Before Blockchain and Why it Matters

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

This article is Part 2 of the author's previous articled titled "Blockchain as a Disruptor of Securities Regulation" which featured in the April 2022 issue.

To paraphrase a well-known concept, to understand the present and anticipate the future one needs to understand the past. Yet this has in general not been the case with most responders to the emergence of Bitcoin, Ethereum and the whole gamut of public, consensus based blockchain cryptoassets that have come after them. As I discussed in last month's edition of this Journal, the primary narrative of the regulatory response is an incrementalist one within an existing paradigm of securities laws reactive to the latest perceived risk to consumers or financial stability. Insufficient attention, or recognition, is given to the distinction between blockchain technology per se and the things done with the technology. While the latter certainly might include financial products, to box public blockchain technology into the service only of finance would be a grave error.

Conceptual Precedents

Blockchain means many things to many people. Essentially based on developments in cryptography and computer science, blockchain has emerged from a context of half a century of debates around electronic commerce, economic competitiveness, privacy, intellectual property rights, export controls, law enforcement and national security. One often hears statements like, "Blockchain didn't exist before Bitcoin" or "Satoshi Nakamoto invented blockchain". However, this does not begin to capture the highly unconventional thinking about what currency was and who could create and transact it, or the socio-political struggles, that preceded and formed the conceptual basis of Nakamoto's seminal paper, "Bitcoin: A Peer-to-Peer Electronic Cash System" in October 2008.

Understanding those precedents, and the issues grappled with, provides important insights that promote a better understanding of the technology's broader possibilities, as compared to any particular iteration of it. It helps to inform the sources of the many different legal issues the technology has given rise to, and will continue to do so as its applications evolve. As stakeholders in society, it helps us appreciate the potential role of the technology in the evolution of commercial interactions, institutional arrangements and community interactions that may be a mechanism of societal evolution via new models of economic governance and coordination. Importantly, it also assists thinking about why and how we might regulate it.

Moreover, the Nakamoto kind of blockchain is only one possible iteration of how a consensus mechanism might work. One may find examples of "blockless" blockchains that build

trust across the network in wholly different ways. The characteristics of such features impact on issues such as governance, interoperability and identity that will affect the shape of an emerging cryptoeconomy.

A Weapons Technology

The prospect for blockchain emerged from a battleground with the United States National Security Agency that was framed by freedom of speech and by the tools of war. Encryption technology was formally classified as a munition in the period following the Second World War and during the Cold War between the United States and the Soviet Union. The discovery of split-key (or public-key) cryptography in 1975 by Whitfield Diffie and Martin Hellman enabled secure communication between two people who didn't need to meet to exchange a secret key in advance (as other cryptography methods had required) and didn't need to know each other's true identity. Trust in another party involved in a communication had thus been replaced by trust in a cryptographic system.

Split-key cryptography formed the basis of secure information-based networks between large groups of people who didn't need to know each other. Newsweek later described the discovery as "a revelation, a true blow against the empire". Bitcoin's genesis block on 3 January 2009 demonstrated a working version of decentralization based on Diffie and Hellman's trust in a cryptographic system. However, before Nakamoto's blockchain was possible, other issues required solving.

In 1988, Timothy May famously foresaw that enabling individuals and groups to communicate and interact with each other anonymously would be the basis for a social and economic revolution. The problem at the time was that computing power was limited and expensive, and the massive connectivity required for networks of computers to form in a public space was yet to emerge in the shape of the Internet. While cypherpunks regarded encryption as a fundamentally private act, an expression of freedom-of-speech, it wasn't until 1999 that controls on cryptography were ruled an impermissible restraint on freedom of speech (*Bernstein v US Department of Justice*, 176 F.3d 1132, United States Court of Appeals, Ninth Circuit). The Bernstein case was a culmination of increased public debate during the 1990s advocating privacy using cryptographic technology.

Electronic Privacy

By the late 1980s, payments for goods and services were beginning to be more automated via electronic payment systems. The possibility of consumer acts being undertaken over electronic systems had started to become a reality, albeit on a centralized basis. While electronic payments enabled better controls and security, it also created, as opposed to the hitherto anonymous payment systems provided by banknotes and coins, privacy issues because third parties could accumulate knowledge about the payer and payee. Conversations were conducted electronically, electronic mail and the Internet emerged, and the Clinton administration was promoting the "Clipper chip" into secure communication products produced by private industry.

