brown Bag 16. 8. 2017

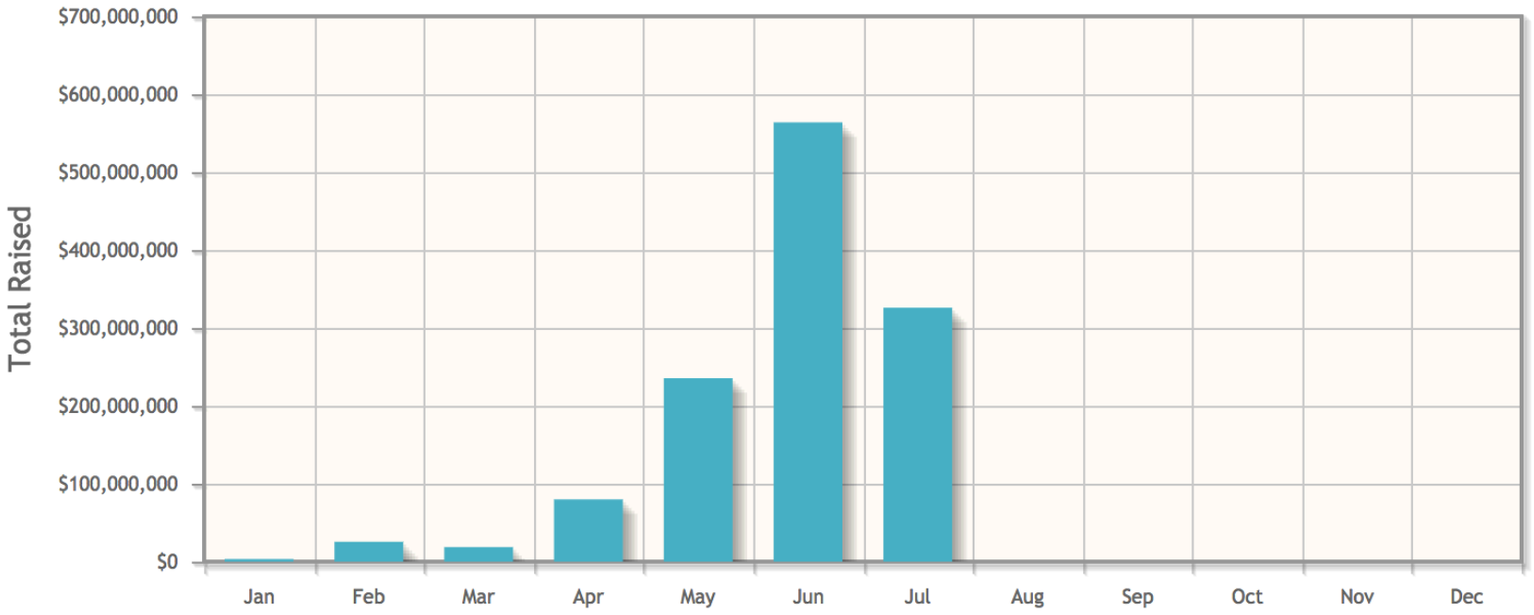
Jörn Erbguth, IT & Law Consultant

joern@erbguth.ch +41 787256027

Boom der Initial Coin Offerings (ICO)

Cryptocurrency ICO Stats 2017

Year: 2017



Totals raised are grouped by the ICO closing date and are valued using BTC exchange rate at that time. Data correct on 18th July 2017 14:00 UTC

Total Raised: $1,252,676,352

Total Number of ICOs: 92

Top Ten ICOs of 2017

Position	Project	Total Raised
1	Tezos	$232,319,985
2	Bancor	$153,000,000
3	Status	$90,000,000
4	TenX	$64,000,000
5	MobileGO	$53,069,235
6	Sonm	$42,000,000
7	Aeternity	$36,960,594
8	Basic Attention Token	$35,000,000
9	Civic	$33,000,000
10	Polybius	$31,645,088

Blockchain

Daimler setzt auf Bitcoin-Technologie und startet 100-Millionen-Euro-Projekt

Christoph Damm am 30. Juni 2017

Einblick. Die Blockchain-Technologie taugt nicht nur beim Handel von Bitcoins. Auch der Autokonzern Daimler will 100 Millionen Euro via Blockchain von Anlegern einsammeln.

