Money Laundering Considerations in Blockchain based International Commerce

Jason Chuah *

Abstract

There is much to be welcomed concerning the role blockchain technology can play to modernise and enhance international trade and create a more level playing field and reduce costs. However, it goes without say that the technology also brings with it the prospect of abuse leading to trade based money laundering. This article explores how the anti money laundering (AML) legislation should respond to the use of blockchain technology in shipping and trade. Drawing on tried and tested forms of blockchain technology based trade transactions, the work examines the fault lines in the current regulatory system and questions how best these gaps should be remedied. It also stresses that even states that have banned the issue and trade of cryptoassets, such as the People's Republic of China (PRC), would not be immune to the new challenges.

Introduction

It is undeniable that the much vaunted introduction of blockchain and smart contracts in shipping and trade is now very much becoming a reality. This chapter explores how the anti money-laundering (AML) legislation should respond to the use of blockchain technology in shipping and trade. Money laundering usually entails three stages – placement, layering and integration of the assets in question. The way blockchain technology helps with the placement, layering and integration of unlawful funds would be explored against the shipping and international trade backdrop.

There are several reasons why shipping based trade[1] is a good case template. Broadly speaking, shipping based trade is cross border in nature and can

* Professor of Commercial and Maritime Law, City, University of London, and Guest Professor of Law, University of Gothenburg.
**I am very grateful to colleagues who have kindly commented on an earlier draft of this chapter. I have also benefitted from my discussions with my doctoral researcher, Ms Amy Chen, who is working on the wider subject of cryptoassets and money laundering. All errors, of course, remain mine. I must also acknowledge the support given by the University of Gothenburg and City, University of London for enabling me to carry out the underpinning research.

[1] A category of the FATF's typology of "trade based money laundering" (FATF Study on Trade Based Money Laundering (2006) at https://www.fatf-

involve the movement of goods in high volume or value. More importantly, shipping based trade is principally conducted on the basis of documents where identity of the participants is not commonly considered to be essential. Contract terms such as the INCOTERMS 2020, frequently used in international trade, entail the sale and purchase, and distribution of goods simply on the tender of documents rather than proof of identity. Compounded to this, where full blockchain technology is to be adopted, the movement of goods and payment would be directed by computing systems automatically leading to an even higher degree of anonymity.

This article therefore highlights the key risks in blockchain based shipping and trade for the fight against money laundering. The focus of this work is on the compliance role for banks and other stakeholders, arguing that despite the introduction of some important milestones by the regulators, there are certain gaps in the existing regulatory system needing attention. It also stresses that even in countries which ban or prohibit the use and trading of cryptoassets blockchain technology based trade money laundering continues to pose a problem for regulators.

The backdrop of this work is mainly the international system for combating money laundering. Domestic and EU regulatory systems would be mentioned in passing and comparison purposes. As regards the methodology, this work presupposes a broad, generic understanding of blockchain technology and smart contracts. The author carried out a survey of the relevant literature on trade based money laundering to examine how this form of money laundering is understood by regulators and to ascertain the scale of the problem.[2]

This study uses what are largely perceived to be the pioneer stories of successful blockchain driven trade as observational targets. The focus as briefly mentioned above is those cases which run on conventional trade finance processes and lines, and which have involved reputable organisations (for example, Maersk, Barclays, IBM, HSBC, ING, BBVA). Using atypical cases would simply not be appropriate in a studying the money laundering opportunities in blockchain technology based trade finance given the *modus operandi* of money launderers which is to "fit into" the conventional methods of trading. This work has relied on archive-based materials and data published by the trade participants themselves. However, in order to avoid bias and puffing, information was drawn also from related secondary resources, such as trial project websites, news and media reports and external reviews. These case studies are then used to build a general process which blockchain technology based trade would follow.

---

gafi.org/media/fatf/documents/reports/Trade%20Based%20Money%20Laundering.pdf). All internet-based resources in this chapter were last accessed on 14 July 2022.

[2] Please see fn. 29 for details of the literature review undertaken.

Taking a text based enquiry of the literature on trade based money laundering, this work identifies the fault lines in the regulatory regime and offers suggestions for gap filling as regards blockchain technology based trade money laundering.

Blockchain technology and international sales[3]

It is beyond the scope of this article to detail in full the workings of blockchain technology. The literature, both in legal and non-legal sources, is voluminous. It suffices for our purposes to understand a blockchain technology-based trade in goods system might work and to appreciate the reasons as to its increasing acceptance.

A blockchain is a decentralised, distributed record or ledger of transactions or activities. Those transactions are stored permanently using cryptographic methods. They are different from traditional databases which are administered and organised by a central entity. Blockchains on the other hand rely on a peer-to-peer networks that no single person has control; the blockchain is managed by computers or servers – called "nodes" – on a peer-to-peer basis without the need for the intermediaries who traditionally authenticate transactions (such as banks in the case of financial transactions). Transactions are authenticated using cryptographical methods, notably a mathematical "consensus protocol". That protocol is a pre-fixed system which determines the rules by which the ledger is updated. That means the participants can trust the authenticity of the record or ledger because no single person has control over the technology or system. There is therefore no need for any trusted third party – the system itself is trustworthy.

The word "distributed" means that identical copies of the ledger database are downloaded from the world wide web and kept on numerous computers spread across a site, an organisation, a country, multiple countries or indeed, the world.

A blockchain can be permissioned or permission-less – that is to say there are blockchains where access can be granted only to those with permission whilst others are more publicly accessible.

