REGULATING CRYPTOGRAPHIC CONSENSUS TECHNOLOGY:
OXYMORON OR NECESSITY?

Syren Johnstone*

Abstract**

This paper examines the dynamics affecting access to highly regulated public capital markets by developers of the technology underpinning blockchain, distributed ledger technology and similar. 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 criminal use. Establishing a sustainable regulatory approach is complicated by features of the technology 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.

Participants within some segments of the industry actively invite regulatory oversight and voluntarily adopt best practices that go beyond their legal obligations. 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. Other participants in the industry either wish to take advantage of the current situation by moving to the lowest commercially viable legal standard or jurisdiction, or advocate that the industry should not be subjected to any regulatory oversight other than by the community participating in cryptos.

After a discussion of the relationship between technology, capital formation and the delivery of social benefits, this paper discusses how the technology intersects with regulatory policy making. It explores the potential uses and dangers of attempts to understand the technology via taxonomies, and suggests that an approach based more closely on the underlying technology could assist policy development. The issues within the industry itself that impact on the ability to regulate it are considered. The building blocks essential for industry maturation in the financial sector and for meaningful, comprehensive regulation to be imposed are discussed. Whether the current trajectory of regulatory thought and action on cryptos is working toward supporting the efficient allocation of risk and industry development is considered.

It is argued that the reality of being able to engage in anonymous yet secure commerce, as a result of scientific breakthroughs, is a significant game-changer that requires regulators to adopt different approaches from that taken previously. It is suggested that solutions can and will be found within the technology itself.

---

* Executive Director of the LLM (Compliance & Regulation) Programme, Faculty of Law, University of Hong Kong; Fellow, Asian Institute of International Financial Law; Solicitor (England & Wales and Hong Kong); Director, Keel Consulting.

** This paper is an independent research study supported by the OAX Foundation Limited. The author would like to thank for their assistance David Tee, Paul Li, Pindar Wong, Tony Lai, Enuma Technologies, James Greaves, Glyph ID, Michael Lardelli, and Kim Larkin. The views expressed and any errors remain solely those of the author.
Contents

1 Introduction 3
   1.1 The initial hurdle 3
   1.2 Structure of this paper 5
   1.3 A note on terminology 6

2 Core concepts: tasks and opportunities 6
   2.1 A consensus mechanism 7
   2.2 Capital investment 8
   2.3 The opportunity to reshape commercial activity 9
   2.4 The ecosystem effect 11

3 Regulatory challenges and responses 12
   3.1 Treatment under existing laws 12
   3.2 Taxonomies and their uses 14
   3.3 Where regulators stand 17
   3.4 Understanding the regulator’s perspective 18
   3.5 Impetus for regulatory development 20
   3.6 Looking backwards, looking forward 23

4 Conundrums in a developing technology 25
   4.1 Standards 25
   4.2 Immutability - *codicem meum pactum* 27
   4.3 Immutability – code governance 28
   4.4 Technical issues 30
   4.5 Development of new classes of financial product 32

5 Evolution of oversight control 34
   5.1 Policy development 34
   5.2 Restriction and possibility 36
   5.3 Looking sideways, looking forward 39
1. INTRODUCTION

Cryptocurrencies, security tokens, utility tokens, and similar ("cryptos") are all based on cryptographically secure consensus technology ("CCTech") such as blockchain and distributed ledger technology ("DLT"). They have attracted increasing amounts of capital, and regulatory attention, as the market develops its assessment of the possibilities and risks they present. The uncertainties that have enveloped the development of CCTech and the space in the public capital market usually occupied by regulated financial services, products and venues shows few signs of being clarified.

The industry continues to express its voice in a partisan manner following the recognition of the possibility and consequences of crypto-anarchy around the early 1980s, which arose as a result of innovative science and technology making anonymous yet secure commerce possible. There are those who see independence from government 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. There are those who actively seek to be regulated as a means of being accepted into mainstream commercial activities, validated as a legitimate activity, and to foster the industry by directing it to applications benefitting society. There are also those who see regulation as a competitive advantage over others who are ill-equipped, or inadequately funded, to cope with the anticipated burden of regulatory oversight.

Different regulatory agencies and persons attached thereto have made widely varying statements as to the potential impact of CCTech on the operation of financial markets, on the real economy, and on society at large. While a generally accepted consensus has emerged that the technology is capable of bringing benefits to human society, there is also recognition that it presents numerous potential risks. There are different views as to whether CCTech should be subject to oversight and, if so, on what basis. This is paired with a keen awareness that introducing regulation too early or improperly targeted could work to damage the burgeoning industry. Cutting across this diversity of opinion is concern that the anonymity provided by CCTech could be used by bad actors to further criminal purposes and that mis-directed regulation could drive the technology, and bad actors, into the shadows of society.

A primary cause of the conundrum is the legacy system of laws, regulations and financial and commercial practices that have been established in a pre-CCTech era. There are those who wish to apply that legacy template to this new industry, often seeking to categorize cryptos based on existing legal classifications, such as whether a crypto is money, a security, a futures contract a commodity, or something else akin to a license, franchise or membership. Others take the view that the same laws require a new interpretation, by the courts if not by lawmakers. Still others consider that the characteristics of cryptos are sufficiently special that meaningful regulation could only come about through the introduction of new, more tailored laws. Finally, there are those who argue that regulation has no place in the industry, a stance that is unlikely in practice to survive intact if CCTech is to take its place alongside other established means of commerce.

1.1 The initial hurdle

One of the difficulties in bringing this science to the public, whether raising development capital or via engagement in commercial applications, is the reality that it is at this stage difficult for the layperson to grasp or assess the full complexity of CCTech. The physicist Robert Oppenheimer once remarked, “the deep things in physics ... are not things you can tell about unless you are talking to someone who has lived a

1 Section 1.3 below defines various terms as used in this paper.
long time acquiring the tradition”. The discoveries of the science underlying CCTech are similarly difficult to assimilate. Nevertheless, in recent years a large number of pundits on CCTech have emerged, though few truly possess a 360 degree understanding from the roots in mathematics, cryptography and computer science to its potential uses and implications in the economy and all the attendant complexities of modern human society ranging from legal relations to tax, accounts and audit, and the operation of the financial system. This paper seeks to steer a course through some of the deeper things that interact with regulatory considerations.

As such, the appreciation of many elements of the science can only be apprehended by analogies or broad concepts: cryptography is at best understood as the ability to create particularly difficult puzzles that could only be solved by, for example, the advent of quantum computing; issues in computer science such as the development of Byzantine fault tolerance algorithms for networked computers, such as in distributed computer networks, are understood broadly as mathematical solutions to the emergence of arbitrary errors as a result of software errors or malicious attacks. Yet while these concepts represent relatively basic working tools for the technology specialist, if the reader has now begun to feel lost, the point has been adequately made: the reader has joined a large club, many members of which are not deterred from engaging in the crypto space.

Assuming there is a feasible commercial use for a particular type of CCTech, such as blockchain, highly technical issues must be dealt with “under the hood” by experts – where they are not properly implemented the proposed human-facing functionality of the technology may fail. Technical complexity has in not a few cases led to the technology wagging the business model in a manner similar to the dot-com era in which businesses sought to increase their valuation simply by changing their name and posting a website without any discernable development in the business model itself. The same is happening today – “blockchain” adds value. This has resulted in blockchain sometimes being used in a way that “over-techs” the business solution. This has not occurred without a measure of vandalism to the reputation of legitimate developments of CCTech.

When a typical investor considers an initial coin offering (“ICO”), a true knowledge gap will frequently exist that places the investor at a significant information disadvantage. This raises the risk that an unfair bargain is being struck. The greater the knowledge gap, the greater is the reliance that is placed on the completeness and accuracy of representations made in white papers and any offering document. Knowledge gaps can be resolved in different ways. Disclosure is one method of consumer protection but whether disclosure alone provides adequate protection to the average investor in an ICO or an exchange traded crypto is open to question. Moreover, disclosure is not a panacea as significant reliance is nevertheless placed on the correct implementation of the technology – as discussed in Section 4.1, coding errors can give rise to significant

---

3 By way of disclosure, the present author’s perspective is that of a lawyer having a career in corporate finance and securities regulation, both as a private practice solicitor and in regulated senior management positions within the investment banking industry, with postgraduate qualifications covering neuroscience and computer programming, and having participated in the Fintech Advisory Group of the Securities and Futures Commission of Hong Kong since its foundation in 2016.
difficulties. Some problems are not adequately solved by merely releasing information and positive regulatory action is sometimes needed.\(^5\)

One means of addressing significant knowledge gaps is to establish standards and/or institutionalize the role of the expert. This is the essence of an auditor who applies standards established by a recognized body. In the Hong Kong market for companies seeking a listing by way of an initial public offering, the regulators require the engagement of a licensed sponsor whose essential role is to provide assurance to the market on the quality of the disclosures. Other markets use underwriters that bear commercial and legal risk. When The Stock Exchange of Hong Kong recently introduced new listing rules allowing large, non-profit making biotech companies to list, they also established a biotech advisory panel comprised of industry experts to advise the Exchange on various aspects of the company’s undertaking including its commercial feasibility and attendant risks.\(^6\) This also facilitates compliance with the applicable disclosure requirements, thus serving to reduce information asymmetries in the primary market. Section 4.1 further discusses the topic of experts and standards.

The adequacy of disclosure and standards are a subset of a wider collection of concerns, including: protecting consumers from misleading and deceptive practices, clarifying the nature of the legal relationships embodied in generating or owning a crypto and the subsequent development of the underlying CCTech, the applicability of industry specific laws such as those governing financial markets, the availability of cross border controls, preventing criminals from using the technology to assist their undertaking, the existence of realistic enforcement mechanisms, and so on.

1.2 Structure of this paper

This paper examines the current dynamic of these views and problems. It considers the elements relevant to moving from the risks of cryptos operating in a grey area of uncertainty, toward more acceptable levels of clarity. It is divided into the following sections after this Introduction.

Section 2 introduces core concepts and discusses the relationships between the technology, capital formation and the delivery of social benefits.

Section 3 is concerned with how CCTech intersects with regulatory policy making. It considers the problem that wanting to be regulated is not the same as being able to be regulated. Actors in the CCTech industry need to develop a deeper appreciation of the context in which regulatory agencies are operating, such as their ambit of legal power, their regulatory objectives, the means by which they are able to regulate or normally do so, and the policy considerations that underlie any proposal to develop new regulation or apply existing regulation in a new way. Section 3 is relevant to the question of whether the current trajectory of regulatory thought and action is working toward supporting the efficient allocation of risk.

Section 4 is concerned with the industry in its present state of development and issues that impact on its ability to be regulated. Features of CCTech, and related issues being debated in the industry, can pose challenges to proposals to regulate it, amongst which includes the lack of some of the building blocks necessary for meaningful, comprehensive regulation to be imposed. As an industry engaged in the technological application of scientific breakthroughs to commercial solutions, it is in a state of rapid change, which in itself poses unique challenges to regulation.

\(^5\) For an interesting view on this, see Amitai Etzioni, ”Transparency Is Overrated”, Jan 13, 2014, available at https://www.theatlantic.com/politics/archive/2014/01/transparency-is-overrated/282990/

Section 5 reviews the process of policy development and the challenges policy makers, and regulatory agencies, are subject to when confronting change. It concludes with a proposal that control oversight must be installed carefully, and in a manner that makes it desirable for the industry to subject itself to oversight.

1.3 A note on terminology

Words and phrases such as blockchain, DLT, cryptocurrency, coins and tokens are often used interchangeably, loosely, wrongly, or with embedded assumptions as to their nature for technical, legal, regulatory, tax, accounting, functional, economic or political purposes. Accordingly, to avoid confusion, this paper adopts the following uses:

"cryptographic consensus technology" or "CCTech" - a computer-based cryptographically secure mechanism that operates to establish a consensus among participants in the mechanism;

"crypto" - any iteration of CCTech that generates a token or cryptocurrency;

"token" - a digitally written entry (i.e., instance) on a computer code implementing CCTech that is able to be controlled, via a system of one or more keys, in accordance with the set of functions the computer code provides or permits (but excluding any token that is a cryptocurrency);

"cryptocurrency" - a type of token that serves no purpose other than a peer-to-peer version of electronic cash and provides no functionality other than the ability to generate a new unique key that represents ownership qua control over the digitally written entry; and

"promoter" – the person(s) ultimately responsible for procuring the deployment of a crypto into the market and any accompanying white paper or similar documentation concerning the crypto.7

For reasons that will become clear later in this paper, these definitions strive to remain close to the science that enables the technology.

2. CORE CONCEPTS: TASKS AND OPPORTUNITIES

The rapid rise of capital that CCTech has attracted has been nothing short of staggering. The working proof of the technology in Bitcoin has led to possibilities for the technology in an ever-widening range of potential commercial applications. Not all applications are bona fides and this has inevitably led to capital being directed to projects of dubious quality and intent. This has to some extent been a distraction from the technology, which is undergoing an ever-deepening technical complexity as it responds to implementation demands. Against this backdrop, significant regulatory concerns have emerged.

