
Centre for Banking & Finance Law
Faculty of Law

# Working Paper

**A Facilitative Model For Crypto-Currency Regulation In Singapore**

**Jonathan LIM**

Adjunct Researcher, Centre for Banking & Finance Law, Faculty of Law, National University of Singapore

jlimwz@gmail.com

18 October 2014

http://law.nus.edu.sg/cbfl/

**Centre for Banking & Finance Law**
Faculty of Law
National University of Singapore
Eu Tong Sen Building
469G Bukit Timah Road
Singapore 259776
Tel: (65) 66013878
Fax: (65) 6779 0979
Email: cbfl@nus.edu.sg

The Centre for Banking & Finance Law (CBFL) at the Faculty of Law, National University of Singapore focuses broadly on legal and regulatory issues relating to banking and financial services. It aims to produce research and host events of scholarly value to academics as well as of policy relevance to the banking and financial services community. In particular, CBFL seeks to engage local and international banks, lawyers, regulators and academics in a regular exchange of ideas and knowledge so as to contribute towards the development of law and regulation in this area, as well as to promote a robust and stable financial sector in Singapore, the region and globally.

# A Facilitative Model For Crypto-Currency Regulation In Singapore

**Jonathan LIM**

Adjunct Researcher, Centre for Banking & Finance Law, Faculty of Law, National University of Singapore

jlimwz@gmail.com

**ABSTRACT:**

Crypto-currencies have received much attention from regulators of late. While many consider regulation necessary because of their potential for illicit use, heavy-handed regulation would over-burden the development of a nascent industry that has captured the imagination of many. This chapter reflects on a number of key issues that arise from crypto-currency regulation in the Singapore context, and proposes a "facilitative" model for optimal regulation in Singapore. A premise of this model is that regulation need not be anti-industry; and facilitative regulation can help to reduce both investor and end-user uncertainty, while promoting widespread acceptance and legitimacy.

## 1. INTRODUCTION

Crypto-currencies such as Bitcoin have received much attention of late. They are, at bottom, simply computer protocols; and like other computer protocols such as TCP/IP and HTML – which birthed the Internet and its myriad modern uses – crypto-currencies are said to have the potential for similar global impact, including by revolutionising the existing e-payments and e-commerce sectors through a process of "disruptive innovation".[1]

Unsurprisingly, these developments have not gone unnoticed by regulators. Lawmakers and regulatory agencies around the world are considering introducing, and indeed some have already introduced, some form of regulation for crypto-currencies. This momentum for regulation has also been motivated, in part, by recent high-profile events such as the failure of the Mt. Gox Bitcoin exchange based in Tokyo, Japan, and the public prosecutions in the US and Australia for Bitcoin-related transactions in illicit goods on the Silk Road marketplace.

Regulatory responses and proposals have, of course, not been uniform but have instead differed greatly across the board. Some jurisdictions, such as Vietnam and Iceland, have instituted some form of ban on the use of digital currencies. Other jurisdictions, such as Germany and the United States, have introduced limited forms of regulation intended to address targeted regulatory interests such as anti-money laundering and counter-terrorist financing. Still more jurisdictions are taking a wait-and-see approach, with regulators keeping silent on the issue of regulation. As yet, no consensus has emerged on an optimal or ideal approach to regulating this new technology.

This chapter reflects on a number of key issues that arise from crypto-currency regulation – and attempts to articulate what the optimal features of such regulation might look like. It situates this discussion in the Singapore context, which provides a useful case study for several reasons. Singapore is an international financial and wealth management centre, with significant flows of funds passing through its shores; at the same time, it is also a rapidly growing regional hub for technology start-ups and innovation. In addition, Singapore has always shown a

[1] Disruptive innovation is a term coined by management professor Clayton Christensen of the Harvard Business School, and describes a process by which an innovation transforms an existing market or sector, initially taking root in simple applications at the bottom of a market, and then relentlessly moves upward and completely redefining the industry as it creates entirely new markets with different value networks. *See* Christensen, C. (1997). *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Cambridge, MA, USA.

willingness to modify its laws or regulations to obtain a pragmatic or economic advantage, and is well known for its market-leading regulatory practices and laws in relation to commercial matters – particularly matters with a strong transnational and competitive dimension, such as foreign investment, finance, or international commercial arbitration.[2] Recent announcements by regulators from the Monetary Authority of Singapore ("MAS") suggest that a similar approach will be followed with regard to crypto-currency regulation.

In these circumstances, this chapter articulates and develops a "facilitative" model for crypto-currency regulation in Singapore. This approach recognises that, while some form of regulation of crypto-currencies is desirable and even necessary, there is a real risk that blunt, heavy-handed regulation would impede the development of a nascent and productive crypto-currency industry and ecosystem.

Indeed, regulation need not be anti-industry; crypto-currency regulation can, if well-calibrated, reduce business and end-user uncertainty, encourage and incentivise innovation, and enhance the legitimacy of crypto-currencies for use in a variety of real-world applications. This is consistent with the view espoused by Mr. Ravi Menon, Managing Director of the Monetary Authority of Singapore ("MAS") at a recent interview, where he opined that, in Singapore, "digital currencies have a role to play, which is why [the MAS has] not sought to ban them, or make it more difficult for them to operate… while there is reason to be cautious about the risks, we have chosen to address these risks in a targeted way so that innovation can continue to take place".[3]

Facilitative crypto-currency regulation should therefore, by design, ensure appropriate space for innovation and legitimate competition, while clamping down on and dis-incentivizing misconduct and harmful behaviour. This would support Singapore in becoming a global leader in the development and marketization of crypto-currency technology, especially if it gains widespread mass-market adoption. Ensuring this balance will of course be difficult in practice,

[2] *See e.g.* The World Bank, *Doing Business 2014: Understanding Regulations for Small and Medium-size Enterprises*, available at http://www.doingbusiness.org/reports/global-reports/doing-business-2014*;* Queen Mary University of London and White & Case LLP, *2010 International Arbitration Survey: Choices in International Arbitration*, at pp. 17-18.
[3] Christopher Jeffrey, *MAS' Ravi Menon on Fed policy, China and global regulation*, Centralbanking.com, dated 10 August 2014.

and the devil will likely lie in the details; the purpose of the facilitative model outlined below is to suggest a useful blueprint or starting point for discussion.

Three aspects of this model or framework will be discussed in the sections below:

a. ***First***, clear and targeted regulations, backed by the force of law, are needed to tackle core regulatory concerns raised by such new technology, such as fraud and anti-money laundering.

b. ***Second***, a self-regulatory framework involving effective partnership between industry and regulators must form an integral part of the regulatory architecture for crypto-currencies.

c. ***Third***, and finally, effective crypto-currency regulation will require coordination and harmonisation with other regulators and jurisdictions, given the de-centralized and often transnational character of crypto-currency transactions and protocols.

