Baker McKenzie.

TMT Blockchain Online Seminar

Online Seminar

Tuesday November 3
2020

Agenda

Technical Background, including Information Security Implications

Use Cases

Legal Aspects

- Data Protection Law Considerations – EU
- Data Privacy Considerations – US
- Compliance Law Aspects
- Enforcement in US

Speakers

Dr. Matthias Artzt
Lawyer and Senior Legal Counsel
Deutsche Bank AG, CIPP/E

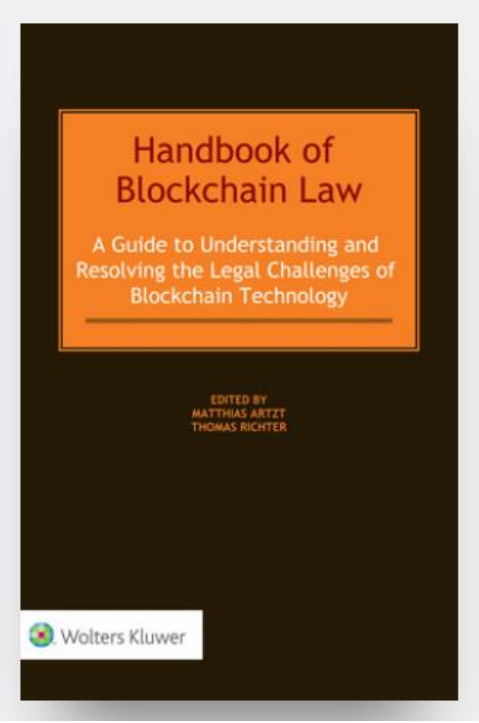
Lothar Determann
Partner
Palo Alto
lothar.determann@bakermckenzie.com

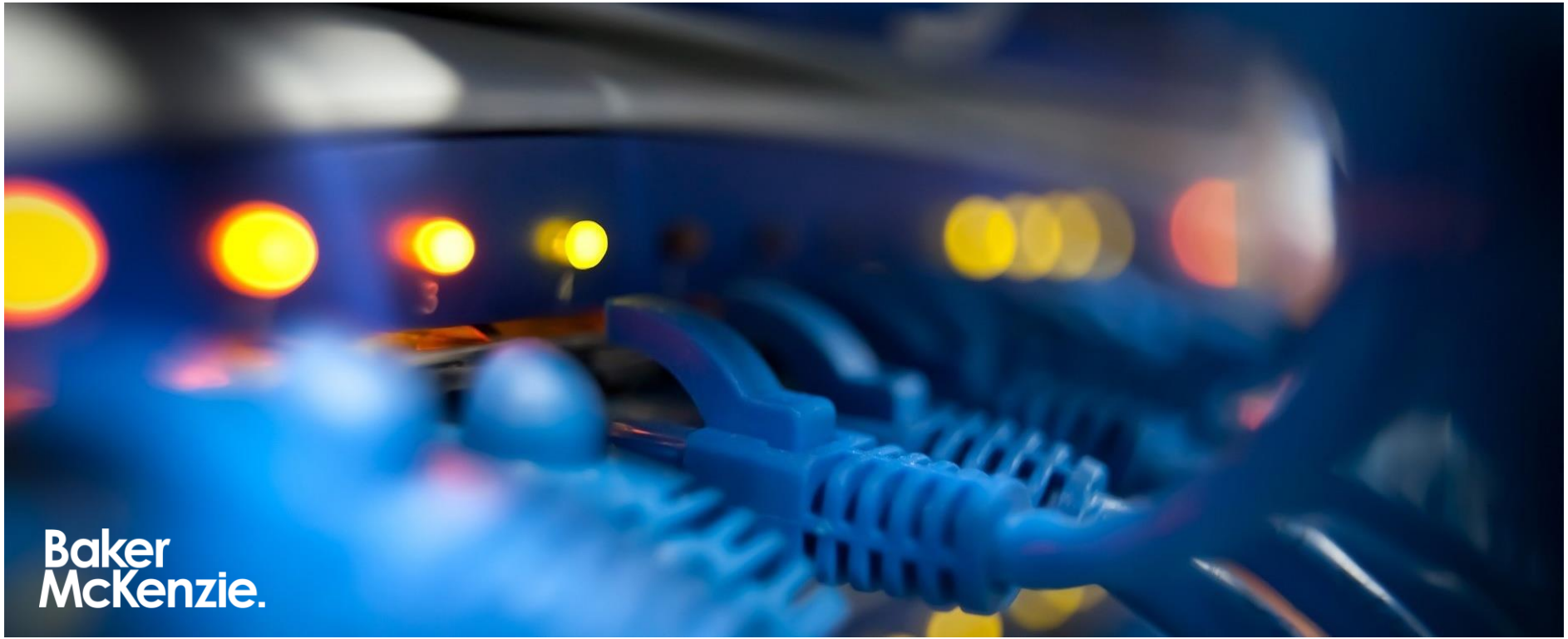
Dave Hirsch J.D., CFE
Senior Counsel
US Security and Exchange Commission

Michaela Nebel
Partner
Frankfurt
michaela.nebel@bakermckenzie.com

Carolina Pardo
Partner
Bogota
carolina.pardo@bakermckenzie.com

Handbook of Blockchain Law





01 Technical Background

- *Dave Hirsch*

Disclaimer

- The Securities and Exchange Commission disclaims responsibility for any private publication or statement of any SEC employee or Commissioner. This speech expresses the author's views and does not necessarily reflect those of the Commission, the Commissioners, or other members of the staff.
- I am not a computer scientist.
- I am not a coder.
- If you ask my manager, or anyone really, I am a giant nerd, but this is not a prerequisite to get involved in this space.

