Chapter 3

Opportunities and risks

3.1 Advances in technology have produced rapid changes in the way Australians are managing their money. While the advent of digital currency has opened up a range of opportunities, it also presents risks. The Australian Payments Clearing Association (APCA), the self-regulatory body set up by the payments industry to improve the safety, reliability, equity, convenience and efficiency of the Australian payments system, recognised both the possible benefits and drawbacks of emerging digital currencies, observing:

> New technologies, particularly network and cloud-based technologies such as the block chain, offer the potential for valuable innovation and competition. However payments system regulation must balance competing policy objectives. It must maintain a balance between stability, efficiency and competition-driven innovation while ensuring confidence and integrity.[1]

3.2 In this chapter, the committee explores the potential opportunities and risks of digital currency.

Benefits of digital currencies

3.3 The European Securities and Markets Authority (ESMA) found that the main attraction of digital or virtual currencies (VC) appeared to be the speed and cost. It stated:

> The main benefits of VC [virtual currency] based financial assets and asset transfers seem to be speed and cost. From the perspective of the user/investor, the speed of VC based financial asset transactions is higher than traditional financial asset transfers and takes place within a couple of hours at most. The cost of transactions seems to be currently somewhere around a couple of Euro cents. Both speed and cost of transactions vary between different VCs.
>
> The benefit of cost and speed equally holds for issuers in terms of listing an asset on an asset exchange. In the case of the NXT asset exchange, a listing currently costs 1000 NXT (currently around 10 Euro) one-off plus transaction costs when sending rewards to investors. Especially for small and medium sized companies this could become an attractive source of funding.[2]

3.4 The European Banking Authority similarly referred to the lower transaction costs and the faster speeds associated with virtual currencies. It noted:

---

1 Australian Payments Clearing Association, *Submission 43*, p. 3.

2 The European Securities and Markets Authority, *Call for evidence, Investment using virtual currency or distributed ledger technology*, 22 April 2015, paragraphs 34 and 35, http://www.esma.europa.eu/system/files/2015-532_call_for_evidence_on_virtual_currency_investment.pdf (accessed 29 May 2015).

> Although reliable and independent data on the exact costs of VC transactions is difficult to ascertain, some anecdotal suggestions have been made that average transaction fees on the Bitcoin network tend to be less than 0.0005 BTC, or 1% of the transaction amount.
>
> This compares with 2%–4% for traditional online payment systems or an estimated 8%–9% for remittance without involving bank accounts via money transmitters. Transactions within or between VC schemes are also not subject to the exchange fees applied to conversions for transactions with third countries, therefore providing further potential for cost savings, (although conversion fees would typically apply as and when VC are exchanged against FC [fiat currency] or vice versa). The increase in competition for transaction services may also have a cost-reducing effect on the costs of conventional transactions in FC.[3]

3.5 In respect to the processing time for transactions, it found:

> Transactions using VCs can potentially be settled faster than those of FCs. For Bitcoins, the total process time is said to be between 10 and 60 minutes. It is claimed that, on average, a new block is added every 10 minutes to the blockchain transaction ledger. In this respect, VC payments appear to compare favourably with credit transfers or card payments, particularly for payments between different currency areas. Also, processing VC payments takes place on a 24/7 basis, unlike payments made through traditional payment systems.[4]

3.6 The European Banking Authority lists a number of other advantages attached to virtual currencies including:

- certainty of payments received—allowing merchants to avoid having to refund transactions, particularly those based on an alleged non-fulfilment of a contract;
- contributing to economic growth—spawning new types of businesses; and
- security of personal data.[5]

3.7 While digital currencies offer numerous advantages, their benefits are not as significant in the Australian context. APCA noted that, unlike some other countries, currently Australia 'enjoys a sophisticated, ubiquitous…globally competitive payment

---

3 European Banking Authority, *EBA Opinion on 'virtual currencies'*, EBA/Op/2014/08, paragraphs 46 and 47, July 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (accessed 29 May 2015).

4 European Banking Authority, *EBA Opinion on 'virtual currencies'*, EBA/Op/2014/08, paragraph 52, 4 July 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (accessed 29 May 2015).

