Seribu Pty Ltd v Commissioner of Taxation 2019/4118

Applicant's submissions

Introduction

1. This application came about from the Applicant using the digital currency bitcoin as part of its ordinary business operations.

2. Essentially, the Applicant sought a ruling from the Respondent that bitcoin is a currency other than Australian currency for the purposes of the Income Tax Assessment Act 1997. This would make it a "foreign currency" for the purposes of that Act.

3. The Respondent responded in the negative both to ruling application and on objection.

4. The Applicant seeks a review of this decision.

Outline

5. The question before the Tribunal is whether bitcoin is a currency other than Australian currency. If so, it would be a "foreign currency" for the purposes of the *Income Tax Assessment Act 1997*.

6. The Applicant's submissions are divided into 4 parts:

   - The meaning of the word "currency" and therefore the meaning of the defined term "foreign currency" as used in the *Income Tax Assessment Act 1997*
   - The nature of bitcoin
   - Application and other observations
   - Observations on the views of the Respondent

The meaning of "foreign currency"

(a) The statute

7. Section 995-1 of the *Income Tax Assessment Act 1997* provides that:

   > Foreign currency means a currency other than Australian currency.

8. To determine whether something is a foreign currency, it is first necessary to define the word “currency”.

9. In *Watson v. Lee* [1979] HCA 53 (1979) 144 CLR 374, the High Court needed to consider the meaning of the word “currency” in the context of its usage in the Australian constitution.

10. Section 51(xii) of the Constitution confers power upon the Parliament to make laws with respect to “[currency], coinage, and legal tender”. It was the extent of this power that was being challenged before the High Court at the time. It therefore defines the boundaries of the term.

11. Stephen J stated that:

> 39. When bank notes were still convertible into gold and before sophisticated concepts of central banking and exchange controls became the commonplace of economists it would, I think, have been appropriate enough to speak of laws concerning the import and export of currency generally as laws concerning the subject matter of "currency"; the word, without more, is not necessarily to be confined in its meaning to the money of a particular nation nor to that which is one nation's legal tender; indeed it has sometimes been used in a quite opposite and special sense to distinguish sterling from the irregular local coins formerly circulating and competing with sterling in some British colonies, particularly in Australia, from which was derived the old description "Currency lads and lasses". In 1900, there was, in Australia, no currency particularly identified with particular colonies, other than Queensland's Treasury notes: there were three Imperial mints, in Sydney, Melbourne and Perth which variously minted Imperial bronze, silver and gold coins and these, together with coins imported from the United Kingdom, circulated in Australia, as did the note issues of local banks: see generally Quick and Garren, Annotated Constitution of the Commonwealth of Australia, pp. 572-576, and Chalmers, A History of Currency in the British Colonies (1893). This situation persisted long after Federation. In such circumstances to confine the legislative head of power conferred by s. 51 (xii.) to Australian currency would have been to exclude the Commonwealth from whole areas concerned with the regulation and control of the everyday currency of the country, and this despite the apparently unrestricted nature of the grant of power in s. 51 (xii.). (at p400)
>
> [emphasis added]

12. The Applicant makes three observations here:

    - Currency does not need to be confined in its meaning to the money of a particular nation.

    - At the time numerous currencies (irregular local coins, or note issues of local banks) were used, not all of which were legal tender. Rum was used as a currency in New South Wales[1]. These were still considered currencies and within the regulating powers of the Commonwealth.

- There can be concurrent currencies circulating and competing with other currency.

13. All of the examples provided of currency share the following characteristics: they are fungible, measurable and used as a medium of exchange for goods and services. This makes sense because if a narrower interpretation of "currency" were to be taken, it would potentially restrict the powers of Parliament to make powers with respect to currency.

14. The same view was expressed again in another matter brought before the High Court. In *Goldsbrough Mort & Co. Ltd v Hall* (1949) 78 CLR 1. Here, Rich J stated:

> 16. Before these Acts were passed the currency in Australia consisted of gold, silver and bronze coins minted in England at the Royal Mint or by branches of that Mint established in Sydney, Melbourne and Perth and of paper money issued by the trading banks. The Treasury Notes Acts, 30 Vict. No. 11 and 56 Vict. No. 37, of Queensland are here irrelevant. (at p22)
>
> …
>
> 21. The metallic currency of England and Australia was, therefore, the same. Substantially the denominations of the coins were the same and their standards of weight and fineness were regulated by the Imperial law which was in force in Victoria or which was introduced into Victoria by force of the provisions already noticed. The paper money issued by the trading banks was payable in gold coin but it was not legal tender.
>
> [emphasis added]

15. In other words, currency can be issued by non-government entities, noting that this may not be legal tender but nonetheless constitutes currency.

(b) History of the statute

16. At this juncture it would be helpful to briefly consider the Act which inserted the term "foreign currency", and its definition as "a currency other than Australian currency", into the *Income Tax Assessment Act 1997*.

[1] See item 17 in Applicant's materials.

17. The Explanatory Memorandum to the Bill[2] introducing the term "foreign currency" provided the following context for the introduction of the provisions[3]:

> 2.3 As explained in Chapter 3, the economic consequences of a foreign currency denominated transaction must be translated into an equivalent amount of A$ (or another appropriate functional currency) for the purposes of determining an entity's Australian income tax liability.
>
> 2.4 This would be a straightforward matter if the tax system only recognised receipts and payments of foreign currency. However, rights to receive and obligations to pay foreign currency are often just as important as the currency itself in determining the tax consequences of a transaction. As rights and obligations denominated in a foreign currency subsist over a period of time, their A$ value may fluctuate.
>
> 2.5 Where this occurs, disparities may arise between the amount of A$ value recognised at a particular point in time, for example when an amount of assessable income is derived, and the A$ value of the consideration ultimately provided in settlement of the transaction. These disparities represent a gain or loss, in terms of A$, that occurs as a result of currency exchange rate movements or fluctuations.
>
> 2.6 The forex provisions provide a statutory framework under which the gain or loss arising from these disparities is brought to account when it has been 'realised'. This is the case even if the monetary elements of the transaction are not converted to A$.
>
> 2.7 Without such a framework, foreign currency gains and losses arising out of 'business' transactions may fall outside the income tax net. This possibility is illustrated by FC of T v Energy Resources of Australia Ltd (1996) 185 CLR 66 ('the ERA case'). In that case, the High Court held that a taxpayer makes no foreign currency gain or loss where a foreign currency denominated obligation is satisfied on capital account without converting any of the proceeds of the transaction into A$ or any amounts of A$ to foreign currency.
>
> [emphasis added]

18. The reference to the ERA case gives some indication as to the type of behaviour the rules were intended to address. The mischief rule, as a guide to statutory interpretation, would require some consideration as to the circumstances of the ERA case and how that would affect the intent and interpretation of the statute.

