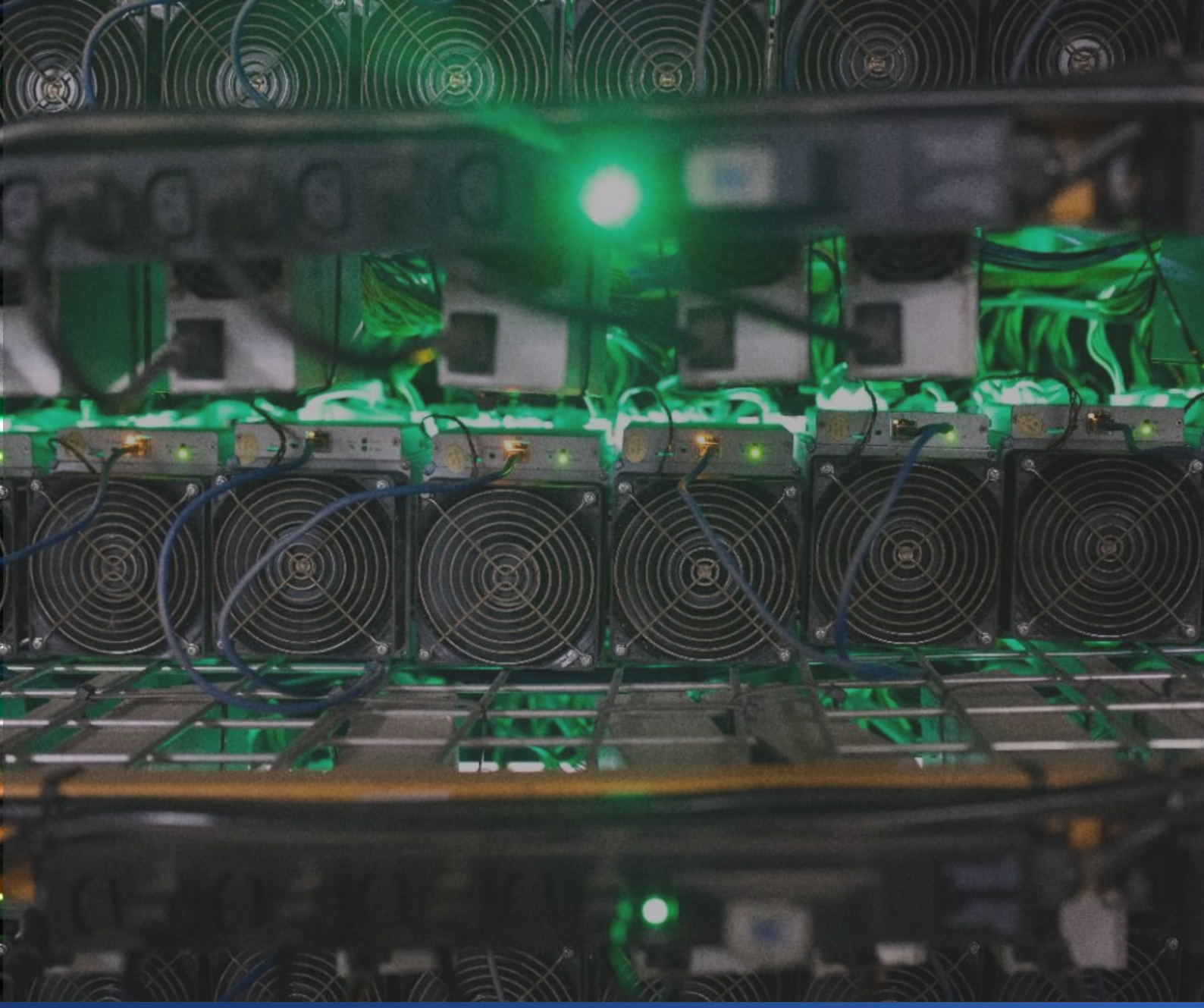


Exploring Cryptocurrency

Cyber Security Industry Advisory Committee

March 2022

CyberSecurity Industry Advisory Committee

On 6 August 2020, the Government released ***Australia's Cyber Security Strategy 2020*** and a $1.67 billion package to help protect Australians from cyber security threats.

The perspectives and expertise of industry and academia in the delivery of Australia's Cyber Security Strategy 2020 is critical to strengthening Australia's overall cyber resilience through a trusted and secure online world.

Recognising this, in October 2020, the Cyber Security Industry Advisory Committee was established by the Government to provide independent strategic advice on Australia's cyber security challenges and opportunities to help guide the Strategy as it enters the implementation phase.