## I. BACKGROUND TO CRYPTO-CURRENCIES

Crypto-currencies are a sub-set of virtual currencies. Virtual currency may be defined as a "digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status… in any jurisdiction".[4] In other words, virtual currencies are digital objects that hold economic value and are functionally similar to fiat currencies that are issued by governments, but which are not issued as such but are instead created pursuant to, and governed by, private agreement among a community or users and other network participants.

Crypto-currencies are decentralised (i.e., issued without a central administering authority) and cryptography-based virtual currencies that are distributed, open source, and function on a peer-to-peer basis.[5] Crypto-currencies are also by definition *convertible* virtual currencies, meaning that they have an equivalent value in real fiat currency, and can be exchanged for such fiat

[4] Financial Action Task Force Report, *Virtual Currencies – Key Definitions and Potential AML/CFT Risks*, June 2014 Report, ("2014 FATF Report") at p. 4.
[5] 2014 FATF Report, at p. 5.

currency. In contrast, non-convertible virtual currencies, such as World of Worldcraft gold or airline miles, are specific to a particular domain or virtual world under particular rules governing their use, and cannot be exchanged for fiat currency.

The combination of these features allows crypto-currencies to function both as currency and as a peer-to-peer payments platform. Understanding these features is crucial to the design of facilitative regulation that accords appropriate space for innovative potential of crypto-currencies and their many commercial applications.

### *A. Bitcoin*

Bitcoin is in many ways *the* archetype crypto-currency. It was the first of its kind when it was introduced in 2009, and the technology has spawned many imitators since. Bitcoin is also today the most widely adopted crypto-currency, with the most obvious potential for commercial and business application to real-world goods and services. Much has been written about Bitcoin, and it provides a useful case study for understanding what crypto-currencies are and how they work.

Unlike traditional currencies, Bitcoins are not issued or backed by any government or central bank, and their value does not derive from precious metals or other similarly tangible proxies of value. Instead, like all crypto-currencies, Bitcoins are essentially digital units of account that are composed of unique strings of characters, and that can be traded electronically via a cryptography system that verifies and records transactions. They are intangible, exist only digitally, and have no intrinsic value.

Instead of a central administrator, the Bitcoin system is run by a decentralised network consisting of over twenty thousand independent computers (or nodes) around the world running Bitcoin software and operating the protocol for administering Bitcoin transactions. Bitcoins are issued to nodes in the network that succeed at being the first to solve a difficult mathematical problem that requires a tedious amount of computation. Not unlike precious metals, the supply of Bitcoin increases at a predetermined rate that gets progressively slower over time, with total supply capped at 21 million Bitcoins.

The de-centralized network validates and verifies transactions using a math-based proof-of-work scheme. Whenever a new block of transactions is created, it is added to the "block chain" where it will be verified by competing nodes in the network through a process that involves solving a mathematical problem that is difficult to solve, but easy to verify. The first node in the network that succeeds in solving the problem receives a reward in Bitcoins and broadcasts the solution throughout the network; this solution is then quickly verified by a majority of other nodes in the network.

The use of a proof-of work concept to generate and administer digital money has been rightly recognized as a technological breakthrough. Because of the competition for mining Bitcoins, and the scarcity of computational resources, proof-of-work ensures that decentralized, independent agents collaborate to maintain the integrity of the system, and builds in incentives for honest users within the network to protect the system from attack by potentially malicious participants.[6] There is thus no need for a central administrator or issuer in such a system. Crypto-currencies other than Bitcoin (also referred to as Altcoins) use different distributed proof systems, including proof-of-stake algorithms which require validation of transactions not through mathematical computations, but through proof of ownership.

As a payments platform, the Bitcoin protocol is capable of transferring value between users on a peer-to-peer basis, thus requiring no middleman between sender and receiver, or between buyer and seller. Transfers can be done almost instantaneously; and either for free, or for a low transaction fee in exchange for additional functionality. Transactions are secured by a dual key system. All users have a Bitcoin address that has both a cryptographic public key and a matching private key known only to the user. When a transaction is initiated, all nodes in the network would be notified of the transfer from the sender's public key to the recipient's public key. The private keys are then used to sign the transaction through a cryptographic process. These processes are handled invisibly, and not noticeable by the end users, for whom the direct peer-to-peer transaction proceeds almost instantly and in a frictionless manner.

[6] It has been described as an "elegant universal solution to the Byzantine Generals' Problem", which is one of the core problems of reaching consensus in distributed systems. *See* http://www.quora.com/Is-the-cryptocurrency-Bitcoin-a-good-idea. *See also* Marc Andreessen, *Why Bitcoin Matters*, New York Times, dated 21 January 2014.

Bitcoin technology records all transactions occurring in the system in a "block chain" which functions as a kind of universal public ledger, with each new block of transactions linked to a preceding block. Every Bitcoin transaction *ever* made can be observed by following this chain backwards. Because the block chain makes available to all a record of every single Bitcoin transaction, attempts to spend the same bitcoin after it has already been transferred can be easily detected by the network. Bitcoin transactions are irreversible the same way that cash transactions are irreversible.[7]

### *B. The Ecosystem*

A sizeable and vibrant crypto-currency ecosystem has developed over time in several leading jurisdictions, including Singapore – with a number of prominent venture capital firms having invested, and continuing to invest, in various crypto-currency start-ups and businesses. This ecosystem broadly comprises participants such as miners, users, exchangers, and transaction service providers, and software developers, among many other stakeholders:

a. Miners are persons or entities that run specialised software to generate solutions to complex algorithms and verify transactions in the crypto-currency network.

b. Users are persons or entities that obtain crypto-currency and use it to purchase goods or services, or to transfer value to another person, or to hold for investment purposes.

c. Exchangers are persons or entities in the business of exchanging crypto-currencies for real or fiat currency, such as the US dollar or the Japanese yen, or for other crypto-currencies or virtual currencies.

d. Transaction service providers are websites that provide transaction services, allowing individuals to store and transact Bitcoins without having to run the Bitcoin client on their own computers. This includes wallet and vault providers.

[7] Reuben Grinberg, *Bitcoin: An Innovative Digital Currency*, (2011) Hast. Sci. & Tech. L. J. 160, at p. 165.

e. Software developers are persons or entities that are involved in researching, designing, making or testing computer software that makes use of crypto-currencies.

Other participants in the crypto-currency ecosystem include market information and chart providers, and merchants that accept crypto-currencies in exchange for real goods and real services. Indeed, an increasing number of merchants also now accept Bitcoin as payment, including a number of established household names across the spectrum such as Dell, Target, Expedia, Bloomberg.com, Paypal and Tesla Motors. Several food and drink establishments in the US, Europe and Singapore also now accept Bitcoin as payment.

