CLIFFORD
CHANCE

# BLOCKCHAIN, TRADE FINANCE AND SANCTIONS ISSUES

— THOUGHT LEADERSHIP

MARCH 2019

# BLOCKCHAIN, TRADE FINANCE AND SANCTIONS ISSUES

Blockchain is the technology that underpins digital currencies such as Bitcoin – but it has far wider applications and is being used in a growing number of areas. Blockchain has the potential drastically to alter the global financial system. Trade finance is one of the areas likely to benefit from the technology first by becoming cheaper, faster and more accessible. However, developers and market participants should be mindful to consider the sanctions implications given the extraordinary reach of sanctions and the magnitude of the penalties for breach.

## What is blockchain?

- Blockchains are used to record data. They are digital ledgers of transactions, assets or agreements – anything that needs to be recorded and verified. Blockchains are distributed across multiple computers, and so are also referred to as distributed ledger technologies, or DLT.
- A blockchain is a special type of database in which the data is set out and built up in successive blocks. Each of the blocks of data includes a small piece of data that verifies the content of the previous block. Because each link in the chain verifies the previous link, the system is able to detect and reject any attempted unauthorised modification, making the ledger tamper-proof.
- It enables corporations, institutions and individuals to share information without the need to trust the other participants as it should be near-impossible for them to corrupt the ledger and introduce fraudulent transactions.
- Each participant in the system is uniquely identified and only authorised participants can make changes to the blockchain.

## How does blockchain help trade finance transactions?

Trade finance was invented by the Italian merchants of the Renaissance and remains to this day a cornerstone of the global economy. However, it is costly, unwieldy and slow. Paper contracts are manually created, reviewed, amended and exchanged. It often takes weeks for exporters to receive payments for their goods as numerous intermediaries must check that goods have been delivered to the importer before the funds are released to the exporter.

Blockchain technology addresses these shortcomings by digitising, optimising and shortening the trade finance process and making it more transparent, cost-efficient and accessible. In the short term, blockchain can be implemented under a single contract between direct stakeholders to the transaction: the exporter, the importer and the finance parties. Blockchain technology uses digitised ledgers of title and assists with execution and settlement, providing parties with real-time updates and greater visibility on the transaction, from the time the transaction is entered into, to the release of payment to the exporter. The automated settlement mechanism cuts out intermediaries, reduces transaction costs and streamlines the cash cycle. In theory, thanks to shared record-keeping, blockchain also mitigates the risk of fraud.

Self-executing chains with fully open ledgers which involve indirect stakeholders – for example the subsequent purchasers of the imported goods, the warehousing companies, the insurers, and the customs, port and rail authorities – have yet to see the light of day and remain a remote possibility as they would require a diverse group of people to agree on a uniform set of rules and standards. Interrogations surrounding governing law and enforceability of cross-border contracts, whilst also relevant to "closed blockchains" are particularly pronounced in the context of fully open ledgers.

Should blockchains be successfully implemented/gain traction in trade finance, the sanctions risks canvassed below would be all the more salient for the parties involved.

## What impact do economic sanctions have on blockchain and trade finance?

Economic sanctions laws and regulations are imposed by governments and multinational organisations to restrict business with certain persons, entities, governments, countries, or territories. Sanctions can include comprehensive trade embargoes or more targeted measures aimed at restricting business with specified groups or individuals.

The US Treasury Department's Office of Foreign Assets Control (OFAC) administers and enforces US economic sanctions. OFAC does not act alone and other US federal agencies and departments such as the Department of Commerce's Bureau of Industry and Security (BIS), the Department of State, and the Department of Justice are also actively involved in US sanctions and export control enforcement.

OFAC's jurisdiction-based sanctions generally prohibit "US persons" from directly or indirectly engaging in transactions involving individuals, entities, governments, or countries that are the target of OFAC sanctions, unless authorised under an OFAC license or exemption. US persons are defined as any US citizen, permanent resident alien, entity organised under the laws of the United States, or any person in the United States. In the case of OFAC sanctions against Cuba and Iran, the prohibitions also apply to non-US entities that are owned or controlled by US persons.

OFAC also prohibits US persons from approving, facilitating, financing, or guaranteeing transactions between non-US persons and sanctions targets where the transaction would be prohibited if performed by a US person.

