RISK MANAGEMENT OF CRYPTOCURRENCY
加密貨幣的風險管理

RMBI NEWSLETTER
風險貳訊

ISSUE 19 | MAY 2021
INTRODUCTION 簡介

Jiwon PARK, Anne (Year 3, 三年級學生)
Advitiya GOYAL (Year 3, 三年級學生)

Chinese translation 中文譯本:
Enoch WONG 王珞心 (Alumni 校友)
Ka Chung LI, Peter 李嘉聰 (Year 3, 三年級學生)

In December 2017, the price of a Bitcoin skyrocketed to about $20,000 and instantly everyone, from high school students to major banks, was discussing ‘crypto’. There is no doubt that blockchain technology is revolutionary, but the question remains whether it is still a viable investment, and if so, what type of investment it is. Presently, all cryptocurrencies are highly volatile, this is due to various reasons like inconsistencies in legislation across countries, speculation and technological challenges to list a few. This article aims to lay out the risks resulting from these various factors and offer insights into how they may be mitigated.

For readers who may not be familiar with the apparent otherworldly workings of cryptocurrencies, refer to the infographic below for a basic idea.

2017年12月，比特幣價格飆升至約20,000美元，令「加密貨幣」成為每個人都在討論的話題。毋庸置疑，區塊鏈技術是革命性的，但問題在於它現時是否一個可行的投資項目？若是，那又會是什麼類型的投資？ 目前，所有的加密貨幣都是高度波動的，造成這種狀況的原因有多方面，包括各國法律不統一，以及存在投機投資和技術挑戰等等。本文旨在分析這些因素造成的風險，並提供有關如何減輕風險的見解。

如果你不了解加密貨幣的運作機制，可先參閱以下圖解，以了解其基本概念。

What is Cryptocurrency?

Cryptocurrency is digital money created from code. The cryptocurrency economy is monitored by a peer-to-peer internet protocol. Cryptocurrency is an encrypted string of data or a hash, encoded to signify one unit of currency.

Source 資料來源：" BLOCKCHAIN INFOGRAPHICS: The Most Comprehensive Collection ” Blockgeeks.
INSURANCE

A great proportion of risk in the cryptocurrency market can be attributed to a lag in supply in insurance of crypto assets. It is not that insurance companies do not insure intangible or digital assets, but that there are no valuation methods that have proven to be reliable over time. Insurance companies will value cyber insurance by estimating the cost of recovery of the affected data or systems of the insuree. Cryptocurrencies, on the other hand, have a lot of unanswered questions. Most importantly, how vulnerable are crypto currencies? In his famous paper introducing Bitcoin, Satoshi Nakamoto addresses how Bitcoin would uphold privacy by keeping public keys anonymous, making Bitcoin effectively a digital bearer asset which raises issues about asserting ownership. Till custody management issues are resolved, insuring Bitcoin would be like insuring cash. The industry has an even bigger hurdle ahead of itself in the form of decentralized exchanges which could live up to the name "The Cryptocurrency Wild Wild West". Nonetheless, major players in the cryptocurrency market have successfully obtained insurance using institutional custody management solutions. According to Thomas Cain, regional director, commercial risk solutions at Aon Financial Services & Professions Group (FSPG), "It is not difficult to assure companies that hold large amounts of crypto assets, but given the newness of the asset class and the publicity some of the crypto breaches have received, applicants need to make an effort to distinguish themselves."

The lag may also be due to the large variety of crypto assets. For example, blockchain networks can mainly be classified as private, public, consortium and hybrid. However, these classes are rather a spectrum, each with its own scalability, level of decentralization and security. The lack of homogeneity necessitates that insurers take into account each characteristic of the crypto-asset or company and the market for crypto insurance has seen slow development. Naturally, building and testing models for effective pricing and valuation takes time. However, no force is stronger than market force. Major crypto assets are increasingly being accepted in the insurance market with an estimated $6 billion of coverage. Nonetheless, this amount is trivial for an asset class where the top three exchanges report trade volumes of over $1 billion daily and the total market capitalization of crypto currencies is over $140 billion. A shortage of insurance underwriters is depriving the cryptocurrencies of the liquidity and investor confidence they need to develop.