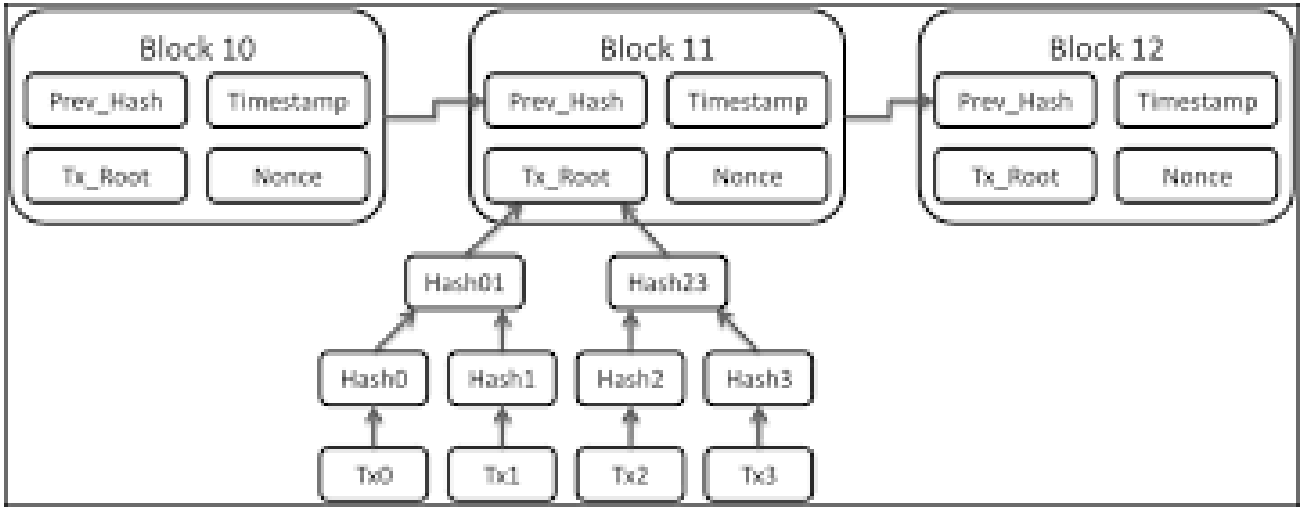
Bitcoin

- BitCoin – Created in 2008
- Pseudonymous Creator – Satoshi Nakamoto
- 9 Page White Paper: “BitCoin – A Peer-to-Peer Electronic Cash System”
- Created and Used as Medium of Exchange
- Distributed Ledger for Tracking All Transactions

Bitcoin

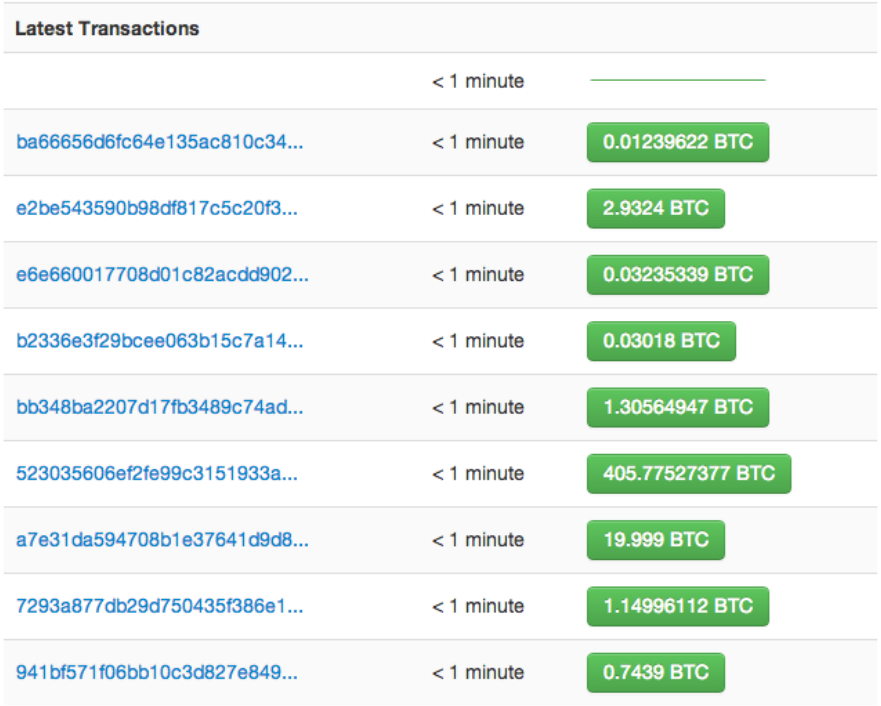
- Decentralized
- Trustless
- Immutable
- Pseudonymous

Immutable


Block 10
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 11
Prev_Hash
Timestamp
Tx_Root
Nonce
Block 12
Prev_Hash
Timestamp
Tx_Root
Nonce
Hash01
Hash23
Hash0
Hash1
Hash2
Hash3
Tx0
Tx1
Tx2
Tx3

Bitcoin – The Blockchain

- Public ledger that confirms every transaction in Bitcoin, for all time
- Used to distinguish legitimate transactions from attempts to re-sell/spend/buy the same coins
- *Blockchain.info*