Lastly, OFAC prohibits US and non-US persons from causing, aiding, abetting, or conspiring to violate any OFAC sanctions. OFAC has successfully brought multi-million dollar enforcement actions against non-US international banks and multinational companies on the basis that they violated OFAC sanctions by involving US persons or the US financial system in transactions with sanctions targets and thereby "caused" the US persons to violate OFAC sanctions.[1]

The implication is that blockchain technology owned or developed in the United States or by US persons is subject to US jurisdiction and may also be subject to US export controls depending on the technology used. Therefore, as a starting point, blockchain software (*i.e.* the code that the participants need to run in order to transact on a particular blockchain system) could not be sold to or licensed for use by sanctions targets (both current and future) without an OFAC or BIS license.

If blockchain is owned or licensed by a US person, OFAC may take the view that any transaction using blockchain which involved a sanctions target could trigger the facilitation prohibition. A US owner or operator may therefore either need to put in place controls to make sure that blockchain could not be used for transactions with sanctions targets, even if such transactions would be permissible within the default rules of the blockchain system. For example, a US-owned or licensed blockchain could not be used by a non-US bank or exporter for an Iran-related trade finance transaction – and the system should therefore be designed to prevent this from happening.

Given that OFAC sanctions are subject to change without notice and could include countries or activities that are currently not subject to sanctions, potential developers of blockchain technology will need to consider:

- Where the technology is developed.
- The locations from which the platform can be accessed (and whether there is any way of restricting access from sanctioned territories).
- The ownership and licensing of the software that is used by participants to administer the blockchain and/or transact on it.

Sanctions are also imposed by other governments and authorities. The European Union, for instance, applies

1 In addition to OFAC-administered sanctions, BIS also administers trade embargoes against certain countries and persons under the Export Administration Regulations. Most exports or re-exports of US-origin goods, technology, or software, including non-US origin items containing more than *de minimis* controlled US-origin content, require a BIS license for sale to embargoed countries or restricted parties.

sanctions and restrictive measures to third countries, entities and individuals in pursuit of its Common Foreign and Security Policy. EU sanctions comprise measures that both implement binding UN Security Council Regulations across the EU, and which give effect to autonomous EU actions (*i.e.* that go beyond the scope of UN resolutions). In general terms, those subject to the jurisdiction of EU member states are prohibited from making funds or economic resources available to designated sanctions targets. Participation in a trade finance transaction which involves financing EU sanctions targets would be prohibited for EU persons absent an applicable license, and that would be the case whether or not the transaction is automated on a blockchain ledger.

## What are the risks?

One of the concepts underpinning blockchain technology is that information is verified by multiple users through a consensus mechanism which ensures that the ledger is complete and accurate – the 'shared truth'. The integrity of the information is then protected by the ledger protocol which keeps track of all changes and ensures that all copies of the ledger must be consistent. For trade finance transactions, this means that a user will need to input into the blockchain ledger, relevant information that is currently in the bills of lading, letters of credit, and other shipping documents (*e.g.* inspection reports, certificates of origin, and the commercial invoices).

Failure to enter in all information relevant to sanctions (even if not all of it is necessary for commercial reasons) may expose those involved in the transaction to OFAC, EU or other sanctions risk. For example, if the ledger did not contain information that the goods were to be transshipped through a sanctioned country or the origin of the goods, then others processing the transaction would not know this and therefore may process or participate in a transaction in breach of sanctions.

OFAC imposes a "should have known" knowledge standard. The question is therefore whether it is reasonable for the bank to rely on the information entered in by the counterparties without looking at or verifying the underlying documentation. Given OFAC's prior guidance to providers of internet-based account services that "a company cannot rely on another firm's compliance program in order to mitigate risk," OFAC could take the position that a bank had not conducted adequate due diligence if it simply screened the electronically available structured data, uploaded and verified by its counterparties, without also conducting a review of the underlying documents or the unstructured data.

There is also a risk that sanctions might deliberately be evaded if, through collusion between the exporter or importer or even the issuing bank, information is included in the ledger that does not accurately reflect the underlying transaction details (*e.g.* the origin of the goods or the ultimate consignee) or material information is omitted.

In such cases, those participating in a transaction for example, as the advising bank, may be exposed to facilitating a transaction that potentially violates sanctions and export controls. If a party decided to mitigate this risk by asking for the underlying documents, it would then undermine the whole purpose for which the blockchain is used, *i.e.* to avoid reliance on the conventional documentary trade system.

One potential solution would be to agree on the information that would need to be entered into the ledger and have an agreement between the parties as to who would be responsible for the accuracy of the data. For example, banks could agree that the "mandatory" information would include:

- The name and address of the exporter and the importer.
- The banks involved.
- The ports of loading, unloading and transit.