GRÜNDERSZENE

Aspekte der Smart Contracts

1. Formulierung der Vertragsbedingungen als Computerprogramm

```
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=0x1234567

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

function Annahme() payable
{
    if(msg.value>=Preis)
    {
```

2. Automatische Vertragsausführung

Formulierung eines Vertrages als Computerprogramm (1)

- ✔ Berechnungen
- ✔ Abläufe
- ✔ Fristen
- ✔ Rechtsfolgen
- ✖ Unbestimmte Rechtsbegriffe (z.B. *Fahrlässigkeit)*

```
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=0x1234567

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

function Annahme() payable
{
    if(msg.value>=Preis)
```

Formulierung eines Vertrages als Computerprogramm (2)

```
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=0x1234567

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

function Annahme() payable
{
    if(msg.value>=Preis)
    {
```

Rechtswirksamkeit ?

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

Formulierung eines Vertrages als Computerprogramm (3)

```
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=0x1234567

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

function Annahme() payable
{
    if(msg.value>=Preis)
    {
```

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

Aspekte der Smart Contracts

1. Formulierung der Vertragsbedingungen als Computerprogramm

```
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=0x1234567

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

function Annahme() payable
{
    if(msg.value>=Preis)
```

2. Automatische Vertragsausführung

Automatische Vertragsausführung

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

Smart Contracts auf der Blockchain

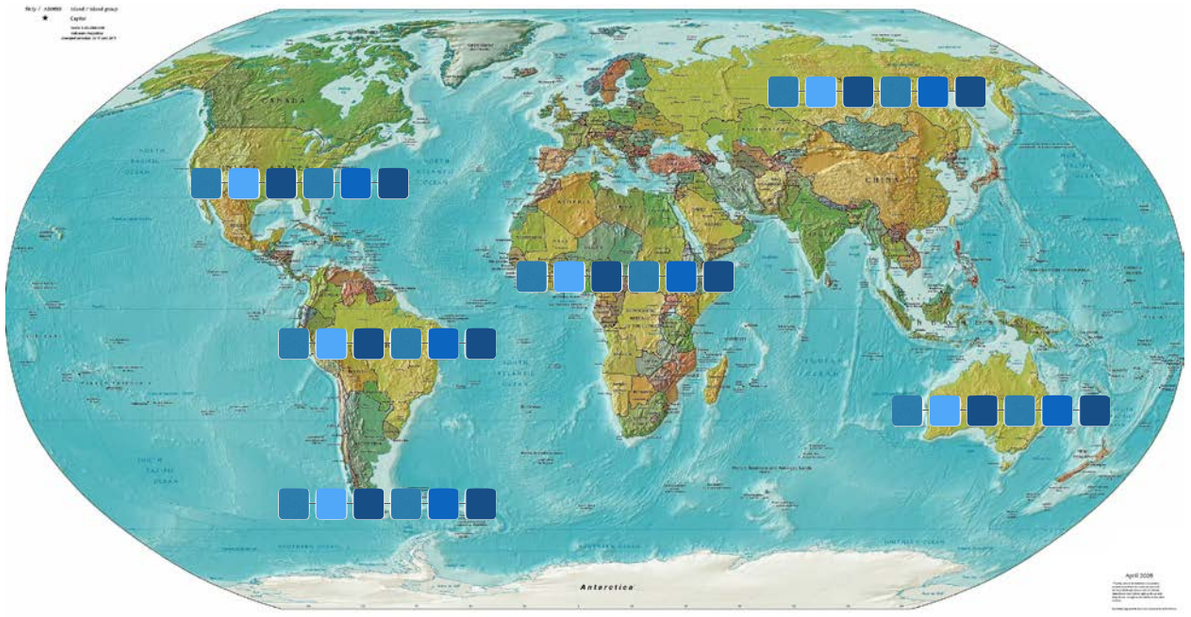
- Kleine Programme
- Erhalten Nachrichten
- Wenn die Bedingungen erfüllt sind, werden Transaktionen durchgeführt

