MANUSCRIPT
(FOR PUBLISHED VERSION, PLEASE REFER TO: 'Technology-Driven Solutions to Banks' De-risking Practices in Hong Kong: FinTech and Blockchain-based Smart Contracts for Financial Inclusion', *Common Law World Review*, Vol. 51(1-2), pp. 83-108 (May 2022, published online)

The permanent link for this article is https://doi.org/10.1177/14737795211071095

Technology-Driven Solutions to Banks' De-risking Practices in Hong Kong: FinTech and Blockchain-based Smart Contracts for Financial Inclusion

Emily Lee*

Abstract

This article examines banks' de-risking practices inside Hong Kong's Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) regime, a problem that has created considerable tension between the demands of AML/CFT prevention and those of financial inclusion. It unravels the public policy tensions stemming from a multitude of financial reform causes, namely the facilitation of AML/CFT regulatory compliance, the promotion of financial technology (FinTech) innovation and an ultimate expansion in financial inclusion. The article argues that tiered account services are an important first step towards financial inclusion, culminating in the introduction of simple bank accounts by some banks to mitigate the effect of de-risking. While proposed solutions such as the know-your-client (KYC) utility system and central data repository may contribute to a digital financial inclusion framework, they are not tailored to solve a specific problem (de-risking). The article therefore proposes and evaluates whether FinTech and blockchain-based smart contracts qualify as alternative solutions to de-risking. The article aims to address those policy tensions and contribute to the regulatory policy formulation and the rule-making for financial law and regulation intended to facilitate financial inclusion.

Keywords
banks, de-risking, FinTech, blockchain, smart contracts, financial inclusion, Hong Kong

Introduction

The Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615) was renamed the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO), Hong Kong's AML/CFT law, on 1 March 2018. [1] The parenthetical phrase '(Financial Institutions)' was removed from the title to

* LLB, LLM, PhD, Associate Professor, Faculty of Law, The University of Hong Kong. This article forms part of the Public Policy Research Project (ID: 2017.A8.064.17C) which was funded by the Public Policy Research Funding Scheme from the Policy Innovation and Co-ordination Office of the Hong Kong Special

reflect the legislation's wider scope of application to a group of entities including, *inter alia*, financial institutions, licensed corporations and money service operators. [2] Furthermore, the revised Guideline on Anti-Money Laundering and Counter-Terrorist Financing (for Authorised Institutions) (the AML/CFT Guideline) allows more flexible approaches to obtaining and verifying customer information (HKMA, 2018a).[3] In terms of the methods used by authorised institutions, such as licensed banks, to obtain information related to customers, authorised institutions are required to implement measures consistent with the risk-based approach to ensure compliance, as they (authorised institutions) are encouraged to exercise discretion while adopting practical options allowed under the revised requirements to improve the efficiency and reduce the unnecessary burden in the 'know your client-customer due diligence' (KYC-CDD) process, a key component of AML/CFT compliance.[4]

The AMLO requires financial institutions to implement customer due diligence (CDD) and record-keeping requirements which are the main strands of the AML/CFT regulatory regime championed by the Financial Action Task Force (FATF). The

Administrative Region (SAR) Government. I am most grateful to the Hong Kong SAR government for their financial support of this project. I thank participants at the 3rd Asian Private Law Workshop on 28 May 2020 for their feedback and insightful discussions. I am also much obliged to Professor Ernest Lim for his many helpful comments. The usual disclaimer applies. Email: eleelaw@hku.hk

[1] For the sake of comprehensiveness, the AML/CFT legislation in Hong Kong includes the Drug Trafficking (Recovery of Proceeds) Ordinance (DTROP, Cap. 405), Organised and Serious Crimes Ordinance (OSCO, Cap. 455), United Nations (Anti-Terrorism Measures) Ordinance (UNATMO, Cap. 575) and Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO, Cap. 615). For the purpose of this article, which has a special focus on financial inclusion in Hong Kong in relation to banks' de-risking practices, however, the AMLO will henceforth be referred to as Hong Kong's anti-money laundering law.

[2] The AMLO also applies to solicitors, foreign lawyers (as defined in section 2(1) of the Legal Practitioners Ordinance (Cap. 159), accountants, real estate agents, and trust or company service providers (collectively referred to as 'designated non-financial businesses and professions' (DNFBPs)) when they conduct certain specified transactions, as DNFBPs are subject to the statutory customer due diligence and record-keeping requirements stipulated in Schedule 2 to the AMLO. Note that licensed corporations, money service operators, as well as the DNFBPs are outside the scope of this article.

[3] Hong Kong Monetary Authority (HKMA) (23 February 2018), Amendments to guideline on anti-money laundering and counter-terrorist financing (for authorised institutions) Ref. B10/1C, B1/15C.

[4] *Ibid*. In practice, know your customer (KYC) and customer due diligence (CDD) are often regarded as similar processes. KYC, however, entails an extensive screening process, while CDD operates within this process and constitutes more of an assessment of the risks associated with a financial institution's business relationship with a client within the AML/CFT framework.

relevant CDD and record-keeping requirements are set out in Schedule 2 to the AMLO.[5] Financial institutions shall perform CDD measures on their clients and beneficial owners.[6] CDD measures include obtaining information on the purpose and intended nature of the business relationship[7] by identifying the customer and using documents (such as an official ID or government-issued passport) to verify this identity, as well as data or other information obtained from a reliable and independent source.[8] CDD measures are determined on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction, thus allowing demonstration to the financial institutions' supervisory authority that the extent of measures has been appropriate in view of the risks of money laundering and terrorist financing (ML/TF).[9] In terms of when the duty is imposed in the application of the CDD measures, financial institutions must verify the identity of the customer before the establishment of a business relationship or the carrying out of an occasional transaction. Such verification, however, may be completed during the establishment of the business relationship if (a) this is necessary to prevent the interruption of the normal conduct of business; and (b) there is little risk of ML/TF occurring.[10]

Accordingly, financial institutions have developed written AML/CFT policies and procedures to comply with applicable provisions of Hong Kong laws.[11] In practice this means that any bank operating in Hong Kong has a duty to investigate and file a 'suspicious transaction report' (STR) concerning the suspect's bank accounts with the Joint Financial Intelligence Unit (JFIU) of the Hong Kong Police.[12] Financial institutions are also required to identify and verify the identity of customers and to keep relevant customer records for six years. Non-compliance with the requirements may render financial institutions liable to disciplinary and criminal sanctions.[13]

---

[5] Legislative Council (2017), Report of the Bills Committee on Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) (Amendment) Bill 2017 and Companies (Amendment) Bill 2017, LC Paper No. CB(1)496/17-18.
[6] Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615), Schedule 2, Part 2.
[7] *Online Tax Rebates Limited v The Commissioners for Her Majesty's Revenue & Customs* [2018] UKFTT 0215 (TC), 2018 WL 01306458, para 70.
[8] *Ibid*, para 80.
[9] *Ibid*, para 81.
[10] *Ibid*, para 83.
[11] *Phillip Securities (Hong Kong) Ltd v 3i Capital Group Corp* [2017] HKEC 2773.
[12] *Interush Limited & Interush (Singapore) PTE Limited v The Commissioner of Police, The Commissioner of Customs & Exercise and Mak Wing Yip Cyril, Superintendent of Police*, HCAL 167/2014
[13] *See* Schedule 2 AMLO. *See also* LC Paper No. CB(1)496/17-18), *supra* note 5.

These new changes pertaining to the AMLO will impact Hong Kong's AML/CFT regime, especially concerning the increased difficulty in opening a bank account in Hong Kong, with the most affected groups being individuals, small- and medium-sized enterprises (SMEs) and start-ups. Financial exclusion is the opposite of financial inclusion. Banks in Hong Kong have purportedly denied financial services to customers that they consider high risks for ML/TF, giving rise to the term 'de-risking' or 'de-banking' (Lee, 2017).[14]

The legal issues underlying banks' recent proclivity towards 'de-risking' are intricately connected with heightened AML/CFT requirements and increased compliance costs for banks in the post financial crisis era. As the Hong Kong Monetary Authority (HKMA) promotes FinTech innovation, some banks have adopted FinTech solutions to help them file STRs and to on-board clients. At the core of the FinTech revolution is a quest to determine what embodies a robust system for checks and balances under the AML/CFT regime. Technical solutions to de-risking, such as FinTech and blockchain-based smart contracts therefore warrant careful consideration by regulators, policy makers and other stakeholders, such as banks and tech firms. Given that AML/CFT actions will continue to be in search of processes driven by FinTech solutions, this article also assesses the current climate of AML/CFT enforcement, referring in particular to the exponential growth of STRs in Hong Kong, alongside governance oversight by regulators as they contemplate applying regulatory technology (RegTech). This article adds to the literatures on financial inclusion, FinTech/RegTech and AML/CFT. Interdisciplinary in its scope and coverage, the article has a multifaceted dimension that intersects with banking governance (banking law), the KYC-CDD requirement (AML/CFT law) and information technology (FinTech and RegTech). In these contexts, this article first takes on the critical task of examining Hong Kong's current AML/CFT law, as, because of the processes associated with legal and regulatory compliance, it can both empower banks and distort the way in which they open and maintain bank accounts. After a brief account of the problem of banks' de-risking practices, the article addresses the public policy tensions between promoting financial inclusion on the one hand and upholding AML/CFT compliance on the other. Finally, this article evaluates FinTech's potential to reduce the problem of de-risking

[14] For a more comprehensive and detailed account of the financial inclusion discourses and the evolution of the perceived financial exclusion problem in Hong Kong, *see* Lee E (2017), Financial inclusion: a challenge to the new paradigm of financial technology, regulatory technology and anti-money laundering law. *Journal of Business Law*, issue 6: 473-498.

through blockchain-based smart contract deployment. The overarching theme of this article is financial inclusion. From a comparative law perspective, access to basic financial services has been recognised as a basic civil right by the European Accessibility Act (EAA).[15] The EAA is a directive that can be relied on to promote better equality for consumers ranging from individuals to SMEs as well as micro-enterprises, and the products and services covered by the EAA include, among others, banking services.[16] Perhaps more relevant to this article, the SME test, a specific assessment of the impacts on SMEs and micro-enterprises, has also been carried out through consultation with an SME panel,[17] implying that special attention must be given to the needs and market opportunities of SMEs, given that their size and limited resources can potentially limit their access to equal rights, a common issue caused by differences in national accessibility requirements that lead to disproportionate problems for SMEs.

