CRIME AND CRYPTOCURRENCY IN AUSTRALIAN COURTS

AARON M LANE* AND LISANNE ADAM**

This article presents the findings of the first empirical study of reported Australian case law involving Bitcoin and other cryptocurrencies between 2009 and 2020. The initial dataset consists of 103 cases, with 59 criminal decisions and 44 other decisions. Focusing on criminal proceedings, the study finds that cryptocurrency has been considered in the context of bail, extradition, restraining orders, trials and sentencing. Significantly, the study finds that the use of cryptocurrency in the commission of an offence is seen by courts as a factor that tends to increase the sophistication or seriousness of the offence — becoming an aggravating factor in sentencing — and leads the court to consider general deterrence above other sentencing purposes.

I INTRODUCTION

There is a perception that Bitcoin, and the other cryptocurrencies that followed, are associated with criminal activity.[1] By our count, there are four dimensions to this perception from the literature — which is briefly surveyed here as introductory context for the first study on crime and cryptocurrency in the Australian courts.

* Senior Lecturer in Law, Graduate School of Business and Law; Senior Research Fellow, RMIT Blockchain Innovation Hub, RMIT University, Melbourne. Honorary Postdoctoral Associate, University of Divinity. Special Counsel, Duxton Hill. Email: aaron.lane@rmit.edu.au.

** Associate Lecturer in Law, Graduate School of Business and Law, RMIT University, Melbourne.

The authors presented preliminary data from this study to the 2019 Australian and New Zealand Society of Criminology Conference and to the Stanford Internet Observatory's Symposium on Cryptocurrency and Societal Harm at Stanford University in 2022. The authors extend thanks to Professor Bronwyn Naylor for her helpful and considered feedback on an earlier draft along with that of two anonymous reviewers.

1 See, eg, Jonathan Lane, 'Bitcoin, Silk Road, and the Need for a New Approach to Virtual Currency Regulation' (2014) 8(4) *Charleston Law Review* 511; Alice Huang, 'Reaching within Silk Road: The Need for a New Subpoena Power That Targets Illegal Bitcoin Transactions' (2015) 56(5) *Boston College Law Review* 2093; Eric Engle, 'Is Bitcoin Rat Poison? Cryptocurrency, Crime, and Counterfeiting (CCC)' (2016) 16(2) *Journal of High Technology Law* 340.

First, law enforcement experts claim that Bitcoin is 'the currency of choice for cybercriminals'[2] in the commission of ransomware attacks and other forms of theft and extortion in the digital environment.[3] Also in this category, are cybercriminals using cryptocurrency to run fraudulent investment scams. Statistics collected by the Australian Competition and Consumer Commission show that '[i]n 2019, reported losses for cryptocurrency scams exceeded $21.6 million from 1810 reports'.[4] Data reported by Chainalysis puts the global figure at USD7.8 billion.[5]

Second, cryptocurrencies are used to exchange illegal goods and services from 'dark web' online marketplaces, such as Silk Road, which exclusively used Bitcoin for the platform's illicit transactions.[6] Famously, Silk Road's founder Ross Ulbricht was convicted in the United States and sentenced to life imprisonment for charges relating to his role in the criminal enterprise.[7] The convictions were upheld on appeal notwithstanding that two federal agents were also charged and sentenced for their conduct in the course of the investigation against Ulbricht, including misappropriating Bitcoin into offshore bank accounts.[8] The Ulbricht saga brought into popular consciousness the fact that cryptocurrencies provided a new payment platform for those seeking to illicitly transact with counterparts across borders, pseudonymously. While estimates vary, the most recent industry analysis reports total illicit cryptocurrency transactions at USD14 billion in 2021 — although this equates to just 0.15% of the total volume of cryptocurrency transactions.[9]

Third, Bitcoin has been described as a 'criminal's laundromat for cleaning money' that has been earned from illicit enterprises.[10] Of course, money laundering is a

2 Steven David Brown, 'Cryptocurrency and Criminality: The Bitcoin Opportunity' (2016) 89(4) *Police Journal* 327, 336.

3 See, eg, Masarah Paquet-Clouston, Bernhard Haslhofer and Benoît Dupont, 'Ransomware Payments in the Bitcoin Ecosystem' (2019) 5(1) *Journal of Cybersecurity* 1.

4 Australian Competition and Consumer Commission, *Targeting Scams 2019: A Review of Scam Activity Since 2009* (Report, June 2020) 18.

5 Chainalysis, *The 2022 Crypto Crime Report: Original Data and Research into Cryptocurrency-Based Crime* (Report, February 2022) 5.

6 See Amy Phelps and Allan Watt, 'I Shop Online — Recreationally: Internet Anonymity and Silk Road Enabling Drug Use in Australia' (2014) 11(4) *Digital Investigation* 261; James Martin, 'Lost on the *Silk Road*: Online Drug Distribution and the "Cryptomarket"' (2014) 14(3) *Criminology and Criminal Justice* 351; Sesha Kethineni, Ying Cao and Cassandra Dodge, 'Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes' (2018) 43(2) *American Journal of Criminal Justice* 141.

7 *United States v Ulbricht*, 31 F Supp 3d 540 (SD NY, 2014).

8 See *United States v Ulbricht*, 858 F 3d 71, 105–14 (2nd Cir, 2017).

9 Chainalysis (n 5) 3–4.

10 Mitchell Hyman, 'Bitcoin ATM: A Criminal's Laundromat for Cleaning Money' (2015) 27(2) *St Thomas Law Review* 296. See also Rolf van Wegberg, Jan-Jaap Oerlemans and Oskar van Deventer, 'Bitcoin Money Laundering: Mixed Results?' (2018) 25(2) *Journal of Financial Crime* 419; Russ Marshall, 'Bitcoin: Where Two Worlds Collide' (2015) 27(1) *Bond Law Review* 89.

serious criminal offence in and of itself.[11] Although, initially, the use of Bitcoin and other cryptocurrencies were not subject to the same regulatory constraints as the use of fiat currency.[12] In 2017, the Federal Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism asserted that '[i]t is recognised globally that convertible digital currencies, such as bitcoin, pose significant money laundering and terrorism financing risks because they allow people to move money around the world on a peer-to-peer basis without revealing their identity'.[13]

On this basis, the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) ('*AML CTF Act*') was amended to require Australian cryptocurrency exchanges to comply with Anti-Money Laundering and Counter-Terrorism Financing laws under the Australian Transaction Reports Analysis Centre's ('AUSTRAC') purview.[14] The stated purpose of the amendments was to 'deter criminals from using convertible digital currencies to move illicit funds and avoid detection' and to 'facilitate the collection of transactional information about exchanges in digital currency for use by law enforcement, intelligence and national security agencies'.[15] At the end of February 2022, AUSTRAC had revoked the registration of seven cryptocurrency exchanges, suspended another, and refused to register a further six exchanges.[16]

Fourth, there are concerns that cryptocurrencies could be used for tax evasion.[17] The Australian Taxation Office has provided guidance on various issues surrounding the tax treatment of cryptocurrency.[18] As with money laundering, the pseudonymous, borderless nature of cryptocurrency transactions — combined with Australia's tax system of self-assessment — means that the task of tax enforcement is more difficult and provides a greater opportunity for tax evasion. Tax evasion is

11 *Criminal Code Act 1995* (Cth) sch div 400 ('*Criminal Code Act*').

12 See Kevin Werbach, 'Trust, but Verify: Why the Blockchain Needs the Law' (2018) 33(2) *Berkeley Technology Law Journal* 487.

13 Commonwealth, *Parliamentary Debates*, House of Representatives, 17 August 2017, 8833 (Michael Keenan, Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism) ('*Parliamentary Debates*').

14 *Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017* (Cth).

15 *Parliamentary Debates* (n 13) 8834 (Michael Keenan, Minister for Justice and Minister Assisting the Prime Minister for Counter-Terrorism).

16 'Digital Currency Exchange Provider Registration Actions', *AUSTRAC* (Web Page) <https://www.austrac.gov.au/digital-currency-exchange-provider-registration-actions>.

17 See, eg, Thomas Slattery, 'Taking a Bit Out of Crime: Bitcoin and Cross-Border Tax Evasion' (2014) 39(2) *Brooklyn Journal of International Law* 829; Jason Clark and Margaret Ryznar, 'Improving Bitcoin Tax Compliance' [2019] (Spring) *University of Illinois Law Review* 70. Cf Arvind Sabu, 'Reframing Bitcoin and Tax Compliance' (2020) 64(2) *Saint Louis University Law Journal* 181.

18 Australian Taxation Office, *Income Tax: Is Bitcoin a 'Foreign Currency' for the Purposes of Division 775 of the* Income Tax Assessment Act 1997*?* (TD 2014/25, 17 December 2014); 'Tax Treatment of Cryptocurrencies', *Australian Taxation Office* (Web Page) <https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/>. See generally Nathan De Zilva, 'The Evolving Tax Treatment of Cryptocurrencies' (2018) 52(7) *Taxation in Australia* 372.

a crime regardless of the underlying legitimacy of the transaction that gave rise to the taxable event.[19]

As this introduction outlines, it appears that criminal entrepreneurs were among the first to find a use case for cryptocurrencies. It is not surprising, therefore, that law enforcement and regulatory agencies around the world have established digital taskforces focusing on crime and cryptocurrency.[20] Domestically, the Australian Federal Police's ('AFP') Cybercrime Operations Unit and the Australian Transaction Reports and Analysis Centre ('AUSTRAC') have primary carriage of these matters among enforcement bodies, in addition to the Australian Cyber Security Centre.[21] State and territory police forces also appear to have developed some capabilities in this area.[22]

Against this background, it was inevitable that criminal cases involving cryptocurrency would come before the Australian courts. However, there is currently no reported data on criminal cases involving cryptocurrency in Australia.[23] The purpose of this article, therefore, is to investigate in what contexts Bitcoin and other cryptocurrencies have been considered in criminal matters before Australian courts and critically analyse how the use of cryptocurrency has factored into judicial decision making in the context of criminal proceedings. This article will proceed as follows. Part two introduces Bitcoin and cryptocurrencies. Part three explains the study's methodology and reports the study's quantitative findings. Part four provides the study's qualitative findings. Part five will bring the study's findings into conversation with theoretical perspectives from the law and economics and criminology literatures. Part six concludes.

II AN INTRODUCTION TO BITCOIN AND CRYPTOCURRENCIES

In January 2009, the Bitcoin network launched with a transaction embedded with an encrypted message, lifted from the front-page of British newspaper *The Times*,

19 See, eg, *Criminal Code Act* (n 11) sch s 134.2; *Taxation Administration Act 1953* (Cth) pt III div 2.

20 See, eg, Attorney General's Cyber Digital Task Force, United States Department of Justice, *Cryptocurrency: Enforcement Framework* (Report, October 2020); AUSTRAC, *AUSTRAC Annual Report 2019–20* (Report, September 2020) 35.

21 'Cyber Security', *Australian Signals Directorate* (Web Page) <https://www.asd.gov.au/cyber>.

22 See, eg, Simone Fox Koob, 'How a Now-Defunct Site on the Dark Web Led Police to the Biggest Cryptocurrency Seizure in Australia', *The Age* (online, 20 August 2021) <https://www.theage.com.au/national/victoria/dark-web-drug-investigation-leads-to-record-cryptocurrency-seizure-20210820-p58kff.html>.

23 For a review of Federal United States decisions, see Claire Nolasco Braaten and Michael S Vaughn, 'Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions' (2021) 42(8) *Deviant Behavior* 958.

'Chancellor on brink of second bailout for banks'.[24] By January 2021, mainstream news outlets were reporting that the price of Bitcoin had surpassed USD40,000 for the first time — pushing the global market capitalisation of cryptocurrencies towards USD1 trillion.[25] Bitcoin leveraged cryptography and a decentralised network of computing power to create a peer-to-peer electronic payment system that promised a 'version of electronic cash' that would allow 'online payments to be sent directly from one party to another without going through a financial institution'.[26] This part of the article outlines the main features of Bitcoin and how cryptocurrencies are acquired and stored, and analyses the significance of this for criminal investigations.

A Bitcoin: A Peer-to-Peer Electronic Cash System

The most significant feature of the Bitcoin cryptocurrency is that it solves the 'double-spending problem' without a trusted intermediary. In the digital environment, it is trivially easy to copy information. Any digital currency must ensure that when Alice pays Bob $100, for example, Alice cannot spend those funds again. Previous attempts to create a native digital currency solved the double spending problem using trusted corporate entities that controlled the issue of currency, processed the transactions, and reconciled the accounts.[27] However, many of these digital currency projects were short-lived because centralisation meant legal exposure to corporate insolvency and other forms of litigation.[28] Bitcoin, by contrast, solved the double-spending problem though decentralisation and transparency.

Bitcoins are a 'chain of digital signatures' that form a timestamped public record of transactions on a peer-to-peer network.[29] Using asymmetric cryptography, users have a pair of keys — one public, one private. Alice can send cryptocurrency to Bob by using her private key to digitally sign a transaction combining a 'hash' of the previous transaction (an algorithmic way of pointing to the previous transaction without needing all the input data) and Bob's public key. This process allows Bob (or anyone else) to 'verify the signatures to verify the chain of ownership'.[30] The transaction from Alice to Bob is 'immutable' in the sense that the transaction

24 'Bitcoin Block 0', *Blockchair* (Web Page) <https://blockchair.com/bitcoin/block/0>, quoting Francis Elliott, 'Chancellor Alistair Darling on brink of second bailout for banks', *The Times* (online, 3 January 2009) <https://www.thetimes.co.uk/article/chancellor-alistair-darling-on-brink-of-second-bailout-for-banks-n9l382mn62h>.

25 See, eg, Charles Bovaird, 'Bitcoin Has Climbed Above $40,000 Again: What's Next?', *Forbes* (online, 14 January 2021) <https://www.forbes.com/sites/cbovaird/2021/01/14/bitcoin-has-climbed-above-40000-again-whats-next/>.

26 Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (White Paper, 31 October 2008) 1 <https://bitcoin.org/bitcoin.pdf>.