The Committee comprises the members listed below:

- Andrew Penn, Industry Advisory Committee Chair, *CEO of Telstra*
- Cathie Reid, Industry Advisory Committee Deputy Chair, *Chair of AUCloud*
- Darren Kane, *Chief Security Officer of NBN Co*
- Chris Deeble AO CSC, *Chief Executive of Northrop Grumman Australia*
- Bevan Slattery, *Chairman of FibreSense*
- Corinne Best, *Trust and Risk Business Leader of PricewaterhouseCoopers Australia*
- Patrick Wright, *Group Executive Technology and Enterprise Operations NAB*
- Rachael Falk, *Chief Executive Officer, Cyber Security CRC*
- Professor Stephen Smith, *Chair of Advisory Board, University of Western Australia Public Policy Institute*
- David Tudehope, *Chief Executive Officer, Macquarie Telecom Group*

Introduction

It is estimated at least three million Australians now own some form of crypto asset[1].

The most well-known crypto asset is cryptocurrency. Cryptocurrencies have proliferated rapidly over the last decade. Many individuals and businesses who purchase cryptocurrencies do so to speculate on their value. The fascination to date with these currencies appears to have been more speculative (buying cryptocurrencies to make a profit) than related to their use as a new and unique system for making payment[2].

However, despite their widespread and accelerating adoption, cryptocurrencies remain a mystery to many Australians.

As Australia undergoes rapid transformation to an advanced digital economy by 2030, it is likely, the use of cryptocurrencies will continue to increase. In turn, a better understanding of what cryptocurrencies are, how they operate and can be used, and associated risks, must be fostered.

Cryptocurrencies offer a myriad of opportunities for facilitating business growth and the streamlining of financial operations. But with the good comes the bad. While the regulatory environment is rapidly evolving, due to the pseudo-anonymity they provide, cryptocurrencies remains a conduit for serious criminal activity. In addition, there are significant cyber security risks that need to be considered as cryptocurrencies are more widely adopted.

The Committee welcomes the opportunity to contribute to robust and effective cyber security outcomes for Australia. Therefore, this report explores the cyber security and cyber crime implications of cryptocurrency and explores how these risks could be better mitigated.

Although this paper discusses the risks and opportunities associated with cryptocurrency it does not offer financial advice or recommend particular investment strategies. Individuals and businesses should continue to seek independent legal, financial, taxation or other advice to check how such investments relate to their unique circumstances.

[1] https://www.afr.com/companies/financial-services/four-million-aussies-set-to-buy-into-crypto-20210608-p57z2g
[2] https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html

This Industry Advisory Council paper explores cybersecurity considerations with respect to:

- What cryptocurrency is;
- The risks associated with cryptocurrency;
- The nexus between cryptocurrency and crime;
- The current state of domestic and international cryptocurrency regulation;
- The opportunities cryptocurrency presents.

Finally, the recommendations provide some forward-facing steps to help foster the secure adoption of cryptocurrencies in Australia, address crypto-related crime, as well as support crypto-driven opportunities in Australia.

What is Cryptocurrency?

Cryptocurrencies are crypto-assets (crypto), also known as coins or tokens. They are an emerging asset class without a physical form - they are digital tokens stored in a digital 'wallet' and are both speculative and opaque.

Cryptocurrency is typically used as a store of value, for investment, payment and to execute automated contracts.[3] The global market is rapidly expanding, with more than 6,000 unique cryptocurrencies worldwide.[4]

Cryptocurrency transactions allow direct peer-to-peer transactions without an intermediary (e.g., bank or other regulated financial entity). This model differs to traditional payment methods, which rely on a central party to maintain records of transactions. Instead, cryptocurrencies use distributed ledger technology - a distributed database shared among a network of computers - to maintain a decentralised record of transactions and currency ownership.

The most common form of distributed ledger technology is the 'Blockchain'. When a new transaction occurs, it forms a part of a new block that is then added to the chain. As a result, the blockchain provides a record of every transaction that has ever occurred and is available to anyone to access. Most blockchain solutions enable a distributed, unanimous, immutable record of data and generates trust without the need for a trusted third party or intermediary[5]. There are some instances, such as Monero, which are private decentralised ledgers that makes it more difficult to identify wallet addresses, transaction amounts, address balances, or transaction histories and therefore providing less transparency and traceability.

[3] https://moneysmart.gov.au/investment-warnings/cryptocurrencies
[4] https://www.statista.com/statistics/863917/number-crypto-coins-tokens/
[5] https://www.euromoney.com/learning/blockchain-explained/what-is-blockchain

Many individuals and businesses who purchase cryptocurrencies do so speculatively. Cryptocurrencies have no legislated or intrinsic value - they are simply worth what people are willing to pay for them[6].