Blockchain as a ledger will allow access to a participant at any time thus improving access. Further, there is open transparency in that every transaction added to the blockchain will be time stamped. There is little risk of tampering because the data is held not in any one place but across the entirety of the peer to peer networks (which may include thousands of computers or servers). These features of blockchain make it very useful for reliably tracing transactions or activities.

[3] The discussion in this section is based on Chuah, J., Law of International Trade (6th edn, Sweet & Maxwell) Chs. 2 and 11.

Smart contracts,[4] which are built on blockchain technology, are computer programmes that self-execute when certain conditions are present. Those conditions *may or may not* be premised any pre-existing agreements between the parties.[5] With a programmable protocol, the smart contract can allow automatically (without human intervention) the execution and performance of its terms. This automated execution of terms of the arrangement is ideally suited to the global trading environment where distance, costs and lack of trust could lead to contract failure. In open account based transactions, the smart contract taken to its natural end could enable the automatic release of payment. As to conventional documentary credit processes, these are premised on centralised business operations – the smart contract system which is built on the distributed blockchain technology reduces the risks centralisation brings about, such as, fraud, forgery and malicious alteration.[6]

How does this new technology change the way international trade is structured?

It might start with the seller or manufacturer setting up or deploying the smart contract exclusively for the buyer's account. The buyer then places an order for the goods in question with a quantity equal to X at the seller's smart contract. The order is sent (for coding or programming purposes, we might label this event something like "SendOrder") which the seller's system would receive the order data and process it. The seller looks for the best shipping price on the carrier's smart contract. It then sends the price (of the shipment and goods) to the buyer (this event might be labelled "PriceSent" for coding purposes).

The buyer then performs the secure payment of the price; if this is performed through cryptocurrencies (or virtual assets in the terminology preferred by the Financial Action Task Force (FATF)[7]), the coins could be paid into the smart contract. The coins would be held there until the goods have been delivered. Where this is paid by fiat currency, the buyer's bank performs the payment function by paying into the smart contract. In this case, the bank is a permissioned participant to the smart contract. The money is not released until delivery is confirmed.

The seller issues the invoice with a delivery date and other relevant information. The buyer receives the data (this event might be labelled "InvoiceSent" for coding purposes). The carrier would concurrently instruct

---

[4] Smart contracts should be distinguished from smart legal contracts. Smart legal contracts are legally enforceable contracts partially expressed and/or executed in code and thus involve the enforcement of legal rights and obligations. A smart contract on the other hand is used to specify software code that is typically stored, verified and executed on a blockchain. See UK Jurisdiction Taskforce "Legal Statement on Crytoassets and Smart Contracts" (2019) at p. 8

[5] See Chang, S.E.; Chen, Y.C.; Wu, T.C. Exploring blockchain technology in international trade. Ind. Manag. Data Syst. 2019, 119, 1712; also the UK Jurisdiction Taskforce "Legal Statement on Crytoassets and Smart Contracts" (ibid).

[6] ibid

[7] FATF amended Recommendations (2018, Recommendation 15 and Glossary)

the goods to be collected and transported. Upon delivery to the buyer, the carrier marks the order on the smart contract as delivered. The smart contract releases payment to both the seller and carrier, as appropriate.

It should be remembered that all the participants (seller, buyer, carrier etc.) have nodes connected to the blockchain.

That is merely one possible means an international sale transaction might be executed by a smart contract.

Thus far, we have not factored the element of trade financing – conventionally in shipping based international trade is provided for by documentary credits. So how does a blockchain based letter of credit work? A simplistic model might assist in our understanding. The process might work like this:

> 1: The buyer creates a documentary credit application for the issuing bank to review and stores it on the blockchain.
>
> 2: The issuing bank receives notification to review the letter of credit. It can approve or reject it based on the data provided. Once approved, access is then provided to the advising or nominated bank automatically for approval.
>
> 3: The advising or nominated bank approves or rejects the letter of credit. If approved, the seller is able to view the terms of the letter of credit. It is further prompted to examine the original application.
>
> 4: The seller ships the goods. It prepares the invoice, export paperwork and any other documents required under the letter of credit. These are then reduced electronically and stored on the blockchain.
>
> 5: The nominated bank is notified of the completion of the electronic records on the blockchain. It then checks the documents and makes a decision to approve or reject the application.
>
> 6: The issuing bank will then examine the data and images. It will identify and highlight any discrepancies for review by the buyer. If the buyer approves the data, the letter of credit is completed and payment is made.
>
> 7: On the other hand, where the buyer is dissatisfied with the discrepancy, it can reject the tender.

Three conventional blockchain based transactions might be used to demonstrate the extent blockchain technology is being used in recent trading relationships.

Case study A: BBVA (Ethereum Blockchain)[8]

[8] https://www.bbva.com/en/bbva-and-wave-carry-first-blockchain-based-international-trade-transaction-europe-and-latin-america/

In 2018, Banco Bilbao Vizcaya Argentaria (BBVA), a Spanish bank, used blockchain technology as a substitute for traditional trade documents. The bank reported that transaction time was reduced from 10 days to around three hours. This project consisted of the exportation of frozen tuna from Mexico. Payment was by means of a letter of credit issued by BBVA. The blockchain solution provider, Wave, would use digitised documentation to replace traditional paper-based documents. The digitised documentation would be verified by an agreed electronic signature. Electronic presentation is enabled during the transit period. Crucially, the digitisation technique could extend to bills of lading in the letter of credit payment processes. Moreover, smart contracts were programmed in accordance with contractual agreements that specified commercial terms and conditional statements of the letter of credit. Blockchain-based[9] letter of credit and bill of lading systems would allow for financing execution through the autonomous features of smart contracts. No manual checking of the documentation is thus required. The bank pays upon satisfying itself that the documentation is in order. However, it is important to note that payment is not made through the blockchain – money is released in the traditional way. Automatic notifications were transmitted to the various participants following each relevant stage – for example, upon delivery enabled by the smart contract, the shipper would be notified.

