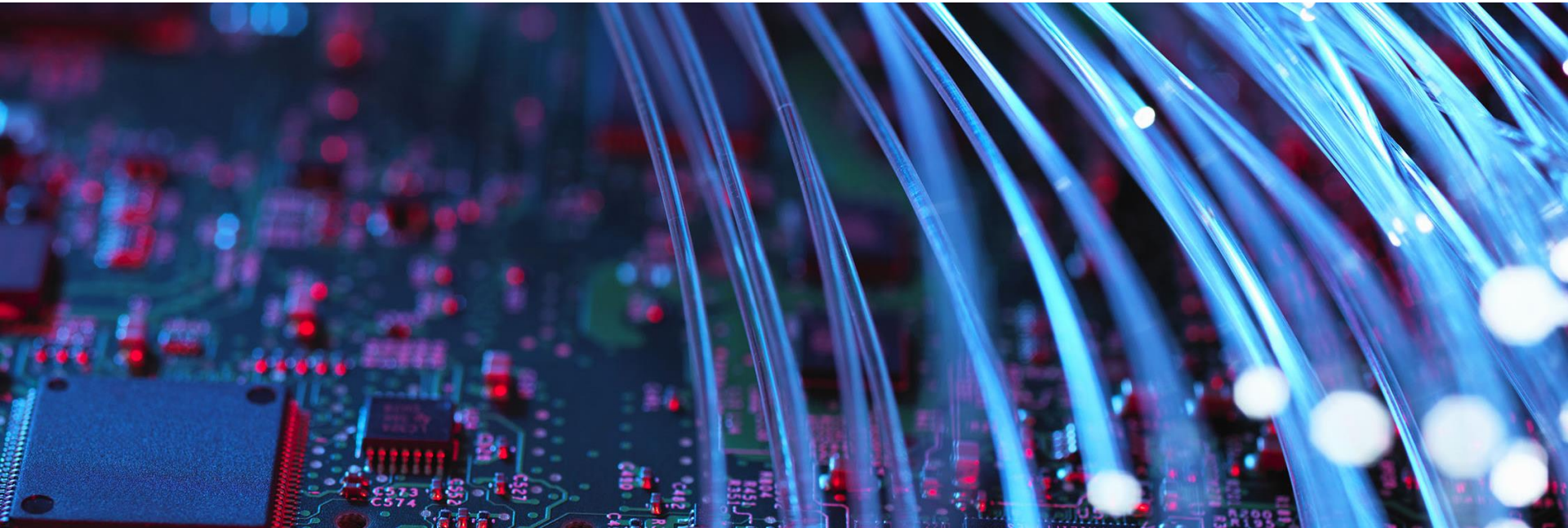
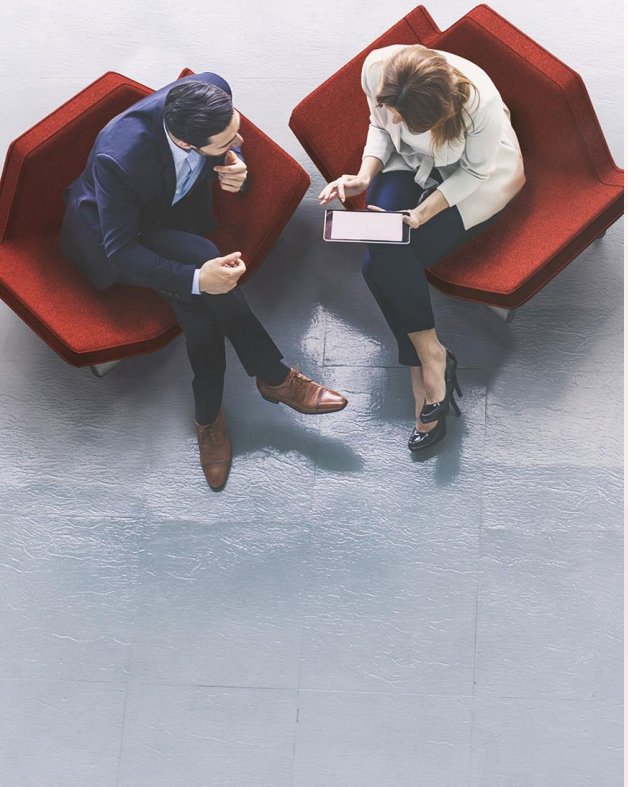
Baker McKenzie.