27 Chris Berg, Sinclair Davidson and Jason Potts, *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics* (Edward Elgar Publishing, 2019) 5.

28 Ibid.

29 Nakamoto (n 26) 2.

30 Ibid.

cannot be reversed. To prevent double spending, a consensus mechanism is needed for network participants ('nodes') to agree on a single transaction history.

The Bitcoin protocol works by newly signed transactions being broadcast to the network of nodes that gather these transactions into a 'block'.[31] Nodes then compete to solve computationally-complex problems for the right to add its block to the chain of previous transactions (providing the monikers 'blockchain' for the underlying technology, and 'proof-of-work' for this type of consensus mechanism).[32] Nodes are incentivised to maintain the network because the right to add a new block comes with a Bitcoin reward, which is currently 6.25 Bitcoin.[33] The Bitcoin protocol is 'permissionless' in the sense that anyone with enough computing power and data speeds can download the software and start 'mining'.[34] On this basis, the proof-of-work protocol effectively converts energy, computing power, and the internet into trust — rather than relying on a third-party intermediary.[35]

In a criminal context, the lack of a central intermediary through a decentralised network is attractive for criminals and simultaneously poses challenges for law enforcement. Significantly, decentralisation means that there is no single authoritative entity keeping transaction records. This is an advantageous feature of a payments system for criminal operators as payments can be sent to counterparties or associates located offshore almost instantaneously, placing assets outside of the jurisdiction of domestic law enforcement authorities and beyond the practical effect of domestic court orders. It also means that the payment system is censor resistant. That is, even if mining or usage is banned in some jurisdictions (eg as occurred in 2021 in China by its central bank), the transaction record is stored in a multitude of locations simultaneously and the network will continue to operate so long as nodes elsewhere continue to run the protocol. Further, decentralisation of control of the cryptocurrency assets to the individual user means that these transactions cannot be prevented without gaining control of the relevant private keys.

Another feature of cryptocurrency payments is the separation between payments and identity. While a cryptocurrency's protocol generally requires that transactions

31 Ibid 3.

32 Ibid.

33 Ibid 4. See also Ted Stevenot and Stephen Hall, 'How Does the Bitcoin Source Code Define its 21 Million Cap?', *Unchained Capital* (Web Page, 23 June 2022) <https://unchained.com/blog/bitcoin-source-code-21-million/>.

34 'The bitcoin system depends upon a process known as mining, by which individuals or groups of individuals use sophisticated computer systems to validate bitcoin transactions. Successfully completing the validation process results in an award to the anonymous miner of newly generated bitcoin.': Benjamin Akins, Jennifer L Chapman and Jason Gordon, 'The Case for the Regulation of Bitcoin Mining as a Security' (2015) 19(3) *Virginia Journal of Law and Technology* 669, 673, citing 'Help: Introduction', *Bitcoin Wiki* (Web Page) <https://en.bitcoin.it/wiki/Help:Introduction>.

35 Berg, Davidson and Potts (n 27) 3.

are public (and therefore traceable through blockchain analytics),[36] the public addresses are pseudonymous. That is, a cryptocurrency address is a unique string of 26–35 alphanumeric characters with no direct link between the address and the user's identity (unlike a bank account number, there is no financial institution for law enforcement to obtain identity documents and account-opening information). In a practical sense, this means that '[t]he public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone'.[37] It is also easy for users to generate additional addresses — so users could maintain their privacy by generating a new address each time they want to receive a cryptocurrency payment.

In summary, decentralisation and pseudonymity make cryptocurrency networks an attractive payments platform for criminals because the technology facilitates borderless and censor resistant peer-to-peer asset transfers, in a way that is difficult to establish the identity of parties behind a transaction. Nevertheless, these challenges for law enforcement are mitigated through how users will acquire and store cryptocurrencies, which is explained below.

B Acquiring Cryptocurrency

There are three ways to initially acquire cryptocurrency. First, cryptocurrency can be generated by 'mining', as discussed above. A cryptocurrency's protocol will determine the rewards — such as newly minted tokens or transactions fees — that will accrue to miners that participate in the network's operations. Mining can be done by a single miner on a large scale or by several miners in a pool. Whether mining proceeds are used to fund illicit activities cannot be readily detected (unless converted to fiat currency through an exchange, discussed below). Instead, recall that mining for proof-of-work consensus mechanisms requires significant computing power and electricity.[38] In an investigation context, this translates to physical evidence (eg computer hardware) and documentary evidence (eg energy consumption records). Law enforcement agencies, using their investigative powers, could obtain and analyse this evidence.

Second, cryptocurrency can be acquired by purchasing it through a cryptocurrency exchange. Exchanges are the onramps to the crypto economy, where users deposit money from a bank account or credit card. Most users acquire cryptocurrency in this way. 'Bitcoin ATMs' were a primordial exchange, existing as a physical kiosk. Today, most exchanges operate online. In Australia, cryptocurrency falls within the definition of 'digital currency' and a cryptocurrency exchange as a 'digital

36 Blockchain analytics is technical field that is becoming increasingly advanced and professionalised, although open-source tools are available to the public — allowing anyone to attempt cryptocurrency tracing.

37 Nakamoto (n 26) 6.

38 Indeed, there is a body of literature on the environmental impact of cryptocurrency mining: see, eg, Jon Truby, 'Decarbonizing Bitcoin: Law and Policy Choices for Reducing the Energy Consumption of Blockchain Technologies and Digital Currencies' (2018) 44 (October) *Energy Research and Social Science* 399; Amanda Gulli, '(Un)Sustainability of Bitcoin Mining' (2020) 46(1) *Rutgers Computer and Technology Law Journal* 95.

currency exchange provider' is required to register with AUSTRAC.[39] The *AML CTF Act* imposes obligations on registered exchanges, including a requirement to verify a customer's identity, undertake on-going customer due diligence, and report suspicious transactions or transactions over $10,000.[40] Exchanges are also required to keep a log of information for reporting purposes including the type of cryptocurrency being used, the value of the cryptocurrency transaction, the user's IP addresses, the user's social media profiles, the user's cryptocurrency wallet details and the user's device details.[41] These 'Know Your Customer' ('KYC') requirements are intended to counteract the pseudonymity typically associated with cryptocurrency transactions.

Third, cryptocurrency can be acquired by receiving it from another person through a direct peer-to-peer transaction. As explained above, decentralisation and pseudonymity make this more difficult for law enforcement to link transactions to an identity. However, if the sender's address can be traced to a cryptocurrency exchange, then there will be a record of the sender's details who can be questioned to identify the recipient of the cryptocurrency. This is more than a hypothetical investigation strategy. As we will see in the next section of the article, witness testimony has played a key role in linking a cryptocurrency transaction to the accused in the context of a criminal trial.

C Storing Cryptocurrency

Once cryptocurrency is acquired, users monitor their holdings in a virtual 'wallet' that can be either 'custodial' or 'non-custodial'. A 'custodial' wallet is where a cryptocurrency exchange holds cryptocurrency on behalf of a user. The cryptocurrency exchange retains control of the private keys but provides a user with the ability to send and receive cryptocurrencies through the user's exchange account. By contrast, a 'non-custodial' wallet is where a user holds their own private keys and uses a software program or a hardware device to store cryptocurrency and perform transactions. If cryptocurrency was initially acquired through an exchange, a user may send from their custodial exchange wallet to a non-custodial wallet for storage.

Both wallet types provide avenues for investigations. In the case of custodial wallets, law enforcement could use investigative powers to obtain information from cryptocurrency exchanges. If a user is known, their transaction history could be obtained. If a public address is known, the identity of the user could be uncovered. Exchange records provide not only general intelligence for investigations purposes but also possible admissible evidence in legal proceedings as a 'business record'.[42] In the case of non-custodial wallets, physical evidence

39 *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) pt 6A ('*AML CTF Act*').

40 See ibid pts 2, 3.

41 *Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No 1)* (Cth) rr 18.2(21A), 19.3(8)(b).

42 See, eg, *Evidence Act 1995* (Cth) s 69 as an exception to the general rule against hearsay.

will exist either as a software wallet that is stored on a computer, tablet, or mobile device or as a standalone hardware wallet. As such, law enforcement could obtain search and seizure orders over this property — and forensic imaging may then be able to ascertain, trace and analyse transaction records. Further, orders may be obtained to compel disclosure of a 'seed phrase' associated with the private keys.[43]

D The Cryptocurrency Ecosystem

Bitcoin was the original cryptocurrency. As at January 2023, there are over 22,000 cryptocurrencies, although Bitcoin still maintains around 41% of the total cryptocurrency market value.[44] Ethereum — initially released in 2015 as a smart contract platform — is the second-largest cryptocurrency with around 19% of the total market value.[45] The aggregate value of the next eight cryptocurrencies by market capitalisation (Tether, BNB, USD Coin, XRP, Binance USD, Cardano, Dogecoin and Polygon) combine for approximately 22% of the market value — leaving the thousands of remaining 'alt coins' sharing in roughly 17% of the market value.[46]

Cryptocurrency is growing in domestic importance to consumers and policymakers. For instance, a Roy Morgan survey found that over 1 million Australian adults owned at least one cryptocurrency — with an estimated aggregate of $21.6 billion invested.[47] This follows an Australian Senate inquiry on blockchain and cryptocurrency issues, which tabled its final report in October 2021.[48] It is important, therefore, that the number of criminal cases involving Bitcoin and cryptocurrency are not overstated as a proportion of this ecosystem and are clearly understood.

III A SYSTEMATIC REVIEW OF REPORTED AUSTRALIAN CASES

This section of the article presents an empirical study of reported case decisions in Australian courts and tribunals. It has been argued that legal scholars regularly

43 'A seed phrase is a unique 12-worded password. In the event that the seed phrase … is lost, forgotten or corrupted, the Bitcoins will become inaccessible.': *Chen v Blockchain Global Ltd* (2022) 66 VR 30, 33 [9] (Attiwill J). Being published in 2022, this decision falls outside the study's dataset.

44 'Global Cryptocurrency Charts', *CoinMarketCap* (Web Page) <https://coinmarketcap.com>. Figures current as of 19 January 2023.

45 Ibid.

46 Ibid.

47 'Over 1 Million Australians now Own Cryptocurrencies such as Bitcoin, Ethereum, Ripple, Cardano, Dogecoin and Shiba Inu', *Roy Morgan* (Web Document, 12 April 2022) <https://roymorgan-cms-dev.s3.ap-southeast-2.amazonaws.com/wp-content/uploads/2022/05/25011419/8929-Cryptocurrency-February-2022.pdf>.

48 See Select Committee on Australia as a Technology and Financial Centre, Parliament of Australia, *Final Report* (Report, October 2021).

make claims about doctrinal trends without robust evidence.[49] Ideally, empirical research should be capable of replication.[50] A methodology known as 'systematic review', originally developed for literature reviews in the natural and medical sciences,[51] is a transparent process of data collection that allows replication and seeks to avoid analytical errors that may occur because of conscious or unconscious bias. In Australia, this methodology has been recently employed in law for conducting both systematic literature reviews[52] and case research.[53]

Professor William Baude and his colleagues advise a four-step process for 'systematic review for legal analysis' that involves: '(1) clearly stating the legal question that is being answered; (2) defining the sample of cases that will be used; (3) explaining how the cases in the sample will be weighted; (4) conducting the analysis of the sample of cases and stating the conclusion.'[54]

This part of the article addresses the first three steps before reporting the study's quantitative results. Part four of the article will then address the fourth step by providing a content analysis.

A Method

1 *Research Questions*

This study investigates two cascading research questions. First, 'in what contexts has blockchain or cryptocurrency been considered before Australian courts and tribunals?' (Research Question 1). As will be discussed below, the search to answer this question led to a significant number of reported criminal cases which informed the second research question. Second, 'in reported Australian criminal

49 William Baude, Adam S Chilton and Anup Malani, 'Making Doctrinal Work More Rigorous: Lessons from Systematic Reviews' (2017) 84(1) *University of Chicago Law Review* 37, 37–9.

50 See generally Lee Epstein and Gary King, 'The Rules of Inference' (2002) 69(1) *University of Chicago Law Review* 1. Cf Jack Goldsmith and Adrian Vermeule, 'Empirical Methodology and Legal Scholarship' (2002) 69(1) *University of Chicago Law Review* 153.

51 See, eg, the *Cochrane Database of Systematic Reviews* published by the Cochrane Library. See also Iain Chalmers, Larry V Hedges and Harris Cooper, 'A Brief History of Research Synthesis' (2002) 25(1) *Evaluation and the Health Professions* 12; Martin Starr et al, 'The Origins, Evolution, and Future of The Cochrane Database of Systematic Reviews' (2009) 25(S1) *International Journal of Technology Assessment in Health Care* 182.

52 See, eg, Alice Klettner, 'Challenges for Regulatory Reform in the Finance Sector: Learnings from the Last Decade' (2019) 30(3) *Journal of Banking and Finance Law and Practice* 151, 152–3.

53 See, eg, Luke McNamara et al, 'Evidence of Intoxication in Australian Criminal Courts: A Complex Variable with Multiple Effects' (2017) 43(1) *Monash University Law Review* 148; Amelia Loughland, 'Female Judges, Interrupted: A Study of Interruption Behaviour During Oral Argument in the High Court of Australia' (2019) 43(2) *Melbourne University Law Review* 822; Antonia Glover, 'What's Plainly Wrong in Australian Law? An Empirical Analysis of the Rule in *Farah*' (2020) 43(3) *University of New South Wales Law Journal* 850.

54 Baude, Chilton and Malani (n 49) 51.

proceedings, how did the use of cryptocurrency impact on the decision before the court?' (Research Question 2).

2 *Sample of Cases*

To address the research questions, a search of publicly available decisions[55] was conducted for all Australian court and tribunal decisions handed down in the period between 1 January 2009 (as the first Bitcoin transaction occurred in this month)[56] and 31 December 2020. The Australasian Legal Information Institute ('AustLII') case database was interrogated using the search terms 'Blockchain', 'Cryptocurrenc*', 'Crypto-currenc*', 'Crypto Currenc*', 'Distributed Ledger' (all deriving from the research questions), 'Bitcoin' and 'Ethereum' (the two most popular cryptocurrencies by market capitalisation), 'Initial Coin Offering' (a form of finance raising using cryptocurrencies), 'Digital Currenc*' and 'Virtual Currenc*' (cryptocurrency is a specific type of digital or virtual currency).

