BITCOIN:
PROPERTY, MONEY, CURRENCY, OR LEGAL TENDER?

DAMIAN LLOYD[1]

WORD COUNT: 22,337

I hereby declare that:

(a) this is my own original work, and that no part of this assignment has been copied from any other source or person except where due acknowledgement is made;
(b) no part of the work has been submitted previously for assessment in this or any other institution; and,
(c) I have read the UQ Academic Integrity and Plagiarism Policy https://ppl.app.uq.edu.au/content/student-integrity-and-misconduct-policy and understand its implications.

Signature: Damian Lloyd
Date: 27 October 2021

Please be advised that your work may be submitted through plagiarism detection software.

[1] LLB, undertaking LLM at the University of Queensland, Australia.

I would like to thank Dr Alan Davidson, Senior Lecturer at the TC Beirne School of Law, University of Queensland, for his guidance throughout the development of this paper. I would also like to acknowledge the unwavering support and patience of my partner, Oliver Neal.

TABLE OF CONTENTS

DISCLAIMER

The views and opinions expressed in this dissertation are those of the author except where due acknowledgement is made. They do not represent the views or opinions of any Australian regulatory body, such as the Australian Taxation Office or Reserve Bank of Australia.

ABSTRACT

The terms 'property' and 'proprietary interest' are routinely used in Australian law to represent the broad category of rights an individual may have with respect to tangible and intangible things. 'Money', 'currency', and 'legal tender' are examples of property that facilitate the exchange of goods and services, settle monetary obligations, and measure wealth within a community. Within the last decade, Bitcoin, a decentralised payment system denominated in its own unit of account ('bitcoin'), has emerged as an attractive form of investment and medium of exchange. Despite its widespread use, Bitcoin's status as property, money, currency, and legal tender for Australian legal purposes remains uncertain.

This dissertation explains how an individual's right to access, redeem and use the value associated with an unspent transaction output ('UXTO') on the Bitcoin blockchain amounts to a proprietary interest for the purpose of Australian law. Each UTXO is discretely encrypted and associated with one or more private/public keypairs, which prevents the UTXO from being redeemed unless that private/public keypair is presented to 'unlock' the UTXO for use in a subsequent transaction. Due to the distributed nature of the Bitcoin blockchain, duplications of that UTXO can exist across the full nodes that maintain the Bitcoin network. Therefore, a separate proprietary right exists on all full nodes that recognise that replicated right, subject to a few exceptions. Further, when an individual redeems a UTXO on a full node, that person implicitly authorises the full node to re-transmit the transaction (and the exercise the right) on the individual's behalf to peer nodes.

This dissertation also explores the evolution of the terms 'money' and 'currency' and examines the legislative meaning of 'legal tender'. Throughout history, many objects have functioned as money, such as cowrie shells, rum bottles, and electronic entries on digitised bank ledgers. Similarly, UTXOs meet the functional and common law definition of money; and, due to its widespread adoption domestically and internationally, UTXOs also satisfy the broadest definition of currency. 'Legal tender', however, is a statutory term referring to the prescribed, 'lawful money' of a nation. UTXOs are not legal tender in Australia as the lawful money of Australia is prescribed by the *Currency Act 1965* (Cth) and *Reserve Bank Act 1959* (Cth). Due to the decree recently issued by the Legislative Assembly of the Republic of El Salvador, bitcoin has been adopted as the legal tender of El Salvador.

The conclusions reached by this dissertation influence the taxation of Bitcoin in Australia, *inter alia*. For example, the application of the capital gains tax (CGT) regime to bitcoin transactions now imposes a significant administrative burden on taxpayers. Each redemption of a UTXO (including re-transmitted transactions) has income tax implications. Further, as UTXOs satisfy the meaning of 'foreign currency' for the purpose of the *Income Tax Assessment Act 1997* (Cth), individuals can elect to account for gains or losses made in relation to UTXOs under the 'foreign exchange rules' instead of the CGT regime.

GLOSSARY

This dissertation uses several technical terms, which are defined by Table 1.

Table 1 – Meaning of technical terms

Term	Definition
bitcoin	The unit of account for the electronic payment system, 'Bitcoin'. There are no discrete physical coins or digital tokens as bitcoin are notionally 'transferred' with the redemption and creation of each UTXO.[2] A UTXO is a 'chain of digital signatures', where each 'transfer' involves digitally signing transactions with the public key of the next owner such that a recipient can validate its chain of ownership by verifying the corresponding signatures.[3]
Bitcoin	The electronic payment system conceptualised by an unknown individual or group known as 'Satoshi Nakamoto' in 2008.[4] The system utilises a digital ledger, the 'Bitcoin blockchain', in conjunction with cryptographic techniques to facilitate and record the transfer of bitcoin between Bitcoin users without using a trusted third party.[5]
bitcoin address	An encoded and shortened version of the public key.[6] It is an alphanumeric string starting with a '1' for a traditional bitcoin address or a '3' for a pay-to-script hash address.[7]
Bitcoin blockchain	The blockchain implemented by Bitcoin.
Bitcoin Core	'Bitcoin Core' refers to the practical implementation of Bitcoin as software. It includes the necessary programs to run 'wallets, a transaction and block validation engine, and a [full node]'.[8] As at the date of this dissertation, the current version of Bitcoin Core is 'Bitcoin Core 0.21.1'.[9]
BitTorrent	A computer communication mechanism based on the technical standard written by Bram Cohen, author of *The BitTorrent Protocol Specification*.[10] BitTorrent enables decentralised data sharing between connected computers, where 'multiple downloads of the same file happen concurrently'.[11]