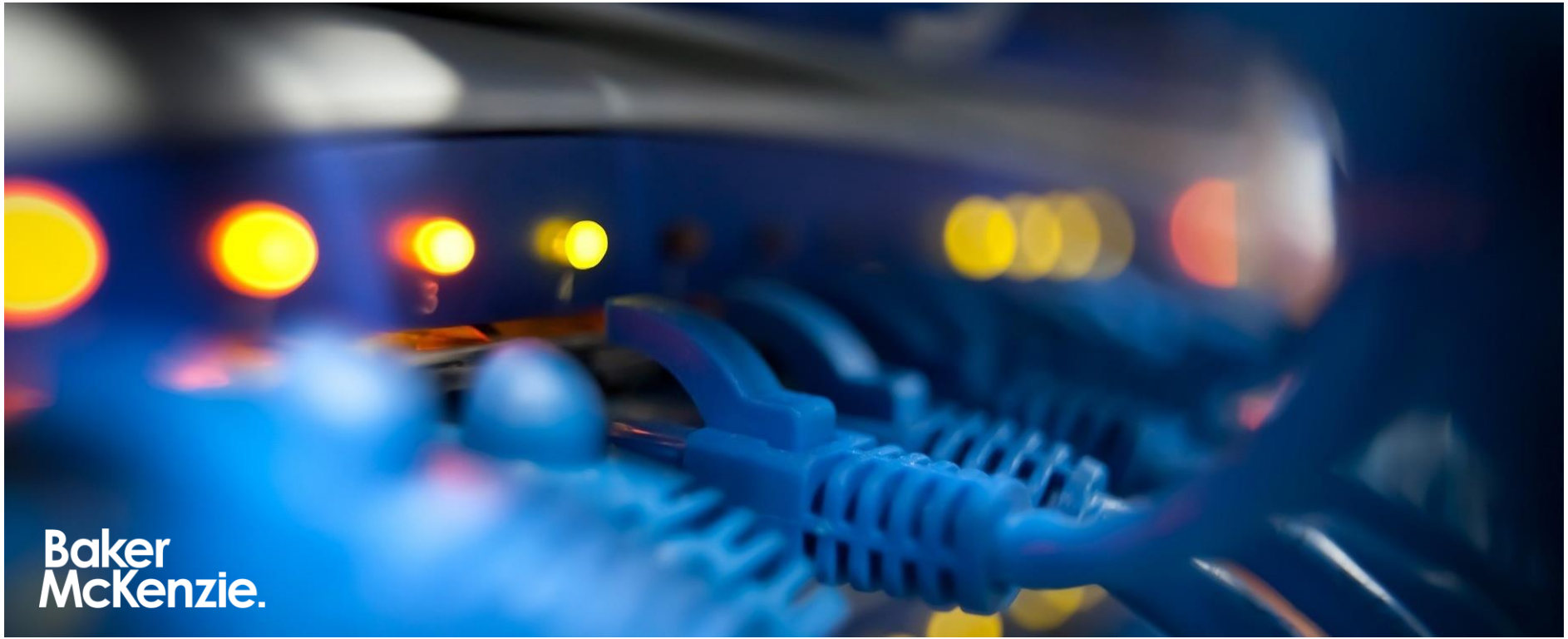
Bitcoin – The real world

- **Good news:**
  - There is no central authority charging a fee on every transaction or picking winners and losers.
- **Bad news:**
  - When things go wrong, there is no central authority who can reverse a transaction, return stolen funds, or decide who is the rightful owner of disputed bitcoins.

- **Good news:**
  - Theoretically, the blockchain can’t be hacked.
- **Bad news:**
  - Exchanges and computers where people hold their bitcoins can be hacked or taken down by regulatory authorities.

Bitcoin – The real world

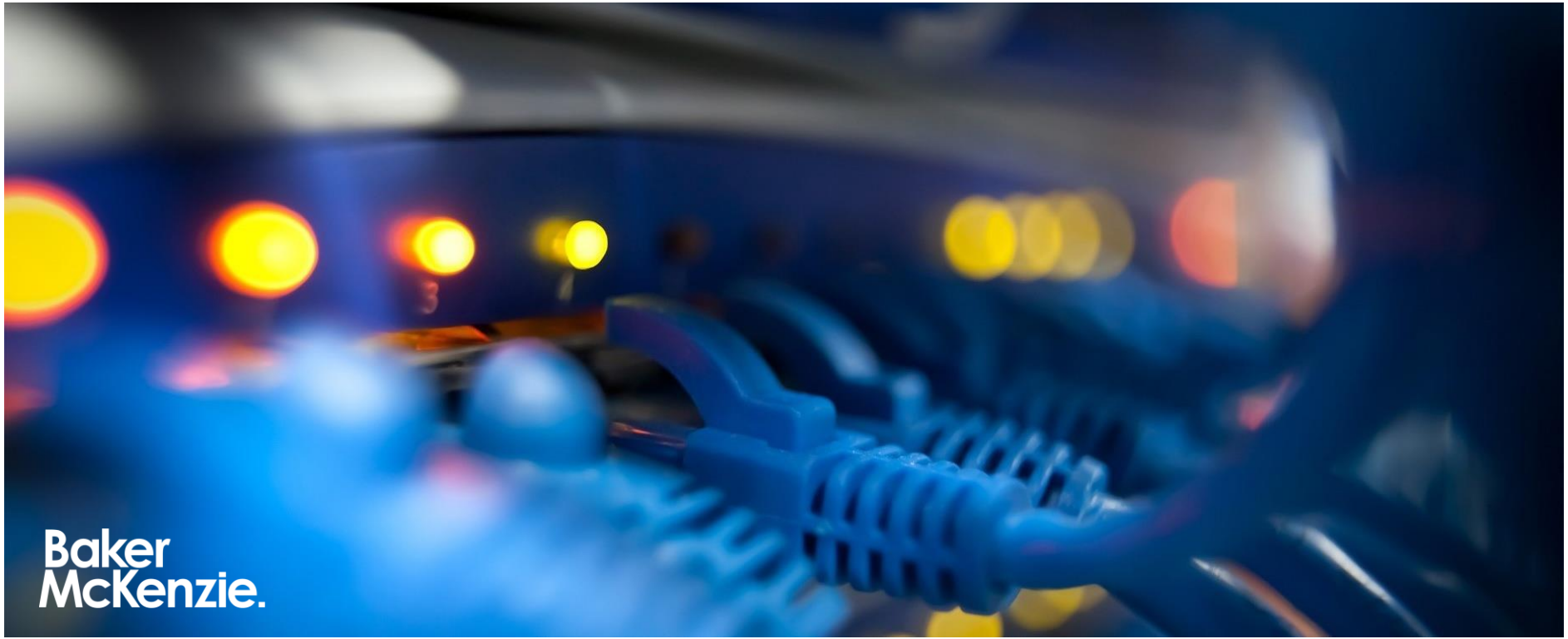
- **Good news:**
  - Miners and exchangers are distributed around the globe and uncontrolled by any single government or regulator.
- **Bad news:**
  - That leaves exchanges vulnerable to manipulation. In March 2017, the SEC disapproved a proposed rule change that would have allowed the first U.S. registered bitcoin ETF in large part because the bitcoin markets are unregulated.