Complex crypto-currency-based financial products are also emerging in the market, particularly with more established crypto-currencies such as Bitcoin. Trading in crypto-currency futures is now possible with derivatives exchanges or trading platforms such as ICBIT and OKCoin. As recently as September 2014, TeraExchange, a Bitcoin derivatives exchange, announced that it had received approval from the US Commodity Futures Trading Commission to trade dollar-denominated Bitcoin currency swaps – the first ever Bitcoin swap approved in the US. Proposals for a Bitcoin exchange-traded fund ("ETF") are currently being considered by US regulators.[8] Some businesses have also introduced interest-bearing crypto-currency accounts and crypto-currency-based peer-to-peer lending services. These developments will likely boost liquidity in crypto-currencies, and potentially reduce volatility in crypto-currency prices. They also increasingly blur the line between the crypto-currencies and the traditional financial system.

### *C. Benefits and Future Applications*

Much of the discussion about crypto-currency regulation has tended to focus on the dangers posed by crypto-currencies. It is true that these risks exist, and there is a need for targeted regulation to address potential harms that flow from this. However, it is equally important not to over-emphasise these risks and lose sight of the substantial benefits, economic or otherwise, that may be gained through legitimate applications of the technology.

[8] Rob Curran, *With a Bitcoin ETF, Risk Isn't Virtual*, The Wall Street Journal, dated 7 September 2014.

To begin with, crypto-currencies can significantly reduce the costs of fund transfers across international borders. The capability for direct peer-to-peer transfers, without the need for an intermediary, can eliminate or substantially reduces transaction costs and time-lag. This technology has the potential to disrupt existing payment systems that involve intermediaries and associated agency costs, such as debit or credit card networks, by providing a platform for more efficient or frictionless mobile or electronic transfers in the future. Even if crypto-currency payments do not become widespread and ubiquitous, competition with existing payment systems and inter-crypto-currency competition are likely to bring down costs or improve the quality of payment services. Efficient and secure payments systems are vital to any well-functioning economy.

A frictionless mode of international money transfer is also particularly valuable in poorer developing countries, where remittance transaction costs tend to be the highest. Crypto-currencies could potentially revolutionise the existing $600 million annual global remittance market.[9] By way of example, Africa's diaspora pays around 12% in fees to send $200 in funds. The use of Bitcoin or other crypto-currencies could significantly cut both the time and costs of such remittances. This would in turn raise the quality of life for migrant workers and their families, and have a positive effect on the world's poorest countries.

Crypto-currencies also make micropayments easy and viable, where such payments would previously have not been cost-effective because of prohibitive transaction costs. This would allow businesses to extract value from low-cost goods or services on the Internet through calibrated and targeted pricing policies that use micropayments, such as one-time article downloads from newspapers, or one-time game or music downloads. Crypto-currency may support financial inclusion through new crypto-currency-based products that serve the un-banked, and can also facilitate crowd funding for small and medium enterprises.

More generally, crypto-currencies – and related block chain technologies – have the potential to be enablers of innovation on a much larger scale, just like other computer protocols such as TCP/IP and HTML. They can provide a platform for further financial or technical innovation, and enable a wide variety of different uses – even ones that have not yet been conceived of –

[9] *See* Mark Anderson, *Bitcoin shakes up remittances as poorer people offered digital deals,* The Guardian, 18 August 2014.

transforming entire industries and markets just as the Internet did. As some commentators have written, because crypto-currencies are protocols for exchanging values over the Internet without an intermediary, these protocols can be adapted to potentially transform any transaction that has traditionally required an intermediary or third party validation, including (1) property transfer; (2) contract execution; and (3) identity verification and management.[10]

## II. CLEAR AND TARGETED REGULATION

The emergence of new technologies, with accompanying new markets and new market actors, has always posed challenging issues for regulation. While it is said that technological innovation "disrupts" and transforms markets and industries, the effects of such disruptions invariably extend also to the regulatory and legal spheres. Pertinent legal issues raised by such technological disruption often encompass the uncertainty of applicability of existing rules, and the potential need for new rules to ban, restrict, or encourage the new technology.

The crypto-currency industry has had to grapple with much regulatory uncertainty of late – which has not been helped by some of the recent negative press coverage, including news surrounding the failure of Mt. Gox – at the time, the world's largest Bitcoin exchange – and the disappearance of 844,000 bitcoins (worth about US$480 milllion) held by it. In addition, Bitcoin's early association with the Silk Road marketplace, and its use for trading in illicit goods, also helped foster an impression among lay persons that Bitcoin and other crypto-currencies were somehow less than legitimate, and less than legal. Even if this was not actually correct in most jurisdictions, which do not ban the use of Bitcoin or other crypto-currencies, mixed signals and divergent proposals from regulators in jurisdictions around the world have further contributed to an uncertain regulatory environment.

Such uncertainty has tangible negative effects. Uncertain regulatory treatment makes it difficult for crypto-currency start-ups to access funding and to establish banking relationships. Regulatory uncertainty impedes the flow of institutional money and much needed investment

[10] Tiffany Wan and Max Hoblitzell, *Bitcoin's Promise Goes Far Beyond Payments*, Harvard Business Review, dated 24 April 2014.

capital into the crypto-currency industry. Consumers also tend to be wary given the uncertain legal status of crypto-currencies, and the lack of endorsement or backing by any government.

Clear and targeted regulations can do much to remedy this and clarify the legal environment, providing the framework for wider adoption of crypto-currencies by businesses and consumers. Targeted laws addressing specifically identified crypto-currency risks or regulatory interests are appropriate and consistent with the facilitative framework: targeted crypto-currency regulation would ensure that products or practices that are harmful are appropriately contained, while at the same time preserve the benefits of innovation and allow new business models to experiment, compete fairly, and flourish. This section explores these issues in the Singapore context, with three specific areas of regulatory focus: (a) anti-money laundering and counter-terrorist financing; (2) securities and financial regulation; and (c) theft, misappropriation and fraud.[11] It aims to capture a snapshot of the salient concerns in each area; although a full treatment of the issues raised will not be possible given the prevailing constraints of time and space.

### *A. Anti-Money Laundering and Counter-Terrorist Financing*

In March 2014, the MAS announced that it would be taking a "targeted regulatory approach" to regulating virtual currencies (which include crypto-currencies), in order to "specifically address money laundering and terrorist financing risks".[12] This is within its mandate as central bank and financial regulator to issue regulations in the area of anti-money laundering and counter-terrorist financing ("AML/CTF"), as expressly authorised by Section 27B of the Monetary Authority of Singapore Act.

