Bird & Bird & Blockchain vs. DSGVO

Blockchain/DLT-Technologien im Konflikt mit der DSGVO ?

Agenda

1) Einführung: Blockchain /DLT
2) Anwendbarkeit der DSGVO
3) Einordnung der Netzwerkteilnehmer
4) Datenschutzgrundsätze
5) Betroffenenrechte
6) Datenschutz-Folgenabschätzung
7) Chancen & Risiken
8) Fazit

Einführung

“The biggest opportunity set we can think of over the next decade.”

— Bob Greifeld, former CEO
NASDAQ

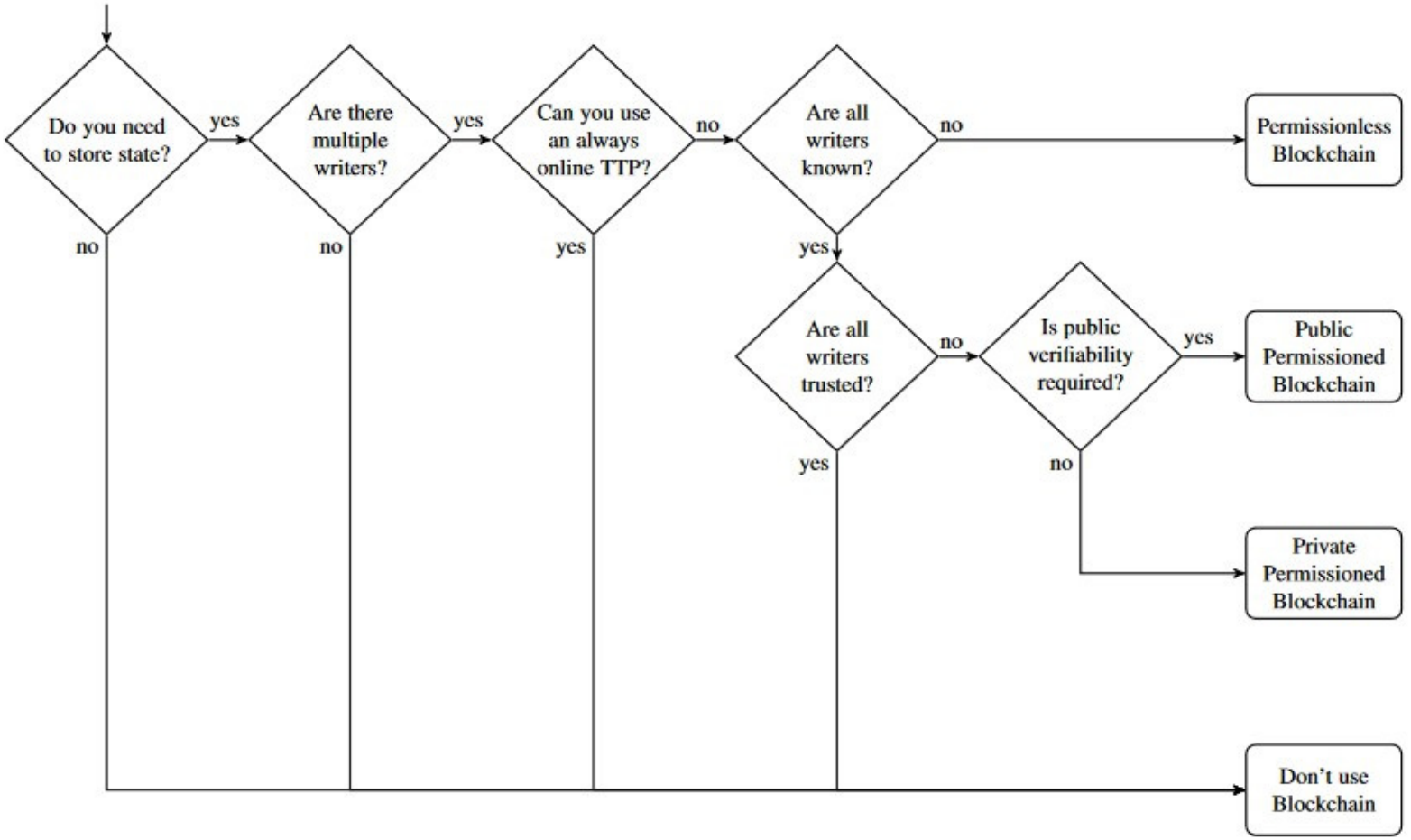
“Stay away from it. It’s a mirage, basically. In terms of cryptocurrencies, generally, I can say almost with certainty that they will come to a bad ending."