5 European Banking Authority, , *EBA Opinion on 'virtual currencies'*, EBA/Op/2014/08, paragraphs 53–59, 4 July 2014, https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf (accessed 29 May 2015).

system with generally high quality regulatory structures and settings'.[6] Australia's payment system is already overwhelmingly digital in nature, with only about 18 per cent of Australian currency existing in physical form.[7]

3.8 For example, EFTPOS transactions in Australia cost 16 cents on average, so there is little room for digital currencies to improve on domestic point-of-sale purchases, which account for around 40 percent of all transactions by value.[8] Australians already have many different payment systems including EFTPOS, interbank transfers, PayPal and international transfer via SWIFT. In this context, digital currencies, such as Bitcoin, do not offer much more additional capability. But in developing countries, digital currencies may provide secure international facilities for the transfer of funds at a much lower transaction cost than available from institutional banking.[9]

Distributed ledger technology

3.9 A distributed public ledger is a major innovation and integral to the appeal Bitcoin. The Chamber of Digital Commerce, a US not-for-profit trade association, explained that the underlying source code or algorithm of the Bitcoin protocol, often referred to as the blockchain, is built for the transfer of information. While the distributed ledger currently stores, transfers and accounts for financial assets, there is potential for the distributed ledger technology to be used to store and transfer other types of digital assets.[10]

3.10 In APCA's view, the use of distributed ledger technology in digital currencies is unique and genuinely new, providing the opportunity to conduct both storage and transmission of value without the traditional financial intermediaries. APCA supported the potential for competition and innovation which could help improve Australia's payment system in the future, noting the potential for the distributed ledger technology to be used in the broader sphere—beyond payments and currencies.[11] Mr Christopher Hamilton, of the APCA, noted:

> As a concept, as a way of recording ownership of assets—it can in principle be any asset including existing currency—it [distributed ledger technology]

---

6 Mr Christopher Hamilton, Australian Payments Clearing Association, *Committee Hansard*, 7 April 2015, p. 1.

7 Mr Christopher Hamilton, Australian Payments Clearing Association, *Committee Hansard*, 7 April 2015, p. 1.

8 Mr Robert Vong, *Submission 4*, p. 1.

9 Mr Mark Pesce, 'Where the bank keeps your money safe', *The Drum* (Australian Broadcasting Corporation), 15 July 2014, http://www.abc.net.au/news/2014-07-15/pesce-where-the-bank-keeps-your-money/5595664 (accessed 29 May 2015).

10 Chamber of Digital Commerce, *Submission 37*, p. 2.

11 Mr Christopher Hamilton, Australian Payments Clearing Association, *Committee Hansard*, 7 April 2015, p. 1.

> is genuinely a new way of doing it. For that reason, it is worth exploring and understanding the implications of it.[12]

International remittance and financial inclusion

3.11 As Australia already has a well-established and efficient payments system, Mr Andreas Antonopoulos, an author and computer security expert, suggested that Bitcoin may represent a unique opportunity in two areas:

> Firstly, bitcoin can introduce much needed competition in the retail payments industry, undercutting the expensive systems offered by credit and debit cards, while significantly improving security and privacy for consumers. Secondly, the bitcoin industry can establish Australia at the forefront of the next wave of innovation in financial services, a wave that can extend financial services to more than two billion people throughout Southeast Asia who are currently underbanked.[13]

International remittance

3.12 Mr Jonathon Miller, co-founder of Bit Trade Australia, advised the committee that he considered the overseas remittance market would be a growth area in Australia for digital currency such as Bitcoin.[14] He also noted benefits for Australians using digital currency to purchase goods and services from overseas, as these types of transactions currently included a currency conversion fee.[15]

3.13 For example, the transaction fees for transferring money from Australia to Samoa are around 12 per cent of the transaction value.[16]

3.14 APCA agreed that there was potential for digital currencies to assist with offshore transmission of money.[17] mHITs Limited, an Australian-based mobile money service company, did not believe that it was likely that digital currencies alone would be used directly for cross-border remittances in the short term. While end-to-end digital currency remittances were unlikely, businesses such as BitPesa have used digital currencies to facilitate remittance services between Kenya and the UK.[18]

3.15 The RBA formed the view that international remittance may be an area where digital currencies might gain traction, noting currently they can be expensive and subject to delays in the receipt of funds.[19] Even so, the RBA considered that the

---

12 Mr Christopher Hamilton, Australian Payments Clearing Association, *Committee Hansard*, 7 April 2015, p. 3.

13 Mr Andreas Antonopoulos, *Committee Hansard*, 4 March 2015, p. 1.

14 Mr Jonathon Miller, Bit Trade Australia, *Committee Hansard*, 7 April 2015, p. 18.

15 Mr Jonathon Miller, Bit Trade Australia, *Committee Hansard*, 7 April 2015, p. 18.

16 Ms Rebecca Bryant, *Committee Hansard*, 7 April 2015, p. 30.

17 Mr Christopher Hamilton, Australian Payments Clearing Association, *Committee Hansard*, 7 April 2015, p. 3.

18 mHITs Limited, *Submission 48*, p. 12.

