ON TARGET

e-Mag of the Institute of Certified Management Accountants
March April 2021 Vol 25, No.2

STRATEGY » FINANCE » MANAGEMENT

Money Laundering: Traditional vs. Digital:

Key Lessons for Bankers and Finance Professionals

CMA AUSTRALIA Certified Management Accountants

ICMA COUNCIL

Chairman
Prof Michael Tse
BA, MCom, PhD, FCMA

President
Prof Brendan O'Connell
PhD, CA, CPA, FCMA

Vice President
Mr David Cartney
MA (Hon), CA(Scot), CA(Aust), FCMA, FCPA, FAICD

Hon. Secretary
Mr Hans Ferdinand
BBus(B&F), FCMA

Hon. Membership Committee Chair
Ms Roshani Perera
MBus (Acc), CPA, FCMA

Hon. Education Committee Chairman and CEO
Prof Janek Ratnatunga
MBA, PhD, FCA, CGBA, CMA

Hon. Treasurer and CFO, COO (Int)
Dr Chris D'Souza
BComm, PhD, FCA, FCMA, CPA

Editor and COO (ANZ)
Dr Chintan Bharwada
MBA, PhD, FCMA

Emeritus President
Dr Leon Duval
MBus (Acc), PhD, CA, FCMA

Immediate Past President
Prof Michael Tse
BA, MCom, PhD, FCMA

Web Master
Mr Jehan Ratnatunga
BEng, BCompSc

Education Advisory Board

The Institute's Education Advisory Board provides expert advice on the Professional Education; Continuing Education and Academic Education for Students and members of the ICMA.

Members of the Education Advisory Board are as follows:

Convenor:	
Prof. Janek Ratnatunga	ICMA
Australian Members:	
Prof Garry Marchant	Charles Sturt University
Prof Stewart Jones	University of Sydney
Prof Vincent Chong	University of Western Australia
Prof Nava Subramanium	RMIT University
Prof Lisa McMannus	University of Tasmania
Prof Carol Tilt	University of South Australia
Prof Chris Patel	Macquarie University
International Members:	
Dr Mohd Nor Ismail	Multimedia University, Malaysia
Prof Allen Wong	Peking University, China
Dr Thaddeus Kambani	Institute of Finance and Management PNG
Dr Paulina Permatasari	Parahyangan Catholic University, Indonesia
Prof Zhijun Lin	Macau University of Science and Technology
Dr Josua Tarigan	Petra University, Indonesia
Mr Kapila Dodamgoda	Academy of Finance, Sri Lanka

Membership Advisory Board

The Institute's Membership Advisory Board provides expert advice on the minimum experience requirements requires for entry to the: (1) MAA, CAT, RCA, RBA, GMA, AMA, CMA, FCMA membership certifications; (2) the CGBA and CIPA professional designations; and (3) the Certificates of Proficiency programs. The Membership Advisory Board also provides expert advice on: (1) membership services; (2) industry and government engagement; and (3) the development of Ethical standards.

Members of the Membership Advisory Board are as follows:

Convenor:	
Ms Roshani Perera	
Australian Members:	
Ms. Anna Stamatelatos	
Mr. Darrel Drieberg	
Mr. John Stanhope	
Associate Professor Prem Yapa	
International Members:	
Dr. Fawaz Hamidi	Lebanon
Mr. Christos Ioannou	Cyprus
Mr. Alireza Najjar Sarraf	Iran
Dr Ana Sopanah	Indonesia
Dr. Dennis Tam	Hong Kong
Professor Bambang Tjahjadi	Indonesia
Dr. Joselito Diga	Philippines
Mr. M. V. Jayafar	UAE
Mr. Asite Talwatte	Sri Lanka
Dr. Ridzwan Bakar	Malaysia
Dr. Simon Mhpeo	Papua New Guinea

Contents

MONEY LAUNDERING: TRADITIONAL VS. DIGITAL: KEY LESSONS FOR BANKERS AND FINANCE PROFESSIONALS

Prof. Janek Ratnatunga
CEO, ICMA Australia

Introduction

Money laundering is the process of making illegally gained proceeds ("dirty money") appear legal ("clean"). In a number of legal and regulatory systems, however, the term money laundering has been extended to other forms of financial and business crimes, and is sometimes used more generally to include the misuse of the financial system (involving things such as securities, digital currencies, credit cards, and traditional currency), including terrorism financing and evasion of international sanctions. Most anti-money laundering laws link money laundering (which is concerned with *source* of funds) with terrorism financing (which is concerned with *destination* of funds) when regulating the financial system.

Typically, money laundering involves three steps: '*placement*', *'layering'*, and *'integration'*.**[1]**

First, the illegitimate funds are introduced into the legitimate financial system (placement). Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts (layering). Finally, it is integrated into the financial system through additional transactions until the "dirty money" appears "clean (integrated).

The 'placement' of dirty money can take several forms, although most methods can be categorised into one of a few types. These include "bank methods; smurfing (also known as structuring); using legitimate cash businesses (such as casinos); currency exchanges, and double-invoicing". Here are typical types of 'placement'.

- *Structuring:* Often known as *smurfing*, this is a method of placement whereby cash is broken into smaller deposits of money, used to defeat suspicion of money laundering and to avoid anti-money laundering reporting requirements. A sub-component of this is to use smaller amounts of cash to purchase bearer instruments, such as money orders, and then ultimately deposit those, again in small amounts.
- *Cash-intensive businesses:* Here, a business that is typically expected to receive a large proportion of its revenue as cash (such as casinos, distilleries, parking garages, massage parlours and strip clubs) uses its accounts to deposit criminally derived cash. Such enterprises often operate openly to derive cash from its legitimate business, in addition to the dirty cash which the business will claim as received in its legitimate business operations. Service businesses are best suited to this method, as such businesses have little or no variable costs and/or a large ratio between revenue and variable costs, which makes it difficult to detect discrepancies between revenues and costs. For example, in the case of a casino, an individual can walk in and buys chips with illicit cash. The money is now 'placed'. The individual will then play for a relatively short time using a few of the chips, cashing in the remaining chips, and

taking the payment in a cheque (or at least get a receipt so they can claim the proceeds as gambling winnings).
- *Bulk cash smuggling:* This involves physically smuggling cash to another jurisdiction and depositing it in a financial institution, such as an offshore bank, with greater bank secrecy or less rigorous money laundering enforcement.

The following methods of 'placement' are used when a corporate entity is used either knowingly or unknowingly:

- *Shell companies and trusts:* Trusts and shell companies disguise the true owner of money. Trusts and other corporate vehicles, depending on the jurisdiction (such as in the State of Delaware, USA), need not disclose their true, beneficial owner. Such companies are sometimes referred to as *ratholes*.
- *Round-tripping:* Here, money is deposited in a controlled foreign corporation offshore, preferably in a tax haven where minimal records are kept, and then shipped back as a foreign direct investment, exempt from taxation. A variant on this is to transfer money to a law firm or similar organisation as funds on account of fees, then to cancel the retainer and, when the money is remitted, represent the sums received from the lawyers as a legacy under a will or proceeds of litigation.

Other methods of money laundering are as follows:

- *Buy Real Estate:* Corporations or individuals purchases real estate with illegal proceeds and then sells the property. The proceeds from the sale look like legitimate income. Alternatively, the price of the property is manipulated: the seller agrees to a contract that underrepresents the value of the property and receives criminal proceeds to make up the difference.
- *Assigning Life Insurance Policies:* The assignment of insurance is the transfer by the holder of a life insurance policy (the assignor) of the benefits or proceeds of the policy to a lender (the assignee), for a particular reason such as a collateral for a loan. In the event of the death of the assignor, the assignee is paid first, and the balance (if any) is paid to the policy's beneficiary. In the case of money laundering, a policy is assigned to unidentified third parties and for which no plausible reasons can be ascertained.
- *Trade-based laundering:* This involves under or overvaluing invoices to disguise the movement of money.
- *Black salaries:* A company may have unregistered employees without a written contract and pay them cash salaries. Dirty money might be used to pay them.

The ultimate method to set-up a money laundry is to *Capture a Bank.* Here, money launderers or criminals buy a controlling interest in a bank, preferably in a jurisdiction with weak money laundering controls, and then move money through the bank without scrutiny.

There are many examples from around the world where individuals have started the 'placement' of dirty cash via slot machines; moved on to buy the entire casino to make it easier to 'place' larger sums of dirty cash; then purchased other legitimate businesses to 'layer' the dirty money with the clean money; and ultimately 'integrate' the washed money by purchasing real estate and ultimately, getting a controlling stake in a bank.

In Australia, cash dealers (especially Banks) are required to report international funds transfer instructions (IFTIs) and significant cash transactions (SCTRs) to AUSTRAC electronically rather than on paper, where the cash dealer has the technical means to do so, and their reporting volumes ***exceed 50 forms per year (***all types aggregated). Suspect transaction reports (SUSTRs) may continue to be reported on paper, although this is not AUSTRAC's preference.

In September 2020, AUSTRAC announced that Australia's Westpac bank will pay A$1.3 billion – the biggest fine in Australian corporate history – for its breaches of anti-money laundering laws and for failing to stop child exploitation payments. This follows AUSTRAC's high-profile investigations into the Commonwealth Bank of Australia (See Appendix 1).

In October 2020, it was revealed this week that AUSTRAC was investigating casino operator Crown for potential breaches of Australia's anti-money laundering and counter-terrorism financing laws; especially looking at "gaps" in regulations around casinos and junket operators. The report outlining the money laundering operations of the Crown casino was released in February 2021.**[2]** (See Appendix 2).

Use of Lawyers and Accountants

In October 2020, *media in Australia and USA* revealed how a secretive international operation is targeting dozens of Australian taxpayers who use a Puerto Rican bank, *Euro Pacific*, co-owned by American celebrity business figure Peter Schiff. The reports sparked concerns with Australia's financial crimes watchdog AUSTRAC that lawyers and real estate agents are being used for money laundering. Following this, an investigation was launched by AUSTRAC to track the lawyers and accountants who have recommended to Australians that they use the bank.

There was some evidence that laundered money was being 'integrated' in the trust funds of lawyers, accountants, and real estate agents to buy legitimate assets such as real estate and share investments. Some of these professionals were being unwittingly used to avoid money laundering detection; but there were also those who are intentionally involved in criminal activity.

The revelations sparked renewed calls from financial crime experts for the federal government to introduce long-stalled laws that would force lawyers, accountants, and real estate agents to report their clients to authorities if they move money in a suspect fashion, including offshore. If this legislation is passed it would include a requirement to submit suspicious matter and transaction reports. In 2018, lawyers, accountants and real estate agents successfully lobbied for the regulations not to apply to them.**[3]**

The Importance of Strong KYC Processes

KYC is a term used to refer to the bank and anti-money laundering regulations which governs these activities. KYC processes are being employed by companies of all sizes for the purpose of ensuring their proposed agents, consultants, or distributors are anti-bribery compliant. KYC is the process of a business identifying and verifying the identity of its clients. Banks, insurers, and export creditors are increasingly demanding that customers provide detailed anti-corruption due diligence information.

Financial Institutions employ *Know Your Customer (KYC)* processes to confirm the identity of their customer. These processes typically involve the collection and verification of a customer's personally identifiable information (PII)—including, but not limited to, government-issued ID, phone number, email address, physical address, and more.

Exact KYC requirements vary by jurisdiction, meaning criminals can use *jurisdictional arbitrage* to choose geolocations with lax KYC procedures to further obfuscate their flow of funds. Strong KYC procedures can mitigate money laundering of both Fiat and crypto currencies.

Money Laundering and Traditional banking

In September 2020, a set of documents known as the *FinCEN* files were released in the USA, detailing that the U.S. government has failed to stop some of the biggest banks in the world moving trillions of dollars in suspicious transactions for suspected terrorists, kleptocrats and drug kingpins.**[4]**

Money laundering is more than a financial crime. It is a tool that makes all other crimes possible – from drug trafficking to political crimes. And the unfortunate reality is that it is not only the dubious banks in less regulated countries that make money laundering possible; but also the banks in supposedly highly regulated countries. [See Appendix 1 on Australia's Comm Bank fiasco].

In a detailed expose, *BuzzFeedNews* named several of the most trusted banks that were engaging in money laundering. Current investigations show that even after fines and prosecutions, well-known financial institutions such as *JPMorgan Chase, HSBC, Standard Chartered, Deutsche Bank,* and *Bank of New York Mellon* are all involved in moving funds for suspected criminals.**[5]**

The *Financial Crimes Enforcement Network* ("FinCEN"), an agency within the *US Treasury Department*, charged with combating money laundering, terrorist financing, and other financial crimes. A collection of "suspicious activity reports" offers a window into financial corruption, and how governments are unable or unwilling to stop it. Profits from deadly drug wars, fortunes embezzled from developing countries, and hard-earned savings stolen in Ponzi schemes, all flow through supposedly reputed financial institutions, despite warnings from bank employees.

These reports are available to US law enforcement agencies and other nations' financial intelligence operations. Although FinCEN is aware of the money laundering activities, it lacks the authority to stop it.

The current financial system largely insulates the banks and its executives from prosecution*, so long as the bank files a notice with FinCEN that it may be facilitating criminal activity.* The suspicious activity alert effectively gives the banks a *free pass*. And so, illegal funds continue to flow through banks into various industries from oil to entertainment to real estate, further separating the rich from the poor – while the banks we have grown to trust make it all possible.

According to the United Nations, the estimated amount of money laundered globally in one year is 2 to 5% of the global GDP, or $800 billion to $2 trillion, with more than 90% of money laundering going undetected today.**[6]**

Money Laundering and the Cryptocurrency Industry

Money today is mostly digital. It has been around well before the advent on Bitcoin. Credit card companies have been creating digital money for over 50-years, by giving you a spending limit on your cards. Governments undertake quantitative easing not by printing physical money, but by electronically crediting bank accounts. The problem is the counterfeiting of money. Whilst physical money has quality related barriers that limit counterfeiting, digital money can be copied millions of times without any loss of quality. This is called the "double-spend problem".

The solution was of course a 'centralised solution'; all transactions are recorded in a banks or financial institution's centralised *bank ledgers* that the public has no access to, and therefore cannot duplicate. This is where Digital tokens (cryptocurrencies) which are a new asset class, powered by Blockchain technologies, comes in. One of the early cryptocurrencies using blockchain technology was 'Bitcoin'. A 'Blockchain' is built-up, using a 'Triple-Entry' accounting system. All accounting transactions are recorded in a general ledger (GL). The two standard entries are for receipts (credits) and payments (debits). The third entry, that is unique to a Blockchain is a verifiable cryptographic receipt of the transaction.

As such, unlike a standard GL of today that is kept under the control of one organisation; a blockchain (in its purest form) is a common ledger that is accessible to everyone and controlled by no one. One of a blockchain's distinguishing features is that it locks-in (or "chains") cryptographically verified transactions into sequences of lists (or "blocks"). The system uses complex mathematical functions to arrive at a definitive record of who owns what, when, where and how. Properly applied, a blockchain can help assure data integrity, maintain auditable records, and even, in its latest iterations, render financial contracts into programmable software.

Bitcoins are traded via a *cryptocurrency exchange* that uses an order book to match up buy and sell orders — and thus controls all the funds being used on the exchange platform itself. Bitcoins can also be traded in a *peer-to-peer exchange* where buyers and sellers are match without holding any funds during the trade. All trades are recorded on the blockchain. [See article titled '*All You Wanted to Know About Bitcoin (But was Afraid to Ask)'* in this magazine]**[7]**

Cryptocurrency exchanges and ATMs are examples of *Virtual asset service providers (VASPs)* that conduct one or more of the following activities or operations:

- exchange between virtual assets and fiat currencies;
- exchange between one or more forms of virtual assets;
- transfer of virtual assets;
- safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
- participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Along with the traditional money laundering schemes facilitated by the traditional banks, the cryptocurrency industry has also been criticised for being a tool for money laundering. However, the statistics give a different picture. It is estimated that only 1.1% of all cryptocurrency transactions are illicit. During its early days, Bitcoin was widely associated with the *Silk Road*, an online dark-net marketplace, where users could purchase weapons and illegal drugs anonymously. [More on this later].

