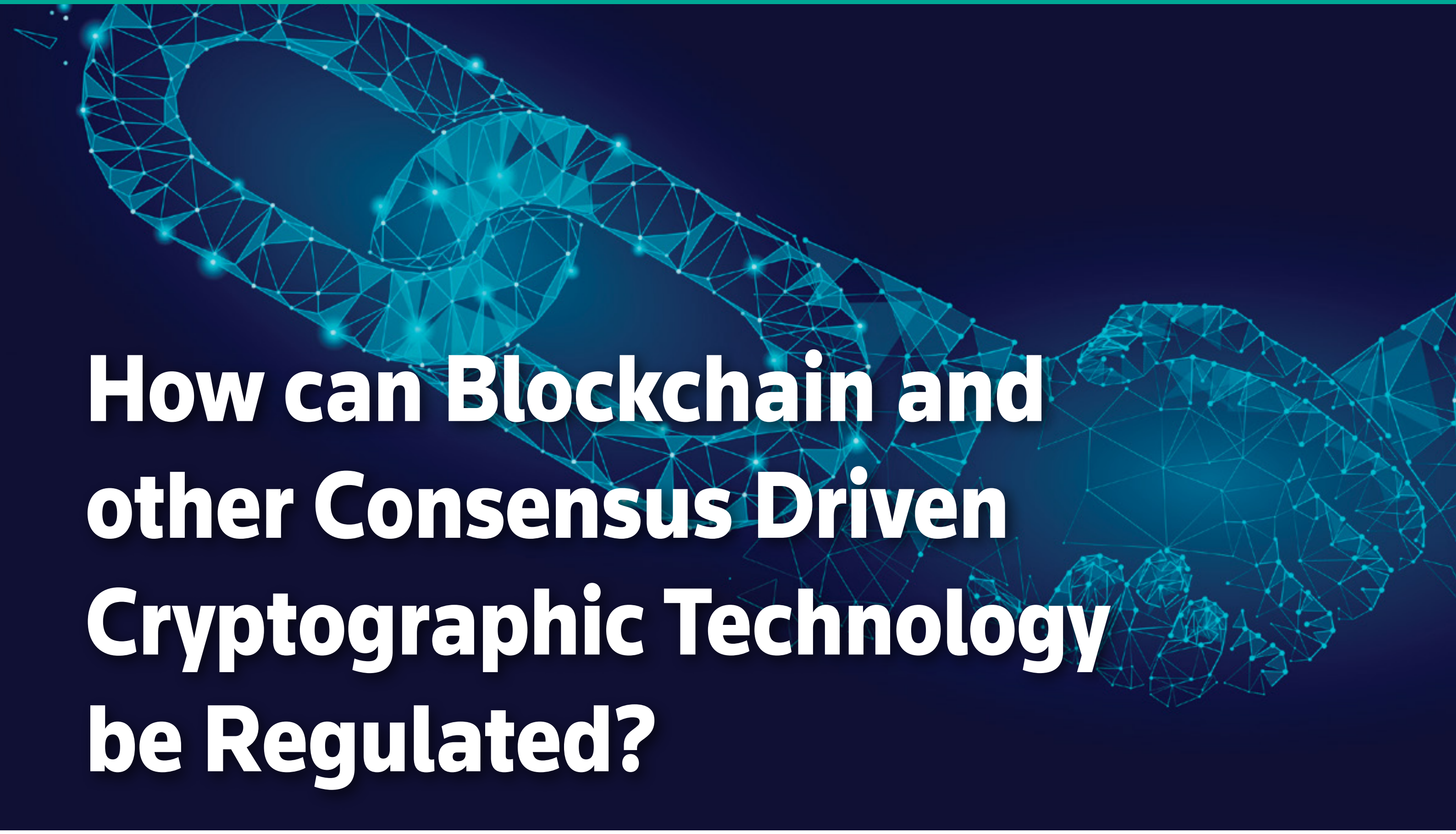


How can Blockchain and other Consensus Driven Cryptographic Technology be Regulated?

