MME

Export control and digitisation – Operational opportunities and challenges using Blockchain and Smart Contracts as examples

Prof. Dr. Andreas Furrer, LL.M. and Peter Henschel, MME Legal | Tax | Compliance

(Tentative Translation of our essay in Schulthess Manager Handbuch 2018/2019, p. 105 pp.)

Introductory remarks

In 2017 and 2018, two important topics arrived at the management levels of Swiss companies: the growing challenges in the area of sanctions and the opportunities and challenges of the blockchain. At first glance, these two topics have little to do with each other. On closer inspection, however, it becomes clear that both topics have an important common denominator: structured processes with defined decision parameters.

The digitisation of businesses is progressing. In Switzerland, Swissmem and SwissT.net have, with the support from the industry, launched an initiative called "Industry 2025" in order to jointly address the issues of digitisation and networking along the value chains. Efforts to organise and control these processes ("Industry 4.0" or "Intelligent Factory") are to be strengthened and coordinated in course of the initiative. In the following, we will pick out the blockchain technology as a current example that covers all these questions and represents an important element in this development due to the so-called Smart Contracts.

On the one hand, we will highlight some important cornerstones of operational and personal responsibility for compliance with sanctions and export controls and demonstrate that the global risk profile in this area has increased considerably. On the other hand, after a brief introduction to the blockchain technology and Smart Contracts, we will discuss the opportunities and risks of digitisation and its potential for an efficient arrangement of export controls.

Organisation and development of export controls

Function of export control in world trade

The term export control is used very differently in practice. In essence, its aim is to use internal processes to ensure that a company complies with all applicable and relevant legal requirements in cross-border trade.

Export control forms part of an overall trade compliance strategy which, in addition to compliance with export and import restrictions, also covers other issues such as compliance with customs and tax regulations, quality and safety standards (such as dangerous goods regulation or CEN standards) or other regulations which may be relevant for the cross-border transport of goods. For the following explanations the export restrictions (economic sanctions and embargoes, regulations for dual-use goods and armaments) will be selected as an example, because the question of the interface between compliance and digitisation can be well represented due to the following factors.

Economic sanctions are used, on the one hand, to fight political conflicts with non-military members in which the sanctioning countries make it more difficult or even impossible for the sanctioned country to gain access to economic and technical resources. On the other

hand, economic sanctions restrict the economic and political freedom of action of persons or organisations below the state level. Dual-use and arms regulation also aims to control and restrict access to military know-how and goods for the production of bio-, chemical- and nuclear weapons.

The USA and the EU in particular, but increasingly also other trading powers such as Russia or China, derive the claim from this overriding objective to apply their own control laws also extraterritorially, i.e. also to actions and processes outside their national territory.

In particular, US re-export law, but also US sanctions have always relied on an extraterritorial effect in the sense that the US authorities responsible for implementing these trade barriers (such as OFAC, BIS, DOJ) have already declared themselves responsible even in the case of a loose link to the USA. It is sufficient if, for example, a payment is made with USD or if US banks, US companies or US citizens are involved in the business. In appropriate cases, they may also impose their domestic sanctions against foreign companies and persons.

The corresponding application requirements are broadly defined in each case. However, they can only (but at least) be enforced in one's own territory. For this purpose, they can, for example, impose fines, import barriers or prohibit business relations with the sanctioned companies if they have a connection with their own state territory.

Moreover, through its central influence on the global financial system, the USA is also in a position to (indirectly) enforce its punishment of foreign companies abroad. By listing a company in a US sanctions list, a company can lose access to the global financial system and the market within days because no bank or business partner will dare to be on the sanctions list itself.

In 2018, for example, despite the support of the Chinese state, the Chinese large corporation ZTE was forced to cease production within days because foreign business partners of their supply chain refused to supply the company any further since it had been listed on a US sanctions list.

In Switzerland, too, OC Oerlikon (formerly Oerlikon-Bührle) had to defend itself against such sanctions because the US authorities placed its former majority shareholder Victor Vekselberg on a sanctions list due to its relations with Russia. As a result, OC Oerlikon saw its worldwide business relations concretely threatened.