Die Blockchain

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

Die Blockchain

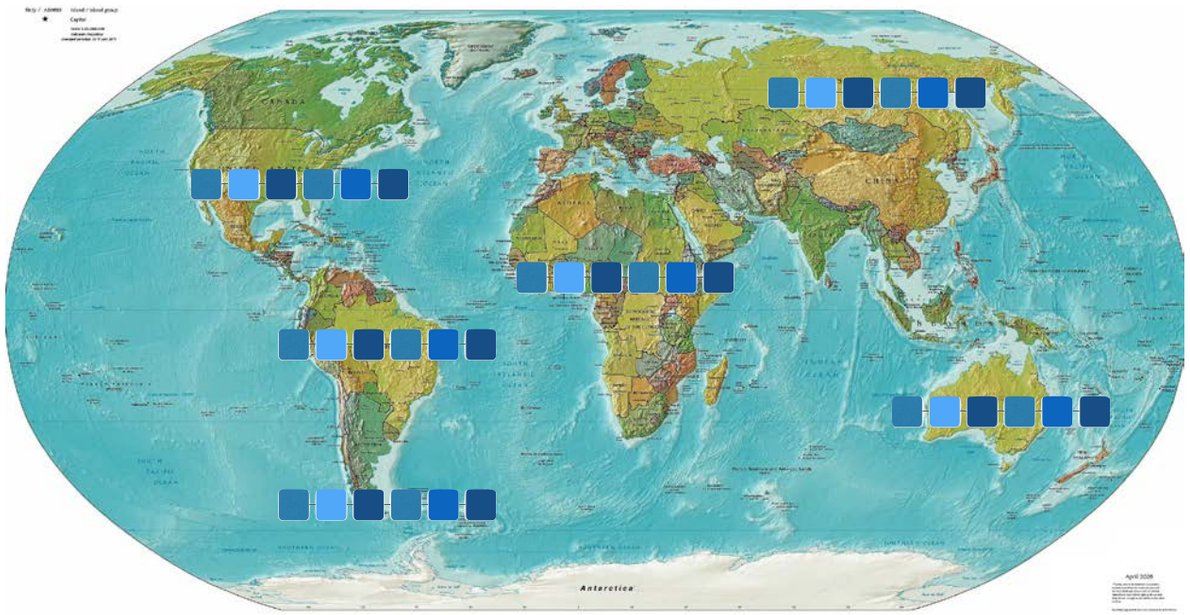
- Speicherung von Daten
- Unveränderlich
- Weltweit verteilt



  - Dezentral
    Jeder Knoten hat vollständige Kopie
    Spezielles Abstimmungsverfahren

Die Blockchain

- Speicherung von Daten
- Unveränderlich
- Weltweit verteilt



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

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

Smart Contracts – warum auf der Blockchain?