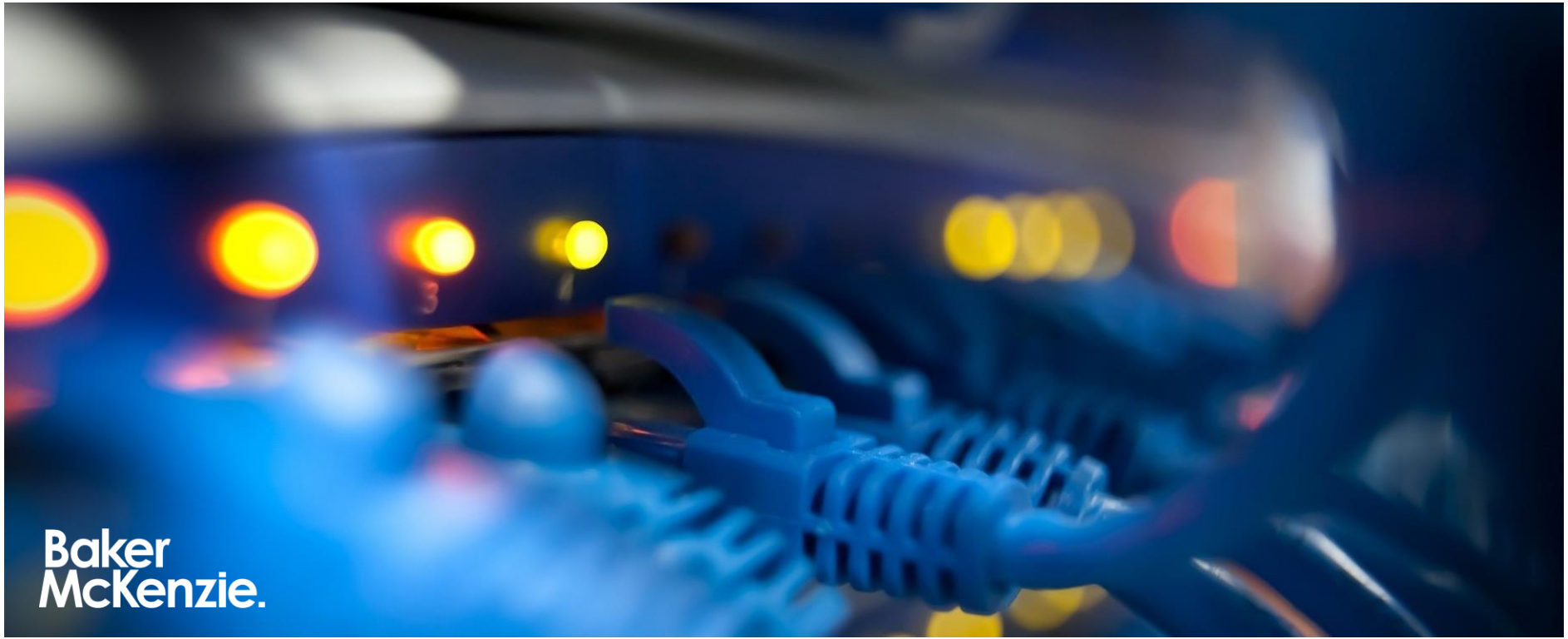
02 Use Cases
- *Matthias Artzt*

Use cases of blockchain technology in the financial industry

- **Payments / Cash Settlement**
  - Particularly machine-to-machine payments
  - Leveraging smart contracts
  - Case-by-case consideration whether DLT / blockchain technology is appropriate for driving the business case
- **Crypto Currencies issued by central banks**
  - Case-by-case consideration whether DLT / blockchain technology is appropriate for driving the business case
- **Trade Finance and insurance sector**
  - Leveraging smart contracts
  - Private blockchain governed by insurance companies and a public authority to administer and trigger payments to customers and generate customer information



03 Legal Aspects



3.1 Data Protection Law Considerations- EU

- Matthias Artzt

Allocation of roles and responsibilities under the GDPR

1. **Exhaustive list of roles under the GDPR:**
   - (Joint) controller, Art. 4 (7), Art. 26
   - Processor, Art. 4 (8)
2. **The usual players in a blockchain environment:**
   - Miners
   - Nodes
   - Wallets
   - Users
   - Developers of smart contracts
   - Oracles
   - Governance bodies

Data subject rights under the GDPR (1/3)

1. **How do data subject rights apply to the blockchain?**
   a. **Applicability of the GDPR**
      - Once one block contains personal data and the block is added to the blockchain ► **storage = data processing pursuant to Art. 4 sec. 2 of the GDPR**
      - Data subject may exercise his rights pursuant to Art. 15 – 22 of the GDPR. **Problem: against whom**?

   b. **Distinction between public and private blockchains in relation to enforcing data subject rights**
      - Private blockchains: Governance body to be the first choice to address any data subject rights. Joint controllers according to Art. 26 GDPR
      - Public blockchains: Data subjects face a challenge to (i) identify the controller, and to (ii) get the controller to carry out his obligations

Data subject rights under the GDPR (2/3)