As a result, large numbers of cryptocurrencies have become insolvent overnight. Many are registered companies in foreign countries with different laws than where they reside and are therefore without any legal recourse. Most are not registered in Australia and neither the government nor the courts have jurisdiction. Additionally, as a store of value, deposits in all modern economies are insured and guaranteed by the local government. This is typically not the case for mainstream cryptocurrencies.

The rise of cryptocurrencies has provided a new opportunity for criminals to launder proceeds of crime. Criminals are known to be early adopters of emerging technologies and it has become the currency of choice on the dark web.

The evolution of crypto

Cryptocurrencies, other than stablecoins, are known for their high volatility[8], some cryptocurrencies have halved or doubled in value in the space of a month. Bitcoin, one of the most well-known cryptocurrencies, is the top performing asset of any class over the past decade – climbing a staggering 9,000,000% between 2010 and 2020[9].

Tokenised "money"

- **Stablecoins** - privately issued digital assets designed to decrease volatility by tracking a fiat currency (e.g. US dollar), commodity (e.g. gold) or basket of other cryptocurrencies (e.g. Circle's USDC). Issued by blue chip, notable and stable firms.
- **Central Bank Digital Currencies (CBDC)** - a new form of digital money that would be a liability of the central bank, these might be retail CBDCs (available to the public) or wholesale (analogous to central bank settlement accounts) (see China's CBDC project)[7].
- **Mainstream cryptocurrencies -** privately issued digital assets that are not denominated in the currency of any sovereign (e.g. Bitcoin, Ether).

Tokenised other assets

- There has been a proliferation of other assets being tokenised, some of these are 'digitally native' (non physical) and are defined by their existence on a blockchain ledger (e.g. Non-fungible Tokens).

  Others may represent pre-existing real world assets such as tokenised representations of real property or financial instruments.

[6]https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html

Due to the evolving nature of cryptocurrency, Australia, like its global counterparts, has been considering the regulatory regime.

Cryptocurrency exchanges

Much like traditional financial exchanges, cryptocurrency exchanges allow customers to trade cryptocurrencies for other assets, such as conventional fiat currency or other digital currencies. Some particular exchanges have adopted a structure, acting as an intermediary, where they hold the relevant private encryption keys required to transact.

Major economies, in some instances, refuse to recognise cryptocurrency as legal tender as this may undermine government authority by circumventing capital controls and by removing intermediaries. Hence, cryptocurrencies can potentially disrupt and destabilise existing financial infrastructure systems.

In 2014, the world's then largest cryptocurrency exchange, Mt Gox, which handled more than 70% of currency transfers, suspended trading, closed its website, and commenced bankruptcy liquidation. This occurred after the theft of about 850,000 bitcoins – worth roughly AU$72 bn - from the exchange's wallet[10].

Since the collapse of Mt Gox, a more rigorous approach and additional scrutiny has been begun to be applied by regulators and customers of cryptocurrency exchanges.

Therefore, exchanges and the regulatory environment surrounding them will play a key role in mitigating crypto theft, the use of cryptocurrencies for criminal activity and ensuring cyber security is up to scratch.

In 2017, the Government amended the Anti-Money laundering/Counter-Terrorism Financing (AML/CTF) Act to regulate Digital Currency Exchanges (DCEs) in recognition of the emerging money laundering and terrorism financing risks. DCEs in Australia are regulated under the AML/CTF Act when they exchange digital currency for fiat currency and vice versa (but not for digital currency/digital currency exchanges).

And in December 2021, the Australian Government signalled it would create a licensing framework for cryptocurrency exchanges as a part of its payments industry overhaul[11].

Australian peak bodies, such as Blockchain Australia, certify exchanges with a code of conduct[12]. Whilst not a cyber security standard or a statement of financial viability, this can give some confidence to consumers regarding best practice standards in legal compliance, reputation, AML/CTF protections and consumer protection.

[7]https://www.rba.gov.au/speeches/2021/sp-so-2021-11-18.html
[8]https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8326316/
[9]https://www.coindesk.com/price/bitcoin
[10]https://www.theaustralian.com.au/business/markets/mt-gox-casts-its-shadow-over-bitcoin/news-story/ccf37dc48d8b6481436920bd947ccab5
[11]https://www.reuters.com/markets/currencies/australia-plans-update-regulatory-framework-payment-systems-2021-12-07/
[12]https://blockchainaustralia.org/

Risky Business

Like any currency, risk is an inherent part of cryptocurrency. However, due to the evolving regulatory environment, its defining tenets of pseudo-anonymity and decentralisation, and its immaturity as an asset class, the risk profile of using and investing in cryptocurrency is higher. It is also subject to the rules and regulations as put forward by the Australian Taxation Office (ATO).