— Warren Buffet

Brauche ich eine Blockchain?

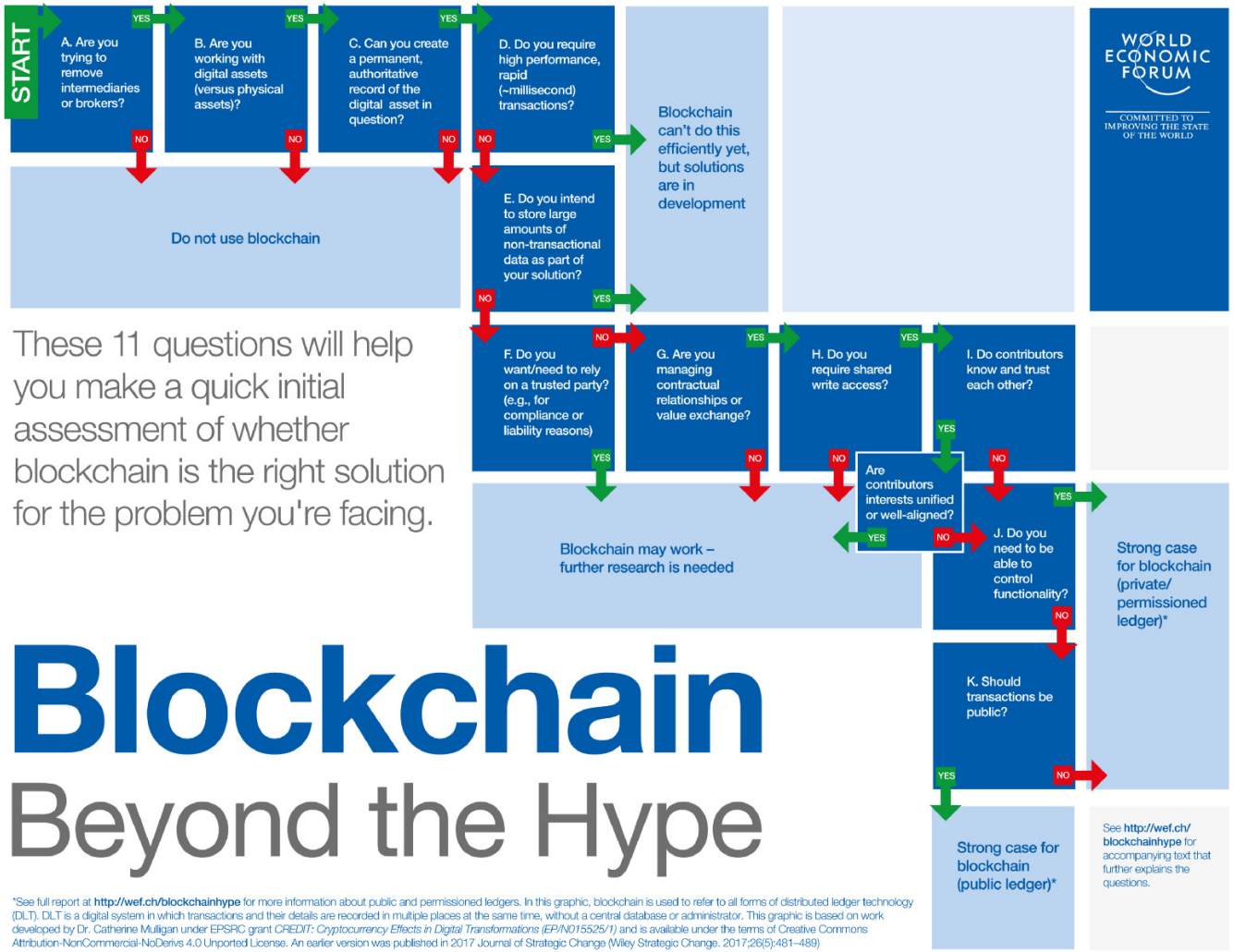
Bird & Bird

Brauche ich eine Blockchain, welche ?



Bird & Bird

Brauche ich eine Blockchain, welche ?