Philip Zimmerman's release of the Pretty Good Privacy (PGP) cryptosystem in 1991 was a touchstone for debates in the 1990s about government oversight programmes and privacy more generally. PGP enabled new digital identities to be created segregated from legal identity. Where cyberspace identity is connected to legal identity, laws that apply can be enforced. However, in the absence of an evidentiary connection between legal identity and cyberspace identity, it seemed not possible to apply laws as traditionally understood and applied.

The emergence of digital information technology also prompted a re-evaluation of the relationship between information and value. The mid 1980s saw the launch of the American Information Exchange, a platform for buying and selling information. In 1993 Timothy May launched his experimental information market, BlackNet, which cryptographically protected the identities of its users. BlackNet was the first working demonstration that enabling parties to transact freely on an unsupervised and anonymous basis represented challenges to the authority of the state, and poses risks to society more broadly. At the time of BlackNet, there wasn't any native digital currency that also protected identity. Ross Ulbricht's Silk Road, a much later example, didn't suffer from that drawback.

Creating Digital Money

Bitcoin certainly was not the first effort to bring privacy to an economic act via a cryptographically protected environment.

One solution to privacy concerns was David Chaum's Digicash, which used cryptography to create digital money, eCash, that preserved spending privacy. It was unable to function as its own currency and required the involvement of the traditional banking sector – as such, it remained centralized. A number of banks took it on in the mid-1990s but it never caught on and DigiCash later filed for bankruptcy.

In 1998 Wei Dai proposed "b-money" as a form of electronic money that could be created and transferred on a peer-to-peer basis without the need for the traditional intermediaries of finance. Another decentralized solution to the question of how money is created was Nick Szabo's bit gold, proposed in the late 1990s. Bit gold was based around the concept of tokens that are provably costly to create. Like b-money, bit gold was proposed in response to, as Szabo put it, "all the trust that's required to make [fiat currency] work [...] but the history of fiat currencies is full of breaches of that trust".

Both b-money and bit gold were decentralized solutions to the question of how money is created. Interestingly, at around the same time, there was a separate academic discussion around the idea of money as depending on collective intentionality. However, neither b-money nor bit gold was realised. It wasn't until the CPU effort to perform calculations was able to priced (Cynthia Dwork and Moni Naor), and a proof-of-work algorithm (Adam Back's Hashcash) and, subsequently, transferable reusable proof of work tokens (Hal Finney) were created that the prospect for bit gold-like tokens that could be created, assayed and exchanged between persons was, at least in theory, made possible.

Perhaps more fundamental than the creation of money was Nick Szabo's observation that any economic mechanism could be run based on a peer-to-peer system without a trusted intermediary. It is at this point that concepts of decentralized commerce not only become feasible but also come to represent a challenge to the status quo – disruption and disintermediation appear as tangible possibilities on the horizon for the first time.

New Prospects for Commerce

Other opportunities presented by advances in information technology had been widely discussed since at least the late 1980s. This included the suggestion that corporate structures would become flatter and more networked than hierarchical. Notions of the virtual organization were explored. Electronic markets theory hypothesized that information technology would reduce the costs of coordination and lead to an overall shift towards markets (rather than hierarchies) to coordinate economic activity. Such discussions foreshadowed decentralized solutions to a variety of social acts. The advent of the DAO (Decentralized Autonomous Organization) post Ethereum is a direct descendant of these discussions.

Much of this was foreseeing a revolution in the way commerce could be undertaken without the parties traditionally involved. Yet despite the richness of the intellectual legacy that underpins concepts made possible by blockchain, concepts that point the way to potentially better mechanisms for social and economic activity, the response from policymakers was generally much simpler. At one end, most if not all public blockchain crytpoassets were bundled under either a consumer protection concern, or a threat to "the important role central banks play as stewards of public trust" (per the General Manager of the BIS in 2018). This sentiment was recently echoed (April 2022) by a member of the executive board of the European Central Bank who compared the cryptoasset landscape to the Wild West – not an entirely unfair comparison – and to the 2007 mortgage crisis but neglecting that out of the Wild West came the 5th largest economy globally, California, and that the mortgage crisis occurred in the heavily regulated banking sector. Perhaps more balanced, Christine Lagarde (also 2018) emphasized the need to distinguish between real threats and needless fears, and to protect against risk without discouraging innovation.