[2] Andreas M Antonopoulos, *Mastering Bitcoin* (O'Reilly Media, Inc., 2nd ed, 2017) ch 1.
[3] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Whitepaper, 31 October 2008), 2 <https://bitcoin.org/bitcoin.pdf>.
[4] Nakamoto (n 3) 1.
[5] Ibid; Bitcoin's first block was 'mined' on 3 January 2009, and the earliest version of the software used to participate on the Bitcoin blockchain was publicly released on 9 January 2009.
[6] Antonopoulos (n 2) ch 4.
[7] The concept of a 'pay-to-script hash address' will not be addressed by this dissertation.
[8] Antonopoulos (n 2) ch 3.
[9] 'Bitcoin Core version history', *BitcoinCore* (Web Page, 25 October 2021) <https://bitcoin.org/en/version-history>.
[10] Bram Cohen, 'The BitTorrent Protocol Specification', *BitTorrent.org* (Technical Standard, 10 January 2008) <https://www.bittorrent.org/beps/bep_0003.html>.
[11] Ibid. The distribution of new versions of code amongst internal Facebook servers utilises BitTorrent: Dror G. Feitelson, Eitan Frachtenberg and Kent L. Beck, 'Development and Deployment at Facebook' (2013) 17(4) *IEEE*

Term	Definition
block	A 'data structure that aggregates transactions for inclusion' on the blockchain.[12] A block is structured into four segments: (a) the block's size, (b) the block's header (the metadata of the block), (c) the number of transactions in the block, and (d) the transactions included in the block.[13]
blockchain	A blockchain, or distributed ledger technology, refers to 'a software system for providing a decentralised record of transactions…in which each participant keeps a record of all transactions ever made…'.[14]
BTC	An abbreviation used for bitcoin, like ASX codes or hard currency abbreviations.[15] Examples of hard currency abbreviations include AUD (for Australian dollars) and EUR (for the Euro).
chainstate	The locally stored database used by a full node which maintains information about the activated and deactivated blocks that form part of its Bitcoin blockchain.[16]
chain reorganisation	Where a full node identifies that there are one or more blocks that satisfy its consensus rules, include a higher difficulty threshold (under the mining process), and extend beyond the full node's current blockchain, the full node reorganises its chainstate by deactivating blocks to reflect the longest, valid chain of blocks.[17]
consensus or protocol rules	A full node possesses a transaction and block validation engine, which is a program with pre-defined protocols or 'rules' that dictate which transactions and blocks are 'valid'.[18] Where full nodes implement the same consensus rules, they *indirectly* reach a consensus regarding the transactions and blocks that form part of the Bitcoin blockchain.

Internet Computing 1, 8 <https://research.fb.com/wp-content/uploads/2016/11/development-and-deployment-at-facebook.pdf>.

[12] Antonopoulos (n 2) ch 9.

[13] Ibid. For examples of the transactions that appear on the Bitcoin blockchain, see Blockchain.com, Inc., 'Blocks' *Blockchain.com* (Web Page, 20 August 2021) <https://www.blockchain.com/btc/blocks?page=1>. Please note that this blockchain does not represent every Bitcoin blockchain in existence. These transactions relate to the Bitcoin blockchain maintained by Blockchain.com, Inc's full node.

[14] *Macquarie Dictionary* (online at 20 August 2021) 'blockchain' (def 1). For a more detailed technical description of a 'blockchain', see Antonopoulos (n 2) ch 9.

[15] Abbreviations for other cryptocurrencies include BCH (Bitcoin Cash), ETH (Ethereum), ETC (Ethereum Classic). Some abbreviations for cryptocurrencies may be misleading. For example, Monero is a privacy cryptocurrency that has undergone several 'forks'. Although there are multiple abbreviations for the purported variants of Monero (for example, XMR, XMO, XMC and XMZ), some of these variants are interoperable.

[16] GR0KCHAIN, 'Understanding the data behind Bitcoin Core', *Bitcoin Developer Network* (Web Page, 25 September 2021) <https://bitcoindev.network/understanding-the-data/>.

[17] Walker, Greg, 'Chain Reorganisation', *Learn me a bitcoin* (Web Page, 6 September 2019) <https://learnmeabitcoin.com/technical/chain-reorganisation>.

[18] See Antonopoulos (n 2) ch 10.