Bird & Bird

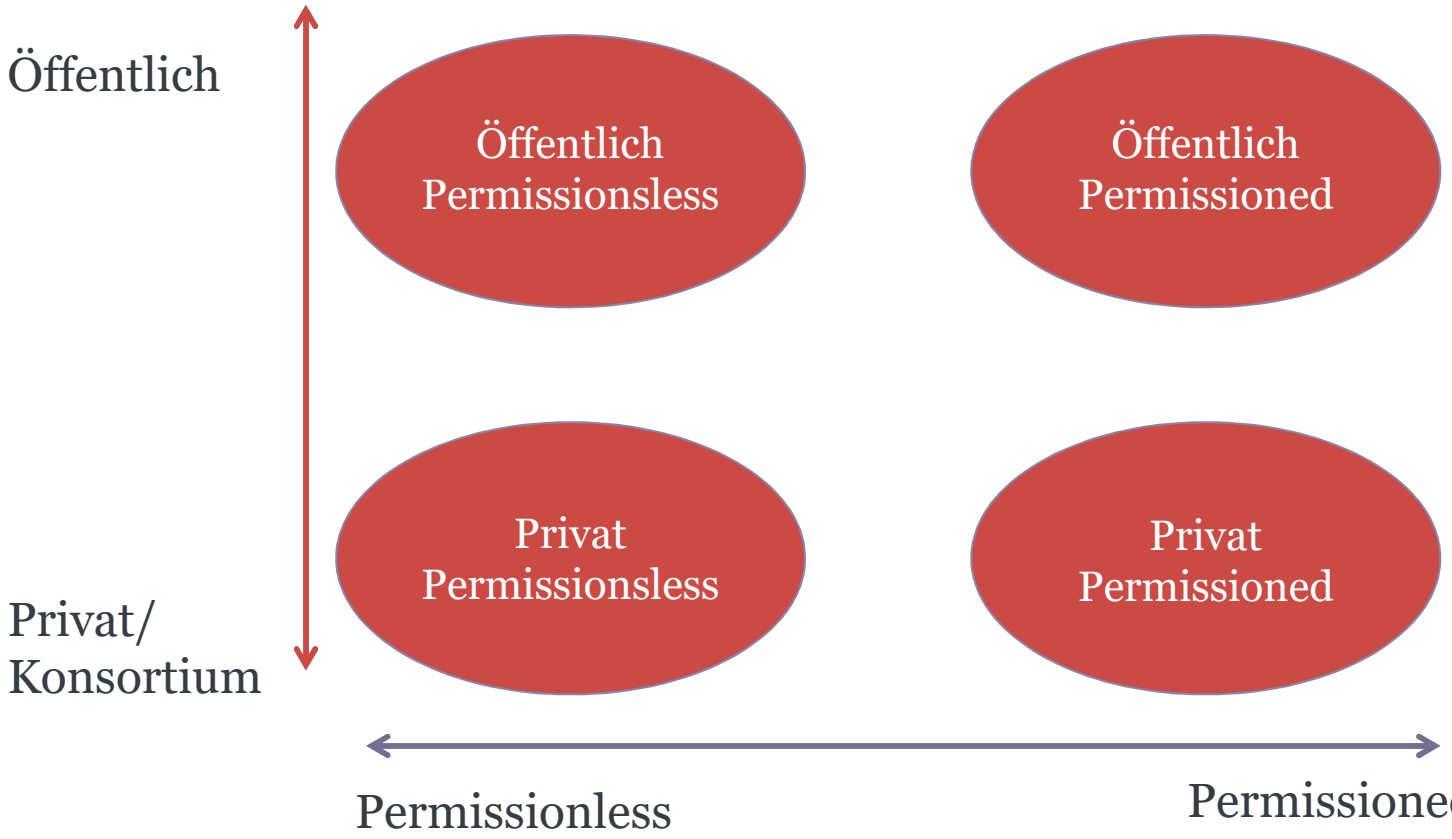
“Die Blockchain."

Was ist "die Blockchain" bzw. DLT?