Although the EAA aims to 'increase the availability of accessible products and services in the internal market',[18] it also identifies that the barriers to the free movement of certain accessible products and services could be attributed to divergent accessibility requirements in the Member States. Given that the de-risking practice by those Hong Kong banks being named and shamed does not have a cross-border nature, nor does it concern the problem of trade barriers associated with divergency in laws, regulations and administrative provisions of the EU's Member States as regards accessibility requirements for certain products and services. The EAA's unique role in facilitating barrier-free cross-border trades across the EU and in implementing accessibility obligations in areas such as public procurement, as well as improving accessibility of products and services for persons with disabilities, has no bearing on the problem of

[15] On 13 March 2019, the European Parliament adopted the European Accessibility Act (Directive 2019/882/EC of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services). The Act establishes mandatory European requirements on certain products and services, including access to basic financial services.
[16] European Commission, Employment, Social Affairs and Inclusion (containing the European Commission's illustration of its policies and activities for European Accessibility Act, https://ec.europa.eu/social/main.jsp?catId=1202.
[17] European Commission (2015) - Commission Staff Working Document. Executive summary of the impact assessment - proposal for a Directive of the European Parliament and of the Council on the approximation of the laws, regulations and administrative provisions of the Member States as regards the accessibility requirements for products and services, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0265&from=EN at 6.
[18] Recital (1), EAA.

financial exclusion in Hong Kong that has led to increased difficulty in bank account opening. However, to the extent that the EAA aims to promote a market environment where products and services are more accessible, thus allowing for a more inclusive society[19], it is consistent with the HKMA's policy aim (HKMA, 2016).[20]

The article is organised as follows. Following this introduction, section two expounds on the connection between banks' de-risking practices and financial exclusion as the author identifies and analyses the key policy tensions associated with them. Section three discusses the existing solution (tiered account services) for tackling the problem of de-risking, alongside other solutions (KYC Utility system and central data repository (CDR)) that have been proposed by regulators, policy makers and commentators. Whereas the existing solution is likely to mitigate the effect of de-risking, the implementation of the proposed solutions will, in the view of the author, be less likely to have a substantial impact as they were not designed for, and hence not intended to solve, this specific problem (de-risking). Section four presents the main research findings of this article as the author proposes alternative solutions (FinTech and blockchain-based smart contracts) different from the existing and proposed solutions, in anticipation of increasing financial inclusion. Section five offers some concluding remarks.

The problems of de-risking and the importance of financial inclusion: key policy tensions

There are five key central policy tension points that may be of concern or interest to the regulators, policy makers and stakeholders of banking institutions. From the public policy vantage point, these central policy tensions have not only had deep implications for banks' AML/CFT law compliance, but have also gravely impacted the opening of bank accounts in Hong Kong, further resulting in the banks' de-risking practices, as alluded to in the Hong Kong Institute of Chartered Secretaries' two survey reports

[19] Recital (2), EAA.

[20] HKMA (8 September 2016), De-risking and financial inclusion, http://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2016/20160908e1.pdf. For this very reason, a circular was issued to banks on 8 September 2016 in which the banking regulator (i.e. the HKMA) warned banks against de-risking, which could potentially force those individuals and business entities deemed 'marginalised' (because of the adverse impacts they suffered due to banks' de-risking practices) to rely on an underground economy for meeting their financing needs, thus increasing the risks to the financial system as a whole because the underground economy, which operates in the dark, might escape the regulator's oversight.

published in 2016 and 2018.[21] In the following paragraphs, the author will first highlight these points of central policy tension and then provide her comments after each central policy tension point.

1. It is debatable whether the risk-based approach, by which banks are on the one hand encouraged to open accounts for individuals or business entities with higher ML/TF risks but will, on the other, be burdened with higher responsibility for the continued monitoring of such accounts for a period of time, is consistent with the financial institutions' expectations.

As set out in the Hong Kong Money Laundering and Terrorist Financing Risk Assessment Report, published periodically by the Hong Kong Special Administrative Region Government, the Government is committed to upholding a robust regime that fulfils the international AML/CFT standards (HKMA, 2018b).[22] In theory, and as recommended by both the local authority (HKMA) and the international authority (FATF), the risk-based approach should be applied by banks for the purposes of client on-boarding and financial transaction monitoring. Considering that many banks have different intelligence teams and functions, an 'experience-based risk assessment' has been advocated as a replacement for the 'risk-based approach' (Shamdasani, 2017: 138).[23] It is suggested that the risk-based approach is problematic, as it highlights potential risks which are more speculative than real and potentially difficult to determine.[24] Whether the experience-based approach is a workable alternative to the risk-based approach is a practical issue.

Since financial institutions have diverse practices and a range in staff experience, the risk-based approach might be contested because risk-based decisions or

[21] The Hong Kong Institute of Chartered Secretaries (HKICS) (September 2016), Bank account opening survey, https://www.hkics.org.hk/media/publication/attachment/PUBLICATION_A_2384_HKICS_Bank_Account_Opening_Survey_report_.pdf. *See* also HKICS (July 2018), 'Bank Account Opening Survey—Continuing difficulties in companies opening bank accounts in Hong Kong', https://www.hkics.org.hk/media/publication/attachment/PUBLICATION_A_2418_HKICS_Bank_Account_Opening_Survey_Report_2018.pdf.

[22] HKMA (19 October 2018), Policy and supervisory approach on anti-money laundering and counter-financing of terrorism', https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2018/20181019e4.pdf. In which the HKMA's AML/CFT Policy was set out in the 'Annex'.

[23] Shamdasani A (2017), Risk-based AML compliance has problems, bank official says. *Hong Kong Lawyer* 138.

[24] *Ibid*.

judgment calls may make inexperienced staff, or those whose firms see limited AML/CFT cases, uncomfortable when it comes to exercising their judgement in AML/CFT compliance procedures. In these circumstances, an alternative approach—that is, the 'experience-based approach'—might be proffered, although it does come with a risk. Allowing a financial institution to rely too much on its own limited experience can lead to uncertainty regarding expectations and make it difficult to apply uniform regulatory treatment in the implementation of the risk-based approach. To avoid such uncertainty and further, to disincentivise financial institutions from excusing themselves from potential AML/CFT liability, the risk-based approach should be upheld and not diminished by the experience-based mechanism. Indeed, the FATF, in facilitating the risk-based approach, has required financial institutions to exercise 'sound judgement' by having a good understanding of the risks, thus requiring the building of expertise within financial institutions through, for instance, training, recruitment, taking professional advice and 'learning by doing' (FATF, 2007).[25] These actions will equip them to assess risks more accurately. Otherwise, financial institutions may overestimate risk, which could lead to wasted resources or the rejection of clients who pose no threat to the financial system, thereby deepening the financial exclusion problem. Or, conversely, they may underestimate risk, thereby rendering themselves vulnerable (FATF, 2007).[26]

At the international level, in the 2017 FATF Guidance on AML/CFT measures and financial inclusion, there exists no officially coined term for the so-called 'experienced-based approach', although the FATF purported the meaning of the term as it demonstrated country examples of CDD measures adapted to the context of financial inclusion (FATF, 2017).[27] But prior to 2017, the utilisation of 'experience' by staff or specific compliance/AML officers—in deciphering suspicious transactions and ML/TF cases—has been advocated by the FATF for the risk-based approach, which is to move away from 'one-size-fits-all' solution, thereby making the AML/CFT regime tailored to

[25] Financial Action Task Force (FATF) (June 2007), Guidance on the risk-based approach to combating money laundering and terrorist financing—high level principles and procedures, http://www.fatf-gafi.org/media/fatf/documents/reports/High%20Level%20Principles%20and%20Procedures.pdf, at 4, paragraph 1.20.
[26] *Ibid*.
[27] FATF (November 2017), FATF guidance anti-money laundering and terrorist financing measures and financial inclusion with a supplement on customer due diligence, https://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf at 3.

specific national or institutional risk context (FATF, 2007: 44).[28] Given that the risk-based approach has already incorporated the use of experienced staff in making judgement calls, it might be argued that the 'experience-based approach' can be used to supplement or complement the risk-based approach, even though the different judgement calls may bring about uncertainty or even result in a lack of uniformity in the final AML/CFT decision-making.

According to the FATF, the risk-based approach also requires 'resource and expertise to gather and interpret information on risks, both at the country and institutional levels, to develop procedures and systems and to train personnel'.[29] In implementing the risk-based approach, 'financial institutions should be given the opportunity to make reasonable judgments. This will mean that no two financial institutions are likely to adopt the exact same detailed practices',[30] added the FATF.