This shows that Swiss companies must also inform themselves about these foreign regulations and take them into account in their business activities.

Export control - responsibility in the company

Every company must organise itself in such a way that it is in a position to comply with the legal framework and to ward off recognisable and avoidable dangers for the company.

This responsibility initially only refers to compliance with Swiss export control and embargo law. Swiss legislation contains a number of criminal sanctions for misconduct, providing for a maximum sentence of 10 years imprisonment combined with sensitive fines.

Since (also) Swiss criminal law in principle sanctions the misconduct of persons and not of companies, the threat of punishment under export control law is directed against those persons who bear the corresponding decision-making and organisational responsibility for the company. According to Art. 102 of the Swiss Penal Code (StGB), the company can only be punished on a subsidiary basis.

A violation of foreign export control law does not directly lead to punishment of the persons responsible for the decision in Switzerland, but it could result in punishment in the state with the corresponding provisions. However, since at least the management bears overall responsibility for the company, they also have the obligation to minimise identifiable and avoidable operational risks. This, in turn, entails the obligation to examine the foreign export control law for corporate risks and to establish appropriate control and decision-making structures in one's own company.

Responsibility of the Board of Directors and the Executive Board

The overall responsibility of a company is one of the non-transferable and irrevocable duties of the Board of Directors (Art. 716 Para. 1 Sections 1 and 2 of the Swiss Code of Obligations, OR, similar to other legal entities). Although these tasks can be delegated internally to individual members of the Board of Directors (or, for example, to an Audit Committee), and in accordance with Art. 716b OR, the Articles of Incorporation may authorise the Board of Directors to delegate individual tasks to the Executive Board by means of organisational regulations. Nevertheless, the overall responsibility is always ultimately focused on the Board of Directors, which is responsible for an appropriate structure of the organisation.

On the one hand, a corresponding organisational structure should include the internal management structure in the Board of Directors and in the Executive Board. On the other hand, an internal compliance program ("ICP") should be established and approved by the Board of Directors. This ICP, which is described in more detail below, must contain the rules for internal processes with regard to information and decision-making responsibility. The Executive Board and the Board of Directors must be kept regularly informed of developments.

For Swiss (and even more so for European) companies, this means that it is not just a matter of complying with the legal requirements of Switzerland, the EU and the USA, but of finding a way out of the dilemma if these legal requirements contradict each other.

Responsibility of the Compliance Officer

For day-to-day business and the examination of individual questions, a person within the company must make the relevant decisions. The Compliance Officer, who can also perform other operating functions depending on the work involved, is responsible for implementing the ICP decided by the Board of Directors in day-to-day operations and, in specific individual cases, for deciding whether a transaction can be approved.

It is therefore his task to ensure that the processes and procedures in the company are lived in such a way that possible violations of Swiss or extraterritorial export control law are detected at an early stage and prevented. For this purpose, he must have an overview of the company from purchasing to product development and manufacture through

to sales and train and sensitise the responsible persons accordingly, as well as implement systemic tests if possible.

The Compliance Officer thus bears considerable responsibility and is fully subject to the criminal provisions of export control law. It will therefore involve the Executive Board or the responsible Board of Directors in the decision-making process in delicate business decisions . However, this integration does not relieve the Compliance Officer of his criminal responsibility. This also repeatedly leads to the termination of Compliance Officers if the Executive Board or the Board of Directors instructs them to nevertheless approve or support sensitive business transactions.

ICP as an instrument for the perception of responsibility

The ICP provides a good framework for regulating and documenting compliance tasks within a company. For example, when applying for an export permit at the State Secretariat for Economic Affairs (SECO), but also when applying for re-export licenses from the American authorities, it is expected that the company has created and implemented such a documented ICP. Larger companies increasingly require their supply chain business partners to have such an ICP.

Although authorities have not precisely defined the content of an ICP, the following elements are usually considered to be a mandatory part of an ICP:

- Management commitment and policy statement on export controls and sanctions;
- Definition of roles and responsibilities to ensure compliance in export controls and sanctions;
- Authorisation requirements: classification of the goods, software and technology to be exported according to the regulations on the control of dual-use and certain military goods;
- "Know your customer" ("KYC"): verification of end user and end use (catch-all clause for non-controlled goods, software and technology, if necessary);
- Training and information for those involved in trade;
- Internal audits.