By Syren Johnstone, Executive Director, *LLM (Compliance & Regulation) Programme, Faculty of Law, The University of Hong Kong*

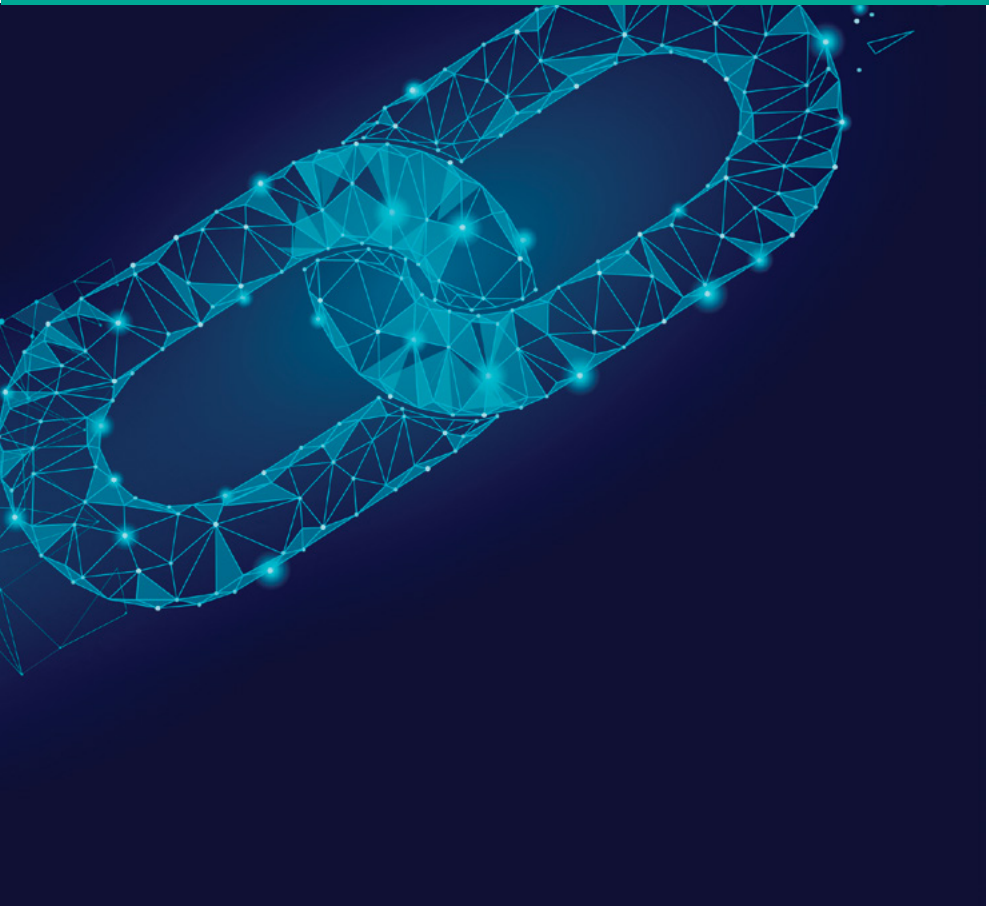
Some participants in the crypto/blockchain/DLT industry actively invite regulatory oversight but policy considerations and the usual patterns of legal and regulatory development can mean that wanting to be regulated is not always the same as being able to be regulated.

This article examines aspects of the technology that make it difficult to regulate the primary and secondary market while at the same time allowing industry development without it being affected by fraud and abuse, or being used to service money laundering and other criminal purposes. It concludes by suggesting the policy approach that regulators should take to this new technology.

The technology is the starting point

In 1988 Tim May famously stated "Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner. Two persons may exchange messages, conduct business, and negotiate electronic contracts without ever knowing the True Name, or legal identity, of the other." Today, that has become a reality in a developing digital ecosystem that is being built on cryptographically secure consensus technology ("CCTech") that forms the basis of blockchain and distributed ledger technology applications.

CCTech enables qualitatively different boundaries of commercial activity than was previously possible. It holds the promise of enabling new ways of undertaking existing commerce that provide efficiency gains, as well as generating new types of commercial activity. The first peer-to-peer version of electronic cash created on 3 January 2009 (Bitcoin), has been followed by other cryptocurrencies, digital tokens that provide access to some service or utility or operate as a security (see Hong Kong Lawyer, March 2018 "ICO Utility Tokens and the Relevance of Securities Law"), and smart contracts (collectively, "cryptos").



Industry growth has involved developers tapping into the highly regulated public capital market in ever-larger offerings. A secondary market facilitated by crypto exchanges has emerged. This is creating significant challenges to regulatory agencies to define how existing laws and regulations might apply.