2. Factual enforceability of particular data subject rights

a. Right to access personal data, Art. 15 GDPR

- Basic right: prerequisite for the exercise of any other right under the GDPR
- Necessary to understand which data is being processed and for what purpose
- **Problem:** In a public blockchain **a controller, once identified, is factually unable to access data** submitted to the blockchain: data is typically encrypted or hashed; impossible to determine whether the related data is personal and relates to the data subject concerned

b. Right to rectify personal data, Art. 16 GDPR

- Right to request rectification of inaccurate personal data and to complete personal data which is incomplete
- **Problem: Impossibility to modify data** registered onto a blockchain

Data subject rights under the GDPR (3/3)

c. Right to erasure („right to be forgotten“), Art. 17 GDPR

- **What does erasure mean?**
  - Data subject may request the erasure of his/her personal data provided one of the conditions set out in Art. 17 sec. 1 GDPR applies
  - **Erasure as a legal term is defined very broadly** (e.g. expunge, overwriting, making data unusable)
  - **Problem: Impossibility to delete any data** once registered onto the blockchain
  - But: This is not a Catch 22 situation since alternative solutions are permissible when the erasure is virtually not viable ► *see techniques to mitigate data protection risks*

Principles of purpose limitation and data minimization vs blockchain finality (1/3)

GDPR

Principle of purpose limitation of data processing

Principle of data minimization

Blockchain

Immutability of information being submitted to the blockchain (blockchain finality)

Principles of purpose limitation and data minimization vs blockchain finality (2/3)

1. **Principle of purpose limitation, Art. 5 sec. 1b GDPR**
   - **Definition:**
     - "Personal data shall be collected for specific, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes" (Art. 5 sec. 1b GDPR)
     - Purpose limitation is the "cornerstone of data protection" (Art. 29 Data Protection Working Party [now: EDPB])
   - **Legal implication on blockchain:**
     - Blockchain, by nature, continuously processes data by storing it onto the blockchain which also includes legacy personal data (data which is not needed any more, e.g. after completion of a particular transaction)
     - Solutions such as a broad purpose description are disputable

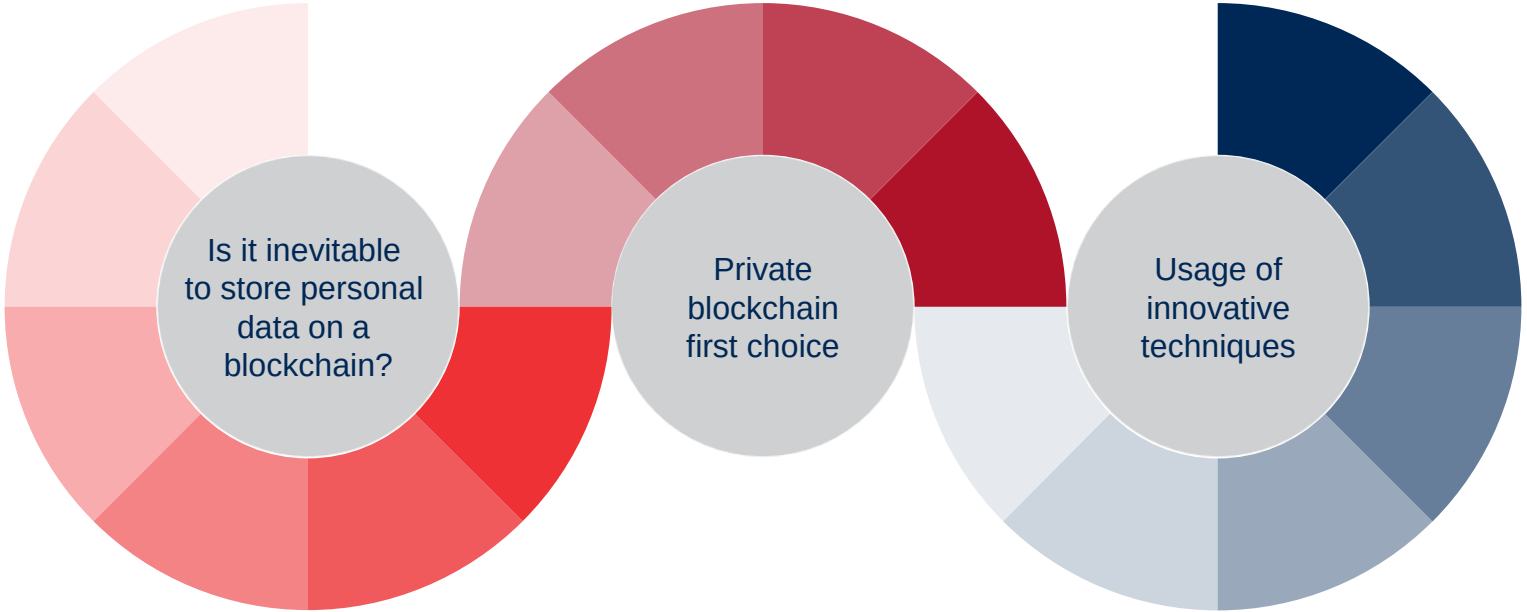
Principles of purpose limitation and data minimization vs blockchain finality (3/3)

2. Principle of data minimization

- **Definition:**
  - Only those data which is necessary to meet the purpose determined by the controller must be collected and processed
  - Period for which the personal data is being stored must be limited to a strict minimum (Recital 39 of the GDPR)
- **Legal implication on blockchain:**
  - Blockchain artefacts clash with the data minimization principle:
    - ► Ever-growing nature of databases containing personal data
    - ► Replication of data in a blockchain network where each node stores a full copy of the database

Techniques to mitigate data protection risks (1/5)

Assessment of the permissibility of submitting personal data to the blockchain:



Techniques to mitigate data protection risks (2/5)