19. The ERA case concerned the issue of promissory notes (Euronotes) denominated in US dollars at a discount. The notes were paid back in US dollars. The exchange rate between the Australian dollar and the US dollar had changed between the date of issue and the date the notes were paid back.

[2] New Business Tax System (Taxation of Financial Arrangements) Bill (No. 1) 2003

[3] On the question of whether the explanatory memorandum can be considered, we refer to section 15AB(2)(e) of the Acts Interpretation Act 1901, noting that the High Court decisions would take precedent

20. The Respondent took issue with the fact that the entire transaction occurred in US dollars and said there should be tax on the movement in currency between the issue date and the repayment (maturity) date. The High Court disagreed, stating:

> 10. Upon the foregoing analysis, questions concerning the conversion of the proceeds and payments in discharge of the Euronotes from US dollars to Australian dollars are irrelevant. This case has nothing to do with currency gains and losses, for the simple reason that the taxpayer dealt only in US dollars. The taxpayer made no currency gains or losses because it never converted any of the proceeds of the notes into Australian dollars. For Australian tax purposes, the only relevant conversion was the cost in Australian dollars of the loss made in US dollars when the taxpayer incurred its liability to pay the face value of the notes.
>
> …
>
> 12. Fundamental to the case for the Commissioner was the assumption that a notional conversion of the proceeds of each issue and a notional conversion of the payments in discharge of each issue had to be made on the day that each of those events took place and that the difference between the respective sums was the taxpayer's gain or loss. The Commissioner treated the lack of any actual conversion of the proceeds or payments as irrelevant. But there is nothing in the Act that requires the making of notional conversions of the taxpayer's transactions. Nor is there anything in the Act that precludes the application of the principles in Coles Myer to the contractual arrangements of the taxpayer in the United States.
>
> [emphasis added]

21. The conclusion was that the gain from the exchange rate effect described above was not brought to tax. In 2003 (before bitcoin was invented), this was rectified by the insertion of Division 775 which also inserted the term “foreign currency”.

22. At para 2.9, 2.21 and 2.22, the explanatory memorandum compares the previous rules (upon which the ERA case was decided) with the new rules and discusses the legislative intent:

> 2.9 The realisation rules, in conjunction with the core translation rule discussed in Chapter 3, confirm the policy intent behind the tax treatment of foreign currency denominated transactions. These rules ensure that foreign currency gains and losses, whether on revenue or capital account, are brought to account, regardless of whether there is an actual conversion to A$. This will generally occur when the gains and losses are realised…
>
> …
>
> New law: Subject to specified exceptions, all foreign currency gains and losses, whether on income or capital account, are brought to account for tax purposes when realised. It does not matter that the amounts have not been converted into an equivalent amount of A$.

> Current law: There is a potential for foreign currency gains or losses arising on capital account to escape tax recognition. This may occur where there is no conversion of foreign currency denominated amounts into A$.
>
> 2.22 The core realisation framework for forex realisation gains and losses is contained in Subdivision 775-B. The purpose of this framework is to ensure that economic gains and losses arising from currency exchange rate effects are brought to account for income tax purposes when realised, regardless of whether there is an actual conversion of amounts into A$.

23. There is a clear intent that transactions denominated wholly in any currency other than Australian currency are brought to taxation. If bitcoin were not included in this, then the intent of the rules could be circumvented simply by denominating the entire transaction in bitcoin (which is possible, there are sophisticated instruments denominated in bitcoin – some of which have led to disputes brought before Courts, as we will note later in this submission). This would be contrary to the statutory intent. It was in this context that foreign currency was defined as a currency other than Australian currency[4].

(c) Conclusion

24. The case law and the guidance around the introduction of the definition of foreign currency into the *Income Tax Assessment Act 1997* supports the following conclusions:

    - The term currency is very widely defined at law and essentially includes anything that is used as a medium of exchange. The examples provided in *Watson* all have the features of fungibility, measurability and acceptance as a medium of exchange. The backing of a foreign government (or even the domestic government) is not required. Nor is it required that it be legal tender.

    - The term foreign currency is intended to be of wide import, particularly covering transactions that might take place (or are capable of taking place) entirely in another currency.

25. It is now necessary to consider the nature of Bitcoin to determine whether it meets this description.

[4] At the time the Respondent was also slightly behind the times with respect to globalization and uses of different currencies in international business as the Respondent argued that US dollars were not cash. Paragraph 16 of the judgement states: "16. The Commissioner contended that US dollars are not cash and that s 21(1) required any reference to US dollars in the course of executing the Euronote agreement to be converted to Australian dollars. In the Full Court of the Federal Court, Hill J expressly rejected this argument."

Bitcoin

26. It is necessary to identify and determine both the purpose of bitcoin and all the salient features of bitcoin if we are to form the correct conclusion as to whether it is capable of meeting the definition of "currency".

27. In order to do this, the Applicant submits that reliance be placed on:

    - The original blueprint set out by the founder and inventor of Bitcoin, Satoshi Nakamoto (the name is most likely an alias)

    - The programming developer guide (the bitcoin developer guide).

28. The advantage of relying on the source material which shows how the bitcoin program is to be designed is that the evidence is in the mathematics. It allows a programmer to create the program so goes to the heart of its functionality. It also makes the purpose of bitcoin clear. Other summaries and extrinsic material can be of some help but may not necessarily address all the key issues as pertain to the matter at hand.