Establishing a sustainable regulatory approach is complicated by features of CCTech still undergoing transformational evolution that pose novel challenges to regulatory policy making and raise fundamental questions about what regulatory oversight might look like, and to what it should attach.

The prospect of regulation

On the prospect of oversight by regulatory agencies, the crypto-industry continues to express its voice in a partisanly manner. There are those who see independence from oversight as a necessary expression of political freedom, or advocate that the industry should not be subjected to any oversight other than by the community participating in cryptos. Other participants in the industry wish to take advantage of the current situation by moving to the lowest commercially viable legal standard or jurisdiction.

There are also those who actively seek to be regulated as a means of being accepted into mainstream commercial activities and validated as a legitimate activity, and to foster the industry by directing it to applications benefitting society. Some see regulation as a competitive advantage over others who are ill-equipped, or inadequately funded, to cope with the anticipated burden of regulatory oversight. However, policy considerations and the usual patterns of legal and regulatory development can mean that wanting to be regulated is not always the same as being able to be regulated.

Regulatory agencies have to date primarily applied existing regulatory standards to the industry where they can. There is a general sense that this will not be enough to facilitate industry development while also dealing with the risk of fraud and consumer abuse. There are also real concerns that the anonymity provided by CCTech could be used by bad actors to further criminal purposes.

The primary hurdle for regulatory clarity is sometimes said to be the legacy system of laws, regulations and financial and commercial practices that have been established in a pre-CCTech era. Industry requests for regulators to specify the features that would determine which regulatory silo a crypto belongs to (money, security, futures contract, commodity, or other) oversimplifies the new context presented by CCTech and underestimate the related policy considerations.

Primary market activity thus remains governed by a singular question: is the crypto a security? This leaves CCTech developers cum promoters to resolve questions that lawyers and regulatory agencies cannot currently clearly define other than by reference to broad functional concepts, or narrow established categories, raising the danger of ex post regulation.

The development of taxonomies that seek to map cryptos onto existing securities laws as a means of assisting regulatory clarity has become a mini-industry. However, these often "solve" the problem without changing the underlying assumptions about how existing laws securities laws apply. As such they are essentially recursive and achieve very little. It is of course somewhat paradoxical to address something new by treating it as though it were something old.

In contrast to the situation in the primary market for securities, regulators in the UK and the U.S. have permitted a futures market to evolve around cryptocurrencies (Bitcoin, and recently Ether). The court in *CFTC v. McDonnell, et al*. (18-CV-361, 2018) has confirmed the oversight powers of the U.S. Commodity Futures Trading Commission ("CFTC") in this regard. Although many in the industry perceive regulatory oversight as abhorrent to the essence of CCTech, regulatory oversight of the futures market has enabled the development of financial products within an established regulated infrastructure that has facilitated the perception of cryptocurrencies as a valid asset class to gain exposure to. Importantly, it means that investors are brought within a context subject to safeguards imposed on regulated intermediaries.

Building blocks

Regulation of the financial services industry in the modern era is based around three primary choke points concerning products, venues and acts. These assume some form of intermediation via markets, brokers and advisers. Regulation has already had to adapt in response to technology that displaces human involvement, such as algorithmic trading and robo-advising, where sentience ceases to form part of the regulated act but rather is embedded in the coding that enables the act to be undertaken.

CCTech presents additional difficulties. There is a venue, but it may be only exist in a code supported on a network of participants. There is an act, but that may take place without intermediation other than the non-sentient operation of a code operated over a network in which the creator no longer has a role. There is a product, but there is a recognised lack of clarity as to how to characterise a crypto for the purposes of regulatory silos. CCTech enables venue, act and product to be collapsed into the operation of code via distributed networks, decentralised and dis-intermediated arrangements, and smart contracts.

The possibility of undertaking commercial activity on a decentralised, peer-to-peer basis represents a qualitatively different kind of issue for regulatory agencies. At some point, adaptability may be challenged to the extent that existing regulatory tools which have developed around centralised, intermediary-based systems may to some extent be rendered obsolete, raising questions as to the continued viability of existing legal silos and traditional choke points, and giving rise to policy concerns.

Even if basic problems were solved about which or whether a law applies to a crypto, or at what choke point to apply it, there remain problematic areas. Regulation proceeds on the basis that regulation is possible but CCTech does not, at the present point in time, provide some of the usual building blocks that enable the meaningful implementation of regulatory objectives.