- **Dezentrale und verteilte Buchführung** über Transaktionen oder Zustände (distributed ledger), Art der dokumentierten Transaktionen/Zustände unerheblich
- **Unveränderbare Speicherung** von Daten (immutabilty); *aber* nachträgliche Änderung "redactable blockchain" möglich
- Validierung/Entscheidungsfindung der "Richtigkeit" der Datenbank über **Mehrparteien-Konsensmechanismus** (PoW, PoS etc.) über peer-to-peer Protokol (Teilnehmer als "Nodes") – **Zero Trust**!
- Verfahren der **kryptografischen Verkettung** in einem dezentral geführten Buchführungssystem technische Basis der Blockchain – andere Verfahren sind möglich (deswegen besser DLT)

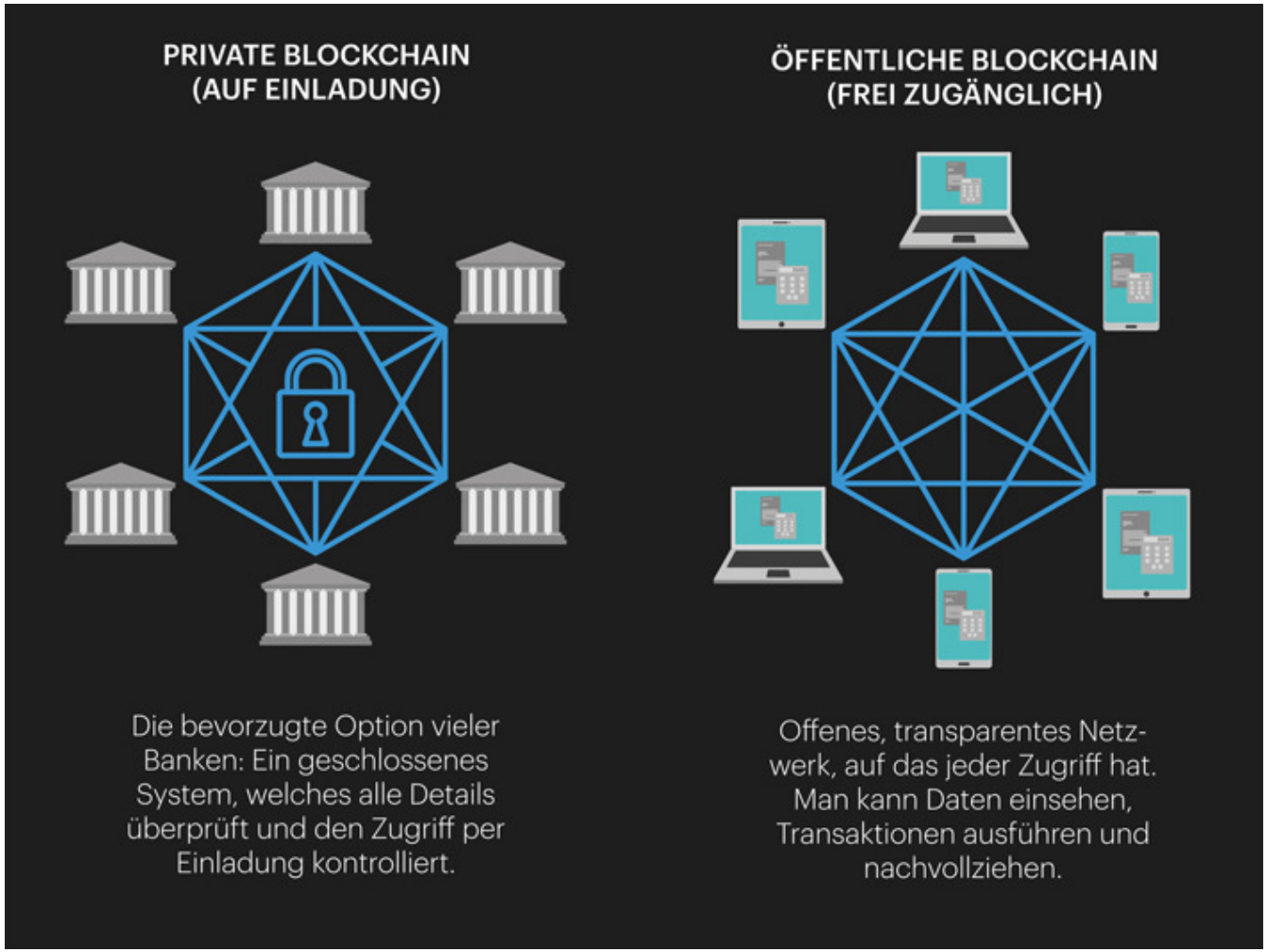
Funktionsweise

Es existieren verschiedene Arten von Blockchains/DLT:



Bird & Bird

Funktionsweise



Quelle: Hochschukle für Wirtschaft Zürich, https://fh-hwz.ch/news/blockchain-kurz-erklart/

Bird & Bird

Konsensmechanismen

Es existieren verschiedene Konsensmechanismen zur Validierung eines Distributed Ledger:

Proof of Work (Bitcoin)

- Validität des neuen Blocks wird durch Nachweis von Arbeitsaufwand (Proof of Work) bewiesen
- Berechnen eines passenden Inputwerts zu bekanntem Outputwert
- Anpassung des benötigten Aufwands durch Difficulty-Algorithmus
- Problem: Hoher Energieverbrauch, Risiko einer 51%-Attacke

Konsensmechanismen

Proof of Stake (Nxt)

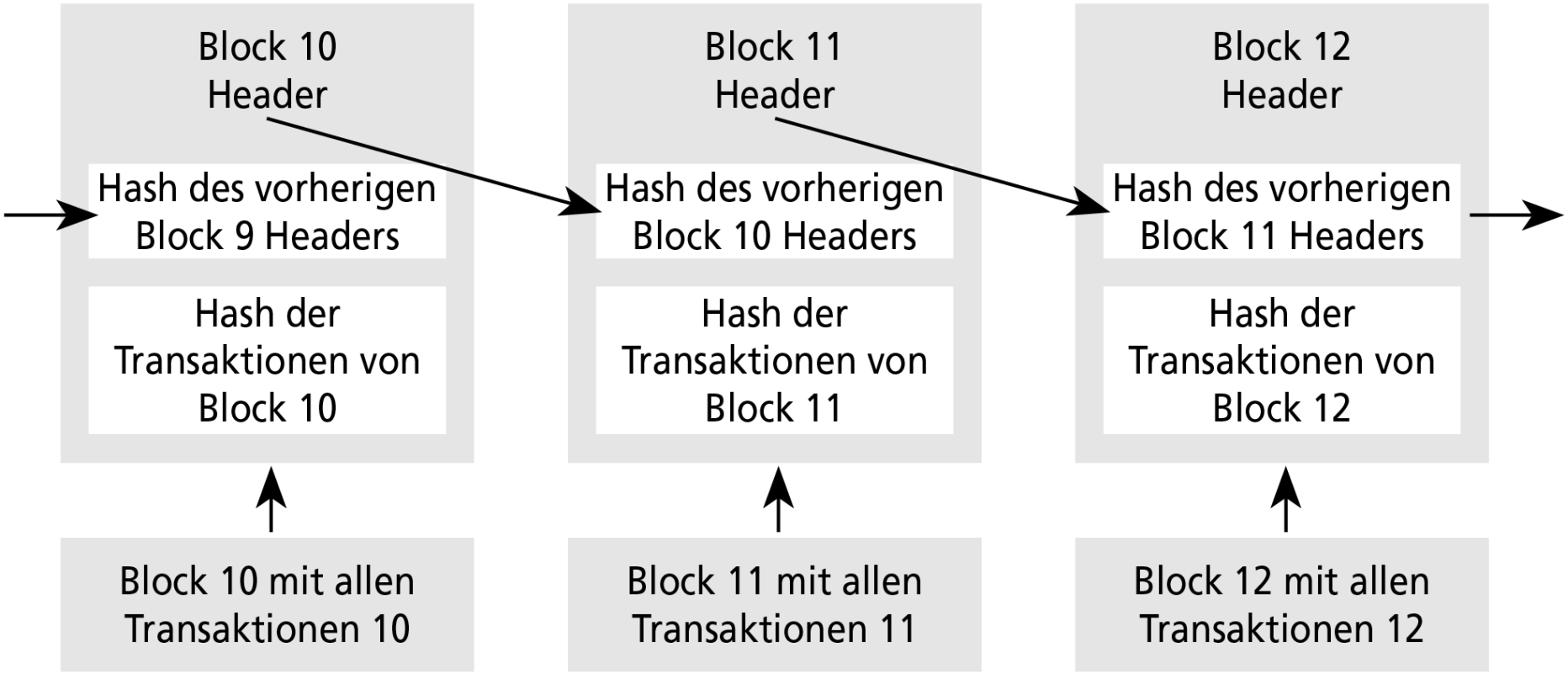
- Ebenfalls Berechnen eines passenden Inputwerts
- Wahrscheinlichkeit, passenden Wert zu berechnen, erhöht sich anteilig zu Anteilen (Stake) am Netzwerk
- Nothing at Stake-Problem
- Kein Risiko einer 51%-Attacke

Tangledatenbank (IOTA)