(a) The original blueprint

29. Bitcoin was invented by a person or persons under alias "Satoshi Nakamoto" in 2008. He set out its purpose and how it was all to work in a paper titled "Bitcoin: A Peer-to-Peer Electronic Cash System" (the ***Satoshi paper***). The Satoshi paper is the blueprint used to code and develop Bitcoin.

30. Insofar as the purpose of bitcoin is concerned, the first line of the paper describes the intention behind the creation and use of bitcoin as follows:

    > A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.

31. The paper then goes on to explain the core features which are elaborated in more detail in the developer guide. These core features support the above intention, as will be shown when we describe how bitcoin functions based on the developer guide.

32. The features described below indicate that bitcoin, mathematically, is essentially a payment waiting to happen. It has no other feature or use. This is further made clear when the process and underlying code is explored.

(b) Developer guide

Denominations

33. Bitcoin is divided into denominations[5]. The denominations as follows:

Bitcoins	**Unit (Abbreviation)**
1.0	bitcoin (BTC)
0.01	bitcent (cBTC)
0.000001	microbitcoin (uBTC, “bits”)
0.0000001	Finney
0.00000001	satoshi

Payments

34. The bitcoin developer guide is quite technical so it would be helpful to provide some background first.

35. Cryptography is essentially a method of communication where messages can be sent in a scrambled form and only someone with a key can unscramble them. This is explained in the article by C.E. Shannon included as item 3 in the materials. An example of this would be a coded message sent in wartime where someone has a key (for example, A = F, B = G, C = H and so on) to translate that message. This concept is important because it forms the foundation of the public/private key pair in bitcoin. Where references are made to a public and private key, essentially the public key would be akin to a coded message and the private key would be the key that is capable of translating that message.

36. The mechanisms to code messages have become quite sophisticated over time. The process of coding messages is referred to as “hashing”. The requirement of a good code is that it is difficult to decipher, so small changes will change the message completely.

37. Bitcoin uses SHA-256. The effect of a small change can be seen in item 5 of the materials. The difference between the coded message for “Bitcoin is a foreign currency under the Income Tax Assessment Act 1997” and “bitcoin is a foreign currency under the Income Tax Assessment Act 1997” is just that one has a capital B and the other does not. However, the SHA-256 code is:

0caae19d54348d514a48a78726c2cbf86d22de5f65250717dd74e45e58ddde64

Vs

03a5745e8ff89d3c08d324584f23fc336d35e9dc6e0f810195ed268148688be4

[5] Bitcoin developer guide – payment processing guide – page 6

38. These are quite different. They are not even the same length. The key to the conversion is to create the same number of bits. Bits is not the number of units, but a unit of information which is essentially measured in the number of instructions provided. The mathematics of computing require this to be a number that has its square root equal to the original number, which means that essentially only 0 or 1 can be used – i.e. binary. However, it can be a little more sophisticated that this, so it could be yes or no, or on or off, etc.

39. Bitcoin is constructed around this messaging system, and transactions are conducted accordingly. The messages and instructions are contained in scripts, which is essentially a program that tells the computer what to do. For example, when one opens an internet browser, one is essentially running a script telling the computer to open the internet browser.

40. Before going into a quote from the technical manual, the arrangement is best understood with a chain involving three people – assume: A sends to B and B sends to C.

41. The transaction from B to C would work as follows:
    - B spends to C
    - C verifies that B is capable of spending to C by verifying that the conditions imposed by A on the spend have been met.
    - The conditions imposed by A are that only someone with B's private/public key pair can spend

42. This chain continues.

43. This is where the public key and private key pair becomes important. Verification is possible because only someone with the private key is able to decode the message (and meet the conditions). The fact that B is able to do so allows C to be confident that B is able to spend.

44. There are a number of other similar verifications that take place to ensure security.

45. The developer guide explains this as follows[6]:

> Each transaction has at least one input and one output. Each input spends the satoshis paid to a previous output. Each output then waits as an Unspent Transaction Output (UXTO) until a later input spends it
>
> The output has an amount in satoshis which it pays to a conditional pubkey script. Anyone who can satisfy the conditions of that pubkey script can spend up to the amount of satoshis paid to it.

[6] Bitcoin developer guide – transactions – page 2

> An input uses a transaction identifier (txid) and an output index number to identify a particular output to be spent. It also has a signature script which allows it to provide data parameters that satisfy the conditions in the pubkey script.
>
> A payment from one person to another is referred to as an output for the payer and would be an input into the transaction for the receiver.

46. Therefore, outputs of all transactions included in the block chain can be categorised as either Unspent Transaction Outputs (***UTXOs***) or Spent Transaction Outputs. For a payment to be valid, it must use only UTXOs as inputs into the next transaction.

47. In other words, either someone has made a payment, or is about to make a payment. Hence, the name "unspent transaction" – it remains unspent until it is spent.

48. The entire system is designed around these two categories. Bitcoin is essentially a payment waiting to happen.

49. Hence[7]:

> When your Bitcoin wallet tells you that you have a 10,000 satoshi balance, it really means that you have 10,000 satoshis waiting in one or more UTXOs.

How a transaction takes place

50. To start a transaction, the two parties each need their own public key and private key. The public key and private of any one individual are paired.

51. A public key is a key that has been derived from a private key with sufficient cryptography to make it difficult to determine the private key, but at the same time to have confidence that the public key was derived from the private key. The public key can (and it is recommended that it should) change after each transaction for security reasons.

52. To spend an output, one simply enters the public key of the recipient and runs the program (whichever program they are using for transacting, or if they develop their own).

53. The program will compare the public key of the sender with the public key that it is supposed to be (which is set out in the script which contains the conditions for the spender to spend the transaction output – the relevance of this is explained below). There are also some other verifications. If the verifications are successful, then the transaction is broadcast and added to the block.