This Section reviews the essential elements of CCTech and provides an overview of the opportunities it presents to reshape commercial activity.

---

7 The market commonly refers to “issuers” of cryptos, which is a misleading analogy to a company that issues securities. Cryptos are not “issued” as such but are generated. The promoter concept is statutorily recognized in securities laws in the United States Securities Act of 1933, Hong Kong’s prospectus law (Companies (Winding up and Miscellaneous Provisions) Ordinance Cap. 32), and the UK’s Financial Services and Markets Act 2000.
2.1 A consensus mechanism

On the 3rd of January 2009, the first Bitcoins were created. A peer-to-peer version of electronic cash, Bitcoins were based on a paper published three months earlier, and important conceptual papers that preceded it, that envisaged an alternative means of undertaking commerce on the Internet that did not require the involvement of a trusted financial institution that intermediated the transaction.

CCTech has been recognized as a theoretical concept for at least a decade prior to Tim May’s 1988 statement:

“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.”

This was more specifically recognized by Wei Dai’s posting a decade later, which contemplated not only the creation and transfer of money but also the effecting of contracts and, upon a dispute, arbitration and subsequent enforced performance or reparation.

Bitcoin enabled the creation of a unique digital asset – dubbed electronic coins - that could be securely transferred between two parties who did not need to know each other. It is not necessary to know the identity of the other person because a set of operations written in immutable computer code and the mathematical proof that the rules of the code have been satisfied replace the need for trust in the counterparty; hence the concept of “trustless trust”. However, as discussed in Sections 4.2 and 4.3, immutability is not without its own set of complex issues. The computing science behind this is complex but the concept is not – early societies typically used as a medium of exchange some form of commodity that required specialized effort to make or obtain. However, unlike commodities of exchange, all transactions in cryptos are recorded and visible to everyone who has access to the network because of the chain of cryptographically secure digital signatures embedded in each crypto.

The design of different consensus mechanisms vary along a number of technical parameters. Whereas consensus is a function, blockchain and implementations of it (such as Bitcoin) are products that represent one of the many possible iterations of computational law. In other words, blockchain is a product that is one means of enabling a consensus function. As with the kinds of products we are used to interacting with, such as for our transportation and communication needs, design affects utility and adaptability over time to new demands and circumstances. In a digital consensus-based medium, key issues include the speed and cost of confirming transactions, and the ability to maintain acceptable performance as more and more participants engage with the mechanism (usually referred to as scalability). Many of these issues turn on highly complex issues, such as cryptography. A simple demonstration is the following:

---

10 As such, it is fundamentally different from electronic money (or “e-money”) which is a term used to refer to fiat currency (such as USD) that is available for transfer via a regulated electronic payment system.
well-known example: "Uijt jt bo fybnqmf". This English language sentence is unintelligible until one discovers (or is given) the key.\textsuperscript{13} Sitting at the crossroads of mathematics and computer science, specialized knowledge is required to appreciate that the difficulty of solving a cryptographic problem is not always correlated with the number of network participants and amount of computing power required to solve it, and significant efforts are going into finding better cryptographic puzzles that are secure yet better enable scalability.

While these and similar issues are discussed further below, for now it can be observed that the ability to improve on design issues will depend on not only solving technical hurdles, but also establishing commercial viability. This requires the investment of capital.

2.2 Capital investment

CCTech has attracted significant capital investment\textsuperscript{14} as a result of the recognition that it is capable of a much wider range of commercial applications than peer-to-peer versions of electronic cash. Legal clarity over the treatment of cryptos, and the ICOs that raise the necessary funding capital, remains wanting. Yet such clarity is an essential component to facilitate the efficient allocation of risk capital.

The raising of capital via ICOs\textsuperscript{15} and the legal issues that surround them, has in various ways been a distraction from the technology insofar as it involves elements that fall within the statutory responsibilities of regulatory agencies: there is an offer to the public; representations (disclosures) are made, often without the same level of transparency experienced in traditional markets; capital is committed and is exposed to risk; a promise or expectation of gain is sometimes involved; the efforts of others may be involved in generating a return on the capital. In short, securities laws may be invoked, often based on a functional test of “securities” for the purposes of investment laws – the Howey test in the United States,\textsuperscript{16} or collective investment schemes in Hong Kong\textsuperscript{17} and the UK.\textsuperscript{18}

Cryptos and ICOs should be clearly differentiated – the former strictly concerns the implementation of technology, the latter is primarily\textsuperscript{19} a method of fundraising. This distinction is well illustrated by Mainland China where ICOs are banned but blockchain and DLT are nevertheless being developed based on capital raised from outside the public capital market.\textsuperscript{20} Heightened regulatory attention in the United States has

\textsuperscript{13}“This is an example.” Key: shift each original letter to the one alphabetically preceding it.
\textsuperscript{14}From around US$300 million during 2014 to 2016, to around US$7 billion in 2017. The first half of 2018 has already raised an amount of capital equal to or exceeding all previous years combined. However, data is inconsistent across websites. For example, Autonomous puts the 2018 number at $15 billion, whereas Icodata puts it closer to US$7 billion. See https://next.autonomous.com/ and www.icodata.com
\textsuperscript{15}Initial coin offerings.
\textsuperscript{16}Originally developed by the United States Supreme Court in SEC v. W.J. Howey Co. (328 U.S. 293 1946) and subsequently supported and developed in numerous cases thereafter. Defined in schedule 1 of the Securities and Futures Ordinance (cap. 571).
\textsuperscript{17}s. 253 Financial Services and Markets Act 2000.
\textsuperscript{18}“Primarily” and not “solely” because ICOs can be used as token generation events (TGE) without accompanying capital raising that distributes crypto-coins with an expectation that doing so will stimulate secondary market trading activity of the token and/or use of the token once the underlying system is functional.
\textsuperscript{20}In Mainland China, this is frequently though not exclusively Government sourced funding. For example, based on the Trusted Blockchain initiative of the China Academy of Information and Communications Technology (CAICT), a research body under the Ministry of Industry and Information Technology. Another example is ConsenSys being appointed by the Government of the Xiongan New Area – as reported by SCMP.com, “Xiongan calls in ConsenSys to bring blockchain technology to Xi Jinping’s dream city”, 23 July 2018.
caused technology developers accessing the United States market to lean toward a not dissimilar model as they are increasingly choosing private sales made via exemptions from securities laws or via venture capital rather than making a public offering which brings with it attendant legal risks. One such high profile example in recent times is Telegram Group Inc., which in 2018 reportedly scrapped plans for a very large public offering in favour of a private sale via an exemption from full compliance with United States securities laws.\textsuperscript{21} Such capital raising exercises can still be described as an ICO, although investors that do not fall into the relevant category (institutional/accredited/professional depending on the jurisdiction) are unable to participate. This has led to the concern that applying securities laws to ICOs “has created an environment where only the rich ... are able to get access to financial deals. The plebeians must stick to the lottery.”\textsuperscript{22} Section 3 discusses the regulatory considerations.

2.3 The opportunity to reshape commercial activity

As global society entered into the 19th century, it greatly benefitted from technological developments now taken for granted. The steam train, evolving out of the engineering product of coal-miners seeking to meet the demand for coal, quickly provided better, cheaper access to markets at greater distances than did its main competitors at that time, horse drawn carriages and canals. The train was thus both a disruptor of the way goods and people were transported, as well as disintermediating businesses that depended on the horse and canal building. More than that, the train also opened up new economic opportunities in the areas it reached, and transport accessibility continues in the modern era to be significantly related to the growth of labour force centres.\textsuperscript{23} It would probably be an overstatement to compare the development of CCTech with the development of transport, but the analogy is not an unreasonable one to draw as CCTech is providing new ways of undertaking existing commerce that promise efficiency gains, as well as new types of commercial activity.

Discussions of how CCTech might work to improve, and change, commerce often revolve around a distinction between cryptocurrencies, tokens and potential uses of DLT/blockchain. That distinction is not entirely helpful when one considers the underlying science of consensus mechanisms. As discussed in Section 3.2, taxonomies of cryptos need to be handled with care as their construction may impact on how development in the industry is regulated.

The primary distinction to make that is consistent with the science and that differentiates between different types of commercial application is the public/controlled/private distinction:

- **public cryptos** - anyone is able to join the Internet-based network running the crypto with read/write permission to contribute to the consensus mechanism enabling the processing of transactions. As such, they are squarely based on the concept of trustless trust as there is no prior relationship;

- **private cryptos** - access to the network is only provided on a permissioned basis, which usually implies some degree of trust between participants of the network. Private cryptos are typically used within an organization and accordingly are of less interest to this paper as they are unlikely to give rise to concerns in the public capital market;

---

\textsuperscript{21} Regulation D. Telegram has to date raised around US$1.7 billion privately.

\textsuperscript{22} Erik Voorhees, founder and chief executive officer of cryptocurrency exchange ShapeShift, see https://twitter.com/ErikVoorhees/status/991759831986982912

controlled (or consortium) cryptos - validation of transactions can only be undertaken by preselected parties with read/write access to the consensus mechanism (the element of control via permissioned nodes). Other persons, either the public or other specified persons, can then participate in reading or sending transactions. Controlled cryptos therefore share some features of public and private cryptos.

Although each of these types of consensus mechanisms may be based on a similar underlying technology, they give rise to different use cases.

Public cryptos allow new commercial economies to develop around them, particularly because of the significant potential for network effects between developers and users. As more users join the system, the value of the system increases, and this may lead to further developments of the system - the development of e-commerce sites such as eBay and Taobao are examples of the network effect. Achieving critical mass to initiate a network effect gives rise to another issue: whether the system is scalable, i.e., capable of handling much larger numbers. As discussed in Section 3.1, some tokens might be regarded as securities, however, to the extent they might be subject to valuation based on network effects they differ in important ways from securities that are not valued in this way.

Private cryptos do not have this feature but do enable cost savings and efficiencies in the recording, transmission and storage of data and may be suitable to a wide variety of uses. As such, they are more suitable for use by an organization, or a group of organizations that agree to manage data in a certain way. For example, a logistics blockchain that tracked product provenance would often be private, but if it was important that public end users of products needed to verify provenance – such as the production origin and certification of a medicine they are to use – a controlled crypto that gave limited permissions to, for example, hospitals or patients might be appropriate.

Controlled cryptos are typically deployed where multiple organizations are engaged in a common market involving the exchange of data. A strong use case for controlled cryptos is a consortium of banks competing on a trading network, and a number of stock exchanges including Nasdaq are exploring the technology. The Australian Stock Exchange has already announced it is moving its clearing and settlement systems to a controlled DLT-based crypto.24 This will enable post-trade verifications, which involve numerous parties, to be collapsed into pre-trade requirements, which promises reductions in the cost and time to confirm a transaction. The State of Delaware has also launched a crypto initiative that will bring greater clarity to records of shareholder ownership as well as the implications of regulatory filings under State laws, something that has at times been problematic.25 Other uses in the financial sector include regulatory reporting, KYC and AML applications, records management, the recording of obligations and their performance.

Out of these distinctions, other considerations arise. It illustrates that cryptocurrencies limited to the original concept of a peer-to-peer electronic coin mined in return for reward and subsequently exchanged, are to be distinguished from tokens intended to serve a wider range of potential commercial purposes. Nevertheless, tokens may take

on a tradeable value based on, *inter alia*, their perceived exchange value. For example: a token that provides access to a fixed amount of cloud storage for a fixed period of time would likely vary in price according to the supply/demand curve for cloud computing; a token that benefits from a network effect may increase in value. Public cryptos tend to suffer from a technical problem that operations on them (i.e. accessing whatever functionality it provides) tend to become slower as the user base expands, leading to the problem of scalability – this has been an increasing problem with Bitcoin (see the discussion in Section 4.4). The handling, storage and custody of private keys evidencing ownership or control is also problematic in a public crypto.

The extent to which a crypto impacts on the way a commercial activity is normally undertaken is usually referred to as disruption and disintermediation. A solution to a commercial need that uses CCTech may enable a more efficient or desirable way of undertaking that activity. It may also cut out (or reduce reliance on) actors from the usual way business is undertaken in the non-digital world. Think of what Uber did for licensed taxi drivers.

With disruption and disintermediation also come the circumvention of established controls – the particular focus of this paper being financial services, it means that activity based on CCTech which is servicing financial needs may take place outside traditional markets that are heavily regulated. This creates obvious risks not only to the immediate participants, but potentially also to the operation and integrity of the financial markets on which the wider economy depends. However, as discussed in Section 3, what characteristics of CCTech-based commerce ought to bring it within existing frameworks of regulation remains open to question, as does the related issue of whether existing regulations need to evolve or change in response to CCTech. The development of automated trading service (“ATS”) platforms that took advantage of the connectivity provided by the Internet disintermediated the human factor in important ways – this not only helped lower overall costs but also avoided the risk of brokers taking advantage of clients’ investing intentions. This reflected a shift of trust from human to machine, something that continues to expand in recent years. Regulators responded with rules concerning how such systems should be designed and operated, which provided clarity for their further responsible development.