#### 1. Justification for AML/CTF Regulation

Decentralised crypto-currency systems have obvious and real AML/CTF risks because they are convertible to real fiat currency and characterised by a high degree of anonymity – certainly a higher degree of anonymity than traditional payment methods such as credit cards. The Bitcoin

[11] These are not exhaustive of the regulatory landscape that determines the crypto-currency business environment. Other regulatory issues such as tax treatment are relatively settled, and are in any event not the subject of this Chapter due to constraints of space and time.
[12] Press Release, *MAS to Regulate Virtual Currency Intermediaries for Money Laundering and T*

protocol does not require identification of participants, and is not set up to monitor suspicious transaction patterns.[13] This system has been more accurately described as "partially anonymous", because although the trail of all transactions made from all accounts can be seen on the "block chain", nothing in the system allows one to tie specific accounts or transactions to real world individuals.[14]

The upshot is that crypto-currencies such as Bitcoin permit completely anonymous transfers on a peer-to-peer basis, with no requirement for the sender and recipient to be identified, and the decentralised nature of the network means that no one individual or entity can be singled out easily for investigation or asset seizure. AML/CTF risks are also particularly heightened because of the global reach of crypto-currencies through the Internet, which allows them to be used to make almost instantaneous cross-border transfers that are difficult to detect and trace.

There is thus a clear and present justification for AML/CTF regulation of crypto-currencies. Indeed, many jurisdictions have imposed or are exploring regulations in this regard. The question is not, then, whether or not to impose AML/CTF regulation, but what kind of AML/CTF regulation is appropriate.

### 2. AML/CTF Regulation in Singapore

Like most developed jurisdictions, Singapore's AML/CTF regime involves a two-prong regulatory strategy, involving criminal sanction for offences on the one hand, and prevention through a regulatory licensing regime on the other. Thus, at least two types of issues are implicated in considering AML/CTF regulation for crypto-currencies: (i) first, in relation to AML/CTF offences and sanctions, whether the existing rules and regulations extend to crypto-currency-related transactions; and (ii) second, in relation to licensing regimes, which entities should be subject to money transmission licensing requirements, and what rules or regulations should apply to such licensed crypto-currency entities.

On the first issue, the governing AML/CTF statutes in Singapore are the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (the "CDSA") and the Terrorism (Suppression of Financing) Act ("TSOFA"). Both statutes are drafted in

[13] 2014 FATF Report, at p. 9.
[14] Reuben Grinberg, *Bitcoin: An Innovative Digital Currency*, (2011) Hast. Sci. & Tech. L. J. 160, at p. 164.

technologically-neutral terms, and adopt very broad, all-encompassing definitions of "property" that are likely to cover crypto-currencies and crypto-currency transaction.

The CDSA sets out four types of money laundering offences, namely: directly or indirectly acquiring, possessing, using, concealing or transferring property that represents the benefits of drug trafficking or criminal conduct; assisting another person in doing the former; failing to disclose or report any knowledge or suspicion to the Suspicious Transactions Reporting Office ("STRO") that any property represents the proceeds of drug trafficking or criminal conduct; and tipping off and disclosing information likely to prejudice an investigation under the Act.[15] These offences will likely apply in the context of crypto-currencies and crypto-currency transactions: the act defines "property" as "money and all other property, movable or immovable, including things in action and other intangible or incorporeal property".[16]

Similarly, the TSOFA sets out a number of terrorism financing offences, namely: providing or collecting property for terrorist acts; making available, using or possessing property for terrorist purposes; and direct or indirect dealing with property of terrorists; failing to disclose information about transactions involving property belonging to any terrorist or terrorist entity; and tipping off and disclosing information likely to prejudice an investigation under the Act.[17] Like the CDSA, the TSOFA is also likely to apply to crypto-currencies and crypto-currency transactions, as it adopts a similarly broad definition of "property" as "assets of every kind, whether tangible or intangible, movable or immovable, however acquired".[18]

On the second issue, the MAS had announced in March 2014 that it would be introducing regulations for "virtual currency intermediaries that buy, sell or facilitate the exchange of virtual currencies for real currencies", to require them to verify customer identities and report suspicious transactions to the STRO.[19] No regulations have been formally introduced as of the

[15] Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A), Sections 39, 43, 44, 46, 47, 48.
[16] Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Cap. 65A), Section 2.
[17] Terrorism (Suppression of Financing) Act (Cap. 325), Sections 3-6, 8, 10B.
[18] Terrorism (Suppression of Financing) Act (Cap. 325), Section 2(1).
[19] MAS Media Release, *MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks*, 13 March 2014.

time of writing of this chapter, but it is anticipated that the regulations would cover a number of existing and future crypto-currency businesses.

As discussed above, a licensing regime for AML/CTF regulation is justified considering the risks posed by decentralisation and anonymity. Licensing requirements can establish accountability structures and allocate responsibility for the policing of the decentralized crypto-currency network for AML/CTF activity. This will boost consumer and institutional confidence in crypto-currencies. At the same time, such licensing and accompanying regulation will mean increased costs of compliance for businesses, and may have the unintended effect of increasing barriers to entry and punishing smaller businesses and start-ups – an outcome inimical to promoting innovation in the crypto-currency industry.

A thoughtful balancing of costs and benefits is therefore necessary in deciding which entities to license, and what regulations to impose on licensed entities. Regulators will need to weigh the potential costs and calibrate any proposed regulation accordingly, in order not to stifle innovation and the potential economic and productivity benefits of a thriving crypto-currency industry. This is well encapsulated by the "risk-based approach" recommended by the Financial Action Task Force ("FATF") – an intergovernmental standard-setting and body, of which Singapore is a member State, with an AML/CTF mandate – which counsels in favour of applying preventive measures that "are commensurate to the nature of risks".[20]

This is also encapsulated in Tenet 5 of the MAS' Tenets of Effective Regulation, which are internal guiding principles for the development and review of the MAS' regulatory framework. Tenet 5 requires MAS regulation to be "impact senstitve", and this requires that the "costs and impact of regulation" not be "disproportionate to the benefits", and that regulation be "targeted clearly at specific and material risks", and to avoid "unintended and unnecessary disruption to market practices".[21]

The definition of the relevant "intermediaries" which are subject to licensing and regulation will become decisive. Two possible approaches are available to the regulators. The first is to extend the existing regime under the Money-Changing and Remittance Businesses Act

[20] *See* FATF Guidance for a Risk-based Approach, *Prepaid Cards, Mobile Payments and Internet-based Services*, June 2013, ("2013 FATF Guidance"), at para. 89.
[21] MAS Tenets of Effective Regulation, at p. 12.