[7] Bitcoin developer guide – transactions – page 2

54. The bitcoin developer guide provides the example of a transaction between Alice and Bob. Alice is sending bitcoin to Bob using Bob's public key:

> "To test whether the transaction is valid, signature script and pubkey script operations are executed one item at a time [to compare the Bob's public key with the public key provided to Alice], starting with Bob's signature script and continuing to the end of Alice's pubkey script." (pages 7 to 9)

55. It also explains how the script is written so that Bob can then spend the unspent transaction as an input into another transaction with someone else[8]:

> "Once Alice [the sender] has the [Bob's public key] address and decodes it back into a standard hash, she can create the first transaction. She creates a standard P2PHK transaction output containing instructions which allow anyone to spend that output if they can prove they control the private key corresponding to Bob's [the receiver's] hashed public key. These instructions are called the pubkey script or scriptPubKey."
>
> …
>
> When, sometime later, Bob decides to spend the UTXO, he must create an input which references the transaction Alice created by its hash, called a Transaction Identified (txid), and the specific output she used by its index number (output index). He must then create a signature script – a collection of data parameters which satisfy the conditions Alice placed in the previous output's pubkey script."
>
> [emphasis added]

56. The record of these transactions creates a chain of transactions, starting from Person A to Person B and then to Person C or whoever else it is that Person B wishes to transact with. Note that the chain results in the transaction between Person B and Person C still referring to the script written by Person A which imposes the conditions on the spend[9]:

> "the data Bob signs includes the txid and output index of the previous transaction, the previous output's pubkey script, the pubkey script Bob creates which will let the next recipient spend this transaction's output, and the amount of satoshis to spend to the next recipient."

57. This creates a chain effect. It is essentially this chain which is referred to as the blockchain. An example of this is in file 7, "bitcoin transaction and blocks" which was submitted with the Applicant's materials. There the style of the hash will be recognisable with the SHA-256 hash examples provided above.

58. Please refer to Annexure A for additional technical details on this process.

[8] Bitcoin Developer Guide – Transactions – page 4

[9] see Bitcoin Developer Guide – Transactions – page 6

Recording of transactions

59. All transactions are reported to other nodes, which is essentially everyone else on the network. All participants combined effectively form the network at any given time. Subsequent transactions are also added to the network and continue to be added as different people continue to make payment transactions. Each node simply looks to the most recently updated block to continue reporting and adding transactions to the network. When a new node joins (or has been disconnected from the network for a while), it just downloads the latest information from the existing nodes that are currently connected. As long as there are nodes on the network, there will always be a number of nodes which have the latest information.

60. The only way a person could create a fraudulent transaction would be to start off with the transaction and then catch up and overtake where the network is up to so that the network starts adding to the fraudulent chain. To do this would require one person to have processing power equal to or greater than the entire network, which is unlikely.

61. Once broadcast, the transaction over time acquires a number of confirmations. 0 confirmations means it has not been included in any block. 1 confirmation means it has been included in 1 block. 2 confirmations means that a new block has been added on top of the block that contains the transaction, 6 confirmations means that the transaction is buried under 6 blocks. As the number of confirmations increases, so too does the difficulty of reversing the transaction which is essentially how double spending of the same bitcoin is prevented[10].

(c) Conclusions

62. The source material makes the following apparent.

    - The objective is to create an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party (see Satoshi paper).
    - Bitcoin represents a payment that is waiting to happen (an unspent transaction).
    - The only function of the entire bitcoin infrastructure is the making and receiving of payments. Payments received remain as unspent transactions until they are spent by making a payment to someone else.

[10] see Bitcoin developer guide – payment processing guide - pages 15 and 16

63. It is well accepted that bitcoin can be and is used for payments. This fact is acknowledged by Parliament, the Courts and even by the ATO on its website (see below), although the ATO takes the reverse position in its submissions.

Application

64. It is submitted that the legal definition of currency, the intention of Parliament in enacting the definition of foreign currency and the facts surrounding the nature of bitcoin make it clear that it is a currency.

65. The Applicant makes the following additional observations:

(a) Leask case

66. The Respondent quotes a passage from *Leask v Commonwealth* (1996) 187 CLR 579.

67. For context, this case relates to the Financial Transactions Reports Act 1988 which has its own statutory definition of currency. This definition is different to the definition in the *Income Tax Assessment Act 1997*.

68. The relevant definitions in that Act are as follows:

> ***currency*** means the coin and paper money of Australia or of a foreign country that:
> (a) is designated as legal tender; and
> (b) circulates as, and is customarily used and accepted as, a medium of exchange in the country of issue.
>
> It also has a definition of foreign currency, which is as follows:
>
> ***foreign currency*** means the currency of a foreign country.

69. Notably, the definition of foreign currency here is the currency of a foreign country, whereas in the *Income Tax Assessment Act 1997* it is a currency other than Australian currency.

70. The other observation that the Applicant makes in relation to the quote is that the full quote provides a slightly different context to the abridged quote provided by the Respondent:

> That effect cannot be determined with the same clarity as the issues that arise in determining the validity of the Act by reference to the power to make laws with respect to currency. The power extends to the making of laws with respect to foreign currency as well as to Australian currency, as this Court held in *Watson v Lee*. Currency consists of notes or coins of denominations expressed as units of account of a country and is issued under the laws of that country for use as a medium of exchange of wealth. It is characteristic of

> currency that effect is given to an intention of the transferor and transferee to transfer property in the notes or coins by physical delivery of the notes or coins. The transfer leaves no record.
>
> [emphasis added]

71. First, the quote refers to "foreign currency" which is already defined in the Act being considered as the currency of a foreign country. It then goes on to make a comment about being issued under the laws of that country. It makes sense that there would be a reference to "the laws of that country", given the case is about foreign currency which is defined as a currency of a foreign country in the statute being considered.

72. Clearly this is not meant to be an exhaustive definition. This is supported by the reference to *Watson*. It is therefore not possible to draw an inference that there should be any restriction based on the laws of another nation.