19 Dr Anthony Richards, Reserve Bank of Australia, *Committee Hansard*, 7 April 2015, p. 45.

potential offered by digital currency was not significant and referred to the work being done through the New Payments Platform, a major industry initiative intended to establish 'new payments infrastructure that will spur innovation in the Australian payments industry'.[20] The RBA explained:

> More broadly, however, many payment attributes of digital currencies are already available in the traditional payments system or will be available, in the case of the new services that may be facilitated by the New Payments Platform project. Accordingly, it remains to be seen what would drive their widespread use domestically, particularly in light of the price volatility of digital currencies observed to date.[21]

Financial inclusion

3.16 Ms Rebecca Bryant, Department of Foreign Affairs and Trade (DFAT), noted that while DFAT has not provided any funding to date for any initiatives involving digital currencies, some of its partners have. Ms Bryant noted that:

> …the Consultative Group for Assisting the Poor [CGAP], and the World Bank—are actively considering the applicability of digital currencies to financial-inclusion initiatives. CGAP has looked closely at the BitPesa start-up, which, in 2014, launched a service using bitcoin to provide cheap and fast remittance services. BitPesa is focused on providing remittance services for the UK-to-Kenya corridor. The UK senders buy bitcoin. These are transferred to Kenya and immediately transferred into Kenyan shillings, which are then deposited into mobile wallets or bank accounts. BitPesa charges a variable rate of three per cent on the transfer. This compares to an average cost of a remittance from the UK to Kenya of nine per cent. [22]

3.17 Ms Bryant advised the committee that DFAT was 'watching closely to see whether new business models, such as BitPesa, could have a wider application, thereby reducing the cost of simple transactions and increasing financial inclusion more broadly'.[23]

Transparency

3.18 Ripple Labs, the San Francisco based developer of the Ripple protocol, an open-source distributed protocol that facilitates payments and funds transfers, suggested that the distributed ledger technology could substantially improve transparency in cross-border funds transfers. It suggested that this is 'particularly true of the Ripple distributed ledger system, which permits visibility of all transactions

---

20 Tony Richards, Head of Payments Policy Department, 'The Way We Pay: Now and in the Future', Speech to the Australian Savings & Deposits Conference 2014, Sydney, 4 June 2014, http://www.rba.gov.au/speeches/2014/sp-so-040614.html (accessed 29 May 2015).

21 Dr Anthony Richards, Reserve Bank of Australia, *Committee Hansard,* 7 April 2015, p. 45.

22 Ms Rebecca Bryant, Department of Foreign Affairs and Trade, *Committee Hansard,* 7 April 2015, p. 28.

23 Ms Rebecca Bryant, Department of Foreign Affairs and Trade, *Committee Hansard,* 7 April 2015, p. 28.

taking place through the protocol, and in which transaction histories of all accounts are available'.[24]

3.19 The Australia Federal Police (AFP) noted that while distributed ledger or blockchain technology records all Bitcoin transactions, the identity of the persons involved in the transactions may not be easily traceable.[25] The identity of the individuals involved in transactions is discussed later in this chapter.

Risks

Taxation non-compliance risk

3.20 The ATO noted that digital currencies had similar compliance risks as those associated with the cash economy. In particular, the capacity for transactions to go unreported and be handled pseudo-anonymously. There was also the potential for digital currency to facilitate international profit shifting or to help hide transactions, as the nature of digital currencies means transactions can be highly mobile internationally.