At the local level, under the HKMA's guideline on AML/CFT for authorised institutions, a bank should appoint at least a compliance officer (CO) and a money laundering reporting officer (MLRO) to implement the authorised institution's AML/CFT systems and to comply with relevant legal and regulatory obligations, as well as ensuring that ML/TF risks are managed effectively (HKMA, 2018c).[31] In particular, the senior management of an authorised institution should appoint a CO at the management level to assume the overall responsibility for the establishment and maintenance of its AML/CFT systems, and a senior staff as the MLRO to act as the central reference point for suspicious transaction reporting.[32] The word 'seniority' implies that the MLRO should be backed by sufficient knowledge and experience, which can be drawn upon when the MLRO makes risk-based decisions and judgment calls. In practice, the MLRO, upon reviewing transaction patterns and volumes through connected accounts, and making reference to any previous pattern of instructions given by a bank client and to the length of the bank's business relationship with the client,[33]

[28] FATF, Guidance on the risk-based approach to combating money laundering and terrorist financing—high level principles and procedures, *supra* note 25, at 44, paragraph 37.
[29] *Ibid*. at [4], paragraph 1.19
[30] *Ibid*, paragraph 1.22.
[31] HKMA (2018), Guideline on anti-money laundering and counter-financing of terrorism (for authorized institutions) (Revised October 2018), https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/g33.pdf, at 12, paragraph 3.5.
[32] *Ibid*. at [13], paragraph 3.7.
[33] *Ibid*. at [63], paragraph 7.17.

should determine whether it is necessary to make a suspicious transaction report. The requisite knowledge and experience regarding the AML/CFT requirements are crucial for the MLRO, who is appointed by an authorised institution to act as a central reference point for reporting suspicious transactions and to serve as the main point of contact with the JFIU and law enforcement agencies.[34]

Based on the above reasons, the author sees no apparent advantage in substituting the risk-based approach with the experience-based approach, the latter of which may have resulted from a misconstruction of the AML/CFT legal requirement given that the term 'experience' often appears as one of the job requirements for AML analysts. For these analysts, experience is acquired when they assist their employer, a bank, in the application of the risk-based approach set by a banking regulator such as the HKMA, in reference to the same risk-based approach set by the FATF. Understandably, an AML analyst's experience with regulatory and compliance management is crucial in fulfilling their job duties and responsibilities, which include overseeing a database of financial transactions, monitoring suspicious transactions, conducting due diligence on suspicious accounts, and helping banks file suspicious activity reports to regulatory authorities.[35]

While banks are expected by the regulatory authorities to adopt the risk-based approach for KYC-CDD purposes, the onus is on the bank to complete the CDD procedure. Even if the risk-based approach is applied, moreover, banks can still freely decide, on the basis of their own experience, whether to accept or reject bank account opening applications, possibly drawing on reports or assessments conducted by their intelligence teams and functions. It is plausible to think, from the bank's perspective, that the experience-based approach is more advantageous than the risk-based approach, as the former will probably help banks build a stronger defence case if their compliance with the AML/CFT law is found wanting. The risk-based approach alone, however, does not explain why banks have become extremely risk averse, as mirrored in the problem of the exponential growth of STRs. As shown by the statistical data released in 2016 by the JFIU, one of the AML/CFT regulatory authorities in Hong Kong to which the STR should be made, the number of cases made annually in the form of STR over the ten-year period 2006 to 2016 are as follows: 14,557 (2006), 15,457 (2007), 14,838

[34] *Ibid*. at [14], paragraph 3.10 and at [61], paragraph 7.9.
[35] ZipRecruiter Marketplace Research Team, What is an [AML] analyst and how to become one, https://www.ziprecruiter.com/Career/Aml-Analyst/What-Is-How-to-Become#AML-Analyst-Job-Description-Sample.

(2008), 16,062 (2009), 19,690 (2010), 20,287 (2011), 23,282 (2012), 32,907 (2013), 37,188 (2014), 42,555 (2015) and 54,572 (2016).[36] Although the JFIU has experienced rapid growth in STR filing, there is no information available as to whether there is a 'conversion' of any additional or successful criminal convictions (over ML-TF charges) directly from these additional STR numbers (Coburn, 2016).[37] The author does not consider the risk-based approach and the experience-based approach to be significantly different. Banks, in other words, may engage in de-risking practices regardless of whether they choose to apply the risk-based approach or the experience-based approach, provided they are intent on shielding themselves from potential criminal prosecution and substantial fines or avoiding possible inconvenience to themselves and regulatory reprisals. The author would therefore suggest adhering to the risk-based approach, given that the experience-based approach offers no apparent advantage in improving AML/CFT regulatory compliance. Adhering to the risk-based approach will closely align Hong Kong's regulatory standard with the international one, as the risk-based approach is recommended by the FATF.

2. A nuanced AML approach is instrumental to financial inclusion, as concerns of non-compliance regulatory liability cannot be assuaged by a reduction in investigation numbers.

According to an international law firm's report published in 2017, the HKMA has reduced AML investigations of financial institutions by about 20 per cent in order to focus on large-impact cases, showing a more effective way to allocate regulatory monitoring resources.[38] Nevertheless, one is prone to think that the reduction in the 'number' of investigations against financial institutions would not necessarily alleviate financial institutions' concerns of AML/CFT compliance costs as it cannot fully capture the likelihood of the 'amount' of fines payable due to perceived non-compliance by the HKMA with the prevailing (more strict) AML/CFT law and regulations. In this regard, the author would suggest that the HKMA establishes a special webpage or detailed guide to define 'large impact cases'. What characteristics do they bear, for example, and

[36] Kwok K S, Joint Financial Intelligence Unit & suspicious transaction reporting, https://www.fstb.gov.hk/fsb/aml/en/edu-publicity/seminar2016/MSO_SuspiciousTransactionReporting.pdf. At the time the presentation was made, Ms Kwok worked as a senior inspector of police at the JFIU.
[37] Coburn N (October 2016) Unclear whether suspicious transaction reports helping to win the AML/CTF fight. *Hong Kong Lawyer,* http://www.hk-lawyer.org/content/unclear-whether-suspicious-transaction-reports-helping-win-amlctf-fight.
[38] Freshfields Bruckhaus Deringer LLP (20 June 2017), Enforcement trends in Hong Kong, at 70.

are they equated with 'highly suspicious cases' and, if so, why are they considered noncompliant? Even a sample check list for regulatory non-compliance would be preferable to nothing. In the absence of such a list, financial institutions may have to prepare to absorb additional or even disproportional regulatory compliance costs whenever new changes are announced.

3. Stricter application of AML/CFT law, coupled with higher AML/CFT compliance costs—which include the fines payable for inadequate compliance or non-compliance, as found by the regulator—may inhibit a bank from trading with customers it considers too risky or from entering into a business relationship with them. In most of these cases, the affected parties cannot provide evidence to prove the legitimacy of their income or source of wealth required by banks on-boarding clients, even though they do not necessarily pose a threat to the financial system.

There is clearly a tension between upholding the regulatory aim of preventing ML/TF risks with stricter application of AML/CFT law, and the banking industry's calling on the regulator (HKMA) to strike a balance between costs and benefits while imposing AML/CFT duties. If the AML/CFT law is too strict, it will likely exclude the poorer sector of the economy from access to the financial system. If the law is too lax, however, law enforcement actions may have to be stepped up in order to contain the increased risks, ultimately resulting in high compliance costs and potential liabilities. FinTech could possibly be used to address this tension, although it offers no panacea. For details, see the next point.

4. FinTech is no panacea for resolving the financial exclusion problem.

This comment is made in response to the industry's claim, albeit technically unverified, that distributed ledger technology (DLT, more commonly known as blockchain technology) can increase financial inclusion. The claim was proffered on a proclamation that DLT is an enabler that can support transaction verification and, as such, can help financial institutions more accurately monitor and capture ML/TF risks. Utilising DLT to store customers' personal data and financial details, furthermore, can facilitate the real-time approval of bank account opening documents. From the financial inclusion viewpoint, the significance is two-fold. First, DLT can reduce banks' locked-in capital (for absorbing default risks) and second, the capital saved can be used to make loans to SMEs or start-ups to which they were previously unavailable.

MANUSCRIPT
(FOR PUBLISHED VERSION, PLEASE REFER TO: 'Technology-Driven Solutions to Banks' De-risking Practices in Hong Kong: FinTech and Blockchain-based Smart Contracts for Financial Inclusion', *Common Law World Review*, Vol. 51(1-2), pp. 83-108 (May 2022, published online)

The permanent link for this article is https://doi.org/10.1177/14737795211071095

The author agrees to some extent that smart contracts which are deployed on blockchain technology may be a possible solution for expanding financial inclusion. Smart contracts are indeed capable of automatic execution and would therefore involve no biases or opportunity for discrimination. In this light, smart contracts could potentially aid in financial inclusion by removing banks' human inclination to deny certain groups access to banking. Blockchain-based smart contracts could be designed to focus on specific and deterministic tasks, such as flagging suspicious transactions. (Detailed discussion pertaining to the pros and cons of blockchain will follow in section four.) Although technology (e.g. blockchain) is in place, large international banks that dominate the financial system may be resisting changes brought about by the technology which makes cross-border payment, a banking service necessary for SMEs in import-export businesses, more efficient than banks' wire transfer services. It boils down to the question of competition. The third-party payment institutions (e.g. PayPal, Alipay) or technology firms that invented digital wallets (also known as 'e-wallets') can hardly compete with large international banks without access to the international funds transfer system, to which the large international banks have access. According to a co-rapporteur on the new EU Task Force on AML Effectiveness, however, the 'large international banks are making it harder and harder for payment institutions to use their services, allegedly because they feel the AML systems introduced by the payment systems are not good enough'.[39] The author envisions that, in time, the role of technological innovation in the international payment system will increasingly become a point of concern for central banks and banking authorities worldwide.