### 2.4 The ecosystem effect

Knowledge that facilitates social development frequently gives rise to problems that require solutions, which in turn brings about the acquisition of further knowledge and technology. Each of the foregoing enables other developments that may draw on other sources of knowledge or experience. This is what has been referred to as a “nexus of forces”\(^{26}\) in the context of the development of the Internet being quickly followed by a matrix of technologies and product applications that feed off of each other - cloud computing, mobile computing, social media, data analytics, artificial intelligence, neural networks, machine learning, robo-advising, etc. CCTech depended on the development of the Internet, computer science and cryptography.

Such mutually facilitated development operates as a win-win network that draws in an ever-increasing number of possible species (acts and actors) to a digital ecosystem that becomes more viable, valuable, and transformational as it grows in size and complexity. In an ecosystem that remains open to competition, and progresses toward increased interoperability, a greater number of interconnections and interdependencies can also lead to potential transactional efficiencies and savings.

Because digital technologies that connect large groups of people enable new things to be done, this can move established players from competing on the basis of an established system of rules to competing for what is in effect a wholly new market with a different set of rules and business dynamics to what they are accustomed. Arguably, some cryptos represent a new asset class.\(^{27}\) Taken together, this presents challenges to laws and regulations developed in a pre-CCTech era, as discussed next.

### 3. REGULATORY CHALLENGES AND RESPONSES

How existing laws and regulations governing commercial activity apply to cryptos and the activity that surrounds them is currently the subject of much discussion within the industry, professional advisers to the industry, regulatory agencies and governments. It is essential, for both the industry and society, that consumers and the capital market are protected from abuse and that the proper allocation of risk capital to commercial activity is able to occur. CCTech is also providing new models of activity proximate to traditional financial services activities concerning venues, participants (such as intermediaries) and products already subject to laws governing securities, futures and commodities.

The struggle is to identify whether or how to regulate cryptos, what or who should be regulated, and to what extent should regulation be applied given that this is a developing technology in its early, diversification phase.

This Section reviews the issues that cryptos present to a legal system that has evolved at a time when CCTech did not exist. It considers the different attempts to develop taxonomies for cryptos, discusses the position of the regulators at the present point in time, and explores the factors that typically give rise to regulatory development. It concludes by considering to what extent looking backwards will assist finding forward-looking solutions.

#### 3.1 Treatment under existing laws

While no crypto is regarded as having legal tender status, the understanding of their status for the purposes of laws governing the securities, futures and commodities markets has been evolving.

In the primary market of new cryptos, up until the second half of 2017, many promoters considered the cryptos they developed and offered to the public to be outside the laws of any jurisdiction. Some had even stated in their whitepaper that the cryptos being issued are “not subject to any law”. Following actions by the SEC\(^ {28}\) in July and December 2017 in relation to the Slock.it and Munchee ICOs, it became clear that tapping the market for capital could be subject to securities laws in certain circumstances. This led to an era of promoters seeking “non security legal opinions” that their proposed crypto would not be subject to securities laws. However, providing such an opinion is difficult given the functional definition of securities used in the United States and in certain other jurisdictions such as Hong Kong and the UK.

In practice, it is easier for a lawyer to opine that a crypto is a security, as this permits the capital raising exercise to be undertaken via a relevant exemption from securities laws. Some whitepapers then started making affirmative statements to the effect that the crypto “is a security”. Of course, that requires the crypto to actually be a security – where it is not, the promoter may have misrepresented that the token is subject to the


\(^{28}\) United States Securities and Exchange Commission
protective regulatory oversight of the securities markets governed by laws and regulatory agencies.

Where a crypto is correctly treated as a security and is offered in accordance with prospectus laws (or relevant exemptions), this gives rise to other consequences. Intermediaries engaged in broking or advisory services in relation to the offer or placement may need to be registered or licensed, but conduct rules that apply to them may be difficult to comply with. An exchange could only handle the crypto if it was registered as an exchange or an ATS under applicable securities and exchange laws. There is also the risk that being treated as a security in one jurisdiction may give rise to difficulties in another jurisdiction that might not treat the crypto in the same way. The latter problem points to the importance of a common approach cross border and it has been argued that the law in the United States, Hong Kong and the UK do take a common approach in this regard.

In the secondary market, cryptocurrencies came under the regulatory spotlight much earlier. In 2013 the United States Financial Crimes Enforcement Network provided guidance to the effect that they may be subject to Federal registration requirements applying to parties engaged in virtual currency-related services. The CFTC has been of the view, at least since 2015, that cryptocurrencies are commodities as defined by the Commodities Exchange Act 1936 (“1936 Act”) and so subject to its enforcement powers, a view confirmed by the court in March 2018. In that case, the court found that virtual currencies are commodities “both in economic function and in the language of the statute” and as such fell within the definition in the 1936 Act of commodities, which includes “all other goods and articles … in which contracts for future delivery are presently or in the future dealt in.” This covers not only cryptocurrencies but also potentially other cryptos.

Although many in the crypto-community perceive regulatory oversight as abhorrent to the essence of CCTech, the CFTC’s oversight has led to benefits, enabling the development of financial products within an established regulated infrastructure. Importantly, this has facilitated the perception of cryptocurrencies as a valid asset class to trade, as further discussed in Section 4.5. In contrast, in the primary market for raising capital, very little headway has to date been made and activity is still preoccupied by a singular question: is the crypto a security? This leaves 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. Section 3.5 discusses a recent criminal case brought in the United States that is likely to explore this issue. The secondary market

---

29 For a discussion, see S Johnstone, “Requisites for development of a secondary market in cryptos”, forthcoming 2018
30 Securities Exchange Act 1934 in the United States; the SFO in Hong Kong; FSMA 2000 in the UK
32 United States Commodity Futures Trading Commission
34 CFTC v. McDonnell, et al., Case 1:18-cv-00361-JBW-RLM Document 29 Filed 03/06/18
35 Ibid., p. 3
36 Title 7 U.S.C. § 1(a)(9)
37 USA v. Maksim Zaslavskiy U.S. District Court, 17-CR-00647 (May, 2018)
context for cryptos and the regulatory options that might facilitate or hinder the market are discussed elsewhere.\(^{36}\)

### 3.2 Taxonomies and their uses

Systems that identify, describe and classify are based on \textit{a priori} constructs (i.e. ideas or theories) or purposes, which can change in response to new or corrected knowledge or new purposes. Consider for example the change experienced in biology following Charles Darwin’s classic work “The origin of species”, which shifted biological taxonomy from systems based on the shared morphology of organisms, to systems based on the genesis of organisms. A biologist might point out that while the former could assist understanding common functions that have led to the development of recurrent structures, information concerning shared and divergent origins and histories, such as responses to changes in the ecosystem, would be lost under a taxonomy based on morphology.

Similarly, when organising cryptos into a taxonomical system, questions that must be asked of the taxonomy include: what purpose is it intended to serve; does it provide information germane to that purpose; does the \textit{a priori} construct it is based on presuppose outcomes; and is it likely to be sustainable as “new species” emerge, i.e. cryptos that are based on developments in CCTech. In Section 1.3, some care was taken to define cryptos minimally, on the basis of the underlying science and its functional scope.

Consider the information that is provided by categorizing cryptos into the following categories: cryptocurrency, platform cryptos, utility tokens, security tokens, natural asset tokens, crypto-collectibles, crypto-fiat currencies and stablecoins.\(^{39}\) While possibly of use when building a commercial business model, it is arguably less a taxonomy than a descriptive list of purposes a crypto might serve. A more structured, hierarchical approach based on the technology and economics of cryptos use has been proposed in which the primary division is whether the crypto represents a programmable value able to be used freely, or some form of claim (on capital, a transformable/consumable or a store of value asset). The former category (general crypto assets) is further divided into those that are limited to peer-to-peer systems, as opposed to those that are platform dependent. The latter category (protocol assets) are divided into application tokens that do not lock value into the parent protocol, and side-chains that do.\(^{40}\) While this approach seeks to assist regulators promoting innovation, it does not speak the current regulatory language of the financial marketplace and as such requires interpolation.

The construction of modern securities regulation in common law countries has been significantly influenced by the approach in the United States, whose fundamental triumvirate of investment laws\(^{41}\) established in the 1930’s was formed around a taxonomy based on "securities”, “commodities” and “exchanges” that was part morphological (for example, the United States Securities Act of 1933 ("1933 Act") and 1936 Act contain a list of things regarded as securities or commodities) and part functional (such as the definition in the 1933 Act of “investment contract” with which

\(^{36}\) See S Johnstone,” Requisites for development of a secondary market in cryptos”, forthcoming 2018


\(^{40}\) Brave New Coin, “A General Taxonomy for Cryptographic Assets” available at www.bravenewcoin.com

\(^{41}\) Securities Act 1933, Securities Exchange Act 1934 and Commodities Exchange Act 1936. One might also add the Glass-Steaagall Act 1932 and the Investment Company Act 1940, though those Acts are less germane to the present topic.
the court was concerned in the influential Howey case). The axiom that empowered it was that, for financial markets to serve their proper function in society, they must be protected through regulation, and this was well supported following the excesses of the 1920s that led to the Great Depression. However, the characteristics of securities are not static over time.

Other taxonomies do use the language of law based on use-case, quantitative or risk based scenarios. For example, the approach taken by the Monetary Authority of Singapore is to put cryptos into three categories: utility tokens, payment tokens and securities. This basic taxonomy has been recast in a similar approach that seeks to understand and develop governance frameworks and codes of conduct with a view to mitigating risk; those used as a voucher that can be redeemed to obtain something else; those that operate purely as a means of payment (cryptocurrency as defined herein); and those used as a financial instrument or asset. Cryptos have also been classified with a view to bringing the same benefits to consumer protection as already accrue under current securities (or other) laws via the oversight of promoters and their disclosures, and intermediaries and their practices, for example: those that represent donation crowdfunding; those that represent rewards-based crowdfunding; those that are currency in nature; and those that amount to some form of equity or investment. Expressed broadly, each of these are dividing cryptos into payment currency, securities, or something else.

In the context of the regulatory question, each of these types of approaches may be interrogated on the basis of their value to policy making, or whether they are rooted in a need for clarity based on existing laws only.

First, while a particular taxonomy might seek to describe something intrinsic to a crypto, intended use and actual use may diverge, causing the taxonomy to break down. For example, given the high degree of transferability of cryptos, one that is classified according to its design as a voucher or utility token may in fact function entirely differently once issued, whether or not intentionally and could perform more like an asset traded for profit, or used as a commodity of exchange based on the embedded expended effort.

Second, the convenience of piggybacking on existing legal and regulatory concepts may constrain the ability to find the best regulatory approach to cryptos because it is essentially based on pre-existing conditions. To that extent it may also constrain the options for the development of commerce - as discussed in Sections 3.4 and 5.1, piggybacking is subject to limitations in relation to decentralized commercial activity. Proposals to leverage off of the crowdfunding experience may be potentially useful as regards establishing familiarity but to the extent the characteristics of ICOs of cryptos

---

42 The United States courts have for some decades been grappling with literalist versus functionalist approaches to the language of the 1933 Act. The view that has in general prevailed is the latter, which requires consideration of the function of an arrangement as more important than its form.
43 S Johnstone et al “Utility Tokens in the Eyes of Securities Law – Toward a Common Approach to a Public Capital Market”, forthcoming, 2018. For example, in the United States Supreme Court United Housing Foundation v Milton Forman (U.S. 837, 852 (1975), one of the characteristics associated with stock was that they confer voting rights in proportion to the number of shares owned, but this was no longer the case a decade later.
44 “Taxonomy for cryptographic assets – v2.3” published by Global Digital Finance in 2018
45 Sometimes called utility tokens or consumable token, although these terms have been contaminated by issuers who have used them in misleading ways.
and crowdfunding differ - and they do in significant regards - misdirection may occur. Regulation that is imposed too early or misses its target can hamper the prospect of creating new models for the undertaking of commerce and the development of new asset classes that support it, as further discussed in section 4.5.

Third, while there may nevertheless be some benefit in legally-themed taxonomies because of their ready recognition by regulators, care needs to be taken that the taxonomy is not merely “solving” the problem without changing the underlying assumptions about how existing securities laws apply, or should be developed to apply, to cryptos. Taxonomies that do so are essentially recursive and in reality achieve very little. It is of course somewhat paradoxical to address something new by treating it as though it were something old. This raises a fundamental jurisprudential question, of whether the purpose of the law is to impose a framework that commercial developments must adhere to, or whether it should reflect commercial developments subject to overarching safeguards. Section 5.1 discusses matters that impact on policy development.