- **Big picture:** How is the data being processed and is there any need to store it on a blockchain? Offchain storage should be the first choice
- **Usage of private blockchains as primary objective**
- **Usage of innovative encryption techniques**, particularly with regard to public blockchains:
  - **Anonymization** as primary approach
  - If anonymization is not doable, **state-of-the-art encryption, particularly hashing**
  - Please note: Hashing is an encryption technique and does not entail anonymization ► Hashing does not turn personal data into not personal data ► GDPR applies

Techniques to mitigate data protection risks (3/5)

- **Usage of interoperable blockchains („multi-layered“)**
  - **Background:** Storage of personal data which is not needed any more („**legacy data**“) in sync with the principles of purpose limitation and data minimization
  - **Removing legacy data from a private blockchain and transferring it to a public blockchain**
  - Both blockchains are intertwined meaning that the public blockchain links to the private blockchain

    ► For real time data processing: private blockchain
    ► For legacy data: public blockchain
  - **Problem:** Legacy data remain on the public blockchain
    ► data is being replicated and still visible
  - **Resume:** Good instrument for safeguarding personal data, but not in line with the principles of purpose limitation and data minimization

Techniques to mitigate data protection risks (4/5)

- **Off-chain storage and hashing of legacy data („hashing-out“)**
  - **Background:** Storage of legacy data in sync with the principles of purpose limitation and data minimization
  - **Removing legacy personal data from the blockchain and storing it in an external off-chain database; linking personal data via hash point**
  - Hashes of the personal data being put off-chain remain onto the blockchain
  - **Problem:** On-chain hashes remain personal data
    ► Hash constitutes the key for the off-chain transactional data
    ► GDPR applies for on-chain hashes

Techniques to mitigate data protection risks (5/5)

- **Erasure of personal data by deleting off-chain legacy data**
  - **Hashing-out and deleting legacy data comply with an erasure request** even though the *hash of the personal data remains on the blockchain*
  - **Rationale:** ► The on-chain hash has nothing to relate to as soon as the corresponding personal data on the external off-chain database has been deleted; the hash becomes a random string with no meaning
    - ► A cryptographic hash function is a „one-way function“: it is not possible to recreate or reverse engineer the original data from the hash function
    - ► Deletion of the off-chain legacy data turns the hash to not personal data
  - Hashing-out also complies with the principles of purpose limitation and data minimization

Legal grounds under the GDPR

1. **Contractual necessity, Art. 6 (1)(b) GDPR** – relevant re smart contracts
2. **Consent, Art. 6 (1)(a) GDPR**
   - Consent can be withdrawn by the data subject at any time
   - Unclear to whom the user must give consent
3. **Legitimate interest Art. 6 (1)(f) GDPR**
   - Controller must demonstrate that its interests are prevailing and carry out a balancing test aiming to consider and to address the competing interests of the relevant parties
   - Submitting of personal data to a blockchain is legitimate if, e.g., the processing activity aims to prevent frauds (Recital 47 of the GDPR)
4. **Compliance with a legal obligation, Art. 6 (1)(c) GDPR**
5. **Public interest, Art. 6 (1)(e) GDPR**