Blockchain & Smart Contracts

RA Dr. Lukas Feiler, SSCP, CIPP/E

LL.M. Informations- und Medienrecht, 16. Dezember 2017





Themen

1 Blockchain

- Technische Grundlagen
- Anwendungsgebiete

2 Bitcoin und andere Krypto-“Währungen”

- Grundlagen & steuerrechtliche Behandlung
- Unterschiede zu staatlichen Währungen

3 Initial Coin Offerings (ICOs)

- ICOs als neues Phänomen
- Rechtliche Einordnung

4 Smart Contracts

- Verhältnis zwischen Recht & Smart Contracts an eines Beispiels
- Rechtliche Grenzen der Automatisierung

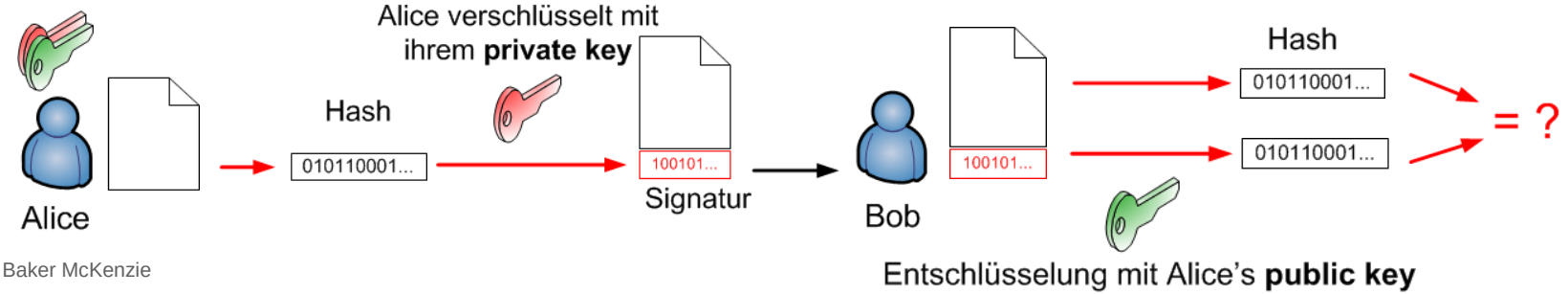
1 Blockchain – Technische Grundlagen

Was ist eine Blockchain? – 1 von 3

- kontinuierlich erweiterbare Liste von Daten-Blöcken; jeder Block enthält
  - Zeitstempel
  - Transaktionsdaten
  - kryptographischen Fingerabdruck („Hash“) des vorhergehenden Blocks
- Krypto-Basics: Hashing
  - deterministische Einwegfunktion
  - Kollisionsresistenz
  - zB SHA-256

Was ist eine Blockchain? – 2 von 3

- Dezentralität – jeder Teilnehmer des Netzwerks
  - speichert die gesamte Blockchain (bei Bitcoin derzeit ca. 135 GB)
  - berechnet Teile neuer Transaktionen – verteiltes Vertrauen
  - gewährleistet Sicherheit mittels asymmetrischer Kryptographie
  - könnte die gesamte Transaktionshistorie nachrechnen
  - bleibt grundsätzlich pseudonym – Vertrauen in das System, nicht die Person
- Krypto-Basics: asymmetrische Kryptographie



Was ist eine Blockchain? – 3 von 3

- Sicherheitseigenschaften der Blockchain?
  - Integrität?
  - Authentifizierung?
  - Non-Repudiation (Nichtabstreitbarkeit)?
  - Vertraulichkeit?
- Dezentralisiertes Vertrauen statt zentrale Institutionen – Anwendungsgebiete und Risiken? Historische Referenzmodelle?