Term	Definition
encode	To encode something is to 'put [a thing] into a coded form'.[19] Bitcoin leverages several forms of cryptography to encode private keys (into public keys) and public keys (into bitcoin addresses).
fork	A fork occurs when the blockchains of two or more full nodes are compared and, at some point in time, the blockchains diverge. Forks are typically resolved when full nodes with dissimilar blockchains communicate with one another and, after identifying which sequence of valid blocks forms the longest chain, undergo a chain reorganisation.[20] Consequently, the full nodes synchronise their Bitcoin blockchains. Where that communication does not occur, the full nodes will continue to develop and maintain dissimilar blockchains, causing a 'chain split' (a version of the blockchain that only possesses identical blocks prior to the fork).[21]
full node	A full node is a computer program that: (a) Possesses and maintains its own version of a blockchain; (b) Applies consensus rules to determine which transactions are added to its version of a blockchain at any given time;[22] (c) Receives transactions from 'lightweight clients';[23] (d) Propagates new transactions and blocks to peer nodes;[24] and, (e) Updates lightweight clients with transactions affecting their wallets.[25]
genesis block	The first block commencing a blockchain, known as Block 0.[26]
hash or hash function	A hash function is an irreversible mathematical algorithm that accepts an input of any length and produces an output of a fixed length ('the hash') without any two inputs ever producing the same output.[27] Specifically, a hash function is a process to encode information.

[19] *Macquarie Dictionary* (online at 20 August 2021) 'encode' (def 1).
[20] Antonopoulos (n 2) ch 10.
[21] See Australian Taxation Office, 'Chain splits', *Transacting with cryptocurrency* (Web Page, 20 August 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?page=2#Chain_splits>; See also the evolution of Bitcoin as compared to Bitcoin Cash.
[22] 'Running A Full Node' *What Is A Full Node?* (Documentation, 2021) <https://bitcoin.org/en/full-node#what-is-a-full-node>.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] See Blockchain.com, Inc., 'Block 0' *Blockchain.com* (Web Page, 30 August 2021) <https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>. Block 0 contains one transaction: the generation of 50 new bitcoin issued to bitcoin address '1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa'. As of 25 October 2021, this UTXO remains unspent.
[27] Karan Singh Garewal, 'Practical Blockchains and Cryptocurrencies' (1st ed, 2020) Apress Media LLC, 38.

Term	Definition
lightweight client	A software program with fewer functions compared to a full node. While lightweight clients can independently store their own private/public keypairs, display the current bitcoin associated with a user's private key, and create and transmit transactions, they must connect with a full node to confirm previous bitcoin transactions. This is because they do not possess their own version of the Bitcoin blockchain.
memory pool, mempool or transaction pool	The memory pool refers to the temporary, digital location where transactions that have been verified by the individual's full node as 'valid' are stored.[28]
miner or mining node	A mining node is a computer that engages in the process of 'mining'. An individual that exploits mining nodes may be referred to as a 'miner'.
mining	Mining refers to the process of creating compatible 'blocks' for a full node's blockchain.
open-source	Open-sourced software refers to software where 'the source code…is freely available to allow others to develop versions and derivatives which again must be made freely available'.[29]
peer node	A full node connected to other full nodes.
private key	A random number between 1 and 1.158 * 10^{77}, typically translated into a 64-hexadecimal string.[30]
private/public keypair	As a public key is produced by encoding a private key, that public key will have a mathematical relationship with the private key. A 'keypair' reflects this mathematical relationship and are distinguishable from public and private keys that have no association.
public key or pubkey	An encoded and shortened version of the private key, which creates a unique mathematical relationship between the public key and the private key.
satoshi	The smallest denomination of bitcoin. One satoshi is equal to one hundred millionth of a bitcoin, or BTC0.00000001.
Tx	An abbreviation of 'transaction'. For example: Tx(1) means the first transaction of a series of transactions.

[28] Bitcoin Project, 'Memory Pool', *Developer Guides: P2P Network* (Documentation, 2021) <https://developer.bitcoin.org/devguide/p2p_network.html>.
[29] *Macquarie Dictionary* (online at 18 August 2021) 'open-source' (def 1). See also Pedro Franco, *Understanding Bitcoin*: *Cryptography, engineering, and economics* (Wiley, 1st ed, 2015) 6—8.
[30] Antonopoulos (n 2) ch 4.

Term	Definition
UTXO or UTxO	An abbreviation of 'unspent transaction out' or 'unspent transaction output'. A UTXO refers to an output in a transaction that has not been subsequently used as an input for a later transaction. Specifically, it refers to an output that is cryptographically secured in relation to a public key such that only the entity with the corresponding private key is authorised to access, redeem and use the amounts of bitcoin associated with that UTXO.
wallet	A wallet 'refers to the data structure [or software] used to store and manage a user's keys',[31] including private and public keys. Using the private keys known to that wallet, the software can track the balance of the UTXOs associated with those private keys and sign transactions on behalf of the user.[32]

[31] Antonopoulos (n 2) ch 5.
[32] Ibid.