- Teilnehmer bestätigen mit einer durchgeführten Transaktion gleichzeitig zwei vorhergegangene
- Entgültige Validierung erfolgt durch Setzen von sog. "milestones" durch zentralen Koordinator
- Entwickelt für IoT Anwendungen

Funktionsweise

Aufbau einer klassischen Blockchain:



Quelle: Screy/ Talhofer, Rechtliche Aspekte der Blockchain, NJW 2017, 1431

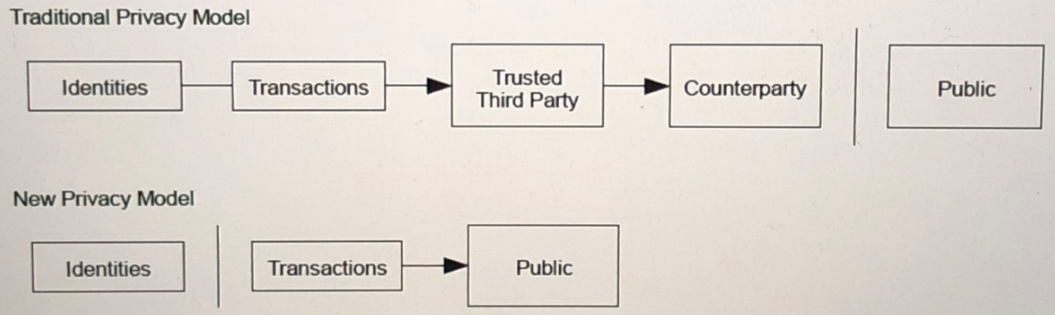
Bird & Bird

Datenschutz

Bitcoin Whitepaper (Satoshi Nakamato)

10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.



As an additional firewall, a new key pair should be used for each transaction to keep them from being linked to a common owner. Some linking is still unavoidable with multi-input transactions, which necessarily reveal that their inputs were owned by the same owner. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner.

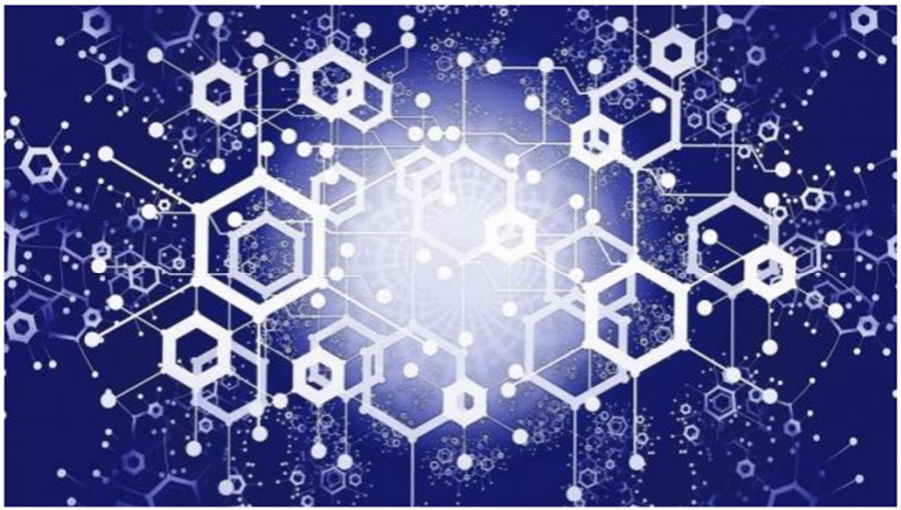
Bird & Bird

23.10.2018 15:01 Uhr

China will Blockchain-Dienste aus der Anonymität holen

Chinesische Nutzer müssen wohl bald ihren echten Namen angeben, wenn sie Blockchain-basierte Dienste wie Bitcoin-Zahlungen verwenden wollen.

von **Stefan Krempl** 14



(Bild: geralt)

Die chinesische Regierung setzt weiter auf ein hartes Regime gegenüber dezentralen Kryptowährungen und anderen Diensten, die auf der Datenbanktechnik Blockchain basieren. Künftig müssen die Anbieter entsprechender Services von Kunden zunächst den echten Namen sowie die Nummer ihres nationalen Ausweises erfassen, berichtet die *South China Morning Post* unter Verweis auf eine Regulierungsinitiative der Cyberspace-Verwaltungsbehörde.