As cryptocurrency is not grounded in physical assets, it is hard to assign a value which means there is less traditional understanding and confidence, which impacts scale of usage and uptake. There are three key areas to highlight as it comes to cryptocurrency risks:

Volatility

Cryptocurrency, with the possible exception of stablecoins, is highly volatile. This volatility arises because of the speculative nature of cryptocurrency, in that its value is not derived from physical or tangible assets, and trading behaviours are amplified by external events, even tweets[13]. For example, in one day in May 2021, the value of Bitcoin plunged 30 per cent China's Banking Association warned member banks of digital currency risks[14].

Secure Storage

Because cryptocurrency is stored in digital wallets, it has become an attractive target for cyber criminals. This is problematic because the anonymity that often attracts users to cryptocurrency also makes it easier for cyber criminals to steal these assets undetected. Digital wallets are divided into two groups – 'hot' (with software connected to the internet) and 'cold' (a wallet that is not connected to the internet and is used for storing private keys)[15]. It is predicted 2022 will see more sophisticated exploits being deployed by cyber criminals and state-sponsored actors targeting digital wallets and exchanges[16]. To help ensure the security of digital wallets:

- Use an encrypted 'cold wallet' (a wallet not connected to the internet), to securely store private keys;
- Only use secure internet connections – do not use public wi-fi;
- Use multiple wallets for different purposes, spreading your cryptocurrency assets around; and
- Use a strong password and change it regularly.

[13] https://www.forbes.com/sites/nicolelapin/2021/12/23/explaining-cryptos-volatility/?sh=117e923e7b54

[14] https://www.cnbc.com/2021/05/19/bitcoin-btc-price-plunges-but-bottom-could-be-near-.html#:~:text=Bitcoin%20plunged%2030%25%20to%20near,paring%20some%20of%20those%20losses.

[15] https://moneysmart.gov.au/investment-warnings/cryptocurrencies

[16] https://www.kaspersky.com/about/press-releases/2021_financial-systems-jeopardized-infostealers-on-the-rise-and-more-cryptocurrency-attacks-a-look-at-financial-threats-in-2022

Case study - Hot wallet hijacking

In December 2021, cryptocurrency trading platform Bitmart was hit by a major hack, with up to US$200 million in tokens stolen. The security breach was reportedly caused by a stolen private key, impacting two of its 'hot wallets' (a wallet connected to the internet). After transferring the funds, the hackers are believed to have used a decentralised exchange aggregator to exchange the stolen tokens, which were then deposited into a privacy mixer, making the cryptocurrency difficult to trace[17].

Exchange Risk

At the most basic level, given the volatility of the cryptocurrency market, there is a higher risk an exchange may collapse. For example, the 2020 collapse of Australian crypto exchange ACX resulted in the loss of millions of dollars by Australian investors, which administrators are still trying to recover[18].

Exchange service outages, which occur when network traffic gets too high, are a key risk that can wipe huge amounts off cryptocurrency values in a matter of hours.

It is estimated outages of the world's two largest crypto exchanges in May 2021 resulted in losses of up to US$1 trillion worldwide[19]. In addition, crypto exchanges are becoming increasingly attractive targets for cyber criminals and state-sponsored actors, with the potential of stealing millions in minutes.

Case Study - Crypto rug pulling

A 'rug pull' is a malicious exploit in the cryptocurrency industry, where developers abandon a project and run away with investors' funds. A recent example was Squid Game cryptocurrency, which leveraged the hype surrounding the television show to appreciate astronomically over two weeks. However, developers falsely claimed to be creating an online game and then sold their entire holdings for approximately US$3.4 million, draining all market liquidity. The cryptocurrency value crashed from US$2,861 to US$0.01 in just five minutes[20]. This highlights the need for consumers to undertake due diligence when investing in cryptocurrency, as some are created with ill intent.