Taxonomies establish systems that facilitate dialogue and common understanding based around it. It is not sufficient that a taxonomy can be said to be “correct” insofar as it is consistent with a set of observable facts – aeroplanes, birds, Icarus and angels all belong to a category of winged things. The relevant test is the usefulness of the taxonomy, what information it provides to develop an understanding of a problem. If the taxonomical question for cryptos is how to determine what cryptos should be considered the subjects of what form of regulation, taxonomies that service legal solutions based on existing constructs of law and regulation may amount to an exercise of arbitrary power inconsistent with the rule of law. They accordingly postpone the essential problem: while they may assist making a regulatory determination, they do so at the risk of finding an outcome that justifies regulatory intervention at the expense of legal clarity.

It is feasible to argue that basing taxonomy around cryptos is not the only focal point to consider given it is the CCTech that drives, and limits, the possibilities inherent in any crypto iteration. One might analogize this to, for example, asking whether an endemic problem is best solved by focussing on animal morphology or genetic heredity. Or to the interconnecting laws and regulations that govern the corporate machinery enabling the creation of corporate securities, as compared to those that govern the issuance of securities into the market. It's a question of level. A taxonomy that brings within its consideration the CCTech itself could potentially assist to resolve some of the current legal uncertainties. This would require taking as its direct concern the core elements of the CCTech itself, much as regulation in parts of the financial services industry has had to move away from simply regulating human behaviour occurring in relation to financial products and services to regulating the behaviour of computer codes while ensuring responsibility for code behaviour rests with relevant individuals.

Shifting the subject of taxonomy away from solely cryptos, which are built on the “genetics” provided by the underlying CCTech, is a subtle one that brings focus to key elements of the technology relevant to questions of whether a crypto might be regarded as having an investment purpose, or whether a common enterprise is (or is

---

48 I.e., what is constructed as law services the power of the authority that is able to apply the construction, as opposed to applying impartial and clearly defined principles of law. For further reading, see J Derrida, "Force of law: The 'mystical foundations of authority'.” In Deconstruction and the possibility of justice, ed. Drucilla Cornell, Michel Rosenfeld, and David Carlson. London: Routledge 1992.

49 For example, in relation to matters such as electronic and algorithmic trading, the operation of dark pools, and the provision of robo-advisory services.
capable of being) formed. This does not derogate from the point that a digital asset is itself “simply code” and that the way it is sold can evidence an investment contract subject to securities laws.\footnote{W Hinman, “Digital Asset Transactions: When Howey Met Gary (Plastic)”, 14 June 2018, available at https://www.sec.gov/news/speech/speech-hinman-061418} Rather, due consideration of the enabling or prohibiting properties of the CCTech may assist policy making and formulating the possibilities for regulatory development, as discussed in Section 5.2.

Appreciating that taxonomies serve different constructs and purposes, with differing potential implications, is relevant when seeking to meld the differing perspectives of the crypto community and the regulatory agencies. Taxonomies are not always transferable from one construct or purpose to another. The fact is that 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.

### 3.3 Where regulators stand

Laws operate according to their own terms of reference and the jurisdiction of one regulatory agency does not exclude the jurisdiction of another.\footnote{The court in \textit{McDonnell} noted this at p. 24-25.} Regulatory agencies are at liberty to assert jurisdiction over a crypto wherever they are regarded as falling within the ambit of their authority. In the United States, this has led some to describe this as a political turf war between the CFTC and the SEC.

A more useful characterization of the situation is to recognize it as a reflection of the challenge that CCTech poses to existing categories of financial regulation because many cryptos do not neatly fit the descriptions and characteristics of securities or commodities that have been laid down in the law and subsequently expanded upon by the courts. At the meeting of the United States Senate Banking Committee in February 2018\footnote{At which the Chairs of both the SEC and the CFTC testified.} it was recognized that if the legislature wants a particular agency to have oversight it has to decide what agency is appropriate, or whether a new agency is needed. One of the upshots of the meeting was that the Committee asked the SEC and CFTC to come up with their views as to what an appropriate regulatory oversight regime of cryptos would look like.

Whether the current uncertainty requires the further development of law is at this stage moot, and fraught with the risk of capturing either too broad or too narrow a spectrum of cryptos. A similar concern has been replayed in the courts for over half a century in relation to physical assets. For example, should the payment of membership fees being used to develop a country club be regarded as securities? The California Supreme Court thought that it should,\footnote{Silver Hills Country Club \textit{v. Sobieski} 55 Cal.2d 811 908-09 (1961). This case established the “risk capital test”.} although Federal courts have been reluctant to follow its approach\footnote{The risk capital test has been acknowledged at the Federal level (in \textit{All Seasons Resorts, Inc. v. Abrams}, 497 N.E.2d 33, 35 (N.Y. 1986); see also \textit{El Khadem v. Equity Sec. Corp.}, 494 F.2d 1224, 1229 (9th Cir.), \textit{cert. denied}, 419 U.S. 900 (1974)). However, this is not the prevailing view of the Federal courts which instead follow \textit{Howey}.} out of the concern of creating an approach to investment law that captures too wide a range of commercial activity. Case law in the United States and the UK is replete with schemes (often related to real estate) that test the perimeter of securities laws.

To the above risk can be added the risk of trying to create new laws in relation to an industry that is still emerging in its details. While the core science has been established, its technological implementation in a commercial context is still subject to
fundamental issues that may change how it works in practice, as discussed in Section 4.

Against these risks is the built-in flexibility of existing laws. As the United States Supreme Court has observed, “the fact that a statute can be applied in situations not expressly anticipated by Congress does not demonstrate ambiguity. It demonstrates breadth”. The drafting of statutory law typically strives to be resilient to changes in the social context that may not in their detail be anticipated by lawmakers. One such change was the development of the Internet, which, in the early 1990s, caused considerable confusion as regards what laws of what jurisdictions should apply to activity undertaken via a form of connectivity that was unprecedented and, like CCTech at present, had yet to fulfill its potential. The question is really about whether a change in society is sufficiently fundamental to exceed the tolerance of laws that might possibly apply. The question asked by sceptics is whether CCTech truly offers something new, or whether it is merely an applied science that enables a new way of doing something old.

3.4 Understanding the regulator’s perspective

As the industry pushes regulatory agencies for clarity, it is important for industry players to appreciate the perspective of regulatory agencies, and the laws that not only empower them but also bind them. Cryptos present regulators with a number of issues and policy challenges. This includes the legal characterization of various aspects of crypto-related commercial activity, the appropriateness of applying existing laws and regulations to cryptos and related activity, who should be the focal points of regulation, and the ambit of any such person’s legal and regulatory duties. Dealing with these issues may or may not eventually require resolution by lawmakers. In response to the perceived desirability of facilitating small and medium-sized enterprises with better access to capital, the JOBS Act was introduced in 2012, with Title III specifically providing for crowdfunding activities and Title IV creating a small offering exemption. The JOBS Act paved a clearer pathway not only for those seeking capital, but also for regulators as the Act created certainty as to the legal position of, for example, the obligations and expectations placed on various actors involved in crowdfunding under Title III. However, as discussed in Section 3.5, there are certain dynamics underpinning regulatory change, and these may not as yet be sufficiently animated in relation to cryptos.

A cursory look around the Internet on anything concerning cryptos reveals an enormous amount of material that suggests some form of responsible control is needed. Sales activities including advertisements for services that will provide information on trading tips, how to make money (for example, because the user will be told the “secret” date on which the price of a crypto will increase), forecasts of wealth gains, and guaranteed returns of hundreds of percent. Many of these appear at face value to be the kind of manipulative schemes that led to the 1933 Act. Not all of these are by shadowy rogue operators bent on fraud. Circle promotes itself as “a global crypto finance company on a mission to make it possible for anyone, anywhere to help change the global economy”. Its website invites consumers to set up an account “in seconds and move money from your bank instantly – as in right now... So you can buy the moment opportunity strikes”, adding “Investing in crypto isn’t just for those who’ve been around the blockchain. With minimums as low as $1, it’s easy to

56 Jumpstart Our Business Startups Act. Titles II, III and IV only become effective in 2013, 2016 and 2015 respectively.
57 Regulation A+ is now sometimes used in connection with ICOs.
58 A leading centralized crypto exchange in which Goldman Sachs has invested.
learn as you go.”59 This approach stands in contrast to stark warnings from regulatory agencies about the risk of investment in cryptos. The Bank of England’s warning was simply put: “anyone buying cryptocurrencies should be prepared to lose all their money.”60

The tools the regulators currently have are limited.

Regulators have been publishing warnings to investors about the risks of investing in cryptos, and to the industry that if a crypto is a security it will be subject to securities laws. Together, this has stemmed the participation of retail consumers and has pushed ICOs (particularly in the United States as well as larger ICOs) to be undertaken via exemptions that remove the offer from retail investors. Paradoxically, this means that smaller ICOs may remain available to retail investors yet these are the startups that may be statistically more likely to fail.

Regulators have also been pursuing a path of information gathering, which has assisted the curtailing of some ICOs and, following investigation, enforcement. The SEC has already pursued and is pursuing a number of fraud cases arising in the crypto industry. It is currently engaged in extensive probes into the crypto market that encompasses not only promoters but also exchanges, professional advisers and investors.61

Even if the basic conundrums were solved about which or whether a law applies to a crypto, there would remain some areas where regulation would be problematic from a policy point of view because some basic building blocks of regulation could not be satisfied. This covers both investor protection and market integrity considerations and includes:

- issues related to account management such as proof of ownership to public audit standards;62
- the ability to assert market transparency and market abuse protections;
- how exchange regulation might work;
- how money laundering risks are to be addressed; and
- how record keeping is to be undertaken.

The possibility of undertaking commercial activity on a decentralized, peer-to-peer basis that removes the need for centralized parties in transactions represents a qualitatively different kind of issue for regulatory agencies. At some point, adaptability may be challenged to the extent that existing regulatory tools that have developed around centralized, 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. The particular challenges

62 S Johnstone,” Requisites for development of a secondary market in cryptos”, forthcoming 2018
and opportunities presented by the centralized-decentralized spectrum of commercial models are discussed elsewhere.63

These are problems because of characteristics of CCTech still in the process of being understood and resolved, both by the industry itself as well as regulatory agencies including accounting bodies. The possibility of embedding tools within CCTech that facilitate solutions to these problems are discussed elsewhere.64

Solving some of the foregoing building blocks are precursors for effective, granular regulation to develop. Regulation proceeds on the basis that regulation is possible. Where it is not possible, regulation is more likely to take the form of a binary question: to permit or ban specified activity?

Where the answer to that question is to permit, it is likely to come with increased watchfulness, and that appears to be the case with the regulation of cryptos in many countries today. Activities captured by existing regulation (or are perceived that they should be), such as ICOs that fall within applicable securities laws, may be subject to a possibly more sympathetic approach where co-operation is forthcoming, as has been the case with the SEC in a number of cases (such as Slock.it and Munchee) as well as the SFC65 (Blackcell Technology).

OFAC66 has taken the step of indicating that it may add digital wallet addresses to its SDN List,67 meaning that doing business with those addresses has OFAC implications carrying potential civil and/or criminal consequences. However, this step has been criticized as potentially driving crypto-exchanges, and the relevant address-holders, to other jurisdictions.68 This reflects the anarchic potential of CCTech that is critical for regulators to fully grasp if regulation is to be successfully developed - as argued in section 5.3, regulatory agencies will need to look for ways of bringing oversight to the industry by using strategies different to those previously employed.

3.5 Impetus for regulatory development

The imposition of regulatory oversight on commercial activity is in general driven by the need to facilitate commerce and address risk. 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 the public more generally.

Under normal conditions, regulation is subject to gradualistic development – the first modern securities law, the 1933 Act, has been subject to this form of development within the larger intent of the Act via the insertion of new provisions. It has survived for 85 years in large part because the concept of securities in the Act is intended to be flexible so as to enable the regulation of investments whatever their form and whatever they are called.69 Courts when interpreting the 1933 Act look to the intent of the legislature in promulgating the law. Legislative change, for example in response to ICOs, would only be necessary if ICOs presented challenges to meeting legislative

63 Ibid.
64 Ibid.
65 Securities and Futures Commission of Hong Kong.
66 United States Treasury’s Office of Foreign Assets Control.
67 List of Specially Designated Nationals and Blocked Persons. OFAC’s FAQ was updated to include this change on 19 March 2018.
68 O Jackson, “Ofac’s crypto blacklist could drive investors to riskier exchanges”, IFLR, April 2018.
objectives because tokens fell outside of the sensible range of flexibility of the securities concept, or if the application of law to tokens resulted in other outcomes that did not sensibly fulfill the legislative intent. The United States has a rich post-War case law on the 1933 Act and its intended scope that has informed the approach to securities regulation in other common law jurisdictions, including Hong Kong and the UK.\(^70\)

Non-gradualistic change is often motivated following a financial crisis. This was the genesis of the 1933 Act, which sought to restore trust in the public capital market following excesses of the 1920s that culminated in the 1929 stock market crash and the Great Depression. Such crisis-driven regulation is often described as focussing on increasing the protection of small investors from abuses perpetrated by knowledgeable insiders.\(^71\) However, this is not the sole, or arguably primary, purpose. An important parallel if not overarching purpose, discussed in a report leading to the implementation of the 1933 Act, is to bring development capital into productive channels of industry by protecting the capital needs of honest business from the competition for capital arising from dishonest securities offered to the public.\(^72\) As such, an important focus of the approach in the United States at that time was focussed on supporting efficient capital formation.\(^73\)

The wider economic benefit to society of bringing capital to productive use is straightforward to appreciate. This objective is no less relevant to consider in the context of the crypto industry, which is also in need of protection. As noted earlier, CCTech presents important opportunities for cost savings in traditional economies, and enables new economies to develop around digital ecosystems. An important challenge to the industry’s competition for development capital is that not all comers to the industry are honest actors, or actors with a real prospect of developing anything useful, yet such actors compete for the same pool of capital.