The AustLII database has previously been used for quantitative research. For example, it is used by Professors George Williams and Andrew Lynch in their long-running statistical survey of constitutional law decisions in the High Court of Australia.[57] Nevertheless, for robustness, a secondary search was conducted with the same search parameters using the Thomson Reuters Westlaw Australia case database — although this did not return any additional results. The search results underwent a preliminary screening for relevance to form the study's dataset. Four decisions were excluded from the dataset following a closer examination.[58]

3 *Categorising and Weighting of Cases*

There were two steps in categorising the cases. First, the total dataset (n=103) was read and manually coded based on year, jurisdiction, and the category of legal proceeding (administrative, civil, criminal, or family) so that criminal decisions

55 'Publicly available decisions' will be subsequently referred to as 'reported decisions' regardless of whether or not the decision has been published in a law report series.

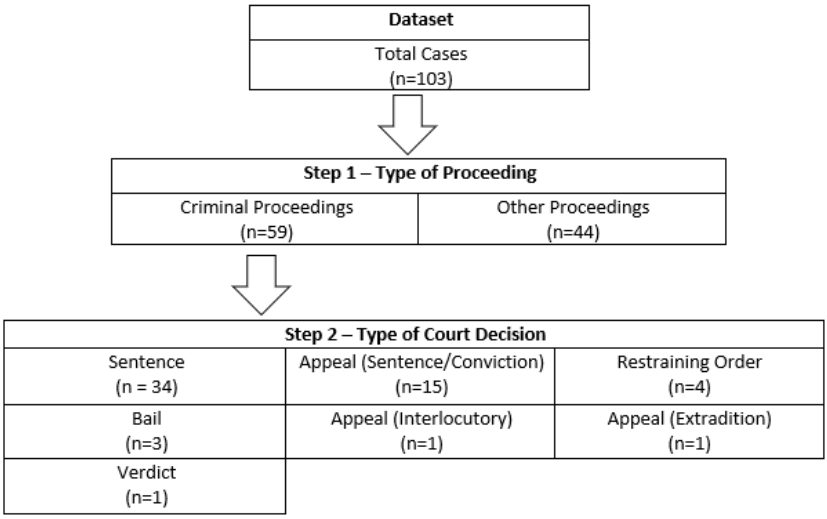
56 'Bitcoin Block 0', *Blockchair* (Web Page) <https://blockchair.com/bitcoin/block/0>.

57 See Andrew Lynch, 'The High Court on Constitutional Law: The 2019 Statistics' (2020) 43(4) *University of New South Wales Law Journal* 1226, app F. Note that an earlier study in this series used the Australian Law Reports: Andrew Lynch, 'The Gleeson Court on Constitutional Law: An Empirical Analysis of Its First Five Years' (2003) 26(1) *University of New South Wales Law Journal* 32.

58 *R v Gerges* [2018] NSWDC 483 was excluded due to an apparent spelling error recording an instructing solicitor's surname as 'Bitcoin' rather than 'Bitcon'; *Barber v Barber* [2016] FCCA 1783 was excluded as the trial judge at [87] uses 'bit-coin money' as a figure of speech; *Commissioner of Australian Federal Police v Arora* [2019] WASC 40 and *Re Sunlea Enterprises Pty Ltd and Federal Commissioner of Taxation* (2018) 108 ATR 427 were both excluded because language of the legislation quoted includes 'digital currency' but is otherwise irrelevant.

could be isolated.[59] A full list of cases is provided in Appendix A. Second, criminal proceedings (n=59) were further analysed and coded based on the subcategory of decisions being made by the court ahead of qualitative analysis. Figure 1 illustrates the categorisation process.

Figure 1: Australian Cryptocurrency Cases, Categorising of Cases



In terms of weighting, the objective of the search was to obtain the entire body of reported cases where blockchain or cryptocurrency had been judicially considered. The objective was not to construct a representative sample of cases. In this respect, the decisions are treated with equal weight from a quantitative perspective (although appellate-level decisions will be given greater weight in qualitative analysis).

There is, however, a limitation in this weighting. Similar to the study of Professor Luke McNamara and colleagues, the inclusion of all *reported* judgements tends to weigh the dataset towards appellate-level court decisions.[60] The specific data collection problem here is that Magistrates' Court or Local Court decisions are not

59 Although technically a civil action, restraining orders are included under criminal proceedings as they are brought by law enforcement bodies under proceeds of crime legislation where there is a reasonable suspicion of a serious or indictable offence. See, eg, *Proceeds of Crime Act 2002* (Cth) ss 18–19 ('*Proceeds of Crime Act*'). Similarly, restraining orders can be brought by corporate regulators investigating alleged criminal conduct under corporate laws. See, eg, *Corporations Act 2001* (Cth) ss 1323–4 ('*Corporations Act*'). Although technically an administrative action, extradition decisions are included under criminal proceedings as the action requires the alleged commission of an offence in the extradition country: see, eg, *Extradition Act 1988* (Cth).

60 See McNamara et al (n 53) 151–2.

ordinarily reported — yet these courts hear the bulk of criminal proceedings.[61] Additionally, while County Court or District Court reported decisions are captured in the dataset, not all cases in these courts are routinely reported either. Moreover, the reporting practices are not consistent across all Australian jurisdictions (providing a caveat in relation to jurisdictional breakdown of the results, below). Further, the dataset does not include cases where the jury returned a verdict of not guilty, where proceedings are discontinued, where the matter is remitted to the Magistrates' Court for summary hearing, or where the matter is dealt with under mental impairment orders. In Victoria, for example, these cases represent approximately a quarter of all criminal proceedings.[62] The implication is that the actual number of cases involving cryptocurrency is likely to be far higher than this study's dataset. Notwithstanding this, adopting McNamara and colleagues' reasoning, constructing a dataset of reported decisions is nevertheless an important quantitative contribution and provides a robust platform for qualitative analysis.[63] Indeed, any weighting towards appellate-level decisions adds strength to the study's doctrinal findings.

B Quantitative Results

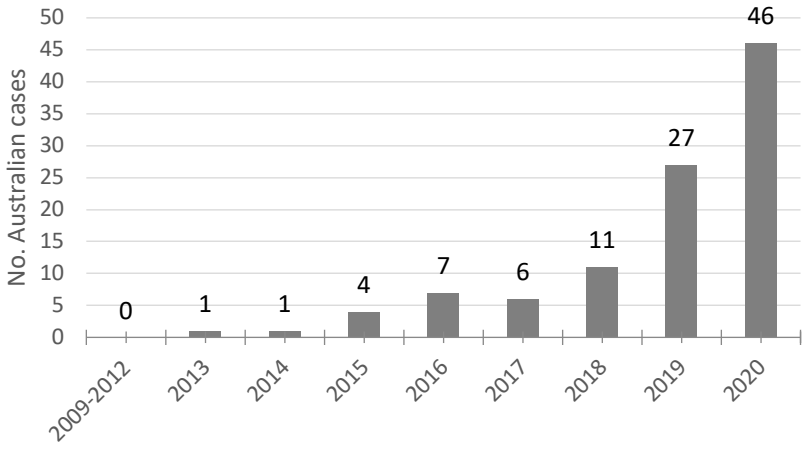
The results reveal no reported cases between 2009 and 2012. The first reported Australian case mentioning 'virtual currency' occurred in 2013 and the first case specifically mentioning 'Bitcoin' occurred in 2014. Starting from a low base, the last few years has seen an almost doubling of cases annually from six reported cases in 2017, 11 reported cases in 2018, 27 reported cases in 2019, and 46 reported cases in 2020. Figure 2 shows the total number of cryptocurrency cases in the Australian courts over time.

61 Ibid 152.

62 County Court of Victoria, *Annual Report 2018–19* (Report, 2019) 21 <https://www.countycourt.vic.gov.au/files/documents/2019-10/ccv-annual-report-2018-19.pdf>.

63 McNamara et al (n 53) 152.

Figure 2: Australian Cryptocurrency Cases, by Year



The results demonstrate that cryptocurrency cases were reported in all Australian jurisdictions in a variety of legal contexts. Figure 3 details the distribution of the collected cases across jurisdiction and type of proceeding. Most cases were criminal law matters (57%), followed by civil law (22%), administrative law (12%) and family law (9%).

In term of jurisdictions, State courts and tribunals in New South Wales (n=18) and Victoria (n=28) recorded the most reported cases, although this may be a function of higher populations. Tasmania recorded the lowest number of cases with just two reported decisions. The reported cases in federal courts and tribunals accounted for all the family law cases (n=9) and most of the civil litigation cases (60.9%) — an expected finding given the Commonwealth's primary jurisdiction over these matters.

Figure 3: Australian Cryptocurrency Cases, by Jurisdiction and Type of Proceeding

	Administrative	Civil	Criminal	Family	Total
ACT	-	-	8	-	8
Cth	9	14	2	9	34
NSW	2	5	11	-	18
NT	-	-	3	-	3
Qld	1	-	2	-	3
SA	-	1	2	-	3
Tas	-	-	2	-	2

Vic	-	1	27	-	28
WA	-	2	2	-	4
Total	12	23	59	9	103

In terms of administrative decisions, three of the 12 cases in the dataset refer to a previous criminal proceeding. Two of the reported administrative law cases refer to previous Australian criminal proceedings that were not reported.[64] Another administrative law case mentioned previous criminal proceedings in the United States, beyond the scope of this study.[65] Of course, it is not uncommon that a criminal conviction may provide the impetus for further disciplinary action brought by regulators under professional registration regimes. These cases provide evidence of unreported criminal cases involving the use of cryptocurrency, as discussed above.

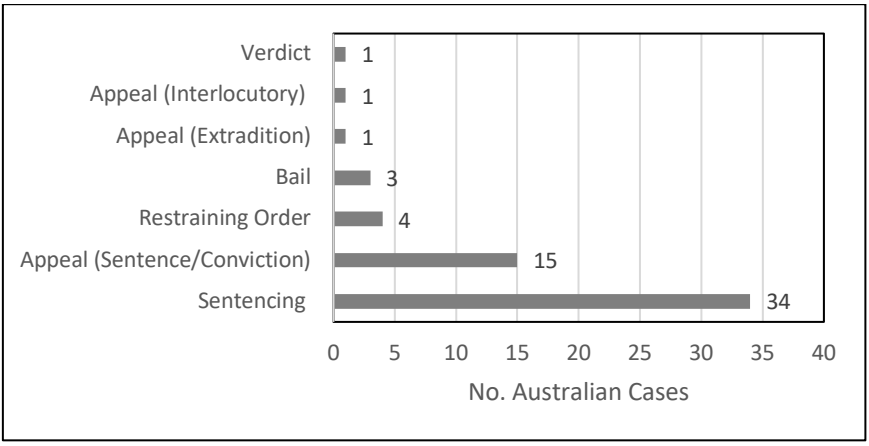
The results show cryptocurrency has been considered in a variety of criminal proceedings. In breaking down these criminal matters, the sheer volume of reported cases were sentencing decisions (n=49, 83.1%). These comprised sentencing decisions at first instance following a plea of guilty (n=32) or following a trial where the jury returned a guilty verdict on some or all the charges (n=2) and sentencing decisions on appeal (n=15).[66] The remaining decisions were applications for bail (n=3), applications for restraining orders seeking seizure of property or preventing the movement of persons (n=4), appeal against an order for extradition (n=1), an interlocutory appeal of an evidentiary ruling (n=1) or a verdict following a trial by judge alone (n=1). Figure 4 illustrates this breakdown.

64 *Health Care Complaints Commission (NSW) v Holbrook* [2019] NSWCATOD 146, involving an application to cancel the respondent's registration as a nurse following convictions in the District Court of NSW for drug offences — where a notebook was seized that referred to Bitcoin payment; *Merchant* [2019] AATA 1080, involving an application for review of a decision to cancel the applicant's visa where the applicant had previously been charged with proceeds of crime offences relating to Bitcoin transactions that were dismissed by the Magistrates Court.

65 *Nash v Chief Executive, Public Safety Business Agency* [2016] QCAT 126. This case involved the review of a decision to deny the applicant a 'blue card' under the *Working with Children (Risk Management and Screening) Act 2000* (Qld). A United States court had found the applicant guilty of conspiracy to commit narcotics trafficking and money laundering for his role in moderating an online chat forum associated with Silk Road, for which he had been paid in Bitcoin.

66 Note that if a reported court decision was subsequently appealed, both decisions are reflected in the summary statistics.

Figure 4: Australian Criminal Cryptocurrency Cases, by Subcategory, 2014–20



At an aggregate level, there are some general observations that can be made regarding the type of cryptocurrency used, the nature of the offending, and the resolution of criminal matters.

The criminal decisions in the dataset either refer to 'Bitcoin' specifically or 'cryptocurrency' generally as part of the case's factual matrix rather than other specific types of cryptocurrencies or blockchain-based crypto-assets. The only exceptions to this general proposition are two of the restraining order decisions in the Supreme Court of NSW where Ethereum and Litecoin are specifically named (discussed further in the next section).

Most of the criminal decisions in the dataset involve offences that relate to the importation, attempted importation or domestic possession or sale of border-controlled materials. Almost 80% of criminal decisions in the dataset (n=46) involved allegations of drug offences of one kind or another (ranging from minor possession charges through to more serious importation and commercial trafficking charges). The balance of the decisions included charges for firearms offences, child abuse material, identity theft, dealing with proceeds of crime, and money laundering. It is noted, however, that there were three decisions in the sub-set of criminal decisions where Bitcoin or cryptocurrency was not acutely germane to the charged offending. Instead, these were mentioned only as being relevant to the accused's personal background[67] or employment history.[68]

In those decisions where Bitcoin or cryptocurrency was relevant to the offending, it was generally identified as a means of payment for illicit goods or as the means by which proceeds of crime were dealt with. A closely related point is the high

67 *DPP (Cth) v To* [2017] VCC 475, [15] (Judge Davis).