I INTRODUCTION

The hare of science and technology lurches ahead.
The tortoise of the law ambles slowly behind.[33]

The Hon Michael Kirby, 1987

A *Background*

Almost twelve years have passed since the concept of a decentralised, trustless, and digital payment system was formulated and refined into the technologies now known as 'Bitcoin'. Early adopters, who were sceptical of the power asserted by established financial institutions, welcomed Bitcoin as a decentralised medium of exchange and promoted the use of bitcoin like hard currency, like Australian dollars, to acquire goods and services, settle monetary obligations, and compensate them in lieu of salary and wages.[34] Like hard currencies, there were also those who exploited the technology's pseudonymity to launder money, finance terrorist campaigns, and pursue other criminal activities. Over time, individuals acquired bitcoin as an investment,[35] seeking to gain from its fluctuating speculative value and rising popularity.

Gone are the days, however, where one could buy two pizzas for BTC10,000;[36] a single bitcoin today is currently worth approximately AUD81,000.[37] CoinMarketCap, a company that monitors the volume and price of bitcoin and other cryptocurrencies, estimates that there are approximately BTC18,850,000 currently in circulation on the Bitcoin blockchain, with a market capitalisation of roughly AUD1.5 trillion.[38] Between 24 and 25 October 2021 alone, the Bitcoin blockchain saw transaction volumes of AUD36.5 billion globally.[39]

Despite such widespread interest and adoption, few common law judicial systems have confirmed how Bitcoin is treated at law.[40] In fact, there are no Australian cases that consider whether bitcoin is 'property', 'money' or 'currency' for Australian legal purposes.[41] Instead, the Australian Taxation Office ('ATO') and the Reserve Bank of Australia ('RBA') have issued

---

[33] Justice Michael Kirby, 'Medical Technology and New Frontiers of Family Law' (1987) 1 *Australian Journal of Family Law* 196, 212.
[34] Australian Taxation Office, 'Paying salary or wages in cryptocurrency', *Cryptocurrency used in business* (Web Page, 21 September 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?page=3#Paying_salary_or_wages_in_cryptocurrency>.
[35] Australian Taxation Office, 'Cryptocurrency as an investment', *Transacting with cryptocurrency* (Web Page, 21 September 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?page=2#Cryptocurrency_as_an_investment>.
[36] Seth Litwack, 'Bitcoin: Currency or Fool's Gold: A Comparative Analysis of the Legal Classification of Bitcoin' (2015) 29(2) *Temple International & Comparative Law Journal* 309, 309. It is worth noting that, if this transaction occurred today, the value of those pizzas would be approximately AUD6.5 billion.
[37] CoinMarketCap OpCo, LLC, 'Bitcoin', *CoinMarketCap* (Web Page, 25 October 2021) <https://coinmarketcap.com/currencies/bitcoin/>.
[38] Ibid.
[39] Ibid.
[40] See *Ruscoe v Cryptopia Limited (in liq)* [2020] NZHC 728; *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17; *Securities and Exchange Commissioner v Shavers,* (D Tex, No 4:13–CV–416, 18 September 2014); *Skatteverket v David Hedqvist* (Court of Justice of the European Union, C-264/14, 22 October 2015); *United States v Faiella*, 39 F. Supp. 3d 544 (SD NY, 2014).
[41] Deputy President Bernard McCabe considered whether bitcoin was a 'foreign currency' for the purpose of Division 775 of the *Income Tax Assessment Act 1997* (Cth) in *Seribu Pty Ltd v Commissioner of Taxation* [2020] AATA 1840.

public guidance to address commonly asked questions about bitcoin, including whether bitcoin is 'property' and therefore a CGT asset for taxation purposes,[42] and Australia's position on bitcoin as 'money'.[43]

As will be explored throughout this dissertation, these views are predicated on several 'one stop shop' explanations of Bitcoin. These explanations fail to identify the specific mechanisms that are relevant when considering the application of existing legal doctrine and, consequently, reduce Bitcoin's complex functions into vague and misleading statements of facts.[44] These 'facts' form the basis of government decisions, shaping how nations deal with Bitcoin at law, and influencing cryptocurrency communities into adopting behaviours to avoid persecution.

Australia's current regulatory treatment of Bitcoin reflects the statement made by the Hon Michael Kirby above. Technology is rapidly evolving, and the law is not keeping pace. Lawyers are struggling to adapt legal principles to these new technologies and fail to grasp the realities of the technology itself. The treatment of Bitcoin by Australian regulators and international courts also highlights a broader lack of technological capability. This is troubling as Bitcoin was conceptualised over a decade ago and is no longer regarded as a new technology.[45]

The purpose of this dissertation, therefore, is twofold. Firstly, it provides a plain English explanation of the relevant concepts that enable Bitcoin to operate. Diagrams and examples are included to deconstruct complex concepts and demonstrate the practical steps involved in bitcoin transactions. Secondly, and as a consequence of the first objective, this dissertation will demonstrate that:

(a) unspent transaction outputs ('UTXOs') on most full nodes amount to separate proprietary interests;

(b) UTXOs are a form of money, but their treatment as money under Australian law may depend on the specific legislative provision applied or cause of action raised;

(c) UTXOs are currency under the broadest definition of the term; [46] and,

(d) UTXOs are not 'legal tender' for the purpose of the *Currency Act 1965* (Cth) or *Reserve Bank Act 1959* (Cth).