Key Take Aways

It is just technology

Law is technology neutral

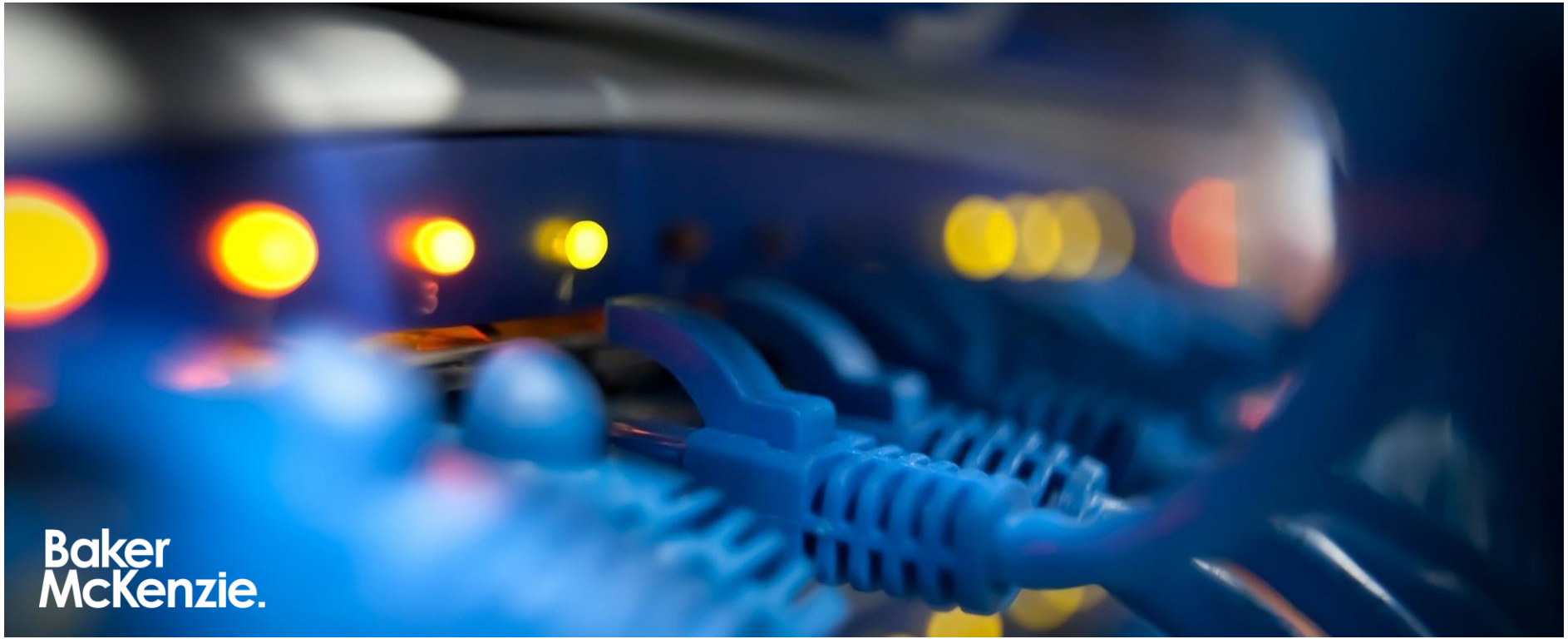
Tensions with GDPR can be overcome

Usage of state-of-the-art encryption is key

Carry out PIA and DPDD

Private blockchain first

Track guidance of data protection authorities



3.2 Data Privacy Considerations – US

- *Lothar Determann*

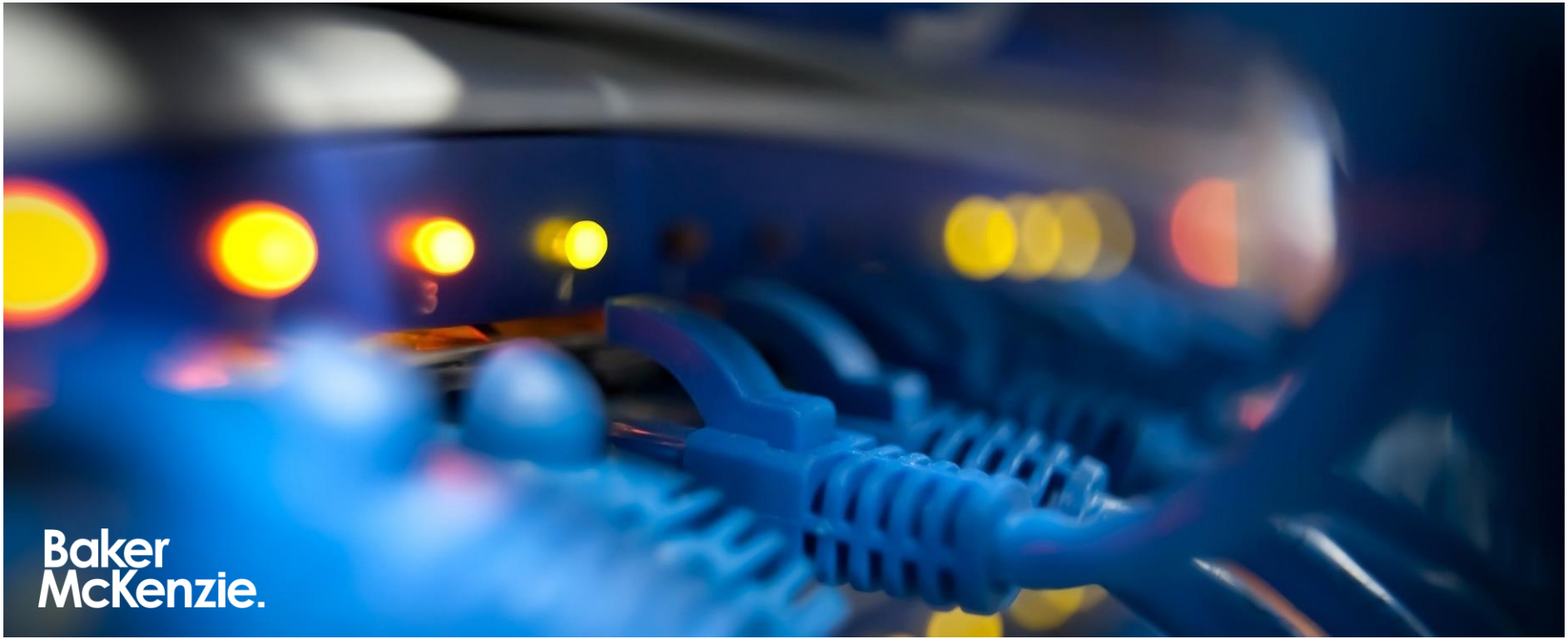
US Privacy Law Considerations

- US Privacy Law Versus EU Data Protection Regulation
  - US: no omnibus statute, but sector-, situation-, and harm-specific privacy laws
- Federal and State Law
- Diverse Terminology
- General US Privacy Laws applied to Blockchain
  - California constitutional guarantee of privacy as well as common law, torts, consumer protection and unfair competition laws

    → Issue clear and simple user manuals and privacy notice to not violate anyone's reasonable privacy expectations
- Specific US Privacy Laws applied to Blockchain
  - No specific privacy law for blockchain, but many sector-, harm- and situation-specific laws may apply

Blockchain and CCPA

- Scope of CCPA
- Which Blockchain Participants Must Comply with CCPA?
- CCPA Compliance Obligations
- Data Access and Deletion Rights
- Sanctions and Remedies



3.3 Compliance Law Aspects
- *Carolina Pardo*

Compliance Law Aspects

1. Assumptions

- BlockChain (“BC”) normally uses encryption technologies that anonymized or pseudo-anonymized the identity of the participants.
- Financial and, more recently, certain commercial entities have regulatory obligations to implement AML systems, including proper measures to identify third parties (clients, vendors, employees, etc.).
- Permissioned BC allows participants to designate an entity or participant as controller of the information in the BC. Public BC, otherwise, disseminates the responsibility among all participants.
- FATF standards allow entities to rely on third parties to perform most of the steps of the KYC process (excluding the ongoing monitoring).