Contrary to popular opinion, it is quite easy to link Bitcoin transactions together in order to identify a user. Even though the Bitcoin network is rapidly growing, 42 million Bitcoin wallets and counting, it is becoming increasingly possible with *FinTech* and *RegTech* software to track transactions on public blockchains.**[8]** This should be obvious, considering that public blockchains are totally transparent and browsable by *anyone*, while private banking transactions remain hidden from plain sight.

Still, criminals are constantly caught for using Bitcoin in illicit activities because they do not understand that Bitcoin *is not anonymous*. In fact, there are barely any cryptocurrencies on today's market that are capable of masking identities when sending, receiving, and spending cryptocurrency*, provided the cryptocurrency exchanges have properly followed KYC regulations.* ***This is the key proviso.***

KYC in Virtual Asset Service Providers (VASPs)

As well as all types of online agents, from ecommerce to banking, crypto exchanges must meet the same requirements of all those regulations affecting them on AML (Anti-Money Laundering) and customer identity verification.

The implementation of AML controls and KYC processes is essential for these platforms to operate online with guarantees and security. One can recognise a baseline cryptocurrency exchange when it complies with current regulations and regulatory standards. This implies having established processes and controls oriented towards:

- A KYC (Know Your Customer) process suitable for customer onboarding.
- AML (Anti-Money Laundering) controls and checks.
- A high-security identity verification process.
- SCA (Strong Customer Authentication) protocols on multiple-factor authentication strategies.

Mr. Chanpeng Zhao "CZ", the Founder & CEO of *Binance*, the largest cryptocurrency exchange by volume in the world, was interviewed by *Forbes magazine* to get his take on money laundering both in the traditional and the digital finance worlds.**[9]** He said:

"*We live in a complex world, where one country may view an act as criminal and the other may not. A lot of people have a black and white view, but the world is actually grey. Not all banks are innocent and not all crypto companies are bad."*

"If you are using Bitcoin, it is a transparent ledger. Once you have a few transactions, you can trace the funds all the way back to where the coins were mined. So, in this way, blockchain actually provides a very transparent ledger for everyone to analyse. If you piece together a few data points and do a cluster analysis, it is not that hard for an algorithm to analyse the origin. Privacy coins are harder to track, but their market cap is not that high, making larger transactions more difficult. So, to be honest, it is much easier to make illicit transactions using fiat than using crypto."

He was of the view that the volume of illicit transactions in crypto versus fiat was probably about thousand times less; because any meaningful amount of money is extremely hard to move in crypto anonymously.

"The cryptocurrency market cap is so small, that if you are moving a $100 million dollars, you cannot do so without going through a centralised exchange, making it even easier to trace."

However, despite these strong words rejecting large-scale money laundering using Bitcoins, according to a recent report from *Cointelegraph*, Binance is being sued by the current owners of Zaif, a Japanese cryptocurrency exchange, which was hacked in 2018. The plaintiffs allege that Binance's weak KYC requirements facilitated the laundering of $60 million stolen from the exchange.**[10]**

Notwithstanding the outcome of the Binance case, it is clear that not all crypto exchanges comply in the same way with their responsibilities in terms of compliance. VASPs with strong KYC protocols will know the real identities of users complicit in transactions involving stolen or nefariously gained cryptocurrency. Strong KYC procedures should also prevent bad actors from registering with fake credentials, such as synthetic IDs or stolen identities, making the laundering of cryptocurrency much harder. Weak KYC procedures, on the other hand, can easily lead to a VASP becoming a *go-to location* for criminals either to convert ill-gotten cryptocurrencies into fiat or to use the VASP as a mixing service, allowing criminals to convert coins and sever ties to previous flows of funds.

Methods Used to Launder Dirty Fiat Money into Clean Cryptocurrency

Despite the promise of the open and transparent Blockchain ledger, and the use of *FinTech* and *RegTech* software, there appears to still be ways of turning ill-gotten money in the real world, into clean cryptocurrency. The methods used still follow the traditional money laundering steps of (1) Placement; (2) Layering and (3) Integration. Some of these methods use the 'Dark Web'.

The Dark Web

The dark web was created for people interested in surfing the internet anonymously. Whilst this was useful to escape the oversight and regulation of 'big-brother' governments; some sites within the dark web, unfortunately, also often cater to illegal activity.

The dark web is made up of sites that are not indexed by search engines and are only accessible through specialty networks such as *The Onion Router* (ToR). Often, the dark web is used by website operators who want to remain anonymous. The darknet encryption technology routes users' data through a large number of intermediate servers, which protects the users' identity and guarantees anonymity. Due to the high level of encryption, websites are not able to track geolocation and IP of their users, and users are not able to get this information about the host. Thus, communication between darknet users is highly encrypted allowing users to talk, blog, and share files confidentially. The 'Dark Web' is a subset of the 'Deep Web'.

The dark web itself is not illegal. It offers plenty of sites that, while often objectionable, violate no laws. You can find, for instance, forums, blogs, and social media sites that cover a host of topics such as politics and sports which are not illegal. As such, using ToR to access and browse the dark web is not illegal. What is illegal is some of the activity that occurs on the dark web. There are sites, for instance, that sell illegal drugs and others that allow you buy firearms illegally. There are also sites that distribute child pornography. Visiting these sites, or making certain purchases, through the dark web is illegal.

Bitcoin Mixes (Tumblers)

There are mixing services available to split up Bitcoin (layering), only to reassemble it later (integration). Bitcoin mixers (also known as "tumblers") purportedly clean dirty cryptocurrency by bouncing it between various addresses, before recombining the full amount through a Bitcoin BTC wallet hosted on the dark web, where people can hide their intentions as well as their identity.

A research study undertaken by *Jean-Loup Richet*, a research fellow at *ESSEC*, and carried out with the *United Nations Office on Drugs and Crime*, highlighted new trends in the use of Bitcoin tumblers for money laundering purposes.**[11]**

Tumblers are a little painstaking to use and are not free (standard fees will range from 1-3 percent of the cryptocurrency to be mixed).

Here is how it is done according to David Canellis (2018).**[12]** He says that one would need one Bitcoin wallet hosted on the *'clearnet,'* (a fancy word for the standard internet). Also, one should open two or more Bitcoin wallets that run exclusively on the **dark web** (there are a few of these wallets available, he says, but you need to be careful, he says).

And of course, one needs some Bitcoin to mix.

To start, Bitcoin is sent from a *clearnet wallet* to one of the hidden *ToR* wallets (placement). These kinds of transactions are called 'hops,' and can be done multiple times across Bitcoin addresses on the Dark Web, adding a layer of obfuscation with every 'hop' (layering).

With it stored on a dark web wallet, it is time to run it through a tumbler. There are many mixing services that claim to be reputable, and charge various fees depending on the level of anonymity requested by the user. The tumbler will automatically split the Bitcoin up across multiple transactions, sending it at randomised intervals

to enough ToR-hosted Bitcoin addresses that the ability to link the transactions together in a meaningful way is removed.

Once the tumbling is complete, the Bitcoin is supposedly 'clean' enough to deposit on a cryptocurrency exchange to be traded for other cryptocurrencies, or even fiat currencies (integration).

It should be noted that researchers have studied these mixing services to determine just how effective they are. Unfortunately, they found even the most well-known and established ones had serious security and privacy limitations, highlighting the danger of using such services for criminal activities.**[13]**

Unregulated Bitcoin Exchanges

Unregulated cryptocurrency exchanges (those without Know-Your-Customer and Anti-Money-Laundering (KYC/AML) procedures, such as identity checks) can also be used to 'clean' Bitcoin, even without using a cryptocurrency mixing service beforehand.

This is done by simply trading the Bitcoin a number of times across various markets. For example, a user can deposit onto an unregulated exchange, swapping it for various *altcoins*. Each time a trader exchanges cryptocurrency for another, they are adding degrees of privacy similar to 'hopping' between wallet addresses. Although, how effective this is depends heavily on the exchange's monitoring technology, so this might not be a totally airtight solution.

The user can then withdraw their cryptocurrency to an external cryptocurrency wallet via other anonymous exchange accounts they own. Depending on the exchange, they could convert it to allegedly 'clean' fiat – but fiat markets on unregulated exchanges are hard to come by, and often short-lived.

Researchers have found that unregulated cryptocurrency exchanges receive an overwhelming majority of the internet's dirty Bitcoin. Even worse, the exchanges in countries where there are little-to-no AML regulations receive 36-times more Bitcoin from money launderers than those with appropriate rules in place.

Researchers estimated that *after* Bitcoin has been cleaned on exchanges, 97 percent of it ends up in countries with extremely lax KYC/AML regulations. In 2016, Dutch police swooped on an international money laundering ring, seizing bank accounts, Bitcoin, luxury cars and ingredients for ecstasy.

Peer-to-Peer Markets

A *peer-to-peer transaction* means that you have data related to the person or entity you are always interacting with. Rather than interacting with several different unknown individuals, as in the case of a cryptocurrency exchange, the information you have on a person in a *peer-to-peer market* can range from a bitcoin wallet address to their forum username, location, IP address, or can even involve a face-to-face meeting.

Inevitably, money launderers turn to shady peer-to-peer markets and other nefarious deeds to turn their Bitcoin into cash.

Digital Currency Exchanger

Another related approach was to use a *digital currency exchanger* service which converted Bitcoin into an online game currency (such as gold coins in World of Warcraft) that will later be converted back into money. It is also worth mentioning there are slightly less illegal (but still questionable) uses of these mixing services. In particular, regulated exchanges like *Coinbase* monitor their networks for possible interactions with prohibited cryptocurrency gambling sites. As such, cleaning digital funds exposed to blockchain casinos before depositing to Coinbase and the like is an often-cited use-case, beyond the *ultra-illegal money laundering.*

Recent Research into Digital Money Laundering Activities

Effective *Know-Your-Customer (KYC)* protocols are a vital part of any anti-money laundering (AML) regime. When done right, KYC processes can help financial institutions better understand and manage their risks and prevent money laundering. However, it is one thing to have strong KYC guidelines on paper and another to implement them. By analysing and probing the KYC processes of over 800 VASPs in over 80 countries, an organisation called *CipherTrace* geographically located where weak and porous KYC protocols could be exploited by money launderers, criminals, and extremists.**[14]**

CipherTrace research has discovered that in 2020, 56% of VASPs globally have weak or porous KYC processes, meaning money launderers can use these VASPs to deposit or withdrawal their ill-gotten funds with very minimal to no KYC. The more porous VASPs that allow deposits and withdrawals up to a specified dollar amount with little to no KYC risk of needing to use conventional money laundering

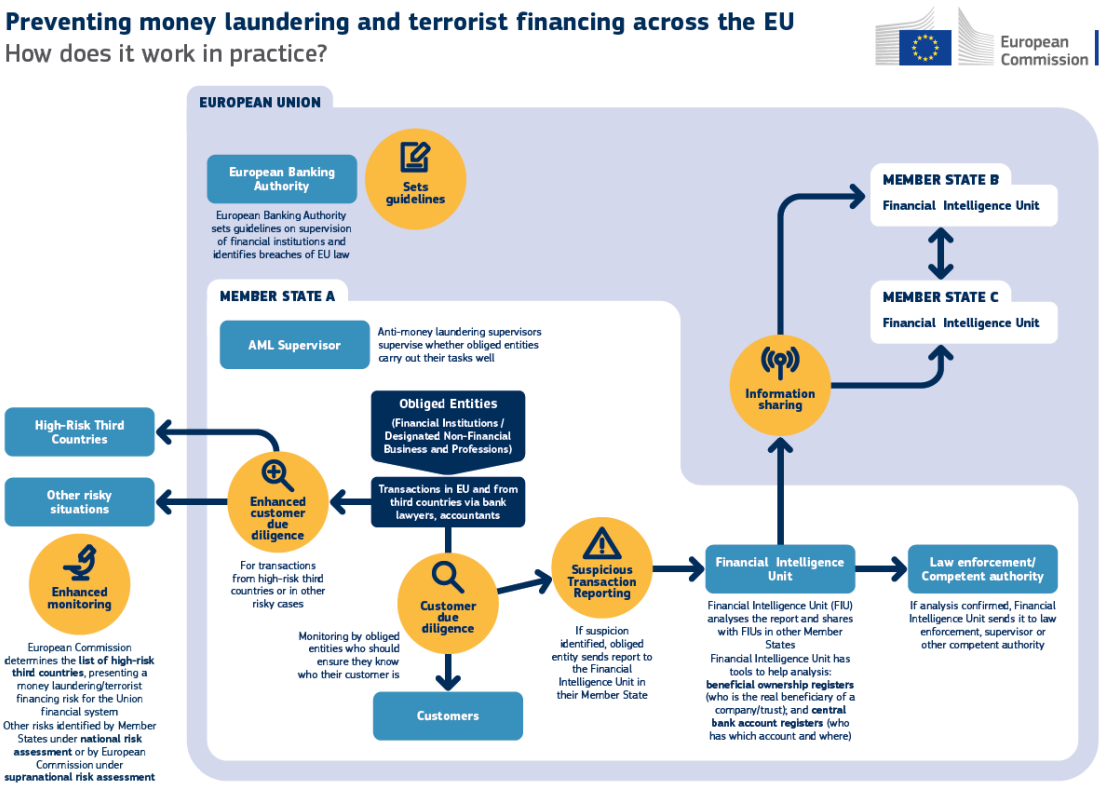


Figure 1

tricks – like structuring to fly under the radar with small frequent deposits.

The European Union (EU) has issued in 2018 the *5th Anti-Money Laundering Directive (AMLD5)* with amendments introduced to better equip the EU to prevent the financial system from being used for money laundering and for funding terrorist activities (Figure 1). Despite this, *CipherTrace* researchers have discovered that Europe has the highest count of VASPs with deficient KYC procedures. Sixty percent of European VASPs have weak or porous KYC.

When looking at the weakest KYC countries in the world, *CipherTrace* analysts discovered that 60% of the top 10 worst KYC countries in the world are in Europe, 20% are in Latin American and Caribbean countries, and the final 20% are in APAC countries. US, Singapore, and UK Host the most VASPs with KYC Deficiencies (see Figure 2).

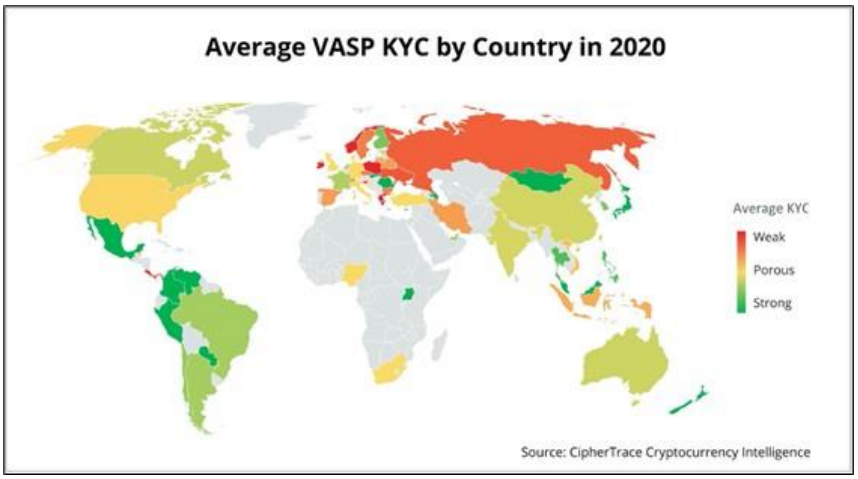


Figure 2

The US, Singapore, and the UK lead as the countries with the highest number of VASPs with weak or porous KYC. Although these regions host a higher volume of VASPs in general, the large count of VASPs in these countries that require little to no KYC demonstrates the ease and volume of potential off-ramps for money launderers.