One attempt at protecting industry from what one might call internal abuse was the Sarbanes-Oxley Act of 2002 (“SOX”). However, SOX created burdens for industry that undermined incentives to take risk leading Congressman Oxley, one of the authors of the Act, to admit that SOX may be damaging economic growth prospects.\(^74\) Alan Greenspan, the Chairman of the Federal Reserve at the relevant time, has referred to “the nexus of risk-taking, regulation, innovation, and wealth creation”.\(^75\)

The most recent financial crisis of 2008 led to a number of reforms, for example, the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 in the United States, which is struggling in its implementation, and new global approaches to the regulation of credit rating agencies and OTC derivatives.

Some non-gradualistic, sporadic changes to regulation might be called “whac-a-mole” regulation. This is equivalent to installing a patch into a system as a reaction to an emergent problem. It is the least satisfactory from the perspective of coherent policy development but may be necessary to deal with gaps or loopholes. For example, the Lehman Brothers minibonds debacle\(^{76}\) led to the introduction of structured product regulation in Hong Kong following prolonged protests by affected investors.\(^{77}\)

The CCTech industry has already experienced significant failure events, arising from the failure to prevent crime, and from fraud. Well-known cases involving large amounts of capital include crypto-exchange hacks at Mt Gox (2014), Bitfinex (2015/2016), Coincheck (2018) and Bitgrail (2018), which together involved losses of over US$1.2 billion.\(^{78}\) These are examples of painful industry lessons arising from internal controls that are inadequate to defend against wrongdoing.

Regulatory responses in relation to the failures of exchanges vary. In Japan, where the two largest exchange hacks occurred, the FSA\(^{79}\) initially established, in 2017, a requirement that crypto-exchanges register with them under the Payment Services Act. Initially directed at oversight by way of information gathering, as opposed to standard setting, they have been, *de facto*, applying adapted versions of their existing exchange and securities industry practices. More recently, this has progressed to regulations that require exchanges to undergo verification and licensing processes that will encompass anti-money laundering matters. There is now speculation that the FSA is prepared to treat cryptocurrencies as a financial product, bringing it under the Financial Instruments and Exchange Act, which would bring stronger protections to investors. The industry has generally welcomed the approach and as such this represents a beneficial collaborative approach.

In the United States, a commissioner of the CFTC\(^{80}\) in 2018 informally recommended that crypto-exchanges should establish self regulatory organizations (“SROs”) to “develop standards around cyber policies, data retention, record keeping, financial records obligations, insider trading, ethics, codes of conduct”.\(^{81}\) In the UK, CryptoUk was formed as an SRO to promote higher standards of conduct – members are required to sign up to a code of conduct directed against illegal activities and providing other consumer oriented safeguards.\(^{82}\) To this can be added the development of industry best practices. Examples include those issued by Coinbase,\(^{83}\) the Fintech Association of Hong Kong,\(^{84}\) and Global Digital Finance.\(^{85}\)

The establishment of SRO standards are important preventative tools because they draw members to minimum standards designed to protect the industry, although the remit of best practices may be significantly constrained by the degree of legal and regulatory certainty attaching to an industry practice, as indeed it is in the case of ICOs at present. If the industry is able to self-organize to a level to prevent

\(^{76}\) Lehman Brothers misleadingly named “minibonds” had been sold to a large number of the retail domestic population, causing losses in excess of HK$12 billion.


\(^{78}\) The exchanges’ losses were, respectively, US$473 million, US$72 million, US$532 million, and US$195 million.

\(^{79}\) Financial Services Agency of Japan.

\(^{80}\) Commodity Futures Trading Commission.

\(^{81}\) Per Brian Quintenz, see https://www.newsbtc.com/2018/02/11/cftc-commissioner-crypto industry-should-regulate-itsel and https://www.youtube.com/watch?v=RzIsIvE3WE4

\(^{82}\) http://www.cryptocurrenciesuk.info/

\(^{83}\) “A Securities Law Framework for Blockchain Tokens” 7 December 2016.


irresolvable material problems emerging, then they will tend to remain largely under the threshold for regulatory reform. However, self-regulation frequently leans toward industry self-interest and weak enforcement mechanisms. In the absence of a “legal stick”, SROs may cite established practices, industry readiness (i.e. the lack thereof), competitiveness, or even cultural values as the basis for rejecting proposals for more stringent standards. Some of these dynamics are reactive, based around the need to survive. They may also operate as mechanisms that defer more formal regulatory oversight by laws that are less adaptable by the industry itself, less avoidable, and which present potential liabilities. As Robert Reich has argued, relying on corporate social responsibility to self-regulate is no substitute for effective laws that facilitate acting in a manner consistent with politically agreed social objectives and punish wrongdoers.

Other changes are proactive to such objectives. The JOBS Act, discussed above, is one such example, as would be the various exemptions created to facilitate foreign access to the United States capital market. Another is the change of Hong Kong’s listing requirements to allow large, non-profitable biotech companies to list as doing so would facilitate raising of capital necessary for the development of potentially important medicines and medical technology. There are many such examples.

In the absence of any of the above factors, legal clarity is not often a sufficient emphasis for legislators to change the framework of laws and regulations that apply to an industry. This is usually left to the purview of the courts, whether in response to litigation initiated by regulatory agencies or privately. For example, Ripple has been subjected to a series of lawsuits, privately brought, alleging that its sale of tokens violated Federal securities laws. While the suit certainly sends a warning signal to other promoters, it is unlikely to influence lawmakers. Should that case come to court, it could establish case law that facilitates an empowered regulator bringing a legal action.

A recent criminal case that has been brought under securities laws in relation to an ICO is of interest in this regard. The defendant sought a motion to dismiss the indictment based on, inter alia, the tokens are not “securities” and the SEC has violated the Administration Procedure Act on the grounds that the application of securities laws is unclear in relation to tokens and that the SEC has not issued interpretative rules despite the prevailing uncertainty. While that motion to dismiss has been rejected, and so the case is proceeding to trial, which will be held before a jury.

3.6 Looking backwards, looking forward

Excusing the fact that we are a year short of being two decades into the 21st century, this Section 3 has been a backward looking review of elements of the 20th century approach to regulating the financial markets. Such a review is necessary because past knowledge and experience so frequently informs – and constrains – the way future development is conceived. One sometimes hears the question, to what extent is 20th century thinking holding back the regulatory oversight of cryptos? The foregoing sections have highlighted the flexibility – and constraints – of established regulatory
categories. It has touched upon the importance of appreciating what taxonomies constructively as well as possibly destructively do, the difference between function and form, and between intent and outcome. However, one needs to be careful in answering the question posed above, for answers can go both ways in terms of consequences.

History is replete with examples of political and legal frameworks based on a priori assumptions, often protective and prescriptive in nature, hampering the development of technology. This sometimes takes the form of partitioning commercial activities in separate silos along business or product lines – while that promotes the development of specialized rules, it also inhibits (or prohibits) inter-silo activity. Partitioning can be done based on principles that are worthy of considered debate: the Glass-Steagall Act 1932 that had separated commercial and investment banking was gradually watered down in the second half of the 20th century until it was repealed in 1999. However, that is regarded by some commentators as a mistake that facilitated the 2008 financial crisis. On the other hand, partitioning along established product lines can be hugely inhibitive of potential benefits – although the separation of telephony and data pre-Internet no longer made sense in a post-Internet context, these silos were not broken down for some time, an example that shall be returned to in Section 5.2.

This Section 3 has also touched upon the question of what the best point to impose regulation might be – promoter, platform, exchange, product - assuming that remains the most sensible classification of actors in relation to CCTech given the significantly different characteristics of cryptos, including their ability to penetrate markets cross-border, their transferability, and their pseudonymity.

As noted, it is necessary to keep a clear distinction between scientific development, the commercial application of scientific discovery and the funding of each of the foregoing. The distinction is important to make as many of the concerns that have been expressed about ICOs, by governments, regulatory agencies and others, should not be confused with the validity or otherwise of the underlying science and its technological implications. Whereas ICOs give rise to policy questions concerning access to the public capital market, any application of scientific discovery in human society gives rise to a fundamentally different set of questions concerning the use case of the application and whether the technology has been properly developed and safely applied. As discussed in the next Section, not all cryptos do what they claim to do, may contain coding errors (i.e., bugs), and may be incapable of being scaled, any of which can result in a variety of practical problems that affect their functioning in practice.

Where these two different concerns – about access to funding for the application of science - intersect is whether the public capital market is being accessed by technology that is or is not fit for purpose. If there is a simple, overarching conclusion to draw from the considerations presented in this Section 3, it would be this question: is the current trajectory of regulatory thought and action on CCTech cum cryptos working toward supporting the efficient allocation of risk capital? In other words, does it facilitate an environment that assists capital find projects that offer, and have a reasonable prospect of delivering, economic and social improvement? If the flow of capital is unduly restricted (or made excessively costly), industry development will

---

92 By the Financial Services Modernization Act of 1999.
suffer. If transparency and accountability in capital flow is not fostered, capital may be diverted to projects doomed to fail.

The corresponding problems of the industry in its current state of development are discussed next. Section 5 considers the difficult questions of policy development.

4. CONUNDRUMS IN A DEVELOPING TECHNOLOGY

One of the inherent difficulties of answering the question of regulation 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 crypto is still evolving notwithstanding some conquests of old technology solutions. To that list can be added a more general disquiet of critics of cryptos, of whom it is sometimes argued that they either do not understand the science or are unable to distinguish between correct technological uses and ones that are bogus. The plethora of ICOs, many of dubious quality, have inadvertently fanned the concerns of critics. There is also the sometimes-heard complaint that “we don't yet know what these cryptos are”, a catchphrase intended to suggest that the nature of cryptos and the relations they implement are as yet to be understood for legal and accounting purposes (amongst others).

This makes policy formation leading to regulatory implementation difficult as these conditions increase the risk that regulations could be made only to see the industry change under it, or that the regulations capture the wrong family of acts – in either case the policy objectives are missed.

The list of technical concerns that hover over CCTech which potentially give rise to legal problems is a longish one that in each case requires 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, privacy, the risk of consensus hijack, denial of service attacks, double spending, scalability, code governance controls, cybersecurity challenges and tools for detecting and preventing money laundering. In lieu of a complete exposition of such problems, this Section selects a few of the present conditions within the industry to demonstrate some of the issues that make the imposition of regulation difficult.

4.1 Standards

Section 1.1 introduced the problem of knowledge gaps and identified that this is often addressed via disclosures and the engagement of independent experts and/or the adoption of standards that act as a measure of conformity. This enables outsiders (i.e. persons not privy to the knowledge possessed by insiders who have been developing a proposal) to make a better-informed assessment of a proposal.

Some ICOs have sought to alleviate this problem by adopting a solution that has been used in the crowdfunding context, namely, establishing message boards that enable potential investors to post questions and receive answers from insiders. While this is a step forward, it lacks the impartiality of, for example, the role of sponsors for companies seeking a listing of their shares on a public market via an IPO as used in Hong Kong and the UK. In countries that do not use sponsors (such as the United States), underwriters are motivated to ensure full disclosure by commercial incentives (financial reward and client relationships) and the risk of statutory and civil liability.

Disclosure standards in the crypto industry currently fall well short of the practices in developed public capital markets. The development of standards often reflects the evolving regulation of an industry, which typically goes through three discrete phases:
no regulation, self-regulation, oversight regulation. In the early stages of industry development there may be no real incentive to establish standards as this may be counterproductive to competitive advantage and counterproductive to purpose. As the industry emerges, there is more money in the industry, which attracts more players having different rationales for entry, including those that seek to make gains from short-term competitive advantage and who may have less incentive to promote standards. This is also the case with scams and fraudsters who will move in and out of the market in short life cycles for the purposes of avoiding detection.

Short-term advantages do not last for long. Other actors catch up. Scammers are forced to move to new tricks as the industry continues to grow and the hallmarks of scams become more readily identifiable. Some of the (legitimate) short-term players may also develop a long-term stake as their costs of investment and benefits received from it need protecting. The interests of long-termers, who frequently identify themselves with the development of the industry per se, also may sit at odds with those of short-termers who are regarded as rent seekers engaging in practices considered undesirable or unsustainable from an industry development point of view. At around this stage, standards start to develop in the form of best practices, often published by newly formed groups that have a stake in the long term development of the industry.