This dissertation will also briefly consider the Australian income tax consequences that follow from each conclusion.

---

[42] See the Australian Taxation Office, 'Transacting with cryptocurrency', *Tax treatment of cryptocurrencies* (Web Page, 19 September 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?anchor=Transactingwithcryptocurrency#Transactingwithcryptocurrency>; See also Taxation Determination TD 2014/26 *Income tax: is bitcoin a 'CGT asset' for the purposes of subsection 108-5(1) of the Income Tax Assessment Act 1997?*

[43] Reserve Bank of Australia, 'What are cryptocurrencies', *Cryptocurrencies* (Web Page, 19 September 2021) <https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html>.

[44] See Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Report, 3 May 2016) <https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf>.

[45] There are almost 12,000 cryptocurrencies in existence as at the date of this dissertation.

[46] Following the decision in El Salvador to treat Bitcoin as legal tender in 2021, UTXOs will be currency even under stricter interpretations of the term. Consequently, Australia must recognise UTXOs as a foreign currency under the *Currency Act 1965* (Cth).

B *Structure*

This dissertation is separated into five chapters. Chapter 1 outlines the issues faced by the Australian legal system following the steady and pervasive uptake of Bitcoin domestically and internationally. It highlights the central hypotheses to be considered, as well as the methodology that will be employed to test those hypotheses. This Chapter concludes by outlining the scope of the author's research and addressing limitations of the dissertation.

Chapter 2 outlines the Bitcoin payment system, its unit of account, and other related technological concepts. This background is necessary to provide a foundation for the subsequent legal analyses and demonstrates why this dissertation necessarily departs from the conclusions reached by Australian regulatory bodies and bitcoin legal commentators.

Chapter 3 reviews the existing Anglo-Australian common law cases that determine when a thing amounts to 'property' or a 'proprietary interest'. By leveraging inductive reasoning, the Chapter distils the legal principles applied by these cases into key indicia. These indicia are subsequently considered with respect to Bitcoin, where it is concluded that unspent transaction outputs ('UTXOs') on full nodes amount to separate proprietary interests. This Chapter then examines the Australian income tax implications that arise from this conclusion.

Chapter 4 considers whether UTXOs amount to money, currency, and legal tender. The concepts of money, currency and legal tender are closely related for Australian legal purposes. Consequently, this Chapter reviews existing Anglo-Australian common law cases and concludes that UTXOs are money and currency. However, UTXOs are not 'legal tender' as defined by the *Currency Act 1965* (Cth) and *Reserve Bank Act 1959* (Cth). Like Chapter 3, Chapter 2 examines the Australian income tax implications that arise from each conclusion.

Finally, Chapter 5 will affirm the broad conclusions made in the preceding Chapters and submit that other cryptocurrencies or crypto-assets that are functionally equivalent may be treated the same by analogy.

C *Methodology*

This dissertation considers two hypotheses. Firstly, it will determine whether Bitcoin amounts to 'property' or a 'proprietary interest' for Australian common law purposes. Once this has been established, it will then determine whether it also amounts to 'money', 'currency', or 'legal tender' for Australian legal purposes.

To test the hypotheses, this dissertation will adopt a doctrinal methodology. A doctrinal methodology refers to the process of systematically analysing 'the rules governing a particular legal category, [analysing] the relationship been the rules', identifying areas of ambiguity and 'extracting general principles from an inchoate mass of primary materials'.[47] This methodology furthers the legal system's ability to achieve constancy and logical consistency whilst adapting

[47] Terry Hutchinson and Nigel Duncan, 'Defining and describing what we do: doctrinal legal research' (2012) 17(1) *Deakin Law Review* 83, 101, 105, citing Council of Australian Law Deans, 'CALD Statement on the Nature of Research' (May and October 2005) 3.

the common law for future developments.

As highlighted by the Council of Australian Law Deans, this method of legal reasoning 'is a subtle and sophisticated jurisprudential concept, a unique blend of deduction and induction, that has engaged legal scholars for generations'.[48] This dissertation intends to leverage inductive reasoning to derive general propositions about the meaning of the terms 'property', 'money', and 'currency'. It will do this by reviewing available primary sources, such as legislative definitions and judicial decisions from an array of relevant Anglo-Australian cases, weighing their relevance in accordance with the doctrines of binding and persuasive precedents.