Three-Quarters of African-Domiciled VASPs with Weak or Porous KYC are Domiciled in the Seychelles.

Decentralised Finance (DeFi)

This is the newest tool in the digital laundry. In contrast to the decentralisation of money through Bitcoin, DeFi aims for a broader approach of generally decentralising the entire traditional financial industry, and would be of particular concern to bankers and finance professionals. The core of the initiative is to open traditional financial services to everyone, in providing a permissionless financial service ecosystem based on blockchain infrastructure.

DeFi is defined as: *"An ecosystem comprised of applications built on top of public distributed ledgers, for the facilitation of permissionless financial services."*

Broadly speaking, DeFi is an ambitious attempt to decentralise core traditional financial use cases like trading, lending, investment, wealth management, payment and insurance on the blockchain. DeFi is based on Decentralised Applications (dApps) or protocols. By running these dApps on a blockchain, it provides a peer-to-peer financial network. Like Lego building blocks, every dApp can be combined with each other. Smart contracts work as connectors — comparable with perfectly specified APIs in traditional systems.

Overall, the blockchain-powered space of *Decentralised Finance (DeFi)* is still nascent but offers a compelling value proposition whereby individuals and institutions make use of broader access to financial applications without the need for a trusted intermediary. Especially people previously without access to such financial services could benefit from this development. At this point in time DeFi is a minuscule format; although there is the promise that it will grow into a full-fledged capital market.

As can be seen, DeFi's permissionless transaction volume creates regulatory risks. The USD value locked in DeFi has grown exponentially in 2020, reaching 16 billion USD. Combine this growth with the fact that DeFi protocols are designed to be permissionless—meaning anyone in any country is able to access them without any regulatory compliance— and it is clear that DeFi has the potential to become a haven for money launderers.**[15]**

Summary

Money laundering risk is a real risk not only in the banking and finance institutions, but also in legal, accounting, and real estate professions. In addition, organisations that deal in large quantities of cash – such as Casinos and Distilleries – need to be aware of the risks posed. These risks are enhanced with the advent of crypto currencies such as Bitcoin.

Frontline officers should be adequately competent in discharging their duties. Even if the banking institutions are equipped with automated risk management solutions, such as *FinTech* and *RegTech*, human expertise and instinct are indispensable in assessing money laundering risk. With the vulnerability of banking institutions in terms of exposure to money laundering in both traditional and digital currencies, satisfactory money laundering risk assessment is vital.

In banking institutions, the frontline officers who are dealing with customers for banking activities such as opening an account, savings, withdrawal and remittance are the frontline of defense responsible to undertake money laundering risk assessment. With the increasing incidence of online banking (even before the Covid-19 lockdowns) the expertise and instincts of a bank manager has been transferred to a computer algorithm. The need therefore to strict online KYC processing is vital in both traditional and digital currency transactions.

Effective Know-Your-Customer (KYC) protocols are a vital part of any anti-money laundering (AML) regime. When done right, KYC processes can help financial institutions better understand and manage their risks and prevent money laundering. However, it is one thing to have strong KYC guidelines on paper and another to implement them.

Further TTR notification is an absolute obligation. The case of the CBA is highlighted in this paper. Once the bank decided to allow cash deposits of more than $10,000 it had to make *absolutely* sure the automatic computer notification triggers worked.

Professor Janek Ratnatunga, CMA, CGMA

CEO, ICMA Australia

The opinions in this article reflect those of the author and not necessarily that of the organisation or its executive.

Appendix 1

Commonwealth Bank of Australia (CBA) Case

In Australia, cash dealers (especially Banks) are required to report international funds transfer instructions (IFTIs) and significant cash transactions (SCTRs) to AUSTRAC (an Australian Federal organisation set up to implement the *Anti-Money Laundering and Counter-Terrorism Financing Act of 2006*). These reports were to be done electronically rather than on paper, where the cash dealer has the technical means to do so, and their reporting volumes exceed ***50 forms per year*** *(*all types aggregated). Suspect transaction reports (SUSTRs) may continue to be reported on paper, although this is not AUSTRAC's preference.

The business news that dominated Australia in early August 2017 was the crisis that hit the Commonwealth Bank of Australia (CBA); which involved allegations of 53,700 contraventions of money laundering and terror financing laws by the Bank. It was alleged that repeated warnings were sent to the bank by the *Australian Federal Police* and AUSTRAC.

Against this backdrop, let us consider what exactly CBA was being accused of. The newspaper headlines screamed "53,000-plus money laundering breaches". Technically, this is correct. There were 53,506 'threshold transaction reporting' (TTR) failures, i.e., the mandatory reporting to AUSTRAC of any single cash deposit of $10,000 or more.

Apparently, the only reason that CBA had so many of these TTR infringements is that back in 2011 it broke ranks with other big banks in Australia and allowed cash deposits of up to $20,000 in its so-called "intelligent" ATMs (IDMs) – other big banks limited such cash deposits (and still limits them) to $5000; and a coding error resulted in not reporting such to AUSTRAC. There were supposedly mass deposits by syndicates, many with fake names, others featuring zombie account owners — flushing hundreds of millions of dollars in cash through CBA smart ATMs, with money then going offshore and in and out of other accounts. The new term *"cuckoo smurfing"* was introduced into banking parlance.

Now the customers of other big banks in Australia were still making a $20,000 deposit "at one time" – they just needed to break it down into (say) four $5,000 successive transactions so as not to be caught by the mandatory TTR reporting to AUSTRAC. However, those "four $5000 successive" deposits *should have*, one assumes, be caught by the separate "suspicious matter report (SMR)" obligations of the banks.

Now it is common knowledge of most Australian businesspeople that cash deposits of more than $10,000 are going to be reported (to someone); and any criminal or terrorist who is dealing in dirty cash will know this in even more detail – and not deposit cash above this limit. This is the reason for also having the SMRs: to pick up deliberate and structuring of cash deposits *below* $10,000. In fact, as AUSTRAC itself has noted, in the CBA case of the 53,506 TTR breaches, only 1,640 related to money-laundering parties, (amounting to $17.3 million); and only a further six might have been considered to be terrorism related. The SMR breaches amounted to 245; where the CBA allegedly failed to lodge a more specific SMR on time or failed to monitor customers.**[16]**

Note that on 23 Sept 2020 — Westpac , another Australian bank, reached a deal with AUSTRAC to settle more than 23 million alleged breaches of anti-money laundering – the largest fine in Australian corporate history.

Appendix 2

Crown Casino Case

In 2019, it was reported in the Australian media that the high-roller room at Crown's Melbourne casino, which was run by the Suncity junket company, was operating "a cash desk" and accepting cash deposits from patrons. In return for bringing high rollers from overseas, junkets were permitted to share in the takings of the casino and often operate their own high-roller facilities within the casino.**[17]**

*In fact, Crown sales staff were told to divide Chinese gamblers into four categories: minnows, catfish, guppies and whales, and offer them gifts, "lucky money" and private jets.**[18]***

Then in October 2019, the ABC TV in Australia aired footage of cash being handed over in the Suncity room in a blue Aldi cooler bag. Cash deposits outside the casino's cage operations, where the identity of patrons and deposits are recorded, raise serious risks of money laundering and of breaching licence conditions.**[19]**

As a result of all this publicity, when Crown wanted a licence for its Casino in New South Wales, the Parliament of NSW set up an enquiry as to its fitness to hold a licence. The result was the *Bergin report*, which was released in February 2021. It which followed a year-long probe into the casino operator; especially its activities in the Casino it was already operating in Melbourne, Victoria. It found there was "no doubt" money laundering involving an international drug trafficking syndicate occurred at the company's Melbourne casino.

The *Bergin report* that showed that the Crown casinos effectively had become bankers to some of the world's worst crime syndicates.**[20]** International gangsters have been using Australia's respectability to turn criminal billions into "clean" money, processed through the gambling tables, that they can then spend and invest with impunity. The Bergin report also found the company "disregarded" the welfare of its staff who were detained in China, accused of illegally promoting gambling in a country where it is illegal to do so. It also said the casino had partnerships with "junket" tour operators linked to organised crime.**[21]**

Even worse was evidence that showed that this Australian Funpark for felons could be open to exploitation by hostile foreign powers. In fact, the *Australian Security Intelligence Organisation (ASIO)* suspected that Crown casino agents gamble cash in Australian casinos to disguise its origin. They could then give it to politicians and political parties as donations or favours, seeking to buy influence. Their aim is not just business favours. Their aim is to turn Australian policy in favour of a foreign government. In short, to subvert Australian sovereignty.

The Bergin report reminds regulators in every country running Casinos that the channels for covert, coercive or corrupt foreign influence remain wide open. The Australia federal agency that tracks illegal money flows, the *Australian Transaction Reports and Analysis Centre*, or AUSTRAC, noted in a December 2020 report that: *"transactions indicate that entities who may be of concern from a foreign interference perspective could be using money held in casino accounts to make political donations with a link to foreign interference."* ***[22]***

The provision of political donations in itself is not illegal in most countries. However, the unusual source of the funds, involving potentially covert international money movement, raises concerns for potential foreign interference. In 2019 alone, Crown's Melbourne casino reported just under 50,000 suspicious transactions to AUSTRAC.

Senators last year demanded to know what AUSTRAC was doing to investigate and enforce anti-money laundering laws. The chief executive of AUSTRAC, Nicole Rose, told a Senate estimates hearing in October that it was "incredibly complex"; pointing out the astonishing fact that AUSTRAC cannot get direct access to casinos' transactions:

"When we go into an enforcement action, we then have to request that information from them – volumes and volumes of data; that's not data that we directly have access to. So, it is a lengthy and complex process."

That is why the Bergin report recommends that the law be changed so that casinos must report their transactions directly to AUSTRAC in future.**[23]**

[1] Janek Ratnatunga (2019), "Anti-Money Laundering Legislations and CFO Responsibilities', *Journal of Applied Management Accounting Research*, Winter, 17 (1), pp.23-26.

[2] Parliament of New South Wales (2021), "Report of the Inquiry under section 143 of the Casino Control Act 1992 (NSW), dated (Volumes One and Two), *House Papers,* Legislative Assembly, February 1st. https://www.parliament.nsw.gov.au/la/papers/Pages/tabled-paper-details.aspx?pk=79129

[3] Anthony Galloway (2020), "Lawyers, accountants and real estate agents should report suspicious activity: AUSTRAC boss", *The Age,* Business, October 23, p.1,28.

[4] Tatiana Koffman (2020), "The Hidden Truth Behind Money Laundering, Banks and Cryptocurrency", Forbes, Sept 27. https://www.forbes.com/sites/tatianakoffman/2020/09/27/the-hidden-truth-behind-money-laundering-banks-and-cryptocurrency/?sh=2ed35c357b37

[5] Jason Leopold; et. al., (2020), "8 Things You Need To Know About The Dark Side Of The World's Biggest Banks, As Revealed In The FinCEN Files' BuzzFeedNews, Sepember 25. https://www.buzzfeednews.com/article/jasonleopold/fincen-files-8-big-takeaways

[6] Op. cit (Koffman, 2020)

[7] Janek Ratnatunga (2021), "All You Wanted to Know About Bitcoin (But was Afraid to Ask)', Tools and Tips, *On Target*, April 5. https://cmaaustralia.edu.au/ontarget/all-you-wanted-to-know-about-bitcoin-but-was-afraid-to-ask/

[8] Janek Ratnatunga (2019), 'The Rise and Rise of RegTech: Does it spell the End of the Annual Audit?", *Journal of Applied Management Accounting Research*, Winter, 17(1), pp. 27-29.

[9] Op. cit (Koffman, 2020)

[10] Andrey Shevchenko (220), "Binance Sued for Allegedly Facilitating Money Laundering with 'Lax KYC'", *Cointelegraph*, September 15. https://cointelegraph.com/news/binance-sued-for-allegedly-facilitating-money-laundering-with-lax-kyc

[11] Richet, Jean-Loup (2013). "Laundering Money Online: a review of cybercriminals methods, *Cornell University*, June, https://arxiv.org/abs/1310.2368

[12] David Canellis (2018), "Here's How Criminals Use Bitcoin to Launder Dirty Money", *The Next Web,* November. https://thenextweb.com/hardfork/2018/11/26/bitcoin-money-laundering-2

[13] ibid

[14] CipherTrace (2020) Geographic Risk Report: VASP KYC by Jurisdiction, *CipherTrace Cryptocurrency Intelligence*, October. https://ciphertrace.com/2020-geo-risk-report-on-vasp-kyc/

[15] Op cit (CipherTrace, 2020).

[16] ibid

[17] Anne Davies (2020), "Crown casino inquiry chair tells CEO money laundering allegations 'extraordinarily troubling'", *The Guardian*, September 23. https://www.theguardian.com/australia-news/2020/sep/23/crown-casino-inquiry-chair-tells-ceo-money-laundering-allegations-extraordinarily-troubling

[18] Nick McKenzie, Nick Toscano and Grace Tobin (2019), "Gangsters, gamblers and Crown casino: How it all went wrong", *The Age,* July 27. https://www.theage.com.au/business/companies/gangsters-gamblers-and-crown-casino-how-it-all-went-wrong-20190725-p52aqd.html

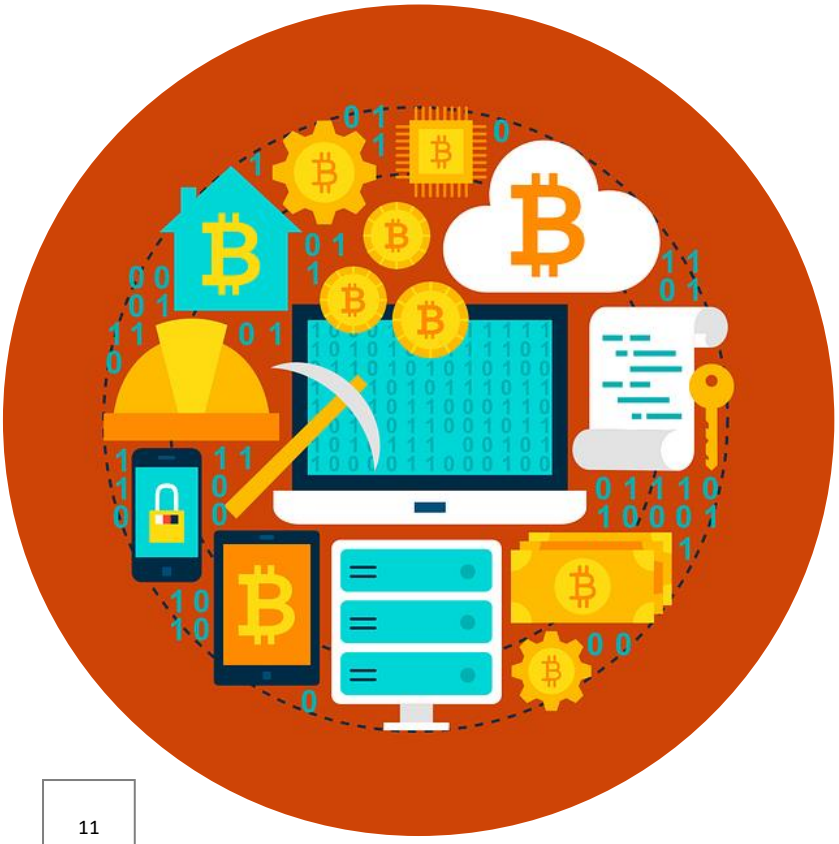
[19] Richard Willingham (2019), "Crown Casino whistleblower alleges gambling giant skirting money-laundering laws", *ABC News*, October 15. https://www.abc.net.au/news/2019-10-15/crown-whistle-blower-fresh-claims-treatment-of-high-rollers/11601232

[20] Op. cit. (Parliament of New South Wales, 2021).