[17] https://www.cnbc.com/2021/12/05/hackers-take-196-million-from-crypto-exchange-bitmart-in-large-breach.html

[18] https://www.theguardian.com/technology/2021/dec/12/the-search-is-on-for-50m-in-lost-cryptocurrency-after-two-australian-exchanges-collapse

[19] https://fortune.com/2021/05/19/coinbase-binance-outage-crypto-bitcoin-crash/

[20] https://www.washingtonpost.com/world/2021/11/02/squid-game-crypto-rug-pull/

Cryptocurrency, cybercrimes and law enforcement

Law enforcement plays a central role in preventing the exploitation of cryptocurrency by criminals and organised crime groups. In Australia, the AFP is responsible for detecting, preventing, disrupting, responding to and enforcing cybercrime offences impacting the whole of the Australian economy, working closely with government and regulators, both domestically and internationally.

The dollar value of cryptocurrency transactions linked to criminal activity continues to increase annually with the market capitalisation of the sector. This trend of increased criminal use of cryptocurrencies is expected to continue in line with the increase in mainstream adoption.

Criminals – notably cybercriminals – are attracted to cryptocurrencies as they are an intangible, internet-native currency enabling almost instant borderless transfers, which can be utilised to quickly transfer the proceeds of crime across jurisdictions. Further, the relative anonymity provided by peer-to-peer cryptocurrency transactions can provide a layer of obfuscation for transactions without the challenges of cash transactions or cash transportation.

COVID-19 and physical border restrictions have led organised crime to look for alternative methods to launder proceeds of crime. Cryptocurrencies have emerged as one of these methods and are now a standard part of a money launderer's toolkit.

Australian law enforcement has noted an increase in organised crime exploring the use of cryptocurrencies to conduct or facilitate cybercrime and launder money.

Breaking the chain

Tracing cryptocurrencies presents new challenges for law enforcement in contrast to the traditional financial system. However, criminals would be aware blockchain transactions are completely transparent and remain forever available for all to see. Because peer-to-peer cryptocurrency transactions don't require an intermediary, no identification details are taken. Therefore, the challenge for law enforcement is to attribute identification to cryptocurrency addresses. Cybercriminals particularly have developed methodologies to try and cover their digital trail including immunity to blockchain forensics and finding 'workarounds' through moving dark web markets to anonymous applications

Held to ransom

Cryptocurrencies are integral to the illicit ransomware ecosystem, with the vast majority of ransom demands made in crypto. While initial transfers from victims may be made using legitimate regulated services onshore, funds are rapidly moved offshore using obfuscation techniques. Hesitancy from some ransomware victims and their security/remediation service providers to report the full details of ransomware payments further hinders law enforcement's ability to identify offenders.

In 2021, a **ransomware attack** on Colonial Pipeline led to the shutdown of the largest fuel pipeline in the US, with attackers demanding payment in cryptocurrency. A $4.4 (USD) million ransom was paid after nearly 100 gigabytes of data was stolen. However, in this case the use of cryptocurrency allowed law enforcement to track the payment and recover $2.3m (USD) in bitcoin that was paid, a first for law enforcement agencies.

The Australian Cyber Security Centre (ACSC) provides advice and guidance on ransomware threat. To access, please visit:

https://www.cyber.gov.au/acsc/view-allcontent/publications/ransomware-australia

Current Threat

The use of cryptocurrency by organised crime is an ever-growing threat. It requires law enforcement and criminal intelligence agencies to equip their people with the necessary tools to ensure they can investigate cyber-enabled crime and successfully identify, trace and seize cryptocurrencies used for nefarious purposes.

Cryptocurrencies are being widely used for cybercrime exploits, including ransomware attacks, business email compromise, malicious cryptocurrency mining and the sale of malware. They are also used to buy and sell illicit goods and services on the dark web, including weapons, drugs and child sexual exploitation material.

To face the challenges criminal use of cryptocurrencies present, traditional law enforcement methodologies require adaptation. Relationships with industry, training of investigators and appropriate regulation of cryptocurrencies and their use and exchange will be vital to meeting this challenge as the use of cryptocurrencies increases.

Under Australia's Cyber Security Strategy 2020, the government confirmed it would invest $89.9 million to bolster the AFPs ability to investigate and prosecute cyber criminals and $385.4 million in enabling and enhancing intelligence capabilities.

On 17 February 2022, the Crimes Legislation Amendment (Ransomware Action Plan) Bill was introduced to Parliament, including reforms enabling law enforcement to seize and freeze cryptocurrency suspected as being proceeds of crime.

Cryptocurrency and Data Asset Policy and Regulation

The opportunity exists for Australia to embrace forward-leaning regulatory settings that enhance confidence in and security of cryptocurrency. Currently, crypto-related financial product and services are regulated by the Australian Securities Invest Commission (ASIC) and DCEs are regulated by the Australian Transaction Reports and Analysis Centre (AUSTRAC).