73. Further, in *M Collins & Son Pty Ltd v Bankstown Municipal Council* (1958) 3 LGRA 216, Sugerman J cast doubts on the use that could be made of the definition of a word or phrase in a statute in the interpretation of that word or phrase in a similar statute in which it was not defined. He considered that the attachment of a meaning to a word in the interpretation clause of a statute very commonly involved some artificial extension or limitation of the natural meaning of the word for the purposes of that statute. Accordingly, statutory definitions depended so much upon context that little, if any, benefit was to be derived in the consideration of the meaning of the defined word for the purposes of another statute[11].

74. Second, the latter commentary about the characteristic of currency being transferred from one person to another is also a characteristic of bitcoin.

75. In any event, it is submitted that the Leask case is not really illustrative, because the term currency there is discussed by reference to the legislative definition in the legislation being considered, which is quite restricted and also different to the tax law and therefore not comparable.

76. The Applicant submits therefore that the more apt case is *Watson*, which considers the term currency by reference to its legal meaning, as derived from its reference in the Constitution. In *Watson*, the term currency is considered in isolation. It is also considered by reference to the legal definition of the word "currency" as the Court in

[11] Para 3.38 of Statutory Interpretation in Australia, seventh edition, DC Pearce and RS Geddes

Watson is considering whether there is a limit on the power of Parliament's powers to make laws with respect to currency.

(b) Travelex

77. This is a case about Fijian currency whether the supply of Fijian currency is a supply in relation to rights so the discussion needs to be viewed in that context. It is not a case about defining what a currency is. It is also talking about the currency of a country already, so whether it is necessary to be connected to a nation is not a question that arises or considered by the Court.

78. This is highlighted in these paragraphs:

> 28. At first instance, Emmett J distinguished between rights that are "the essential character or substance of the supply, or of a separately identifiable part of the supply" and those that are "merely integral, ancillary or incidental to another dominant part of the supply". The key to the distinction was identified by Emmett J as being whether the supply "binds" the parties in some way. A supply that does not bind the parties in some way was said to be "not a supply that is made in relation to rights".
>
> 29. Two preliminary points may be made about this distinction. First, if the distinction is to be drawn, it is one which must be applied to the particular supply in question: the identified "financial supply" of disposing of an interest <u>in the currency of a foreign country</u>. Secondly, if the distinction is to be drawn, it is not one whose application would be confined to financial supplies.
>
> [emphasis added]

79. Following from that, this is the comment made:

> 26. By the supply which is constituted by the sale and delivery of the foreign currency, the supplier supplies to the acquirer the rights that attach to the tokens (be they notes or coins) that are the foreign currency. The supply (by sale) is not sufficiently described as a sale of the particular tokens. Those tokens are valuable because they are currency in at least the country or area of issue. Because the tokens are currency, the holder of the tokens can use them as a medium of exchange and as a store of economic value. Currency has value only because of the rights that attach to
> it.

80. In this case the Court notes that currencies can be used as a medium of exchange and a store of economic value. It is not a definition, but it is noted that bitcoin has both of these characteristics.

81. In this context, this is interesting:

> 32. Observing that rights attach to currency, and pass upon negotiation of the currency by delivery, does not constitute any "juristic disaggregation and classification of rights" that fails to reflect "the practical reality of what is in fact supplied". On the contrary, recognising that a sale of foreign currency transfers to the purchaser the rights that attach to the notes does no more than recognise the evident purpose of the transaction. Further classification or identification of the rights that pass, whether as rights against an issuing central bank, or as rights akin to those of the holder of a promissory note, is not necessary. What the Act requires is that there be a supply "in relation to" rights; the operation of the Act does not call for attention to be given to the particular content of the rights.

82. It suggests that a currency does not need to involve a central bank, although the language does not exhaustively define currency.

83. Another feature is described by Heydon J:

> 47. … Apart from those rights, the pieces of paper had little value. They might have been used to stop an uneven table wobbling, or to jam shut a loose door, or to amuse small children, or to light a cigar. If the currency included coins, the coins might have been used to turn stiff screws or to lay on railway lines for the purpose of being flattened. But uses of that kind, which are very remote from their real purpose, would not prevent both the pieces of paper and the coins from being almost worthless. The supply of the currency was a supply in relation to the rights it gave because these rights constituted the pith and substance of the transaction.

84. Essentially the feature described here is of something that has no inherent value outside its real purpose – being a medium of exchange. The same is true for bitcoin.

(c) The ambulatory approach

85. In *Lake Macquarie Shire Council v Aberdare County Council* (1970) 123 CLR 327 the question arose whether a reference to the powers of a council to supply ‘gas’ included the supply of liquefied petroleum gas. It was clear from an examination of the relevant Act that the legislature had in contemplation only coal gas when the Act was passed – simply because it was the only type of gas then available. Barwick CJ and Menzies J considered that the word ‘gas’ was used in its generic sense and was thus not limited to coal gas. Barwick CJ said (at 331):

> I can see no reason why, whilst the connotation of the word ‘gas’ will be fixed, its denotation cannot change with changing technologies. Indeed, in my opinion, it would be odd that in granting trading powers, including the power to supply gas for heating and lighting, the Act should intentionally close the door on access by the local government bodies to developing methods of trading gas for heating and lighting

86. The term "currency" as referred to in the definition of "foreign currency" was introduced in the *Income Tax Assessment Act 1997* in 2003, before Bitcoin was invented. Given the context in which the term was introduced into the legislation (as discussed above), it certainly should be the case that bitcoin would be included in the definition of currency and be considered a foreign currency.

87. There are number of examples of bitcoin being used in financial transactions similar to those engaged in and referred to in the ERA case both locally and internationally:

- *SEC v Shavers* in the United States concerned a scheme where essentially loans or similar securities were issued in exchange for bitcoin. The Court considered whether the loans or similar securities that were issued were in compliance with the Securities Act.
- *Commissioner of Federal Police v Bigatton* [2020] NSWSC 245 related to the use of bitcoin in connection with a managed investment scheme.

88. The general usage of bitcoin in normal business transactions and also in more complex financial transactions has led to its judicial consideration in a number of jurisdictions.