("MRBA") via interpretive guidance from the MAS, potentially clarifying that certain crypto-currency businesses, particularly exchanges, fall within the MRBA definition of a "remittance business".[22] This is similar to the approach taken by the US Treasury Department's Financial Crimes Enforcement Network ("FinCEN") which issued interpretive guidance documents in March 2013 and January 2014 to extend existing registration, reporting and recordkeeping requirements for "money services business" under the US Bank Secrecy Act[23] to crypto-currencies. The second approach is to enact *sui generis* regulations for crypto-currencies, similar to New York's recently proposed "Bitlicense" proposal. Which approach Singapore regulators choose may ultimately be a matter of form rather than substance, although the latter approach would allow for greater customisation of rules to fit the needs and risk-profile of the crypto-currency industry and ecosystem.

Regardless of which approach is taken, what is vital is that regulators calibrate the scope of the licensing regulatory regime such that participants in the crypto-currency ecosystem which are *not* in the business of exchanging, transmitting or trading crypto-currencies for real fiat currency or for other crypto-currencies – i.e. miners or users using crypto-currency to purchase real goods and services, and merchants accepting crypto-currency – are not regarded as money transmission *intermediaries*, and therefore not unduly subject to potentially onerous compliance requirements. This is consistent both with FATF's risk-based approach and current international best practices, as reflected by the US FinCEN guidance and German BaFin rules.[24] AML/CTF regulation that covers miners and end users would be over-inclusive, contrary to best practice, and significantly bog down the crypto-currency ecosystem in Singapore with unnecessary costs.

As regards the specific regulations applicable to licensed entities, the MAS had announced in March 2014 that it would be introducing basic AML/CTF rules such as customer due diligence requirements, transaction reporting and recordkeeping requirements. These would likely be similar to those that exist under the MRBA, which stipulates all of the above requirements in

[22] Defined in Section 2(1), Money-Changing and Remittance Businesses Act (Cap. 187), as "the business of accepting moneys for the purpose of transmitting them to persons resident in another country or a territory outside Singapore".
[23] 18 U.S.C. § 1960; 31 CFR §§ 1022.210, 1022.300, 1022.380(e), 1022.400.
[24] FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies* (2013), FIN-2013-G001, at p. 5.

relation to transaction amounts of SGD$5000 and above.[25] These rules are appropriate, justified and consistent with international best practices as crystallised in the FATF Guidance.[26]

It is unclear from the MAS announcements whether Singapore regulators will extend to crypto-currency-related businesses the existing rules under the MRBA that are meant to apply to "remittance businesses" or "money-changers" – in particular, the rules stipulating requirements for a minimum capital of SGD$100,000 and a SGD$100,000 bond,[27] or rules requiring licensees to have a "permanent place of business" in Singapore in order to operate.[28]

Applying such rules to crypto-currencies would be inappropriate: those rules are designed for and are rooted in a different contextual background, and extending them to the crypto-currency ecosystem will have unintended costs and consequences. For instance, the requirement for a physical "place or location in Singapore" for business activities is both unnecessary and awkward when applied to crypto-currencies, especially given that a large diversity of crypto-currency business models do not involve or necessitate brick-and-mortar premises. Similarly, the rules requiring a minimum capital or bond sum were expressly introduced in order to create "higher entry requirements" so that only large or well-established remittance firms remained, thus "weed[ing] out the weaker players in the industry".[29] This stated justification is at odds with the promotion of Singapore as an innovation-friendly hub or ecosystem for crypto-currency start-up companies.

An optimal AML/CFT regulatory regime for crypto-currencies should be facilitative, with customised rules appropriate for the industry, and with suitable breathing space for innovation; it should not dis-incentivise or exclude small, nimble and innovative business models from legitimately participating in business activities within the regulatory umbrella.

[25] Money-Changing and Remittance Businesses Act (Cap. 187), Sections 21, 32-33; MAS Notice 3001, *Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Money-Changer's Licence and Remittance Licence*, 1 July 2014, at paras 3-6, 8-10.
[26] 2013 FATF Guidance, paras 63-70,
[27] Money-Changing and Remittance Businesses Act (Cap. 187), Sections 9, 10.
[28] Money-Changing and Remittance Businesses Act (Cap. 187), Section 11.
[29] Second Reading, *Money-Changing and Remittances (Amendment) Bill*, 15 August 2005, Column 1227-1228.

### *B. Securities and Financial Regulation*

Another mode of potential crypto-currency regulation is through securities or financial regulation. Such rules target and deal with very different regulatory interests from AML/CTF regulation: securities regulation deals with consumer protection and market integrity issues in the financial services sector, while financial regulation is concerned more fundamentally with issues of systemic risk and financial stability.

Singapore regulators have expressed that crypto-currencies would not be considered "securities" under the Securities and Futures Act (the "SFA").[30] This is consistent with Section 2(1) of the SFA, which defines "securities" as, inter alia, debentures or stocks issued by governments or private corporations, any right or option or derivative in respect of any such debentures or stocks, any unit in a collective investment scheme, or any unit in a business trust or its derivative.[31] Crypto-currencies are thus not subject to the investor protection and market integrity regulation under the SFA and the Financial Advisers Act in Singapore, including the various registration, disclosure, and anti-fraud obligations under those statutes.

However, this does not preclude investment products or investment schemes that are based on crypto-currencies from being regulated under securities regulations. Distinct from the purchase and exchange of crypto-currencies themselves, crypto-currency-based financial products, such as ETFs or derivatives, involve the use of regulated investment structures and therefore attract the application of the relevant securities regulations.

For instance, crypto-currency ETFs would constitute "collective investment schemes" under the SFA, with the shares of such ETFs qualifying as "securities" under the SFA.[32] Similarly, crypto-currency derivatives will likely fall within the regulatory umbrella of Parts VIA and VIB of the SFA and the requirements therein. Even though crypto-currency derivatives are not currently defined as "specified derivatives contracts" by existing guidelines, which is limited to interest rate and credit derivatives,[33] Sections 124 and 125 of the SFA clearly envisage that

[30] FT Article 13 March 2014. Deputy Prime Minister and Minister in charge of MAS, Mr Tharman Shanmugaratnam, "Reply to Parliamentary Question on Virtual Currencies", MAS, Notice Paper 62 of 2014 (21 February 2014)
[31] Securities and Futures Act (Cap. 289), Section 2(1).
[32] Securities and Futures Act (Cap. 289), Section 2(1).
[33] Securities and Futures (Reporting of Derivatives Contracts) Regulations 2013, Regulation 5.

the MAS may prescribe that the regulations to apply to such derivatives. In any event, these crypto-currency-based financial products are only at a very early stage of development, and do not raise significant regulatory concerns yet.

As for financial regulation, the effects of crypto-currencies on monetary policy and financial stability are currently unclear. Crypto-currencies are not issued or backed by any governmental authority, and, at current adoption levels, do not have sufficient market capitalization to significantly impact the supply of money or otherwise affect macroeconomic policy. In addition, crypto-currency businesses, unlike banks, do not have access to public safety nets or central bank liquidity, and therefore there is little or no justification for prudential regulation for safety and soundness concerns.