Recently, the Australian Prudential Regulation Authority (APRA) confirmed it is seeking to "modernise" the prudential architecture in a multi-year project, which recognises emerging business models – including those using digital currencies or other crypto assets – do not fit into current regulations, meaning new rules are required to protect financial stability[21].

Australia's Regulatory Landscape

Regulatory settings for crypto-assets must be flexible enough to foster innovation but strong enough to provide adequate cyber security and consumer protections.

Australia's approach to regulating crypto-assets to date has been 'light-touch', seeking to expand existing financial services regulation to digital assets. While this provides some confidence to digital asset market participants, regulatory uncertainty has created hesitancy in Australian companies and consumers in crypto adoption.

The Bragg Report

The Senate Select Committee on Australia as a Technology and Financial Centre issued its final report in October 2021, making 12 key recommendations addressing regulatory and policy issues relating to crypto assets. These included several recommendations for reform including the introduction of a market licensing regime for DCEs and a new custody and depository regime for businesses holding crypto assets. The committee also recommended a token mapping exercise be conducted to determine the best way to characterise the various types of digital asset tokens in Australia[21]. The Federal Government has accepted these recommendations and has been begun consultation on a new licensing framework for DCEs.

In addition to the domestic AML/CTF laws, the key risk globally is the existence of unregulated cryptocurrency exchanges in jurisdictions that do not regulate, or do not effectively regulate, such businesses. Given the borderless nature of cryptocurrency, this provides a pathway for criminals to convert crypto proceeds to fiat currency.

As such, global bodies such as the Financial Action Task Force (FATF) and Basel Committee continue to express their concern over the current crypto regulatory environment.

Going dark: Privacy coins

AML/CTF requirements and market pressure from other regulated entities, have led many Australian DCEs to delist 'privacy coins', like Monero. These coins obfuscate the 'public key' or account details of users on the blockchain, which can hinder law enforcement and tracing efforts. These coins differ from other currencies, including Bitcoin and Ethereum, that link transactions to public keys, are openly recorded on the blockchain and, with investigation, can be linked to individuals.

Digital Currency Exchanges

There are currently about 400 DCEs registered in Australia.

To date, regulation of crypto in Australia has centred on services provided by DCEs. Australian-based exchanges must abide by AML/CTF requirements and Know Your Customer (KYC) policies that apply to traditional financial institutions. They must also be registered with AUSTRAC.

Currently, there are no financial audit powers or minimum security baselines for DCEs, nor are there explicit consumer protections. This is despite the fact some exchanges oversee billions of dollars worth of trade each year and hold assets of significant value. The lack of security baselines has hindered the integration of more established and legitimate exchanges into the broader economy and impacted their ability to deal with banks and traditional financial intuitions. This has led to some of Australia's largest DCEs calling for the introduction of minimum security standards[23].

Exploring Cryptocurrency

[21]https://www.afr.com/companies/financial-services/apra-says-crypto-will-force-changes-to-the-regulatory-architecture-20220202-p59t77

[22]https://parlinfo.aph.gov.au/parlInfo/download/committees/reportsen/024747/toc_pdf/Finalreport.pdf;fileType=application%2Fpdf

[23]https://www.afr.com/technology/crypto-exchanges-beg-for-regulation-as-low-bar-poses-investor-risk-20210808-p58gvg

Mining for opportunities

Blockchain Technology

As mentioned throughout, distributed ledger technology maintains a decentralised record of transactions and currency ownership which underpins cryptocurrency. Blockchain, the most commonly used distributed ledger technology is useful to businesses beyond its cryptocurrency capabilities. It can increase brand trust through its ability to enhance transparency and provide an immutable record of assets for other purposes.

One such example is tracking supply chains. This not only enhances supply chain integrity but also provides greater assurances for consumers increasingly concerned with sustainability and the ethical production and sourcing of goods[24].

Global car manufacturers Volvo, Ford, BMW and Mercedes are developing blockchain initiatives, enabling production and process information regarding their products to be stored on the blockchain[25]. For example, Volvo is implementing blockchain technology to enhance traceability of raw materials used in its batteries, enhancing compliance with environmental protections and human rights[26].

Other proofs of concept and emerging applications have shown how tokenisation and blockchain technology could be applied in a range of circumstances to reduce friction in existing processes. Some examples include tokenised financial assets such as loans[27], carbon credits[28] and real estate[29] .

Payment acceptance

The adoption of cryptocurrency as a means of payment alongside fiat currency is increasing. It is estimated more than 2,300 US businesses accept Bitcoin[30], including large consumer brands like Microsoft, PayPal, the US National Basketball Association and Hockey League, and food giants KFC, Subway and Pizza Hut[31].