(i) US v Faiella

89. In this case, the Court observed as follows:

> Following indictment, Faiella moved to dismiss Count One of the Indictment on three grounds: first, that Bitcoin does not qualify as "money" under Section 1960; second, that operating a Bitcoin exchange does not constitute "transmitting" money under Section 1960; and third that Faiella is not a "money transmitter" under Section 1960. Following full briefing, the Court heard oral argument on August 7, 2014.
>
> Upon consideration, the Court now denies defendant Faiella's motion, for the following reasons:
>
> *First,* "money" in ordinary parlance means "something generally accepted as a medium of exchange, a measure of value, or a means of payment." Merriam–Webster Online,,, http:// www. merriam- webster. com/ dictionary/money (last visited Aug. 18, 2014). As examples of this, Merriam–Webster Online includes "officially coined or stamped metal currency," "paper money," and "money of account"—the latter defined as "a denominator of value or basis of exchange which is used in keeping accounts and for which there may or may not be an equivalent coin or denomination of paper money" *Id.* Further, the text of Section 1960 refers not simply to "money," but to "funds." In particular, Section 1960 defines "money transmitting" as "transferring *funds* on behalf of the public by any and all means." 18 U.S.C. § 1960(b)(2) (emphasis added).

> Merriam Webster Online defines "funds" as "available money" or "an amount of something that is available for use: a supply of something." Merriam–Webster Online, http:// www. merriam- webster. com/ dictionary/ fund (last visited Aug. 18, 2014).
>
> 2 Both "money" and "funds" are ordinary English words and should be given their ordinary meanings. The parties make reference, instead, to Black's Law Dictionary, which would only be relevant if Congress intended that these terms be given special meanings as legal "terms of art"—something not remotely suggested in Section 1960. In any case, several of the definitions in Black's Law Dictionary support the rulings here.
>
> Bitcoin clearly qualifies as "money" or "funds" under these plain meaning definitions. Bitcoin can be easily purchased in exchange for ordinary currency, acts as a denominator of value, and is used to conduct financial transactions. *See, e.g., SEC v. Shavers,* 2013 WL 4028182, at *2 (E.D.Tex. Aug. 6, 2013) ("It is clear that Bitcoin can be used as money. It can be used to purchase goods or services.... [I]t can also be exchanged for conventional currencies....").

(ii) Skatteverket

90. In this case the Court observed as follows:

> 11 According to the order for reference the 'bitcoin' virtual currency is used, principally, for payments made between private individuals via the internet and in certain online shops that accept the currency.
>
> The virtual currency does not have a single issuer and instead is created directly in a network by a special algorithm. The system for the 'bitcoin' virtual currency allows anonymous ownership and the transfer of 'bitcoin' amounts within the network by users who have 'bitcoin' addresses. A 'bitcoin' address may be compared to a bank account number.
>
> 17 According to the Revenue Law Commission, the 'bitcoin' virtual currency is a means of payment used in a similar way to legal means of payment. Furthermore, the term 'legal tender' referred to in Article 135(1)(e) of the VAT Directive is used in order to restrict the scope of the exemption as regards bank notes and coins. It follows, according to the Revenue Law Commission, that that term must be taken to mean that it relates only to bank notes and coins and not to currencies. That interpretation is also consistent with the objective of the exemptions laid down in Article 135(1)(b) to (g) of the VAT Directive, namely to avoid the difficulties involved in making financial services subject to VAT.
>
> 24 It must be held, first, that the 'bitcoin' virtual currency with bidirectional flow, which will be
> exchanged for traditional currencies in the context of exchange transactions, cannot be characterised as 'tangible property' within the meaning of Article 14 of the VAT Directive,

> given that, as the Advocate General has observed in point 17 of her Opinion, that virtual currency has no purpose other than to be a means of payment.
>
> 25 The same is true for traditional currencies, since it involves money which is legal tender (see, to that effect, judgment in *First National Bank of Chicago*, C-172/96, EU:C:1998:354, paragraph 25).
>
> 42 The 'bitcoin' virtual currency, being a contractual means of payment, cannot be regarded as a current account or a deposit account, a payment or a transfer. Moreover, unlike a debt, cheques and other negotiable instruments referred to in Article 135(1)(d) of the VAT Directive, the 'bitcoin' virtual currency is a direct means of payment between the operators that accept it.
>
> 49 Transactions involving non-traditional currencies, that is to say, currencies other than those that are legal tender in one or more countries, in so far as those currencies have been accepted by the parties to a transaction as an alternative to legal tender and have no purpose other than to be a means of payment, are financial transactions.
>
> 51 It therefore follows from the context and the aims of Article 135(1)(e) that to interpret that provision as including only transactions involving traditional currencies would deprive it of part of its effect.
>
> 52 In the case in the main proceedings, it is common ground that the 'bitcoin' virtual currency has no other purpose than to be a means of payment and that it is accepted for that purpose by certain operators.
>
> 53 Consequently, it must be held that Article 135(1)(e) of the VAT Directive also covers the supply of services such as those at issue in the main proceedings, which consist of the exchange of traditional currencies for units of the 'bitcoin' virtual currency and vice versa, performed in return for payment of a sum equal to the difference between, on the one hand, the price paid by the operator to purchase the currency and, on the other hand, the price at which he sells that currency to his clients.

(iii) Bigatton

91. The Respondent also refers to Bigatton in its submissions. Again, it is helpful to provide the full context.

92. The Court noted the use of bitcoin and described it as a virtual currency that may be considered a form of electronic money. There is also a reference to a law firms that accept cryptocurrencies for some of their transactions:

> 24 I should say something about the nature of cryptocurrency. Cryptocurrencies are known as virtual currencies and may be considered a form of electronic money, although I understand

> that Mr Bigatton would dispute that. A unit of a cryptocurrency, such as a bitcoin, is created from code using an encrypted string of data blocks in the form of numbers known as blockchain. Cryptocurrencies can be bought and sold on exchange platforms and can be used to pay for goods and services from a person or entity that is willing to accept the particular cryptocurrency as payment. Mr Bigatton used as an example law firms apparently starting to use cryptocurrencies in some of their transactions.