风险警訊

香港科技大學 風險管理及商業智能學

保障

加密貨幣市場的大多數風險是因對加密資產（Crypto Asset）的保障需求所產生。保障公司乃為了減少數資產的損失提供保障，但目前尚未有長期可靠的估值方法。保障公司在評估保障的價值時，會估算受保人的受影響數據或系統的復原成本。另一方面，加密貨幣仍有很多未解決的問題，更重要的是，加密貨幣是否很脆弱？中本聰 (Satoshi Nakamoto) 在他的著作《介紹比特幣》中談到了比特幣將如何通過保持公共密鑰（Public key）匿名來保護私鑰，從而使比特幣有效地成為數碼貨幣貨資，同時亦產生了確定所有權的問題，在託管管理問題解決之前，為比特幣提供保障有如為現金提供保障。銀行業更大的障礙是去中心化（Decentralised）交易所，這將是名副其實的「Cryptocurrency Wild Wild West」。

但是，市場上的加密貨幣主要參與者，已利用機構託管管理而成功獲得保障。怡安（Aon）的亞洲金融服務和專業業務部商業風險領域顧問 Thomas Cain 表示：「向擁有大量加密資產的公司提供保障並不困難，但是對於資產類別的新穎性和加密漏洞，申請人需證明自己與其他人不同。」

加密資產種類繁多亦是導致保險業在加密資產保障需求後的原因，例如，區塊鏈一般可分為私人、公共、財團和混合類型。但是，這些分類的範圍很廣，每個分類都有不同的可擴展性、去中心化程度和安全性，缺乏同質性導致保險公司必須考慮到加密資產公司或公司的每個特徵，令加密貨幣市場出現緩慢發展。建立和測試有效的定價模型和估值亦需要時間。不過，沒有任何力量比市場力量更強大。保險市場對主要加密資產的接受度不斷提升，估計保障額達60億美元，但加密市場總資產超過1400億美元，而且三大加密資產的每日交易額超過10億美元，因此相比之下，這個保障額可謂微不足道，在保險承保商短缺的情況下，削弱了加密貨幣的流動性及投資者的信心，但這些都是發展加密貨幣所必需的。
MARKET RISK

The present number of crypto currencies available to the public stands at over 3,600 (compared to 180 fiat currencies). There is evidently a very low barrier of entry but unfortunately the same cannot be said about exit from the market. Of all the cryptocurrencies in existence, only a select few have been able to provide a level of liquidity that meets the average investor’s basic requirements of easy, quick and low-cost transaction. Illiquid cryptocurrencies then have very narrow exits because of non-convertibility between such cryptocurrencies. As investors look for ways to exit the market, they will experience downward price pressure which is especially dangerous with the completely mark to market and volatile nature of cryptocurrencies.

Any person with a basic knowledge of risk management or finance would understand the importance of ‘diversifying’ one’s assets. Historically, cryptocurrencies have been shown to be unrelated to the traditional economy and rather strongly positively correlated with each other. According to research conducted by Binance in January 2020, the average correlation between the market capitalisations of leading altcoins (cryptocurrencies other than Bitcoin) in 2019 was 0.7. This means a portfolio of various cryptocurrencies is extremely susceptible to major swings that can be brought on even by the most minor of fluctuations. A market as volatile as that of cryptocurrencies and the narrow exits can have serious implications for investors.

The above charts show the market capitalization of Bitcoin and that of the entire cryptocurrency market. Not only does this illustrate the domin ance of Bitcoin in the cryptocurrency market, it also shows the strong relationship between them.