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

Smart Contracts und Krypto-Währungen

Smart Contracts können

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

Smart Contract – Beispiel

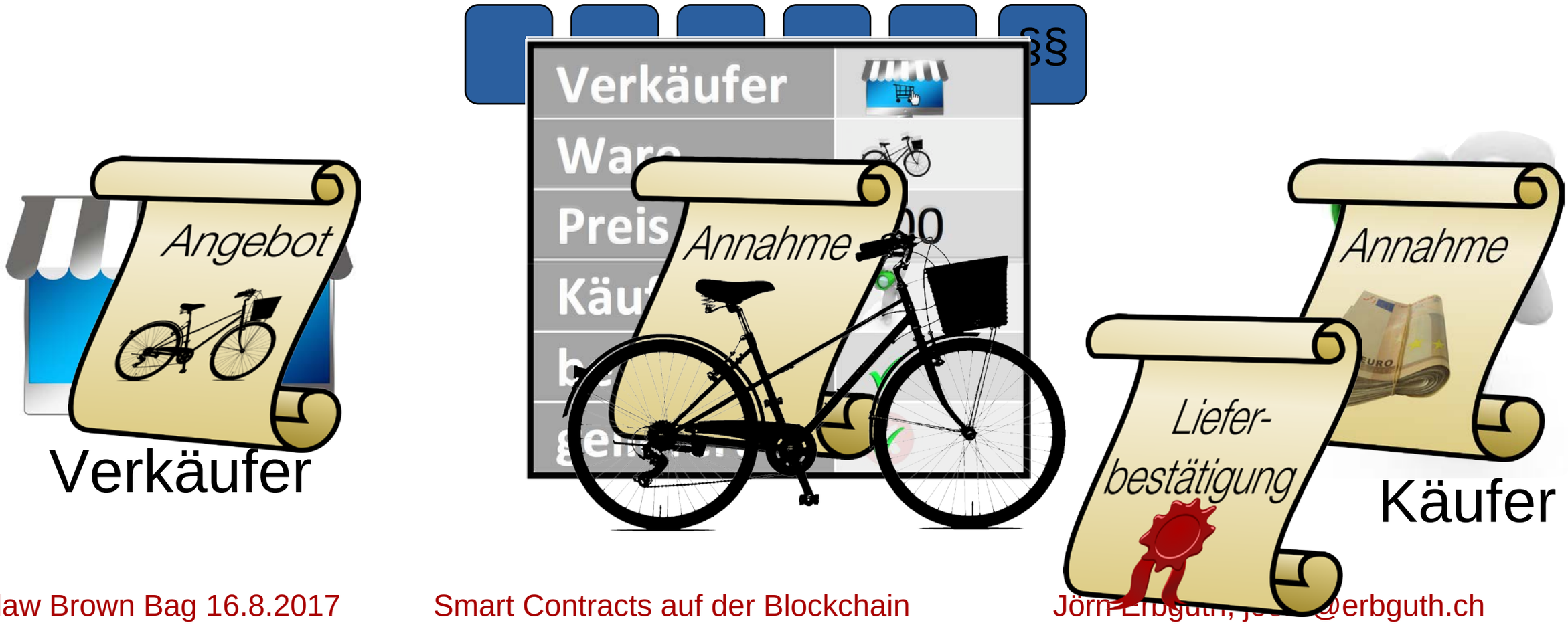
Blockchain basierte Handelsplattform

- Transparente Regeln
- Komplett automatisiert
- Ohne manuelle Eingriffsmöglichkeit