Anwendbarkeit der DSGVO

DSGVO grds. bei der Verarbeitung personenbezogener Daten anwendbar:

- In der Regel werden auch pb Daten (weite Definition) auf der BC/DLT verarbeitet, oft pseudonyme pb Daten
- Pseudonymisierte Netzwerk(teilnehmer)adressen (public keys)
  - Absolutes vs. relatives Verständnis
  - Breyer-Rspr. des EuGH
- Transaktionsdaten können enthalten:
  - Personenbezogene Daten des Netzwerkteilnehmers
  - Personenbezogene Daten Dritter

Anwendbarkeit der DSGVO

- **Problem:** Dezentrale und verteilte Registerführung führt zu maximaler Transparenz für alle Teilnehmer
- Art. 29 Gruppe: *Hashing* ist eine Technik der Pseudonymisierung, nicht der Anonymisierung
- In Zukunft jedoch technische Lösungen denkbar, "GDPR-compliant chains" bzw. Use Cases, z.B. durch off-chain Speicherung von pb Daten
- CNIL: "*Moreover, in a more general manner, it is important not to store personal data in cleartext on a blockchain.*"

Anwendbarkeit der DSGVO

- DSGVO nicht bei rein privaten Verarbeitungszwecken anwendbar
- CNIL: "*natural persons who enter personal data on the blockchain, that do not relate to a professional or commercial activity, are not data controllers (pursuant to the "purely personal or household activity*", exclusion set out in Article 2 GDPR)
- Reichweite str.
  - Enge Auslegung EuGH: Zeugen Jehovas, Lindquvist (Datenverarbeitung ***ausschließlich*** zu persönlichen oder familiären Zwecken), Problem der eindeutigen Identifizierung des Zwecks
- Wer ist Verantwortlicher?

Einordnung der Netzwerkteilnehmer: Unternehmen

CNIL:

- Jeder, der Mittel und Zwecke der Verarbeitung selbst bestimmt, ist Verantwortlicher (aber wer bestimmt Mittel und Zweck wirklich?)
- Jedes Unternehmen, das Businessmodel auf BC betreibt ist Verantwortlicher

- Möglichkeit der Gemeinschaft von Unternehmen:
  - Gründung einer Gesellschaft als Verantwortlicher
  - Bestimmung eines alleinigen Verantwortlichen
  - Gemeinsame Verantwortliche gem. Art. 26 DSGVO

Einordnung der Netzwerkteilnehmer: Miner

- Bloße AV, wenn ausschließlich weisungsabhängig
  - Dann AV-Vertrag erforderlich
  - Hoch problematisch bei öffentlichen Blockchains
- Fraglich ob Miner nicht (gemeinsam) Verantwortliche
  - Wesentlicher Einfluss auf das Netzwerk
  - Essentiell für das Funktionieren der Blockchaintechnologie
  - Verfolgen eigene Zwecke

Einordnung der Netzwerkteilnehmer: Smart Contract Entwickler

- CNIL: Einordnung abhängig von Ausmaß der Datenverarbeitung durch Entwickler:
  - DSGVO nicht anwendbar, wenn bloße Bereitstellung des Programmcode
  - AV, wenn weisungsabhängige Verarbeitung
  - Verantwortlicher, wenn Verfolgung eigener Zwecke

Einordnung der Netzwerkteilnehmer

- Die Bestimmung der Rollen lässt sich bei privaten permissioned Blockchains von Unternehmen/Konsortien naturgemäß leicht umsetzen

- Unternehmen/Konsortien können die Rollen ihrer Teilnehmer und die Informationsflüsse selbst (vorab) definieren, Regeln für die Datenverarbeitung festlegen und Netzteilnehmer auf bestimmte Bedingungen verpflichten

- Public permissionless Blockchains stellen hinsichtlich der Rollenbestimmung eine große Herausforderung dar, noch nicht abschließend geklärt

Datenschutzgrundsätze: Datenminimierung

- Menge der Daten für den jeweiligen Zweck angemessen, erheblich und auf das notwendige Maß beschränkt (auch Speicherdauer)

- Widerspruch zu Blockchain Use Cases: dauerhafte Speicherung

  - Für Netzwerkadressen (public keys) unumgänglich

  - Bei Transaktionsdaten ist "Verbesserung" durch Verschlüsselungsmechanismen möglich

Datenschutzgrundsätze: Privacy by Design

- Privacy by Design Art. 25 DSGVO: "(...) trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen – wie z. B. Pseudonymisierung –, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen (...)"