However, the future holds promise. Despite the large number of cryptocurrencies and their correlations, as time passes and the cryptocurrencies reach their plateau of productivity in the hype cycle, individual cryptocurrencies will have achieved their specialized utility and come into their own as an asset. Hopefully, they can move from their present position as reductive representatives of blockchain technology to being valued for their specific function and reducing, if not eliminating, their correlation as well as the excessive number of altcoins.
MACROECONOMY
In some ways, cryptocurrencies carry less risk than traditional investments. Compared with fiat currencies, the supply of which is directly dependent on economic and political circumstances, the supply of cryptocurrencies follow an algorithmic model. The amount of cryptocurrencies that will be in circulation at a given time can be predicted with certainty. Owing to the independence of supply from political and economic factors, it has been widely claimed that Bitcoin can act as a hedge against the traditional economy, and it would perhaps be an interesting avenue for investors but the evidence to support the claim is mixed which could rightly be construed as lack of correlation.

宏觀經濟
在某些方面，加密貨幣帶來的風險要比傳統投資少。法定貨幣的供應直接取決於經濟和政治環境。相反，加密貨幣擁有程式供應模型。我們可以確切地知道在特定時間將有多少加密貨幣流通。由於加密貨幣的供應，獨立於政治和經濟因素，人們普遍認為，比特幣是對沖傳統經濟的一種手段。這也許是一個有趣的途徑，但缺乏相關性。支持這一說法的證據參差不齊。

TECHNOLOGICAL RISK 技術風險
As investors’ demand for cryptocurrencies increases, the pertinent technological structure poses new risks ranging from a loss of monetary value, custody management issues, and cybersecurity breaches.

隨著投資者對加密貨幣的需求增加，相關的技術結構帶來了新的風險，包括貨幣價值損失、存在託管管理問題和網絡安全漏洞等。

LOSS OF MONETARY VALUE
In order to facilitate cryptocurrency exchange, information about digital transaction is combined into blocks of data, eventually creating what we call a “blockchain”. Blockchain technology provides transparency for trading parties, winning the attention of (a new generation of investors in) the digital era. However, cryptocurrency’s dependence on blockchain technology results in the potential risk of a loss of monetary value. From a technical standpoint, blockchain faces the possibility of becoming obsolete, which would cause the cryptocurrency to lose its entire monetary value. In essence, if a blockchain becomes outdated, the monetary value of the cryptocurrency will be lost.

貨幣價值損失
為了促進加密貨幣的交易，有關數碼交易的信息合併為數據塊，最終創建了我們所稱的「區塊鏈」。區塊鏈技術支援交易方具有透明度，在新數碼時代贏得了關注。但是，加密貨幣對區塊鏈技術的依賴導致潛在的貨幣價值損失風險。從技術角度而言，區塊鏈面臨過時的可能性能導致加密貨幣不再持有貨幣價值。本質上，如果區塊鏈過時，將會丢失加密貨幣的貨幣價值。
CUSTODY MANAGEMENT

Another technological risk emerges from the issues of custody due to the absence of a central authority. Taking Bitcoin as an example, for every transaction on the network, public keys create addresses while private keys authorize transactions. To unlock cryptocurrency functions, the investor must hold a private key. This key then acts as the proof of ownership and whoever possesses the private key has ownership. Losing the private key either digitally or physically would mean the owner cannot reclaim the value of the cryptocurrency. In fact, if a private key is lost, the associated cryptocurrency value may never be retrieved. For conventional markets, asset management firms’ role is to protect their customers’ assets. In cryptocurrency exchanges, utilizing a blockchain not only removes that broker or middleman in a transaction, but also eliminates a central manager or authority who, in traditional settings, can regulate the market. In other words, with cryptocurrencies, no one performs the role of managing assets, and traditional custodians such as bankers lack expertise in public-key cryptography or crypto assets.

CYBERSECURITY

Due to the network governance model of blockchain technology, investors face unique, although rare, challenges that threaten the security of cryptocurrency. The network governance model describes a process in which validating transactions require a majority of miners to reach an agreement to do so. Under a hypothetical situation where a cryptocurrency network contains a relatively small number of participants, a group of users acting in unison can recall or disrupt transactions if they constitute 51% of the platform. This scenario, called a 51% cyber control attack, occurred in 2018 when an attack drained $550,000 USD worth of ZenCash currencies from exchanges. Another type of attack is the sybil attack, commonly present in peer-to-peer networks, this is when a single node feigns to assume a large number of identities or nodes. These events are difficult to contain without compromising the nature of blockchain technology in cryptocurrencies.