68 *DPP (Cth) v Avignone-Green* [2018] VCC 755, [40] (Judge Coish); *DPP (Cth) v White* [2020] VCC 1846, [64] (Judge Wraight).

proportion of criminal decisions in the dataset that involved purchases from dark web markets — that is, exchanges that are 'carried out on an encrypted part of the internet called the TOR network'.[69] Just under half (47.5%, n=28) of criminal decisions in the dataset employ such various generic terms — 'dark net', 'dark web', 'deep web' or name specific marketplaces (including 'Alphabay', 'Black Market Rebooted', 'Dream', 'Olympus', 'Sheep' and 'Silk Road').

Amongst sentencing decisions, most proceedings were resolved by way of a plea of guilty — avoiding the need for a trial and the leading of evidence of cryptocurrency transactions. For those matters heard at first instance, 32 of 34 decisions involved the accused pleading guilty. In the two matters where the accused pled not guilty, the accused was ultimately convicted on some or all the charges and subsequently appealed.[70] The remaining appellate-level sentencing decisions (n=13) revealed that the appellant had pled guilty at first instance and was appealing the sentence imposed by the court below rather than appealing the conviction. The next section of the article unpacks these general observations further and draws out implications from a doctrinal standpoint.

IV QUALITATIVE ANALYSIS OF CRIMINAL DECISIONS

This section continues our systematic review, turning to a qualitative content analysis[71] of the reported criminal proceedings to answer our second research question — 'how did the use of cryptocurrency impact on the decision before the court?' (Research Question 2). The significance of cryptocurrency will depend on its legal context. For example, the legal considerations for granting bail are different from the legal considerations applying to sentencing. Accordingly, this section will separate the analysis based on the stage of the criminal proceeding: pre-trial applications (focusing on bail and restraining orders), trial (focusing on physical and documentary evidence, witness testimony and accused testimony) and sentencing decisions (where analysis considers aggravating factors and general deterrence).

A Pre-Trial Applications

1 *Bail*

An application for bail will be made where an accused has been detained because the police have refused bail or do not have power to grant bail. The legal test for courts granting bail differs between jurisdictions. Nevertheless, the structure of the decision-making process is similar. Generally, there is a presumption for bail

69 James Martin, *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs* (Palgrave Macmillan, 2014) 2.

70 *R v Baker [No 3]* [2019] ACTSC 365 ('*R v Baker*'); *Baker v The Queen* [2020] ACTCA 55 ('*Baker v The Queen*'); *DPP (Vic) v Zarghami* [2019] VCC 1520 ('*DPP (Vic) v Zarghami*'); *Zarghami v The Queen* [2020] VSCA 74 ('*Zarghami v The Queen*').

71 See, eg, Mark A Hall and Ronald F Wright, 'Systematic Content Analysis of Judicial Opinions' (2008) 96(1) *California Law Review* 63.

consistent with the presumption of innocence. However, for serious offences (including, relevantly, drug offences) the accused will be required to first 'show cause'[72] as to why detention is not justified, establish that there are 'special or exceptional circumstances'[73] or identify a 'compelling reason' or 'exceptional circumstances'[74] which justify the grant of bail (depending on the jurisdiction and on the charged offence). If bail is presumed or otherwise justified, then the prosecution has the burden of establishing that the accused would be an 'unacceptable risk' that could not be mitigated by bail conditions.[75] The dataset reveals that cryptocurrency is relevant to the nature and manner of the offence, the strength of the prosecution case, and the risk that the accused would fail to answer the charges if not detained.

In *Director of Public Prosecutions (NSW) v Hing* ('*DPP (NSW) v Hing*'),[76] the accused was initially granted bail in the Supreme Court of NSW and the Director of Public Prosecutions subsequently applied to the Court of Criminal Appeal for a 'detention application' to remand the accused.[77] The accused was charged with offences including supplying a large commercial quantity of drugs and dealing with proceeds of crime — suspected of laundering money using Bitcoin — and was required to 'show cause' as to why his detention was not justified. The evidence before the Court was that the accused met with 'a male witness' (who reportedly operated a legitimate Bitcoin business) and paid the witness $190,000 in cash in exchange for Bitcoin transferred either to the accused or an associate of the accused.[78] The witness 'told police he had sold Bitcoins to the [accused] in exchange for cash on at least five previous occasions for amounts between $10,000 and $60,000'.[79] Although there were no direct submissions or discussion about Bitcoin in the Court's reasons, this fact was directly relevant to the Court's consideration of bail in two respects. First, the act of exchanging cash for Bitcoin forms part of the actus reus of the offence of dealing with proceeds of crime, and the Court described the nature of the alleged offending as 'extremely serious organised, and somewhat sophisticated, criminal activity'.[80] A similar observation can be made about the relevance of digital currency in the sole extradition case in the dataset.[81] Second, the evidence of Bitcoin transactions from a witness — who had direct knowledge of the Bitcoin transactions — cooperating with the police

72 See, eg, *Bail Act 2013* (NSW) s 16A ('*Bail Act* (NSW)').

73 See, eg, *Bail Act 1992* (ACT) s 9C(2) ('*Bail Act* (ACT)').

74 See, eg, *Bail Act 1977* (Vic) ss 4A, 4C ('*Bail Act* (Vic)').

75 See, eg, ibid s 4E.

76 [2017] NSWCCA 325 ('*DPP (NSW) v Hing*').

77 See *Bail Act* (NSW) (n 72) s 50.

78 *DPP (NSW) v Hing* (n 76) [19]–[21] (Simpson JA, RA Hulme and Wilson JJ).

79 Ibid [20].

80 Ibid [61].

81 See *Rojas v United States of America* [2019] FCA 22, [11], [18] (Bromwich J).

contributed to the strength of the prosecution case. Ultimately, the Court concluded that the accused had not shown cause and bail was denied.[82]

In *Re Abaker*,[83] it was alleged that the accused 'utilised the "dark web" to purchase stolen credit card details using bitcoin' and used the stolen credit card details to make multiple purchases ('deception matters').[84] The accused was also charged with more serious armed robbery and drug trafficking offences. The applicant, appearing before the Supreme Court of Victoria, was required to show the existence of a compelling reason justifying a grant of bail. Among other submissions, the applicant relied on expert evidence from a psychologist who conducted an IQ test and determined that the applicant had 'extremely low intelligence'.[85] This is curious as the deception matters as alleged — ie using Bitcoin and the dark web — requires a degree of technical sophistication (compared with physically using a stolen credit card, for example). On this point, opposing bail, the prosecution argued that this evidence was 'inconsistent with how the applicant presented to police in the interview and in the intercepted phone calls, was inconsistent with the evidence of [a youth justice worker], and was *inconsistent with the offending itself*'.[86] Inconsistency could be a factor in the accused's favour if a low IQ — or a generally low technological competency — was adduced to prove that the accused could not have committed the charges as alleged, and this undermines the strength of the prosecution case.[87] This line of reasoning was not open in this case, however, as the accused had made admissions in respect of the deception charges.[88] Justice Tinney considered that the IQ evidence was 'highly questionable' but held that it was more relevant to sentencing considerations than the granting of bail — ruling that the accused had not met the test for bail based on other surrounding circumstances.[89]

In *Re Baker*,[90] the use of Bitcoin was directly raised by the prosecution in opposing an application for bail. In this decision, the accused was charged with serious drug offences meaning that there was no presumption for bail. The prosecution called a police informant who gave evidence that, amongst other matters, included cryptocurrency:

82 *DPP (NSW) v Hing* (n 76) [72]–[74] (Simpson JA, RA Hulme and Wilson JJ).

83 [2018] VSC 714 ('*Re Abaker*').

84 Ibid [15] (Tinney J).

85 Ibid [22].

86 Ibid [41] (emphasis added).

87 *Bail Act* (Vic) (n 74) s 3AAA(1)(b).

88 *Re Abaker* (n 83) [18] (Tinney J).

89 Ibid [44]–[49].

90 [2018] ACTMC 27 ('*Re Baker*').

> Constable Hawke suggested there is intelligence evidence to suggest that the applicant purchased significant bitcoin or crypto currency for the purposes of importing the drugs.
>
> There is no indication as to where that crypto currency is at the present time and given the restraints on the applicant's assets the concern is that he will access the crypto currency for the purposes of escape.[91]

On this evidentiary basis, the prosecution 'submitted that in their view there is a risk of failing to appear because of the access to the dark net and the crypto currency'.[92] Although it was not directly stated, the logic is clear — the accused could use cryptocurrency to fund an escape of the jurisdiction. The relevance is that the Court was required to consider 'the likelihood of the person appearing in court in relation to the offence'.[93] Although it was not one which the Court appeared to give significant weight as, in deciding to grant bail, Special Magistrate Hunter held that the 'risk of flight is a low level risk which could be mitigated by conditions'.[94]

2 *Restraining Orders*

Law enforcement agencies are empowered under proceeds of crime legislation to make an application to the court to restrain the respondent from dealing with property that is suspected to have been derived from criminal activity.[95] Corporate regulators can also seek restraining orders where the alleged criminal conduct breaches the *Corporations Act 2001* (Cth) ('*Corporations Act*').[96] The four restraining order decisions in the dataset are illuminating in terms of what can be inferred from the coverage of the orders and what the orders required of respondents.

Restraining orders must identify the particular property that is covered by the scope of the order. In *Commissioner of the Australian Federal Police v Kogan* ('*Kogan*'),[97] an application was made in the Supreme Court of NSW against two individuals suspected of money laundering along with two related companies. The AFP traced the relevant funds to the purchase of real estate, cars and cryptocurrency — with the orders pertaining to 'cryptocurrency' generally held in the name of one of the individuals and one of the corporate entities.[98] Compare this general order with the cases of *New South Wales Crime Commission v Ward*

91 Ibid [23]–[24] (Special Magistrate Hunter).

92 Ibid [37].

93 *Bail Act* (ACT) (n 73) s 22(1)(a)).

94 *Re Baker* (n 90) [53].

95 See, eg, *Criminal Assets Recovery Act 1990* (NSW); *Proceeds of Crime Act* (n 59).

96 *Corporations Act* (n 59) ss 1323–4.

97 [2019] NSWSC 1866 ('*Kogan*').

98 Ibid [12] (Beech-Jones J).

('*Ward*')[99] and *Commissioner of the Australian Federal Police v Bigatton* ('*Bigatton*')[100] that specifically identified the type of cryptocurrency.

In *Ward*, the Court ordered the restraint of 'all crypto, digital or virtual currencies (including but not limited to Bitcoin, Ethereum and Litecoin)' held by the defendant and seized by police.[101] The inclusion of Ethereum in addition to Bitcoin is perhaps not surprising given it is the second largest cryptocurrency by market capitalisation value (and was included in the initial search terms for the systematic review on this basis).[102] The specific inclusion of Litecoin in the orders may indicate that either law enforcement authorities had reason to suspect that this cryptocurrency is being used for illicit activity generally or in this specific case. Alternatively, Litecoin may have been included by virtue of its longevity (Litecoin was established in 2011 as a variation of the Bitcoin protocol, and transactions can be tracked in a similar way) or its continuing popularity (in the top ten cryptocurrencies by market capitalisation value at the time). In *Bigatton*, the Court ordered the restraint of Bitcoin in a digital wallet held by the first defendant, and Bitcoin and Ethereum in digital wallets held by the second defendant.[103] As such, the inclusion of 'Ethereum' in the *Bigatton* orders was based on actual evidence of asset holdings rather than an attempt to draft a broad order covering the field of cryptocurrencies.

Courts have the power to make ancillary orders that it considers appropriate, including requiring the respondent to provide information.[104] In *Kogan*, the Court made orders requiring one of the respondents to 'provide information about passwords, passcodes and security accounts relating to the storage of cryptocurrency' and orders for the Official Trustee to take control of the property.[105] Similar orders were made in *Bigatton*.[106] In both cases, although the courts did not provide a discussion of the logic behind these ancillary orders, it is envisaged that information orders were sought to give effect to the primary order.

For cryptocurrency, control is possession. A person does not possess cryptocurrency in a physical sense; the ability to transact using a particular cryptocurrency address demonstrates possession. Accordingly, if the facts of a case suggest the use of a hardware or software wallet, an ancillary information order will be required so that the device and the application can be unlocked, and the private keys can be revealed, and the cryptocurrency to be transferred under the control of the trustee. Additionally, the court will need to have regard to whether

99 [2019] NSWSC 140 ('*Ward*').

100 [2020] NSWSC 245 ('*Bigatton*').

101 *Ward* (n 99) sch 3.

102 See above Part III.

103 *Bigatton* (n 100) schs 2, 4.

104 *Proceeds of Crime Act* (n 59) s 39.

105 *Kogan* (n 97) [16]–[17] (Beech-Jones J).

106 *Bigatton* (n 100) [66] (Cavanagh J).

other restraining or ancillary orders are required over the devices themselves (such as phones, computers and hardware wallets). If the facts of a case suggest the use of an account on a digital currency exchange, an ancillary information order will be required to reveal the login details to the exchange's website along with any additional information required to meet any two-factor-authentication requirements (such as inputting information from an automated text message or an email upon attempting to log in). Alternatively, law enforcement agencies in some jurisdictions may use separate information gathering powers to obtain login information[107] or may seek warrants to compel information from a digital currency exchange. In *Ward*, cryptocurrency had been already 'seized by police'[108] following the respondent's arrest so control over the cryptocurrency was not in issue, accounting for why law enforcement did not apply for ancillary information orders — it sufficed that the NSW Trustee and Guardian was ordered to take control of cash property.[109]

An order of a different nature was made in *Australian Securities and Investments Commission v Vella-Arpaci*,[110] where the defendant was accused of fraudulent share sales. An ex parte application was made — and orders were granted — 'requir[ing] the defendant to deliver up to the Court her passport and prohibit her from leaving Australia without the consent of the Court'.[111] The Australian Securities and Investments Commission ('ASIC') submitted that the defendant was a flight-risk based, among other facts, on the information and belief that she had 'access to assets overseas, particularly assets held in the form of virtual or digital currencies'.[112] We are unable to speculate as to the extent of the information that ASIC held with respect to these assets as the brief reasons for the decision do not elaborate on this point and the affidavit in support of the application is not extracted. Nevertheless, recall that we have seen a submission of this kind before — namely, by the prosecution in *Re Baker* in the context of resisting a bail application, which was discussed above. Accordingly, in this case, as in *Re Baker*, the existence of cryptocurrency was one of the factual grounds for granting the order restraining the defendant's movement rather than as a basis for restraining any cryptocurrency assets.