Case study 2: HSBC (R3 Corda Blockchain)[10]

Here, the end-to-end transaction was executed on R3's Corda blockchain platform. The platform, as was intended, was a single shared application. There was no need for multiple isolated digital systems across various counterparties who are based at various locations across the world. It is an open source blockchain platform; it is different from other blockchain platforms in that it uses what is called permissioning technology to control how data is shared on the platform but this system allows for the network participants could be increased and widened thereby improving scalability. It is also able to give access control to "dominant parties"[11] which means there can be a central party managing the flow. The letter of credit was issued by ING Bank for Tricon Energy USA (the buyer) with HSBC India as the advising and negotiating bank for Reliance Industries, India (the seller). However it is important to note that transfer of funds did not happen over the blockchain, only title in the goods had transferred over the blockchain "transfer" of the bill of lading.

Case study 3: Maersk (Hyperledger Fabric)[12]

---

[9] "Blockchain based" means that the letter of credit is embedded in the blockchain but funds are not transferred using the blockchain.

[10] https: //gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/

[11] Usually the banks

[12] Reported at https://www.forbes.com/sites/tomgroenfeldt/2017/03/05/ibm-and-maersk-apply-blockchain-to-container-shipping/#b8f6e73f05ec; archived materials with Maersk.

In December 2016, Maersk initiated a tracking project with IBM for flower shipments from Kenya to the Netherlands. Participating parties in the blockchain using Hyperledger Fabric included the traders, shippers, freight forwarders and customs authorities. The rationale was to improve how the logistical chain could be better monitored and how the shipment traceability could be improved. The shipping company, Maersk, and the IT services provider, IBM, worked jointly to digitise and dematerialise the traditional documentation. The controlling party in the blockchain is Maersk. The blockchain allowed all participants to track and trace the movement of the goods thereby reducing the physical processes and the need for constant communications between the parties. The information about the shipment was held in the blockchain for all the participants to consult, including approvals and clearances given by customs. Cryptography was used to prevent counterfeiting of the records. In this particular example, Maersk had also provided the necessary trade financing for the sale ***and*** purchase[13] – this means that the shipping company, not a bank, had taken on the role of making payment on behalf of the buyer. In other words, if the Maersk trade finance is not being used, any letter of credit might be outside the blockchain. More recently, Maersk and IBM have developed their own blockchain platform called TradeLens which works on similar lines.[14]

It is vital to note that as these case studies demonstrate, in most conventional blockchain based trade the payment by letter of credit is not made through the blockchain although the terms of the letter of credit are embedded in the blockchain. That means payment in these conventional cases remains to be made using traditional way and in fiat currency. The next ambitious step is to enable payment to be made automatically and using cryptocurrencies, thereby potentially by-passing the banks.

We shall return to these case studies following a discussion of the money laundering context.

The Money Laundering Context

Trade Based Money Laundering has been recognised by the Financial Action

---

[13] The facility would be transacted through Maersk Trade Finance A/S incorporated in Copenhagen, Denmark, part of the Maersk Group. Its website describes its workings in this way – (a) Goods shipped through Maersk will be taken as collateral. It will be LIBOR linked. (b) Pricing is transparent, there are no hidden costs. (c) Shipment must be done through Maersk (although it is possible to use the trader's own current forwarder/Customs House Agents for logistics management). (d) Need assignment of receivables by the exporter. (e) A credit facility will be sanctioned for a designated period. (https://fs.maerskline.com/faq). It is important to note that the finance produce can be offered to **both buyers and sellers**. For sellers, the financing is offered as pre-shipment financing and the seller might still require the buyer to pay by letter of credit. The proceeds from the letter of credit would be used to service the pre-shipment financing.

[14] https://www.maersk.com/news/articles/2019/07/02/hapag-lloyd-and-ocean-network-express-join-tradelens

Task Force (FATF)[15] in its landmark study published in 2006, as one of the three main methods by which criminal organisations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy.[16] The FATF Study 2006 highlighted the increasing attractiveness of trade-based money laundering (TBML) as a method for laundering funds, compared with misuse of the financial system (both formal and alternate) and through physical movement of cash (cash smuggling).[17] The revision of FATF standards undertaken in 2003 entailed stricter controls on the financial system and on cash couriers, which may have had an unintended consequence of leaving the trade finance sector more vulnerable to ML and TF.[18] There is no doubt that the increased volumes, speed and value in globally traded goods and services coupled with the often opaque and complex trading arrangements have led to an increasing abuse of trade financing as a means to commit money laundering. The casting of blockchain technology into the mix creates additional problems for regulators.

The FATF also took pains, when the report was released, to state that trade based money laundering has long been under the radar and had not benefited from the same level of analysis and study other forms of money laundering schemes had attracted.[19] In 2011, the Australian Institute of Criminology published a research paper[20] asserting the same sentiments. Since then, there have been more work done on trade based money laundering but there remain various controversies and debates around definitions and means of combating it.[21]

How should trade based money laundering be defined?