With its combined forces of technology and innovation, FinTech prevails in a financial industry embroiled in a period of digital disruption and transformation. Although FinTech has surged in transforming payments, lending and wealth management, among other banking activities, and has aided in the improvement of the customer's experience with banking, the challenges and impediments brought about by FinTech are also known to FinTech stakeholders, including banking specialists, computer scientists and data analysts. Their vested interests in FinTech make them particularly aware of certain issues ranging from cybersecurity to the financial services industry's intermediary role, the latter of which is threatened by the new decentralised, disintermediated and autonomous systems that FinTech represents, particularly in regard to blockchain technology. In his opening speech on the second day of the Future of Finance 2017 in Singapore, Emmanuel Daniel, chairman of the Asian Banker,

[39] A private email exchange on 2 June 2020 between the author and a co-rapporteur regarding the new EU Task Force on AML Effectiveness on (a) the impact of stricter application of AML/CFT law on banks' de-risking practices; and (b) the challenges of FinTech innovations for easier cross-border payments.

flagrantly suggested that the word 'FinTech' should be banned, as he contemplated and warned about the potential loss of financial services industry's intermediary role.[40] Similarly, three American academics, who documented FinTech's disruptive effect by focusing on the Internet of Things, robo-advising, and blockchain, all regarded as the most valuable FinTech innovation types, also stated that 'FinTech innovations affect industries more negatively when they involve disruptive technologies',[41] adding that the incumbent market leaders, such as traditional banks, need to invest heavily in their own innovation to avoid much of the disruption by start-ups.[42] To further add to their point, the authors stressed that the promises and pitfalls of FinTech will, to a large extent, depend on the design of a particular FinTech innovation tailored to the needs of different categories of customers or investors, as in the case of robo-advisory.[43] Apparently, these positions contrast with the Techno-utopian perspectives which, explained by Campbell-Verduyn et al, are prone to treat technology and its by-product, such as big data, as 'a powerful tool to address various societal ills' [44] and 'the new panacea to most human problems'[45] which may include financial exclusion (Campbell-Verduyn et al., 2017: 222). The author disagrees with the Techno-utopian view of FinTech as it risks overstating the value of FinTech while downplaying its potential risks to the financial industry and its customers alike.

5. The principle of proportionality, the risk-based approach and the cost-benefit approach should be jointly considered in weighing the pros and cons of adopting FinTech innovations.

The principle of proportionality denotes a flexible, less intrusive principle calibrated to the regulatory objectives of general interests recognised by the law or the regulators' governing policies, taking into account the bank's size, its internal organisation and the scope and complexity of its business model and activities (Chiti et al., 2020: 663).[46] Being a flexible and multifaceted principle, this particular feature also leaves some

[40] TABLive (16 June 2017), Let's ban the word 'FinTech', [it's] not a panacea, https://live.theasianbanker.com/video/lets-ban-the-word-fintech,-its-not-a-panacea.
[41] Goldstein I, Jiang W and Karolyi GA (2019) To FinTech and beyond. *The Review of Financial Studies* 32(5): 1656-1657.
[42] *Ibid* at [1657].
[43] *Ibid*. at [1656].
[44] Campbell-Verduyn M, Goguen M and Porter T (2017) Big data and algorithmic governance: the case of financial practices. *New Political Economy* 22(2): 222.
[45] *Ibid*.
[46] Chiti MP, Macchia M and Magliari A (2020) The principle of proportionality and the European Central Bank. *European Public Law* 26(3): 663.

room for proportionality in its implementation. Indeed, the principle of proportionality can be applied in different types and sizes of financial institutions and interpreted differently by regulators across jurisdictions (Busch et al., 2019: 278).[47] From an ex-ante perspective, proportionality is capable of governing and orienting banks' actions or responses towards the legislative and administrative requirements to which they are subject,[48] giving rise to the concept of banking supervision and the very idea of prudential regulation (Chiti et al., 2020: 643). The latter is 'inherently associated to a risk-based approach that takes into account the banks' risk profile' (Chiti et al., 2020: 664).[49] In light of this, the principle of proportionality is not only reflected in the supervisory regulatory framework but also tailored to the risk-based approach. Since the risk-based approach is advocated by the FATF, the international standard setter, and in turn adopted by the HKMA, the local regulator, for the implementation of AML/CFT law, applying the proportionality principle into the decision-making process of the HKMA also implies that the HKMA has 'the relevant experience and in-depth knowledge of the banks they supervise' (Chiti et al., 2020: 665).[50] A banking supervisor such as the HKMA will therefore be best placed to ensure a case-by-case proportional application of the substantive law, such as the AML/CFT law, by exercising its discretionary power (Chiti et al., 2020: 665).[51] Such flexibility will likely generate the most interest or concern in a case where the supervisor lays down penalties against a bank considered to have fallen short on its compliance duty. In those circumstances, the supervisor should duly consider the necessity of the measure, meaning it should only be taken where alternative or less restrictive means are inapplicable.

Proportionality— a balanced approach to legislation— should be adopted in order to minimise regulatory burden and compliance costs on affected businesses. Proportionality is a cardinal principle in the application of the global AML/CFT regime. Following this line of thought, the risk-based approach should include, but is not limited to, the proportionality approach and the cost-benefit balancing approach. Consideration of FinTech's potential to reduce the problem of de-risking should also be given to the value added to regulatory compliance. The reason is two-fold. First, since banks play a predominant role in Hong Kong's financial system, there may be little or no incentive

[47] Busch D, Ferrarini G and Solinge GV (ed) (2019) *Governance of Financial Institutions*. Oxford: Oxford University Press (In 'Part II Governance structure and regulations, 11 Compensation in financial institutions: systemic risk, regulation, and proportionality' at 278 (11.63)).
[48] Chiti MP, Macchia M and Magliari A, *supra* note 46 at 643.
[49] *Ibid*. at [664].
[50] *Ibid*. at [665].
[51] *Ibid*.

for them to adopt innovative but expensive technology-based methods in order to verify customer identity and store biometric data (e.g. fingerprints and iris scans) in the expectation of increasing access to the banking system. This may well be a reason why financial inclusion was difficult to achieve satisfactorily in the first place. Second, potentially higher costs are involved in the initial stages of building a financial infrastructure that meets KYC-CDD requirements. In an informal interview conducted by the author, a senior executive in a leading investment bank in Hong Kong revealed the state of impenetration of FinTech in Hong Kong for KYC-CDD purposes, stating plainly, 'We do not know whether the client will stay for two years or ten years.'[52] The effect of uncertainty cannot be easily overcome or mitigated without a robust cost-benefit analysis. Since the costs of FinTech investments are potentially high and will ultimately be borne by banks, sustainability is a hard factor that must be grappled with and carefully assessed by banks, which are profit-making institutions, to ensure their projected revenue income is positively linked with the number of clients interested in engaging their services. Banks are understandably reluctant to develop these alternative identification data for CDD when dealing with customers who lack standard identification documents or a stable income. Individuals, start-ups and SMEs with low income or revenue are cases in point, and banks make little or no money in providing services to them. In such circumstances, banks would have to decide for themselves whether to bear the cost of using a real-time verification system enabled by FinTech for acquiring and storing customer information.

In view of banks' calls on the regulator (HKMA) to strike a balance between costs and benefits while imposing AML/CFT duties, the answer, or rather, the decision, very much depends on the HKMA's future regulatory policy towards FinTech and RegTech developments. The HKMA's policy directives have so far been rather positive towards financial inclusion. To tackle the issue of financial inclusion, which has strong public policy implications, however, the HKMA has the mandate and responsibility to continue seeking to determine whether financial exclusion, which is the opposite of financial inclusion as is typified by banks' de-risking practices, is a short-term or long-term problem for Hong Kong.

The Existing and Proposed Solutions to De-risking

[52] The interview took place on 16 November 2018. The interviewee, who wished to remain anonymous, explained to the author why his institution had reservations about embracing FinTech for KYC-CDD purposes.

MANUSCRIPT
(FOR PUBLISHED VERSION, PLEASE REFER TO: 'Technology-Driven Solutions to Banks' De-risking Practices in Hong Kong: FinTech and Blockchain-based Smart Contracts for Financial Inclusion', *Common Law World Review*, Vol. 51(1-2), pp. 83-108 (May 2022, published online)

The permanent link for this article is https://doi.org/10.1177/14737795211071095

1. Existing solution: Tiered account services

'Existing solution' refers to a practice or process already adopted by (some) banks to mitigate the problem of de-banking. Progressive or tiered CDD approaches, as demonstrated in the FATF Guidance for promoting financial inclusion, have recently and gradually been put into practice in Hong Kong, and their impact is likely to be quite positive (FATF, 2017: 10).[53] These approaches have been developed as a result of the application of the risk-based approach to CDD measures (FATF, 2017: 10).[54] By implication, in order to facilitate financial inclusion, reasonable flexibility is given to banks with respect to the types of identifying information required.