Crypto-currency firms and businesses also do not pose the same systemic risks as banks do in the form of a structural vulnerability to "runs", because they do not carry out maturity transformation, i.e. the conversion of short-term liquidity needs of depositors into long-term funding commitments for borrowers. As the Diamond-Dybvig model illustrates, it is the structural mismatch between the liquidity and maturity profiles of a bank's funding structure – i.e., the fact that banks borrow short to lend long – that gives rise to the potential for systemically destabilizing "runs".[34] Since crypto-currency firms are not generally in the business of performing maturity transformation, and do not pose the same systemic risks as banks, financial regulations such as capital requirements or public insurance schemes are not appropriate.

That said, drawing the line between typical crypto-currency firms and banks will become less clear-cut over time, as lending in crypto-currencies and crypto-currency fractional reserve banks becomes possible and more widespread. It is too early to tell whether this "financialisation" trend will continue, but at present crypto-currency banking and lending services remain quite niche and do not yet pose any real regulatory concerns. Hasty regulation in this area would be both unwarranted and unwise, and poses more risks than benefits.

---

[34] *See* Douglas W. Diamond & Phillip H. Dybvig, *Bank Runs, Deposit Insurance, and Liquidity*, 91 J. Pol. Econ. 401, 404 (1983); Jonathan Lim, *Untangling the Money Market Fund Problem: A Public-Private Liquidity Fund Proposal*, 19 Stanford J. Law. Bus. & Fin. 63, at pp. 83-84.

### *C. Theft or Misappropriation*

Like cash or other forms of money, crypto-currencies function as a store of value and a medium of exchange, and contain or signify a degree of economic value for its owner. Similarly, just like cash, crypto-currencies can be lost or stolen (from virtual wallets), thus resulting in effective destruction of that economic value for the owner. However, while there are clear civil and criminal laws that protect one's property rights in tangible hard currency or cash, it is unclear under existing laws whether such private remedies or criminal sanctions extend to the theft or misappropriation of crypto-currencies.

Under Singapore law, it is uncertain whether private remedies for theft or misappropriation apply to crypto-currencies. Conversion is the principal civil remedy under English or Singapore law in respect of theft or misappropriation of personal property (including money),[35] and provides the original owner with a means of vindication where those rights have been interfered with, including through tracing his original property and demanding the return of the property or its equivalent in kind from third parties. However, the current state of Singapore case law has left undetermined the question of whether conversion remedies are available for intangible property – a category that includes crypto-currencies.

As the Singapore High Court recently held, it "remains an open question in Singapore whether intangible property can form the subject matter of conversion".[36] In another recent decision, the Singapore Court of Appeal – Singapore's apex court – cited to the approach by the majority of the English House of Lords in the *OBG v Allan* case,[37] which had held that conversion protects only interests in physical chattels, and that there cannot be conversion of intangible property such as choses in action.[38] However, the Singapore Court of Appeal held on its facts that a narrow exception documentary intangibles (i.e., where the intangible property in question has a corporeal representation, such as in the case of cheques or share certificates) applied in

[35] *Kuwait Airways Corporation v Iraqi Airways Co (No 3)* [2002] UKHL 19 (HL).
[36] *Tjong Very Sumito and Ors v Chan Sing En and Ors* [2012] 3 SLR 953, at p. 985.
[37] *OBG Ltd v Allan* [2008] 1 AC 1.
[38] *Alwie Handoyo v Tjong Very Sumito and another* [2013] 4 SLR 308, at para. 131

that case, and that it was therefore not necessary to determine whether conversion could apply to purely intangible property.[39]

Crypto-currencies need not have their existence reflected in a physical document, and would therefore be classified as purely intangible property. It is unclear whether conversion remedies would be available for theft or misappropriation of crypto-currencies. Practically, this means that a victim of crypto-currency misappropriation or theft might only have a personal remedy against the relevant exchange or counterparty (under contract, tort or other related personal actions such as unjust enrichment), but not a proprietary remedy that can be used to make recovery against third parties that come into possession of the intangible online property.

A number of prominent legal commentators have rightly criticised the distinction between tangible and intangible property as arbitrary and without basis. Indeed, a fixation with physical possession as the traditional criterion for the availability of the remedy of conversion is inappropriate and out of place in a modern economy, where many things of value are intangible.[40] As a matter of principle, conversion should apply to protect property interests – whether tangible or intangible – that are excludable from others and capable of being controlled in a broader and not just physical sense.[41] Unfortunately, this is not yet the current state of the law in Singapore; however, it is hoped that the realities of a functioning crypto-currency and significant peer-to-peer economic activity will shape the law towards abolishing this distinction between tangible and intangible property.

As for criminal sanctions, Singapore law has equally little to say about theft or misappropriation of crypto-currencies: intangible property is not covered by criminal offences for theft or misappropriation of property under Singapore law. Theft is defined under Section 378 of the Penal Code with reference to dishonest taking of "movable property", which is defined in Section 22 as including "corporeal property of every description". The same goes for criminal misappropriation of property under Section 403 of the Penal Code, which also makes reference to "movable property". Thus, unlike other jurisdictions such as the UK, whose

[39] *Alwie Handoyo v Tjong Very Sumito and another* [2013] 4 SLR 308, at para. 132 to 137.
[40] Susannah L.K. Shaw, *Conversion of Intangible Property: A Modest, but Principle Extension? A Historical Perspective*, at pp. 434-435.
[41] Susan Green, *To Have and To Hold? Conversion and Intangible Property*, 71(1) M.L.R. 114, (2008), at p. 117.

1968 Theft Act expressly defines protected "property" to include "things in action and other intangible property", Singapore's criminal legislation does not address theft or misappropriation of intangible property. The one exception is the offence of "cheating", which is defined under Section 415 of the Penal Code to include dishonestly inducing the delivery of "any property". This has, however, only a limited scope and will not cover all instances of theft or misappropriation.

Singapore's cybercrime legislation, the Computer Misuse and Cybersecurity Act, does little to address the above lacunae in relation to theft or misappropriation of intangible online property. That Act relies on a predicate offence approach, and punishes the use of a computer to commit certain crimes or offences involving "property, fraud, dishonesty or which causes bodily harm".[42] Without a predicate offence for theft or misappropriation under the Penal Code, all the cybercrime legislation does is criminalise very narrow classes of online misdemeanours, including "unauthorised access to computer material", and "unauthorised modification of computer material".[43] While these provisions may address to some extent particular hacking and cyber-security breach concerns, they do not address many situations of theft or misappropriation of crypto-currencies – which may not necessarily involve a breach or lack of authorisation.