107 For instance, law enforcement authorities may compel a suspect to unlock their devices whilst conducting a search pursuant to a special search warrant: see, eg, *Crimes Act 1958* (Vic) ss 465AAA(2)–(3), (7); *Summary Offences Act 1953* (SA) ss 74BR, 74BW; *Crimes Act 1914* (Cth) s 3LA; *Police Powers and Responsibilities Act 2000* (Qld) ss 154A–154B. For a discussion about the introduction and enforcement of these provisions, see Lisanne Adam and Greg Barns, 'Digital Strip Searches in Australia: A Threat to the Privilege Against Self-Incrimination' (2020) 45(3) *Alternative Law Journal* 222.

108 *Ward* (n 99) sch 3 (Davies J).

109 Ibid order 4.

110 [2019] FCA 644.

111 Ibid [1] (Davies J).

112 Ibid [8].

B Trial

The dataset reveals seven instances where the fact finder — a judge or a jury — considered evidence involving cryptocurrency. The seven decisions comprise five separate criminal proceedings: one interlocutory appeal,[113] one verdict of a judge-alone trial[114] and three jury trials resulting in a conviction on at least one of the charged offences.[115] Here, we distinguish between physical or documentary evidence, witness testimony and the accused's testimony.

1 *Physical or Documentary Evidence*

The acquisition and use of cryptocurrency will result in records stored on computers or other electronic devices that can be tied to a particular individual — in addition to the pseudonymous transaction records that exist on the blockchain network. Police could obtain this evidence using a search warrant or exercise police powers of search and seizure upon arresting a suspect.

In *Director of Public Prosecutions (WA) v Tran* ('*DPP (WA) v Tran*'),[116] the accused stood trial in the District Court of Western Australia before a judge and jury on one count of attempted drug possession and a second count of possessing unlawfully obtained property.[117] The Court at first instance heard that the accused's computer hard drive and mobile telephone were seized, among other items, following the execution of a search warrant at the accused's residential address.[118] An examination of the items revealed '[a] number of messages confirming purchases by the [accused] of Bitcoin' and '[i]n a one month period, about the time of the alleged commission of count 1, the [accused] made Bitcoin transactions worth $7,000'.[119] It is unclear if the accused put forward a positive defence in relation to the Bitcoin transactions. What is clear, as the Court of Appeal observed, is that the jury must have been satisfied beyond a reasonable doubt that the accused used Bitcoin to attempt to purchase drugs.[120] These factual findings were not challenged on appeal.[121]

113 *North (A Pseudonym) v DPP* (Cth) [2020] VSCA 1. Note that it is not clear how this proceeding was resolved due to the use of a pseudonym.

114 *R v D, CM* [2016] SASC 38 ('*R v D, CM*').

115 *R v Baker* (n 70); *Baker v The Queen* (n 70); *Tran v Western Australia* [2019] WASCA 50 ('*Tran*'); *DPP (Vic) v Zarghami* (n 70); *Zarghami v The Queen* (n 70).

116 (District Court of Western Australia, Petrusa DCJ, 17 October 2017) ('*DPP (WA) v Tran*').

117 *Tran* (n 115) [2] (Buss P and Mazza JA). Note that the decision at first instance does not form part of the dataset.

118 Ibid [16], [19].

119 Ibid [20].

120 Ibid [70].

121 Note that the appeal is discussed further in this section under sentencing.

In future trials, it is anticipated that the prosecution will adduce blockchain transaction records (for example, by a police informant or an expert witness to undertake tracing of cryptocurrency transactions)[122] or tender records held by digital currency exchanges.[123]

2 *Witness Testimony*

In addition to physical or documentary evidence of cryptocurrency transactions, or in cases where it has not been obtained, a witness may be called to provide this evidence. This occurred in *R v Baker [No 3]* ('*R v Baker*').[124] In this case, the accused pled not guilty to 12 charges relating to drug trafficking and dealing with proceeds of crime in the Supreme Court of the Australian Capital Territory. At trial, the prosecution's case was 'largely dependent'[125] on the evidence of an accomplice who had prior convictions but cooperated with police and agreed to give evidence against the accused in exchange for immunity and other charges being withdrawn.[126] The accomplice gave evidence that he and the accused sourced illicit drugs from China using a computer and paid with Bitcoin that the accused had obtained from another associate, which was relevant to one of the counts on the indictment.[127] Significantly, there was no direct evidence that confirmed the use of Bitcoin — although there was supporting evidence of a notebook at the accused's address containing the names of various drug suppliers on the dark web.[128]

In *R v Baker*, the reliability of the witness was in issue. Courts have long recognised there is a risk that evidence is unreliable in circumstances where a witness is an accomplice and obtains a benefit by giving evidence under immunity, and the trial judge has discretion to direct the jury on this basis.[129] Such a direction was given to the jury[130] — but the accused was nevertheless found guilty, indicating the jury had accepted the accomplice's evidence beyond reasonable doubt.[131] The accused was convicted and subsequently appealed. The Court of Appeal confirmed the need for the jury to scrutinise the accomplice's evidence but

122 See *Evidence Act 2008* (Vic) s 79 ('*Evidence Act* (Vic)').

123 Ibid s 48.

124 *R v Baker* (n 70). See also *Baker v The Queen* (n 70).

125 *R v Baker* (n 70) [5] (Burns J); *Baker v The Queen* (n 70) [9] (Mossop, Loukas-Karlsson and Abraham JJ).

126 *Baker v The Queen* (n 70) [9] (Mossop, Loukas-Karlsson and Abraham JJ).

127 *R v Baker* (n 70) [9] (Burns J).

128 *Baker v The Queen* (n 70) [75], [77] (Mossop, Loukas-Karlsson and Abraham JJ).

129 See, eg, *R v Checconi* (1988) 34 A Crim R 160, 167–72 (Roden J, Street CJ agreeing at 161, Slattery CJ at CL agreeing at 161).

130 *Baker v The Queen* (n 70) [67] (Mossop, Loukas-Karlsson and Abraham JJ).

131 *R v Baker* (n 70) [5] (Burns J). See also ibid [67].

held that the jury had been properly directed, and that the verdict was reasonably open to the jury.[132]

Alternatively, a witness may mention cryptocurrency while giving evidence — not for the purpose of proving the existence of cryptocurrency or a particular transaction, but for some other purpose. This was the circumstance of the references to 'Bitcoin' in the combined judge-alone trial of *R v D, CM* in the Supreme Court of South Australia.[133] In this case, three co-accused were charged with two counts of blackmail of another inmate while two of the accused were held on remand for other offences. The prosecution case relied almost exclusively on the victim's testimony. Bitcoin was mentioned by this witness in two respects. First, in relation to the witness' own previous offending, using Bitcoin for the purchase of drugs on the dark web.[134] Previous offending can be relevant to the assessment of the witness' credibility, affecting how much weight should be given to their testimony.[135] Second, in relation to the witness' conversations about Bitcoin with another person.[136] This was relevant to the likelihood of separate conversations taking place between the alleged victim and two of the co-accused. Ultimately, Sulan J found all the co-accused not guilty because the witness' evidence was untruthful or not reliable on a crucial matter.[137]

3 *Accused Testimony*

In any criminal trial, an accused cannot be compelled to give evidence as a witness in their own trial. This derives from the presumption of innocence and also the privilege against self-incrimination which the High Court has described as 'a basic and substantive common law right', and 'not simply a rule of evidence'[138] — notwithstanding that it also finds legislative expression.[139] A jury is not permitted to speculate about the reason or draw any negative inferences from the accused's failure to give evidence or call witnesses.[140] An accused does, therefore, have a choice about whether to give evidence in support of their own defence.

In *Director of Public Prosecutions (Vic) v Zarghami*, the accused chose to testify.[141] In that case, the accused was stopped and searched by police as he was leaving a casino. At the time, he was carrying thousands of dollars of cash in his

132 *Baker v The Queen* (n 70) [95] (Mossop, Loukas-Karlsson and Abraham JJ).

133 *R v D, CM* (n 114).

134 Ibid [41]–[43] (Sulan J).

135 *Evidence Act* (Vic) (n 122) s 55(2)(a).

136 *R v D, CM* (n 114) [121] (Sulan J).

137 Ibid [92], [146], [148].

138 *Reid v Howard* (1995) 184 CLR 1, 11 (Toohey, Gaudron, McHugh and Gummow JJ).

139 See, eg, *Evidence Act* (Vic) (n 122) s 17(2).

140 See, eg, *Jury Directions Act 2015* (Vic) ss 41, 42.

141 *DPP (Vic) v Zarghami* (n 70).

pockets, and over $100,000 was found in a backpack located in his car — along with illicit drugs and electronic devices containing incriminating materials. The accused was charged with offences under the *Drugs, Poisons and Controlled Substances Act 1981* (Vic). The possession of cash was the basis for a further charge of dealing with the proceeds of crime.

The accused chose to put forward a positive defence that the possession of cash was not related to drug dealing but related to his success as a gambler and a cryptocurrency trader.

> [The accused said that] the money alleged by the prosecution to be the proceeds of crime in fact came from [his] great success at gambling, with those legitimately obtained funds having then been invested in cryptocurrency transactions. [He] told the jury that [he] had recently … cashed out of those trades and that the money in the backpack related to those legitimately obtained and then retrieved funds.[142]

The jury acquitted Zarghami of the proceeds of crime charge.[143] The fact that the accused was involved in cryptocurrency trading was not disputed by the prosecution.[144] It stands to reason that the jury was not satisfied beyond reasonable doubt that the cash was proceeds of crime. However, the jury did not accept that the possession of drugs was for personal use and convicted him on the trafficking charges. Zarghami successfully appealed against the sentence on matters not relating to cryptocurrency.[145]

C Sentencing

Sentencing occurs where the accused pleads guilty or is found guilty following a trial. The accused may be re-sentenced if an appellate court finds an error in the sentencing decision and finds that it would impose a different sentence.[146] In Victoria, the *Sentencing Act 1991* (Vic) ('*Sentencing Act*') provides that the only purposes for which sentences may be imposed are punishment, deterrence, rehabilitation, denunciation, community protection, or a combination of those purposes.[147] Although different sentencing legislative regimes operate in each Australian jurisdiction, the general sentencing principles and factors are broadly consistent due to the unified common law.[148] Through a process known as

142 Ibid [9] (Judge Tinney).

143 Ibid [3].

144 Ibid [10].

145 See *Zarghami v The Queen* (n 70).

146 See, eg, *House v The King* (1936) 55 CLR 499.

147 *Sentencing Act 1991* (Vic) s 5(1) ('*Sentencing Act*').

148 Mirko Bagaric, Richard Edney and Theo Alexander, *Sentencing in Australia* (Lawbook, 8th ed, 2020) 5.

'instinctive synthesis'[149] the court considers all of the relevant factors — including aggravating and mitigating factors — in determining a just sentence. Legal scholars have identified hundreds of separate aggravating and mitigating factors that are relevant to sentencing.[150] This study adds a further factor — the use of cryptocurrency in the commission of the offence. This study's dataset contains 34 sentencing decisions at first instance and 15 appeals. The cases in the dataset fall into two broad themes: first, where the court found that the use of cryptocurrency contributed to the seriousness or the sophistication in the offending; second, and relatedly, where the court invokes the application of the sentencing purpose of general deterrence. This section will also discuss cases where the use of cryptocurrency was a neutral consideration or was explicitly held by the court not to be a relevant consideration.

1 *Seriousness and Sophistication of Offending*

The first doctrinal theme of the sentencing decisions is that sentencing judges have considered the fact of cryptocurrency to be an aggravating factor in sentencing. The rationale is that the use of cryptocurrency indicates a greater level of sophistication in the offending — which goes to the seriousness of the offence — as opposed to cryptocurrency being simply just another method of payment. This is relevant to the punishment and denunciation purposes of sentencing. Let us first consider the authorities in support of this proposition.

In *Director of Public Prosecution (Vic) v Millar*, the defendants pled guilty to indictable offences involving the importation and trafficking of drugs, along with other summary offences.[151] The defendants purchased drugs online via 'unknown websites' which were 'paid for through the online payment system Bitcoin'.[152] To finance the transactions, the defendants made cash deposits into a company's bank account and Bitcoin was then transferred into Millar's Bitcoin wallet.[153] The drugs were delivered to a post-office box in the name of an associate.[154] In one of the first reported cases to deal with cryptocurrency, Judge Wilmoth described Bitcoin as 'a legal system, but it allows purchasers to trade anonymously in unidentified goods, such as drugs as in this case'.[155] In response to defence submissions that the offending had the character of personal use (and was therefore less serious), Judge Wilmoth found that 'while the system used was simple in its concept and

149 See, eg, *Markarian v The Queen* (2005) 228 CLR 357, 378 (McHugh J): 'By instinctive synthesis, I mean the method of sentencing by which the judge identifies all the factors that are relevant to the sentence, discusses their significance and then makes a value judgment as to what is the appropriate sentence given all the factors of the case. Only at the end of the process does the judge determine the sentence.'.

150 Bagaric, Edney and Alexander (n 148) 270.

151 [2015] VCC 1883, [2], [5]–[6] (Judge Wilmoth).

152 Ibid [9].

153 Ibid [10].

154 Ibid [8], [12].

155 Ibid [10].

execution, an element of sophistication was demonstrated by the planning behind it'.[156]

In *R v Wallis* the defendant pled guilty to seven counts including drug offences.[157] Wallis made admissions to police 'that he bought the drugs online and paid for it by Bitcoin'.[158] In considering the seriousness of the offence, Mahony DCJ said that 'there was a degree of sophistication *in the manner in which he purchased the substances on the internet*, under a false name, and had them shipped to an abandoned warehouse to avoid detection'.[159] That is, the use of cryptocurrency was one factor among others which was indicative of seriousness.