3.21 Mr Michael Hardy, ATO, advised the committee that the ATO does 'not have a sense of an enhanced non-compliance risk with Bitcoin transactions.' He stated:

> Of course, people do not put on their tax returns, 'This was my money from bitcoin.' It is just part of their assessable income. But our own monitoring has not indicated that there is a particularly high non-compliance risk from bitcoin transactions.[26]

3.22 In addition to its assessment that the fiscal risk associated with Bitcoin was low, the ATO's submission noted that the total worldwide value of Bitcoin was relatively small at approximately AU $5.96 billion when compared to Australia's GDP in 2012–13 which was $1.5 trillion.[27]

Financial stability

3.23 Researchers from the Finance Discipline Group, University of Technology, Sydney, analysed the Bitcoin public ledger and found that Bitcoin is currently held primarily for investment, rather than used as a medium of exchange. The researchers noted that the size of Bitcoin investments and transactions was relatively small compared to other assets. As such, they did not consider that Bitcoin is an immediate risk to financial stability or the Australian economy as a whole. However, they emphasised the level of risk was based on size, and may be affected by a significant increase in the acceptance of Bitcoin or similar digital currencies in the future.[28]

---

24 Ripple Labs, *Submission 21*, p. 9.

25 Australian Federal Police, *Submission 34*, p. 3.

26 Mr Michael Hardy, Australian Taxation Office, *Committee Hansard*, 4 March 2015, p. 15.

27 Australian Taxation Office, *Submission 8*, p. 7.

28 Finance Discipline Group, University of Technology, Sydney, *Submission 7*, p. [12].

3.24 Ripple Labs did not consider digital currencies to be a threat to financial stability and encouraged the committee to look at digital currencies as 'complementary currencies' rather than currencies that compete with government-issued currencies, stating:

> While we believe that utilizing digital currencies could be particularly attractive for facilitating cross-border payments, Ripple Labs does not share the view that digital currencies should replace fiat currencies. For many reasons, including geo-political considerations, it is highly unlikely that any digital currency could pose a meaningful threat to monetary or fiscal stability for the foreseeable future.[29]

3.25 Mr Shapiro from Promontory Financial Group LLC, a regulatory risk management and compliance consultancy, told the committee he did not believe digital currencies would replace national currencies:

> It is simple. People understand their Australian dollars, their US dollars and their British pound, and I think a lot of the future of this is actually going to be allowing consumers to hold balances in the currencies they understand and use the back end of this for payments just as merchants today can use services.[30]

3.26 APCA maintained that private currencies were not a new phenomenon and unlikely to affect the payment system adversely, so long as the bulk of activity continued to occur in fiat currencies.[31] It also noted that while the distributed ledger technology has a lot of interesting potential, it did not necessarily follow that digital currencies would have a massive role in the Australian economy.[32]

Price volatility

3.27 A number of submitters referred to the price instability of Bitcoin. Ripple Labs noted that as digital currencies involve volatile assets with inherent price volatility and risks, they may not be suited for direct consumer interaction.[33]

3.28 Mr Christopher Guzowski, ABA Technology, observed, however, that there had been a downward trend in volatility of Bitcoin noting, the main reason for this development was that 'more exchanges are opening up around the world, there are more traders, there are more market makers, there is more market depth, more liquidity and therefore the spreads are being lowered and the volatility is reducing'.[34]

---

29 Ripple Labs, *Submission 21*, p. 9.

30 Mr Adam Shapiro, Promontory Financial Group LLC, *Committee Hansard*, 26 November 2014, pp. 45–46.

31 Mr Christopher Hamilton, Australian Payments Clearing Association, *Committee Hansard*, 7 April 2015, p. 1.

32 Mr Christopher Hamilton, Australian Payments Clearing Association, *Committee Hansard*, 7 April 2015, p. 10.

33 Ripple Labs, *Submission 21*, p. 3.

34 Mr Christopher Guzowski, ABA Technology, *Committee Hansard*, 26 November 2014, p. 24.

Pseudo-anonymity

3.29 Digital currencies such as Bitcoin do not provide complete anonymity for users. This type of digital currency is better described as offering pseudo-anonymity. The Attorney-General's Department explained:

> To use Bitcoin as an example, every Bitcoin transaction is linked to a corresponding public key, which is then stored and made publicly available to view in the block chain. If a person's identity were linked to a public key, then it would be possible to look through the recorded transactions in the block chain and easily see all transactions associated with that key. In other words, Bitcoin offers users the ability to transact under the concealed identity of their Bitcoin address/public key, but all of their transactions are available for full public viewing and therefore for law enforcement scrutiny. When these transactions were examined and used to construct a pattern of behaviour, analysts in a simulated experiment were able to reveal the identities of approximately forty percent of Bitcoin users.[35]