Die Blockchain aus datenschutzrechtlicher Sicht

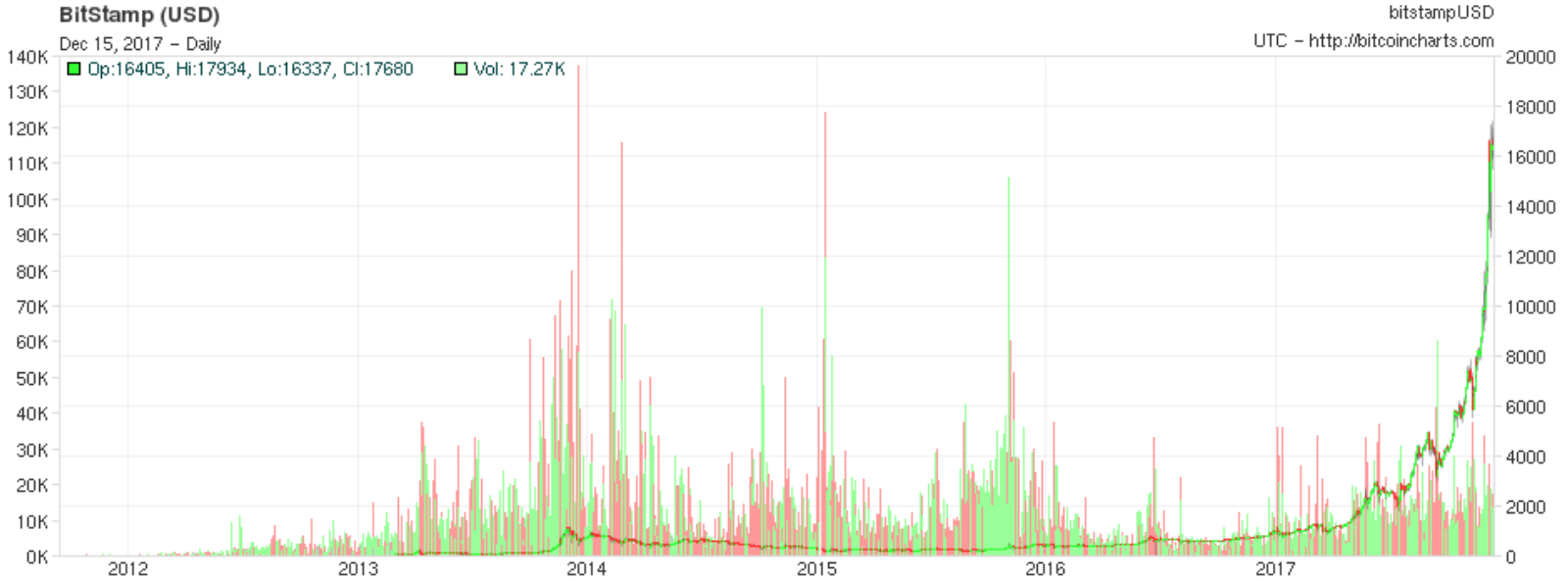
- Grundlegende Eigenschaften der Blockchain
  - Nutzung erfolgt pseudonym
  - alle Transaktion werden protokolliert
  - mit Offenlegung der Verknüpfung zwischen Pseudonym und Nutzer-Identität werden alle vergangenen Transaktionen rückwirkend zuordenbar
- Handelt es sich um personenbezogene Daten iSd DSGVO?
- Wer ist Verantwortlicher, wer ist Betroffener?
- Was ist die Rechtsgrundlage der Datenverarbeitung?