Once these broad legal principles have been expounded, the dissertation will employ deductive reasoning and analogy to examine whether concepts relating to Bitcoin fall within those principles. Where relevant, this dissertation considers the judgments reached by international courts in other common law countries. Secondary sources, like related peer-reviewed articles and journals, regulatory publications, official dictionaries[49] and legal encyclopaedias, will also be referenced.

This dissertation leverages several technical sources of information, including the Bitcoin whitepaper, Bitcoin Core developer guides, Bitcoin expert publications, and blogs or forums which share insights into the practical mechanics of the Bitcoin software. There exist few peer-reviewed books and reports that explain these concepts in the same level of detail as these blogs and forums. Rather, peer-reviewed publications typically provide a concise overview of the technology at the expense of those critical, practical steps that enable Bitcoin to operate. Including the information outlined in technical blogs and forums ensures that the factual matrix reflects these practical steps.

Ultimately, the conclusions reached by this dissertation will be predicated on logic, seeking to predict the decisions that Australian courts would reach if presented with the same facts.

D *Limitations*

This dissertation is subject to several limitations that must be outlined. Firstly, the views expressed in this paper are strictly limited to Bitcoin as implemented by 'Bitcoin Core 0.21.1'. It does not refer to any Bitcoin blockchains maintained by full nodes that adopt consensus rules that are incompatible with Bitcoin Core 0.21.1. For example, this dissertation does not address Bitcoin XT, Bitcoin Cash, Bitcoin Unlimited, Bitcoin SV, or the assortment of 'altcoins' that leveraged the open-source implementation of Bitcoin to create a distinct cryptocurrency. While they may be functionally similar, the author has not considered their features in any detail and cannot guarantee that they are functionally equivalent. Further, this paper does not address other cryptocurrencies or 'crypto-assets' for similar reasons.[50]

Secondly, this dissertation provides an exposition of the critical mechanisms of Bitcoin. There

[48] Council of Australian Law Deans, 'CALD Statement on the Nature of Research' (May and October 2005) 3.
[49] See Melbourne University Law Review Association, *Australian Guide to Legal Citation* (Melbourne University Law Review Association Inc, 4th ed, 2018) r 1.9.1.
[50] 'Crypto-assets' include customisable digital tokens (like ERC20 tokens), non-fungible tokens (like ERC721 tokens), and stablecoins (like Tether). This is because the process of creating, accessing, redeeming, and using crypto-assets is dissimilar to Bitcoin.

are other features to this system, but these features will not be explored in any detail. It will not explore the precise mathematics or cryptography underpinning the Bitcoin software nor the physical methods used by computers to store data relating to the Bitcoin. None of these features or topics contribute to a person's understanding of Bitcoin for the purposes outlined by this dissertation.

Thirdly, this dissertation does not consider the arrangements where a person reaches an agreement with a third party, such as a digital currency exchange ('DCE'), to facilitate bitcoin transactions on their behalf. While these arrangements are common, exploring the form and manner in which these arrangements can be carried out would not contribute to the conclusions reached by this dissertation.

Finally, as highlighted by the Methodology, this dissertation recognises that there are limited Australian and international cases that directly discuss the application of legal concepts to Bitcoin concepts. Similarly, existing peer-reviewed articles and reports provide broad overviews of the technology but fail to consider the critical mechanisms that enable Bitcoin to operate. As the reliability of the information presented in these reports is questionable, the author has curated information about Bitcoin from a range of technical sources (such as Bitcoin developer forums and official Bitcoin Core documentation) to ensure the mechanics of Bitcoin are accurately recorded. While the author has made every effort to ensure the accuracy of this information, this dissertation cannot guarantee that these sources are not fallible as they have not been formally peer-reviewed.

II THE NATURE OF BITCOIN

> *We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-work to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of CPU power. The network is robust in its unstructured simplicity.*[51]
>
> **Satoshi Nakamoto, 2008**

The notion of 'Bitcoin' refers to the electronic payment system conceptualised in 2008 by an unknown individual or group known as Satoshi Nakamoto.[52] The system utilises a digital ledger, the 'Bitcoin blockchain', in conjunction with cryptographic techniques to facilitate and record the movement of 'bitcoin' between Bitcoin users without using a trusted third party.[53]

Andreas Antonopoulos, author of *Mastering Bitcoin*,[54] explains that 'Bitcoin is a collection of concepts and technologies that form the basis of a digital…ecosystem' that has 'no "central" server or point of control'.[55] Instead, the Bitcoin blockchain is distributed to all participants in the ecosystem, who communicate using peer-to-peer networks (such as the Internet or the BitTorrent protocol). Provided that one has access to some form of computing device, such as a laptop or smartphone, anyone can download the open-source software called 'Bitcoin Core' (or another suite of programs available), operate a full node or lightweight client, and participate in the Bitcoin network.[56]

Despite the ease with which one can connect with the Bitcoin network, its automated mechanisms conceal a complex payment system. This paper expands upon the critical concepts that allow the movement of bitcoin between users to occur. These concepts include:

(a) Bitcoin does not track individual bitcoin or any denomination ('the satoshi').
(b) 'Full nodes' maintain their own Bitcoin blockchain.
(c) The 'memory pool' stores validated transactions.
(d) Full nodes 'gossip' with peer nodes.
(e) The relevance of 'mining'.
(f) A 'fork' cannot occur on a full node's Bitcoin blockchain.