This includes an assortment of investor protection and market integrity considerations, such as: integrity of ownership and integrity of transactions, issues related to account management including proof of ownership to public audit standards, custody and segregation, how record keeping is to be undertaken, how exchange regulation might work, the ability to assert market transparency and market abuse protections, how money laundering risks are to be addressed.

To this can be added technical issues that the industry is actively trying to solve, many of which potentially give rise to legal issues and have implications for investor protection and market integrity. These often require an appreciation of how the science and technology operate and their weak points such as how they might be gamed by bad actors. They include: the management of keys and wallets, the risk of consensus hijack, denial of service attacks, double spending, scalability, code governance controls and cyber security challenges.

Disclosure is another building block. Key disclosures might address: does the underlying code do what it is expected or promised to do, is the governance of the code appropriate (such as agreeing on roll-backs), has it been properly written so that it is free of bugs that might facilitate hacks or other problems, has the security protocols been properly implemented, is the crypto scalable to benefit from network effects. Not all codes are the same in this regard and coding errors have caused significant problems in the past, yet there are no established standards for audits of code writing.

Not all problems are adequately managed by merely releasing information. Positive action is sometimes required. This can take the form of an industry regulating itself via standards and best practices, but the industry is in its nascent stages in this regard. An area of development to watch is the standards being developed by the International Organisation for Standardisation in their ISO/TC 307 programme. Nine new projects concerned with blockchain and DLT are currently in their proposal or preparatory stages.

Resolving some of the above building blocks is therefore a precursor for effective, granular regulation to develop. Solutions are likely to come from the technology itself as it develops in response to regulatory expectations. This may serve to facilitate the development of regulatory technology, which presents opportunities for creating avenues within the underlying CCTech code for interactions between the actors involved in any crypto generation or exchange, any buyer of a crypto, and regulatory agencies.

One of the inherent difficulties of addressing the regulation question is the reality that the industry is in its early stages of maturation. Core concepts are still subject to significant debate, the potential technological implementations of the science remains in a discovery and development phase, and the prospects for commercial use cases of CCTech is still evolving. This makes the policy formation that leads to regulatory implementation difficult as these conditions increase the risk that regulations are made only to see the industry change under it, or regulations are made that capture the wrong family of acts – in either case the policy objectives are missed.

The dynamics that animate regulatory change are subject to two related overarching considerations: to what extent is meaningful regulation possible and, if it is, how and when should regulatory oversight be imposed? Regulatory intervention that is too early, too heavy, or misses the target runs the risk of slowing the growth of the industry and damaging the beneficial prospects it offers to commercial activity and society more generally.

The technology is also the end point

The present state of regulatory uncertainty creates risks to the industry itself. It increases the cost of industry development because raising capital in an uncertain legal environment gives rise to increased liability risk. To this can be added the risks (including attendant industry costs) already observed in traditional capital markets (primary and secondary) that include fraud, money laundering, theft, mis-disclosure, manipulative practices, internal control failures, misfeasance, and adequate custody and handling of money, or securities or other assets belonging to another.

Whatever regulatory controls might be put in place, the reality is that the nature of CCTech presents a fundamental obstacle to oversight control because of the possibility - and consequences - of an alternative means of undertaking commerce on Internet-based networks that does not require the involvement of a regulated financial institution that intermediates transactions.

The intractable problem created by CCTech is how to bring cryptos within an appropriate oversight mechanism given its particular technological capability to subvert – unmeasured oversight control runs the risk of achieving the opposite effect of driving activity further out of sight. The proposal by the United States Treasury's Office of Foreign Assets Control ("OFAC") that it may add digital wallet addresses to its SDN List was criticised for just that. This reflects the anarchic potential of CCTech that is crucial for regulators to fully grasp if regulation is to be successfully developed. Regulatory agencies may need to look for ways of bringing oversight to the industry by using strategies different to those previously employed.

Actors in the industry seeking to be regulated are doing so for a number of commercial reasons including validation and legitimacy, the usual assurances provided to the market by regulatory oversight, industry risk reduction, and access to a larger pool of capital. It is proposed that these reasons can be engaged to make regulation a desirable option.