2 Bitcoin und andere Krypto-“Währungen”

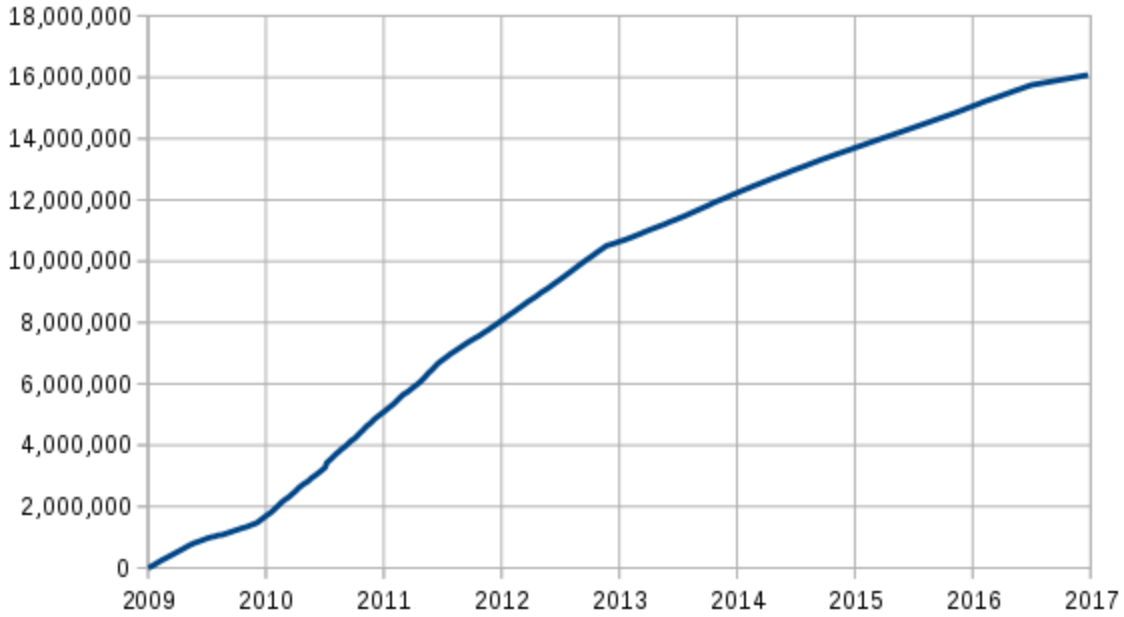
Bitcoin – Grundlagen

- Blockchain-basierte Krypto-“Währung“
- Entwickelt von „Satoshi Nakamoto“; Open Source Software
  - User: Jeder User hat ein Schlüsselpaar; er signiert alle seine Transaktionen mit seinem Private Key
  - Bitcoin: entspricht einem Schlüsselpaar; nur wer Private Key hat, kann Bitcoin ausgeben
  - Wallet: Speichert Schlüsselpaare der Bitcoins eines bestimmten Users → Sicherheit?
  - Mining: Wer hilft Transaktionen zu berechnen, erhält Bitcoins; Komplexität steigt
  - Künstliche Verknappung:
    - Belohnung für Mining wird immer geringer, weshalb immer weniger Bitcoins hinzukommen
    - Ab 21 Millionen Bitcoins: Keine Belohnung mehr für Berechnung von Transaktionen
  - Exchanges: “Wechselstuben”, um Bitcoins in staatliche Währungen zu wechseln