As the industry matures, standards are at their most basic level, borne out of the usual practices that have emerged – at least among the more influential group promoting their own practices as standards. In that sense, standards are backward looking and, depending on the dominance of the standard setters, can operate as anti-competitive mechanisms, forcing out players unable to comply with the standards or, where the standards result in an increased start-up cost, working as a barrier to new entrants to a market. It thus becomes a competition to establish standards aligned with one’s own priorities.

As standards become more widely accepted, two things start to happen. First, they should, if meaningfully set, begin to service outsiders in the reduction of the knowledge gap. Second, as standards are essentially backward looking, competitive advantage comes from looking forward, which will eventually lead to the development of new standards as higher standards come to be more widely expected as the norm.

Meaningful industry standards that go beyond “best practices” are yet to emerge in relation to one of the key disclosure items of interest in any purchase of cryptos, namely, the underlying code: does it 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, have the security protocols been properly implemented. Not all codes are the same in this regard. These are not problems unique to small start-ups – bugs are a ubiquitous risk of writing complex code. Financial institutions that depend on any form of computer programming to undertake commercial activities will often engage at least one secondary layer of coders whose task specifically is to proofread the code-writer’s work to ensure it does not contain any errors or inappropriate code. The Ethereum Foundation runs a bounty program that makes payments to anyone who discovers and reports discovery of a bug on a private basis to the Foundation.95 This enables fixes prior to the bug being exploited by malicious users.

In the interim, there is an evolving practice of having the quality of the code reviewed by an auditor, usually themselves a developer skilled in identifying bugs and other flaws in code, yet standards remain pre-nascent. How to verify that a code says what it does and there are no bugs in it is not a simple task. At present, different entities

95 https://bounty.ethereum.org/
are developing, and guarding, their own practices and experiences. However, if standards were established for code writing on which assurances could be based, a clean audit opinion would raise an investor’s confidence. Theoretically, this should result in lowered risk and more efficient pricing for investments in cryptos including via ICOs. However, no such agreed standards currently exist.

In addition to the foregoing technical considerations, other standards concerns relate to the real world demands placed on what the code is expected to deliver: what enforceable legal relations are established, how ownership of the crypto can be proven, whether the crypto can be subject to meaningful custody arrangements, how it might interact with the tax system – see further Section 4.5.

An important area of development to watch in these regards is the standards being developed by the International Organization for Standardization in their ISO/TC 307 programme. As at the date of writing, nine new projects concerned with blockchain and DLT are in their proposal or preparatory stages, including taxonomy, custody, smart contracts, and interoperability.  

4.2 Immutability - codicem meum pactum

The concept of immutability is a fundamental one to CCTech as it is intimately tied to the central concept of peer-to-peer consensus mechanisms based on trustless trust enabled by cryptography. Immutability implies that, once a crypto has been developed and deployed, it is unchangeable by subsequent human acts – it relentlessly performs as it has been set up to perform. As such, immutability is an assurance or performance and this has been expressed as “the code is the law”, alternatively as “codicem meum pactum” – the code is my agreement. However, in a system based on the concept of consensus, immutability is not the only foundation of CCTech and the two concepts, being different in nature, give rise to anomalies that may be difficult to resolve.

Immutability has been described as guaranteeing predictability, however, that is not entirely correct. Predictability is more correctly described as an objective, since written code may or may not be successful in implementing intent depending on how the code has been written. Where not written correctly, mis-performance occurs. A coding “error” may be taken advantage of by actors deemed by others as malicious. But if one accepts the code as law, an embodiment of what has been agreed to, then a “hack” may be properly regarded as legal because the “hacker” is simply using the rules in the code. Although this may not be in accordance with intent of the creators of the code, it is in accordance with how the code operates and therefore fair when judged by those parameters. Put another way, the “hacker” is simply taking their own advantage from a set of rules that are only flawed when measured against how the creators, and subsequent participants, had hoped the code would operate. One might paraphrase Roland Barthes and state that the deployment of a code represents the death of its creator and the birth of the user.  

The above issues were realized in June 2016 when a smart contract crypto running on the Ethereum network called “The DAO” was subject to an intrusion that drained around US$50-60 million via a bug discovered in the code. The DAO had raised over US$150 million in its ICO, at that time the largest amount ever raised, and its “hack” had sent the price of Ether down by over a third. When the Ethereum Foundation then proposed solutions that sought to undo the problem a person claiming to be the perpetrator of the act in an open letter disputed that their act should be characterized

96 https://www.iso.org/committee/6266604.html
as theft, and pointed out that the terms of the DAO are fully set out in the smart contract code, which expressly states:

"Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO’s code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO’s code ... The DAO’s code controls and sets forth all terms of The DAO Creation."  

In legal terms, this is effectively equivalent to contractual estoppel. The letter thus suggested that their action was a reward permitted by an explicitly coded feature of the smart contract, and its writer threatened to take legal action against anyone who tried to invalidate his work. The consequence of the event was that Ether holders eventually voted by almost 9:1 to execute a reversal – a hard-fork that created what is now Ethereum; Ethereum Classic is the original unforked version of Ethereum. The event was a significant one in the industry’s history as it brought into focus questions about immutability of the code, and the proper role of decision-making based on consensus.

4.3 Immutability – code governance

A hard-fork is inconsistent with the concept of immutability, and some users regarded it as a departure from principles. However, the size of the vote in favour of the hard-fork appears to indicate the strength of belief that sometimes the code should not be the law. This has led to developing the concept of immutability from “code is the law” to “the intent of the code is the law”. This shift mimics what happens in the real world vis-à-vis contract law and the fundamental requirement that there must be a meeting of minds – a consensus ad idem – that determines what the parties had intended, as opposed to the bare contractual language. Judicial tests to establish what was intended, such as the reasonable bystander test, are in the digital context mapped onto different forms of governance mechanisms that enable events deemed inconsistent with intent to be rolled back and corrected.

Since a code-is-law approach requires adopting the belief that the technology of consensus meets the relevant needs, it implies irrevocably accepting the possibility it may not and that in such cases remediation is (or may in normal circumstances be) out of the question. In the language of financial systems, the latter possibility equates to risk and therefore impacts negatively on the value proposition as compared to an equivalent system that was free of such a risk. While that represents a financial dynamic, the base problem is that society is not defined by a set of laws so much as laws reflect social values and agreed normative expectations and standards involving justice and fairness.

The debate has led to new CCTech being developed based on dispute resolution or a revised understanding of immutability. The chief protagonist in this context is EOSIO, although it’s role and the emergence of other actors in this topic has been evolving rapidly. In EOS, intent is determined by a super majority of a community arbitration forum (“ECAF”), comprised of “elected producers”, who undertake essentially a similar role as arbitral bodies of traditional commercial contracts. Rules of the ECAF seek to

---

98 The open letter is available at https://pastebin.com/CcGUBgDG
100 I.e. a rollback of the blocks that reversed transacted blocks to the block prior to the hack.
101 https://block.one/news/block-ones-proposal-for-eos-constitution-v2-0/
comply with legally accepted principles of procedural fairness and natural justice, and empower the ECAF to apply remedies including revocation of tokens and damages awards. ECAF has already had one test, and failed, leading to block producers (i.e. the EOSIO equivalent of miners) taking unilateral action in what some in the crypto community regarded as an abuse of power. This situation has been very poorly received in the EOS community leading to questions concerning the continuance or removal of the EOS developer, Block.One, which again raises the spectre of collective decision-making. As demonstrated in the Ethereum hard fork, consensus can be a fickle friend – it can also depart from its original purpose where, such as in the case of EOS, a small minority own most of the tokens cum votes.

The latest EOS proposal is to move dispute resolution to Ricardian contracts that use human readable terms capable of expressing intent. This merely pushes the problem one step away rather than resolving it. Lawyers and law courts are engaged on a daily basis with interpreting intent in contracts that were meant to express intent – while this sometimes arises out of poor or ambiguous drafting, it often also arises out of unexpected scenarios that neither party may have actually contemplated. The fact is that commercial contracts reflect commercial intent rather than defining it. In that sense, both code-as-law and intent-as-law are equally Cartesian, that is, reducing human dealings to the geometry of moving parts presumptive of intent or purpose. As such, it is open to fraud, manipulation and gaming of unintended errors.

Code governance is now a core area of interest in the development of CCTech, whether failsafe mechanisms are necessary or challenge the concept of immutability, and whether or how principles of law long established in the traditional markets ought to be managed (or not). The emergence of Telos as a reaction to the problems EOS is experiencing is of interest as they are seeking to change from a pure one-token-one-vote principle to a system that caps votes by capping the maximum number of tokens that can be held, somewhat reminiscent of earlier corporate laws that limited voting power, none of which have survived going into the late 20th century.

It seems likely that the industry will struggle with the topic of code governance as a matter of political philosophy and commercial workability for some time. In the meantime, establishing minimal standards of performance vis-à-vis predictability of outcome, or clarity of the relationship with traditional legal sources of dispute resolution, may become of interest to SROs or regulatory agencies.

Concepts such as disclosure and caveat emptor are excellent concepts but are frequently inadequate replacements for arrangements (be it legal, regulatory or otherwise) that establish or prescribe a more formal approach for identifying and dealing with issues such as those that might arise out of code as written and code as intended. In the financial services sector, the adoption of technology solutions such as algorithmic trading and robo-advising have caused regulators to recognize that what they had previously regulated via codes of conduct – human behaviour – now required

---


According to a white paper by Telos, 1.6% of EOS holders own 90% of the tokens, as cited here: https://www.coindesk.com/fed-up-and-forking-rival-eos-blockchains-are-becoming-a-reality/

Essentially contracts that record documents as a signed legally binding contract with both digital and human readability.

different types of regulation that were capable of targeting the underlying codes themselves. In Hong Kong and the UK, this has resulted in highly tailored regulatory codes that are outcome focussed, and increased accountability being brought to senior management responsible for code writing, such as the head of a technology function.\footnote{The FCA’s Senior Managers and Certification Regime and the SFC’s Manager in Charge Regime.} Nevertheless, there is a considerable extent of uncertainty as to what that might mean where, for example, an algorithm begins to make trading decisions that are unable to be understood (in real time) by a human with failsafe control over the system.

The position in the CCTech industry as well as the traditional financial services industry both illustrate the basic conundrum of translating human concepts of what is reasonable to do in any given situation to machine implementations that operate at a rate faster than a human can assess and approve or correct – this is particularly problematic where machine learning, operating on the basis of highly automated probabilistic determinations, is used.

The problems surrounding immutability harks back to issues reminiscent of post war behavioural psychology which proposed the possibility of society being run on the basis of behavioural equations that were capable of being mathematically expressed.\footnote{Clark L Hull, “Principles of Behavior”, Appleton-Century-Crofts, New York, 1943.} The controversial psychologist Hans Eysenck expressed it as a need for “a technology of consent which will make people behave in a socially adapted, law-abiding fashion, which will not lead to a breakdown of the intricately interwoven fabric of social life.”\footnote{Hans J Eysenck, “The Technology of Consent”, New Society, p. 688, 1969.}

It is ironic that CCTech could also lead back to a cold orderliness that sooner or later may, unchecked, lead to an atomization of commercial relationships and a corresponding loss of socially embodied common sense in performing them. It is suggested that code governance should promote informed, responsible and accountable freedom of action (as properly understood), not used as a tool replace it.

4.4 Technical issues

In addition to the foregoing issues, which frequently border on the philosophical, other technical issues that are still trying to be fully understood and resolved directly impact on the ability to regulate meaningfully. Yet others represent issues that could give rise to regulatory concerns if the industry is subject to regulatory oversight.

One set of issues arise out of the consensus mechanism that leads to the creation of, for example, orphans and forks, and the risk of double spending. The problem of forks, as discussed above in relation to The DAO, creates real legal issues to be resolved, and because these sit at the centre of a debate on how a consensus mechanism is supposed to work, this makes it difficult for regulations to be laid down without imposing on the industry constraints that may inhibit development toward the best commercial solution. Double spending also gives rise to legal concerns as miners may using spoofing techniques that take advantage of processing time delays to create chains that are later orphaned, but in the intervening period transact the cryptos to obtain some other good or service. When the block is later orphaned, the provider of the good or service has lost the value of their trade. In legal terms, this would appear to amount to fraud where done intentionally.

Both problems are the subject of a considerable amount of industry effort to find solutions. They are also examples, as seen in many industries in development phases, of industry being the best placed to understand how the technology could be optimized. It was not until a steam engine on one of Stephenson’s trains blew up and
killed its driver that the spring-safety-valve was incorporated, in 1827, a feature that subsequently became standard.\textsuperscript{111} One might also cite the commercial interest Lloyds of London took in what was later to become the Plimsoll Line. Section 3.5 discussed the typical progress from no regulation to self-regulation to oversight regulation. However, where the industry is unable to reach agreement on issues that lead to material negative consequences in core areas of regulatory concern – such as consumer protection, market integrity and financial stability – regulatory oversight may nevertheless trump any contemporary concerns for industry development. In the modern context, an important function of regulation is of course to be proactive and identify problems before any material damage is incurred.