A useful starting point for a general definition of money laundering might be the Vienna Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988. Article 3(1)(b) of the Convention is a good starting point at providing the essence of the money laundering offence which

---

[15] The FATF describes itself in these terms "The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas. With more than 200 countries and jurisdictions committed to implementing them. The FATF has developed the FATF **Recommendations,** or FATF Standards, which ensure a co-ordinated global response to prevent organised crime, corruption and terrorism." (https://www.fatf-gafi.org/about/)

[16] FATF 2006: 25

[17] ibid

[18] Asia-Pacific Group on Money Laundering, Typology report on Trade Based Money Laundering (2012) at para 27

[19] The FATF said: "[trade based money laundering] has received considerably less attention in academic circles than other means of transferring value" (FATF (2006):3)

[20] Sullivan, C. & Smith, E., Paper 115: Trade-based money laundering: Risks and regulatory responses (2011) at pp. 4-5; see also the Asia Pacific Group on Money Laundering (FATF) Typology Report on Trade Based Money Laundering (2012) p. 39 at http://www.fatf-gafi.org/media/fatf/documents/reports/Trade_Based_ML_APGReport.pdf

[21] See for example FATF, Best Practices on Trade Based Money Laundering (2012); US GAO, Report to Congressional Senate "Trade Based Money laundering" (2020) at pp. 19-22

contracting states should adopt in their domestic legal systems. That article provides:

(i) The conversion or transfer of property, knowing that such property is derived from any offence or offences established in accordance with subparagraph a) of this paragraph[22], or from an act of participation in such offence or offences, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an offence or offences to evade the legal consequences of his actions;

(ii) The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from an offence or offences established in accordance with subparagraph a) of this paragraph[23] or from an act of participation in such an offence or offences.

A similar concept of money laundering was extended to cover assets and proceeds derived from organised crime by the Convention against Transnational Organized Crime 2000, the so-called Palermo Convention[24]. The subsequent Convention against Corruption 2004 extended the fight against money laundering to proceeds from bribery and corruption.

At a generic level, from the definition it follows that money laundering involves three phases – placement, layering and integration of the assets in question. Placement involves the transfer of the illicit assets into the legitimate financial system. Layering is that part of the process which sets out to hide or disguise the true source of the asset. Once the asset has been "laundered", it is removed from the legitimate repository and be used by the criminal beneficiary.

There are three primary methods of money laundering: the laundering of money through the financial system, the physical movement of money (such as through cash couriers), and trade based money laundering.[25] FATF has defined trade based money laundering as "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins.[26] On the other hand, in its Best Practices Paper on trade based money laundering, "trade based money laundering" is defined more broadly as: "the process of disguising the proceeds of crime and moving value through the use of trade transactions in an attempt to legitimise their illicit origins or finance their activities."[27] That said, it is submitted that the words "finance their activities" do not add much

[22] That subparagraph (a) generally provides for production, manufacture, sale, distribution, transport, import etc of illicit narcotic drugs.
[23] See above fn. 9
[24] See art 6
[25] See Financial Action Task Force, Trade Based Money Laundering (2006)
[26] Ibid, at 3
[27] FATF (2008a: 1)

to the working definition. The important consideration in this form of money laundering is the use of trade transactions to place, layer and integrate the "dirty assets".

The FATF considers trade primarily to be international trade – domestic trade does not appear to be included in its working definitions.[28] Again, it is not clear if this absence (if indeed it is excluded) would leave a significant gap in the law. Most AML systems are domestically oriented and FATF recommendations are merely for guidance. It is difficult to envisage a situation where domestic AML would exclude home based trade money laundering from the definition of the money laundering offence.

How extensive is trade based money laundering?

It is difficult to estimate the scale of the problem of trade based money laundering. The clandestine nature of the crime makes it gruelling to ascertain or scope the magnitude of the problem. This work has drawn on an extensive literature review[29] to give the reader a sense of the scale of the problem. The net conclusion is that these works all have various limitations as regards the method used in delineating the scale of the problem but there is enough evidence, even if not properly empirical, showing trade based money laundering to be significantly substantial a problem. It is noteworthy to quote the following from the US Government Accountability Office:

> "Some U.S. officials and knowledgeable sources believe that, based upon available evidence, TBML is likely one of the *largest forms of money laundering*. In addition, as countries have strengthened their controls to combat other forms of money laundering, various U.S. government reports and officials, as well as knowledgeable sources have stated that there are indications that criminal organizations and

[28] In its Best Practices Paper, FATF (2008a: 2) defined a 'trader' as "anyone who facilitates the exchange of goods and related services across national borders, international boundaries or territories. This would also include a corporation or other business unit organized and operated principally for the purpose of importing or exporting goods and services (eg import/export companies)". It follows thus that participants in a domestic trade transaction appear not to be included.

[29] The literature surveyed includes: Zdanowicz, J., "Trade-Based Money Laundering and Terrorist Financing," Review of Law and Economics, vol. 5, no. 2 (2009): 855; McSkimming, S., "Trade-Based Money Laundering: Responding to an Emerging Threat," Deakin Law Review, vol. 15, no. 1 (2010): 37; Forstater, M., Illicit Financial Flows, Trade Misinvoicing, and Multinational Tax Avoidance: The Same or Different? (Center for Global Development, Policy Paper 123, 2018); Global Financial Integrity, Illicit Financial Flows to and from 148 Developing Countries: 2006–2015 (2019); Walker, J. and Unger, B., "Measuring Global Money Laundering: 'The Walker Gravity Model,'" Review of Law and Economics, vol. 5, no. 2 (2009): 821; Soudijn, M. (2014), "A critical approach to trade-based money laundering", Journal of Money Laundering Control, Vol. 17 No. 2, 230. As to policy and research papers published by international bodies, a survey was carried out in respect of the FATF documents (the Trade Based Money Laundering Report (2006) and Best Practices Paper on Trade Based Money Laundering (2008)); the UNODC Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes (2011); and WCO Illicit Financial Flows via Trade Mis-invoicing (2018). The US GAO, Report to Congressional Senate "Trade Based Money laundering" (2020) was also consulted.

