Smart contracts, blockchain and export control compliance



Export control compliance professionals would be well advised to investigate the potentially significant compliance benefits that blockchain technology can offer, write Prof. Dr. Andreas Furrer, Peter Henschel and Chris Gschwend.

The years 2016 and 2017 were dominated by the hype of Bitcoins and the large amount of capital raised via blockchain technology in initial coin offerings ('ICOs'), also known as token sales or token generation events ('TGEs'). While public discussions focus mainly on Bitcoin and 'cryptocurrencies', the compliance community responsible for export controls should take a closer look at the real potential of blockchain technology in business process digitisation and the important role of compliance officers in such blockchain projects. This article will give a high-level overview of the impact of blockchain-enabled business processes on the role of compliance managers and officers.

Blockchain beyond Bitcoin: impact on international trade

More and more established businesses are now considering blockchain technology (also known as distributed and decentralised ledger technology, or 'DLT') to improve their business processes. Blockchain technology uses cryptography, a type of random computer-generated and unbreakable code, to ensure that transactions remain private and secure. Enterprises should consider this technology to safeguard the integrity of business processes or to store data in a manner that cannot be changed, stolen or otherwise compromised by malicious software or third parties.

Another key benefit of DLT in the context of compliance management is the opportunity to automatically perform complex business processes and contractual commitments via smart contracts, a software that defines a set of orders in computer code and automatically enforces those obligations, triggered by external data sources (so-called 'oracles').

To illustrate how smart contracts can apply in the context of international trade and compliance management, imagine that a ship arrives into port, after which the container is discharged and carried to the buyer's warehouse. The parties agree that the first portion of the payment from buyer to seller is automatically triggered when the ship arrives at the port (e.g., via GPS information), and the payment of the second portion when the goods are delivered, timely and undamaged, at the warehouse (scan and goods-in check by the officer at the ramp of the warehouse). In this case, the payment between buyer and seller is realised peer to peer via a smart contract system. The smart contract transacts the blockchain-based payment of goods after being triggered by oracles (GPS data and goods-in scan info). In such smart contract-based letter of credit systems, the need for trustees as intermediaries (insurances/banks) can be eliminated.

Currently, blockchain protocols such as Ethereum provide the ability to deploy such smart contracts in a secure and transparent way. The setup of these smart contracts allows a high degree of integration and automation, which may render intra-company interfaces and communications obsolete, or at the very least greatly minimised. These smart contracts will be increasingly triggered by blockchain-enabled smart devices (Internet of Things applications serving as oracles) and potentially controlled by artificial intelligence without any human interaction. We are looking at a future where integrated hardware and software will allow any inter-company transactions to be fully digitised and automated, running on decentralised blockchain systems. However, certain legal and compliance boundaries will continue to exist in automated decentralised transactions.

Legal transactions via smart contracts

While blockchain technology advances, many new and innovative business solutions and applications are being developed. At the same time, regulators around the world are increasing their efforts to qualify the new blockchain elements, such as smart contracts,

wallets and tokens, within their existing regulatory framework. In all legal jurisdictions, many questions remain regarding financial market regulations (e.g., 'When is a token a security?'), data protection (e.g., implementing the 'right to forget' under the EU's new General Data Protection Regulations), as well as the transfer of title, claims, and data. While the underlying transactions of smart contract systems must comply with applicable regulations, the binding effect of the smart contract's execution must be analysed and safeguarded under the applicable law. Similarly, for transactions facilitated by decentralised groups of individuals (e.g., blockchain-based decentralised gambling or money-exchange sites) the applicable jurisdiction and laws must be established.

Faced with such uncertainty and unanswered questions, export control compliance administrators would nevertheless do well to remember that trade, customs and export control compliance is very often technology-neutral. Compliance managers are used to dealing with a multijurisdictional setup in which certain local requirements as well as multinational and even extraterritorial rules must be followed. Wherever and however a transaction takes place (triggered by individuals or by an oracle, recorded on the blockchain or in a cloud) compliance processes and systems must ensure adherence to relevant regulations, regardless of the technological means applied. As the same rules and regulations will continue to apply to business processes executed on a decentralised smart contract system, compliance administrators must ensure that the new business processes remain compliant. Compliance may even become more automated, with controls being integrated into smart contract systems.

Smart contract transactions enable 'compliance by design'

Today many compliance officers struggle with the variety of tasks that must be completed to ensure compliance, often due to lack of resources, lack of process integration, lack of system support or poor master data. In addition, the threat of fraud in paper-based systems puts even the most robust compliance management system at risk of mis-declaring or transacting illegally. Blockchain technology and the ability to automate business processes on the blockchain will allow compliance officers to integrate rules and checks into the smart contract code, such as sanction screening or licence checks. Having all transactions securely recorded on the blockchain will allow compliance officers to easily perform post-transaction auditing. Even more, in a blockchain ecosystem with identified parties and availability of relevant data, such as end-user information, classification and licensing, the task of a compliance officer may become predominantly a role of process and smart contract design.

[Blockchain technology] will allow compliance officers to integrate rules and checks into the smart contract code, such as sanction screening or licence checks.

Compliance functions in a smart contract system

Sanctions and embargo checks will continue to become a standard compliance function within smart contract systems. KYC (here defined as 'Know your Counterparty') processes are already used by many blockchain projects, in particular those dealing with the exchange of cryptocurrencies and fiat currency (the latter being recognised by governments as legal tender). The 'on-ramping' of blockchain users (i.e., receiving crypto-currencies in exchange for fiat), or the 'off-ramping' from cryptocurrencies back to fiat, requires blockchain-based exchange operators to establish relevant KYC processes, which aim to identify individuals or entities that may be sanctioned or may represent an elevated risk for money laundering. In the future, to the extent that the underlying business process requires a KYC check, such KYC processes must also become a standard function in smart contract execution.

Blockchain may also enable innovative KYC solutions, e.g., self-governed identity, which will allow fully automated self-identification and whitelisting for frictionless b2b and b2c transactions. The integration of technologies such as zero-knowledge proof and cryptography will bring the privacy elements needed to protect personal and corporate information recorded on DLTs.

Several companies are currently working on the digitisation and blockchain solutions for all kind of documents used in logistics transport-ation. These will be the basis for not only sanctions and embargo screening of consignee, end-user and end use, but will also allow export licence checks/ management as a smart contract function. Trade and export control compliance could be ensured by smart contract design and compliance managers should play an active role.

Summary and recommendation

The technology surrounding blockchain and decentralised smart contracts is still not yet at a stage where traditional companies can easily realise blockchain-enabled business processes or full blockchain-based business models. However, the technology has shown very promising use cases and is here to stay. We will see more and more business-ready solutions being developed, and it's only a matter of time before we see large-scale adoption of certain elements of blockchain technology and smart contracts, chief among those being the ability to run software code on a decentralised system and ensuring the integrity of shared data.

If a company considers improving its business processes based on blockchain technology, its compliance managers should be involved from the onset to ensure the integration of trade controls into smart contract codes. This is a unique opportunity for enterprises to integrate compliance by design right from the initial design phase, ultimately reducing legal and financial risks, as well as the cost of compliance management.

Prof. Dr. Andreas Furrer is a legal partner at MME in Switzerland, where Peter Henschel is managing director of compliance and Chris Gschwend is a senior compliance advisor.

andreas.furrer@mme.ch
peter.henschel@mme.ch
christine.gschwend@mme.ch