Businesses stand to benefit from cryptocurrency innovation just as much as consumers, with quick and irreversible payments, low transaction fees and improved transactional security[32]. Additionally, markets with the most rapid uptake of cryptocurrency as a method of payment have been those without access to traditional banking systems or mistrust in traditional financing. This enables businesses to tap into a new set of customers.

[24] https://hbr.org/2020/05/building-a-transparent-supply-chain

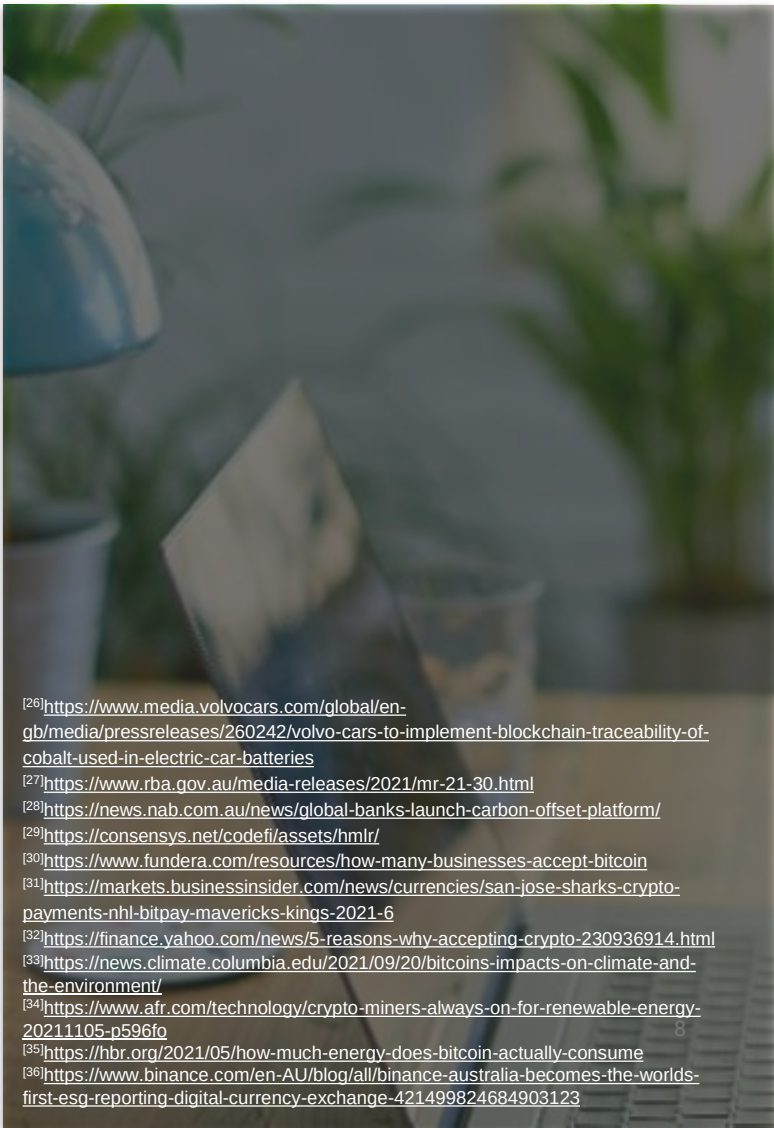
[25] https://www.press.bmwgroup.com/global/article/detail/T0307164EN/bmw-group-uses-blockchain-to-drive-supply-chain-transparency?language=en
https://media.mercedes-benz.com/article/c48af76e-e285-4020-b3d2-327f61aac23f

Carbon Zero

The environmental impact from the significant energy used by some cryptocurrency mining has not gone unnoticed. Bitcoin is thought to consume 707 kwH per transaction. In addition, the computers used consume additional energy because they generate heat and need to be kept cool [33].

Many large players in the crypto industry are actively attempting to offset carbon emissions, including positioning themselves as buyers of excess power [34], leveraging renewable energy sources, such as hydro, in situations where the energy would otherwise be 'wasted' [35].

Some Australian entities are leading the carbon neutral crypto activities, with an AUSTRAC-registered Australian exchange becoming the world's first digital currency exchange to commence reporting on Environmental, Social, and Governance (ESG) metrics to increase the transparency of the ESG footprint of organisations in the digital asset industry[36].