Thus, while the challenges to the status quo were apparent, so too were the responses predictable. The quality of policy development is frequently negatively impacted by economic, political, or institutionally sourced influences that bring about marginal, if any, adjustments to the status quo.

Where to Next?

Technology and the social systems it interacts with are fundamentally entangled. Development in one may interact with the other to bring about change in ways that cannot be predicted from prior experiences and rules that have applied in the past. Technologists themselves get it wrong – Gavin Wood (co-founder of Ethereum) has said that while Ethereum had started out as a "bitcoin thing" with an extended scripting language, by the time they'd built it they didn't know what it was exactly and how to think about it.

Such remarkable developments inevitably raise difficult questions. How might a public blockchain ecosystem fit into the established systems of society we are accustomed to as it evolves further? What does it disrupt and what can it confederate along the way? What social forces will drive its shape from this point in time? Should cryptoassets remain moored to a binary financial/non-financial dichotomy or should it be positioned within a larger commercial and institutional context? Should blockchain be portrayed as a competition between centralization and decentralization or, as the cypherpunks might put it, between state-imposed order and libertarian free market ideology?

For the reasons I have touched on above, we need better regulatory solutions that address the underlying potential of the technology in order to facilitate its broader integration into society via genuine innovation. Applying a financial taxonomy based on laws and practices built around what was possible in the 20th century will only get us so far. ■

This article is based on *Rethinking the Regulation of Cryptoassets* by Syren Johnstone (Edward Elgar Publishing), which makes five key proposals for regulatory reform.

區塊鏈出現之前的情況及其重要性

作者：香港大學法學碩士（合規和監管）執行主任 Syren Johnstone

本文是作者「區塊鏈對證券監管的挑戰」一文的第二部份，該文於 2022 年 4 月號發表。

套用一個眾所周知的概念，要知道現在、預測未來，就要了解過去。然而，對於比特幣、乙太坊及隨後出現的所有公開、基於共識的區塊鏈加密資產的過去，大多數人卻不甚了解。正如我上個月在本刊所述，現有的證券法對消費者或金融穩定性的最新感知風險採用漸進式主義的監管。對區塊鏈技術本身及使用該技術衍生出來的產品，缺乏足夠的關注或認識。雖然後者可能包括金融產品，但將公共區塊鏈技術僅用於金融服務，是一個嚴重的錯誤。

概念先例

區塊鏈對不同的人意味不同。區塊鏈本質上是基於密碼學和電腦科學的發展，它是在圍繞電子商務、經濟競爭力、隱私、智慧財產權、出口管制、執法和國家安全的長達半個世紀的辯論中出現的。人們經常聽到這樣的說法：「區塊鏈在比特幣之前並不存在」或「Satoshi Nakamoto 發明了區塊鏈」。然而，這並沒有解釋什麼是貨幣、誰可以創造和交易貨幣，或社會政治鬥爭的非傳統觀點，這些思維在 2008 年 10 月 Satoshi Nakamoto 的論文《比特幣：點對點的電子現金系統》之前已形成了概念基礎。

了解這些先例及當中的問題可以提供重要的洞察力，可加深理解該技術更廣泛運用的可能性，有助對該技術引起的許多法律問題追根溯源及技術應用的持續發展。作為社會的利益相關者，這有助我們理解科技在商業互動、制度安排和社區互動的演變中的潛在作用，這些可能是社會演變的一種機制。重要的是，它還有助於思考為什麼以及如何對其進行監管。

此外，Satoshi Nakamoto 的區塊鏈只是共識機制運作的一種可能性。我們可以找到「無區塊」的區塊鏈例子，以完全不同的方式在網絡中建立信任。這類特徵影響管治、相互可操作性和身份等問題，而這些問題將影響新興加密經濟的形態。

武器技術

區塊鏈源自美國國家安全局的戰場，這個戰場由言論自由和戰爭工具所構成。加密技術在第二次世界大戰後和美蘇冷戰期間被正式列為武器。1975 年，Whitfield Diffie 和 Martin Hellman 發現了分鑰（或公鑰）密碼學，這使得兩個人之間的安全通信成為可能，而無需像其他加密技術那樣要事先見面交換密匙，也無需知道對方的真實身份。因此，對參與通信的另一方的信任，被對加密系統的信任取而代之。