Each of these concepts will be explored in further detail below.

[51] Nakamoto (n 3) 8. The irony is that the purported 'unstructured simplicity' of Bitcoin leads to a complex application of common law concepts.
[52] Nakamoto (n 3).
[53] Nakamoto (n 3) 1.
[54] Antonopoulos (n 2).
[55] Antonopoulos (n 2) ch 1.
[56] Antonopoulos (n 2) ch 1.

A *Bitcoin does not track individual bitcoin*

It is important to note that Bitcoin does not track each individual bitcoin (or its smallest denomination, the 'satoshi').[57] Instead, Bitcoin tracks the 'parcels' of bitcoin that have been spent or remain unspent as at a point in time. The bitcoin, themselves, do not have a physical or even digital form – they are merely 'implied in transactions that transfer value from sender to recipient'.[58] Nakamoto expresses this concept in *Bitcoin: A Peer-to-Peer Electronic Cash System*, highlighting that:

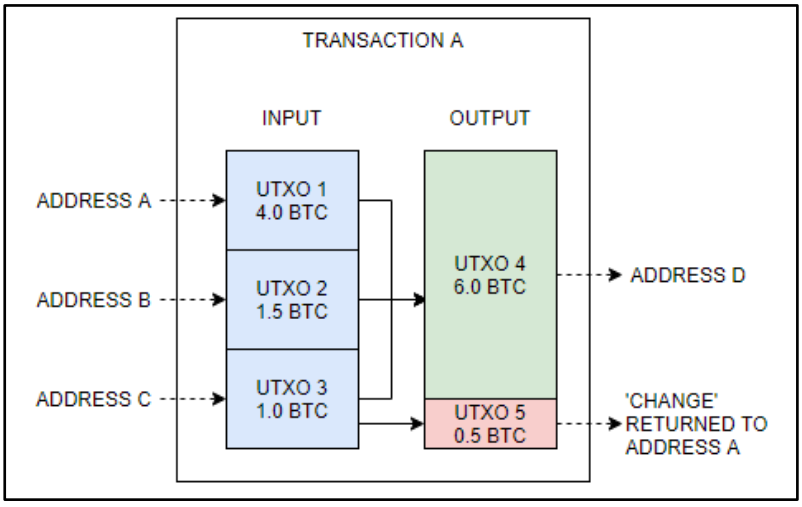
> [a]lthough it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.[59]

These unspent transaction outputs ('UTXO') are then used as inputs for new transactions. For example, in Diagram 1 below, Individual A controls three 'parcels' of bitcoin totalling BTC6.5:

(a) UTXO 1 associated with bitcoin address A contains BTC4.0.[60]
(b) UTXO 2 associated with bitcoin address B contains BTC1.5.
(c) UTXO 3 associated with bitcoin address C contains BTC1.0.

Individual A wishes to transfer BTC6.0 to Address D, held by Individual B. Unfortunately, Individual A does not possess a combination of UTXOs that equal the desired transfer amount. As it is not possible to use a portion of the bitcoin associated with a UTXO in a transaction, all Individual A's UTXOs are required as inputs for this transaction.

Diagram 1 – How bitcoin transfers are implied in UTXOs



[57] Nakamoto (n 3) 5.
[58] Antonopoulos (n 2) ch 1. Cf Sarah Green, 'It's Virtual Money' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019) [2.05].
[59] Nakamoto (n 3) 5.
[60] Public key hashed and encoded in certain format creates a bitcoin address.

Consequently, two *new* UTXOs are created.[61] UTXO 4, which contains BTC6.0, becomes associated with Address D. UTXO 5, which contains BTC0.5 (Individual A's excess bitcoin), becomes re-associated with Address A.[62] This is commonly referred to as the 'change' mechanism.

This means that, when a person refers to controlling bitcoin or having a set holding of bitcoin, they are referring to the UTXO that is cryptographically secured such that only that person's public/private keypair is permitted to access, redeem, and use the amounts of bitcoin associated with that UTXO.[63] The UTXO can only be spent if the individual presents:

(a) The public key that matches the hash ('fingerprint') of the UTXO, and
(b) A signature from the private key associated with the public key used in (a).[64]

However, as will be explored next, a UTXO is recorded on a full node's own Bitcoin blockchain. It is critical to note that the public key must match the hash of the UTXO as it appears in the full node's blockchain. When a full node communicates with other full nodes, transmitting transactions and blocks, these UTXOs are replicated on the Bitcoin blockchains of other full nodes.