Under existing Singapore law, therefore, it remains unclear whether (or which) private remedies or criminal sanctions will be available in a case of theft or misappropriation of crypto-currency. The laws in this area appear to be still grappling with an old-world distinction between tangible and intangible property, with protection from interference largely available only for the former. As stated above, this is unsustainable in a modern economy where, as is the case in the crypto-currency system, systems of value and commerce are built upon intangible, but highly valuable, property. A developed and flourishing crypto-currency business sector requires commercial certainty and clearly defined and enforceable property rights in respect of crypto-currencies; this is currently lacking under the current legal landscape in Singapore, and will require further clarification or reform, whether through courts or legislators.

[42] Computer Misuse and Cybersecurity Act (Cap. 50A), Section 4.
[43] Computer Misuse and Cybersecurity Act (Cap. 50A), Sections 3, 5 to 8.

## III. A SELF-REGULATORY FRAMEWORK

In addition to clear and targeted regulations, effective crypto-currency regulation requires a robust self-regulatory framework involving effective partnership between industry and regulators. This is a matter of regulatory architecture or structure; and not simply a matter of substantive content, as with the specific regulatory norms discussed in the preceding section. A self-regulatory process or framework involves the setting, policing and enforcement of standards governing firms or individuals within an industry by *private* actors or industry professionals, rather than by external *public* regulators. In other words, self-regulation involves, structurally, a degree of private sector involvement in the regulatory process, by the regulated industry itself.

There are a number of benefits to this approach. Self-regulation is said to lower monitoring and enforcement costs: a self-regulatory body will usually have more technical expertise and knowhow than external regulators, and this is especially true in fast-moving industries with a high rate of technological change, and which by nature often involve regulators playing catch-up with industry knowhow. It is also said to create incentives for voluntary compliance by the industry, reduce costs of amending and adapting standards, and also increase collaborative behaviour and positive interaction between the industry and regulators. Self-regulation can also help to foster trust between consumers, regulators and the industry, and can thereby encourage further investment and innovation.[44]

Self-regulation has thus proven suitable in industries characterised by dynamism, complexity or innovation. For instance, self-regulation has been used as a regulatory tool in connection with complex financial markets with significantly fast-moving financial innovations, such as the regulation of financial derivatives, as in through the use of Swap Execution Facilities and Futures Exchanges acting as self-regulatory organisations in post-2008 US Dodd-Frank Title VII regulations. Self-regulation reflects a regulatory attitude of accommodating disruptive

[44] Daniel Castro, *Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising,* The Information Technology & Innovation Foundation, 1 December 2011, at p. 3.

innovation, and is premised on innovation being a necessary component of a competitive and productive economy.

In addition, self-regulation is also particularly appropriate for regulating internet-based activities and businesses, such as in the crypto-currency ecosystem, because it allows for regulatory structures that "mirror" the internet as a global, private and decentralized network.[45] Indeed, regulation of the "code" layer (as distinct from the "physical" or "content" layer)[46] of the Internet is and has always been carried out through the self-regulatory, private initiatives of the Internet Corporation for Assigned Names and Numbers ("ICANN").

Varying degrees of self-regulation are possible, depending on the degree of collaboration between the self-regulatory organisation and government agencies, the powers granted to the self-regulatory organisation, or the legal or binding character (or lack thereof) of the self-regulation norms. Indeed, depending on various calibrations of these factors, self-regulatory organizations can: play a gap-filling interpretive role within a legal framework with "hard" enforceable rules; exercise a rule-making function but without any formal supervisory or enforcement functions; or take on full-fledged regulatory functions that cover the entire gamut of rule-making, supervising compliance, and enforcement.

Self-regulation tends to work best when paired with government involvement or support. Indeed, commentators have stated that "self-regulation cannot function without the support of public authorities", whether that support is found in wilful non-interference, endorsement or ratification, or through active collaboration and enforcement support.[47] Self-regulation should not be seen as a substitute for traditional regulation through legislation and formal enforceable rules, but rather as a complement to such a legal framework.

Self-regulation may involve the use of "soft" norms through non-binding codes of conduct or informal guidelines. Such norms do not come attached with legal sanctions for non-compliance, and instead rely more on reputational sanction and market incentives for compliance. In certain industries involving sophisticated participants, soft norms can be more effective than binding and enforceable rules. Indeed, the "regulatory uncertainty principle"

[45] Bertelsmann Foundation, *Self-regulation of Internet Content*, 1999, at p. 21.
[46] Lawrence Lessig, *The Future of Ideas: The Fate of Commons in a Connected World* (2001), at p. 23.
[47] Bertelsmann Foundation, *Self-regulation of Internet Content*, 1999, at p. 22.

holds that when a rule crystallises as a binding financial regulation, it will cause adaptive behaviours and changes in the regulated institutions' risk management practices such as to water down the rule's effectiveness – in other words, it will result in regulatory arbitrage to circumvent the rule.[48] In such an environment, the flexibility and adaptability of soft norms may be more effective in incentivising voluntary compliance, especially when normative content is generated from within the industry.

These principles are not merely abstract; they are readily applicable in the Singapore context. Indeed, self-regulation is consistent with the MAS' Tenets of Effective Regulation, which expressly recognise that a "self-regulatory approach" can be "effective and appropriate" when applied in the right circumstances.[49] Thus, the "Stakeholder-Reliant" principle "acknowledge[s] and encourage[s] the contribution that financial institutions individually, the financial industry collectively and other stakeholders" can make in "achieving outcomes aligned with the MAS' supervisory objectives".[50] Likewise, the "Business-Friendly" principle espouses due regard to "business efficiency and innovation", and calls for regulators to "adopt a consultative approach to regulating the industry".[51]

MAS' Tenet 2 on "Shared Responsibility" clearly articulates the MAS' regulatory philosophy that "[t]he design of regulation should wherever appropriate provide for rather than take away from financial institutions and stakeholders' responsibility and incentives to contribute towards regulatory outcomes" – specifically, with the regulated institutions, including their "board and senior management", and the "industry collectively", taking on such responsibility for regulatory outcomes.[52] The MAS does rely, in practice, on self-regulatory organisations to carry out several regulatory functions; for example, the Singapore Foreign Exchange Market Committee ("SFEMC") and the Singapore Exchange ("SGX") carry out self-regulation in relation to conduct or market integrity issues in foreign exchange and securities markets.