Compliance Law Aspects

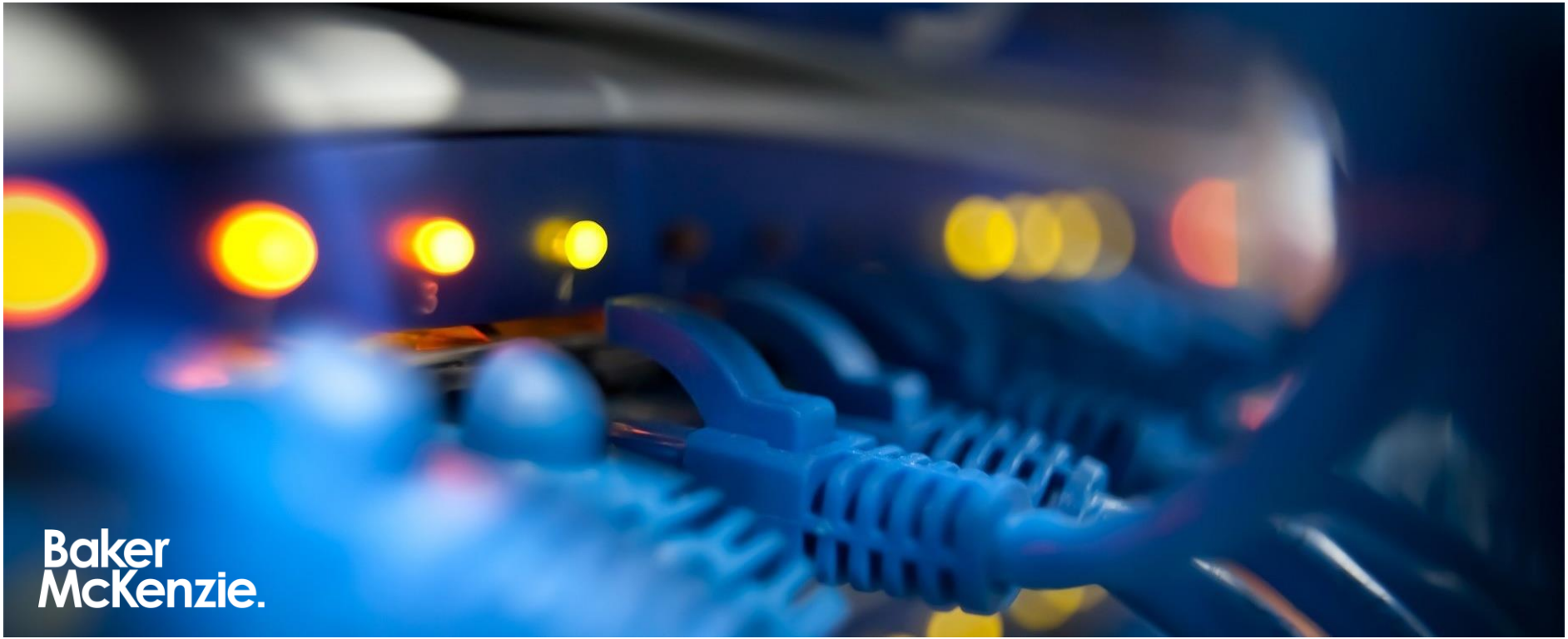
2. Advantages of using BC

- Permissioned BC allows participants to centralized on one entity the AML Compliance.
- BC allows creating a regulator ID to grant it direct access to the relevant information. This reduces the number of RFIs, the time of response, and increase regulator timely actions.
- BC also allows participants to rely on the administrator to perform KYC procedures on all participants in the BC (economies of scale).
- Multilateral transactions can rely on the same standard of KYC and Suspicious Operations identification (information symmetry). No contradictory results on the KYC, less false positives.
- BC allows participant to have permanent access to a record of KYC processes and transactions.
- BC saves transactional cost associated with the KYC process, KYC can rely on prior KYC processes or BC signup KYC procedures.
- BC allows having a general and practical approach to any participant's commercial behavior. This allows to identify suspicious transactions or unusual behaviors in all its transactions and not only in vis-à-vis relationships.
- BC record allows participants to use their own data as an input for proper segmentation, identification, measurement, and monitoring of their own AML risks (more accurate and up-to-date AML risk matrixes).

Compliance Law Aspects

3. Possible downsides

- Anonymity and pseudo-anonymity of participants may difficult KYC processes and involve risk to participants.
- Regulators not always allow the possibility of rely on third parties for KYC processes and other AML system elements and measures.
- Regulators keep the responsibility for KYC to the individual entities. Any mistake on conducting proper KYC process will not only affect the transactional safety of the BC, but the regulatory obligations of the participants.
- Lack of regulatory obligations, standards, and professionalization of the administrators of permissioned BC in AML may create systemic risks.
- Participants must standardized and agreed on the KYC process to be performed by the administrator. Not al the transactions of the participants will take place within the BC.
- Not all Data Privacy Regimes are compatible with BC. Data Privacy Impact Assessment need to be performed before implementing the BC.
- BC with participants in different jurisdictions may be subject to different regulations and the sharing of personal data will entail a transnational transfer of data (sometimes highly regulated or forbidden).



3.4 Enforcement
- *Dave Hirsch*

Enforcement

Filed Actions

- SEC v. Shavers
- BTC Trading Corp.
- The DAO - 21(a) Report
- Multiple Fraud Actions – PlexCoin, ReCoin, AriseBank, Centra, Blockvest, and others

Enforcement

- AirFox and ParagonCoin – Unrelated ICOs that did not register with the SEC and raised more than $27 million.
  - Settled – Agreed to pay a penalty, notify investors of right to seek reimbursement, set up claims process, and register their securities.

- Gladius – self-reported and settled without a penalty.

Baker McKenzie: Further Reading

https://www.bakermckenzie.com/en/insight/publications/2018/11/eu-blockchain-observatory-blockchain-gdpr

https://www.bakermckenzie.com/en/insight/publications/2018/10/french-data-protection-authority-issues-guidance

Blockchain blog: http://blockchain.bakermckenzie.com/

CLE/CPE Attendance Code: AVA73R10

Baker McKenzie.