Smart Contract - Beispiel Handelsplattform

§§

Smart Contract
Entwickler



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 abgewickelt;
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         abgewickelt=Verkaeufer.send(Preis);
35     }
36 }
37 }
```

Auswirkungen (1)

Disintermediation

airbnb

iTunes

UBER

ebay

Google play

Booking.com

Auswirkungen (2)

Neue direkte Geschäfte

DECENT

golem WORLDWIDE SUPERCOMPUTER

wagerr

Binded

BLOCKTIX

matchpool

AdEx

bitJob

BidLend

True Flip
First Already Working Blockchain lottery

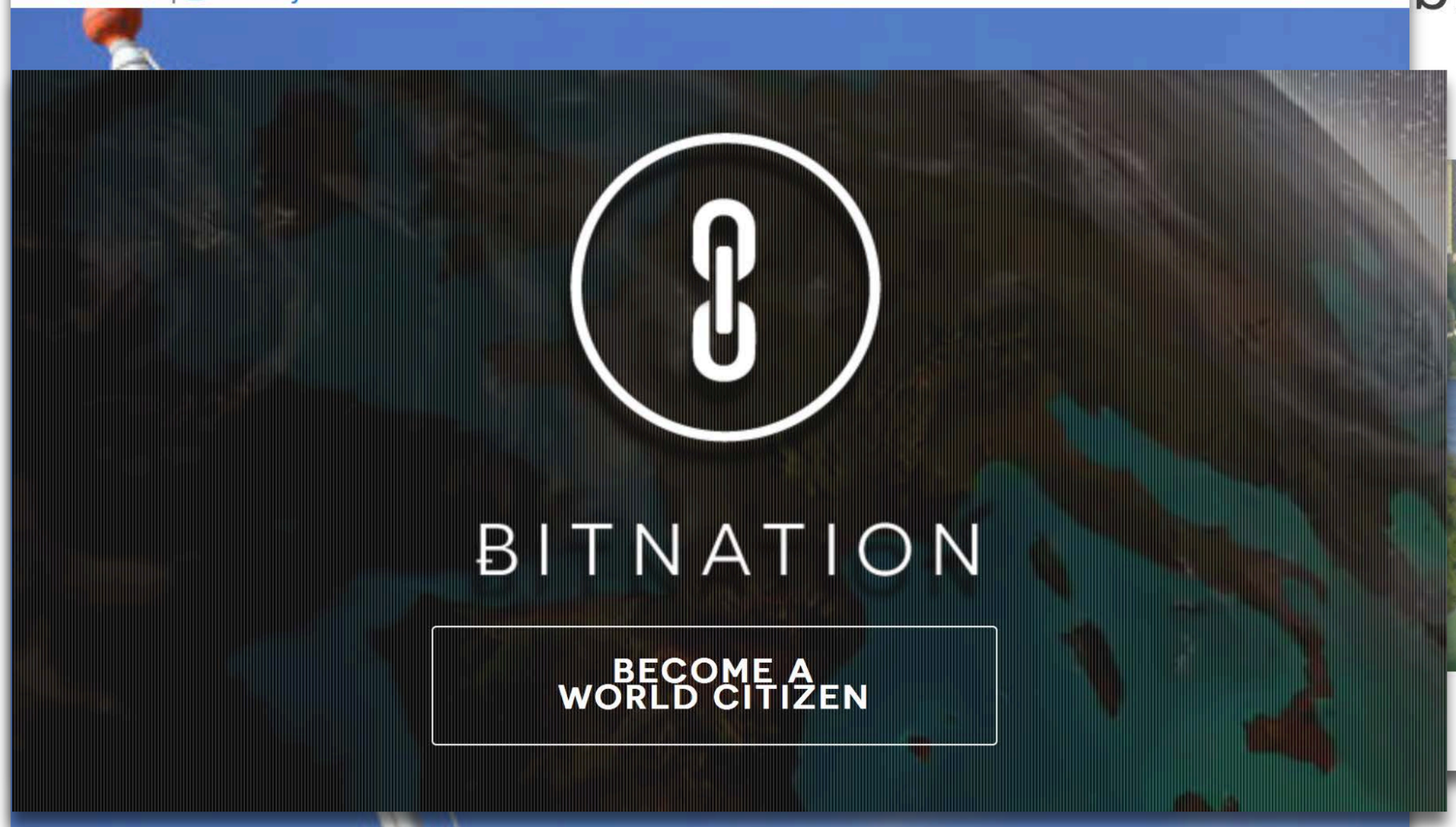
Auswirkungen (3)

eGovernment

- Grundbücher

Schweden geht weitere Schritte in Richtung Blockchain-Grundbucheinträge

31. März 2017| Alina Ley



blockchain

Auswirkungen (4)

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

Reaktionen und Konsequenzen

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

Vielen Dank für Ihre Aufmerksamkeit!

Fragen, Diskussion