分鑰密碼學組成了一大群人之間基於安全資訊網絡的基礎，這些人不需要互相認識。《新聞週刊》後來把這個發現描述為「一個啟示，一個對帝國的真正打擊」。2009 年 1 月 3 日，比特幣的創世區塊展示了一個以 Diffie 和 Hellman 的加密系統信任為基礎的去中心化工作版本。然而，在 Satoshi Nakamoto 的區塊鏈建立之前，出現了其他需要解決的問題。

1988 年，Timothy May 預見到，讓個人和團體能夠以匿名方式進行交流和互動，將成為社會和經濟革命的基礎。當時的問題是計算能力有限且昂貴，而在公共空間中形成電腦網路所需要的大規模連接尚未以互聯網的形式出現。雖然 cypherpunks 認為加密從根本上講是一種私人行為，是言論自由的表現，但直至 1999 年，對加密技術的控制才被裁定為對言論自由的不可允許的限制（*Bernstein v US Department of Justice*, 176 F.3d 1132, United States Court of Appeals, Ninth Circuit）。Bernstein 案令 90 年代主張使用加密技術保護私隱的公眾辯論達到了巔峰。

電子私隱

到了 80 年代末，有賴於電子支付系統，商品和服務的支付更加自動化。通過電子系統進行消費已經開始成為現實，儘管它仍然是在中心化的基礎上進行。雖然電子支付能更好地控制和保障安全，但與使用紙幣和硬幣的匿名支付系統相比，電子支付也產生了私隱問題，因為協力廠商可以積累付款人和收款人的資料。隨著以電子方式進行對話、電子郵件和互聯網的出現，克林頓政府推動把「Clipper 晶片」安裝於私營企業生產的安全通信產品。

Philip Zimmerman 於 1991 年發表的 Pretty Good Privacy（PGP）密碼系統，是 1990 年代政府監督計劃和私隱辯論的試金石。PGP 容許建立與合法身份分離的全新數碼身份。如果網絡空間身份與合法身份有聯繫，便可以執行適用的法律。然而，在法律身份與網絡空間身份缺乏聯繫的情況下，按照傳統理解和適用的方式適用法律似乎是不可能的。

數碼資訊技術的出現，也促使人們重新評估資訊與價值之間的關係。1980 年代中期，American Information Exchange 出現了，它是一個買賣資訊的平臺。1993 年，Timothy May 推出了他的實驗性資訊市場 BlackNet，以加密方式保護用戶的身份。BlackNet 首次示範了如何在不受監督和匿名的基礎上自由進行交易，代表對國家權威的挑戰，亦對社會構成更廣泛的風險。在 BlackNet 時代，沒有任何保護身份的數字貨幣。Ross Ulbricht 的 Silk Road 是其後出現的例子，它並沒有受到這個缺點的影響。

創造數字貨幣

比特幣不是通過加密環境為經濟行為帶來私隱的先驅。

David Chaum 的 Digicash 是解決私隱問題的一種方法，它使用加密技術來創建數字貨幣 eCash，同時保障消費私隱。eCash 不能獨立作為貨幣使用，需要傳統銀行的參與，因此它仍然是中心化的。1990 年代中期，有些銀行開始使用 eCash，但它從未流行起來，DigiCash 後來申請破產。

1998 年，Wei Dai 提出了 b-money，它是一種電子貨幣，可以在點對點的基礎上創建和轉移，而無需透過傳統的金融仲介機構。Nick Szabo 在 90 年代末創立了 bit gold，它是解決如何創造貨幣這個問題的另一個去中心化答案。Bit gold 以代幣的概念為基礎，而代幣的創造成本很高。與 b-money 一樣，Szabo 說 bit gold 的創立是為了回應「令［法定貨幣］發揮作用所需的信任［...］但法定貨幣的歷史充滿了對這種信任的破壞」。

b-money 和 bit gold 都是對如何創造貨幣這個問題的去中心化答案。有趣的是，大約在同一時間，圍繞著貨幣

取決於集體意向的想法，出現了一場單獨的學術討論。然而，無論是 b-money 還是 bit gold 都沒有真正落實。直至 Cynthia Dwork 和 Moni Naor 提出工作量證明這一概念（它要求發起者進行一定量的運算，也就意味著需要消耗電腦一定的時間）、Adam Back 發明 Hashcash（Hashcash 是一種工作量證明機制）以及 Hal Finney 之後發明了可重複使用的工作量證明，類似 bit gold 的代幣可以創造、檢驗和交換的前景才變得可能，至少在理論上是如此。