93. Notably, the Supreme Court of NSW is using the word "currency" to describe bitcoin. There was no imperative for it to do so, other than its desire to briefly describe what bitcoin was. "Currency" was the word used which indicates its use to describe bitcoin in general and judicial parlance.

(iv) GST vs income tax

94. The GST law was recently amended to ensure that bitcoin and other digital currencies would be treated in the same way as state fiat currencies.

95. The GST legislation is not directly relevant to the income tax legislation, but the change does bring out a number of notable observations that could be relevant to the question before the Tribunal.

(a) The term "digital currency" is inserted into the legislation. This term defines a digital currency as digital units of value that:

- Are designed to be fungible; and
- Can be provided as consideration for a supply; and
- Are generally available to members of the public without any substantial restrictions on their use as consideration; and
- Are not denominated in any country's currency; and
- Do not have a value that depends on, or is derived from, the value of anything else; and
- Do not give an entitlement to receive, or to direct the supply of, a particular thing or things, unless the entitlement is incidental to:
    - Holding the digital units of value; or
    - Using the digital units of value as consideration

In creating this definition, Parliament broadly considered what features a currency has. Paragraph 1.21 of the relevant Explanatory Memorandum[12] states:

> The amendments define digital currency as needing to broadly have the same features as state fiat currencies. In particular, in the same way as state fiat currencies, the value of digital currency must derive from the market's assessment of the value of the currency for the purposes of exchange, despite it having no intrinsic value.

The Respondent considers that bitcoin meets all of the above requirements, according to its website[13].

(b) Contrary to the Respondent's submissions at paragraph 31(c), bitcoin is not comparable to frequent flyer points or ride tokens in amusement parks. The same explanatory memorandum addresses this issue as follows:

> 1.27 This requires that <u>digital currencies must be suitable for use as a medium of exchange</u>. Digital assets that are not suitable for use as consideration, or which are only available to the public subject to substantial restrictions on their use are not digital currency. Such assets cannot be used in the same way as money. Examples of such digital assets include:
>
> - Loyalty points provided by retailers that may only be redeemed for products; and
> - 'currencies' used in many online multiplayer games, that cannot be used outside of the context of the game under the terms under which the 'currency' is made available.
>
> [Emphasis added]

Given the Respondent has formed the view that bitcoin is a digital currency within the definition, and the definition expressly requires that bitcoin be more than simply the equivalent of loyalty points or used in games, it is assumed the inclusion of this point in its submissions was merely another typographical error on the part of the Respondent.

(c) The choice of the word "currency" in "digital currency" is notable. Whilst this is a defined term, it was open to parliament to choose any word or set of words as a descriptor, yet the word "currency" was chosen.

(v) <u>The usage of bitcoin</u>

[12] Treasury Laws Amendment (2017 Measures No. 6) Bill 2017

[13] https://www.ato.gov.au/Business/GST/In-detail/Your-industry/Financial-services-and-insurance/GST-and-digital-currency/

96. The Applicant has submitted evidence showing the usage of bitcoin. The entire application to the Tribunal was made possible due to the Applicant's use of bitcoin. There are also cases described above which indicate usage – not just in general transactions but also in more complex arrangements. It is possible to lend bitcoin and earn interest on bitcoin. It is possible to invest in derivates and securities using bitcoin. It is possible to pay for goods and services using bitcoin.

97. The Respondent provided some international examples relating to bitcoin. These are not strictly relevant, as they relate to the laws of different countries that are not necessarily comparable. What can be of use, however, are references in other jurisdictions relating to the use of bitcoin which indicate its prevalence. In this regard the comments made by the Respondent are of assistance – they show that bitcoin is prevalent enough in nature for it to attract the attention of the relevant regulatory bodies in those jurisdictions. It is unlikely that this would have occurred if their use was "limited" as the Respondent suggests in its submissions.

(a) Switzerland

The Swiss Federal Tax Administration has confirmed that Bitcoin should be treated in the same way as the Swiss franc or other fiat currency – that is, trading Bitcoins is neither a delivery nor a service for the purpose of Swiss value added tax (VAT). As a result, a Bitcoin transaction is VAT-free[14].

If Bitcoins are used to pay for the supply of goods or services subject to Swiss VAT, the usage of Bitcoins is considered a mode of payment. Consequently, the seller must not charge any additional VAT on a taxable transaction due to the use of Bitcoins as means of payment. This is also the case for other forms of native transaction tokens.

In 2016, Zug, a municipality in Central Switzerland (near the Swiss Alps) added bitcoin as a means of paying city fees, in a test and an attempt to advance Zug as a region that is advancing future technologies.[15] Swiss Federal Railways, government-owned railway company of Switzerland, sells bitcoins at its ticket machines.[16]

(b) Sweden

Sweden considers Bitcoin as currency for taxation purposes. The Swedish Tax Agency has given a preliminary ruling on Value Added Tax (VAT) on bitcoins, stating that trade in bitcoins is not subject to Swedish VAT, but is instead subject to the

[14] Article 21(2) of the Swiss VAT Act

[15] https://www.dw.com/en/alpine-crypto-valley-pays-with-bitcoins/a-19371082

[16] https://www.sbs.com.au/news/swiss-rail-to-sell-bitcoins

Finansinspektionen (Financial Supervisory Authority) regulations and treated as a currency. The decision has been appealed by the Swedish Tax Authority and was upheld by the Swedish Supreme Administrative Court.[17]

The governmental regulatory and supervisory body Swedish Financial Supervisory Authority (Finansinspektionen) has legitimized the fast growing industry by publicly proclaiming bitcoin and other digital currencies as a means of payment. For certain businesses interacting with fiat (mainly exchanges) the current regulation dictates that an application for approval/license must be filed and all the AML/CTF and KYC regulations applicable to more traditional financial service providers must be followed.

On October 6, 2014 representatives of the Swedish Enforcement Authority announced that that it will start to investigate and seize Bitcoin holdings when collecting funds from indebted individuals. The Swedish Enforcement Authority is a government agency that enforces judgments for both private and public claims.[18]

(c) Other

Additional materials and examples of the use of bitcoin have been provided in the Applicant's materials.