terrorist organizations have increased their use of TBML to launder their funds. For example, FinCEN[30] has reported that since the Mexican government increased restrictions on U.S. dollar cash deposits at Mexican financial institutions in 2010, Mexican drug cartels appear to have increasingly turned to TBML as an alternative means of repatriating profits from U.S. drug sales. Similarly, in Australia, as controls on large cash deposits at ATMs have increased since 2017, criminals have increased their use of TBML to hide their profits, according U.S. officials at Embassy Canberra. In addition, the 2020 National Strategy for Combating Terrorist and Other Illicit Financing notes that there has been a steady decrease in seizures related to bulk cash smuggling from 2012 through 2018 and states that this decrease could indicate that criminal organizations are increasingly turning to other means to move illicit money, including TBML."[31] (emphasis added)

The continued growth in blockchain technology in international trade is likely to have an exacerbating effect.

Blockchain technology trade based money laundering

Our case studies, as has been stressed, represent by and large the current, conventional forms of blockchain technology based trading arrangements. Lessons from how they work will be useful in our evaluation of the money laundering perspective.

From the case studies discussed above, there are several features of blockchain technology based trade which could be envisaged as giving cause for concern. It certainly goes without saying that these risk aspects too are what make blockchain technology based trade attractive to business. The position taken in this chapter is that regulation must balance risk of money laundering against the benefits of blockchain.

Those features are:

(a) Paperless
(b) Ease of establishing the contractual networks
(c) No central party in the blockchain consortium
(d) Removal of intermediaries; human agency replaced
(e) Possible use of cryptocurrency or virtual assets – diffused loci of assets

Looking at the case studies, one commonality is clearly the dematerialisation of paper documentation. There is potential for documentation, including supportive, secondary documents such as packing lists, survey reports, inspection reports etc., also to be embedded into the blockchain. A blockchain system which does not adequately allow for cross checking of the information could be abused by money launderers to create trade description fraud. A blockchain based system could go beyond a simply digitisation of the

[30] The US Financial Crimes Enforcement Network
[31] US GAO, Report to Congressional Senate "Trade Based Money laundering" (2020) at pp. 19

documents for the purposes of international trade – blockchain based technology on which smart contracting is based could effectively automate the document checking process. The effectiveness of the system to prevent anomalies and other "red flags"[32] to be picked up leaves is questionable.

Trade description fraud is one of the more common forms of trade based money laundering. It can include:

(a) Over- and under-invoicing of goods and services As FATF explains, "[t]he key element of this technique is the misrepresentation of the price of the goods or service in order to transfer additional value between the importer and exporter"[33].
(b) Multiple invoicing of goods and services where the same goods (also called carousel transactions) are invoiced repeatedly often using multiple financial institutions to pay. In a highly publicised fraud in the port of Qingdao, PRC, companies controlled by a China-born, Singaporean businessman were alleged to have used invoices for the same metals stockpiles several times to milk the banks out of large sums of money.[34]
(c) Under shipment of goods; documents are created to indicate a misrepresent the true (and smaller) amount of goods shipped, and there are no genuine buyers at the point of discharge.
(d) False description of goods: misrepresenting the goods to be of a higher quality or value than they really are.

These trade based money laundering activities could also be helped by the fact that blockchain technology based trade could be exploited for the setting up of false or fictitious entities. In order to prevent false entities from being established, the blockchain based system will need to create systems to replicate physical checks on identity. Due diligence must be exercised, not only in respect of the exporter – it is tempting take a more lackadaisical approach with the importer, erroneously assuming that the money laundering risk lies primarily with the "seller". Blockchain technology can facilitate the creation of a distributed marketplace where there are not only multiple buyers but also where buyers can become sellers and vice versa in chains of contracts. A large scale distributed marketplace could make it more challenging to apply customer due diligence (CDD) and "know your customer" (KYC) principles.[35]

---

[32] See FATF Best Practices (2006); these red flags might relate, for example, to where the goods are said to be coming from or entering, the presence of any free ports, type of goods, corporate structures of consignors and consignees, trade patterns, etc.

[33] (2006: 4)

[34] This case has led to multiple legal claims involving competing ownership rights. It is made worse by the fact that there is lack of legal clarity as to where the assets are located for the purposes of redress and seizure. The port of Qingdao was also sued for failing to spot the fraud thereby causing substantial losses to the banks. CNBC reports that the losses suffered by banks and trading houses were in the region of USD 900 million (https://www.cnbc.com/2014/ 08/03/legal-fight-chills-china-metal-trade-after-port-fraud-probe.html)

[35] See generally CDD and KYC principles described by the FATF (see section D,FATF Recommendations (Updated 2019) at http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf); note that CDD and KYC requirements will differ from jurisdiction to jurisdiction.

It is more difficult properly to evaluate the risk when there are many small scale purchasers and sellers, as against a large transaction.

The challenge of identifying the user or participant and carrying out due diligence is further exacerbated by the fact that in a blockchain based system there is usually no central controller – the platform provider, unlike in conventional digitised trade involving electronic bills of lading and electronic letters of credit, is not in theory involved in monitoring the execution of the smart contracts. The smart contracts are intended to be self-executing. That said, as we have seen in the HSBC (R3 Corda Blockchain) case study above, there is a controller (usually the bank which is under a duty, generally speaking, to carry out checks for anti-money laundering purposes), thereby actually modifying the pure form of blockchain technology. Where there is no controlling party would also mean, anti money laundering legislation could well be frustrated. Moreover, where the blockchain users all have access to the same information held in the blockchain, data protection laws might make it even harder for any interested participant (if any) to discern any identity anomalies.