託管管理

另一個技術風險是由於缺乏中央機構而產生的保管問題，以比特幣作例子，對於網絡上的每宗交易，公鑰 (Public Key) 都會創建交易地址，而私鑰 (Private Key) 則授權交易，要發揮加密貨幣的功能，投資者必須持有私鑰，然後，該私鑰將作為擁有權的證明，擁有私鑰的人將獲得所有權，在網絡或物理上丟失私鑰的可能情況下，投資者無法收回加密貨幣的價值，實際上，如果私鑰丢失，將不能收復連帶的加密貨幣價值。於常規市場中，資產管理公司致力於確保其客戶資產的保管保護，在加密貨幣交易中，利用區塊鏈不但會在交易過程中删除經紀人或中間人，而且缺乏在傳統環境下可以調節損失的中央管理人或機構，換句話說，在使用加密貨幣的情況下，沒有資產管理的角色，而傳統的保管人，例如銀行家，則缺乏公共密鍵密碼學或加密資產的專業知識。

網絡安全

區塊鏈技術的網絡治理模型，令投資者要面對雖然罕見但獨特的挑戰。這些挑戰威脅著加密貨幣的安全性。網絡治理模型描述了一個過程，在該過程中，驗證交易需要大多數礦工 (Miner) 達成共識。在沒有假設的情況下，如果加密貨幣網絡只有相對較少的參與者，而其中一組用戶成為了平臺的51%，就可以聯合取消或干擾交易，這種情況稱為51%網絡控制攻擊，它發生於2018年。當時攻擊從交易所取走了價值5 500 000美元的ZenCash貨幣，另一種可能的攻擊是通常在對等網絡 (Peer to Peer) 中出現的Sybil攻擊，在不損害加密貨幣中區塊鏈技術本質的情況下，要遏制這些事件非常困難。
REGULATORY RISKS 監管風險

Cryptocurrencies are exchanged globally without a central authority controlling the means or regulations. In fact, the absence of control is the cause of the emergence of political and regulatory risks for cryptocurrencies. For every distinct protocol, each country perceives cryptocurrency and its influence from contrasting viewpoints, which foreshadows the risk of political dispute and legality issues. Some countries do not recognize virtual currencies as legitimate while others welcome blockchain technology in business. As previously explained, there are multiple issues in response to the lack of regulation, such as the increased technological risk of information theft and cyber breaches. However, a range of alarming legal risks have emerged as well. One of the concerns raised by officials includes the manipulation of cryptocurrencies to evade tax responsibilities. By employing cryptocurrencies as means of payment, taxes may be incorrectly categorized and assessed, increasing the risk of tax evasion. Cryptocurrencies introduce new methods to conceal the actions of money laundering, fraud, and other cybercrimes. Blockchain could also heighten the legal risks of being unable to nullify smart contracts, leading to an ambiguous legal status. In truth, the scope of and demand for cryptocurrencies continues to grow, while loopholes are exploited.