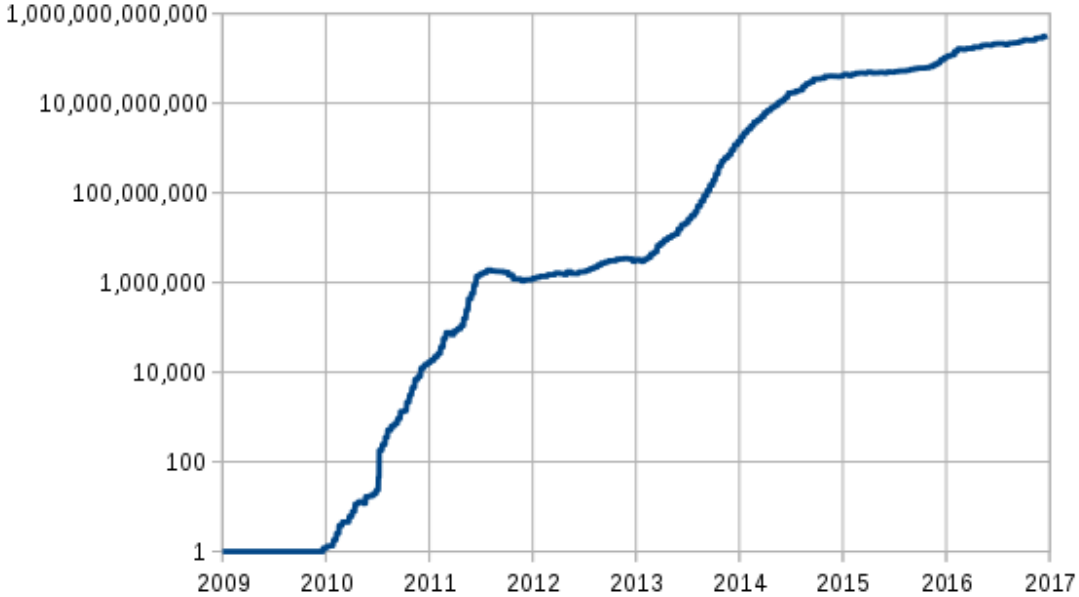
Bitcoin in Zahlen – Wechselkurs BTC/US$



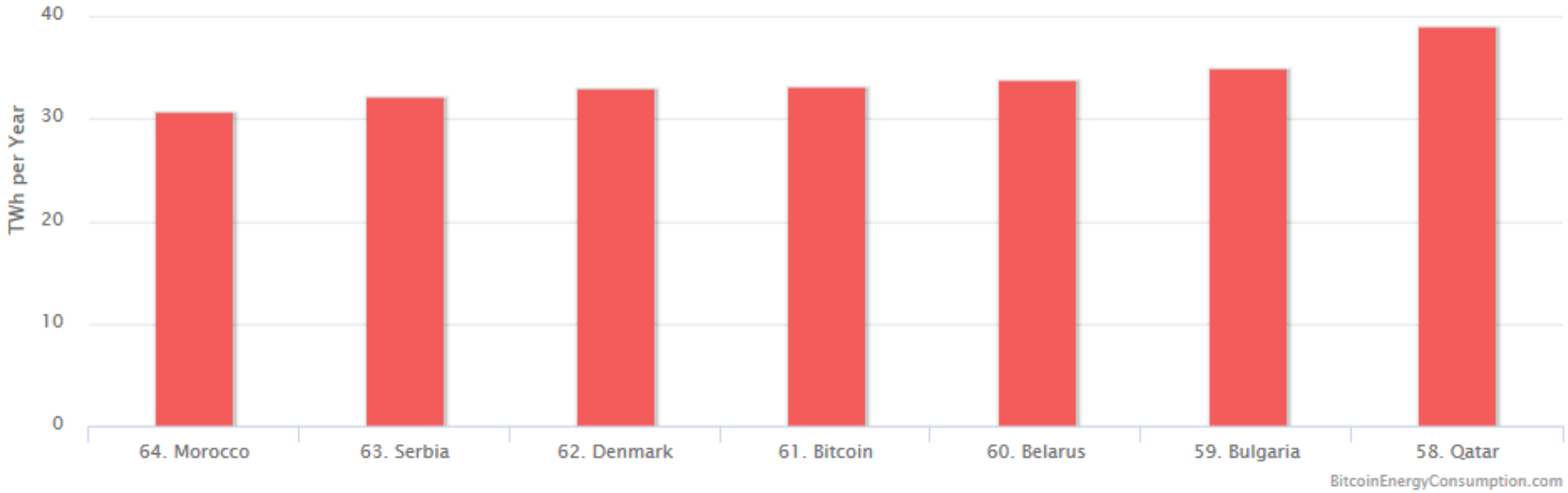
Bitcoin in Zahlen – Anzahl der Bitcoins



Bitcoin in Zahlen – Mining Difficulty



Bitcoin in Zahlen – Energieverbrauch für Mining



Bitcoin – Steuerrechtliche & regulatorische Behandlung

- Umsatzsteuer
  - Umtausch von Bitcoin in staatliche Währung steuerfrei (EuGH 22.10.2015, C-264/14 – *Hedqvist*)
- Einkommensteuer
  - im privaten Bereich: Veräußerungsgewinne steuerpflichtig, wenn innerhalb 1 Jahres veräußert (Spekulationsfrist)
  - im gewerblichen Bereich: Veräußerungsgewinne steuerpflichtig (Einkünfte aus Gewerbebetrieb)
- Regulatorische Einordnung
  - E-Geld iSd E-Geld-Gesetzes? → Konzessionspflicht des Emittenten (§ 3 Abs 1)?
  - „elektronisch gespeicherter monetärer Wert in Form einer Forderung gegenüber dem E-Geld-Emittenten […]“? (§ 1 Abs 1 E-Geldgesetz)