[26] https://www.media.volvocars.com/global/en-gb/media/pressreleases/260242/volvo-cars-to-implement-blockchain-traceability-of-cobalt-used-in-electric-car-batteries
[27] https://www.rba.gov.au/media-releases/2021/mr-21-30.html
[28] https://news.nab.com.au/news/global-banks-launch-carbon-offset-platform/
[29] https://consensys.net/codefi/assets/hmlr/
[30] https://www.fundera.com/resources/how-many-businesses-accept-bitcoin
[31] https://markets.businessinsider.com/news/currencies/san-jose-sharks-crypto-payments-nhl-bitpay-mavericks-kings-2021-6
[32] https://finance.yahoo.com/news/5-reasons-why-accepting-crypto-230936914.html
[33] https://news.climate.columbia.edu/2021/09/20/bitcoins-impacts-on-climate-and-the-environment/
[34] https://www.afr.com/technology/crypto-miners-always-on-for-renewable-energy-20211105-p596fo
[35] https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume
[36] https://www.binance.com/en-AU/blog/all/binance-australia-becomes-the-worlds-first-esg-reporting-digital-currency-exchange-421499824684903123

Looking forward: Building a crypto-secure future for Australia

While there are a number of important steps being taken to better regulate and provide increased transparency for cryptocurrencies in Australia - with the Bragg Report setting the direction of the developing regulatory framework in addition to the existing and evolving ASIC, AUSTRAC, and APRA requirements as well as consumer protection laws - there is more work to be done.

There is a need for regulatory settings that provide greater clarity and confidence about how the cryptocurrency market can operate in Australia.

Clarifying the regulation of the broader range of cryptocurrency service providers beyond those DCEs regulated for AML/CTF purposes (including products and services), and harmonising with international regulatory best practice, could support the continued maturing of the sector and make Australia a more attractive market for legitimate innovation, investment in and use of cryptocurrency.

Cyber security and cyber crime mitigation must be key considerations of crypto adoption. While in our paper we have considered various aspects of cryptocurrency, the following recommendations look at crypto through the lens of cyber security and cyber crime, not the wider financial system and its stability. The Industry Advisory Committee recommends the following areas should be further explored by the Federal Government to help ensure the safe adoption of cryptocurrencies in Australia.

Minimum cyber security standards: Cyber security has to be a key consideration when it comes to the adoption of cryptocurrencies. The committee recommends the consideration of mandated minimum cyber security standards for registered DCEs and businesses that hold crypto assets operating in Australia. However, this must be a shared responsibility and businesses using cryptocurrencies should also take appropriate steps to ensure strong cyber security measures are in place.

Capability: Industry, government, law enforcement, regulatory and criminal intelligence agencies need to be properly resourced to meet the demands of the complex digital world. There should be a focus on increased specialist training about the nexus between the cryptocurrency opportunities and cyber crime and increased public awareness messaging about the role cryptocurrency plays in facilitating crime.

The Australian Government has confirmed it is working with state and territory governments to prioritise efforts and equip agencies with the relevant capabilities. This includes investments to bolster the AFPs ability to investigate and prosecute cyber criminals, seizing and freezing cryptocurrency suspected as being proceeds of crime and enhancing intelligence capabilities.

Follow the lead: Coordinate more purposefully with like-minded nations to ensure 'breaking the chain' work is coordinated, tax evasion is managed and International Funds Transfer Instruction (IFTI) reporting is implemented to track the movement of illicit funds and related penalties.

A number of nations are taking significant steps to building cryptocurrency capacity and capability domestically. Australia should follow the example of countries leading the way, learning from their experiences and coordinating international best practice with respect to cybersecurity in cryptocurrency.

Transparency: Consumers would be encouraged to make more informed decisions about using and investing in cryptocurrency if there was increased transparency around registered DCEs and providers of blockchain- based financial products or services that hold AFSLs.

Educational programs with accurate, consistent messaging will allow investors to better understand both the investment and cybersecurity risks while helping to demystify cryptocurrencies for all Australians.

The Federal Government's implementation of The Bragg Report recommendations will play a key role in creating an environment of increased transparency, building consumer confidence into the future.

Crypto Resources

The following resources provide guidance, support and the latest developments, including actions to take on the secure use of cryptocurrency:

- MoneySmart content on ASIC
- ASIC's Information Sheet 225 Crypto-assets
- Bragg Report
- Review of the Australian Payment Systems
- Parliamentary Joint Committee on Corporations and Financial Services – Mobile Payment and Digital Wallet Finance Services
- Transforming Australia's Payment System (Government response to the above 3 reports)

Cyber Security Industry Advisory Committee

March 2022