3.30 The AFP also noted that although the distributed ledger is public, the identity of persons involved in the transactions may not be readily traceable. The AFP was concerned that pseudo-anonymity and the ability to conduct digital currency transactions outside the regulated financial framework would make it difficult to determine the true owners of digital currencies.[36]

Criminal activities

3.31 The nature of digital currencies, which can be traded online without face-to-face customer relationships, provides a greater degree of anonymity compared to traditional non-cash payments methods. The Attorney-General's Department observed that digital currencies provide 'a powerful new tool for criminals, terrorist financiers and sanctions evaders to both move and store illicit funds out of the reach of law enforcement and other authorities and purchase illicit goods and services'.[37]

3.32 The Attorney-General's Department also noted that the risks associated with digital currencies were not hypothetical. In May 2013 the US Treasury and the Department of Justice undertook a coordinated enforcement action against Liberty Reserve, a centralised convertible digital currency system being used to facilitate US $6 billion worth of illicit online activity, including identity fraud, credit card fraud, computer hacking and online scams. Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny to assist criminals to distribute, store and launder the proceeds of illegal activities by enabling anonymous, untraceable financial transactions.[38]

---

35 Attorney-General's Department, *Submission 42*, p. 8.

36 Australian Federal Police, *Submission 34*, p. 3.

37 Attorney-General's Department, *Submission 42*, pp. 6–7.

38 Attorney-General's Department, *Submission 42*, pp. 6–7; see also FATF, *Virtual Currencies—Key Definitions and Potential AML/CTF Risks*, June 2014, pp. 10.

3.33 Further, decentralised digital currencies such as Bitcoin, which do not have a central server or service provider, are of greater concern for law enforcement authorities and regulators than centralised convertible currencies such as Liberty Reserve. The Attorney General's Department explained that the now-defunct Silk Road website demonstrated features that make decentralised digital currencies attractive to criminals seeking to launder money and either purchase or accept payment for illicit goods and services. The Silk Road website was a black market site on the Dark Net, the portion of internet content that is not indexed by standard search engines. Silk Road took advantage of the pseudo-anonymous nature of Bitcoin and anonymising 'Tor' software to create a marketplace where mail-order drugs and other licit and illicit goods and services could be traded. The FBI shut down the Silk Road website in October 2013 following a two-year investigation.[39]

3.34 The Attorney-General's Department advised that there appeared to be little evidence to date indicating the use of digital currencies as a means of financing terrorism. It noted that AUSTRAC concluded in its 2012 typologies and case studies report that while the 'anonymous nature of digital currencies may appeal to criminal groups and individuals, their overall utility for criminals at this point may currently be limited to niche crimes in the cyber environment and individual or smaller-scale illicit activity'.[40]

3.35 The AFP noted in its submission that its main experience with digital currencies to date had been with Bitcoin. It identified four main areas of crime involving digital currency that had been investigated:

- the alleged theft of Bitcoin via hacking;
- Bitcoin exchanged as payment for the importation of illicit narcotics into Australia from major online black marketplaces such as Silk Road;
- domestic supply and trafficking of narcotics for payment in Bitcoin; and
- money laundering and dealing with the proceeds of crime via Bitcoin.[41]

Hacking

3.36 A number of submitters noted that custodial accounts pose a significant risk to consumers and should be the focus of regulation.[42] Mr Antonopoulos stated:

> In fact, any accounts that take control of Bitcoin keys, and therefore remove them from the protection and security of the Bitcoin network, create areas of centralisation. And we have seen before, many times, that such environments are prone to hacking, theft and, in many cases, what we suspect to be embezzlement and insider action. Those types of

39 Attorney-General's Department, *Submission 42*, p. 7.

40 Attorney-General's Department, *Submission 42*, p. 10.

41 Australian Federal Police, *Submission 34*, pp. 2–3.

42 Mr Andreas Antonopoulos, *Committee Hansard*, 4 March 2015, pp. 2–3; Mr Chris Mountford, *Submission 40*, p. 4; Coinbase, *Submission 41*, p. 6.

> organisations that have custodial access have all of the problems of traditional centralised financial networks. In short, if you give someone your money they will run away with it. So the need for regulation is paramount, as is the need for oversight, audit and all of the traditional financial controls that are imposed in those situations.[43]

Organised crime, purchase of illicit drugs and avoiding detection

3.37 The committee reiterates ASIC's advice to consumers on the risks associated with digital currency, including the possibility of being hacked, fluctuations in value and money being stolen from a digital wallet.