In principle, most of these elements of an ICP also make sense for companies that are not active in the field of dual-use or military goods and should be formalised in order to ensure compliance with strict export control requirements.

Many companies also have a comprehensive Compliance Management System ("CMS"), which should ultimately include the elements of an ICP. This enables internal structures to be implemented in a lean, efficient and cost-effective manner.

Operational opportunities and challenges of Blockchain and Smart Contracts

Blockchain and legal transactions via Smart Contracts

This is not the place to explain the Blockchain technology in detail. For these purposes, it is sufficient to note that in industrial applications, the blockchain offers the possibility of storing, supplementing and transferring information (data or code) using a very sophisticated cryptographic encryption technology. This data is stored on a decentralised database (the so-called "ledgers"), be it on public or private blockchains. The high security

standard is guaranteed by the fact that the control and verification of the individual entries on the ledgers are carried out by neutral testing bodies ("miners") (which are designed differently depending on the selected protocol). There are still some technical obstacles to overcome for wide industrial applications, such as limited data throughput and high energy consumption.

Blockchain technology is both over- and underestimated today. Some see it as a saviour for any problem, others want to dismiss it as mere hype. The years 2016 and 2017 were marked by the high flight of the Bitcoin and the raising of capital with the help of blockchain technology via so-called Initial Coin Offerings (ICOs, also known as Token Sales or Token Generation Events, TGE). The public discussion focuses on Bitcoin and "crypto currencies", although the industrial application of blockchain technology in connection with business process digitisation is in the foreground.

Of particular importance for industrial applications is the possibility of activating programs on this decentralised blockchain (Smart Contracts), which automatically trigger corresponding processes on the basis of the supplied data and thus generate new transactions. For example, payments can be initiated automatically, information, offers or reminders can be sent, or an almost unlimited number of other actions can be triggered.

In all legal systems, many questions of digitisation are controversial and unresolved, such as in the area of financial market regulation (e.g. "When is a token a security?"), data protection (e.g. implementation of the "right to oblivion" according to the new General Data Protection Regulations of the EU) as well as private law implementation (e.g. transfer of property, claims and data). The underlying transactions of smart contract systems must comply with the applicable regulations. However, the Smart Contracts must also be programmed in such a way that the transactions they trigger are legally binding.

Regulatory authorities around the world are intensifying their efforts to qualify the new blockchain functions such as Smart Contracts, wallets and tokens within their existing regulatory framework. For these purposes, but also with regard to the legal relevance of automated actions of Smart Contracts, the discussion about a generally recognised classification of the different types of tokens will gain in importance, as MME has developed with its "Conceptual Framework for Legal and Risk Assessment of Crypto Tokens" (https://bit.ly/2takE5a).

Compliance is technology-neutral

Blockchain technology is used today to develop many new and innovative business solutions and applications. Its potential cannot yet be determined.

Most compliance regulations are basically technology-neutral and must also be taken into account in this new field. Since the export control rules apply to all types of business processes, they also apply to transactions executed on the blockchain. The operational compliance processes and systems must ensure compliance with the relevant regulations, regardless of the technical means used.

In many companies, the potential of blockchain and Smart Contracts is currently being assessed intensely or tested on first prototypes for their own business area. The responsible Compliance Community should closely accompany these internal discussions and projects at an early stage. If used properly, this technology also has great potential for

simplifying internal export control processes so that they can be made more efficient and partially automated. This new technology can thus be used to consistently implement the "Compliance by Design" concept.

Until now, the Compliance Officer's work often focused on sensitising the persons responsible for the compliance processes so that the compliance-relevant transactions could be identified and fed into the compliance process. The compliance officer should now extend his control to the planned blockchain-based processes. In the context of the digitalisation of business processes, decisions based on predefined parameters are increasingly being made automatically. For example

- letters of credit via Smart Contracts without the involvement of banks,
- payments made automatically in the event of certain occurrences (e.g. freight has left customs), or
- compensations because the temperature-controlled freight has exceeded the defined temperature.