Kryptowährung vs. klassische Währungen

	Kryptowährung (zB Bitcoin)	Klassische Währungen
Währungspolitik	nein	ja
Inhärenter Wert	nein	ja (Annahmepflicht)
Anonymität	nein	tw
Intermediäre	grds nein	grds ja
Vertrauen in	Technik	Institutionen

3 Initial Coin Offerings (ICOs)

Initial Coin Offerings – Ein neues Phänomen

- „Moderne“ Form der Kapitalbeschaffung für Startups
  - Startup gibt eine eigene, selbst erschaffene virtuelle „Währung“ aus
  - Startup erhält Zug um Zug von Interessenten etablierte Krypto-Währungen (häufig Bitcoin oder Ether)
  - Motivation der ICO-Interessenten
    - Hoffnung, dass sich neue Krypto-Währung etabliert und an Wert zunimmt
    - Erwerb eines Rechts gegenüber Startup (Anteil an zukünftigen wirtschaftlichen Erlös, „Unternehmensanteile“, …)

Initial Coin Offerings – Rechtliche Einordnung

- Ausgebendes Unternehmen als konzessionspflichtiger E-Geld-Emittent?
  - E-Geld bezeichnet (§ 1 Abs 1 E-GeldG)
    - jeden elektronisch gespeicherten monetären Wert in Form einer Forderung gegenüber dem E-Geld-Emittenten
    - der gegen Zahlung eines Geldbetrags ausgestellt wird
    - um damit Zahlungsvorgänge […] durchzuführen
    - und der auch von anderen […] Personen als dem E-Geld-Emittenten angenommen wird.
- Konzessionspflicht nach BWG?
  - Einlagengeschäft (Entgegennahme Fremder Gelder; § 1 Abs 1 Z 1 BWG)?
  - Ausgabe von Zahlungsmittel (§ 1 Abs 1 Z 6 BWG) – Anerkennung durch größeren Kreis von Dienstleistern?
- FMA: „ICOs unterliegen zumeist keiner Regulierung und keiner Aufsicht“

Initial Coin Offerings – Eine Gute Idee?

- Zusätzliche Risiken aus Sicht des Ausgebenden Unternehmens?
  - Betrug (§ 146 f StGB)
  - Geldwäscherei (§ 165 StGB)
  - Irreführende Geschäftspraktik (§ 2 UWG)

4 Smart Contracts

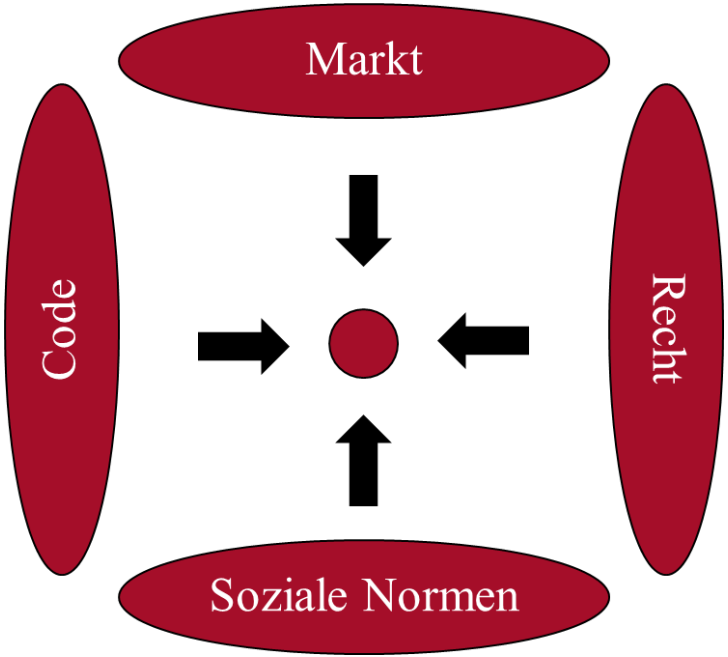
Smart Contracts – Ein Annäherungsversuch

- Was sind Smart Contracts?