In short, the best way to establish regulation may be to make it attractive. That may not be a regulatory end-point but a point from which regulators can begin to better work with the industry. For that dynamic to work, it is essential that oversight controls do not undermine the opportunities that cryptos offer to new ways of engaging in commercial activity. Regulations must be based on outcomes that are independent of specific technologies and activities, such as fair disclosure, industry standards, and accountability for wrongdoing. Care must be taken that oversight controls do not to operate as anti-competitive tools.

The range of relations that CCTech can possibly create, and the behaviours in the market once they are created, are at once simulacra of human commerce and a potential further development of it. It remains to be seen whether the current trajectory of regulatory thought and action is working toward supporting the efficient allocation of risk and industry development, wherein capital finds projects that offer, and have a reasonable prospect of delivering, economic and social improvement.

For a more in-depth analysis, see "Regulating Cryptographic Consensus Technology: Oxymoron or Necessity?", available from the author's page at SSRN.com.■

如何監管方塊鏈及其他共識驅動密碼技術？

作者: Syren Johnstone，法學碩士（合規和監管）課程執行主任，*香港大學法律學院*

密碼貨幣／方塊鏈／DLT產業的一些業內人士積極要求當局對該產業進行監管，但從政策考慮及法律和監管發展的通常模式來看，願意接受監管與是否能夠被監管經常是兩碼子事。

本文探討導致一級市場和二級市場存在監管困難的技術層面，但它同時可讓產業在不受詐騙及濫用，或被利用作清洗黑錢和其他犯罪目的情況下得以發展。在結論中，本文提出監管者對這項新科技應當採取的政策方向。

科技是起點

Tim May在1988年作出了以下的著名論述：「今天的電腦科技將可使個人及團體以完全匿名的方式進行相互溝通和互動。」人與人之間可以在完全不知曉對方的真實姓名、法律身份或其他資料的情況下進行訊息交流、業務往來及商議電子合同。在當今正在開發的數碼生態系統中，這已經成為現實，而它是以密碼安全共識技術作為基礎，從而使區塊鏈及分佈式分類帳技術應用程式得以發揮作用。

密碼安全共識技術為商業活動提供不同質量界限，並為現今商業運作提供新途徑，　及提升效率和開創商業活動的新類型。自從電子現金的第一個點對點版本於2009年1月3日啟用後（比特幣），接著再有其他可供使用或作為證券用途的加密貨幣和數碼代幣（參看2018年3月號《香港律師》所登載的《ICO功能型代幣以及與證券法的關聯性》文章）及智能合同（以下合稱「密碼貨幣」）的出現。

產業增長使開發商更大規模進入受高度監管的公共資本市場，而密碼貨幣交易促使二級市場興起，這對監管機構在如何適用現行法規方面構成重大挑戰。

由於密碼安全共識技術的發展仍然處於轉型階段，使得建立可持續的監管途徑變得複雜，以及為監管政策的制定帶來新挑戰，　並產生監管機構應如何進行監督及誰是監管對象等基本問題。

監管前景

在監管機構的監督方面，密碼貨幣的業者持續表達各自意見。有些人希望能獨立自主，不受任何監管，以呈現政治自由風尚；有些人認為只應接受業內群體監督；而其他人則認為應利用現況，在可行的商業條件下，接受最低程度的法律標準和管轄。

此外，也有人認為應該積極尋求受當局監管，作為獲許參與主流商業活動及成為認可活動的一個途徑，並藉著將它引向為社會帶來裨益的應用而推動該產業增長。一些人認為與那些面對未來的監管負擔，但條件和資金仍不充足的企業比較，接受監管可以讓他們在競爭上享有優勢。然而，從政策考慮及法律和監

管發展的通常模式來看，願意接受監管與是否能夠被監管經常是兩碼子事。

監管機構目前只能在可行情況下，對該產業適用現行的監管準則。一般看法是，由於需要應付詐騙及被消費者濫用的風險，因此它並不足以有效促進該產業的發展。此外，也有人認為，密碼安全共識技術的匿名運作方式可被壞分子利用作犯罪用途。

一些人士指出，主要對明確性構成妨礙的，是在密碼安全共識技術時代之前建立的傳統法規、金融和商業運作制度。該產業要求監管機構給它們指明某一密碼貨幣應具有甚麼特性，以決定它是屬於哪一個監管範疇（現金、證券、期貨合約、商品），這是過度簡化密碼安全共識技術所面對的情況及低估了有關的政策考慮。