Other issues of considerable interest to the viability of the industry may be of lesser interest to regulators beyond the question of fair disclosure. One such issue would be the scalability of a crypto, which might alternatively be described as the ability of a crypto to cope with success. The problem is that the more users who join a network (primarily a problem for public cryptos), the more the consensus mechanism may slow, resulting in a variety of problems including higher transaction costs. The current transaction rates on established DLT such as Bitcoin and Ethereum compare very poorly to other tech-based services such as credit card and stock exchange systems.\textsuperscript{112} These other systems are fast because the processing of the transaction is centralized. DLT applications are by their nature decentralized, which impacts on speed because of the time consumed in meeting the requirements of the consensus mechanism (i.e. proof-of-work). As noted above, delay also gives rise to a risk – arising from both statistics and bad actors - that a transaction may not be confirmed when the next block in the chain is confirmed. This is an area where technical rethink of the underlying science are exploring solutions, including Ripple\textsuperscript{113} and Zilliqa\textsuperscript{114} that are seeking to increase speeds to match that of credit card companies – necessary if they are to compete as a payment platform. The other aspect of the scalability problem is the use of legacy systems and the borrowing and reusing bits of earlier code writing because doing so provides a lower cost option for a start up as compared to building from scratch a new protocol. As CCTech built on legacy systems becomes more widely taken up, small issues can quickly become more significant and new issues emerge that may be made more difficult, or more expensive, to solve because of the earlier cost savings. Dealing with legacy systems is already a significant issue in the banking sector, and it is likely to be an issue for CCTech going forward, particularly if new standards or regulatory requirements are imposed that may be rendered more difficult to comply with because of legacy issues.

An important aspect of the scalability problem arises out of a fundamental choice of a system technology that is decentralized not centralized. Both systems currently compete in the same markets for commercial activity. Credit card systems and online

\textsuperscript{112} Estimates vary but Bitcoin comes in at around 5 transactions/second ("t/s") and Ethereum at around 15-20 t/s. This compares poorly to other tech-based services: Visa can process transactions at around 24,000 t/s, Facebook can processes likes at around 52,000 t/s, and regulated stock exchanges process transactions in the order of 60,000 t/s. Visa data 2010, from Visa, see https://usa.visa.com/run-your-business/small-business-tools/retail.html; Exchange data from HKEX, see https://www.hkex.com.hk/News/News-Release/2018/180123news?sc_lang=en
\textsuperscript{113} Ripple processes transactions at around 1,500 t/s and claims it is scalable to 50,000 t/s (as at July 2017). https://ripple.com/xrp/
\textsuperscript{114} Zilliqa launched a private testnet with a transaction volume of 2,488 t/s with 3,600 nodes in the network, that is said to be able to increase the number of transaction per second as the number of nodes in the network increases. This is achieved via a process known as sharding that enables transactions to be processed in parallel. So, for example, it proposes that a network size of 10,000 nodes would deliver expected throughput of approximately 8,000 t/s). See https://cryptopotato.com/zilliqa-ico-evaluation/
payment systems such as Alipay are fast because the technology managing the tasks is centralized and so does not require any consensus task to be undertaken. However, having a central point of control is also their primary drawback as it represents a concentration of risk in the provider of the technology cum service.

Beyond the technical and commercial aspects of the scalability issue, there is a more fundamental industry, regulatory and social debate concerning centralized and de-centralized models. In part, this is based in political philosophy because it concerns the question of whether economic units (such as individuals) should be enabled to trade with each other directly without a centralized control gateway that facilitates, for example, oversight of who they are and what they are doing. There are valid social issues involved here, which again concern the use of the capital market and commercial activity toward socially appropriate ends.

Discussions about the differentiation of centralization from de-centralization frequently miss the point that a commercial function is not the same as the means by which that function is serviced. If a primary concern of regulation is to ensure commercial activity is appropriate to social needs, then its proper focus is the underlying purpose of the commercial function, not the specific means by which it is implemented. Centralization looks like a familiar friend to regulators because of its obvious structural similarities to existing solutions, such as stock exchanges. However, the distinction between function and implementation sits at the heart of financial technology and the possibilities it enables. New thinking about exactly what might need to be subject to regulatory oversight becomes necessary where CCTech enables wholly new approaches to servicing commercial functions. How this plays out in the context of secondary market activity involving intermediaries and different exchange models is discussed elsewhere.115

In these regards, the shift of the ICO market toward private capital in the United States has forestalled some of the more pressing regulatory concerns there concerning public capital. However, this is an interim stage and better solutions to issues such as the above must be resolved for the industry to be made more accessible to a wider public market. Accessibility necessarily also entails rendering problems such as the foregoing subject to meaningful disclosures that encompass the entire stack of technology on which a particular crypto relies, including the governance of the source code on which a crypto is built, and the attendant risks at each level. Nevertheless, as already noted, not all problems can simply be resolved by disclosure, and positive regulatory action is sometimes needed, for example, that direct specific disclosure requirements or standards.116

4.5 Development of new classes of financial product

At the present stage of development of CCTech, certain building blocks are absent that would be required to gravitate the industry, or parts of it, toward something proximate to the regulated financial services industry. The above discussion has already touched upon the issue of speed and the integrity of transactions – both of which are fundamentally connected to price formation and risk taking in an active market. Investment risk in cryptos is currently somewhat naked owing to the absence of financial products that better allocate risk, adequate price formation mechanisms, risk modelling and the development of trading strategies based on these, each of which

require other precursors to develop meaningfully, including some of those discussed below.

This has been improving as a result of the regulatory recognition of cryptocurrencies as commodities. It has enabled the development of financial products including derivative products such as Bitcoin futures, funds that provide exposure to the cryptocurrency market, and indices.117 Because these products are traded on exchanges such as the CBOT118 and CFE,119 which are regulated by a statutory regulator, this has facilitated the perception of cryptocurrencies as a valid asset class to trade. In addition, persons engaged in the brokering of such products need to be authorized by the relevant statutory regulator,120 which means that persons wishing to gain financial exposure to cryptocurrencies may do so in a context subject to regulatory safeguards, including codes of business practice and internal control requirements, that protect investors from abusive or inappropriate practices. These developments also facilitate capital raising exercises because they enable the providers of capital to subsequently hedge risk in a well-regulated market.

While the foregoing is an example of regulatory oversight facilitating the industry, lack of regulatory clarity as to whether a crypto is or is not a security remains a hindrance. Notably, there are currently no such regulated derivative products for cryptos that are securities (or that might be regarded as a security). Futures contracts to date, such as XRP in the UK (October 2016) and XBT in the United States (December 2017), have been based exclusively on Bitcoin, leaving other cryptos uncovered owing to doubt as to whether they should be treated as a commodity or as a security. This has started to change with Crypto Facilities, an FCA121 regulated platform, launching Ether futures in May 2018, a move expected to be followed by futures exchanges in the United States following remarks made in June 2018 by a director of the SEC that Ether is not a security.122

Adequate market transparency in the underlying asset class is another significant hurdle to overcome. This is demonstrated by the attempts of Bats BZX Exchange to create an exchange traded fund,123 which requires regulatory approval of the SEC as the regulator of the exchange’s rules. The proposal has been rejected on the grounds that requirements imposed under the Securities Exchange Act 1934 (“1934 Act”)124 are not met as fraudulent and manipulative acts and practices may not be able to be prevented.125

Not unrelated to the foregoing concern is the adequacy of systems that identify the ownership and control of cryptos via private keys and pseudonymous bitaddresses.126 This is essential to, for example, the integrity of ownership, and the ability to operate custodial services able to provide client account segregation. Proof of ownership for the purposes of accounting and auditing standards is currently highly problematic owing to the concern that while a person might be able to demonstrate control over a

---

117 Indices are important because they allow other financial products to be built around them. The CME CF Bitcoin Reference Rate and CME CF Bitcoin Real Time Index were launched in November 2016 and generate a Bitcoin price based on data from contributing exchanges.
118 Chicago Board of Trade, a member of the CME Group.
119 Cboe Futures Exchange.
120 The CFTC in the United States (they must also become members of the National Futures Association), the FCA in the UK, and the SFC in Hong Kong.
121 Financial Conduct Authority (UK).
123 The Winklevoss Bitcoin Trust.
124 Section 6(b)(5).
125 SEC (Release No. 34 -83723; File No. SR-BatsBZX-2016-30).
126 For example, see www.bitaddress.org
token, private keys can be copied and shared, which means that another person could in theory also demonstrate ownership and control.

These are just some of the issues that need to be resolved for the industry to become part of a regulated financial services industry. Some of them require a combination of developing the underlying CCTech, and an assessment of whether existing requirements are appropriate to apply to cryptos. In the absence of this, would-be regulators of intermediaries or exchanges wishing to handle crypto (whether or not regarded as a security under existing laws) have a fundamental problem – how can the regulatee comply with a basic regulatory premise if the technology does not support the relevant building block, such as safe custody of client assets subject to formal audit requirements? These issues are discussed elsewhere.127

5. EVOLUTION OF OVERSIGHT CONTROL

CCTech undeniably enables quantitatively and qualitatively different boundaries of commercial activity than was previously possible. It has caused aspects of market behaviour to shift from competing on the basis of an established system of rules to competing for what is in effect a wholly new market with a different set of rules and business dynamics.

Yet the legacy systems attaching to traditional activities must continue to apply, adapting where they can. Where adaptation presents fundamental difficulties that risks losing sight of overarching social objectives of regulation, amongst which includes the facilitation of development capital into productive channels of industry, the need for policy development emerges.

This Section reviews some of the working dynamics of policy development and the challenges policy makers, and regulatory agencies, are subject to when confronting change. It considers industry responses to calls for regulatory oversight and the restrictions placed on regulatory agencies. It concludes with a proposal that control oversight must be installed carefully, and in a manner that makes it desirable for the industry to subject itself to oversight.

5.1 Policy development

Policy decision-makers will typically collect information about competing definitions of the problem to be solved, how the problem is manifesting itself in the world, and the range of policy tools that might be deployed to solve the problem.128 While that may seem largely empirical, establishing agreement on the nature and scope of a policy problem can be challenging because stakeholders engage both tacit and explicit knowledge about the nature of the problem.129 That predisposition makes the question of how to facilitate the potential of an ecosystem built around CCTech much more difficult because policy makers will tend to look for solutions from within the extant regulatory framework, which diverts effort from the development of other tools that are possibly more innovative and effective.130 Section 3.2 noted that taxonomies of cryptos might inadvertently create similar obstructions to more innovative solutions.

130 J Winn, op. cit. p. 39.
Laws and regulations inevitably make assumptions about the way a financial system works and this is to some extent reflected in regulatory architecture. A strength of the 1933 Act that has assisted it to survive largely intact for 85 years, is its specific focus on the relationship between disclosure and fraudulent practices in the capital market. The well-known quote “Sunlight is said to be the best of disinfectants; electric light the most efficient policeman”\(^{131}\) is attributed to one of the authors of the Act, whose ideas were a major influence on the disclosure philosophy of regulation.\(^{132}\)

What the 1933 Act did was to provide a specific statutory focus on a matter the common law has long provided for, fraud, thus facilitating the task of bringing an action in relation to wrongdoing in the public capital market. However, the Act was not entirely product neutral – it addressed investments and focussed its concerns on the concept of “securities”, thus initiating a chain of silos that included exchanges and commodities via the 1934 Act and the 1936 Act, respectively. Having established those silos, regulation of activities within them, while remaining based on disclosure, also become progressively more prescriptive and detailed. Building on this approach, regulation of the financial services industry in the modern era became based around three primary choke points concerning products, venues and acts. The latter two of these assume some form of intermediation via markets, brokers and advisers.

Regulation has already had to adapt in response to technology enabling the displacement of sentient humans from the regulated act. This occurred with the advent of ATS then, more recently, with the development of robo-advising. In both, sentence does not form part of the regulated act but rather is embedded in the coding that enables agency trading to occur or advice to be given. This has required industry participants, such as legal advisers and compliance staff, to shift their attention to the process and operation of coding and the parameters that control the outputs of the code – regulatory agencies have been forced to follow the shift to code functionality, while leaving responsibility with regulated actors.

Product regulation, which has yet to undergo a similar process in traditional markets, is premised on disclosure (by a discloser) and assumptions about product suitability. Exemptions may be granted in relation to offerings based on the nature of the investor (institutional investor, accredited investor, professional investor, etc) or the investee (for example, in the United States context, if the issuer is a foreign private issuer). Prescriptive product and offering rules for access to the public capital market may be established via listing and disclosure standards or via product specific requirements applying to listed securities or investment products. However, these approaches presume a venue, an act, and a particular kind of product that is based on existing financial instruments and corporate or trust laws.