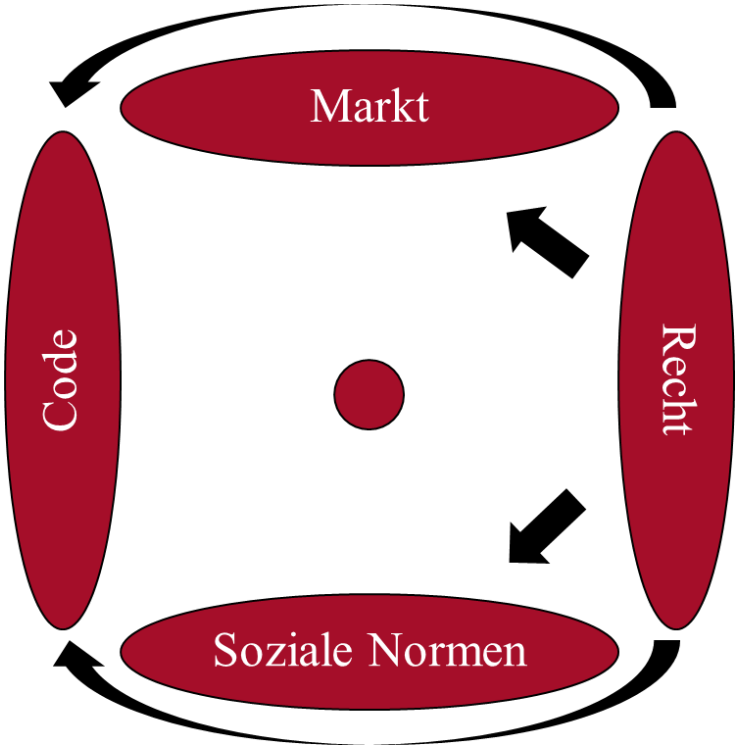
  Nick Szabo (1997): *Smart contracts go beyond the vending machine in proposing to embed contracts in all sorts of property that is valuable and controlled by digital means.*

- Implementierung auf der Blockchain
  - In Code implementierter Contract wird auf der Blockchain ausgeführt
  - grds kein Vertrauen gegenüber Vertragspartner erforderlich
  - automatische Durchsetzung
- Anwendungsfälle?

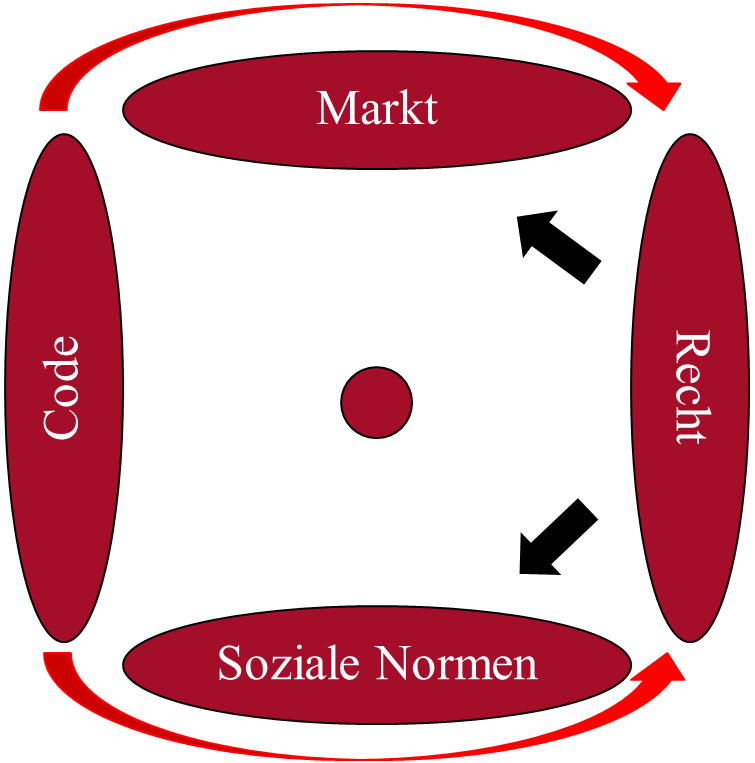
Smart Contracts – Code is Law? – 1 von 3



Smart Contracts – Code is Law? – 2 von 3



Smart Contracts – Code is Law? – 3 von 3



Verhältnis zwischen Recht & Smart Contracts?