To put the risk-based approach into practice, 'tiered account services' is a new initiative adopted by the HKMA to promote financial inclusion in Hong Kong. In order to enhance the customer experience, while following the risk-based approach, the HKMA has explored with banks the introduction of 'simple bank accounts' (SBAs), a new tier of bank accounts derived from traditional accounts which focus on the provision of basic banking services (such as deposits, withdrawals, local and cross-border remittances, etc.) (HKMA, 2019).[55] The narrowing of the service scope and transaction volume of traditional bank accounts means that the risks involved in SBAs are lowered and less extensive KYC-CDD measures are required; in practice, the result is less detailed customer information and fewer supporting documents from applicants (HKMA, 2019).[56] According to the HKMA, as of 12 April 2019, three note-issuing banks in Hong Kong[57] have launched the SBAs' services for corporate customers, including SMEs and start-ups but excluding offshore companies with complex structures, emphasising that there is no 'one-size-fits-all' approach for SBAs and that individual banks may therefore design their own SBAs in accordance with their business strategies and risk management strategies.[58] By the same token, individual banks can exercise discretion as to whether to implement SBAs and, if so, the extent to

[53] FATF (November 2017), FATF guidance anti-money laundering and terrorist financing measures and financial inclusion with a supplement on customer due diligence', *supra* note 27, at 10.
[54] *Ibid*.
[55] HKMA (12 April 2019), Tiered account services: a new initiative on promoting financial inclusion, https://www.hkma.gov.hk/eng/key-information/insight/20190412.shtml.
[56] *Ibid*.
[57] Three commercial banks, namely the Hongkong and Shanghai Banking Corporation Limited (i.e. HSBC, Hong Kong), Bank of China (Hong Kong) Limited, and the Standard Chartered Bank (Hong Kong) Limited, have been given authorisation by the Hong Kong government to issue bank notes in Hong Kong.
[58] HKMA, Introduction of tiered account services, Circular, ref: B1/15C, B9/67C, B10/1C. *See also* HKMA, Tiered account services: a new initiative on promoting financial inclusion, *supra* note 55.

which a narrower scope of services is to be offered, on the basis of their own risk assessments and simplified CDD measures. The successful launch of tiered account services has prompted the HKMA to call upon other banks to participate in the initiative by addressing the needs of corporate customers in the initial and subsequent stages, in order to help further promote financial inclusion in Hong Kong. While some business customers may not require the full range of banking services at the initial opening of the account, as their businesses grow and mature, they may require services generally offered by traditional accounts. SBAs are closely in line with the overarching principles of the risk-based approach because tiered accounts may transition to accounts offering a wider range of services and, were they to do so, banks would have to conduct further CDD measures commensurate with the risks involved.[59] Currently, it is unclear whether the SBAs will be offered to individuals previously excluded from access to banking.

The author presupposes that providing the option of SBAs is only one step on a long road, although SBAs represent an important step for the HKMA, which set up a dedicated team in March 2017 to handle public enquiries about opening bank accounts in Hong Kong. This followed a litany of financial exclusion reports and a circular issued by the HKMA to banks, warning against the risk of de-risking (HKMA, 2016).[60] From the author's viewpoint, the progressive or tiered CDD approaches can be further incorporated into the jurisdiction's existing AML/CFT legislation to enable financial institutions to rely on specific legislative provisions that permit flexibility in financial institutions' identity verification. The implementation of this approach can potentially increase the level of financial inclusion for at least two reasons. First, in cases where banks cannot fully ascertain the client's identity using prescribed AML/CFT measures, they can open deposit bank accounts for low-risk clients, to allow for financial inclusion. Such is the practice in Canada, where flexible means of identifying customers have been put in place through regulatory amendments to the country's AML/CFT framework that came into force in June 2016 (FATF, 2017).[61] Second, if public policy so directs, banks may be willing to take calculated risks in accepting bank account opening applications when full disclosure of information in relation to CDD is not available or impossible to obtain from the potential customer. Such willingness on the part of banks, however, does not easily materialise without legislative backing. That is to say, if the existing legislation can permit banks flexibility in applying different

[59] *Ibid*.
[60] HKMA, De-risking and financial inclusion, *supra* note 20.
[61] FATF (November 2017), 'FATF guidance anti-money laundering and terrorist financing measures and financial inclusion with a supplement on customer due diligence', Box 8. 'Canada-Flexible means of customer's identification when prescribed measures cannot be used', *supra* note 27.

identity verification controls in a reliable and risk-based manner, it could incentivise banks to gradually open banking access to low-income individuals or businesses (especially entrepreneurs who are representatives of start-ups that generate low income for themselves and their businesses) that were previously denied bank accounts because of their inability to provide residential or business addresses or other information required by the bank, although they did not necessarily pose a threat to the stability of the financial system. This is especially the case if they were using hot-desks or rented co-working spaces, which are perfectly legitimate reasons for not having business addresses. To enhance public policy in promoting financial inclusion, and as a start, regulators may wish to consider granting reasonable flexibility to banks of good standing, which are normally technically equipped and capable of conducting identity verification, provided that these banks can prove to the regulators' satisfaction that any customer data, whether technology-based or not, are acquired with due customer consent and governed by stringent data protection and privacy measures to ensure data integrity and prevent data leakage. The reason is self-explanatory: in the digital age, in which technology is deployed for conducting KYC-CDD, money launderers and terrorist financiers can use leaked data to commit fraud.

2. Proposed Solutions

Proposed solutions are those that have not been adopted by banks but have been proposed by regulators, policy makers and commentators. Details are spelled out below.

2.1 eKYC (KYC Utility system)

In the post global financial crisis era, the heightened KYC requirements connote not only higher AML/CFT compliance costs, but also grandiose liabilities for non-compliance by those upon whom the legal responsibilities to conduct CDD have been imposed. In Hong Kong, the AMLO and the various AML guidelines impose statutory CDD and record-keeping obligations on financial institutions, thus incentivising banks to invest in new digital technology for on-boarding new clients and storing client information using cloud and digital bank identification (ID). A digital ID solution is being explored as Hong Kong aspires to become a smart city. To that end, a government-led initiative to support a digital ID solution is the cornerstone to e-KYC through a KYC utility (KYCU) system.

In practice, digital ID and KYC utilities are thought to be the building blocks to addressing issues surrounding individual and corporate digital ID in the AML/CFT

CDD process. This being the case, the government may extend the current digital ID system that already contains the core CDD data to the financial institutions for the purposes of AML/CFT regulatory compliance.[62] An element of public ownership of KYCU is desirable, as it can enhance trust from the financial customers' perspective, whether they are individuals, SMEs, start-ups or large corporations, since the core CDD data are generally issued by agents of the government. In that respect, reliance by financial institutions on the accuracy of core CDD data is warranted. In terms of cost and responsibility sharing for FinTech errors and malfunctions, the KYCU infrastructure could be built by the government, the private sector (e.g. financial institutions) or through the joint efforts of both. The goal is to strategically optimise the AML/CFT CDD process in risk management, assessment and monitoring and, ultimately, increase the penetration of financial inclusion in this region. However, as FinTech is still under development, liability for incomplete or incorrect CDD provided to the KYCU can be hard to gauge, particularly because potential ownership models for a KYCU include public, private and hybrid models.[63] This lack of clarity can be a source of grave concern for financial institutions that volunteer to participate in building a KYCU. Likewise, data privacy and cybersecurity are two key challenges for customers deciding whether to accept a KYCU, if and when they are requested by financial institutions or KYCU system owners to give their personal data.[64]

2.2 Central Data Repository

To devise a cost-effective solution for banks, as well as to seek to drive adoption of a digital financial inclusion framework, thereby enhancing data quality and protection for financial customers, the Financial Services and the Treasury Bureau (FSTB) has led a working group to discuss the development of a central data repository (CDR) to be used by financial institutions in Hong Kong.[65] The CDR, which involves using the cloud to store data under strict control standards, can be used for account opening purposes as it

[62] The core CDD data are safely stored and readily available, and can generally be issued by agents of the government of the Hong Kong Special Administration Region, China. These external trusted sources of data are extant, readily available, and kept by multiple government departments such as the Inland Revenue Department (including the business registration unit), the Immigration and Transport Departments. *See* (Hong Kong) Financial Services Development Council (June 2018), Building the technological and regulatory infrastructure of a 21st century international financial centre: digital ID and KYC utilities for financial inclusion, integrity and competitiveness', FSDC Paper No. 35.
[63] *Ibid*. at [36].
[64] *Ibid*. at [35].
[65] *Ibid*. at [33].

should cover the initial and ongoing KYC requirements under the AML/CFT laws and regulations in Hong Kong.[66]

Realistically, a CDR is like a warehouse into which the individual can deposit his/her CDD information. To ensure data privacy and financial customer protection, the individual is the owner of the information and can therefore decide on what information to give and to share with parties involved in, say, a smart contract for making transactions or payments. To verify the truthfulness and accuracy of the information input to the CDR, an individual's information shall be audited by auditors who may be located at different jurisdictions. That is because trust is absolutely necessary in this case and needs to be addressed and built into the process of information sharing and coordination, particularly when it entails cross-border transactions empowered by smart contracts.

Alternative Solutions: FinTech and Smart Contracts

In the view of the author, although the KYCU system and CDR have been flaunted in order to assist financial institutions with AML/CFT regulatory compliance, their core value lies in the construction and utilisation of digitalised ID pertaining to financial customers in the context discussed in this article. The KYCU system and CDR will be positive to enhance digital financial infrastructure, which is fundamental to financial inclusion, but they will likely be neutral to the de-risking problem. Stated differently, the KYCU system and CDR were not strategically or specifically designed to mitigate the effect of de-risking, and do not, in and of themselves, provide feasible solutions. Instead, this article proposes that FinTech and blockchain-based smart contracts may provide alternative solutions to the de-risking problem.

1. FinTech and Blockchain-based Smart Contracts: Technical Solutions to De-risking

These are different from the existing and/or proposed solutions described in section three, given that artificial intelligence (AI) would be applied to support blockchain, which, if so desired, could be functionally designed to address some of the policy tensions shown in section two. For instance, blockchain-based smart contracts could be designed to focus on specific and deterministic tasks, such as the flagging of suspicious

[66] Standard Chartered Bank (January 2019), How to make on-boarding new customers simpler, faster and better, and the role for KYC utilities, https://www.sc.com/fightingfinancialcrime/av/kyc-utilities-thought-piece.pdf.

transactions, that are closely associated with banks' obligations to identify and mitigate ML/TF risks. The *modus operandi* would be dictated by code deployed on a blockchain, and merged with AI, which would enhance the governance and monitoring activities. These activities would be determined by a blockchain protocol and smart contract code, and executed on an autonomous system, which would then support the retrieving or recording of information, making banks' filing of STRs more reliable as regards the flagging of signals. If implemented, this reporting tool would not only enhance AML/CFT compliance, but also mark a fundamental change from a bureaucratic paper-based system to a technologically driven code-based system, which could empower regulatory monitoring and governance, given that the blockchain data system would record an auditable trail of activities performed from or tied to a particular account or smart contract (Filippi and Wright, 2018: 197).[67] Applying technology-driven solutions would also imply that banks are less likely to use AML/CFT compliance as a reason or excuse to deny financial customers access to the banking system, as mirrored in de-risking.

