*Swiss Chinese Law Review*, Volume 1, Issue 1, 2020.

Gunka, Charlotte, 'Upgrading Regulatory Compliance Information Sharing with Blockchain', pages 36-8.

Charlotte Gunka

# 'Upgrading Regulatory Compliance Information Sharing with the Blockchain's Distributed-Ledger Technology'

Covid-19 exposed the private and public sectors' pressing dependence on new technologies to process information faster at lower costs while maintaining sufficient trust. This has been particularly true for organisations that continuously monitor their customers' and third parties' activities for regulation compliance. Notably, standards set to combat money laundering, terrorist financing, fraud and corruption require increasingly sophisticated systems to enforce. How should lawyers consider blockchain and distributed ledger technology (DLT) as a solution in this race for confidence?

Alongside DLT, blockchain has attracted considerable attention in recent years as an innovative and secure software for gathering and sharing information. Several key economic stakeholders, including the World Bank and J. P. Morgan have trialed its application. The World Economic Forum released its own blockchain deployment toolkit in May 2020. It noted that, if there were still doubts over the value of blockchain's DLT, the Covid-19 crisis eradicated them.

Evidently, certain technological and practical improvements must be consolidated to make blockchain's DLT a fully operational tool. I will explore legal considerations that currently circumscribe and enhance the blockchain and DLT as a due diligence data-sharing platform.

## Blockchain DLT as a Tool for Efficient Regulatory Compliance Information Sharing

While the terms blockchain and DLT are often used interchangeably, they refer to separate but complementary software. The blockchain is a computer program that uses an algorithm and cryptography to record information in a highly secure and structured sequence of data "blocks", which all relate to each other in an unalterable logical relationship. In turn, a distributed ledger or DLT describes a specific type of database that allows information to be accessed and shared in synchronicity within a computer network. This could be located across multiple sites, without the need for a designated managing party. A distributed ledger will generally consist of clustered registers, maintained private or public by the participants located at each "node" of the network. No new data "blocks" can be added to the network without all nodes instantly registering the same changes. Because the DLT ledger is replicated simultaneously across many individual computers this transparency and credibility is increased. Any local attempts to manipulate the ledger are quickly exposed.

In contrast, traditional databases are structured as centralised platforms, or decentralised in complex guarded networks. They require an administrator's approval to be shared between different users. Within a group of institutions, stored information is generally managed by a single user who authorises others to access a unique server. However, blockchain's DLT can create a shielded peer-to-peer network without intermediaries, built upon a consortium of several users. They share their knowledge by default to facilitate consulting the information registered by each user.

The instrumental features of blockchain's DLT stand out in the mandatory information exchange by financial institutions for the purposes of *anti-money laundering and combating the financing of terrorism* (AML/CFT for short). Its unmodifiable and encrypted nature offers traceability and security

for exchanging sensitive data within financial groups with complex interconnectedness. Notably, this is also true regarding customer due diligence (CDD) obligations and third party verification. The Financial Action Task Force (FATF, who set international standards for AML/CFT) repeatedly reminds private and public organisation – most recently during the pandemic – that effective information sharing is a cornerstone of a well-functioning AML/CFT framework. In the European Union (EU), the May 2018 Fifth Anti-Money Laundering Directive (5AMLD)[1] introduced enhanced CDD requirements for entities dealing with high-risk countries. It also regulated information sharing within group financial institutions, with financial institutions in different groups, and between AML/CFT-competent authorities.

Blockchain's DLT is a cost-saver for group financial institutions who are likely to face greater regulation. In France, the sum of all fines imposed by the banking regulator multiplied by a factor of fourteen in two years – from €4.9 million in 2016 to €70 million in 2018. The consulting firm McKinsey & Company estimated in June 2019 that blockchain's DLT-based solutions for customer identification could create up to $1 billion worth of savings in operating costs for retail banks globally. What is more, it could reduce regulatory fines by $2-3 billion and lower annual losses from fraud by $7-9 billion. Despite the initial costs associated with switching from a centralised system to DLT, increased AML/CFT regulation and the growing risks of fines calls for speeding up its implementation. In the long-term it will effectively prevent money laundering, terrorist financing and similar criminal activities.

That said, implementing a blockchain DLT, within financial institutions and other organizations, must comply with the numerous domestic laws and regulations that regulate information exchange. At the same time it should contribute to safeguarding individual rights and public interests.