Other views expressed by the Respondent

98. The Respondent refers to the introduction of new facts by the Applicant – for example, paragraph 13 and 14 of the submissions.

99. Although this charge was levied at the Applicant before the Applicant had made any submissions or indicated the use of its material, the Applicant wishes to address this point by simply saying that no new facts have been introduced.

100. The matter before the Tribunal concerns the nature of bitcoin and whether it is a foreign currency. The Applicant is obliged to assist the Tribunal by providing adequate information. It does not assist in coming to the correct conclusion if material that is relevant is withheld. However, the Applicant is ultimately in the Tribunal's hands as to whether this material has been of assistance. The Applicant certainly hopes that it has been.

101. In any event, the Applicant addresses the point made by the Respondent that the material provided by the Applicant, which includes material by some commentators, foreign authorities on legal issues surrounding Bitcoin and evidence that Bitcoin can be

[17] https://www.skatterattsnamnden.se/publiceradeforhandsbesked/2013/handelmedbitcoins.5.14dfc9b0163796ee3e777b4c.html

[18] www.loc.gov/law/foreign-news/article/sweden-enforcement-authority-to-collect-bitcoins/

used to purchase specific goods or services should not be considered by the Tribunal based on *Commissioner of Taxation v McMahon* (1997) 79 FCR 127; *Rosgoe Pty Ltd v Commissioner of Taxation* [2015] FCA 1231; *Commissioner of Taxation v Eichmann* [2019] FCA 2155.

102. These cases create limitations only where new facts are introduced into the factual matrix concerning the private ruling. There ruling was simply on the question of whether bitcoin is a currency other than Australian currency (i.e. a foreign currency). Therefore, material assisting in the accurate description of bitcoin is relevant.

103. If the objective is to reach the correct conclusion, then this material needs to be included.

Conclusion

104. The Applicant submits that the bitcoin is a currency other than Australian currency, and therefore is a foreign currency for the purposes of section 995-1 of the *Income Tax Assessment Act 1997* for the following reasons:

- The legal definition of currency covers fungible and measurable mediums of exchange.
- The legal definition is intended to be broad, both historically (in a constitutional context) and under the *Income Tax Assessment Act 1997*.
- Bitcoin is essentially a payment that is waiting to happen. It has no other purpose. This was described as its purpose by its founder. This is also verified by the mathematical design of bitcoin.
- The term “currency” is used by Parliament, the Courts and in general parlance to refer to bitcoin.
- An unwarranted narrowing of the definition of currency would be both incorrect and essentially limit the Parliament’s power with respect to currency (such as bitcoin) under the Constitution which relies on the same definition.
- An unwarranted narrowing of the definition of currency would also result in the intention of the provisions introducing the term in the Income Tax Assessment Act 1997 inoperable in circumstances where they were intended to operate, thereby creating a loophole for the mischief which was closed by the laws to be re-opened.

105. It is respectfully submitted that the objection decision be set aside and that the question asked in the private ruling be answered in the affirmative.

Annexure A: additional technical detail:

Payer/spender 1 → receiver 1 → receiver 2

The validation process is as follows (for going from receiver 1 to receiver 2) – see my notebook:

- The signature from the receiver is compared against the pubkey script of payer/spender 1. This is done as follows:

    - Take the signature from the receiver 1 and the pubkey script from payer/spender 1 (which contains the conditions for receiver 1 to spend the output).
    - The signature from receiver 1 has the public key.
    - The payer/spender 1's pubkey script is run and it creates a copy of the public key of receiver 1.
    - These two need to be the same (return ''true''), otherwise the transaction will not validate.
    - The pubkey script from payer/spender 1 then executes and checks the signature provided by receiver 1 against the now authenticated public key. If the signature matches the public key (return ''true'') and was generated using all of the data required to be signed, then the transaction is valid.
    - The full redeem script needs to hash to the same value as the script has that payer/spender 1 put in their output. It then processes the redeem script exactly as it would if it were the primary pubkey script, letting receiver 1 spend the output if the redeem script does not return false.
    - There is also a standard transactions test, which tests the pubkey scripts and signature scripts against a small set of believed-to-be-safe templates. These are:

        - Pay to Public Key Hash (P2PKH) – the most common form of pubkey script used to send a transaction to one or multiple bitcoin addresses.
        - Pay To Script Hash (P2SH) – the transaction gets sent to a script hash. This has the advantage of being able to store text (so you can write messages/comments). To redeem a P2SH transaction, the spender must provide the valid signature or answer in addition to the correct redeem script. The initial part of the signature script acts as the "signature script" in P2PHK/P2Multisig, and the redeem script acts as the "pubkey script"
        - Multisig – a pubkey script that provides *n* number of pubkeys and requires the corresponding signature script provide *m* number of signatures corresponding to the provided pubkeys

        - Pubkey – Pubkey outputs are a simplified form of the P2PKH pubkey script, but aren’t as secure as P2PKH, so they generally aren’t used in new transactions anymore.
        - Null Data – Arbitrary data added to provably unspendable pubkey script that full nodes don’t have to store in their UTXO database. Null data scripts cannot be spent, so there’s no signature script.

- If you use anything besides the standard pubkey script in an output, peers and miners using the default Bitcoin Core settings will neither accept, broadcast, nor mine your transaction. Instead, you will receive an error if you broadcast the transaction to a peer. Standard transactions must meet the following conditions:
    - The transaction must be finalized – its lock time (which indicates the earliest time or earliest block when the transaction can be added to the blockchain) must be in the past (or less than or equal to the current block height), or all of its sequence numbers must be 0xffffffff
    - <100,000 bytes
    - Signature scripts must be < 1,650 bytes (which allows 15-of-15 multisig transactions in P2SH using compressed public keys)
    - The signature script can only put data to the script evaluation stack.
    - The transaction must not include any outputs which receive fewer than 1/3 as many satoshis as it would take to spent it in a typical input (currently 546 satoshis).