因此，主要市場活動面對的唯一問題依然是：加密貨幣是否屬於證券的一種？這讓密碼安全共識技術的開發者及推廣者需要解決一些問題，而這些問題是律師和監管機構除了運用廣泛的功能概念或狹窄的已確立類別，目前仍然不能對其作出清晰界定的問題，因而帶來事後監管的風險。

試圖將現行證券法施加於密碼貨幣，作為提升監管的明確性的方法，其相關的分類學已發展成為一個微型產業。然而，它通常只能「解決」問題，但無法改變現行證券法如何適用的相關假設。因此，它們只是不斷周而復始，但最終不能取得重大成果。事實上，將一些新興事物當作舊東西來處理，本身便是自相矛盾。

與一級證券市場相比，英國及美國的監管機構已批准成立密碼貨幣期貨市場（比特幣及近期的以太幣）。法庭在*CFTC v. McDonnell, et al.* (18-CV-361, 2018)一案中，確認美國商品期貨交易委員會在這方面享有監督權。雖然該產業有許多人認為監管機構的監督與密碼安全共識技術的本質相互抵觸，但它可以促進在已建立的受監管基礎設施中的金融產品開發，並促使更多人認同密碼貨幣是一個有效的資產類別。但更為重要的是，它意味著投資者從當局對受監管中介人所實施的監管中獲得保障。

designed by Freepik

基石

現代金融服務業的監管主要是以三項因素作基石，即：產品、場地和行為，而後兩項因素是假定有某種中介形式通過市場、經紀及顧問來形成。然而，現代監管必須追上該等排除人為參與的科技發展（例如：運算交易及機器人顧問），將感知去除，不再成為受監管行為的一部分，並將其植入促使作出該等行為的編碼程序中。

密碼安全共識技術亦帶來了一些額外困難，因為：雖然有場地，但它只存在於一個由參與者網絡所支援的密碼中；雖然有行為，但此等行為是在沒有中介的情況下作出，那是由一個密碼，在其創設者並無扮演任何角色的網絡中，進行沒有感知的操作；雖然有產品，但在如何就監管範疇確定某一密碼貨幣的特性方面缺乏明確性。因此，密碼安全共識技術使場地、行為和產品結合成為一種通過分佈式網絡、分散性和去除中介的安排、智能合同等而進行的密碼操作。

面對分散式和點對點基礎進行商業活動的可能性，監管機構須面對性質上截然不同的問題。到了某一個階段，它的適用性將會受到挑戰，原因是從集中和中介制度發展出來的現有監管工具已過時，並產生現行法律範疇及傳統關鍵因素是否繼續有效的問題，亦同時帶來對政策的關注。

即使對於：有哪些法律適用於或某項法律是否適用於密碼貨幣，以及，在哪一個節點運用它等各項基本問題獲得解決，但當中仍然存在未能解決的問題。監管的進行，是建基於有可能對有關情

況進行監管，但在現階段，密碼安全共識技術並未能有效達到監管目的。

這包括對投資者的保障及市場健全等各項考慮因素，例如：擁有權及交易的建全性、與帳戶管理有關的問題，包括就擁有權作出證明並達至公開審計的標準、保管及隔離、如何保存紀錄、如何實施交易方面的監管規則、堅持市場透明度及防止市場被濫用的能力、以及如何處理清洗黑錢等問題。

此外，在這方面還需要考慮的，是該產業正在積極嘗試解決的技術性問題，而它們當中有許多導致法律問題的產生，並對投資者的保障和市場健全造成影響。這通常需要我們了解相關的科學及技術如何運作，以及它們的弱點，例如它們會如何被壞份子利用，這包括：鑰匙及錢包管理、共識駭客的風險、阻斷服務攻擊、重複花用、可測量性、密碼管治監控、網絡安全挑戰等。

資料披露是另一個重要基礎，而主要的資料披露可針對以下情況：相關密碼是否能夠發揮的作用、有關的密碼管治是否適當（例如在還原方面達成協議）、密碼編寫是否妥當，沒有任何病毒會協助駭客或產生其他問題、安全協定是否妥實施、該密碼貨幣是否與網絡效應的得益相符。雖然所有密碼在這方面都相同，但密碼編寫的錯誤可以導致重大問題出現，但目前卻沒有任何已確立的標準來審核密碼的編寫。