In theory, the risk-based approach should be applied for the purposes of client on-boarding and financial transaction monitoring; but in effect, banks cannot identify, assess or mitigate ML/TF risks without good intelligence. In this regard, the HKMA has worked with Deloitte to share insights into technology-based investigations in the context of AML/CFT RegTech adoption by affirming some banks' use of network analytics and non-traditional data elements, which are, according to the HKMA, 'more useful for intelligence-led investigations rather than for passive monitoring' (HKMA, 2021).[68] To this end, network analytics are deemed as 'a valuable tool for inquiry, rather than [merely] a tool to generate [suspicious transaction] alerts' (HKMA, 2021).[69] In maximising the utility of AML/CFT analytic techniques, network analytics manifest a sector-level initiative through intelligence-sharing partnerships, utilising a team effort that involves banks and other stakeholders from across the AML/CFT ecosystem (HKMA, 2021: 9).[70] To attain financial inclusion – in light of the HKMA's circular of 8 September 2016 against the practice of de-risking (HKMA, 2016)[71] – the deployment of

[67] Filippi PD and Wright A (2018) *Blockchain and the Law—the Rule of Code*. Cambridge, Massachusetts: Harvard University Press at 197.
[68] HKMA (January 2021), AML/CFT RegTech: case studies and insights, https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2021/20210121e1a1.pdf, at 15.
[69] *Ibid*.
[70] *Ibid*. at [9].
[71] HKMA, De-risking and financial inclusion, *supra* note 20.

DLT (i.e. blockchain technology), an initiative that aims to assist financial institutions such as banks in meeting AML/CFT regulatory requirements during the KYC-CDD procedure, is on the rise. Although blockchain is at the peak of the hype-cycle now, there is significant application in law for the DLT that blockchain presents. While the DLT ushered in a period of change, the promises and perils of blockchain also symbolise the opportunities and challenges it offers for financial law and regulation. Developers of DLT have advocated for blockchain's usefulness in verifying bank account opening information in a more scientific and systematic way, as well as in meeting the financial institutions' continuous monitoring responsibility (Shamdasani, 2017: 138).[72] The HKMA circular further dissuaded banks from applying disproportionate AML/CFT measures (Vagen, 2016: 115).[73] In practice, however, unless individuals or business entities applying for bank account opening can prove the legality of their income or source of wealth, in order not to pose any ML-TF risks, banks are entitled to choose to protect themselves by rejecting outright any applications that might lead to AML non-compliance fines.

Technically speaking, blockchain technology builds on existing internet-based computing networks as it provides a new, decentralised and disintermediated platform for financial and commercial transactions, making it a linchpin of the 'Internet of Things'. The term Internet of Things (IoT) denotes information and communication technologies, although what the IoT encompasses, in terms of its actual scope of coverage, is unclear. According to the International Telecommunication Union, IoT is 'a global infrastructure for the Information Society', under which advanced services are enabled by interconnecting either physical or virtual things based on information and communications technologies that are existing and evolving and interoperable (Wortmann and Flüchter, 2015: 221-224).[74] Accordingly, IoT concerns a system of interrelated devices connected to the internet, where data could be gathered for intended purposes by design. For example, Beacons, which are wireless sensors that can be connected to the internet to gather local data, have been used to enable bank staff to

[72] Shamdasani A, *supra* note 23.

[73] Vagen T (2016) Only a nuanced AML approach will keep Hong Kong 'open for business', says law firm. *Hong Kong Lawyer* at 115.

[74] Wortmann F and Flüchter K (2015) Internet of things technology and value added. *Business & Information Systems Engineering 57*(3): 221-224. In this article, the authors further referred to the International Telecommunication Union's standards that help define the internet of things. *See* International Telecommunication Union (2012), New ITU standards define the internet of things and provide the blueprints for its development, http://www.itu.int/ ITU-T/newslog/New?ITU?Standards?Define?The?Internet? Of?Things?And?Provide?The?Blueprints?For?Its?Develo pment.aspx.

personally greet and help customers as they walk in (Crosman, 2015).[75] Beacons also allow banks to collect information about customers. A bank's app can then autofill customers' data into a banking form for a mortgage application, to give an example.[76] With digital banking currently on the rise, the IoT could be part of the global technology system leveraged for data analytics owing to its data gathering ability. For the purpose of this article, since data analytics can be designed to attain regulatory functionality, such as in flagging suspicious transactions in compliance with AML/CFT regulatory requirements, the IoT has a role to play in bank technology driven by FinTech or RegTech aspirations. Taking as an example international money transfers, a financial transaction service often required by SMEs, since DLT allows direct interaction between the sender of the payment and the beneficiary banks, this may impact financial institutions in two ways: eliminating the role of correspondents and reducing information arbitrage. For financial institutions, even though the latter impact is affirmative, as the integrity of the financial system will be strengthened, the former impact is disquieting because of its potential to weaken their dominance in the global payment system. On the other hand, for a sender of a payment (an SME, for instance), conducting international money transfers through DLT could provide real-time settlement, thereby increasing profitability by reducing liquidity and operational costs.[77] Information arbitrage has a bearing on KYC-CDD in correspondent relationships. Banks—being correspondent banks to other non-local banks to facilitate cross-border payments—are required to know their customers as well as their customers' customers (Lee, 2017).[78] Information arbitrage is a concern that could further develop into a trap for financial institutions, which could lose sight of a deliberate and inadvertent facilitation of the movement of illicit proceeds from criminal activities which have been passed through a non-local correspondent bank. Coordination between correspondent banks is therefore paramount in the working of a financial payment system. So is collaboration between national and international regulatory authorities. Coordination and collaboration could also contribute to the expansion of financial system access to legitimate businesses which depend on banks' provision of cross-border payment services. According to the FATF, 'A co-ordinated approach among international organisations, technical assistance providers, policy makers, standard setters,

[75] Crosman P (19 November 2015) Why the internet of things should be a bank thing. *American Banker.* https://www.americanbanker.com/news/why-the-internet-of-things-should-be-a-bank-thing.
[76] *Ibid*.
[77] World Economic Forum (2016), The future of financial infrastructure-an ambitious look at how blockchain can reshape financial services, http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf at 39.
[78] Lee E., *supra* note 14, at 476.

supervisors and private sector can help generate necessary will to address de-risking in a meaningful manner' (FATF, 2018).[79]

To help smooth the banking industry's payment system by reducing the gap in payments, a recent FinTech development—which would verify in real time that a payment is going into a valid account, instead of being rejected days later because of transaction errors—is being tested by at least 76 of the world's biggest banks which have joined the Interbank Information Network (IIN) (Noonan, 2019).[80] The IIN, which operates on the industry's leading blockchain technology, would be more useful for international payments, although it, too, can assist in domestic payments. According to the *Financial Times*, the IIN will impact the AML/CFT compliance on a global scale because of banks' leading role in cross-border payments. As a matter of fact, banks already replicate a lot of the same infrastructure to secure messaging, document file transfer and data modelling.[81] The example of IIN shows that blockchain technology can be designed and has indeed been deployed to facilitate both AML/CFT compliance and payment transactions, signalling a positive impact on financial inclusion. As Hong Kong embraces smart banking, a FinTech-based solution warrants some consideration and, if implemented, should be proportionate to its functional design and the cost borne by the banks that intend to adopt it.

2. The Relationship between Blockchain and Smart Contracts

Blockchain is the underlying technology for smart contracts. Stated differently, smart contracts are deployed on blockchain technology. Blockchain-based smart contracts allow parties to enter into binding commercial relationships using computer codes generated by software, as opposed to using the natural language of traditional contracts, to manage contractual performances. Since smart contracts are written in software codes, they can be duplicated for a more standardised use of smart contract-based provisions, or licensed to assist in public scrutiny, feedback and monitoring. Smart contract code can also be specifically designed to implement certain functionalities that routinely appear in legal contracts (Filippi and Wright, 2018).[82] Libraries of smart contract code, for example, could be written to govern the transfer of payments over a

[79] FATF (November 2018), FATF report to the G20 leaders' summit, http://www.fatf-gafi.org/media/fatf/documents/reports/Report-G20-Leaders-Summit-Nov-2018.pdf, para 35.
[80] Noonan L (21 April 2019) JPMorgan to widen use of blockchain system. *Financial Times*, https://www.ft.com/content/87ae3010-61ec-11e9-b285-3acd5d43599e?shareType=nongift.
[81] *Ibid*.
[82] Filippi PD and Wright A, *supra* note 67, Part 2, 4. 'Smart contracts as legal contracts'.

specified amount, as well as the velocity of money, as both are capable of triggering alerts for ML/TF risks.

Smart contracts also allow parties to enter into business relationships for services without trust in or knowledge of the true name or legal identity of the other party. There are limitations to smart contracts, however, not least because of concerns of privacy risk, data breach, technology immaturity and rigid, code-based contract formalisation. Such issues make smart contracts unsuitable for agreements that have strict confidentiality requirements, or that contain arrangements with vague and open-ended provisions. Smart contracts are therefore not likely to replace traditional legal contracts. Currently, smart contracts normally form part of a more complex legal contract written in natural languages. The courts, therefore, still retain jurisdiction over the legal effects of a smart contract and will continue to do so.[83]

Notwithstanding smart contracts' inherent limitations, their ability to enable autonomous agreement execution could potentially reduce reliance on human decision-making, as the process does not allow for biases or opportunity for discrimination. In this light, smart contracts could potentially aid in financial inclusion by removing banks' human inclination to 'de-risk' by categorically denying certain customer groups access to banking.