加密貨幣在沒有中央機構或法規監管下，在全球範圍內交易。實際上，缺乏控制會衍生出加密貨幣的政治和監管風險，對於每個不同的加密貨幣協議，每個國家都會有不同的觀點理解加密貨幣及其影響。這預示了會產生政治爭議和合法性問題方面的風險。一些國家並未正式將虛擬貨幣列為合法，而另一些國家則歡迎在商業中使用區塊鏈技術。如前所述，由於缺乏監管，出現了多個問題，例如信息竊竊和網絡入侵的技術風險增加。但是，加密貨幣也會產生一系列的法律風險，官員們提出的擔憂之一包括透過操縱加密貨幣以逃避稅務責任。透過使用加密貨幣作為支付手段，可能會錯誤地分類和評估稅收，從而增加了逃稅的風險。加密貨幣引入了新的方法來掩蓋洗黑錢、欺詐和其他網絡犯罪行為。區塊鏈還可能增加無法取消智能合約(Smart Contract)的法律風險，從而產生誇張性的法律地位。實際上，在漏洞被利用的同時，加密貨幣的範圍和需求繼續增長。
The truth is crypto assets are an entirely new asset class with very few similar attributes compared with traditional assets. It is only fair to assume that a radical change in type of investment would lead to a change in risk management strategies. The financial theory of the traditional market is based on economics and assumptions that need not necessarily stand in the crypto world. As a taste, consider the distinct possibility that the total supply curve for an entire currency is perfectly inelastic as would be the case for inflation neutral cryptocurrencies, what implications might that have for the cryptocurrency market and the valuation of an asset? Even more fascinating, and cryptocurrencies’ unique selling point is the implications of having decentralized protocols. Without effective, or rather reliable, valuation methods extreme volatility may ensue. Maybe the first step is to draw new economic theories using the relatively short period that crypto has been in existence and only then would we be able to ascertain the value of 1 Bitcoin, 1 Ethereum or 1 LiteCoin.

事實是，加密資產是一種全新的資產類別，它幾乎沒有與傳統經濟類似的屬性，我們可以公平地假設，投資類型的改變需要不同的風險管理策略。傳統市場的金融理論是建立在經濟學和假設之上，這些假設在加密貨幣世界不一定成立。例如，考慮一下呈通貨膨脹中性的加密貨幣的情況，在整個貨幣的總供給曲線完全無彈性的特別情況下，會對加密貨幣市場和資產估值產生什麼影響？擁有去中央化的協議，是加密貨幣的獨特賣點，也是其吸引之處，在沒有有效或相當可靠的估值方法下，加密貨幣會出現極大的波動性。也許第一要以加密貨幣所流行的幾年經驗來創立新的經濟理論，只有到那時，人們才能確定一個比特幣，一個以太幣或一個萊特幣的價值。

CONCLUSION 結論

There is no denying that crypto assets have a place in the future and increasing acceptance across industries is evidence of this potential. But cryptocurrencies have a lot of hurdles ahead of them and by extension, so do their investors and stakeholders. As an investment, the increasing acceptance of cryptocurrencies coupled with technological and ideological advancements will certainly help answer some questions about valuation and risk management. However, strategies for managing risk in the crypto world, for now, seems scarce and traditional strategies seem to be ineffective; however, with the development of new economic theories, it may be possible to create models that will enable us to understand crypto assets better.

無可否認的是，加密資產在未來會佔有一席之地，行業接受度不斷提升也印證了這一點。不過，加密貨幣以及其投資者和持份者，仍要面對很多障礙，加密貨幣作為一項投資，其接受程度的提高以及技術和意識形態的發展，將有助解決加密貨幣的疑難並降低其風險，目前，用於管理加密貨幣世界風險的策略看來比較稀缺。而傳統策略看來又不太奏效。但是隨著新經濟理論的發展，也許可以創造出讓我們更加了解加密貨幣市場的模型。
REFERENCES 參考


“Global Charts.” CoinMarketCap, coinnmarketcap.com/Charts/.


ADVISORS 顧問

Prof. Kai-Lung HUI (Program Director) 許佳龍教授
Prof. James Tin-Yau KWOK (Program Co-Director) 郭天佑教授
Prof. Kani CHEN (Program Co-Director) 陳卡你教授
Prof. Jean Jiying WANG (Undergraduate Program Coordinator) 王繼英博士

Risk Management and Business Intelligence Program
The Hong Kong University of Science and Technology

2358 8229
rmbi@ust.hk
http://www.rmbi.ust.hk
hkstrmbi
hkust.rmbi

RMBI NEWSLETTER 風險薈訊

ISSUE 19 | MAY 2021

All contents and information are subjected to copyright protection. Republication, redistribution or unauthorized use of any content is expressly prohibited without the prior written consent.