並非所有問題都可以藉發放資料而得到充分處理，有時候確實需要採取積極行動，並可透過準則及最佳常規來對該行業自身進行監管，但問題是這項產業正處於它的萌芽階段。一個需要關注的發展範疇，是國際標準化組織在其ISO/TC 307計劃中正在制定的準則。現時在其提議和預備階段中，共有九個與區塊鏈及DLT有關的新項目。

因此，解決上述基本問題的方法，是為有效和完備的法規制定先導辦法。然而，解決問題的方法經常是來自科技本身， 因為它的發展是為了對監管期望作出回應，而這將有助促進監管性技術的發展，並同時在與密碼貨幣世代或交易的參與者、密碼貨幣賣家、監管機構之間的互動有關的密碼安全共識技術密碼方面，帶來創造途徑的機遇。

處理該監管問題的其中一個內在困難，是該產業正處於初創時期。它的核心概念仍然被激烈爭論，這門科學的潛在技術實施，仍然處於發現和開發時期，而密碼安全共識技術在商業上的運作亦可能仍在發展階段，這使得為了實施監管而進行的政策制定面對一定困難，因為該等情況會使風險增加，亦即是所作出的監管，只能看到該產業在其下發生的改變，又或是該等監管是錯誤地以其他行為作對象—而這兩種情況都會導致政策目標失焦。

推動監管改革的動力受制於兩項重要考慮因素：有效的監管是在多大的可能範圍內實施，以及，該等監管應如何以及在何時進行？過早、太繁苛、或失去焦點的監管介入，會令產業的增長減慢，並給為商業活動及社會整體提供的有利前景帶來損害。

技術也是終點

目前的監管不確定性情況為該產業帶來了風險。由於需要在不確定的法律環境中集資，導致法律責任風險上升，因此增加了產業開發成本。除此以外，該產業也需要面對傳統資本市場（一級及次級市場）的風險（包括隨之而來的產業成本），當中包括詐騙、清洗黑錢、盜竊、錯誤資料披露、操控行為、內部管控失效、不當行為、充分監管和處理屬於其他人士的款項或證券等等。

無論是採取什麼監管措施，實際的情況是，密碼安全共識技術的性質會為該等監管帶來基本障礙，因它可以提供另類途徑，使得人們可以在以互聯網為基礎的網絡上進行商業活動，而無需有任何獲信任的金融機構參與，作為有關交易的中介人。

與密碼安全共識技術有關的問題，是如何將它置於適當的監管機制之下。有鑑於它獨特的技術顛覆能力—無法量度的監管控制會帶來適得其反的結果，使有關的活動進一步離開視線範圍。美國海外資產控制辦公室（「OFAC」)建議在其SDN 清單中加入數碼錢包地址，正是為此緣故而被批評。這反映了密碼安全共識技術的無政府狀態潛力，因此若要成功建立監管，監管機構便必須充分掌握有關狀況—監管機構可能需要尋找方法和運用與過往不同的策略，從而將該產業置於其監管之下。

尋求接受監管的業內人士是基於若干商業上的原因而有此意願（包括有效性和合法性）、監管機構所作的監督為市場提供的可靠保證、產業風險的降低、能夠有更多途徑取得資本等等。有意見認為，此等原因可促使監管成為一個獲大家接納的選項。

簡而言之，建立監管的最有效途徑，是使它變得具有吸引力，而這是讓監管者與該產業能夠更有效協作的一個起點而非終點。要有效地將其付諸實行，所作出的監管控制，不能損害密碼貨幣所帶來的機遇—就是提供參與商業活動的新途徑。該等監管必須基於特定科技及活動以外的結果，例如：公平披露、行業準則、對不當行為問責等。另外必須注意的是，所實施的監管控制不能成為反競爭工具。

密碼安全共識技術所可能建立的一系列關係，以及一旦建立後所展現的市場行為，便馬上有如人們的商業活動一般 ，並具有進一步發展的潛能。現行的監管思維和行動是否能夠有助風險的有效分擔及該產業的發展，從而使資本得以投入能促進經濟和社會進步的項目中，我們還須拭目以待。

如欲細閱更深入的分析，請登錄作者的網站 – SSRN.com閱讀“Regulating Cryptographic Consensus Technology: Oxymoron or Necessity?”全文。 ■