[21] Paul Sakkal (2021), "Andrews urged to launch urgent probe into Crown's Melbourne operation", *The Age*, February 10, Business, p. 1,3.

[22] Anthony Galloway and Patrick Hatch (2020), "Casino junket operators 'exploited, infiltrated' by crime syndicates, foreign spies", *Sydney Morning Herald*, December 11. https://www.smh.com.au/politics/federal/casino-junket-operators-exploited-infiltrated-by-crime-syndicates-foreign-spies-20201211-p56mpl.html

[23] Peter Hartcher (2021), "Australia's fun park for felons leaves the nation vulnerable to hostile foreign powers", *The Age*, Comment, February 16, p. 22.



ALL YOU WANTED TO KNOW ABOUT BITCOIN (BUT WAS AFRAID TO ASK)

Bitcoin, Blockchain, Cryptocurrency…you have heard these terms… what do they mean?

The price of a Bitcoin is currently over A$50,000 … if you do not have such money, can you invest in Bitcoin?

I will attempt to answer all these questions and more. But first, you can invest in a small fraction of a bitcoin – rather than purchase a full bitcoin. Just A$100 can get you on your way. Therefore, if you have some spare cash (and are ready to lose 50% of it) then it is worth dipping your toe into the bitcoin water. After all, if things go your way, you can double your money!

Digital tokens (cryptocurrencies) are a new asset class, powered by Blockchain technologies. One of the early cryptocurrencies using blockchain technology was 'Bitcoin'.

A 'Blockchain' is built-up, using a 'Triple-Entry' accounting system. All accounting transactions are recorded in a general ledger (GL). The two standard entries are for receipts (credits) and payments (debits). The third entry, that is unique to a Blockchain is a verifiable cryptographic receipt of the transaction.

As such, unlike a standard GL of today that is kept under the control of one organisation; a blockchain (in its purest form) is a common ledger that is accessible to everyone and controlled by no one. One of a blockchain's distinguishing features is that it locks-in (or "chains") cryptographically verified transactions into sequences of lists (or "blocks"). The system uses complex mathematical functions to arrive at a definitive record of who owns what, when, where and how. Properly applied, a blockchain can help assure data integrity, maintain auditable records, and even, in its latest iterations, render financial contracts into programmable software. *It is a general ledger on steroids.* ***[1]***

Is Bitcoin Like Money or Like Gold?

In other words, is Bitcoin a *'Store of Value'* or a '*Claim upon a Value'* (i.e., a currency) or both?

Often there is a confusion as to what is a *store of value, and what is a measure* of *value. Money is not a store of value. It is a measure of (or claim upon) a value.*

Let us take a simple example. Imagine a box of Cadbury's chocolates. That box is a *store of value*. If one opens it and eats all the chocolates, it will not only taste good, but also create energy in one's body. Now imagine a piece of paper next to the box that says *'whoever holds this is entitled to claim this box of chocolates'*. That is a *claim upon a store of value*. If a group of people come to believe in the validity of that claim, the note can be passed around as a means of metaphorically 'transferring' Chocolate value, or – more accurately – to transfer access to a box of chocolates. This note is then a form of money (or currency).

The fundamental difference between the 'note' and the actual 'box of chocolates' can be tested by a simple experiment of incinerating them sequentially. Imagine that you incinerate *only* the box of chocolates in a furnace. Nobody can ever eat it now – and you have destroyed its value. The note is simultaneously rendered meaningless, even though it was not incinerated. It is now just a piece of paper saying you can claim a non-existent thing.

Prof. Janek Ratnatunga
CEO, ICMA Australia

Now imagine that instead of incinerating the box of chocolates, you burn the note instead. The box of chocolates remains intact, and no value has been destroyed. All that has happened it that you have destroyed your claim to that value. This is what happens when your wallet gets stolen, or your bank account is hacked. This is also what happened when the Government of India announced the demonetisation of all Rs.500 and Rs.1,000 banknotes in 2016. The' goods' that Indians could buy before they were demonetised remained; but the notes themselves were rendered meaningless.

Let us now scale up this chocolate vs. note scenario. Imagine a nation of people with the energy, intellect, and resources to make things (e.g., China). This is real productive capacity, and it is a source of real value in the form of real goods and real services. Now imagine a piece of paper (e.g., a US Dollar) that says, *'whoever holds this dollar note is entitled to claim goods and services from the people of any nation'*. That is a claim upon value. Now imagine that 1.4 billion people believe in that claim. A network like that is so powerful that it is in nobody's interest to not believe in the claim.

Most financial advisors will caution you about keeping money under the mattress as cash and will almost always advise you to put any excess money you have into a 'store of value' (gold, real estate, bonds, stocks and shares, etc.). This is the entire driving principle behind the *investment* industry. If money itself were the store of value; *investing* in other assets would make no sense. In investing in 'stores of value', it is worth remembering that it is a 'risk vs. return' relationship. Values can appreciate or depreciate.

But what about investing in other currencies as 'stores of value'? Rather than a box of chocolates, you invest your excess Australian dollars (AUD) in US dollars (USD). At the end of a period, the value of your USD could potentially appreciate or depreciate vis-à-vis the AUD; just like any other store of value.

And what about Gold? True that it is clearly a 'store of value' today, but was it not used as a 'currency' in the past? Can it be both? This then is the confusion we have about 'gold' and its modern-day electronic equivalent, Bitcoin. It all boils down to the 'Trust Model'.

Changing the Trust Model

In the old days, people trusted 'Something' like gold or silver for conducting business. These precious metals were used both as *store of value,* ***and*** *as a measure of value.* People went around buying things that were priced in the weight of gold. But this became highly cumbersome; as the gold nuggets had to be cut into smaller pieces to buy minor items. Thus, it became easier to have coins pressed in gold and other precious metals (e.g., silver) that had a specific weight and thus a specific *measure of value*.

However, rather than having to lug around heavy chests full of gold coins to undertake commerce, governments stepped in with printed paper notes with the promise that they could be exchanged for gold. Thus, gold became a 'store of value' that could be exchanged for paper. The 'trust' model had changed from '*something*' to '*someone*'. The 'someone' was the government.

Paper money was issued based on a *gold* standard in which the standard economic unit of account was based on a fixed quantity of *gold*. Each dollar held, entitled the holder to an equivalent value of gold. In the USA, the mined gold was deposited at Fort Knox, and the quantity of US dollars issued was based on these gold reserves. But the USA moved away from the gold standard in 1970; followed by all other countries. These pieces of paper were called *'Fiat'* money, i.e., *by decree*. The pieces of paper were accepted as money, not because you could exchange it for some underlying asset, but simply because the government decreed it to be money.

Such Fiat money, however, had two drawbacks. One, its control was *centralised*; and two, its supply was, theoretically, *unlimited*. Therefore today, a government simply decides how much and when to print and distribute money without basing it on any reserves it holds, be it gold or any other precious metal. During the Covid-19 pandemic, all governments resorted to *quantitative easing*, or colloquially, *money printing*. Paradoxically, in a pandemic and in a global recession, the world is awash with money.

Digital Money and the Double-Spend Problem

Money today is mostly digital. It has been digital well before the advent of Bitcoin. Credit card companies have been creating digital money for over 50-years, by giving you a spending limit on your cards. Governments undertake quantitative easing not by printing physical money, but by electronically crediting bank accounts. The problem is the counterfeiting of money. Whilst physical money has quality related barriers that limit counterfeiting, digital money can be copied millions of times without any loss of quality. This is called the "double-spend problem".

The solution was of course a 'centralised solution'; all transactions are recorded in a banks or financial institution's centralised *bank ledgers* that the public has no access to, and therefore cannot duplicate.

This 'centralised solution' is not without its drawbacks. It can be subjected to *fraud* (e.g., Wells Fargo uncovered 1.4 million fake accounts set-up by employees in 2017); or it can be *mismanaged* (as what happened in the 2008 sub-prime fiasco); or the central authority may simply *cancel* the currency note making one unable to make a claim on a value (as what happened to the Rs. 500 and 1,000 notes in India in 2016).

This is where Bitcoin comes in. It offers a decentralised solution to the "double-spend problem" by using blockchain technology. To take down bitcoin, one would need to take down the blockchain of 1,000s of computers. Also, the transactions are both verifiable and transparent to all. There are no 'coins' in bitcoin, only rows of transactions, which shows the movement of bitcoins between *digital wallets* (see Figure 1). The names of the owners of the wallets remain anonymous to the public, however (more on the extent of anonymity later).

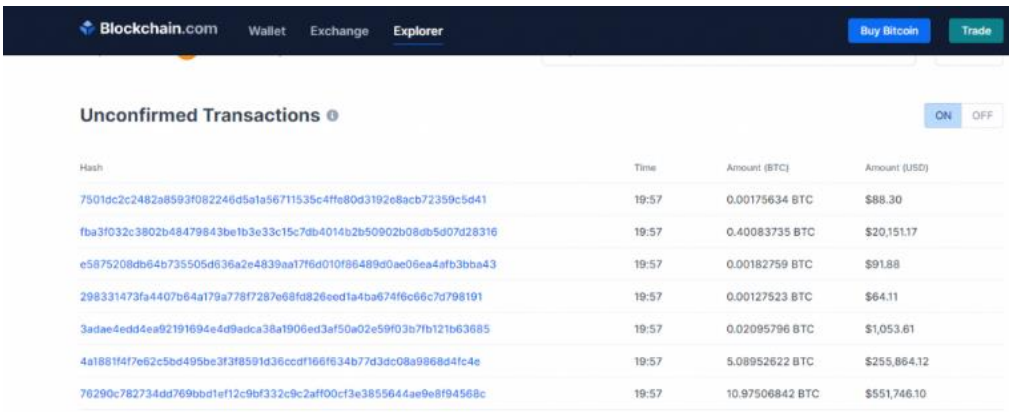


Figure 1: Bitcoin Transactions on the Blockchain

Bitcoin Mining

As discussed above, Bitcoin was conceived as an alternative to Fiat money. As Bitcoin does not have a central government to issue them, it must be mined, just like gold. Bitcoin miners use special software to solve a random maths problem and are issued a certain number of bitcoins in exchange for their effort. This provides a smart way to issue the currency; and creates an incentive for more

people to mine. However, just like the gold mining in the old days; Bitcoin mining is not easy. Gold mining required a lot of pickaxes, muscle-power, blood, sweat and tears. Bitcoin mining requires a lot of computing power, time, energy, and cost. It is estimated that today you need A$50,000 of electricity and computing power to mine one bitcoin, which can anyway be bought over the counter for about the same price!

Further, there has been a limit placed on how much Bitcoins can be mined (just like technically Gold has a finite limit on earth); and therefore, the more miners that join, the harder it gets to actually mine Bitcoins. Once a Bitcoin is mined, it can be either stored in a personal digital wallet (just like gold kept at home), or deposited in a cryptocurrency exchange (very dangerous if kept for long periods).

Every Bitcoin miner is essentially a minor 'banker'. Each time the random problem is solved, and their solution is confirmed by other miners already on the Blockchain network, their coins are registered in the ledger. The successful Bitcoin miner becomes part of the decentralised Blockchain's transaction verification and control network. All new and existing Bitcoin transactions are verified by the Bitcoin miners. See Figure 2.

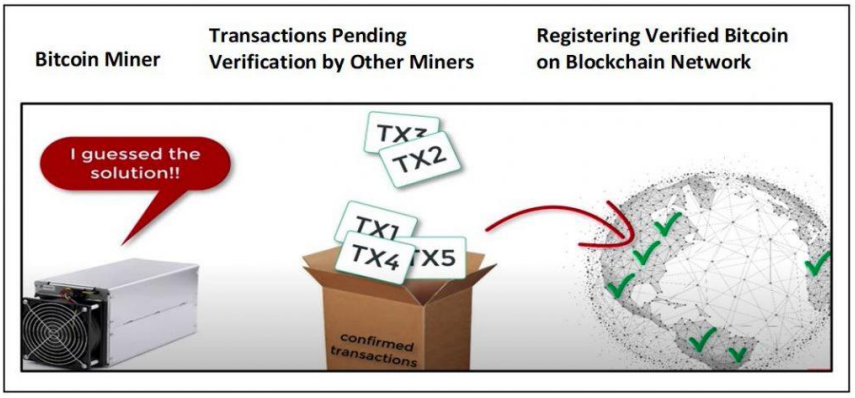


Figure 2: Bitcoin Mining, Verification and Recording on the Blockchain

There are only 21 million bitcoins that can be mined in total. Once Bitcoin miners have unlocked all the bitcoins, the planet's supply will essentially be tapped out. As of February 14, 2021, 18.638 million Bitcoins have been mined, which leaves 2.362 million yet to be introduced into circulation. Of the existing 18.5 million Bitcoin, around 20 percent —worth around US$140 billion in January 2021 — appear to be in lost or otherwise stranded wallets, according to the cryptocurrency data firm *Chainalysis*.**[2]**

Early Bitcoins were both a *store of value* ***and*** *a measure of value,* but the values were extremely small. One could buy a cup of coffee at some restaurants which accepted bitcoins in lieu of cash. There is an urban legend that the first transaction was where two bitcoins were used to buy a pizza. It was a bartering system. The early bitcoins were of novelty value as they could not be converted to cash. Today, bitcoin is the 'internet of money'. [This article will cover next the Buying and Selling Bitcoins, and Withdrawing the Cash by converting Bitcoins].

Buying Bitcoins

Before considering buying bitcoins, the following table comparing a cryptocurrency account as against traditional bank account needs to be understood; and the following equivalencies in terminology should be recognised:

Before one begins, there are several things that every aspiring Bitcoin investor needs:

1. A personal ***Bitcoin wallet*** (to be kept separate to Cryptocurrency exchange account).
2. A bitcoin address (obtained from the wallet)
3. A cryptocurrency exchange account.
4. Personal identification documents (if you are using a *Know Your Customer (KYC)* platform).
5. A method of payment.

Note that a cryptocurrency exchange uses an order book to match up buy and sell orders — and thus controls all the funds being used on the exchange platform itself. A peer-to-peer exchange match buyers and sellers without holding any funds during the trade.

Step 1: ***Get a Bitcoin Wallet:***

This manages and stores one's bitcoins. There are many Bitcoin wallets available which you can use to setup a wallet and private key. The **crypto wallet is a program that stores public and private keys** and cooperates with the blockchain to allows users to send and receive digital currency online.

Think of the Bitcoin wallet like a post-box. Anyone can put letters into the post-box (using your public key); but only the postman can take the letters out (using your private key) and then deliver them to a recipient's address. Thus, the public can put bitcoins INTO your wallet using the public key, but only you can take the bitcoins OUT OF your wallet (to sell them; use them to purchase goods or services; or convert to FIAT money) by using the private key.

Traditional Banking	Bitcoin Trading via Cryptocurrency Exchange
Your Account Name (KYC Checked by Bank)	Your Account Name (KYC Checked by Exchange)
Your Bank Account Number	Your Cryptocurrency Exchange's Account Recognition Method (e.g., a number/ an email address/an email case, etc.)
Online Banking: Your 'Username'	Your Bitcoin Wallet Address (called, 'Public Key')
Online Banking: Your 'Password'	Your 'Private Key'
Transactions Verification: By bank staff and Recorded in your Bank's Centralised Ledger	Transactions Verification: By Bitcoin Miners and Recorded in The Blockchain's Decentralised Ledger

The functions of a Bitcoin wallet are for:

- Storing keys
- Digitally Signing Transactions (which require a private key as your digital signature) (see Figure 3)
- Broadcasting Transactions (so that they can be verified by the Bitcoin Miners and entered on the Blockchain Ledger) (see Figure 4).

The main issue in this step is if to use a Software Wallet or a Hardware Wallet. The pro's and con's are as follows:

- *Software Wallets*
  - Run on your computer /Mobile Phone.
  - Good enough for small amounts
  - Free to use.
  - Less secure as linked to the internet.
- *Hardware Wallets*
  - This is a device that connects to your computer when needed only.
  - Good for large amounts.
  - Costs money to buy (AUD $100 to $500)
  - Much safer.