A much lauded benefit of blockchain technology based trade is the fact that intermediaries could be dispensed with. Although it is undeniable that intermediaries are often the cause of delays and additional costs, they also play an important role in helping verify the different supply chain nodes and participants. In anti money laundering legislation where knowing the customer is a key plank of the law, this added layer could assist in the customer identification and verification process. Moreover, these third parties are often involved in verifying the goods and their description. For example, an inspector could well notice that a container does not appear to be as heavy as the declared weight might suggest.[36] In a blockchain world, unless the contract calls for the intervention of a third party inspector and/or the computing system is programmed to detect anomalies like that, such trade based money laundering activities could go undetected.

We have seen in our case studies that none has gone to the extent of enabling actual payment using cryptocurrencies through the blockchain. However, it would be ill-advised to assume that crypto-payment would not be used to pay for international sale contracts. Indeed, despite serious set-backs, it could not have gone unnoticed that Venezuela had attempted to require its oil buyers to use its virtual currency, Petro, as a result of the lack of tradability in its fiat currency due to economic sanctions.[37]

Once cryptocurrencies come into the picture, the scene does get rather

---

[36] For example, as part of a trade based money laundering scheme to over-declare the quantity of the goods. See above.

[37] See https://www.bloomberg.com/news/articles/2020-01-16/venezuela-s-crypto-mandate-spurs-some-to-pause-oil-purchases; Bloomberg also reports, "Most companies taking Venezuelan crude no longer pay cash. Instead, they engage in swap transactions, where they take crude oil in exchange for gasoline or diesel. Others, like Eni SpA and Repsol SA, get oil in payment for old debts."

murkier. The argument that cryptocurrencies could be conveniently used for money laundering purposes is well rehearsed. In this work, the focus is on how crypto-payment facilitated by the blockchain based trade might be used for money laundering. For ease of reading, we shall use the term cryptoasset or cryptocurrency instead of the FATF preferred terminology, virtual asset.

Cryptocurrency and trade based money laundering

The use of cryptocurrency in trade based money laundering is not unknown. The US Drug Enforcement Agency has reported that trade based money laundering involving cryptocurrency has been observed in schemes whereby goods from the Peoples Republic of China (PRC) are being shipped to Mexico and South America.[38] Whereas in the past, "wire or bulk cash smuggling" would be used for payment, that has been replaced in a number of cases by payment in bitcoin. Payment by bitcoin, it is reported, is preferred by certain PRC manufacturers as it allows them to avoid the PRC capital controls. Moreover, and of interest to us, is the fact that the purchase of bitcoin from a licenced money service business (MSB) faces less scrutiny, compared to a wire transfer from the US to the PRC. It is also not unusual that the bitcoin would also be purchased from unregulated brokers in jurisdictions outside the US who would intertwine its use for trade based money laundering with capital flight devices. Cryptocurrency works best in money laundering where it could be converted back to fiat currency easily.[39]

Another cryptoasset needing consideration is "stablecoins", so-called. Although there is no universal definition of "stablecoins", it might be useful to borrow that applied by the Financial Stability Board. It describes stabelcoins as a type of crypto "that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets to other assets".[40] As regards trade based money laundering, the type of stablecoins most at risk of abuse are those which could be scaled up quickly for mass adoption. That said, even where stablecoins are used in a small scale setting, the fact that they can be used under the cloak of anonymity and may be easily exchanged or converted

---

[38] Drug Enforcement Administration (DEA], "2017 National Drug Threat Assessment" (2017, October) p. 130

[39] That explains why it is less commonly used by terrorist groups which are more geographically restricted such as Boko Haram. Groups, like Hamas, Hezbollah, and al Qaeda, whose presence is found in numerous geographic locations across the world with several points of transfer between the initial source of funds and the ultimate beneficiary, would find the use of cryptocurrencies more viable (see Report by Goldman, Maruyama, Rosenberg, Saravalle, & Solomon-Strauss, "Terrorist Use of Virtual Currencies: Containing the Potential Threat" (2017), p. 27 at https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReportTerroristFinancing-Final.pdf)

[40] FSB, Addressing the regulatory, supervisory and oversight challenges raised by "global stablecoin" arrangements: Consultative document, April 2020; The FATF explains in its Report to the G20 on Stablecoins (June 2020) at https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-FATF-Report-G20-So-Called-Stablecoins.pdf : "the value of a so-called stablecoin may be pegged, for instance, to the value of a fiat currency or a basket of assets that may include fiat currencies, digital currencies, investment securities, commodities and/or real estate. A so-called stablecoin may also employ algorithmic means to stabilise its market value." (para 23).

to another cryptoasset make them vulnerable to money laundering activity.[41]