3. The Pros and Cons of Blockchain

Blockchain is bundles of electronical data grouped into blocks that are linked together to form a sequential, timestamped chain of information which, in the context to which this article refers, pertains to personal identification or financial transaction records, or both. In practice, blockchain entails the use of both a public and a private key to enable users to send encrypted messages, make payments or store customer information. The public key serves as a reference point for communication, whereas the private key acts as a secret password for parties using blockchain's cryptographic systems to send encrypted messages (to which a digital signature may be attached for increased authentication) and to conduct transactions via a range of mechanisms inclusive of smart contracts, which are also underpinned by blockchain technology.[84] Public-private key cryptography thus enables parties to conduct transactions conducive to both transparency and confidentiality. As a matter of technological design, a blockchain record is immutable and pseudonymous. In practice, this implies that

[83] *Ibid*.
[84] *Ibid*.

blockchain technology has the potential both to strengthen and weaken the existing legal framework for AML/CFT purposes. From a risk-reward point of view, blockchain can be deployed for either constructive or destructive ends (Kaza, 2018: 53-54).[85]

On the positive side, blockchain yields transparency. The reader should note that there are two types of blockchain: private and public. Whereas private blockchain requires permission to allow access to private parties, public blockchain does not require special permission, as the information recorded on the blocks is open to the public—an underlying characteristic that makes blockchain more adaptable for the prevention of fraud or money laundering. Simply put, given the non-repudiable and tamper-resistant nature of blockchain, there is, in theory and likely also in practice, only a remote possibility of overriding an existing control of the underlying blockchain network by a network participant. Not only is an attempt highly unlikely, it would also be cost prohibitive. Success would require destroying literally every copy of previously recorded data possessed by other network participants, an exceptionally difficult feat, even for powerful computers. Since participants are all connected by peer-to-peer networks supported by a decentralised infrastructure that gives each participant in the networks (a 'node') access to informational resources, any participant who wants to recreate blockchain data that have been destroyed can easily and quickly do so because the data, written in code, are highly replicable.

On the negative side, and perhaps of more concern to legislators and regulators, blockchain's intrinsic disintermediation function prevents central control by powerful intermediaries such as banks, which have traditionally dominated the financial system and which are accountable to regulators. Blockchains are further characterised by their pseudonymity, which brings further complexity to the issue, as users of blockchain-based remittance services (nodes) can use fake names. Pseudonymity therefore creates a governance concern as it 'may embolden parties' to commit crimes in heavily regulated areas such as money laundering (Kaza, 2018: 53).[86] Regulators need to take blockchain into their regulatory mapping which is integral to compliance functions. Although blockchain is associated with bitcoin, blockchain is bigger than bitcoin or other virtual currencies which use blockchain for their underlying architecture. Even if bitcoin (launched in 2009) were to fail tomorrow, blockchain technology would continue in business because it is already in use for hundreds of applications, not just as a currency but also as a vehicle for financial transactions and the storage of governmental information, because of its built-in design for record-keeping and authenticity

[85] Kaza G (fall 2018), The blockchain revolution. *Regulation* 41(3): 53-54.
[86] *Ibid*. at [53].

verification (Norman, 2017).[87] Putting aside temporarily the legal challenges blockchain presents in terms of governance, the technology has imbued the financial system with enough confidence to support transparent, resilient, tamper-resistant registries, which could disincentivise parties to act opportunistically (Filippi and Wright, 2018).[88]

FinTech blockchain provides a new infrastructure to create decentralised organisations whose governance leans on computer code-based rules and other means of algorithmic governance rather than human management. The governance of blockchain is informed by the consensus of all participants on the peer-to-peer network and the blockchain-based protocols, as opposed to a centrally controlled financial intermediary or governance agency (that implements regulatory constraints). With this self-governance structure, blockchain can be steered to complement or circumvent the law. Blockchain and blockchain-based smart contracts are indeed capable of complementing or circumventing the existing law, depending on the designer's desired outcome (Filippi and Wright, 2018: 52).[89] If blockchain technology were to dominate the social and financial systems, nuanced assessments would be necessary to examine and test the adaptability of the existing law, or otherwise, enact alternative regulations to address the risks associated with blockchain deployment more effectively. The author warns that blockchain may evade regulatory intrusion by circumventing disciplinary governance, which has traditionally taken a top-down approach within a highly centralised, hierarchical structure and therefore will not easily translate to the new decentralised, disintermediated and autonomous systems deployed on a blockchain.

4. Blockchain's Impact on RegTech

According to a sample study of FinTech patent applications from 2003 to 2017 in the United States, the banking industry and the payments industry are the first and second-most active industries, respectively, to use and invest in blockchain technology (Chen et al., 2019: 2075).[90] This study clearly indicates that FinTech innovation is strongly linked to payments, mobile transactions and the payment system, of which banks and payment companies play an integral part. In this respect, smart contracts can be applied

[87] Norman AT (2017) *Blockchain Technology Explained: The Ultimate Beginner's Guide about Blockchain Wallet, Mining, Bitcoin, Ethereum, Litecoin, Zcash, Monero, Ripple, Dash, IOTA and Smart Contracts*' (Kindle version).
[88] Filippi PD and Wright A, *supra* note 67, Part 1.
[89] *Ibid*. at [52].
[90] Chen MA, Wu Q and Yang B (2019) How valuable is FinTech innovation. *Review of Financial Studies* 32(5): 2075.

and designed to improve the efficiency of the payment system, which will directly impact financial inclusion. Technically, payments under smart contracts would require coordination of blockchains because payments would be triggered by tamper-proof consensus on contingent outcomes and financing (Cong and He, 2019: 1754).[91] Despite the potential benefits of smart contracts in automating payments, the concerning possibility of greater collusive behaviour has been raised in view of blockchain's decentralised consensus. While decentralised consensus is designed for mitigating information asymmetry and encouraging contracting efficiency, it may result in payments by smart contracts escaping the regulator's oversight and thus may not benefit financial consumers in the end (Goldstein et al., 2019: 1655).[92] However, for the sake of argument, setting regulatory concerns aside, blockchain-based smart contracts are still, in theory, capable of being used to eliminate biased human decision-making, which could help in attaining financial inclusion.

The author envisions that blockchain-based smart contracts can be used for AML/CFT regulatory compliance purposes. The implementable laws and regulations pertaining to smart contracts, however, are nuanced and complex as the latter are products of interdisciplinary labour; lawyers, computer engineers as well as regulators must work together to effectuate smart contracts. RegTech development in this regard may reduce the regulators' burden: their job will consist of preparing and asking a list of questions pertinent to the AML/CFT regulations and monitoring, and the results will be outcome-based. However, if the situational problem lies with the smart contract itself, a key objective will be to discern how to ensure the code matches the parties' commercial intent (since the smart contract is written in computer codes). To that end, computation of any algorithm model will require model testing and simulations, likely to be carried out on a private server, before it gains public recognition.

Under the current AML/CFT system, the duty to report suspicious transactions to the authority, which gives rise to the duty to delay or prevent such transactions in accordance with the instructions of the regulator, is placed on the financial intermediaries, such as the banks, which are traditionally regarded as the gatekeepers to the existing financial system. A more radical change would be to shift the monitoring function directly to the regulator, if only for reasons of efficiency. Doing so would, in

[91] Cong LW and He Z (2019) Blockchain disruption and smart contracts. *Review of Financial Studies* 32(5): 1754.
[92] Goldstein I, Jiang W and Karolyi GA (2019) To FinTech and Beyond. *Review of Financial Studies* 32(5): 1655.

theory, maintain the attractiveness of the distributed ledger system, which enables self-verification and self-execution of smart contracts in a decentralised system that excludes or minimises the role of financial intermediaries in the payment system (Sathyanarayan et al., 2018: 180).[93] Requiring the incorporation of the AML/CFT legal requirements into the distributed ledger, however, would add 'legal impurities' (to the ledger), as these two are incompatible. The reason for this is that cryptographers and other technologists behind these DLT decentralised systems would not have expected or wanted to incorporate legal requirements into the tool they helped to design, known as DLT. Not only are legal requirements beyond technologists' scope, they may very well be incompatible with DLT's design. Instead, technologists would focus on things such as data mining and ensuring that hash functions match. The purpose may be for a miner to find a nonce that will produce a matching hash value pattern. It would follow that legal impurities are likely to create obstacles to the efficiency of DLT. Although technology such as DLT may force changes and adaptations in law in order to safeguard legal integrity and value, the process of incorporating legal requirements into computer coding will not be free of friction because law and code are not necessarily compatible due to a lack of interoperability. Even so, the benefit of DLT, a technology that promises new means of transferring data and value, cannot be materialised unless such transfers are recognised by law (Finck, 2019: 85),[94] including the AML/CFT regulations. Put another way, technology 'simply cannot refuse to account for external legal requirements and systems' (Finck, 2019: 85).[95] The success of DLT is therefore contingent on recognition by the AML/CFT governance framework. From a RegTech point of view, DLT may well be regarded as a tool which needs to give way to desirable regulatory aims. That is to say that, while the incorporation of legal impurities (e.g. AML/CFT requirements) into the technical workings of the distributed ledger system is undesirable from a technological perspective, the law's mismatch with technology (DLT) does provide reasons to justify allowing the regulator to gain control over a payment system that is prone to threats of money laundering, especially given the vulnerabilities of cross-border transactions. Of course, complex issues of trust that would allow national regulators to coordinate investigations and combat financial

[93] Reed C, Sathyanarayan UM, Ruan S and Collins J (2018) Beyond bitcoin-legal impurities and off-chain assets. *International Journal of Law and Information Technology* 26: 180.
[94] Finck M (2019) *Blockchain Regulation and Governance in Europe*. Cambridge: Cambridge University Press at 85.
[95] *Ibid*.

crimes do arise (Sathyanarayan et al., 2018: 179, 182).[96] Although the law is imprecise and context-dependent, making it difficult to build into technological systems that aim at exactitude, the value of DLT, a FinTech tool now widely accessible to both the regulator and the public, including those subject to the AML/CFT regulation, may be built on the RegTech need to preserve the order of its payment system and safeguard the integrity of the financial market.