Cryptos, and acts undertaken in relation to cryptos, present difficulties for these traditional approaches. There is a venue, but it may 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 recognized lack of clarity as to how to characterize a crypto for the purposes of regulation-by-silo. CCTech accordingly challenges the three primary choke points because it enables venue, act and product to be collapsed into the operation of code, such as via distributed networks, decentralized and disintermediated arrangements, and smart contracts. At some point, adaptability may be challenged to the extent that fundamental questions arise as to the continued viability of existing legal silos and

---

\(^{131}\) Justice Louis D Brandeis "Other People's Money And How the Bankers Use It", 92, (1914).

traditional choke points, thus giving rise to policy concerns. Nevertheless, cryptos may be subject to regulation under multiple laws - in the United States they are subject to regulation by State and Federal criminal prosecutors, the SEC, the CFTC, OFAC, the Financial Crimes Enforcement Network and the Inland Revenue Service. While this phenomenon is not unique to cryptos, it does present burdens for a industry in development.

In addition to specific developments in market practices and emergent financial technology, policy development is also subject to a number of larger factors that impact on the means by which regulatory oversight may develop. This includes the structure of the political and legal system and regulatory culture that gives rise to different models of change. As has been amply described in relation to the transformation of payment systems, the United States (and to a lesser extent the UK) traditionally leans in the direction of letting the market decide through industry trial and error (emergent coordination) within a framework of disclosure and enforcement. By contrast, the approach in the European Union is often characterized more by bureaucratic oversight and regulatory diktat. The suggestion that has been made is that emergent coordination responds better than others to periods of rapid change because a wider range of relevant information can be gathered from market experiences that facilitates a more effective decision making process. Indeed, one of the tenets of regulatory philosophy in the United States is that the collective judgment of the marketplace is on balance wiser than government control of private-sector conduct. As such, the test “is whether it is preferable to leave certain decisions to market institutions instead of relying more on government officials, who also err, to dictate results through regulation”.

In view of the wider policy-development considerations discussed above, the better role for regulatory development may be to steer away from prescriptive regulations and to instead set broad wait-and-see frameworks that focus only on core consumer objectives such as the prevention of fraud. That is arguably the approach being taken in the United States, and other markets, as of the date of writing.

5.2 Restriction and possibility

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. A complaint commonly made by market practitioners is that in the absence of legal clarity and guidance, and the assurance provided by regulatory oversight, the environment remains challenging for ecosystem development. To this can be added the risks to the industry (including attendant industry costs) already observed in traditional capital markets (primary and secondary) that include fraud, money laundering, theft, mis-disclosure, internal control failures, misfeasance, and adequate custody and handling of the money or securities belonging to another, among others. Many of these issues are currently being addressed through best practices self-regulation, as discussed in Section 3.5.

Regulation brings with it well established benefits. Higher degrees of investor confidence that is built on trust in responsible oversight mechanisms serves to lower the cost of capital. Concerns that CCTech may be used in connection with criminal and

---

133 J Winn, op. cit.
134 J Winn, op. cit. p. 4
136 For example, as has been done in Malta via the Virtual Financial Assets Act and the Innovative Technology Arrangements and Services Act.
immoral activities can be more squarely addressed. The risk that enforcement agencies might need to engage in resource-consuming ex post litigation is reduced. Together, this increases regulatory efficiency.

Legal uncertainty under existing regulatory silos is often named as the primary hurdle to regulatory oversight, the proposed solution to which is for regulators to provide guidance as to what cryptos would be regarded as securities. For the reasons discussed above, that suggestion oversimplifies the new context presented by CCTech (and as such presents only a partial, and probably interim, solution) and underestimates the policy considerations that go with it. This is particularly the case in relation to secondary market considerations. Sections 3 and 5.1 touched upon the question of imposing regulatory requirements at traditional choke points such as exchanges and intermediaries to bring cryptos within an oversight framework. While that approach adopts the usual stance to regulation based on prescriptions coupled with the threat of sanctions for non-compliance, it assumes exchanges and intermediaries are visible and identifiable, and exist within the borders of a jurisdiction’s enforcement perimeter – in practice this may be difficult to establish.

In any case, regulatory agencies do not have a free hand in this regard as they are bound by the ambit of their statutory powers and the other laws that govern the industry subject to their oversight. While regulators can indicate to the market how they intend to perform their functions, their functions do not encompass providing interpretations of legislation – they would in any case not be binding on a court.

Where a matter falls within a regulatory agency’s scope of oversight powers, a tool possibly at their disposal is the use of no-action letters ("NAL"). Rather than being based on any express statutory power, the use of NALs is often policy based, premised on meeting the overarching purposes and objectives of regulation. The SEC has a long history of issuing NALs dating back at least to the postwar period in consequence of the Hoover Report issued in 1955, which encouraged the SEC to provide advice to interested persons as to their compliance obligations under the 1933 Act. Other regulatory agencies, including the CFPB and the UK’s FCA, have used NALs sparingly. The SFC has not used NALs at all, although they arguably could. NALs can be, and typically are, coupled with a requirement for information sharing with the regulator, as has been done in various sandboxes used in connection with novel financial technology. Building on this, regulatory technology presents obvious opportunities for creating avenues within the underlying source code itself for interactions between the actors involved in any crypto generation or exchange, any purchaser of a crypto, and the regulatory agency.

As discussed in Section 3.2, a taxonomical approach to cryptos that shifted focus to CCTech refocuses attention on key elements of the technology that may be relevant to, inter alia, existing securities law as well as regulatory development. This encompasses, for example, the operation of transfer mechanisms including the ability to impose restrictions, the operation of the consensus mechanism, the role of identity, and the access points for subsequent amendment of the underlying code – not just the

---


138 Bureau of Consumer Financial Protection (United States).

139 Section 6(1) of the SFO gives the SFC considerable discretion to act in such manner as it considers most appropriate to meet its overarching regulatory objectives. This includes the power under s. 5(4)(e) of the SFO to issue materials as to how it proposes to perform its functions. The use of NALs could possibly be used in furtherance of its general duties, which includes “facilitating innovation in connection with financial products and with activities regulated by” the SFC (s. 6(2)(b) of the SFO).
particular crypto being developed by a promoter but the underlying CCTech on which it is being built.\textsuperscript{140}

Transferability is one of the features of tokens that gives rise to concerns under securities laws because this may be consistent with or promote investment intent, and because of the possibility that an exchange will list the token irrespective of the intent of the promoters.\textsuperscript{141} This problem could be addressed by a NAL safe harbour created for cryptos (i.e., tokens) that requires, \textit{inter alia}, specified transfer restrictions – where the NAL requirement is complied with, the token would not (in the absence of other relevant considerations) be subjected to enforcement under securities laws. The argument might be made that this renders the token less attractive to purchasers, but to the extent that argument is an accurate description of purchaser intent then perhaps the token indeed does function like an investment \textit{qua} security. Additional information requirements under a NAL based safe harbour could focus on risk-management priorities that deal with the prevention of fraud and criminal use via disclosure and identity requirements, and subsequently monitoring by all stakeholders.

A taxonomy refocused on CCTech could also assist to better separate regulation of the crypto as a product cum investment from regulation of acts related to the crypto such as offers, advertisements and advisory and other services in the primary and secondary markets. Regulation of the crypto as a product may encompass product development considerations including, for example, assessment of its design (such as transferability or minimum holding periods), feasibility to implement successfully (such as scalability), identification of risks and intended target market, etc. This type of approach has been successfully implemented with complex products\textsuperscript{142} - similar to cryptos that are based on existing CCTech capabilities, complex products are creatures of design based on existing financial tools. It could also assist to understand or establish what type of crypto is being encoded, and to remove the risk to promoters of actual use departing from intended design.

The essential limitation is that cryptos that are not securities under current laws fall outside the ambit of regulatory agencies, and those that are will nevertheless be subject to laws that extend beyond the powers of those agencies. In the former case, a NAL would need to operate as a confirmation of the regulatory agency’s view. In the latter case, a NAL would need to operate as a policy of non-enforcement subject to the relevant conditions being met. For example, to deal with the risk of criminal elements using the technology, regulatory (or even tax) advantages could be provided to cryptos built on CCTech that requires identity capture in a fully traceable system. This might be effected by creating allowances for exchanges that undertake identity checks consistent with anti-money laundering laws and deal in cryptos that embed such requirements in its code such that a traceable record of identity of buyer and seller is immutably written in the code at the point of each transaction. This is made possible by the emergence of viable methods of verifying identity online. While bad actors may steer away from such a system, good actors would be encouraged to enter the system creating benefits for systems that are compliant with the relevant requirements. However, this or similar proposals require coordinated action of policy makers. Where NALS do not provide an adequate pathway forward, one must turn to the legislators.

The structural restrictions imposed on regulatory agencies can, in the context of CCTech, be regarded as a legacy system. Some lessons can be drawn from history. Pre-Internet regulations that treated voice, image and data as different things was an

\textsuperscript{140} For example, the fixing of bugs in Ethereum is approved and merged into the source code by core Ethereum owners who have the relevant level of permission.  


\textsuperscript{142} "Guidance in Internal Product Approval Process", SFC, 30 April 2014.
example of regulatory silos developed along product lines that no longer continued to serve the best interests of consumers and social development more generally. The problem was that they were prescriptive in design rather than performance or functional-outcome based. Whereas the former assumes a static technology and prescribes how things should be done to avoid/mitigate risks, the latter addresses risks more directly. Where a risk does occur, functional laws may be better at bringing restitution than are prescriptive laws that focus on the breach not the consequence. It was the context of the changing technology and "obsolete assumptions & enduring mental models” that led to Isenberg’s well-known paper “Rise of the stupid network”\(^\text{143}\) in which he discussed the built in design assumptions, around which various technical and regulatory matters revolved, that no longer applied. Similarly, the emergence of CCTech suggests that the type of regulation likely to have a better chance of achieving meaningful oversight is one that avoids the prescriptive risk of presupposing too much about products, venues and acts and is instead designed around functional-outcome risk management in which the judgment of the marketplace and the stakeholders in disruption have their due voice.

### 5.3 Looking sideways, looking forward

Irrespective of how one is politically or philosophically aligned, or whatever regulatory controls might be put in place, the reality is that the nature of CCTech presents a fundamental obstacle to oversight control, as Tim May pointed out three decades ago.\(^\text{144}\) The advent of crypto billionaires presents the added complexity of networks being able to be formed that represent new economic systems that may, as they grow larger, progressively interact less and less with traditional economic systems, and to that extent oversight of material parts of the economy may also disappear from oversight control by, for example, governments and their regulatory agencies. A significant point of interaction presently occurs with fiat currency and the banking system, though this might not always be the case as other media of exchange develop. Tim May’s 1988 statement is often described as advocacy for anarchy or as a prediction but it is suggested that, correctly understood, it was simply a descriptive statement of cause and effect contingent on an enabling technology that subsequently emerged.\(^\text{145}\)

While control oversight causes some in the industry to position the debate along an axis of freedom versus Orwellian fears, appropriate measures of oversight and control have in the past assisted human society progress beyond the shadows cast by rogue operators and those who would deal in acts widely considered immoral, such as human trafficking.

The intractable problem is how to bring CCTech within an appropriate oversight mechanism given its particular technological capability to subvert. Notwithstanding the difficulties considered in Sections 3 and 4, the actors in the industry that are seeking to be regulated are doing so for a number of good reasons - it is proposed that these reasons can be engaged to make regulation a desirable option, subject to the extent structural issues discussed in this Section 5. This includes the following:

1. regulation has the effect of validating an activity’s legitimacy;

2. regulation provides assurances to participants that oversight control facilitates the minimization of avoidable risks;


\(^{144}\) See Section 2.1 above.

\(^{145}\) Reflecting Tim May’s comments made at the Hackers Congress HCPP16. His interview is available at https://www.youtube.com/watch?v=TdmpAy1hI8g
(3) regulation builds on the reputation of an actor;

(4) items (1) to (3) above represent a competitive advantage over actors not submitting to regulatory oversight;

(5) regulation provides access to a significantly larger capital market than the crypto industry is currently able to tap into as a result of, primarily, regulatory uncertainties and hard to gauge risks;

(6) taken together, the foregoing represent opportunities to bring more value to the business at a lower risk level.

In short, the best way to establish regulation may be to make it attractive. The desire for validation, legitimacy and capital growth may actually be the best motivators for bringing the development of cryptos toward a framework that provides a prospect for fair and balanced regulation. It also provides an appropriate nexus for regulatory technology to be amalgamated with CCTech in a symbiotic manner. That may not be an 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. And care must be taken that oversight controls do not to operate as anti-competitive tools.

Within the scope of the above six tenets, there is considerable latitude for getting the degree of oversight and market/industry voices properly balanced. That may or may not need to invoke existing categories of financial services activity, but it certainly will need to be based on outcomes that are independent of specific technologies and activities, such as fair disclosure and accountability for wrongdoing.

Such an approach will not remove all bad actors from using CCTech. Indeed, it is likely that no approach will, short of oversight control that becomes draconian and oppressive. Pools of socially desirable and undesirable activity will always exist in relation to CCTech, just as they have always existed in human society. The issue is establishing meaningful enforceability able to constrain the resources available to bad actors while at the same time fostering the opportunities available to those who assist in the progress of society.

Syren Johnstone
Hong Kong, 08 October 2018