In certain jurisdictions such as the PRC, the issuing and trading of cryptoassets, other than the state backed digital yuan, are banned. The digital yuan too is not based on blockchain technology. However, three points should perhaps be mentioned. First, the banning of cryptoassets and removing blockchain from the state backed digital currency does not mean an exclusion of blockchain technology from international trading. Indeed, the PRC has taken a lead in introducing its own national blockchain based service network – akin to a grand scale platform backed by the state. The platform is intended to enable all blockchain technology apps to operate across any cloud, portal or framework.[42] Secondly, this state backed service is intended to be accessible to as wide as user base as possible, with various access points.[43] The Blockchain Based Service Network development team also stated, "in principle, the BSN is a multi-chain, multi-ledger blockchain system."[44] The availability of such open access, despite the fact that permission might be required, does not remove the risks for money laundering and the challenges for financial institutions and other stakeholders (the so-called AML Reporting Entities), required under PRC law,[45] to undertake the necessary checks. Indeed, many of the guidance papers on customer due diligence issued by the China Banking Regulatory Commission and the People's Bank of China currently do not refer to blockchain technology based trade as a money laundering typology.[46] Thirdly, where the digital yuan is to be used in place of more conventional cryptoassets, in theory, that has some value in the anti money laundering efforts. The trials concluded in October 2020 and it has been reported that its use in the sale and purchase of goods has been successful.[47] As regards money laundering, the advantage with the digital yuan is that as it is not blockchain based and is more like electronic cash, the banks issuing it will have a record of what has been exchanged for the digital yuan. That record will allow the banks to help monitor the flow of the digital yuan in the economy, which in turn could held the law enforcement agents track illicit flows of funds, including money laundering or terrorist financing. In practice, the issue is that once the digital currency or the fiat currency used to exchange for the digital currency is internationalised (which is part of the PRC's plan to reduce reliance on the US dollar) that tracking and tracing

---

[41] This latter feature is called "chain hopping" and could allow for multiple layering of illicit funds within a short timeframe, thereby allowing a more sophisticated disguise of the origins of funds. (ibid, at para 35)

[42] See the service's website at https://bsnbase.io/g/main/index

[43] The PRC's BSN Development Association, Blockchain Based Service Network: Introductory White Paper (September 2019), at chs. IV and V.

[44] Ibid, at p. 7

[45] Law of the People's Republic of China on Anti-money Laundering (2006) No. 56 (Adopted at the 24th session of the Standing Committee of the 10th National People's Congress); and

[46] A survey of the 2019 IMF Staff Country Report for the PRC: Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism (No. 19/172; 2019), and IMF Staff Country Report for the PRC: Report on the Observance of Standards and Codes-FATF Recommendations for Anti-Money Laundering and Combating the Financing of Terrorism (Country Report No. 19/173; 2019)

[47] See Reuters' report dated 22 October 2020 at https://www.reuters.com/article/us-china-currency-digital-explainer/explainer-how-does-chinas-digital-yuan-work-idUSKBN27411T

would not be an easy exercise for the issuing banks. In sum, more work needs to be had to develop better practical measures for all reporting entities.

The impact and reach of anti money laundering controls

In the UK, EU and elsewhere the anti money laundering regimes have evolved to provide for controls over those individuals involved in the movement of cryptoassets, whether blockchain technology based trade is used or not. On the other hand, by default, any transaction using blockchain technology but does not involve the use of cryptoassets would not be subject to special rules. Instead the general rules would apply. In short, that means the case studies in this study would all fall to be dealt with using traditional KYC and CDD. In the light of the discussion of the risks above, even if the traditional risk based approach is adopted for CDD and KYC processes special protocols may need to be established to ensure good practice amongst financial institutions involved in the sanctioning of funds transfers and payments. There is rise in the number of commercial enterprises providing, for a fee, programmes to assist in the KYC and CDD processes. Whilst that is not objectionable and, indeed, can be of tremendous assistance to smaller financial institutions and firms tasked to undertake anti money laundering checks, firms must be careful not to place the entirety of their responsibility on those for-profit service providers.

KYC and CDD are protocols to be undertaken by the regulated financial institution or firm. However, blockchain technology based trade, as we see in our case studies, could well dispense with the need for a controlling or central entity. Without this key entity, the anti money laundering regime will need to focus, in the main, on the entrance or exit points – namely where the money laundering proceeds are placed into or taken out of the system to be spent. As to whether anti money laundering legislation applies to blockchain platform providers, the issue depends very much on whether they could be deemed to be providing services in like manner as financial institutions, lawyers, accountants, foreign exchange dealers, art dealers, auction platforms etc[48] or whether they are also cryptoasset exchange platforms.[49] If the latter, they could be directly bound by the due diligence and reporting duties of anti money laundering regulations.

The pressure is more palpable in the case of cryptoasset or cryptocurrency. Here too there is often no central body responsible for controlling the movement of the funds. As a result, the FATF's recommendation is for national authorities critically to ensure that originators and beneficiaries of financial transactions are identifiable and are not anonymous. Cryptoasset

[48] See for example regs 10-15 of the UK Money Laundering Regulations 2017 as amended by the *Money Laundering* and Terrorist Financing (Amendment) *Regulations* 2019

[49] See the EU 5th Anti Money Laundering Directive generally; also *Money Laundering* and Terrorist Financing (Amendment) *Regulations* 2019 reg.

providers[50] and financial institutions must comply with the "travel rule".[51] The travel rule is a *non-legally*[52] binding recommendation[53] exhorting countries to ensure that originating cryptoasset providers obtain and hold required and accurate originator information and required beneficiary information on cryptoasset transfers, submit that information to the beneficiary cryptoasset provider or financial institution (if any) immediately and securely, and make it available on request to appropriate authorities. Countries should ensure that beneficiary cryptoasset providers obtain and hold required originator information and required and accurate beneficiary information on cryptoasset transfers and make it available on request to appropriate authorities. Other requirements which were applied to traditional funds transfers (such as monitoring of the availability of information, and taking freezing action and prohibiting transactions with designated persons and entities) would apply on the same basis to cryptoassets.[54] The same obligations apply to financial institutions when sending or receiving virtual asset transfers on behalf of a customer.