**Domestic Laws as Practical Safeguards to Blockhain's DLT-based Information Sharing**

For the purpose of AML/CFT, financial institutions must assess a number of factors to decide whether a blockchain can be adopted at group level. FATF's guidance expects countries to impose and monitor financial groups' information exchange policies and procedures to prevent money laundering and terrorist financing. This covers the parent company, branches and majority-owned subsidiaries, domestic and foreign. This monitoring includes data related to customers and beneficial owners identification (KYC information), and account and transaction monitoring. The latter covers suspicious transaction reports (STRs) and enhanced CDD analysis. Considerations should also include elements such as products and services, location, existing legislative and regulatory frameworks, the confidentiality and sensitivity of any shared information and other risks and context.

Overall, countries have similar definitions of KYC information but even within the EU countries differ over STR sharing. In France, for example, STRs are confidential and their disclosure is forbidden under Article L. 561-18 of the French Monetary and Financial Code except to the state's financial intelligence unit (FIU). However, the STRs' underlying data and the fact that it has been submitted, may be revealed under conditions of strict confidentiality to group entities located in countries that are not provisionally considered by the EU as high-risk jurisdictions. In contrast, in the United States, banks (including foreign banks' US branches) can share STRs, but only with their

[1] Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018, amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. The 5AMLD should have been transposed into all EU member states' national laws on January 10, 2020.

parent entity, whether located in the US or abroad.[2] In other countries, exchanging STRs-related information may be subject to prior approval by domestic FIUs or, in some cases, forbidden.

Bank secrecy rules for protecting clients' privacy in certain jurisdictions may further constrain the implementation of a blockchain DLT. Although the FATF requires countries to ensure that bank secrecy laws do not inhibit their AML/CFT standards, certain jurisdictions remain extremely restrictive. Even a legitimate interest, security concerns or client's express consent may not allow certain banks to unveil a financial secret. According to the 2020 Tax Justice Network's Financial Secrecy Index, the ten top-rank countries in this regard are, unsurprisingly, the Cayman Islands, the US, Switzerland, Hong Kong, Singapore, Luxembourg, Japan, Netherlands, the British Virgin Islands and the United Arab Emirates. In Switzerland, the Tax Justice Network reported in 2020, each current and prospective client could have to consent to a data transfer to a foreign group entity, depending on the recipient entity's jurisdiction.

Furthermore, specific trade and state secrecy laws intended to protect states' interests could also prohibit cross-border information transfers between group entities. In both France and Switzerland, governmental approval is required before any evidence or sensitive information can be transferred out of the country, notably in the context of a criminal proceeding.

However, such privacy and data protection laws might actually be compatible with blockchain. One example is the EU's General Data Protection Regulation (GDPR). It imposes strict rules on collecting, processing, storing and transferring personal data by organisations located in the EU, and beyond, if they offer goods or services to persons in the EU. While some issues remain, the European Parliament has encouraged the use of blockchain DLT solutions on the condition that they are private and require permissions to access (as opposed their public default setting) for group-wide information sharing. Specific concerns over the eternal nature of blockchain data could be addressed by encryption techniques which make registered information virtually inaccessible after a certain time. Numerous safeguards would nevertheless need to be introduced, including the adoption of binding corporate rules, a prior data protection impact assessment shared with relevant regulators and the designation of a data controller who can attest of the lawfulness of any data processing (such as AML/CFT and CDD). Informing the client about their rights and the purpose of the blockchain DLT would also be necessary in contract clauses.

Despite the financial sector's specific conditions, legal constraints regarding implementing a blockchain DLT-based information sharing system could be overcome. Common sense does not call for blockchain to be used systematically where traditional, and perhaps more flexible, solutions are available. Yet, it could, if designed to comply with the relevant legislation, represent an efficient tool for transparency within group organisations. Beyond AML/CFT obligations, companies across the board are now subject to heightened anti-corruption regulations. In response to the Covid-19 crisis, the Network of Corruption Prevention Authorities issued a statement on 11 May calling upon regulators and private entities to strengthen their internal anti-corruption measures. Blockchain presents an optimal means of storing transparent and accurate databases to this end.

---

[2] FinCEN, "Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates", Guidance (FIN-2010-G006), November 23, 2010.