Sentencing judges reached similar conclusions in the cases of *Director of Public Prosecutions (Cth) v Howard*,[160] *R v NE*,[161] *R v Baker*,[162] *Director of Public Prosecutions (Cth) v Petkovski*,[163] *Director of Public Prosecutions (Vic) v Kerovec*,[164] *R v Ha*[165] and *Director of Public Prosecutions (Cth) v Lou*.[166] These decisions involve a single judge, predominantly at the District or County Court level. There are, however, four appellate decisions in the dataset that consider the use of cryptocurrency and the seriousness of offending — providing weight to this first doctrinal theme.

First, in *Dunning v Tasmania* the Court of Appeal of Tasmania considered a sentencing appeal where the appellant was convicted and sentenced for three counts of attempting to import a marketable quantity of a border controlled drug.[167] The appeal was made on the basis that the sentencing judge had erred in not giving sufficient weight to the appellant's guilty plea and the imposed sentence was manifestly excessive.[168] The first ground is not relevant for the present discussion. As to the second ground, the Court noted that at first instance defence counsel attempted to characterise the offending as 'amateurish' as the drugs had been sent by post, and although there was a 'rudimentary attempt to disguise the contents of the package' there was 'no attempt to disguise [the appellant's] identity as the

156 Ibid [47].

157 [2016] NSWDC 94, [1] (Mahoney DCJ).

158 Ibid [15].

159 Ibid [27] (emphasis added).

160 [2013] VCC 70.

161 [2015] ACTSC 352.

162 *R v Baker* (n 70).

163 [2017] VCC 1529.

164 [2018] VCC 382.

165 [2019] NSWDC 572. See also *Tran v The Queen* [2020] NSWCCA 204.

166 [2019] VCC 1399.

167 [2018] TASCCA 21, [1]–[3] (Estcourt J) ('*Dunning v Tasmania*').

168 Ibid [5].

intended recipient of the package'.[169] This was not accepted by the sentencing judge who held that there were factors that pointed to sophistication, one of which being the use of Bitcoin:

> It is true that you made no real attempt to disguise your identity as the recipient of the package. On the other hand, there are aspects of your conduct which indicate a degree of sophistication. The purchase of the drugs through specialised and, probably, covert websites, your use of software intended to mask your computer transactions, and evidence which suggests that *you paid for the drugs by digital currency*, demonstrates that you had given some thought to protecting yourself from investigative scrutiny.[170]

In considering the sophistication of the offence, Porter AJ agreed with the sentencing judge's approach:

> For the appellant … [it was argued] that there was little evidence of sophistication in what the appellant did. The high point of this is undoubtedly the fact that the appellant had the drugs addressed to himself at his home. It was not challenged however, that the appellant had used his mobile phone to arrange payment with Bitcoin, and the sentencing judge was entitled to draw the inferences he did about the use of the 'masking' software found on the appellant's tablet, and the covert conduct engaged in.[171]

Second, in *Tran v Western Australia* ('*Tran*'),[172] the appellant sought leave from the Court of Appeal in Western Australia to appeal a sentence on the grounds that the sentencing judge 'made assumptions about the applicant's use of bitcoins, resulting in factual conclusions as to the connection between the use of bitcoin and other uncharged acts' and on the grounds of manifest excess.[173] Relevantly, in refusing leave on the first ground, the Court of Appeal held that:

> There is no merit in the submission that the learned sentencing judge erred in finding that the appellant's offending was sophisticated and brazen. The appellant attempted to conceal his activities by using the darknet and by making payments via Bitcoin, plainly with the intention of making his wrongdoing more difficult to detect. These measures may be properly characterised as sophisticated.[174]

In refusing leave on the second ground, the Court of Appeal, constituted by Buss P and Mazza JA, held that '[t]he sentence reflected a proper exercise of the sentencing discretion'[175] which included approving the sentencing judge's

169 Ibid [8], quoting *Tasmania v Dunning* (Supreme Court of Tasmania, Brett J, 11 April 2018) ('*Tasmania v Dunning*').

170 *Dunning v Tasmania* (n 167) [8] (Estcourt J), quoting *Tasmania v Dunning* (n 169) (emphasis added).

171 *Dunning v Tasmania* (n 167) [49].

172 *Tran* (n 115).

173 Ibid [38] (Buss P and Mazza JA).

174 Ibid [76].

175 Ibid [93].

characterisation of the use of cryptocurrency as one factor amongst others contributing to a 'sophisticated enterprise'.[176]

Third, the Court of Appeal in Western Australia had a further opportunity to consider the issue in *Day v The Queen* ('*Day*').[177] In this case, the self-represented appellant had pled guilty to offences including the importation of firearms purchased from the dark web marketplace 'AlphaBay'.[178] The appellant's submissions noted his cooperation in forfeiture of the Bitcoin.[179] At first instance the use of Bitcoin was said to be a relevant factor, among others, to the seriousness of offending because it indicated a 'considerable effort to disguise' the offending and a 'considerable degree of planning'.[180] The Court of Appeal, constituted by Buss P, Mazza JA and Allanson J, agreed that 'by withdrawing money for the purchase of Bitcoin which [the appellant] intended to use to illegally purchase guns … the appellant's conduct demonstrates a degree of planning' notwithstanding there were only three transactions over a short period of time.[181]

Fourth, in *Edmonds v The Queen* the appellant successfully sought leave in the Court of Criminal Appeal of the Northern Territory to appeal against their sentence on the grounds of manifest excess.[182] The appeal was allowed. At first instance, the applicant pled guilty to two drug offences.[183] In the course of a police interview, the accused admitted to the use of Bitcoin — purchased from a cryptocurrency exchange for the purpose of purchasing drugs though dark web markets — which formed part of the agreed facts for the purpose of the plea.[184] The Court of Criminal Appeal noted that 'the use of Bitcoin and the dark web in order to purchase the drugs elevated the gravity of the offending because it demonstrated a degree of sophistication (of a sort), and it gave rise to obvious and intended difficulties in detecting the activity'.[185]

However, these were matters that were 'not in dispute'.[186] Instead, the appeal turned on the characterisation of funds in the applicant's bank account as proceeds of drug supply and the 'scope and nature of the applicant's commercial operation'.[187] Although the characterisation of the use of cryptocurrency was not

176 Ibid [85].

177 [2019] WASCA 60 ('*Day*').

178 Ibid [1], [8] (Buss P, Mazza JA and Allanson J).

179 Ibid [30].

180 Ibid [14].

181 Ibid [51].

182 [2019] NTCCA 1, [3] (Grant CJ, Blokland and Barr JJ).

183 Ibid [1].

184 Ibid [5], [9].

185 Ibid [28].

186 Ibid.

187 Ibid [29].

contested — similar to the findings in *Dunning v Tasmania* discussed above — the reasoning nevertheless formed part of the first instance sentencing decision which was subsequently accepted by the parties and the appellate court.

One problem for doctrinal certainty is that it is difficult to separate the payment of Bitcoin and the use of dark web markets. This is particularly problematic as almost half of the criminal decisions in the dataset involve the use of the 'dark web' (however described).[188] Helpfully, there are two decisions in the study's dataset that explicitly isolate cryptocurrency.

First, in *Director of Public Prosecutions (Cth) v Nickless* ('*Nickless*'), the defendant pled guilty to seven drug-related offences, having imported drugs using the dark web.[189] Judge Mullaly held that the '*[u]se of cryptocurrency adds a level of sophistication and planning* that also increases problems of detection and thus suppression of harmful drug use in our community'.[190]

Second, in *R v Poulakis* ('*Poulakis*'),[191] there was a more detailed consideration of whether the use of cryptocurrency was a factor indicative of sophisticated offending. In this case, the defendant pled guilty to drug offences along with firearm and money laundering offences.[192] Relevantly, the defendant converted money provided by others into Bitcoin and ordered two separate consignments of drugs on the internet.[193] The Bitcoin was purchased through multiple cash deposits (a practice known as 'structuring') with the intention of avoiding thresholds for *AML CTF Act* reporting.[194] Competing submissions were made in relation to the use of cryptocurrency and the seriousness of offending. Counsel for the prosecution submitted that 'the purchase of the drugs using Bitcoin' and 'the acquisition of that Bitcoin using structured deposits' (along with the purchase of a mobile phone in another person's name) were 'significant matters' that showed that defendant went to 'great lengths to conceal the nature of his criminal activity'.[195] Counsel for the defendant advanced a different contention — conceding that there was a 'degree of planning' involved but arguing that 'the offending was not particularly sophisticated, given it was readily identified by recorded telephone calls … together with computer records capturing the offender's Bitcoin purchases'.[196] That is, 'these two aspects "increased the syndicate's ability to be detected by authorities" as the transactions were "recorded in detail both by

188 See above Part III.

189 [2020] VCC 1428, [2] (Judge Mullaly) ('*Nickless*').

190 Ibid [10] (emphasis added).

191 [2020] ACTSC 247 ('*Poulakis*').

192 Ibid [1]–[2] (Loukas-Karlsson J).

193 Ibid [3]–[4].

194 Ibid [18]–[19].

195 Ibid [49].

196 Ibid [37]

transaction records and telephone intercept"'.[197] On this basis, defence counsel submitted that the offending was 'amateurish' and 'actions that were always going to fail'.[198] The Court did not appear to have been persuaded by the defendant's submissions. Justice Loukas-Karlsson stated that it was open to the Court to find that '[t]hese purchases were done *in a manner that reflected additional criminality* and further demonstrated the offender's awareness of the criminal enterprise he was involved in'.[199]

There are five decisions in the dataset where the use of cryptocurrency appeared to be a neutral consideration in sentencing. In *R v Smith* ('*Smith*'), the defendant faced charges in the Supreme Court of the Australian Capital Territory relating to the importation and attempted possession of drugs and related offences.[200] The defendant ordered the drugs online through the dark web using Bitcoin as payment.[201] In sentencing, Mossop J described the offending as 'a relatively unsophisticated method of importing the drugs'.[202] In this case the parcels were addressed to the defendant[203] rather than to another name or to a post-office box, and the defendant was 'the only person involved at the Australian end'.[204] This demonstrated a decreased level of concealed criminal activity and was more easily detectible by law enforcement. It is notable that the facts here are broadly aligned with those in *Dunning v Tasmania*, discussed above, where a different conclusion was reached in relation to sophistication. In *R v Sagnelli*,[205] Mossop J expressed a consistent disposition. Notwithstanding that the defendant imported drugs using the dark web and Bitcoin, his Honour held that '[t]he importation was unsophisticated' because the defendant was a sole operator, used his own name and address, and 'took few protective measures to avoid the discovery of his activities'.[206] Courts reached similar conclusions in the Victorian cases of *Director of Public Prosecutions (Vic) v Gould*,[207] *Director of Public Prosecutions (Vic) v Ragauskas*[208] and *Director of Public Prosecutions (Cth) v Hogan-Keogh*.[209]

One decision in the dataset considered the implications of the use of the dark web and cryptocurrency for the sentencing purpose of facilitating an offender's

197 Ibid [40]

198 Ibid [37].

199 Ibid [44] (emphasis added).

200 [2019] ACTSC 196 ('*Smith*').

201 Ibid [7] (Mossop J).

202 Ibid [15].

203 Ibid [4]–[6].

204 Ibid [15].

205 [2020] ACTSC 348.

206 Ibid [11].

207 [2016] VCC 322, [26] (Judge Punshon).

208 [2016] VCC 1232, [64] (Judge Pilgrim).

209 [2020] VCC 261, [38] (Judge Cannon).

rehabilitation. In *R v Meginess* ('*Meginess*') the defendant was a relatively young offender who purchased a commercial quantity of various drugs from the dark web using Bitcoin for payment.[210] Amongst other sentencing considerations, the sentencing judge had regard to the implications of the defendant's technical skillset; holding that 'there was nothing to be gained by sending the [defendant] to prison'.[211] As the Court of Criminal Appeal of the Northern Territory summarised:

> [The sentencing judge] expressed concern that a term of actual imprisonment could adversely affect the [defendant's] prospects of rehabilitation, and risk his falling into the company of 'new friends' who could take advantage of the respondent's skill and experience in accessing the dark web and using bitcoin to purchase dangerous drugs. His Honour expressed the view that it was in the interests of the community primarily, that the [defendant] not be sent to prison.[212]

Obtaining and using cryptocurrency for payments does require a degree of technical skill compared to the general population which may be unfamiliar with these payments. Accordingly, the sentencing judge in *Meginess* found that the use of cryptocurrency was a *mitigating* factor in sentencing, contrary to the weight of authority discussed above, having regard to rehabilitation. This decision should be treated with caution. After the sentencing judge imposed a wholly suspended term of imprisonment, the Crown appealed the sentence on the grounds that it was manifestly inadequate. The appeal was allowed. The Court of Criminal Appeal did not appear to take issue with the sentencing judge's reasoning regarding rehabilitation.[213] However, the Court did find that there was an appellable error in overlooking 'the prime importance of general deterrence in sentencing for offences of this nature'[214] thereby placing 'undue emphasis on rehabilitation at the expense of punishment, denunciation and general deterrence'.[215] The Court of Criminal Appeal also found error in the sentencing judge's assessment of seriousness, that 'failed to reflect the true criminality of the offending'.[216] This decision was the only case example in the dataset where the use of cryptocurrency — specifically, having the technical skills to use cryptocurrency — has been held by a sentencing judge to be a mitigating factor in sentencing.

Finally, it is important to distinguish between the use of cryptocurrency as an aggravating factor and where the use of cryptocurrency forms part of the actus reus of the charged offence. For example, in *R v Mead* the defendant pled guilty to several charges that included laundering Bitcoin which was the proceeds of

210 [2019] NTCCA 5, [3]–[4] (Kelly, Blokland and Barr JJ) ('*Meginess*').

211 See ibid [12].

212 Ibid.

213 'His Honour was properly entitled to take into account the [defendant's] youth, lack of prior convictions and an informed assessment of the [defendant's] prospects of rehabilitation.': ibid [32].