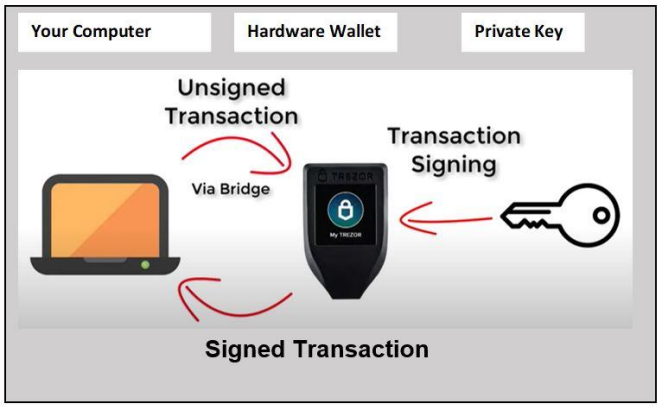


Figure 3: Digitally Signing Transactions

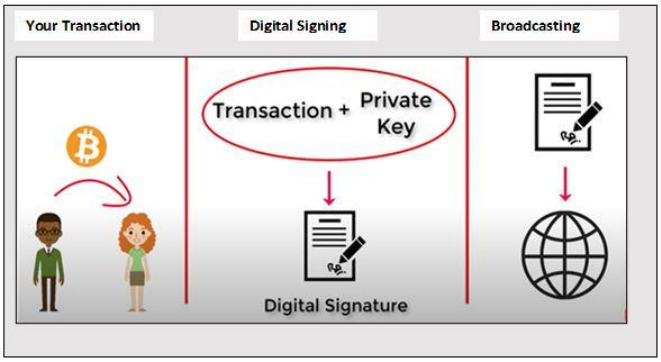


Figure 4: Broadcasting Transactions

Step 2: *Find Your Bitcoin Address.*

Each wallet automatically generates a bitcoin address. This has two parts: A Public and Private Key.

- Your Public key is like your 'user name' in a traditional online bank account.
- Your Private key is like your 'password' in a traditional online bank account.

Public Key

- This is for others to payments to the wallet.
- To get your Public Key, you first must click the Accounts tab toward the top of the screen.
  - This opens your list of cryptocurrency wallets.
  - Your active wallet will have a blue line to the left of the wallet name.
  - To generate your Public Key, click the Receive button.
- You can also find your Bitcoin Cash (BCH) or Bitcoin (BTC) address for receiving payments into your Bitcoin wallet by tapping "Receive" on the bottom toolbar of your hardware wallet.
  - A BTC address is alphanumeric and always starts with a 1 or a 3.
  - Example: This is an example of a receiving address: **3FZbgi29cpjq2GjdwV8eyHuJJnkLtktZc5.**

Private Key

- A Bitcoin private key is a secret number that will enable you to send and receive Bitcoins to and from your wallet.
- Bitcoin wallet has an inbuilt program that will randomly generate a 256-bit long number – This will be your private key.
  - The private key is meant to be secret, hence the word "private" and it is used to send your Bitcoins to another Bitcoin address.
  - Additionally, the private key is a 256-bit long number that *looks something like this* **"5Kb8kLf9zgWQnogidDA76MzPL6TsZZY3.**
- Every Bitcoin wallet can have 1 or more private keys stored within the wallet itself.

Step 3: *Obtaining A Cryptocurrency Exchange Account.*

- Signing up for a cryptocurrency exchange will provide you with an account that will allow you to buy, sell, and hold cryptocurrency. (Find an exchange suitable for your country on Google)
- This cryptocurrency exchange account is like your bank account in a traditional bank, and to set it up you will need to identify yourself and go through Know Your Customer (KYC) formalities (see Step 4)
- However, unlike a personal bank account number, some exchanges (e.g., Coinbase) recognise you via your email address or case number (if you have submitted an email case).
- It is generally best practice to use an exchange that allows its users to also withdrawal their crypto to their own personal wallet for safer keeping (There are many exchanges and brokerage platforms that do not allow this – be cautious of these exchanges).
- Other points to check:
  - Accepted countries.
  - Accepted payment methods.
  - Fees
  - Exchange rate.
  - Buying limits.
  - Reputation.
- An important thing to note when creating a cryptocurrency exchange account is to use safe internet practices.
- This includes:
  - using two-factor authentication and

- using a password that is unique and long, including a variety of lowercase letters, capitalized letters, special characters, and numbers.

Step 4: ***Personal Identification Documents (If Using a KYC Platform)***

- There are many types of cryptocurrency exchanges that exist.
  - The ethos of Bitcoin is decentralization and individual sovereignty.
  - As such, some exchanges allow users to remain anonymous and do not require users to enter personal information.
- Exchanges that allow this operate autonomously and are typically decentralized which means there is no central point of control.
- In other words, there is no CEO and no person or group for any regulatory body to pursue should it have concerns over illegal activity taking place.
- While these types of systems do have the potential to be used for nefarious activities:
  - they also provide services to the unbanked world; i.e., refugees or those living in countries where there is little to no government or banking infrastructure to provide a state identification required for a bank or investment account.
  - Some believe the good in these services outweigh the potential for illegal use as unbanked people now have a means of storing wealth and can use it to climb out of poverty.
- Right now, the most commonly used type of exchanges are not decentralized and ***do require*** KYC (These exchanges include Coinbase, Kraken, Gemini, to name a few).
- Once you have chosen an exchange, you now need to gather your personal documents.
- Depending on the exchange, the information you may need can depend on the region you live in and the laws within it.
- These may include:
  - pictures of a driver's license or passport,
  - social security number (in USA) or other national identification number,
  - information about your employer and source of funds.
  - The process is largely the same as setting up a typical brokerage account in the traditional world.

Step Five: ***Connect to a Method of Payment.***

- After the exchange has ensured your identity and legitimacy, you may now connect a payment option.
- With many of the reputable exchanges, you can connect:
  - To your bank account directly, or
  - To your debit or credit card.
- While you can use a credit card to purchase cryptocurrency, it is generally something that should be avoided due to the volatility that cryptocurrencies can experience.
- It is also possible to get Bitcoin at specialized ATMs and via P2P exchanges (very rare).
- However, be aware that Bitcoin ATMs were increasingly requiring government-issued IDs as of early 2020.

Selling Bitcoins

How to Sell Bitcoin

Cashing out your Bitcoins is not as straightforward as buying them. If you decide to sell your Bitcoins online, you can either do it: (1) Via an exchange; (2) direct trade; or (3) via a peer-to-peer transaction.

Outside of the comfort of your own home, you can: (1) withdraw flat money using a Bitcoin ATM, or (2) sell your Bitcoins in person (p2p).

Selling via an Exchange.

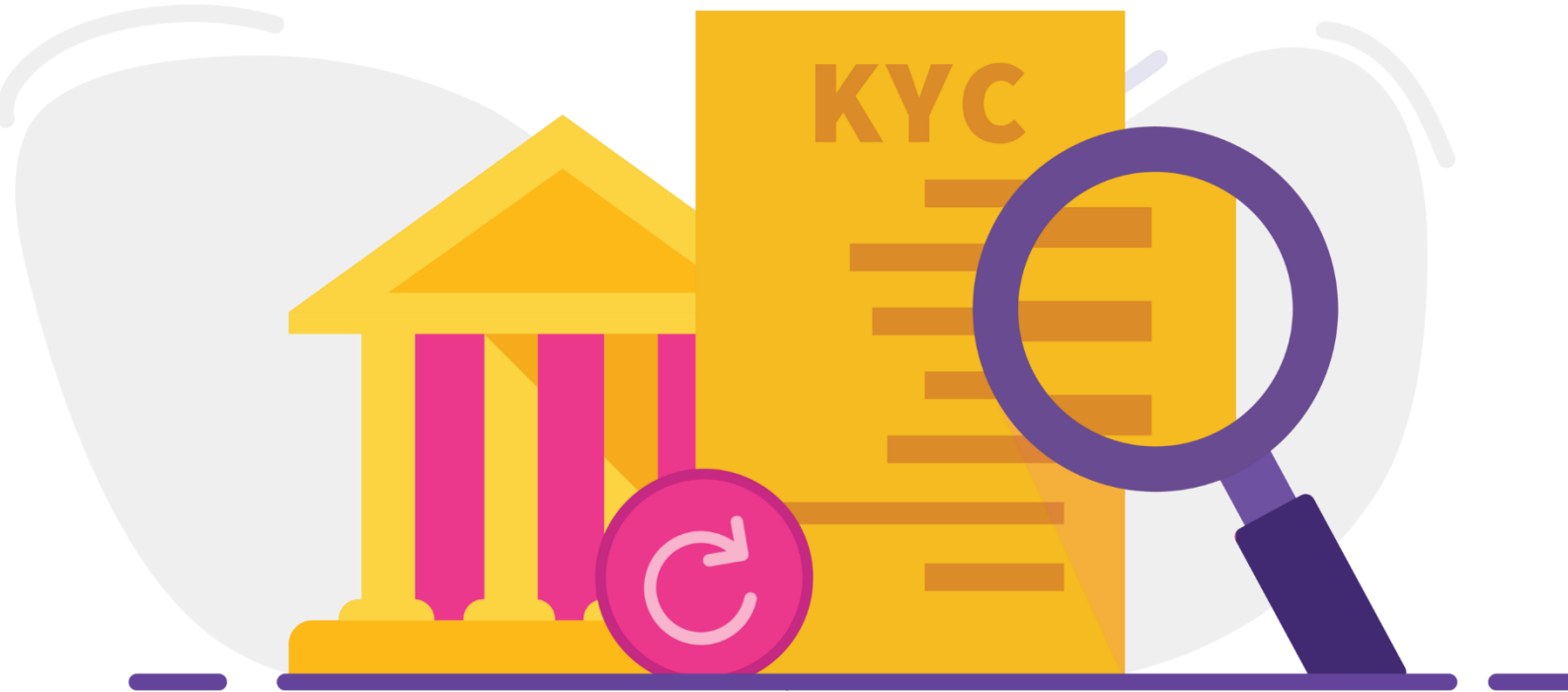
Assuming you already have an account in an Exchange you just simply place a 'sell offer,':

- stating the type of currency that you wish to trade,
- its amount and your asking price per unit.

The exchange will automatically complete the transaction once someone matches your offer.

- After the funds are credited to your account,
- you will need to withdraw them to your connected bank account.

This can sometimes take an excessive amount of time, especially if the exchange is experiencing issues with its banks or facing liquidity problems. Several months before its bankruptcy, the Mt. Gox



exchange was experiencing this exact problem. Moreover, some banks just outright refuse to process transactions with funds obtained via cryptocurrency trading.

It is also important to consider a fee you will need to pay in order to use some exchanges. For example, one of the world's biggest cryptocurrency exchanges **CEX.io** charges:

- a flat fee of $50 for withdrawal via Bank transfer,
- $3.80 if you are withdrawing your funds to a Visa card, and
- 2 percent of a transaction + $3.80 if you are using MasterCard.

The withdrawal fees can vary drastically depending on an exchange, but transaction fees are almost always either tiny or non-existent at all. In addition, most exchanges will have a limit on the amount of money you are allowed to store. The limit will increase over time if you stay loyal to a particular exchange.

Finally, it is important to remember that despite offering wallet services, exchanges are by no means a secure and reliable place to store your funds. They are very prone to hacker attacks, and there have also been instances of exchanges shutting down and running away with their users' funds. Therefore, you should take full responsibility for your own funds and store any amount that is not immediately needed in a secure offline wallet.

Direct Trades

Another way of selling your Bitcoins is via a direct trade with another person. This service is accessible on websites usually associated with exchanges, and includes an intermediary facilitating the connection. The steps are as follows:

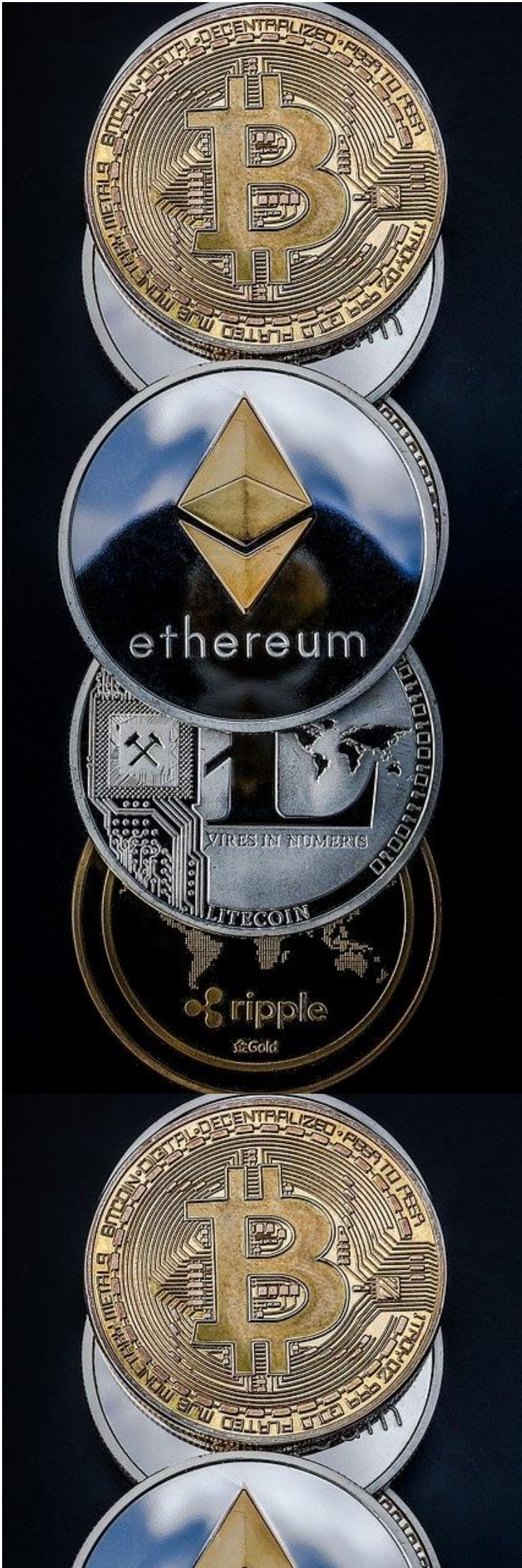
- First, you will need to register as a seller.
- Apart from setting up your profile, you will need to fully verify your identity.
- Once you are registered, you can post an offer indicating your intention to sell some Bitcoins.
- When a buyer wants to trade with you, you get a notification from the service and from then on you are only interacting with the buyer.
- The website merely serves as a platform to complete the trade.

The process of selling Bitcoins on some of those sites can be quite involved and time-consuming. Therefore, it is imperative to do your research before deciding on a trading platform, and to make sure you have the time and patience required.

Some of the websites offering the option of direct trading are BitBargain, Bittylicious, Coinbase, Openbitcoins, Bitsquare and LocalBitcoins.

Online P2P trading

Peer-to-peer trading marketplaces are a relatively new development in the Bitcoin world. There is no direct exchange of funds taking place. Instead, those websites essentially work as a platform that brings people with different, yet complementary needs together.



The service is designed for the mutual benefit of people who would like to:

- Buy Bitcoins with their credit card, and/or
- Spend their Bitcoins to buy goods from places that do not accept digital currencies as a form of payment.
- As a result, the former gets their flat currency exchanged to BTC, while the latter can buy discounted goods.
- The websites facilitating the service provide users with an escrow service for the transaction, as well as a wallet to store Bitcoins.

All of the platforms offering this service are online-based centralized platforms.