In relation to crypto-currencies, the Association of Crypto-Currency Enterprises and Start-ups, Singapore ("ACCESS") presents a ready candidate for a crypto-currency self-regulatory

[48] Speech by Jaime Caruana, *Financial regulation, complexity and innovation,* Bank of international Settlements Promontory Annual Lecture, 4 June 2014, at p. 3.
[49] MAS Tenets of Effective Regulation, at p. 31.
[50] MAS Tenets of Effective Regulation, at p. 10.
[51] MAS Tenets of Effective Regulation, at p. 10.
[52] MAS Tenets of Effective Regulation, at p. 11.

organisation. ACCESS was formed on 30 May 2014 as a registered society with the Registry of Societies in Singapore, and its objectives are, first, to promote dialogue with regulators and other stakeholders; and second, to conduct "self-regulation" of the crypto-currency industry, including through establishing a code of conduct for firms that will become a criteria for membership. ACCESS appears ready and willing to take on the mantle of self-regulation, although it is still unclear at this stage what kind of regulatory role it could play within the system, and what degree of collaboration with regulators would be possible.

For the reasons above, a robust self-regulatory framework involving effective partnership between ACCESS and regulators such as MAS would produce contextually adaptable regulations that complement the legal framework, lower regulatory costs, and support innovation – and should be encouraged if Singapore is to augment its position as a regional or global hub for crypto-currencies and next-generation financing.

## IV. INTERNATIONAL COORDINATION AND HARMONISATION

Finally, the international dimension of any crypto-currency regulation warrants attention. Owing to the de-territorialized and often international nature of crypto-currency transactions, effective regulation will require a significant amount of coordination and harmonisation among regulators and jurisdictions.

Indeed, the Internet and crypto-currency transactions are by nature borderless, and this sits uncomfortably with traditional regulatory boundaries of jurisdiction and sovereignty. This is particularly so in the case of cybercrime and online misdemeanours: they can originate in one jurisdiction, but have deleterious effects in another, and sometimes on nationals of yet another jurisdiction.

Thus, no single jurisdiction can guarantee a protected cyber-security environment on its own: crimes in one territory can go without detection or punishment because they cannot be effectively monitored or enforced against persons outside the jurisdiction. Coordination and cooperation among regulators and law enforcement authorities to address such issues is thus essential. The importance of such cooperation is underscored by the recent failure of Mt. Gox,

where reportedly more than US$480 million of customers' crypto-currency had disappeared as of February 2014, allegedly due to large-scale hacker attacks which have to this date gone unpunished.

However, international cooperation on cyber-security issues can be as complicated as it is necessary, particularly as different countries can take very different approaches in their national laws, policies or attitudes on issues of cybercrime and cyber-security. Some countries see vital state and national security interests as implicit in such cyber-security issues, and have regulatory or legal structures that allow extensive governmental intrusion into the sender and recipient details of every single transmission, and the contents of such transmissions. Other countries see that proper Internet governance requires balancing security concerns against certain constitutionally protected freedoms, and accordingly have legal structures that emphasise privacy and data protection.[53] These differences are fundamental and may be difficult to reconcile in specific cases, as the recent WikiLeaks episode illustrates.

In Singapore, regulators have pursued more partnerships with other regulators on the cyber-security front in recent years, including through the signing of information sharing and collaborative agreements with other regulators in jurisdictions such as Japan and South Korea. Commentators believe that international cooperation will continue to scale upwards with the opening of the INTERPOL Global Complex for Innovation in Singapore in 2014, and the deepening of cooperative ties with the European Cybercrime Centre.[54]

Effective crypto-currency regulation will require further and more detailed cooperation arrangements with foreign regulators, and particularly on crypto-currency- and Bitcoin-specific cyber-security issues. This will go some way to creating a stable regulatory environment that will boost consumer confidence and support the crypto-currency industry.

Aside from cyber-security issues, many crypto-currency regulations in foreign jurisdictions, such as in the US or Canada, are expressed to have extraterritorial effect, and this subjects

[53] David Satola and Henry L. Judy, *Towards a Dynamic Approach to Enhancing International Cooperation and Collaboration in Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Frameworks: Reflections on the Proceedings of the Workshop on Cybersecurity Legal Issues at the 2010 United Nations Internet Governance Forum*, William Mitchell Law Review 1743, at p. 1750.
[54] Winnie Chang, *Amendments to the Computer Misuse Act*, E-finance & Payments Law & Policy, February 2013.

crypto-currency firms in Singapore to a "double deontology" risk, where they may be subject to potentially conflicting and irreconcilable rules at the same time. For instance, Canada's recently released virtual currency regulations, issued by the Financial Transactions and Reports Analysis Centre of Canada ("Fintrac"), are stated to have extraterritorial effect and captures foreign firms that either have a place of business in Canada, or are offering services to Canadians. Thus, a crypto-currency firm operating in Singapore may have to comply not just with Singapore regulations, but also with Canadian crypto-currency regulations, to the extent it has a Canadian office or markets to Canadian customers. In a case of conflict, the firm may have no choice but to comply with the stricter standard, even though its competitors may not be similarly constrained; worse still, in cases of more fundamental conflict, complying with either standard may put a firm in breach of the other standard it is subject to.

As such, the extraterritorial reach of foreign regulations could impose particularly onerous compliance obligations on crypto-currency firms, and have a significant impact on their costs and competitiveness. This also adds to the existing regulatory uncertainty, especially when the applicable laws to any particular transaction may be different and potentially in conflict. Given the inherently cross-border nature of most crypto-currency business models, this creates very real risks for firms operating in this space.

A facilitative regulatory model should accommodate the decentralised, diverse and international nature of the crypto-currency markets. This requires that cross-border harmonisation of regulations in Singapore and other leading jurisdictions be prioritised and pursued to the extent possible, in order to minimise regulatory uncertainty, reduce unnecessary costs, and eliminate opportunities for rent-seeking and regulatory arbitrage.

## V. CONCLUSION

With the globalisation of commerce and the increasing porosity of territorial boundaries, the use of crypto-currencies will only continue to grow. There is a real demand for private currencies that are not necessarily tied to any particular government, and for a frictionless payment system that accommodates and best suits the increasingly de-centralised and transnational character of modern e-commerce. This is a technology that has the potential to

transform the way people buy and sell services across the world, with almost limitless economic potential flowing from this.

Thoughtful and well-designed regulation can play a large part in this development, by clarifying the business environment and boosting both consumer and investor confidence. This requires, on one hand, the weeding out of real and present dangers, such as money laundering, terrorist financing, cybercrimes, and other misdemeanours. On the other hand, this also requires a regulatory approach that recognises the risks of over-regulation, including its negative effects on productivity and innovation. The facilitative model outlined in this chapter aims to strike the appropriate balance between promoting innovation and preventing illegitimate use; and outlines the legal, extra-legal, as well as international aspects of how such a balance would be struck. This will provide a foundation for crypto-currencies to flourish in the real world, such that the industry's much-talked-of potential will become an economic and commercial reality, rather than just a geeky pipedream.