214 Ibid.

215 Ibid [33].

216 Ibid [29], [33].

crime.[217] The laundering was carried out by the defendant making withdrawals from a cryptocurrency exchange and making payments to his personal credit card and another prepaid MasterCard account which he had obtained using false documents. Judge Haesler noted that these charges were part of the 'sophisticated measures [which the defendant had] taken to avoid scrutiny'.[218] However, in this case, the act of exchanging Bitcoin and then making a Bitcoin BPAY payment to a credit card account was part of the charged act (ie rather than using cryptocurrency for payment for illicit drugs, cryptocurrency was used for disguising illicit profits). As such, the use of cryptocurrency was not indicative of a relatively more serious commission of drug offences. Instead, in determining the seriousness of offending on the laundering charges the Court had regard to the 'number of transactions and the period over which the transactions occurred'.[219] The Court faced a similar sentencing issue in *Poulakis*, discussed above, where Loukas-Karlsson J was careful to note that 'double counting must be avoided'.[220] That is, there would be an element of double punishment if there was a penalty for the use of the cryptocurrency as part of a charged act (eg dealing with the proceeds of crime) and as an aggravating factor in another charged act (eg importing drugs). In these circumstances, the use of cryptocurrency will be most properly considered in the sentencing for the primary offence rather than as an aggravating factor. Another option to avoid the problem of double counting is for the sentencing judge to impose a wholly concurrent sentence.[221]

In summary, the review of sentencing decisions in Australia has shown that, on balance, the use of cryptocurrency as part of the commission of an offence will be treated as an aggravating factor in sentencing. The rationale is that the use of cryptocurrency is a factor — either in and of itself or alongside other factors — that is indicative of planning or obfuscation and therefore a greater degree of sophistication or seriousness of offending. A critique of this position will be offered in the discussion section.[222]

2 *General Deterrence*

The second, and related, doctrinal theme of the sentencing decisions in this study's dataset is that sentencing judges have considered the fact of cryptocurrency to be a factor relevant to the purpose of general deterrence in sentencing. That is, the court may impose a sentence of sufficient weight to not just deter the offender from re-offending ('specific deterrence') but also to deter the public at large from engaging in criminal conduct of the same or a similar nature ('general

217 [2017] NSWDC 1, [21]–[22], [65] (Judge Haesler).

218 Ibid [47].

219 Ibid [48].

220 *Poulakis* (n 191) [49].

221 See, eg, *Day* (n 177) [16] (Buss P, Mazza JA and Allanson J).

222 See below Part V.

deterrence').[223] Of the sentencing decisions reviewed in this study, in ten cases the sentencing judge specifically called out the need for general deterrence. Of those decisions, all involved the actual or attempted purchase of drugs (n=9) or weapons (n=1) from dark web marketplaces using cryptocurrency.

As a starting point, courts have noted the importance of general deterrence in sentencing tasks to discourage online drug dealing. For example, in *Matthews v The Queen* the Court of Appeal in Victoria issued the following warning:

> [A]ny sentence passed on [the appellant] was required to give full effect to the need to deter others and to denounce his conduct. *If there be a perception among some that the on-line trading in drugs, or their purchase or sale by post, is somehow less serious than more traditional forms of dealing, those perceptions need to be dispelled* by sentences which adequately reflect the need for general deterrence.[224]

Similarly, in *R v Collopy* before the South Australian Court of Criminal Appeal,[225] Peek J (with Blue J agreeing at [4]) agreed with Lovell J's decision that the sentence at first instance was manifestly excessive, but added that the resentencing on appeal must, and did in his Honour's view, adequately address the need for general deterrence:

> [I]n an era when many people spend a great deal of their time on the internet, persons who would otherwise not have become 'traditional' drug dealers might become fascinated by a *modus operandi* involving 'the darknet', 'bitcoins' and so forth and foolishly decide to try the same thing themselves.
>
> …
>
> [I]f this type of enterprise continues to be encountered in South Australia in the future, a heightened need for general deterrence may become apparent and lead to a significant increase in the length of prison sentences in cases of the present kind.[226]

Similar sentencing dispositions were expressed in the decisions of *Meginess*,[227] *Day*[228] and *Nickless*,[229] all discussed above, along with *R v Azabal*.[230]

One appellant in the dataset unsuccessfully attempted to challenge the general assumption that online drug dealing is as harmful as the more traditional forms of the trade. The appellant in *R v Morrison* ('*Morrison*') sought leave to appeal in the

223 See, eg, *Sentencing Act* (n 147) s 5(1)(b).

224 *Matthews v The Queen* (2014) 44 VR 280, 301 [75] (Warren CJ, Nettle and Redlich JJA) (emphasis added), cited in *DPP (Cth) v Vince* [2018] VCC 1808, [65] (Judge Cohen).

225 [2017] SASCFC 64.

226 Ibid [2]–[3].

227 *Meginess* (n 210) [33] (Kelly, Blokland and Barr JJ).

228 *Day* (n 177) [56] (Buss P, Mazza JA and Allanson J).

229 *Nickless* (n 189) [10] (Judge Mullaly).

230 [2019] NSWDC 523, [30] (Haesler DCJ).

Queensland Court of Appeal on the basis that the sentence was manifestly excessive.[231] Amongst other grounds, the appellant argued that 'his case [was] "unique as the public was never aware of [his] activities", because his customers ordered online.'[232] Without the benefit of the full written submissions, the problem with how the appellant's argument is framed is that what matters for general deterrence is not lower notoriety but lower social harm. The Court dismissed the contention as unpersuasive without any substantive discussion,[233] and ultimately refused leave.[234] It is also noted that in this case, the appellant challenged the characterisation of the offending as sophisticated because he used encrypted messages that were password protected — asserting, correctly in the authors' view, that 'this is considered best practice for anybody doing any type of business online with the risk of your personal information being stolen'.[235] Further, the appellant had received payments to two Bitcoin addresses — one of which was through a digital currency exchange,[236] which was not indicative of a serious attempt to hide the transactions.

Other decisions in the dataset were acutely focused on the need for general deterrence where a crime is difficult to detect. In this context, the use of the dark web and cryptocurrencies were specifically noted as factors. This finding is not surprising given the type of offences in the dataset. This is consistent with the High Court's observation in the 2001 decision of *Wong v The Queen* that 'deterrence is to be given chief weight in the sentencing task' in circumstances where the offending in question is difficult to detect.[237] For example, in *Dunning v Tasmania*, discussed above, the Tasmanian Court of Criminal Appeal restated the sentencing judge's comments recognising that 'general deterrence must be the predominate sentencing consideration':[238]

> Some factors which are relevant to the need for general deterrence in this case include the quantity of the drug involved, in particular the amphetamine, the grave social consequences which would flow from the dissemination of that drug in that quantity, the difficulty of detecting the crime, which depended upon effective and comprehensive surveillance of the enormous volume of postal articles coming into the country, *and your use of covert websites and digital currency to complete the transaction*.[239]

231 [2020] QCA 93, [6] (McMurdo JA, Sofronoff P agreeing at [1], Morrison JA agreeing at [2]) ('*Morrison*').

232 Ibid [34].

233 Ibid [38].

234 Ibid [48].

235 Ibid [35].

236 Ibid [18]–[19].

237 (2001) 207 CLR 584, 607–8 [64] (Gaudron, Gummow and Hayne JJ).

238 *Dunning v Tasmania* (n 167) [10] (Estcourt J, Marshall AJ agreeing at [29]), quoting *Tasmania v Dunning* (n 169).

239 *Dunning v Tasmania* (n 167) [10] (Estcourt J, Marshall AJ agreeing at [29]), quoting *Tasmania v Dunning* (n 169) (emphasis added).

Similarly, the Court in *Director of Public Prosecutions (Cth) v Allami* held that the factors relevant to specific and general deterrence included 'the serious social consequences which would flow from the dissemination of these drugs into the community, the difficulty in detecting the crime, the use of covert websites, *the use of digital currency to complete the transaction*, the use of a false name'.[240]

The next section of the article will consider the broader implications of the study's findings.

V DISCUSSION

The systematic review of the Australian case law has provided insight into the various contexts that blockchain and cryptocurrencies have been considered in reported matters before Australian courts. It has found that matters involving cryptocurrency have appeared in administrative tribunals, trial courts and appellate courts throughout all Australian jurisdictions. In the criminal jurisdiction, cryptocurrency has been considered in a range of contexts including pre-trial decisions (such as bail and restraining orders), trial (including physical and documentary evidence, witness testimony, and accused testimony), judge alone verdict, sentencing and appeals.

The quantum of sentencing decisions meant that doctrinal conclusions could be drawn. On balance it was found that the use of cryptocurrency by an offender will be treated as an aggravating factor in sentencing — the use of cryptocurrency being indicative of a higher degree of sophistication or a more serious example of the offending. However, this has not been applied consistently in all cases — where other facts show that the offending was of an unsophisticated nature or where the use of cryptocurrency forms part of a charged offence. Additionally, the use of cryptocurrency has been held to indicate efforts to conceal or disguise the transaction — prompting sentencing judges to consider the purpose of general deterrence in deciding an appropriate sentence. There is scope for critiquing the assumptions underlying these doctrinal findings which is the focus of this section.

As a starting point, there is a risk that sentencing courts may be too eager to adopt a relatively simplistic characterisation in relation to the use of cryptocurrency being a marker of obfuscation and, therefore, sophistication. In many of the sentencing decisions there is little if any consideration given to the type of cryptocurrency transactions being made. This information is important. Certainly, courts should make a distinction between those transactions using custodial wallets held in an account with a centralised digital currency exchange (ie KYC requirements means that identity can be readily obtained — not dissimilar from transacting using internet banking)[241] and those transactions that are made exclusively through non-custodial wallets, where it might be inferred that the offender intended to keep the transactions private. Similarly, the courts should

240 [2020] VCC 1114, [9] (Judge Gucciardo) (emphasis added).

241 See, eg, *Day* (n 177); *Smith* (n 200); *Morrison* (n 231).

make a distinction between those transactions that are made direct peer-to-peer and those transactions that involve strategies, such as using multiple or 'pass through' addresses or employing 'mixing' or 'tumbling' protocols, where it might be inferred that the offender intended to obscure the transaction. Additionally, the type of cryptocurrency being used matters in the assessment of obfuscation — a distinction should be made between using the open and transparent cryptocurrency payment networks such as Bitcoin, and so-called 'privacy coins' such as Monero which was designed to facilitate untraceable transactions.[242] Therefore, the reality is that sophistication exists along a spectrum, and it is not sufficient to identify that cryptocurrency has been used and simply infer sophistication compared to other types of financial payments.

Another assumption underpinning the reasoning that cryptocurrency contributes to the seriousness of the offending is that online drug dealing is at least as harmful as the more traditional forms of this offence. A body of work from the social sciences treats this assumption with greater nuance. For example, Australian criminologist James Martin has advanced the 'gentrification hypothesis' which asserts that dark web markets 'reduce systemic violence [commonly associated with traditional drug markets] by ensuring anonymity and physical separation between drug buyers, sellers, and other offenders'.[243] There is emerging empirical support for the gentrification hypothesis.[244] Transaction cost economics provides a similar explanation.[245] That is, there is a high degree of trust involved in committing criminal activity as criminals cannot enforce transactions through legitimate institutions such as courts or consumer protection agencies. In addition, every criminal exchange occurs with the risk that the counterparty might expose your activity to law enforcement (whether inadvertently or deliberately). As such, contractual enforcement therefore takes the form of other (often violent) methods.[246] Economists have shown that criminal enterprises exist in hierarchies.[247] Instead of every criminal exchange occurring on the black market, criminals form firms (ie cartels, gangs, or other descriptors) to govern their activities. Limiting membership to trusted individuals helps enforce deals and avoid detection. In this way, a trusted hierarchy may reduce violence compared to unorganised crime.[248] Criminal enterprises also require a payment network to store and manage ill-gotten gains. The invention of cryptocurrency provides a new way to govern the payments side of criminal transactions. This lowers the transaction

242 See Nicolas van Saberhagen, *CryptoNote v 2.0* (White Paper, 17 October 2013) <https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf>.

243 James Martin, 'Cryptomarkets, Systemic Violence and the "Gentrification Hypothesis"' (2018) 113(5) *Addiction* 797, 797.

244 See James Martin et al, 'Selling Drugs on Darkweb Cryptomarkets: Differentiated Pathways, Risks and Rewards' (2020) 60(3) *British Journal of Criminology* 559, 569.

245 See Richard A Posner, *Economic Analysis of Law* (Wolters Kluwer, 9th ed, 2014).

246 Ibid 284.

247 See, eg, Steven D Levitt and Sudhir Alladi Venkatesh, 'An Economic Analysis of a Drug-Selling Gang's Finances' (2000) 115(3) *Quarterly Journal of Economics* 755, 756.

248 Posner (n 245) 285.

costs of payment (direct payments, across international borders) and provides for reduced opportunism (immutable records, identity shielded by pseudonymity). As such, cryptocurrency provides a way of reducing the transaction costs — and therefore the violence associated with the drug trade — without necessarily forming criminal hierarchies.

On the other hand, as Martin acknowledges, dark web marketplaces also lead to new and increased opportunities for social harm beyond illicit drugs including 'stolen credit cards, child [abuse material] or contract killing'.[249] Additionally, the ability to earn indirect profits from cryptocurrency investment may increase the returns to, and therefore the attractiveness of, criminal activity.[250] As such, whether the use of dark web markets and cryptocurrency increases or decreases social harm overall is an empirical question that is far more complex than courts have currently considered and requires further research from social scientists.