- To be able to sell Bitcoins using those services, you will usually need to fully verify your identification, which obviously voids Bitcoin trading off its anonymity.
- Moreover, once you have managed to sell your BTCs, you will need to withdraw them to your bank account or a bank card.
- Often, this process will take an exceptionally long time and will incur some fees.

Here is an example of how it works.

Bob posts his required wish list including the discount amount he wishes to receive, which normally goes up to 25 percent.

- Jack then accepts the trade and pays for Bob's goods through the marketplace, stating Bob's delivery address.
- Once the goods are delivered, the marketplace releases Jack's money from escrow and transfers the funds into Jack's wallet.

While this system allows Jack to acquire Bitcoins relatively easily using just his bank card, it also charges him quite a high fee for the service.

Some of the websites providing this service are Purse, Brawker and OpenBazaar.

Offline Trading.

Two popular offline trading methods are: (1) Bitcoin ATMs; and (2) Selling Bitcoin in person.

1. **Via Bitcoin ATM**

Despite looking like traditional cash machines, Bitcoin ATMs are not ATMs in the traditional sense. Instead of connecting to the user's bank account, they are connected to the Internet in order to be able to facilitate Bitcoin transactions.

- Bitcoin ATMs can accept money in cash and exchange it to Bitcoins given as a paper receipt with a QR-code on it or by moving the funds to a wallet on a Blockchain network.
- They usually charge very high transaction fees – e.g., there are media reports citing fees as high as seven percent.

However, Bitcoin ATMs can be quite difficult to locate. In some countries, this requires a money transmitter license, while current regulations in other countries prevent any Bitcoin ATMs from being installed.

2. **Selling Bitcoin in person**

In many ways, trading digital currency in person is about as easy as it gets. All you need to do to sell your Bitcoins is scan a QR-code on someone's phone and receive cash on the spot.

If you are selling to friends or relatives, you only need to set them up with a Bitcoin wallet, send them the necessary amount and collect your cash. However, if you are dealing with a random person:

- You will most likely go through lengthy rounds of negotiations discussing the price,
- place of meeting and other relevant conditions.

Moreover, you need to take a few things into consideration to ensure your safety and the safety of your funds.

- Verify seller's identity.
- Use Escrow when possible.
- Wait for 3 confirmations before money is released.

Withdrawing Funds

If you are selling Bitcoins online, you will inevitably face the problem of withdrawing funds.

- The most common way to move money is international wire transfer and most prominent exchanges support this method of transferral.
- Recently, however, some exchanges began to accept credit and debit card withdrawals.

Therefore, if you are opening a bank account specifically for withdrawing money made on Bitcoin sales, you need to do your research and chose the bank that best suits your needs.

Summary

I hope all your questions have been answered, and you are ready to dip your toe into the bitcoin water!

[1] Janek Ratnatunga (2020), "Blockchains and the Supply Chain", IN – Ratnatunga, Janek (Editor), *Strategic Management Accounting (4th Edition),* Chapter 15, Quill Press, 310 pp.

[2] Nathaniel Popper (2021), "Lost Passwords Lock Millionaires Out of Their Bitcoin Fortunes", *New York Times*, Jan. 14, https://www.nytimes.com/2021/01/12/technology/bitcoin-passwords-wallets-fortunes.html?action=click&module=RelatedLinks&pgtype=Article

THE TRUE COST OF THE GOVERNMENT'S CHANGES TO JOBSEEKER IS INCALCULABLE. IT'S AS IF IT DIDN'T LEARN FROM ROBODEBT

By Peter Martin, Crawford School of Public Policy, Australian National University

Poor people are different to rich people, and not only in the amount of money they've got. They are also different in something that flows from it.

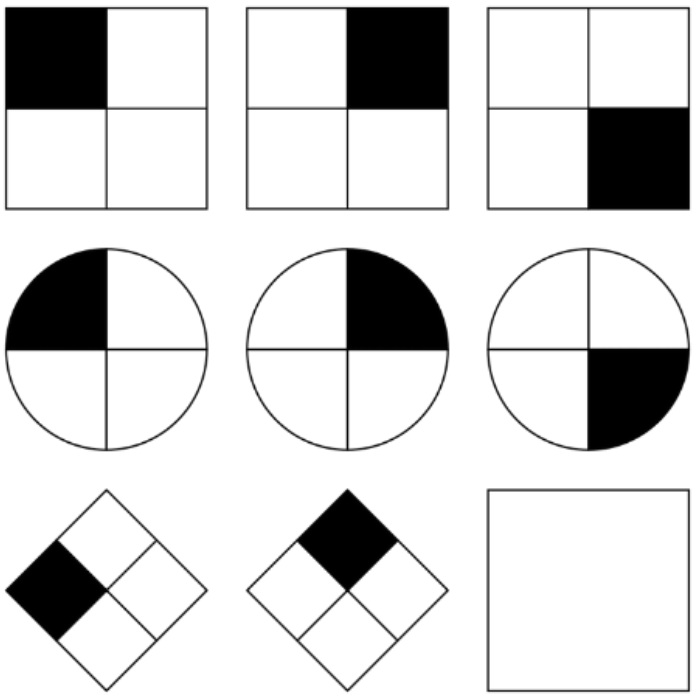
It's (lack of) ease. And the consequences can be severe.

Economist Sendhil Mullainathan and psychologist Eldar Shafir outline these in their book Scarcity: Why Having So Little Means So Much.

They asked shoppers at a New Jersey mall to take part in a so-called fluid intelligence test. Fluid intelligence is problem-solving ability unrelated to language or knowledge.

The test is usually presented as a series of eight images, each different from the one before, followed by an invitation to guess the ninth.

What's in the missing box?



Raven's Progressive Matrices test. LifeofRiley/Wikipedia. CC BY-SA 3.0

It's usually pretty easy. And it was indeed easy for the first half of the shoppers they tested. Comparing the scores against self-reported income, the researchers found no significant differences – "**the rich and poor looked equally smart**".

Just before they presented the first half of shoppers with the test, they also presented a hypothetical scenario:

Imagine that your car has some trouble, which requires a $300 service. Your auto insurance will cover half the cost. You need to decide whether to go ahead and get the car fixed, or take a chance and hope that it lasts for a while longer. How would you go about making such a decision?

For the second half of shoppers they presented the same scenario with just one change. Instead of the car service costing $300, it cost **$3,000**.

The one simple change had a remarkable effect on the test results of just one group of shoppers – those on low incomes.

Although completely fictional, the scenario got them thinking about how they couldn't afford a $3,000 bill from out of the blue. They mightn't know where to find the money.

Instead of performing as well as the high earners (which low earners had done without the $3,000 prompt) they did dramatically worse. Their mental impairment was as bad as if they had lost an **entire night's sleep**.

Stress is costly when ends can't meet

The researchers have replicated the results time and time again. Even when they pay for correct answers (which might be expected to incentivise low earners more than high earners) low earners can't concentrate enough to do well.

The authors' conclusion is that it is incumbent on authorities not to send such people over the edge – not to make them fill in multi-page forms or reapply for assistance or attend recurring pointless meetings, and not to send them unexplained unpayable bills out of the blue – not to do anything that will remind them of how their finances don't really allow them to cope.

When that happens, when what Mullainathan and Shafir call mental bandwidth is flooded, it is hard to think properly about things such as caring for children and getting work.

Australia's treasury gets it. Its well-being framework sets out five points it believes should be considered in designing programs and policies. Point five is the cost to individuals of "dealing with unwanted complexity".

Not so treasury's political masters. When on Thursday the government boosts

JobSeeker by a meagre $25 a week, it will cut the amount job seekers actually receive by a net $50 per week because of the end of the coronavirus supplement.

Mutual obligations impose stress

To offset that generosity – the first real increase in the base rate in 30 years – from April 1 it will ramp up its "mutual obligation" requirements. Job seekers will have to show they have applied for 15 jobs a month, climbing to 20 jobs a month on July 1 – that's a fresh application every working day.

Failures will attract demerit points. Too many demerits and payments will be stopped.

There will be increased auditing of job applications to ensure they are "genuine", a return to the compulsory face-to-face meetings suspended during the pandemic, and a **dob-in line** for employers to report job seekers they think aren't genuine.

The Productivity Commission drew attention to the link between mutual obligation requirements and mental health in its unresponded-to report.

That this will dangerously ramp up stress on the people most susceptible to it, and make it hard for them to do things such as care for their children, ought not to surprise the government.

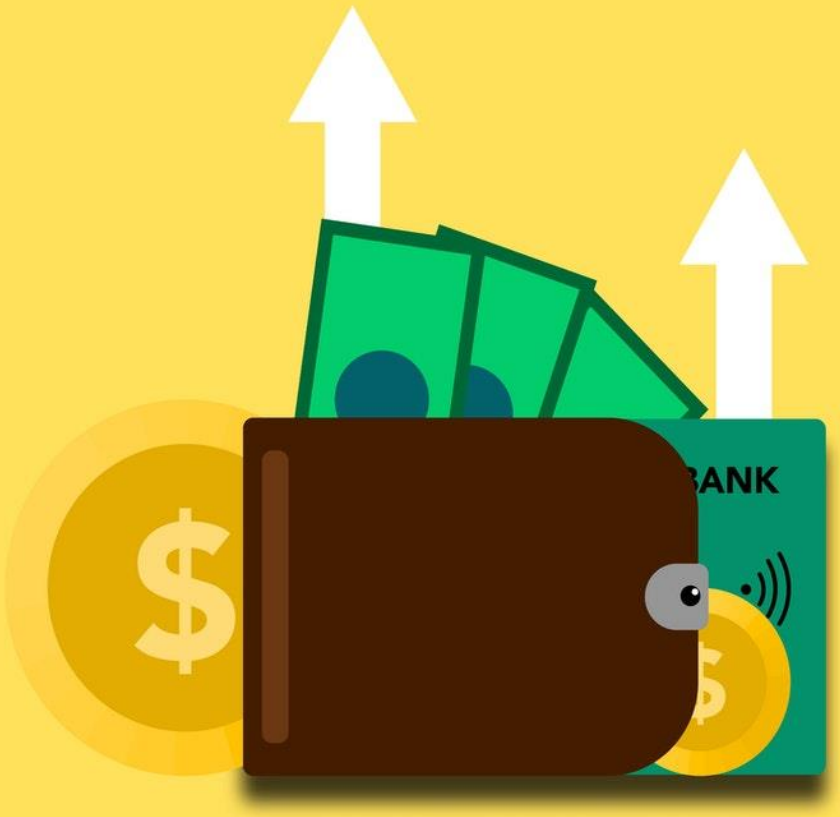
To offset that generosity – the first real increase in the base rate in 30 years – from April 1 it will ramp up its "mutual obligation" requirements. Job seekers will have to show they have applied for 15 jobs a month, climbing to 20 jobs a month on July 1 – that's a fresh application every working day.

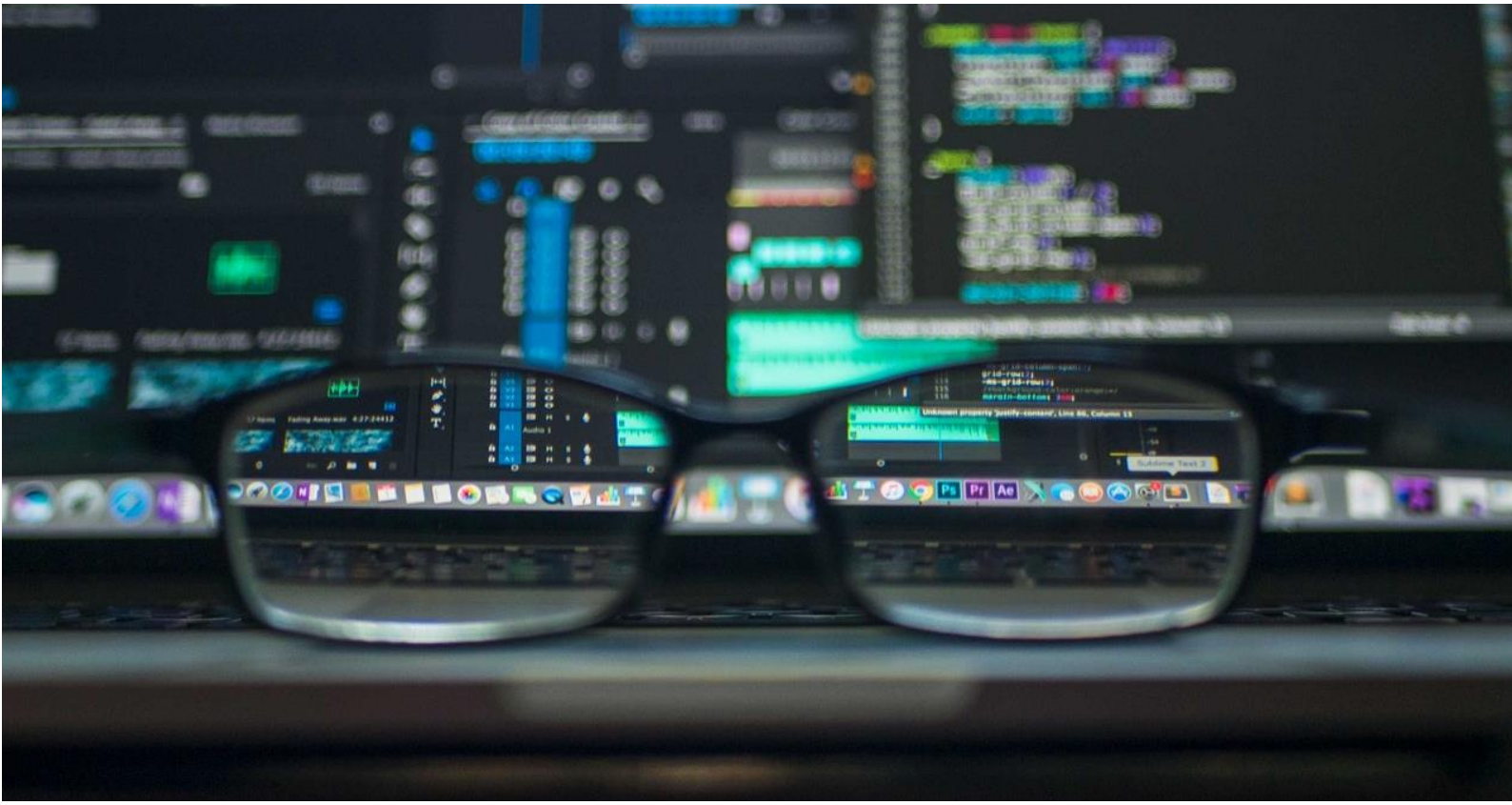
Failures will attract demerit points. Too many demerits and payments will be stopped.

There will be increased auditing of job applications to ensure they are "genuine", a return to the compulsory face-to-face meetings suspended during the pandemic

About the author:

Peter Martin, Visiting Fellow, Crawford School of Public Policy, Australian National University





ATO SET TO INTRODUCE REAL-TIME DATA MATCHING

The Australian Taxation Office (ATO) has announced it will use real-time data tracking on passengers coming into and out of Australia.

The ATO will look to access historic and future data to improve compliance with Australian tax obligations.

BDO Australia has cautioned that individuals need to be mindful of the tax issues which might arise if they are usually based outside of Australia but return home.

Overseas employers should also be aware they need to track employees coming to Australia and potentially take steps to manage unforeseen Australian tax obligations.

James Trainor, Tax Partner at BDO in Australia said, with ATO estimates indicating around 670,000 individual records will be obtained each financial year, the new data matching could see returning Australians liable to pay tax on overseas income.

“Aussies returning home could now face a tax bill on their overseas earnings,” James said.

“In the post-pandemic environment, expats are keen to come home but continue to work for their foreign employer. They and their employer could now be asked to pay up.”

“There are two scenarios that would trigger tax implications for Australian employees and foreign employers of Australians.