3.38 Veda, a company best known for consumer credit reporting, is also a provider of online fraud, identity and credit risk services. It noted that 'wherever there is something of value, there will be fraud and money-laundering—regardless if it cash, property or a painting'.[44]

3.39 Dr John Moss, Australian Crime Commission (ACC), commented that with every emerging technology criminal elements would be among the early adopters. Organised crime groups such as outlaw motor cycle gangs have used Bitcoins to store and move value.[45] He reported that the ACC was not currently seeing digital currency being used for large scale money laundering; however it was being used by 'mums and dads' to purchase illicit commodities, such as narcotics, over the internet.[46] Dr Moss noted that we have a unique window which should be seized for the regulation of digital currency before use escalates from purchasing a coffee to moving millions of dollars.[47]

3.40 The Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church of Australia, was concerned that digital currencies, along with a range of other payments methods, are being used on commercial child abuse websites to help users avoid detection.[48]

Scams

3.41 The ACCC advised that over the last three years there had been only about 100 complaints through its information centres regarding digital currencies. Mr Marcus Bezzi, ACCC, reported that the vast proportion of the complaints received were related to alleged scams. He stated:

> What we have noticed in relation to those issues is that digital currencies have been alleged by the complainants to have been used in a way that

---

43 Mr Andreas Antonopoulos, *Committee Hansard*, 4 March 2015, pp. 2–3.

44 Veda, *Submission 20* , p. [1].

45 Dr John Moss, Australian Crime Commission, *Committee Hansard*, 4 March 2015, p. 13.

46 Dr John Moss, Australian Crime Commission, *Committee Hansard*, 4 March 2015, p. 13.

47 Dr John Moss, Australian Crime Commission, *Committee Hansard*, 4 March 2015, p. 13.

48 Justice and International Mission Unit, Synod of Victoria and Tasmania, Uniting Church of Australia, *Submission 30*, pp. 9–12.

> perhaps would have been able to be used by ordinary currencies. So it is just another tool used by a scammer to rip off—to use a colloquial expression—consumers.[49]

3.42 With regard to another aspect of potential criminal activity, the AFP noted that the nature of digital currencies created challenges for the ability of law enforcement agencies to recover proceeds of crime.[50] The Centre for Internet Safety recommended that law enforcement should be resourced so they are able to 'innovate their investigative tools and techniques alongside this new technology in order to ensure investigations are not impeded by any improvement in criminals' ability to move funds anonymously'.[51]

Current level of risk

3.43 Despite the potential for digital currencies to be used for criminal activity, Mr Jared Taggart, AFP, noted that digital currencies were not currently a significant operational issue. He warned, however, that if the predictions were correct and digital currencies become more widely used, it could become an issue in the future.[52]

3.44 Mr Antonopoulos argued that Bitcoin was a rather benign form of digital currency, noting:

> There are other [digital currencies] that are much stealthier, much more anonymous, and may be encouraged to grow if onerous legislation is passed. Now, certainly bitcoin has been used for criminal purposes. That is a fact. To use a slightly humorous analogy, it has come to my attention that the vast majority of criminals also use shoes. That does not mean that shoes are the problem.[53]

3.45 Mr Hamish Hansford, ACC, explained that from a law enforcement perspective, digital currency was just another type of encryption:

> Encryption is used in a whole range of different areas, from communications, where we are seeing encrypted communications…right through to the use of darknets, or hidden parts of the internet, and payment through virtual currencies.[54]

Conclusion

3.46 The committee acknowledges that digital currency presents opportunities, including the broader application of the distributed ledger technology, increased competition in the payments system, and especially in transactions involving international remittances and providing services in developing countries. There are,

---

49 Mr Marcus Bezzi, ACCC, *Committee Hansard*, 7 April 2015, p. 35.

50 Mr Tony Alderman, Australian Federal Police, *Committee Hansard*, 4 March 2015, p. 9.

51 Centre for Internet Safety, *Submission 29*, p. 2.

52 Mr Jared Taggart, Australian Federal Police, *Committee Hansard*, 4 March 2015, p. 9.

53 Mr Andreas Antonopoulos, *Committee Hansard*, 4 March 2015, p. 4.

54 Mr Hamish Hansford, Australian Crime Commission, *Committee Hansard*, 4 March 2015, p. 9.

however, risks associated with the use of this new technology requiring careful and constant monitoring.