An assumption underpinning the reasoning that the use of cryptocurrency in offending invokes the need for general deterrence is that offences which are harder to detect are more costly to enforce or come with an increased probability of social harm. There are, of course, costs of enforcing any laws. But the cost of undercover operations on the dark web are particularly costly as they require specialist intelligence and policing teams with additional costs in terms of training and expertise.[251] Arguably, therefore, a harsher sentence for offences involving cryptocurrency is a mechanism to reduce the propensity of potential offenders to commit those offences without necessarily increasing the enforcement budget[252] — predicated on the assumption that potential offenders rationally respond to incentives.[253] Nevertheless, this assumption overlooks the possibility that offenders may be using cryptocurrency for necessity or convenience rather than using it to conceal offending. Most of the sentencing decisions in the dataset involve dark web marketplaces. In these settings, cryptocurrency is necessary because it is the only accepted form of payment — and that decision has been made at the platform level rather than by the individual buyer or seller (albeit for reasons of decentralisation and privacy that cryptocurrency provides, dark web marketplaces may be preferred by parties on this basis over other alternatives). In other cases where there is an alternative payment method open to the offender, cryptocurrency may have been used out of convenience (eg cheaper, frictionless global payments; not having to use and transport cash). In Professor Petter Gottschalk's framing, '[c]onvenience comes at a potential cost to the offender in

249 Martin (n 6) 365.

250 See Posner (n 245) 285.

251 See, eg, Gemma Davies, 'Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers' (2020) 84(5) *Journal of Criminal Law* 407.

252 See, eg, George J Stigler, 'The Optimum Enforcement of Laws' (1970) 78(3) *Journal of Political Economy* 526.

253 Gary S Becker, 'Crime and Punishment: An Economic Approach' (1968) 76(2) *Journal of Political Economy* 169. For a more recent empirical study: see Menusch Khadjavi, 'Deterrence Works for Criminals' (2018) 46(1) *European Journal of Law and Economics* 165.

terms of the likelihood of detection and future punishment'.[254] Applied here, the use of cryptocurrency provides a relatively seamless global payment system but comes with increased costs in two respects. First, that there is a record of the transactions that will exist on exchanges, computers, or other personal devices. Second, most cryptocurrency transactions exist on open and traceable public networks — exposing the offender's identity if cryptocurrency proceeds can be traced to a known wallet or are cashed out through a cryptocurrency exchange. Again, the implication of both necessity and convenience is that courts (and counsel), if maintaining that the cryptocurrency is more than a neutral factor, will need to closely consider the reasons that cryptocurrency was used in a particular case.

Finally, there are practical implications flowing from this study. Most of the cases in the dataset show that the offenders were caught using traditional policing methods such as intercepting packages, telephone intercepts, physical surveillance, search warrants and obtaining admissions under questioning. This is perhaps a reflection of the relatively *unsophisticated* nature of the offending in many of the cases where offenders obtained physical goods online that were traced back to the offender's address, a post-office box under the offender's control, or that of an associate — offending that is vulnerable to being caught through traditional surveillance. It is also perhaps a reflection of the offenders' cooperation with law enforcement in many of the cases, meaning that more complex digital analytics were not required as the transactions were not disputed and charges were not contested. Two cases in the dataset, however, showed that Victorian and Western Australian police had caught offenders through undercover operations as sellers on dark web marketplaces.[255] At a minimum, this required those police agencies to be able to perform basic cryptocurrency transactions, including setting up cryptocurrency wallets to receive cryptocurrency payments. Cases also note forensic analysis of electronic devices which revealed cryptocurrency usage.[256] As such, this study has shown that law enforcement agencies have developed basic technological capacity around cryptocurrency. Two other cases noted that police had seized cryptocurrency, although neither case provides detail on how these seizures were carried out.[257] For instance, was there a cryptocurrency exchange involved? Was it a computer installed with a software wallet that had been seized? Or was a hardware wallet seized? Was cryptocurrency transferred into another wallet controlled by the police? Or were the private keys disclosed? This study's dataset does not reveal the answers to these questions.

254 Petter Gottschalk, 'Convenience in White-Collar Crime: Introducing a Core Concept' (2017) 38(5) *Deviant Behavior* 605, 605. This framework was applied in Braaten and Vaughn (n 23).

255 *R v Falconer* [2017] VCC 1596, [13] (Judge Murphy); *Day* (n 177) [10]–[11] (Buss P, Mazza JA and Allanson J).

256 See, eg, *Pollard v The Queen* [2015] VSCA 138, [7] (Ashley, Redlich and Weinberg JJA) ('*Pollard*'), quoting *DPP (Vic) v Pollard* [2014] VCC 1786, [21] (Judge Lacava) ('*DPP v Pollard*'); *R v Grey* [2020] QCA 77, [24] (Morrison JA).

257 *Pollard* (n 256) [7], quoting *DPP v Pollard* (n 256) [21]–[42] (Judge Lacava); *New South Wales Crime Commission v Ward* [2019] NSWSC 140, sch 3 (Davies J).

What is known is that capacity to perform seizures of cryptocurrency has existed for almost a decade, as media coverage of *Pollard v The Queen* ('*Pollard*') reported that Bitcoin was seized in 2013.[258] In *Pollard*, the seized Bitcoin was disposed of by way of a public auction. While not apparent in the dataset, the AFP is now publicly acknowledging that it has sophisticated '[c]ryptocurrency tracing' capabilities that it credits for shutting down 'one of the world's largest phishing services'.[259] There are many questions that remain here, too. What is the scale of these operations? How are policing methods keeping pace with changes in the use of the technology? How is knowledge being diffused throughout and amongst the various agencies? This study's data is insufficient to paint a complete picture of law enforcement and regulatory agency capabilities, but the questions raised here provide interesting avenues for future research utilising other complementary research methodologies.

A final practical implication is that criminal legal practitioners are likely to have to deal with the perception that cryptocurrency is associated with crime and must carefully craft submissions for the court based on the facts. All criminal legal practitioners will need to be blockchain and cryptocurrency literate so that they are able to seek appropriate court orders, obtain and review expert witness reports, and understand the commercial and legal significance of cryptocurrency transactions.

VI CONCLUSION

Cryptocurrencies have been used by offenders in the commission of criminal offences, notwithstanding that cryptocurrency and the underlying technology also has a range of legitimate uses as new infrastructure for the digital economy.[260] This article presented a systematic review of criminal cases in Australia up to December 2020 and demonstrated that cryptocurrency has been considered in the full spectrum of criminal proceedings from pre-trial applications (bail, restraining orders), trials by jury and judge alone (physical and documentary evidence, witness testimony, accused testimony), through to post-trial decisions (sentencing, appeals). This study found that the use of cryptocurrency is treated as an aggravating factor in sentencing due to the sophistication of offending of which it is indicative, calling for general deterrence. Although, we have argued that the rationale for this treatment has largely been unchallenged and deserves greater nuance. Finally, it was observed from the cases that law enforcement agencies have developed technological capabilities around cryptocurrency, but most investigations appear to have been reliant on traditional policing methods of documentary and human intelligence rather than more advanced blockchain analytics methods. While the Bitcoin network was first deployed in 2009, the first reported Australian decision specifically mentioning 'Bitcoin' did not appear until

258 *Pollard* (n 256). See, eg, Diana Ngo, 'Australian Authorities About to Sell at Auction 24,500 BTC Confiscated from Silk Road Drug Dealer', *Cointelegraph* (online, 31 October 2014) <https://cointelegraph.com/news/australian-authorities-about-to-sell-at-auction-24500-btc-confiscated-from-silk-road-drug-dealer>.

259 Australian Federal Police, *Annual Report 2020–21* (Report, 9 September 2021) 56.

260 Berg, Davidson and Potts (n 27) 153.

2014. Australia is therefore still living through the first decade of cryptocurrency cases and further developments are inevitable as its adoption continues to grow.

APPENDIX A: TABLE OF CASES (BY DATE)

Year	*Citation*
2013	*Director of Public Prosecutions (Cth) v Howard* [2013] VCC 70
2014	*Matthews v The Queen* [2014] VSCA 291
2015	*Australian Securities and Investments Commission v Ostrava Equities Pty Ltd* [2015] FCA 425
	Pollard v The Queen [2015] VSCA 138
	R v NE [2015] ACTSC 352
	Director of Public Prosecutions (Vic) v Millar [2015] VCC 1883
2016	*R v D, CM* [2016] SASC 38
	Director of Public Prosecutions (Vic) v Gould [2016] VCC 322
	Stebbins v Tasmania [2016] TASCCA 6
	R v Wallis [2016] NSWDC 94
	Nash v Chief Executive, Public Safety Business Agency [2016] QCAT 126
	Director of Public Prosecutions (Vic) v Ragauskas [2016] VCC 1232
	Australian Securities and Investments Commission v Ostrava Equities Pty Ltd [2016] FCA 1064
2017	*R v Mead* [2017] NSWDC 1
	Director of Public Prosecutions (Cth) v To [2017] VCC 475
	R v Collopy [2017] SASCFC 64
	Director of Public Prosecutions (Cth) v Petkovski [2017] VCC 1529
	R v Falconer [2017] VCC 1596
	Director of Public Prosecutions (NSW) v Hing [2017] NSWCCA 325
2018	*Director of Public Prosecutions (Vic) v Kerovec* [2018] VCC 382
	Burt v Merrill [2018] FamCA 162
	Re ICandy Interactive Ltd [2018] FCA 533
	Matter Technology Ltd v Mrakas [2018] NSWSC 507
	Director of Public Prosecutions (Cth) v Avignone-Green [2018] VCC 755
	Re Baker [2018] ACTMC 27
	Director of Public Prosecutions (Cth) v Vince [2018] VCC 1808
	Fowles v Fowles [No 5] [2018] FamCA 929
	Re Abaker [2018] VSC 714
	Director of Public Prosecutions (Vic) v Schembri [2018] VCC 2269
	Dunning v Tasmania [2018] TASCCA 21
2019	*Edmonds v The Queen* [2019] NTCCA 1
	R v Meginess [2019] NTCCA 5
	Rojas v United States of America [2019] FCA 22
	New South Wales Crime Commission v Ward [2019] NSWSC 140
	Merchant [2019] AATA 1080
	Tran v Western Australia [2019] WASCA 50

Keyes v Keyes [2019] FCCA 927
Day v The Queen [2019] WASCA 60
Australian Securities & Investments Commission v Vella-Arpaci [2019] FCA 644
ZLT v NSW Trustee & Guardian [2019] NSWCATAP 143
Harlow v Stansfield [2019] SADC 75
R v Azabal [2019] NSWDC 523
Kolaka v The Queen [2019] NTCCA 16
R v Smith [2019] ACTSC 196
R v Ha [2019] NSWDC 572
Griffiths v Power Ledger Pty Ltd [2019] FCCA 2224
Director of Public Prosecutions (Cth) v Lou [2019] VCC 1399
Director of Public Prosecutions (Vic) v Zarghami [2019] VCC 1520
Health Care Complaints Commission v Holbrook [2019] NSWCATOD 146
Vernon v Peter Saddler Transport Pty Ltd [2019] VCC 1779
Torok v Becker [2019] NSWSC 1662
Noicos v Dawson [2019] FCA 2197
Commissioner of the Australian Federal Police v Kogan [2019] NSWSC 1866
R v Dando [2019] NSWDC 833
R v Baker [No 3] [2019] ACTSC 365
Director of Public Prosecutions (Cth) v Singh [2019] VCC 2034
Chaves v Chaves [2019] FamCA 1022

2020 *North (A Pseudonym) v Director of Public Prosecutions (Cth)* [2020] VSCA 1
Director of Public Prosecutions (Cth) v Watkins (A Pseudonym) [2020] VCC 25
Hague v Cordiner [No 2] [2020] NSWDC 23
Australian Securities and Investments Commission v AGM Markets Pty Ltd (in liq) [No 3] [2020] FCA 208
Commissioner of the Australian Federal Police v Bigatton [2020] NSWSC 245
Director of Public Prosecutions (Cth) v Hogan-Keogh [2020] VCC 261
Director of Public Prosecutions (Vic) v Hughes [2020] VCC 296
Zarghami v The Queen [2020] VSCA 74
CRPS and Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs [2020] AATA 872
Wade v Alawi [2020] FCCA 832
R v Grey [2020] QCA 77
Isignthis Ltd v ASX Ltd [2020] FCA 567
R v Morrison [2020] QCA 93
Balsam v Lackner [2020] FCCA 1115
Seribu Pty Ltd and Commissioner of Taxation [2020] AATA 1840
Green v Fairfax Media Publications Ltd [2020] WASC 250
Banca Sella Holdings SpA v Dominet Digital Corporation Pty Ltd [2020] ATMO 124
Director of Public Prosecutions (Cth) v Allami [2020] VCC 1114

Lescosky v Durante [2020] FamCAFC 179
Australian Securities and Investments Commission v Dawson [2020] FCA 1144
Tran v The Queen [2020] NSWCCA 204
Vu and Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs [2020] AATA 2876
Le and Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs [2020] AATA 3130
NPP Australia Ltd v Ripple Labs, Inc [2020] FCA 1237
NPP Australia Ltd v Ripple Labs, Inc [No 2] [2020] FCA 1253
Director of Public Prosecutions (Cth) v Nickless [2020] VCC 1428
R v Conroy [2020] NSWDC 604
Tran and Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs [2020] AATA 3600
R v Poulakis [2020] ACTSC 247
R v Yavuz [No 2] [2020] ACTSC 248
Director of Public Prosecutions (Vic) v Hough [2020] VCC 1534
Mango Credit Pty Ltd v Saad [2020] NSWSC 1324
Director of Public Prosecutions (Vic) v Baker [2020] VCC 1618
Australian Securities and Investments Commission v AGM Markets Pty Ltd (in liq) [No 4] [2020] FCA 1499
Green v Fairfax Media Publications Ltd [2020] WASC 376
Green v Fairfax Media Publications Ltd [No 2] [2020] WASC 485
Gluszak v Yeap [2020] WASC 360
Griffiths v Power Ledger Pty Ltd [2020] FCCA 2846
Torok v Becker [2020] NSWSC 1570
Cooley and Minister for Immigration, Citizenship, Migrant Services and Multicultural Affairs [2020] AATA 4561
Powell v Christensen [2020] FamCA 944
Director of Public Prosecutions (Cth) v White [2020] VCC 1846
Vuong [2020] AATA 5388
Baker v The Queen [2020] ACTCA 55
R v Sagnelli [2020] ACTSC 348
Jia v Khajeh [2020] FamCA 1068