1. **Employees:** Australians working overseas for extended periods are typically not taxed in Australia on their overseas income. However if that person frequently returns to Australia, for example because their family has remained here, then Australia may seek to tax all of the overseas income. The ATO will now have ready access to data to determine how frequently the person has been in Australia. Australians working in low or nil tax countries (i.e. UAE, Singapore and Hong Kong) are particularly impacted.
2. **Employers:** Australians who are usually based overseas for work may decide to return to Australia to ride-out COVID and work in Australia remotely for their overseas employer. Extended periods spent working in Australia could result in the employee being subject to income tax in Australia on the salary, which is paid by their overseas employer. The overseas employer also has employer tax obligations, such as income tax withholding from the salary, superannuation, fringe benefits tax and payroll tax. Further the employee may cause the overseas employer to have a taxable presence in Australia, notwithstanding it does not have a registered business in Australia. The actions of the employee may have ramifications for the employer, and we are aware of cases where the employer does not know where its employees are working, so the employer tax obligations and potential penalties for failure to comply are sleeper issues for the employer. However, the ATO will be armed with information, which may surprise some employers.

DYSFUNCTIONAL FINANCIAL MARKETS ARE MAKING INEQUALITY WORSE ALL THE TIME – HERE'S WHAT TO DO ABOUT IT

The global market in government bonds has been bleeding red lately. "Bond market screams for help but no one answers", says Bloomberg. It is "the worst start to a year in bonds since 2015", according to the Financial Times.

Though bonds have been declining since last summer, the sell-off became a lot more violent in February. This meant that the yield on ten-year US Treasury bonds, which is inversely related to the price, rose by around 60% to peak at over 1.6% a couple of days ago, before falling back to 1.5% at the time of writing.

Trading View

The US ten-year strongly influences the price of everything from mortgages to business loans in the US, and by extension around the world, so such a sharp rise has the potential to reduce borrowing and weaken the economic recovery from COVID – especially when there is so much debt in the global system. The world's rampant stock markets responded by going into reverse in February as they factored in higher interest rates, as well as higher production costs because of surging commodity prices.

Bond prices can fall for several reasons. It can mean that the market thinks that economic growth is going to pick up (meaning investors shift their money into riskier investments). But it can also reflect fears that inflation is on the way without much accompanying economic growth, meaning that interest rates need to go higher so that lending is still profitable.

In the present case, it is a bit of both: the rollout of the vaccination programmes has made many observers more optimistic about the prospects of a recovery. But the rise in the price of commodities like oil, copper and coffee is more about pandemic-related supply issues than because this optimism has prompted a step-change in demand.

When Fed Reserve Chairman Jay Powell failed to announce any immediate intervention to put a floor under the sell-off in bonds during a public appearance in early March, it appeared to trigger more selling – a sign that falling bond prices have been more a reflection of fears than optimism.

Interestingly, in the hours since the new US$1.9 trillion (£1.4 trillion) US stimulus package has been agreed by Congress, the bond market and stock market have both been rising. Though there have been fears that sending US$1,400 stimulus cheques to most Americans will cause a further surge in inflation, the extra consumer demand will also prop up the economy. On balance, then, this appears to have been received as a net positive by the markets.

QE and perverse consequences

Any attempt to explain what is happening in the markets needs to be in the context of quantitative easing (QE). Shortly after the first wave of lockdowns in early 2020, central banks stepped in to help their national economies. They announced huge new QE plans in which they would create new money with which to buy government bonds and other financial assets. This drove up bond prices and hence kept yields (and interest rates) at very low levels to encourage as much borrowing from consumers and businesses as possible.

Most central banks originally began QE programmes after the 2007-09 financial crisis (besides the Bank of Japan, which began a few years earlier). This was primarily to help companies get access to capital to boost their business, in the hope that they would then hire staff, which would help to reduce unemployment rates that had been sent soaring after the crisis.

However, some companies took advantage of these low interest rates in another way: they borrowed cheaply and invested it in the stock market. With investors doing likewise, this has helped to drive the relentless rise in global stock markets over the past decade. It also helps to explain why these markets have been mainly climbing ever since the COVID panic sell-off of March 2020.

Trading View

In the coming months, economies are going to reopen, but interest rates are to stay low. Fed Reserve Chairman Jay Powell may have declined to announce any new interventions to date, but it is fairly clear that he will only let yields rise so far.

This gives investors a great opportunity to continue taking advantage of the situation. So long as the gain from your investment in stocks is greater than the interest rate you have to pay on your borrowings, you are a winner. Better still, buy stocks in a company such as Apple whose bonds central banks have been buying as part of their QE activities. Apple is still trading at over double the lows of March 2020, even after the February correction.

But if you are not in a position to take advantage of this one-way bet, you are a loser. The central banks have already created a situation where major institutions like the biggest hedge funds and investment banks are achieving record earnings while many families are sinking into poverty on the back of the pandemic.

The endless stimulus is in danger of creating an ever more divided society. While it is true that the latest US package (and the support measures announced in the UK budget) will temporarily help those struggling during the pandemic, the shot in the arm is also another way of propping up markets that seem too overvalued to fail.

And if they can no longer survive without central bank life-support to keep bond yields low, the question is how to prop up the markets without exacerbating inequality. It's not clear that anyone has the answer. It might be that a shift to a much more redistributive politics to offset the widening gap between rich and poor is about the best that we can hope for.

About the author

Arman Hassanniakalager, Lecturer in Finance, *University of Bath*

FRAUD RISK TO RISE, DESPITE MOVE AWAY FROM REMOTE WORKING

Australian businesses say the risk of fraud will increase this year, despite an expected move away from the widespread remote working which left them more open to being a victim, a KPMG Forensic survey has revealed.

The survey of over 70 businesses found a large majority (72 percent) believed their risk of fraud rose last year during the COVID crisis, with almost two-thirds saying the general move to working from home had increased the risk. 62 percent of respondents reported the insider threat was their most significant fraud and corruption challenge, with employees assessed as presenting the biggest danger for organisations.

Dean Mitchell, KPMG Forensic Partner, said: "We were surprised to find that many businesses think the worst may still be to come in terms of fraud, given that widespread remote working may start to ease during 2021. Experience has shown that many internal controls don't travel well which would explain most finding the risks were higher last year."

"One explanation may be that traditionally a year or two passes before a fraud is identified – and where there is an internal perpetrator, who knows the company systems and is able to cover their tracks, this period of fraud can extend further. As a result fraud is likely occurring right now but remains undetected. Over 40 percent of respondents said they had been inhibited by the crisis from investigating allegations of fraud and over 30 percent had had to delay antifraud and corruption programs – so their concern about rising fraud levels in 2021 may be understandable."

More than 65 percent said they were 'not', or were only 'somewhat', confident that they had identified most of the fraud that occured during the last year. Cyber-risk was the biggest challenge, with an overwhelming 92 percent believing that the danger of cyber-related fraud had increased during the pandemic – nearly a quarter 'significantly' so.

Key findings

- 72 percent said the COVID pandemic had increased the risk of fraud
- 92 percent believed the risk of cyber-fraud had increased during the COVID era
- 67 percent were unsure if their business had detected frauds taking place during the crisis
- 65 percent said their own organisation was more vulnerable to fraud than before COVID
- 51 percent said their ability to investigate possible fraud had been compromised
- 65 percent said widespread remote working had increased fraud risk

Organisations reported increasingly turning to technology to help identify the fraud and corruption that was occurring in the new remote working world. 38 percent stated they were now using artificial intelligence or forensic data analytics to identify fraud in their operations.

Dean Mitchell said: "Fraudsters leave traces when they attack organisations – clues that can be identified. In response, forensic analytics is needed but this is not simply deploying 'off the shelf' data tests to terabytes of data. An optimum response involves bringing together former fraud detectives, data scientists and forensic accountants to uncover the warning signs in your financial data."

Key considerations for organisations using technology to reduce fraud and corruption threats

- Ensure analytics is built on real world fraud not generic testing
- Fraudsters often create quasi-legitimate entities shortly before embarking on their schemes, deploy analytics to identify suppliers who registered their business shortly before delivering their first invoice to you
- Trusts or obscure ownership structures are often used to conceal beneficial ownership from victims, ensure the analytics highlights these vendors
- Fraudsters often leave an unintended digital clue in less scrutinised employee vs vendor matching criteria, dive deeper beyond name and bank account matching
- Changes to addresses and bank accounts are common flags, target emerging schemes including bank account substitution where accounts are switched back to avoid detection

There were some interesting observations from participants in the survey, which gave further insights into the findings:

"A lack of visibility of parts of the supply chain, particularly losing the ability to complete in person audits/inspections has increased the corruption risk in overseas markets. I think the move to people working from home will remain in organisations and I don't think this risk has been properly understood in the long term. I see this in terms of a general lack of supervision, but also a lack of connection to the business day to day which may influence poor decision-making".

"Many of the fraud items will not have been uncovered yet because remote work practices mean those who intend to cover their activity still have that scope. Counter-fraud resources have been diverted away from many existing programs, increasing their risks. New programs have been rushed out of the door with limited consideration for fraud, which will increase exposure for organisations. Government programs providing relief has also meant that businesses have been targeted to have their details stolen by criminals seeking to defraud the government

SOMETIMES PEOPLE CAN DO WITH A BREAK: 3 WAYS TAX DEBT RELIEF RULES ARE TOO TOUGH

By Ann Kayis-Kumar, UNSW; Kevin O'Rourke, UNSW, and Michael Walpole, UNSW

When Debbie (not her real name) lost her main client and was left without a reliable income, the sole trader sold her home and adjoining investment unit to pay off her debts and ensure she had the means to support her daughter and herself.

But things didn't work out as she had hoped.

A year later she was still mired in debt – only now to the Australian Tax Office, owing more than A$70,000 in capital gains tax from the sale of the investment property. By the time the payment deadline came, she still owed about A$61,000 plus A$13,500 in ATO-charged interest.

So she applied for tax relief under the "serious hardship" relief provisions that have been part of Australian tax law since 1915.

Her case might seem exactly the sort of reason why Australia's Taxation Administration Act gives the Commissioner of Taxation discretion to release individuals "in whole or in part" from tax debts, if they will "suffer serious hardship" by being required to pay.

Debbie had always paid her taxes on time. A single mother, she had never drawn child-support payments. She was not in good health, having had breast cancer and depression. But her application was rejected. Twice.

Because Debbie's claim had a fatal flaw, according to the rules governing the tax commissioner's discretion. She couldn't show that having her tax debt waived would, on its own, save her from serious financial hardship.

That is, the rules effectively say a tax debt can only be waived if it is the only debt pushing a person into serious hardship. But even without the tax debt, Debbie couldn't meet her living expenses. Her application was therefore rejected.

So, perversely, the greater the financial hardship a person finds themselves in, the less likely a tax debt will be waived.

This, and a few other significant quirks, is why the ATO's tax relief rules need reform.

No published data since 2013

We know Debbie's story because she is one of a very small number that have appealed the tax commissioner's decision to the federal Administrative Appeals Tribunal.

Just 34 appeals have been made in the past 50 years, according to our analysis. All but four lost those appeals.

One interpretation of these numbers is the tax office almost always makes the right decision – granting relief when appropriate and denying it when not. We're not convinced.

How many people apply and are granted relief in any year? We don't know.

The Australian Tax Office hasn't published those figures since 2013. The numbers for that year show about 15,000 people applied. About 2,500 were granted full or partial tax debt forgiveness.

We can only speculate about why this data is no longer published. But one effect is to minimise awareness that people in financial hardship can apply for tax debt relief. Our research suggests many more than 15,000 people could potentially qualify.

Perverse rules

But the perversities of the rules mean those most needing help don't necessarily get it, as shown by the 34 cases we have examined.

The median tax debt in those cases was about A$80,000. A majority (19 of the 34) represented themselves, while the tax office was represented by lawyers.

The reasons they found themselves in debt were generally complex – involving serious mental and physical health problems, relationship breakdowns, carer responsibilities preventing full-time return to work, and so on. Seven were self-employed.

Looking at the reasons most of these claims were rejected, we see the need for three key reforms.

1. The greater the hardship, the less relief offered

As outlined above, the tax commissioner can release someone from a tax debt only when it is "solely" the payment of that tax debt that will cause "serious hardship".

This was the case in the two appeals that succeeded. In cases such as Debbie's, no relief was granted because waiving the tax debt would not resolve all the person's financial troubles.

This causal link should be removed.

2. Penalised for paying other debts

This leads to the second reform. Evidence of a person paying off other debts is grounds to disqualify them from tax debt relief.

The rationale is that tax obligations shouldn't be treated as less important than other debts. But it has the perverse outcome that someone who pays off a credit card debt before their tax is effectively barred from serious hardship relief.

Rather than a "one strike and you're out" approach, the law should recognise degrees of culpability – distinguishing between someone who deliberately and intentionally disregards their obligations and someone who gets in financial trouble due to losing their job, sickness, business failure, relationship breakdown and so on.

3. GST-related debts are excluded

Arguably the most problematic aspect of the rules is they make no provision for financial difficulties arising from being a sole trader or running a small business. In particular, the rules exclude forgiving GST debts.

On one level this makes sense. GST is meant to be collected with every invoice, then forwarded to the tax office with quarterly Business Activity Statements. A GST debt is therefore pocketing other people's tax.

But these days many people are forced into being small business people, such as through working as contractors. They can be overwhelmed by the paper work, and not have the cash to pay a bookkeeper to do it for them. In our experience from running a tax clinic, people who come to us for help on average are eight years behind on tax returns and seven years on business activity statements.

The rules should recognise this reality and allow GST-related tax liabilities to be forgiven in some circumstances.

Time for a serious rethink

When someone is genuinely experiencing serious financial hardship, it is futile to chase them for money they cannot pay. Forcing them into bankruptcy doesn't help anyone.

We need more compassionate rules that reflect the reality of why people find themselves in debt.

Such reform has been made even more urgent by the COVID economic crisis.

Federal government subsidies and relaxation of normal rules have enabled many small businesses to stay afloat during the COVID crisis.

It hardly makes sense, given all the public money spent in other ways, for outdated tax-relief laws to force people into insolvency and bankruptcy now.