The rapid evolution of FinTech spawns a similar revolution of RegTech, as the latter's development is driven by industry participants, including financial institutions that aim to leverage FinTech growth to reduce their compliance costs (Arner et al., 2017: 2, 14).[97] As the financial industry is capitalising on technology that could offer solutions to compliance reporting, a process necessary for showing the regulatory authorities that all the legal requirements and regulatory standards are being satisfied and adhered to, the next stage of RegTech is likely to be driven by regulators who are responsive to the industry's keen interest in developing a compliance-by-design framework. 'Compliance by design' entails the application of 'a systematic approach to integrating regulatory requirements into manual and automated tasks and processes' (Gehra et al., 2017: 4). [98] Through this approach, a regulatory standard such as the KYC standard can be built into a bank's AML/CFT control process to ensure globally harmonised and locally calibrated compliance activities (Gehra et al., 2017: 4).[99] To this end, it is not difficult to appreciate that RegTech can be taken to include the use of technology by regulated entities to comply with their regulatory and compliance, or by regulators for supervisory oversight operations such as market surveillance and risk identification and monitoring. To differentiate between these two, RegTech that is used and applied by regulators, also referred by the OECD as 'oversight bodies', is known as 'SupTech'.[100] Although FinTech and RegTech shared a similar path of evolution in terms of technological development and application, the former focuses on finance

[96] Reed C, Sathyanarayan UM, Ruan S and Collins J (2018), *supra* note 93, at [179], [182].
[97] Arner DW, Barberis J and Buckley RP (2017) FinTech and RegTech in a nutshell, and the future in a sandbox. CFA Institute Research Foundation Briefs, at 2, 14.
[98] Gehra B, Leiendecker J and Lienke G (2017) Compliance by design: banking's unmissable opportunity. The Boston Consultation Group White Paper, https://image-src.bcg.com/Images/Compliance-by-Design-Dec2017_tcm9-198779.pdf, at 4.
[99] *Ibid*.
[100] Organization for Economic Co-operation and Development (OECD) (2018), G20/OECD policy guidance financial consumer protection approaches in the digital age, https://www.oecd.org/finance/G20-OECD-Policy-Guidance-Financial-Consumer-Protection-Digital-Age-2018.pdf, at 16.

while the latter focuses on regulatory monitoring, compliance and reporting. Therefore, it has been suggested that RegTech should not be treated as a subset of FinTech. Even so, they share some common ground in the use of technology, particularly information technology, for transforming information into digital data that include personal and commercial data. Indeed, the use and application of RegTech has brought about new compliance tools made possible through artificial intelligence (AI), deep learning, machine learning and natural language processing, data reporting, regulatory codification and big data analysis technologies, all of which are good examples of technologies which have the potential to enhance or improve consumer data protection, market supervision and prudential regulation.[101]

RegTech, which is distinguishable from FinTech, will be developed to enable a 'compliance by design' framework. As a regulator, the HKMA will have to rely on a robust RegTech model in which there is an algorithm for producing the risk profiling result. Risk profiling can be viewed as an approach taken by the regulator that is efficacy-oriented (Londras and Davis, 2010: 19-47).[102] The HKMA must efficiently allocate its supervisory resources by focusing on banks with relatively high risks resulting, for example, from their customer base or their products or services. In effect, the intensity of supervision rests on an individual bank's risk profile: the higher its risk profiling result is perceived by the regulator, and the more the likelihood it will adversely affect the financial market, the higher the impact it will have. Consequently, the regulator must allocate its supervisory resources by focusing more on banks with high(er) risk profiling and hence with high(er) impact. Understandably, there would be very little marginal gain if the regulator were to allocate its resources to banks with a low risk profile. This is an especially important issue for Hong Kong as the HKMA is constrained by human resources available for AML regulatory enforcement and monitoring. According to a public lecture given at the University of Hong Kong in April 2017 by Ms Meena Datwani, Executive Director of the Enforcement and AML Department of the HKMA, this department has only 35 staff responsible for supervising approximately 200 financial institutions in Hong Kong.[103] For that very reason, Ms

[101] *Ibid*. at [16]. *See also* Arner DW, Barberis J and Buckley RP, FinTech and RegTech in a nutshell, and the future in a sandbox, *supra* note 97, at 14.
[102] Londras Fd and Davis FF (2010), Controlling the executive in times of terrorism: competing perspectives on effective oversight mechanisms. *Oxford Journal of Legal Studies* 30(1): 19-47.
[103] Meena Datwani, The risk-based approach – a regulator's perspective, a public lecture given on 19 April 2017 at the Faculty of Law of the University of Hong Kong.

MANUSCRIPT
(FOR PUBLISHED VERSION, PLEASE REFER TO: 'Technology-Driven Solutions to Banks' De-risking Practices in Hong Kong: FinTech and Blockchain-based Smart Contracts for Financial Inclusion', *Common Law World Review*, Vol. 51(1-2), pp. 83-108 (May 2022, published online)

The permanent link for this article is https://doi.org/10.1177/14737795211071095

Datwani confirmed that the HKMA has looked into the FinTech matrix.[104] It is therefore reasonable to expect that the HKMA may in the future promote the automated compliance by design framework. If this is the case, the financial institutions' regulatory compliance duty will be brought well in line with the latest RegTech innovation.

Conclusion

As a member of the FATF since 1991, Hong Kong published its Money Laundering and Terrorist Financing Risk Assessment Report on 30 April 2018.[105] This report has further incentivised the Hong Kong government to align local practice with the international command on combating ML/TF risks. The HKMA further encourages banks to apply FinTech solutions in their regulatory compliance towards, say, the jurisdiction's AML/CFT law, with the policy goal of increasing financial inclusion. In effect, whether and how FinTech innovation may be deployed to augment the internal risk-monitoring model and AML/CFT compliance policies is a question that concerns not only the regulator but also the regulatee. Since regulators cannot force banks to accept bank account opening applications, banks will have to use their discretion to decide whether to on-board clients with less than stellar credit history or worthiness, depending on the banks' intelligence teams' experience. In these circumstances, the presence of risk factors associated with financial crime does not necessarily mean that potential business would be turned away, because the totality of circumstances (e.g. business models and clientele, project profit and loss, directorship, alternative funding source, expected bank account activities) needs to be considered (Shamdasani, 2017: 138).[106]

While blockchain can be utilised as the underlying technology for the purposes of enhancing AML compliance, there will likely be a high cost to be borne by financial institutions. According to a report in the *Financial Times*, Citigroup invests US$8 billion a year in technology (Noonan, 2019).[107] According to the same report, however, expectations for the DLT have been falling sharply, despite the fact that blockchain was once seen as a panacea for all that ails the financial services industry. The report cites Citigroup boss Mike Corbat as saying he believes that '… blockchain will not be

[104] *Ibid*.
[105] The Government of the Hong Kong Special Administrative Region (30 April 2018), Publication of Hong Kong's money laundering and terrorist financing risk assessment report, press release, https://www.info.gov.hk/gia/general/201804/30/P2018043000851.htm.
[106] Shamdasani A, *supra* note 23.
[107] Noonan L (20 February 2019), Banks' blockchain comedown. *Financial Times*, https://www.ft.com/content/122de77c-3483-11e9-bd3a-8b2a211d90d5?shareType=nongift.

'transformational' in the short term'. Corbat further explains that '… in many of these things, the expectations and the pace of implementation far exceed... what's there' (Noonan, 2019).[108] Apparently, one main reason for falling expectations is that DLT development is still in its infancy. In the light of this industry awareness, a balanced approach underpinning an economically robust cost-benefit analysis is crucial for accommodating blockchain technology into future AML legislative frameworks in Hong Kong or elsewhere. It is no surprise that most banks in Hong Kong adopt a 'wait and see' mentality in exploring FinTech's potential application and are therefore not keen to address the downsides of DLT, given that it is a technology that has not yet been widely used. It is arguable that the HKMA's FinTech policy cannot be complete without a thorough cost-benefit analysis. Individuals, start-ups and SMEs are cases in point, and banks make little or no money in providing services to them. In addition, potentially higher costs are involved in the initial stages of building a financial infrastructure that meets KYC-CDD requirements.

FinTech is said to be an enabler, but so far whether, or to what extent, blockchain technology can enhance banks' ability to expand financial inclusion seems rather uncertain. Success in achieving that aim will rely heavily on data accuracy, which is not always within the control of banks, since their clients may lie or fail to cooperate on a consistent basis. With a financial system that no longer positions banks in the centre but moves instead towards a consumer-based system that values financial democracy and inclusion, the author suggests that financial inclusion be incorporated into part of the AML/CFT laws and regulations in Hong Kong. In Europe, access to basic financial services has been recognised as a basic civil right, without which individuals or firms will face social or economic marginalisation.[109] It is thus not merely a value that can be added on to a public policy, which is in and of itself a driving force, though without the necessary power for legal enforcement.

[108] *Ibid*.

[109] European Accessibility Act, Improving the Accessibility of Products and Services in the Single Market, European Commission Employment, Social Affairs & Inclusion, ec.europa.eu/social/BlobServlet?docId=14795&langId=en.