也許比創造貨幣更重要的，是 Nick Szabo 觀察到，任何經濟機制都可以在沒有可信仲介的點對點系統的基礎上運行。正是在這一點上，去中心化商業的概念不僅變得可行，而且還對現狀作出挑戰 — 對現狀的挑戰和去仲介化首次以有形的形式出現。

商業新前景

自 80 年代末起，資訊科技進步帶來的其他機會被廣泛討論，包括認為企業結構將變得更扁平化和網絡化，而不是等級化。虛擬組織的概念被探討。電子市場理論假設資訊科技將降低協調成本，導致整體轉向市場（而不是等級制度）以協調經濟活動。這種討論預示著各種社會行為將會去中心化。乙太坊之後出現的分散式自治組織 (DAO)，就是由這些討論而起。

這些討論在很大程度上預視了一場革命，商業可以在沒有傳統參與方的情況下進行。然而，儘管區塊鏈所帶來的知識遺產非常豐富，這些概念指向了更好的社會和經濟活動機制，但政策制定者的回應通常要簡單得多。一方面，大多數公共區塊鏈加密資產均被連結至對消費者保障的關注，或對「中央銀行作為公眾信任的管理者所發揮的重要作用」的威脅（根據 BIS 總經理在 2018 年的說法）。最近 (2022 年 4 月)，歐洲中央銀行執行委員會一名成員重申了這個觀點，他把加密資產比喻作 Wild West（這個比喻並非完全不公道）以及 2007 年的次貸危機，但卻忽略了 Wild West 誕生了全球第五大經濟體 - 加州以及次貸危機發生在受嚴格監管的銀行業。或許更平衡的說法應該是 Christine Lagarde 在 2018 年強調指出的，需要區分真正的威脅和不必要的恐懼，並在不妨礙創新的情況下防止風險。

因此，雖然對現狀的挑戰是顯而易見的，但反應也是可預測的。政策制定經常受到經濟、政治或體制的負面影響，這些影響對現狀的調整卻微不足道。

何去何從？

區塊鏈為了金融目的而發展不無好處。它為進一步完善技術和解決問題，如速度、可擴展性和相互可操作性等，提供了背景。行業規模的普遍增長，意味著更多人力資源會被吸引加入該行業，他們擁有必要的編程技能和推進技術更新、更好、更深刻地發展的想法。隨著這一趨勢的持續，技術和資本（包括財政和人力）資源的限制將越來越少，而更多地是關於這些資源的界限、由誰來設立界限，以及為了什麼目的設立界限。

科技與社會系統是糾纏在一起的。其中一方的發展可能與另一方產生相互作用，帶來無法從以往經驗和規則中預測到的變化。科技專家們也會犯錯 — 乙太坊的聯合創始人 Gavin Wood 曾說過，雖然乙太坊一開始是帶有擴展指令碼語言的「類似比特幣的東西」，但創立時他們並不知道它到底是什麼，也不知道應該如何看待它。

這種發展無可避免地引起了一些複雜的問題。隨著公共區塊鏈生態系統的進一步發展，它將如何融入我們習慣的社會既定體系？它會擾亂什麼，又能與什麼結盟？什麼社會力量會推動它的形成？加密資產應該繼續停留在金融 / 非金融的二元對立中，還是應該將其放在更大的商業背景中定位？區塊鏈應該被視為中心化和去中心化之間的競爭，或者正如 cypherpunks 所言，是國家強加的秩序與自由市場之間的意識形態競爭？

基於上述原因，我們需要更好的監管方案，解決該技術的潛在問題，以便它更廣泛地融入社會。運用 20 世紀的法律和實踐的金融分類法，將會令我們裹足不前。■

本文以 Syren Johnstone 的《*Rethinking the Regulation of Cryptoassets*》（Edward Elgar Publishing）為基礎，當中對監管改革提出了五個關鍵建議。