About the authors:

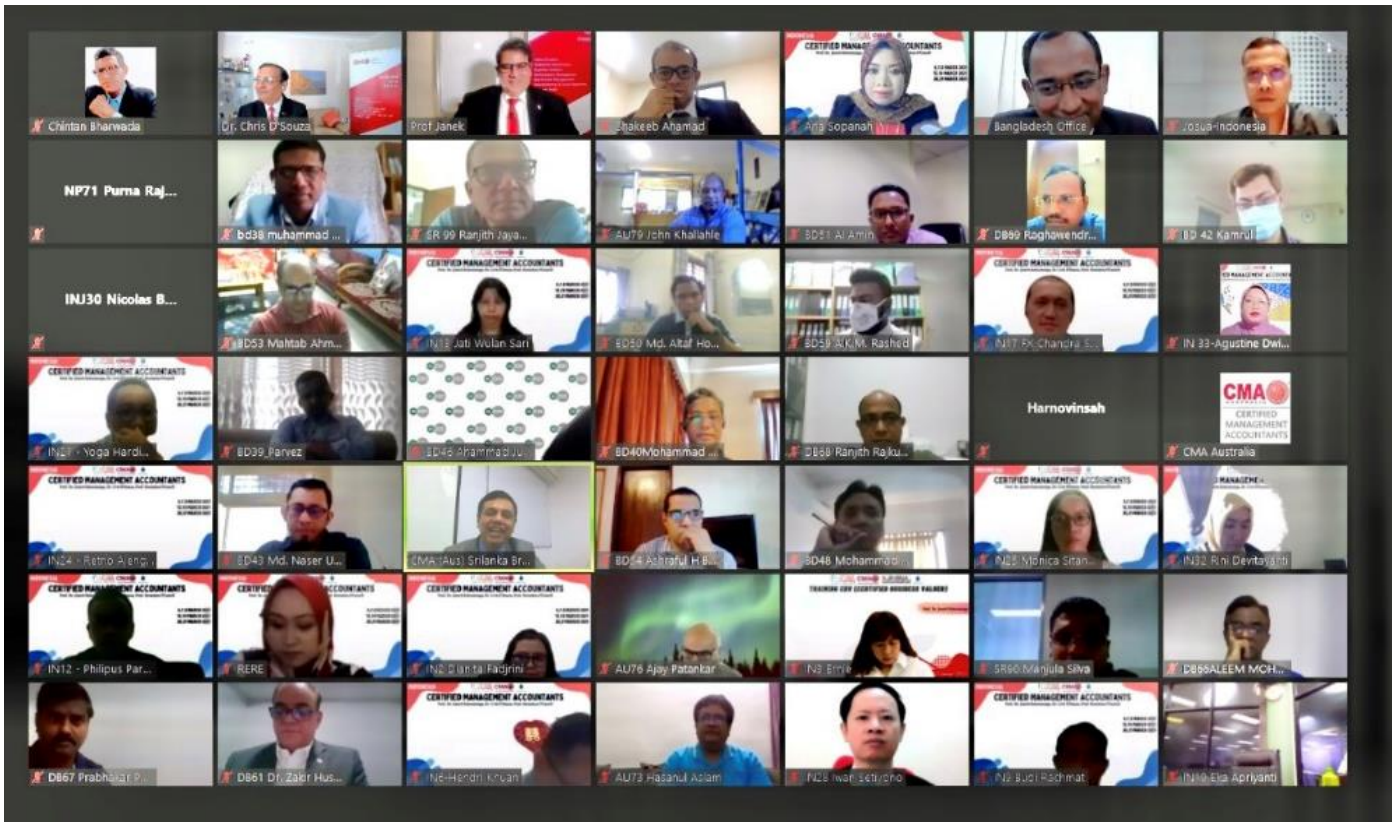
Ann Kayis-Kumar, Associate Professor, UNSW; Kevin O'Rourke, Lecturer, UNSW, and Michael Walpole, Professor, UNSW

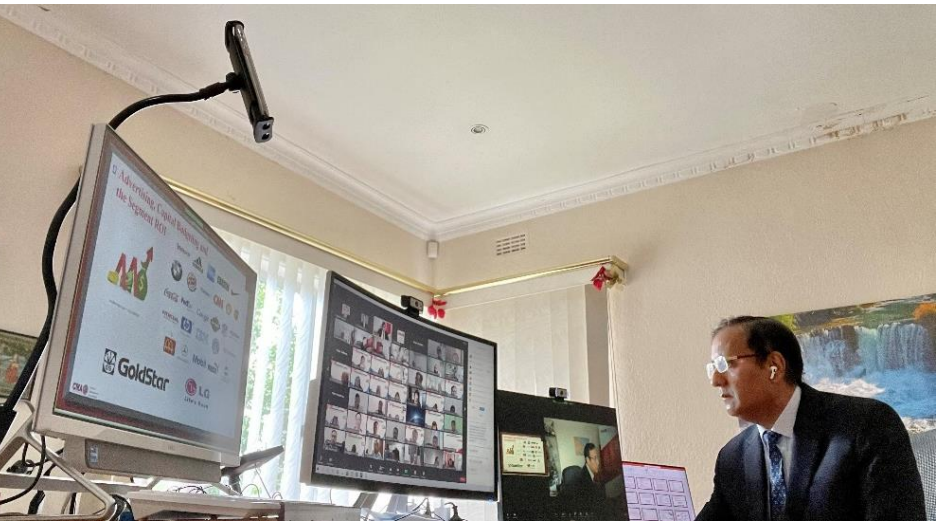
REGIONAL OFFICE AND BRANCH NEWS

GLOBAL ZOOM CMA PROGRAM

The second Global Zoom CMA Program was held over 3 weekends in in March 2021. It was an immense success with 102 participants from 20 countries. It commenced at 2pm AEDT and finished at 10pm each day. There were those who tuned in from Canada at Midnight the day before; and from New Zealand who finished after midnight the day following! There were also participants from Germany, the UAE, Bangladesh, PNG, Singapore and also Australia.

The presenters were Prof Janek Ratnatunga, Prof Brendan O'Connell and Dr. Chris D'Souza; and the Zoom Host was Dr Chintan Bharwada; ICMA's COO. Given the incredible logistics involved, it was a team-teaching effort on all the days. From the comments posted in the chat boxes; it was extremely well received. Special commendation must go to Dr Ana Sopanah who was responsible for a large contingent of participants from Indonesia; and also Mr. Sazzad Hassan, the Regional Director of Bangladesh, Mr. Kapila Dodamgoda, the Regional Director of Sri Lanka and Shakeeb Ahmed of the Regional Director of UAE.





Dr Chris D'Souza presenting the CMA program from his hime studio in Melbourne, Australia.

INDONESIA ZOOM WEBINARS

Throughout the Covid-19 pandemic, ICMA Australia Indonesia Brach continued its commitment to facilitate the capability development for CMA Members, professionals and academics in the fields of accounting and finance. In the March-April period 3 more webinars were held. ICMA facilitated the events, which were moderated by ICMA Australia's Indonesia President, Mr. Daniel Godwin Sihotang, Dr Ana Sophana, Mr. Nursakti Niko Rosandy, the Branch Treasurer.

SRI LANKA EVENT

Those attending the Global CMA Zoom program in the premises of the Academy of Finance. In the picture is Kapila Dodamgoda, the Regional Director of Sri Lanka and his "Kapila's Angels'.

Those attending the Global CMA Zoom program in the premises of the Academy of Finance. In the picture is Kapila Dodamgoda, the Regional Director of Sri Lanka and his "Kapila's Angels'.

A WARM WELCOME TO NEW MEMBERS (Feb & March 2021)

Aliten, Jocelyn
Arenas, Maria Cecilia
Aruneswaran, Chrishanthi
Aslam, Hasanul
Aynsley, Tim
Bajaher, Mohammed
Basaria, Maya
Bavishi, Hemal
Brice, James
Chan, Ka Ying
Chau, Hon Chung Andrew
Chen, Shiqin
Chhan, Sareth
Choudhary, Ajit
Chung, Sau Yin
Coenraad, Dilraj
Dam Thi Thu, Hang
Dilrukshi, Prithika
Do Minh, Thang
Dsouza, Merlyn
Dworzak, Anton
Edirisinghe, Suranga
Edwards, Simone
Fernando, Menash
Fernando, Shakthi
Frost, Alex Electra
Hossain Farazi, Mohammad Mostofa
Hossain, Iqbal
Hossain, Md Shameem
Islam, Mohammad
Joseph, Subha
Karunarathne, Nimali
Koo, Dreyfus
Le Thi Yen, Ngoc
Le Tu, Hue
Leung, Fung Ha
Lo, Chi-kwong
Luong Hien, Thuy
Luong Xuan, Quy
Mai Thi Thu, Suong
Mohibbullah, S.M.
Mutto, Louisa
Ng, Ho Man
Ng, Wai Han
Nguyen Manh, Hien
Nguyen Minh, Tuan
Nguyen Phuoc Quy, Hung
Nguyen Song, Vuong
Nguyen Thi Huyen, Trang
Nguyen Thi Mai, Huong
Nguyen Thi My, Linh
Nguyen Thi Thanh, Van
Nguyen Thi Thu, Ha
Nguyen Thi Thu, Hien
Nguyen Thi, Ngan
Nguyen Thu, Van
Nguyen Thuc, Khoa
Oosthuizen, Martha
Per, Bernice
Pham Dang, Khoa
Phan Vuong, Nhat
Rahman, Muhammad Habibur
Roy, Pankaj
Saguliannita, Meriza
Sharma, Shimul
Sidharthan, Sharika
Slade, Marcus
Sumajit, Racquel
Ta Thi Thu, Hien
Ta Thi, Hanh
Talukder, Md. Tahorim
Tan, Jensen
Tran Trong, Duc
Tran Viet, Hung
Unwin, Steven
Verwey, Brian
Vo Van, Dien
Wong, Man Chi
Yarkhan, Najeeb
Zega, Mogantara

CPD OPPORTUNITIES

Registration link: https://cmaaustralia.edu.au/ontarget/

Webinars **(Free for members)**

March 25, 2021, Prof Janek Ratnatunga "Money Laundering: Traditional vs. Digital: Key Lessons for Bankers and Finance Professionals"

April 15, 2021, Prof Brendan O'Connell "How Accounting and Finance Professionals Can Help in Climate Action"

May 5, 2021, Lasanka Perera and Lee Eaton of Independent Reserve on "Bitcoin and Crypto: Why They Are Viable Investment Options"

May 13, 2021, Dr Chris D'Souza "Project Management in a Post-Covid World"

Online CPDs

Business Valuation

Enterprise Risk Analysis

International Business Analysis

Project Finance Analysis

Project Management Analysis

(Special Promotion Members get 90% off for a limited time)

CMA EVENTS CALENDAR

- **March 25, 2021** Webinar by Prof Janek Ratnatunga "Money Laundering: Traditional vs. Digital: Key Lessons for Bankers and Finance Professionals"
- **April 15, 2021** Webinar by Prof Brendan O'Connell "How Accounting and Finance Professionals Can Help in Climate Action"
- **May 5, 2021** Webinar by Lasanka Perera and Lee Eaton of Independent Reserve on "Bitcoin and Crypto: Why They Are Viable Investment Options"
- **May 21, 2021** Webinar by Dr Chris D'Souza and Kieran Keleher "Project Management in a Post-Covid World"
- **July 10, 2021** Certificate of Proficiency in Strategic Cost Management, SMU Academy, Singapore (6th Intake). (Online).
- **July 23, 2021** Certificate of Proficiency in Strategic Business Analysis, SMU Academy, Singapore (6th Intake). (Online).
- **August 5, 2021** Webinar in Strategic Cost Management, Workplace Skills Development Academy (WSDA). (Online).
- **September 4, 2021** CMA Intensive Program Over Zoom – September 2021
- **October 1, 2021** Webinar in Strategic Business Analysis (Part 1), Workplace Skills Development Academy (WSDA). (Online).
- **October 8, 2021** Webinar in Strategic Business Analysis (Part 2), Workplace Skills Development Academy (WSDA). (Online).

Private Providers

Wharton Institute of Technology and Science (WITS), Australia

Syme Business School, Australia

Academy of Finance, Sri Lanka

IPMI (Indonesian Institute for Management Development), Indonesia

Singapore Management University Academy (SMU Academy)

Business Sense, Inc. , Philippines

HBS for Certification and Training, Lebanon

SMART Education Group, UAE

Institute of Professional and Executive Management, Hong Kong

AFA Research and Education, Vietnam

Segal Training Institute, Iran

PT Angka Bisnis Indonesia (Business Number Consulting), Indonesia

Inspire Consulting, Indonesia

ManAcc Consulting, New Zealand

STRACC Learning LLP, India

Workplace Skills Development Academy (WSDA), Bangladesh

Ra-Kahng Associates Ltd, Thailand

Academy of Management Accountancy, Nepal

Blue Globe Inc, Japan

New Zealand Institute of Business, Fiji

ICMA Australia

Global Head Office
CMA House
Monash Corporate Centre
Unit 5, 20 Duerdin Street
Clayton North, Victoria 3168
Australia
Tel: 61 3 85550358
Fax: 61 3 85550387
Email: info@cmaaustralia.edu.au
Web: www.cmaaustralia.edu.au

OTHER CENTRES

New South Wales
Professor Chris Patel, PhD, CMA
Branch President
Macquarie University

Tasmania
Professor Lisa McManus, PhD, CMA
Branch President
University of Tasmania

South Australia
Prof Carol Tilt, PhD, CMA
Branch President
University of South Australia

Western Australia
Dr. Vincent Ken Keang Chong
Branch President
UWA Business School

Queensland
Dr. Gregory Laing, PhD CMA
Branch President
University of the Sunshine Coast

OVERSEAS REGIONAL OFFICES

BANGLADESH
Mr. Sazzad Hassan, CMA
Regional Director – Bangladesh
Email: sazzad.hassan@gmail.com
Website: http://www.icmabangladesh.org

CHINA (including Hong Kong and Macau)
Prof. Allen Wong, FCMA
Regional Director and CE - Greater China
Email: info@cmaaustralia.org
allen.wong@cmaaustralia.org

CYPRUS
Mr. Christos Ioannou BA (Hons), MBA , CMA
Regional Director-Cyprus
Email: chioanou@cytanet.com.cy

EUROPEAN UNION
Mr. Rajesh Raheja CMA, Branch President
9, Taylor Close, Hounslow, Middlesex TW3 4BZ, United Kingdom
Tel: +44 208 582 0025
Email: rajesh@cmaeurope.net
http://www.cmaeurope.net

FIJI
Dr. Chris D'Souza, CMA
Country Head – Fiji (Pro-Temp)
New Zealand Institute of Business
Website: http://www.cmafiji.org

INDIA
Mr. Jayafar MV, CMA
Deputy Regional Director – India
Email: mvjayafar@gmail.com
Website: http://www.icmaindia.org

INDONESIA
Special Capital Region (Jakarta) Regional Office
Ms. Arum Indriasari – Jakarta Centre
IPMI Business School
E-mail : arum.indriasari@ipmi.ac.id

West Java Regional Office
Ms. Paulina Permatasari, FCMA
Regional Director - West Java
Email: paulinapssj@gmail.com

East and Central Java Regional Office
Dr. Ana Sopanah, CMA
Regional Director - East Java
Email: anasopanah@gmail.com

IRAN
Mr. Alireza Sarraf, CMA
Regional Director- Iran
Email: sarraf@experform.com

JAPAN
Mrs. Hiroe Ogihara
Country Head – Japan
Email: y.al.ogi999@gmail.com
Website: http://www.cmajapan.org

LEBANON
Dr. Fawaz Hamidi, CMA
Regional Director - Lebanon
Email: hbs@cmamena.com
www.cmamena.com

MALAYSIA
Mr. Jensen Tan, CMA
Country Head – Malaysia
Email: j.tanjensen@gmail.com
Website: http://www.cmamalaysia.com

West Malaysia Regional Office
Dr. Ridzwan Bakar, FCMA
Deputy Regional Director - **West Malaysia**
Email: ridzwan.bakar@mmu.edu.my

CAMBODIA
[To be Appointed]

NEPAL
Mr. Kumar Khatiwada, CMA
Regional Director – Nepal
Email: kumar_kha@hotmail.com
Website: http://www.cmanepal.org

NEW ZEALAND
Dr. Louw Bezuidenhout, CMA
Regional Director – New Zealand
Email: loubez@bizss.co.nz
Website: www.cmanewzealnad.org

PAPUA NEW GUINEA
Dr Thaddeus Kambanei, CMA
Regional Director - PNG
Email: Thaddeus.Kambanei@yahoo.com
http://www.cmapng.com

PHILIPPINES
Mr. Henry Ong, FCMA
Regional Director - Philippines
Email: hong@businesssense.com.ph
http://www.cmaphilippines.com

SINGAPORE
Dr Charles Phua, CMA
Country Head – Singapore
Email: charles_phua@solarisstrategies.com
Website: http://www.cmasingapore.com

SRI LANKA
Mr Kapila Dodamgoda, CMA
Regional Director - Sri Lanka
Email: kapiladodamgoda@yahoo.com
http://www.cmasrilanka.com

THAILAND
Mr. David Bell, CMA
Regional Director – Thailand
Email: david.bell@rakahng.com
Website: http://www.cmathailand.org

UNITED ARAB EMIRATES
Mr. Shakeeb Ahmed, CMA
Regional Director - U.A.E. & GCC Countries
Email: shakeeb@smarteducationgroup.org
Mobile: +971-55-1062083
Website: www.cmadubai.org

VIETNAM
Mr. Long Phan MBus (Acc), CPA, CMA
Regional Director- Vietnam
Email: longplt@afa.edu.vn

CMA AUSTRALIA | Certified Management Accountants