The Compliance Officer must therefore ensure that the corresponding transactions cannot be executed without a prior compliance check. Whether these transactions will be fully automated, or ultimately require manual support from the compliance officer, will be one of the key questions.

New Compliance - Challenges due to the Blockchain

The blockchain technology in its various applications also creates new challenges in the area of export control, since the coins or tokens to be transferred can be valuable in each case. These values are transferred with a transaction on the blockchain, which is equivalent to a relevant provision from the point of view of export control.

Both the American authorities (US Office of Foreign Asset Control, OFAC) and the Swiss SECO have confirmed that transactions with crypto currencies or the use of tokens (e.g. in Smart Contracts) fall under US and Swiss sanction and embargo law. In response to questions from the authors, SECO emphasised: "Crypto currencies or digital information units with possible intrinsic value are to be regarded as money or economic assets with regard to sanctions. The prohibitions laid down in the ordinances (in particular prohibitions on provision) must be complied with accordingly".

The US OFAC has already announced that in the near future it will place blockchain addresses (unique alphanumeric identifiers known as public keys or wallets) on Specially Designated Nationals ("SDNs"). According to OFAC, this is to inform the public about certain public keys assigned to a sanctioned person. The entry in the sanction list will also contain an indicator of the corresponding sanctioned crypto currency.

Accordingly, not only the verification of the wallet addresses involved is relevant for companies that want to use open blockchains. In many cases, a KYC process must also be implemented to ensure that the persons involved and their wallets are not sanctioned.

Export control and Smart Contract Design

Sanctions and embargo checks will probably establish themselves as a standard function within Smart Contracts on public blockchains. KYC processes are already being used in

many blockchain projects, especially when exchanging crypto currencies for fiat currencies.

Many companies today suffer from the abundance of compliance requirements, because these are often still implemented by manual processes, which are based on paper documents. So far, automation has often failed due to insufficient system integration or incomplete master data.

Blockchain technology requires that business processes are digitised so that they can run automatically via the blockchain. Several companies are currently working on digitisation and blockchain solutions for all types of documents used in logistics transport. These will not only be the basis for sanctions and embargo screening of recipients and end-users, but also, for example, for the control of export licences. Compliance managers would have to integrate the corresponding rules and audit steps into the Smart Contracts used.

By securely and unalterably recording transaction data on the blockchain, compliance officers or auditors can easily perform a subsequent audit of the transaction. The blockchain also ensures that all parties can be identified and that all relevant data (e.g. end user information, classification and licensing) is available and documented at all times.

The compliance officer should concentrate on skilfully integrating his control tasks into the digital processes and the design of Smart Contracts. This enables him to design many tasks more efficiently and thus to initiate the compliance tasks even more deeply in operations and also in the end-to-end processes. Ultimately, this also gives him the opportunity to focus on the core tasks of controlling and auditing.

Conclusions and recommendations for action

The digitisation of internal company processes offers the potential to partially automate the fulfilment of increasingly complex compliance requirements. These simplifications also make it possible to introduce stricter standards, especially since export control law per se knows no value limits.

Blockchain technology also expands digitisation by integrating third parties into business processes. Thanks to Smart Contracts, third parties in a supply chain can be directly integrated into internal business processes beyond the (system) boundaries of the enterprise system. Compliance checks can then also be integrated and automated across these company boundaries. The increased compliance risks that may arise as a result can be avoided and (partially) automatically controlled by neatly integrating the specifications into the corresponding Smart Contracts.

However, the ultimate responsibility for risk decisions will remain with the Compliance Officer, the Executive Board and ultimately also the Board of Directors.

"Compliance by smart contract design" will present companies with exciting challenges in the coming years, but also has the potential to meet the increasingly complex requirements in a smart way.

Key messages

- The Board of Directors, Executive Board and the Compliance Officer are jointly responsible for ensuring compliance with domestic and relevant foreign sanctions and export control provisions.
- The digitisation of operational processes allows efficient integration of export control, but the corresponding measures must be taken early and systematically.
- Blockchain and Smart Contracts hold great potential for the efficient design of export control, including the behaviour of business partners.
- Compliance officers face a major task when their companies have to adapt to the new digital challenges and introduce appropriate measures.