- The vessels.
- The insurers and shipping companies.
- The origin, description, and a Harmonized Tariff Schedule (HTS) or a Harmonized System (HS) code of the goods being shipped.

The party responsible for entering the data would be required to also upload the underlying supporting documentation that could be audited by the other users using a risk-based approach. The risk of tampering and fraud does not necessarily loom larger in blockchain. In fact, the risk of inaccurate information being submitted is also present in a paper based system. Blockchain technology may even promote compliance: every transaction on the blockchain leaves a digital footprint that cannot be erased. Tracing ship routes and identifying the origin of goods should be easier, making due diligence to mitigate enforcement risk less complicated. This will require innovative systems and controls to match the novelty of blockchain technology. Ultimately, for security and certainty, it will be critical to get input from OFAC, EU and other regulators that the approach would satisfy regulatory expectations.

## What do developers need to consider from a sanctions perspective?

Here are four sanctions-specific functionalities that we believe developers should consider when creating and building blockchain for trade finance. Although we have focused on trade finance, these same sanctions-specific functionalities could be used in the development of other blockchain solutions.

1. As a starting point, blockchain technology should incorporate sanctions screening technologies so that the information on the ledgers can be screened for any sanctions issues and the user of the system can be alerted anytime that there is a sanctions-related event that is logged in the ledger. For example, if the update to the ledger indicates that Iranian-origin goods have been loaded onto a vessel in Dubai, this should automatically generate an alert for the users.
2. For US banks, as well as other US persons, it will be important to have the ability to block the property or the property interest of a blocked person such as a Specially Designated National (SDN) in the possession or control of the US bank. Under EU sanctions, there is a requirement to freeze assets of sanctions targets. In either case, to do so, blockchain technology must have the capability to identify when possession or control of the property or property interest transfers and then also have the capability to allow relevant persons to block or freeze the property or property interest as applicable in compliance with legal requirements. For example, if a negotiable instrument is transferred on the blockchain to the control of a US or EU bank, the bank should be able to block the negotiable instrument if it determines that the instrument is the property or property interest of a blocked person such as an SDN. Similarly, even where blocking sanctions would not apply and the US or EU bank would only be required to reject the transaction, the blockchain functionality must allow for such rejections.
3. Given that trade finance is built around the concept of certainty, sanctions provisions should be built into blockchains, allowing for termination of the transaction where its consummation would give rise to a sanctions issue. In addition, the blockchain functionality should be able to pick up sanctions events as they occur and self-execute the sanctions provisions.
4. Blockchain technology should include the ability for users to record data in accordance with their regulatory requirements and retrieve all of the data in the ledgers if required to produce the data to the relevant authorities, in a manner consistent with data privacy or other restrictions that may be applicable. This means that if

blockchain technology is hosted in a jurisdiction which places restrictions on data sharing due to bank secrecy or data privacy considerations, it may not be suitable for use in a bank's global operations.

Trade finance is an area where developers are already very active in developing blockchain-based solutions, but it is clearly also an area where the legal issues are complex, subject as it is to the jurisdictions of multiple regulators and involving long chains of transacting parties with different priorities and concerns. Sanctions regimes in their current form cut against the vision of a global financial system underpinned by blockchain technology, *i.e.* a wide-open ledger that disintermediates traditional gatekeepers such as banks and trading houses, and with which governments and regulators cannot interfere. Ultimately, blockchain advocates will have to submit to the reality of cross-border, extra-territorial regulation, including sanctions. An open and frank discussion on where the sanctions pitfalls lie in implementing blockchain solutions can help developers to focus on these commercial and regulatory challenges.

# CONTACTS


**Ali Burney**
**Counsel**
T: +65 6506 1964
E: ali.burney@cliffordchance.com

**Megan Gordon**
**Partner**
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

**Brian Harley**
**Registered Foreign Lawyer**
T: +852 2826 2412
E: brian.harley@cliffordchance.com

**George Kleinfeld**
**Partner**
T: +1 202 912 5126
E: george.kleinfeld@cliffordchance.com

**Paul Landless**
**Partner**
T: +65 6410 2235
E: paul.landless@cliffordchance.com

**Jacqueline Landells**
**Counsel**
T: +1 202 912 5061
E: jacqueline.landells@cliffordchance.com

**Michael Lyons**
**Partner**
T: +44 20 7006 4317
E: michael.lyons@cliffordchance.com

CLIFFORD

CHANCE



www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ



J20172610171525