The FATF Recommendations also require states to take effective and proportionate enforcement measures against firms and financial institutions that fail to enforce anti money laundering standards.[55] However, the money service businesses providing cryptoasset services tend to decentralised and could be established in multiple geographical locations. Many cryptocurrency exchanges also do not have the infrastructure to obtain, hold and transmit identifying information of the participants in a transaction.[56] There is no denying that at present there is no universal consensus as to the technology on which information and data sharing would be managed, resourced and regulated. A compounding fact making compliance with the travel rule exceedingly difficult is the existence (and anecdotally, prevalence) of crypto mixers which mask and hide the actual source of the cryptoassets. The net result is thus that there will be many cryptoasset providers which will be outside the reach of the law and also many providers intending to apply the travel rule but are actually unable to do so properly.

The FATF Recommendations also expressly provide for sanctions and enforcement measures to be taken against the perpetrators of money laundering.[57] These measures include criminal prosecutions and, importantly, asset confiscation. The 2019 FATF Recommendations state that countries must adopt measures which include the power:

---

[50] Called "virtual asset service providers" by the FATF
[51] The travel rule is not a new tool; indeed, it has been applied in the US in 1990s in relation to wire transfers (Title 31 of the Code of Federal Regulations 1995, Section 103.33(g)). See too Annex A to the FATF, 12-Month Review of the Revised FATF Standards on Virtual Assets/VASPs (June 2020).
[52] Emphasis added.
[53] R.16, FATF (2019)
[54] ibid
[55] See Section D (FATF Recommendations 2019)
[56] Where the participants are in trade related blockchain, it should be recalled that the information would be generally available.
[57] Section B (FATF Recommendations 2019)

> "… to: (a) identify, trace and evaluate property that is subject to confiscation; (b) carry out provisional measures, such as freezing and seizing, to prevent any dealing, transfer or disposal of such property; (c) take steps that will prevent or void actions that prejudice the country's ability to freeze or seize or recover property that is subject to confiscation; and (d) take any appropriate investigative measures"[58]

It is immediately obvious that where the asset in question had been dematerialised into a cryptoasset or if it had been mixed, these sanctions and seizures would be hugely problematic. That is, even before factoring in the question as to where the asset is located. Where no cryptoasset is involved, such as in a "conventional" blockchain technology based trade, the key to enforcement lies very much in international cooperation.[59] However, many developing countries (also being exporting countries) do not have a sufficiently developed international law enforcement cooperation infrastructure.

Against this backdrop, it is indeed a positive feature that the EU's new 6th AML package of weaponry. The 6th AML Directive clarifies the term 'criminal activity' in art 2[60] and narrows it down to 22 predicate offences.[61] A predicate offence is a criminal activity that enables a more serious crime. For example, a predicate offence would be any crime that generates the money but the larger crime would be laundering of that money or the use of that money to finance terrorism. Both the predicate and larger offence would be subject to the criminal law. There is increased criminal sanctions on the natural persons who have committed crimes[62] under the 2018 Directive. The maximum jail term goes up from 1 year to 4 years. Moreover, art 6 of the 6th AML Directive provides that the regulator shall have the power to request the removal of any person convicted of money laundering, any of its predicate offences or terrorist financing from the management role of the "obliged entities". Supervisors shall have the power to remove members of the senior management that are not deemed to act with honesty and integrity and possess knowledge and expertise necessary to carry out their functions. The inclusion of the requirement for knowledge and expertise is

---

[58] R.4 ibid

[59] RR. 36-40 Section G (FATF Recommendations 2019)

[60] Directive (EU) 2018/1673 on combating money laundering by criminal law

[61] These include the so-called white collar crimes such cybercrime, tax crimes, insider trading and market manipulation, fraud to the more conventional ones such as illegal human trafficking, piracy, kidnapping, theft etc.

[62] These are offences which to an appreciable extent conform to the FATF's definitions. The main provision is art 3(1) Directive 2018/1673: " Member States shall take the necessary measures to ensure that the following conduct, when committed intentionally, is punishable as a criminal offence: (a) the conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action; (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity; (c) the acquisition, possession or use of property, knowing at the time of receipt, that such property was derived from criminal activity."

problematic – does it mean that the firm would be prevented from relying on third party expert blockchain based trade financing service providers? It is submitted that the provision is not intended to have such a far-reaching effect but there is no precedent and managers are well aware that the consequences for getting things wrong could be highly damaging to the firm.

Conclusion

The current anti money laundering risk based approach advocated by the FATF recognises the magnitude of the problem but considers that as there are many socio-economic impediments to scaling up in the mass adoption of cryptoassets, the measures being taken are reasonably acceptable.

It is argued that although a reality premised approach is appropriate, it must be appreciated that given the scale of trade based money laundering, the use of blockchain and cryptoassets in international trade could well make matters worse. That is not to say that blockchain should not be a present and important feature in international trade. Indeed, the technology itself could be exploited to provide helpful anti money laundering solutions; blockchain technology can assuredly assist in the satisfying the requirements of the travel rule, KYC and CDD. So too are market forces and structures – if there is no easy way to extract the laundered assets, for example, the money launderer would try something else. However, as regards the policy and law, it is important to keep watch on how trade based money laundering activities are continually shifting and changing. The anti money laundering rules and standards should thus continue to be reviewed in the light of those changes. This chapter serves, in some modest way, to identify how trade based money laundering might evolve in the light of blockchain technology and smart contracting and demonstrate what anti money laundering law should be alert to.