Blockchain and Law with a focus on Data Protection and Anti-Money Laundering

Distributed ledger technology (DLT) has great potential and is increasingly being used in different industries. Many legal challenges in connection with DLT do not differ from already known ones in the field of information and communication technology (ICT). Some other challenges, though, are inherent to the design of certain DLTs and raise specific legal questions. The authors aim to show in an extremely succinct overview how DLT can be embedded into the existing legal framework for data protection and anti-money laundering (AML), two concepts of high relevance for banks.

by Alisa Burkhard, Boris Inderbitzin, Leandro Lepori and Raj Unny

Introduction: DLT and Blockchain

DLT can be categorised into: (1) permissioned, private shared ledger (technology is owned, participants are limited and known, i.e. BankChain); (2) permissioned, public shared ledger (technology is owned, validation through known and trusted validators, everybody can participate, i.e. Ripple); (3) unpermissioned, public shared ledger (technology is open source, the public can participate and contribute to the validation process through a consensus mechanism, i.e. Bitcoin). A blockchain is a specific form of a DLT and is a digital data structure (ledger) in which records are organised in blocks that are cryptographically sealed and time stamped, replicated, distributed, and synchronised over a peer-to-peer network, and often maintained by a consensus algorithm. Blockchain technology is often used as a status transition machine, whereby a certain «thing» represented by a cryptographic value within the blockchain («token» / «coin») is given a status. The legally most challenging combination is an unpermissioned, public blockchain, which is the type of DLT that the following overview refers to (hereinafter called «Blockchain»).

Blockchain and Data Protection

Blockchains are designed with a high level of transparency, which ensures trust in the system. However, this transparency also makes it challenging to comply with data protection and professional confidentiality requirements (i.e. banking secrecy, duty of confidentiality of medical personnel, etc.). While the following comments focus on General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) because of its broad applicability, the concepts are equally applicable to any professional confidentiality requirement. Blockchain's transparency may be incompatible with data protection, as Blockchain is not anonymous but pseudonymous. This means that a person is represented in the system by a public key or the cryptographic address derived from it (i.e. a «Bitcoin address»). Depending on the dataset, data triangulation and data analysis technology can be used to guesstimate the identity of a person behind a pseudonym. The GDPR defines personal data as any information relating to an identified or identifiable natural person. Furthermore, public keys result from pseudonymisation methods and are therefore qualified as personal data in accordance with the opinion of the Article 29 Working Party (05/2014 – WP 216) on anonymization techniques. Adding data to a Blockchain is the result of performing significant computation on certain cryptographic calculations. Once data is written on a Blockchain, replacing it requires a prohibitive amount of computing power, essentially making editing or deleting personal data impossible. Moreover, the dualistic categorisation by the GDPR of data processors into Controllers and Processors raises the following issue: There is no Controller in a Blockchain. Therefore, many of the rights individuals are granted towards a Controller cannot be addressed (and enforced), as Blockchain technology is not controlled by any centralized entity. These tensions between Blockchain and data protection result in the following challenges: Irrefutability of the Blockchain vs. right to rectification (Art. 16 GDPR); immutability of the Blockchain vs. right to erasure («right to be forgotten», Art. 17 GDPR); right to object (Art. 21 GDPR); automated individual decision-making (Art. 22 GDPR).

It is very important to note that Blockchain is an underlying technology. On the application level, responsible Controllers and Processors can be identified. At this stage, the challenges of enforceability are the same as in any potentially international ICT environment: Unknown provider, alien jurisdiction, applicability of regulations, conflict of laws and many more. «Data protection by design and default» is crucial when using DLT. Blockchains can grant more privacy only if the data architecture is designed accordingly. Strong pseudonymisation techniques can be employed as well as data minimisation or keeping personal data on off-chain data storage, transferring only the key to the personal data in the Blockchain. Finally, a Data Privacy Impact Assessment (Art. 35 GDPR) is a must for Blockchain-based utilities.

«Data protection is crucial when using DLT»

Cryptocurrencies on the Blockchain and AML

Financial market supervisory authorities in all OECD countries and beyond have long made AML a top priority. Money laundering can generally be defined as an act that is aimed at hiding, concealing or disguising assets resulting from a criminal act, whereby the definition and the relevant criminal acts vary depending on jurisdiction. Compared to exchanging one legal currency (CHF) into another (USD), exchanging legal currency (CHF) into virtual currency (such as Bitcoin), potentially combined with further exchanges into other currencies or the use of mixing services, creates a similar potential for concealing assets' origin, if not an even greater one. Blockchains that make use of pseudonyms make it difficult to link transactions to an individual and to trace the origin of the assets because, while every transaction is traceable through a pseudonym, the keys and thus the transactions are not tied to anyone's identity. Moreover, even if a cryptocurrency can be linked to a wallet, this wallet can be transferred from user to user without it being possible to identify the origin of the assets or their beneficial owner. These factors, and cryptocurrencies' transfer speed and usability across currency lines, make cryptocurrencies attractive for illicit activities such as money laundering. However, paper money is no different. In fact, its path is completely untraceable, unlike the public record that transfers on the Blockchain leave behind. One would have expected paper money to be outlawed. Instead, legal frameworks were developed to help financial institutions identify and mitigate risks from cash transactions. Comparing them can be useful to identify best practices and ideas on how to adapt existing regulations to the realities of new technologies. For example, existing OECD AML regulations generally require banks to supervise a business relationship – including its transactions – in a risk-oriented way, and retailers are generally required to observe certain due diligence obligations when accepting cash. Other favored methods of money laundering, such as real estate transactions, are counteracted by best practice guidelines published by professional organizations. The same principles apply to analyzing the risks related to cryp-

continued from page 35

tocurrency transactions. Applied to Blockchain technology, AML implies Know Your Customer (KYC) processes and, at times, conducting due diligence on the origin of the assets by tracing transactions – or requiring the bringer of the funds to furnish such proof. The challenges lie in (i) the early (company-level) implementation of high KYC / AML standards and (ii) the ability to understand the technology underlying the Blockchain in order to be able to identify the origin of the assets. When implementing a Blockchain-based business, a company should thus work with KYC / AML tools even when raising private funds.

«A commitment to best practices, transparency and compliance will make the difference.»

These tools can, for example, include an application programming interface (API) integrated into the registration process on a website, into which customers enter their basic personal information. Online fraud management and AML scanning tools can undertake background checks and document whether a source of funds seems plausible. After this, the usual precautions apply for a bank when choosing whether to accept a company dealing with cryptocurrencies as a business partner: Examining whether or not there is reason to suspect that transactions or funds may have a connection to illicit activities. This risk analysis is no different than the one conducted for a company that runs a cash or otherwise high-risk business – other than that it is new. Adaptations of existing legislation and new layers of AML compliance will be a boon for banks and allow them to make such decisions more easily. An example is the upcoming amendment of the 4th EU AML Directive (2015/849), which will explicitly make virtual currency exchanges and custodian wallet providers subject to existing AML obligations in all implementing countries.

Conclusion: It's Doable

Understanding Blockchain enables comprehension of its potential and challenges and mitigation of its risks. It is important to understand the tools at hand before initiating or evaluating a Blockchain-based project. We recommend that both project developers at company level and their financial partners, such as banks, involve technical and legal experts from the beginning to ensure correct implementation of regulatory requirements in Blockchain applications. Furthermore, a commitment to best practices, transparency and compliance already at company level will make the difference for financial institutions – and create the most sustainable Blockchain businesses.


© sdecoret – Fotolia.com