- Keine Anwälte und keine Richter nötig?
- Beispiel: ein Smart Contract zur Vermietung eines Selbstfahrenden Autos
- Was ist Vertragsinhalt?
  - Wenn Smart Contract: Smart Contract muss sich am Gesetz messen lassen
    - Auslegungsregeln (§ 914 f ABGB) und grenzen der Sittenwidrigkeit
    - AGB-Kontrolle (§§ 864a, 879 Abs 3 ABGB, § 6 KSchG)
  - Separate Vereinbarung: Smart Contract als Ausführungsinstrument → muss sich am Vertrag messen lassen
    - Leistungsstörungsrecht

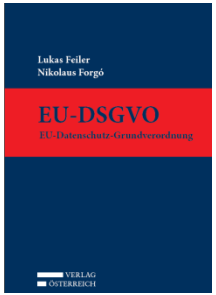
Grenzen der Automatisierung – Besitz- und Eigentumsschutz

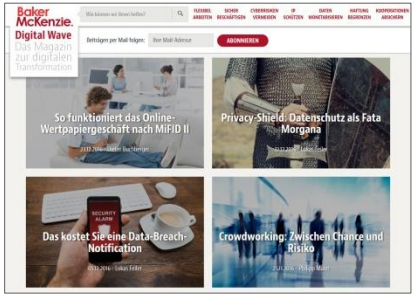
- Durchsetzung vertraglicher Rechte an Smart Property zB durch
  - Einstellung des Betriebs bei Verzug mit einer Leasing-Rate oder Vertragsverletzung
  - „Rückführung“ des gemieteten/geleasten Smart Property bei Vertragsverletzung/Kündigung
  - Löschung digitaler Waren / Deaktivierung der Software bei Lizenzablauf
- Besitz- und Eigentumsschutz
  - § 126a StGB – Datenbeschädigung: „wer […] Daten, über die er nicht oder nicht allein verfügen darf, [unbrauchbar macht]“
  - § 126b StGB – Störung der Funktionsfähigkeit eines Computersystems: „wer die Funktionsfähigkeit eines Computersystems, über das er nicht oder nicht allein verfügen darf, dadurch schwer stört, dass er Daten eingibt“
  - Schutz vor Besitzstörung (Selbsthilfemaßnahme nur wenn staatliche Hilfe zu späte käme & gelindestes Mittel; zB LG St. Pölten 18.5.1998, 7 R 75/98d)

Grenzen der Automatisierung - DSGVO

- Art 22 DSGVO: Vollautomatisierte Einzelentscheidungen mit rechtlichen Folgen oder ähnlich schweren Beeinträchtigungen nur zulässig, wenn
  - gesonderte Rechtsgrundlage
    - ausdrückliche Einwilligung oder
    - für Abschluss oder Erfüllung eines Vertrags zwischen Betroffenem und Verantwortlichen erforderlich
  - Recht des Betroffenen auf
    - Erwirkung des Eingreifens einer Person seitens des Verantwortlichen,
    - auf Darlegung des eigenen Standpunkts und
    - auf Anfechtung der Entscheidung
  - Vorab: Information über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen der Entscheidung

Baker McKenzie.





Dr. Lukas Feiler, SSCP CIPP/E
Senior Associate
Leiter des Teams für IT-Recht in Wien

Schottenring 25
1010 Vienna

T: +43 1 24 250
lukas.feiler@bakermckenzie.com

Lukas Feiler ist Co-Autor des eines Kommentars zur Datenschutz-Grundverordnung und des ersten Praktiker-Buches zur DSGVO sowie Herausgeber des Gesetzbuch Datenschutzrecht. Er begleitet Unternehmen auf www.digitalwave.at bei der digitalen Transformation.

www.bakermckenzie.com