- Schon beim Design der BC/DLT sollte der Grundsatz beachtet werden und entsprechend technisch umgesetzt werden

- Auch hier gilt: Genaues Assessment durch Unternehmen notwendig; welche Probleme kann BC/DLT für mich leichter lösen als herkömmliche Technologien?

Betroffenenrechte

Unproblematisch sind Rechte, die nicht durch Unveränderbarkeit der Blockchain berührt werden:

- Auskunftsrecht nach 15 DSGVO
- Recht auf Datenportabilität aus Art. 20 DSGVO

Betroffenenrechte

Hochproblematisch dagegen:

- Recht auf Löschung, Art. 17 DSGVO
- Recht auf Berichtigung, Art. 16 DSGVO

➢ Basieren beide grds. auf rückwirkender Änderung
➢ Dies erlaubt die Blockchaintechnologie (in der Regel) nicht

❖ Mögliche Lösung:
➢ Anonymisierung des alten Datums (+ Speichern des neuen korrigierten Datums)
➢ "redactable Blockchains"

Datenschutzfolgenabschätzung

- Art. 36 DSGVO "Hat eine Form der Verarbeitung, **insbesondere bei Verwendung neuer Technologien**, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko..."

➢ in Abhängigkeit der technischen Ausgestaltung der BC/DLT ggf. durchzuführen, aber wohl nicht automatisch bei jeder Verwendung von BC/DLT

Datenschutzfolgenabschätzung

- Nach Einschätzung der CNIL: Positive Datenschutz-Folgenabschätzung kann ausnahmsweise unverschlüsselte Speicherung von pb Daten auf BC DSGVO-kompatibel machen

- Dazu erforderlich: Rechtfertigung durch Verarbeitungszweck und Annehmbarkeit der Restrisiken

- Verpflichtung zur öffentlichen Zugangsmachung kann ausnahmsweise sogar unverschlüsselte Speicherung auf Public BC erlauben

Risiken & Chancen

Risiken

- Kompromittierung von Daten durch Angriffe auf die Blockchain
- Drohende Zentralisierung bei zu wenigen Minern führt zu Vertrauensverlust der Nutzer/Verlust der Eigenschaft als Blockchain/DLT
- Pseudonymität der pb Daten kann leicht aufgehoben werden, maximale Transparenz führt zu Datenschutzverletzungen

Chancen

- Erfüllung der Anforderungen der DSGVO (eingeschränkt) möglich – wichtig: Bestimmung der Rollenverteilung muss im Einzelfall erfolgen (Verantwortlicher, gemeinsame Verantwortlichkeit, Auftragsverarbeiter, Betroffener)

- *Privacy by Design*, technische Ausgestaltung der BC/DLT kann höheres Datenschutzniveau für Betroffene verwirklichen

- Dezentrale Speicherung verringert Manipulations- und Herrschaftspotential bisheriger zentraler Modelle ("GAFA")

Fazit

Fazit

- Blockchain und DLT Use Cases/Anwendungen oft nur im eingeschränkten Maße DSGVO-konform - aber grds. Frage der technischen/organisatorischen Ausgestaltung
- Bestimmung der Rollenverteilung sollte immer im Einzelfall erfolgen: (gemeinsame) Verantwortliche(r) oder Auftragsverarbeiter?
- "Verschlüsselung pb Daten und Minimierung der Verarbeitung auf der Blockchain oft Voraussetzung für Konformität
- Genaue Einordnung von Minern als Netzwerkteilnehmer dringend nötig
- Chance eines erhöhten Datenschutzes durch Verwendung von Blockchains (z.B. Identitätsmanagement)

"As this paper will explain, **GDPR compliance is not about the technology, it is about how the technology is used.** Just like there is no GDPR-compliant Internet, or GDPR-compliant artificial intelligence algorithm, **there is no such thing as a GDPR-compliant blockchain technology. There are only GDPR-compliant use cases and applications.**

— *Blockchain and the GDPR*, The European Union Blockchain Observatory & Forum

Oliver Schmidt, LL.M.
Rechtsanwalt
Bird & Bird LLP (Düsseldorf)
T: +49 (0) 211 2005 6162
M: oliver.schmidt@twobirds.com

Johannes Kevekordes
Wiss. Mitarbeiter, Referendar
Bird & Bird LLP (Düsseldorf)
T: +49 (0) 211 2005 6364
M: johannes.kevekordes@twobirds.com

Vielen Dank für Ihre Aufmerksamkeit