B *Full nodes maintain their own blockchain*

Bitcoin does not have a central server, opting for a distributed digital ledger that is maintained by 'full nodes'. These full nodes are computer programs that serve several functions, including:

(a) Possessing and maintaining their own version of the Bitcoin blockchain;
(b) Applying pre-programmed protocols and rules ('consensus rules') to determine which transactions are added to their version of the Bitcoin blockchain at any given time;[65]
(c) Receiving transactions from connected 'lightweight clients';[66]
(d) Propagating new transactions and 'blocks' to connected full nodes;[67] and,
(e) Updating connected lightweight clients with transactions that affect their wallets.[68]

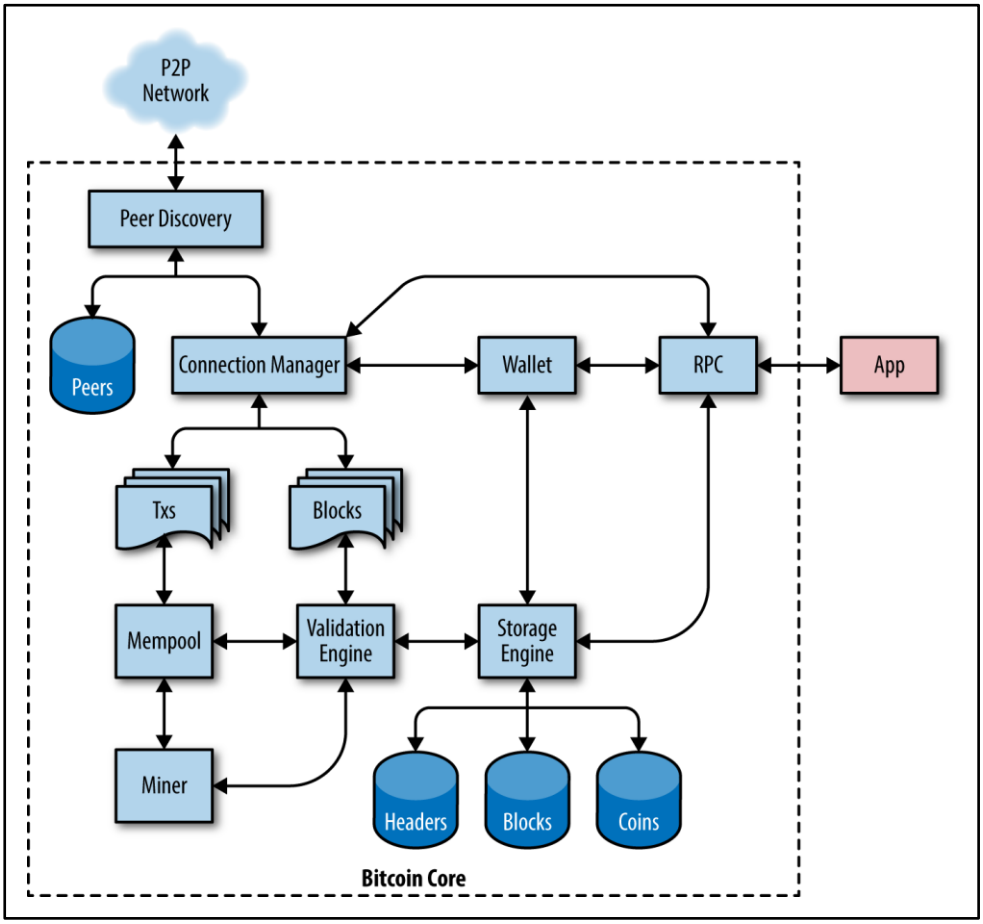
An individual can download the necessary software ('Bitcoin Core') to operate a full node from the Bitcoin Core website: https://bitcoin.org/en/download. This software is a collection of files containing data and operations stored onto the individual's computer.[69] An overview of the various components of Bitcoin Core are shown in Diagram 2. Other versions can be downloaded; however, their range of functions differs to the software for operating a full node.

---

[61] See UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smart contracts* (Legal Statement, November 2019) [45].
[62] Please note that this example does not include the transaction fees that are typically paid to process the transaction by miners.
[63] For completeness, a UTXO is always associated with a bitcoin address, which is generated by an individual's public key (which in turn is generated by the individual's private key).
[64] Bitcoin Project, 'Introduction', *Developer Guides: Transactions* (Documentation, 18 August 2021) <https://developer.bitcoin.org/devguide/transactions.html>.
[65] 'Running A Full Node' *What Is A Full Node?* (Documentation, 2021) <https://bitcoin.org/en/full-node#what-is-a-full-node>.
[66] Ibid.
[67] Ibid.
[68] Ibid.
[69] See *Macquarie Dictionary* (online at 18 August 2021) 'software' (def 1).

These alternative versions include 'lightweight clients'. Lightweight clients still require a connection with a full node to validate transactions and update wallet balances based on that full node's Bitcoin blockchain.[70] If there is only one full node operating Bitcoin but many lightweight clients, Bitcoin would become a centralised ledger. This is because the full node would be the only computer that possesses a full version of the Bitcoin blockchain necessary to validate transactions and add new blocks to the Bitcoin blockchain.

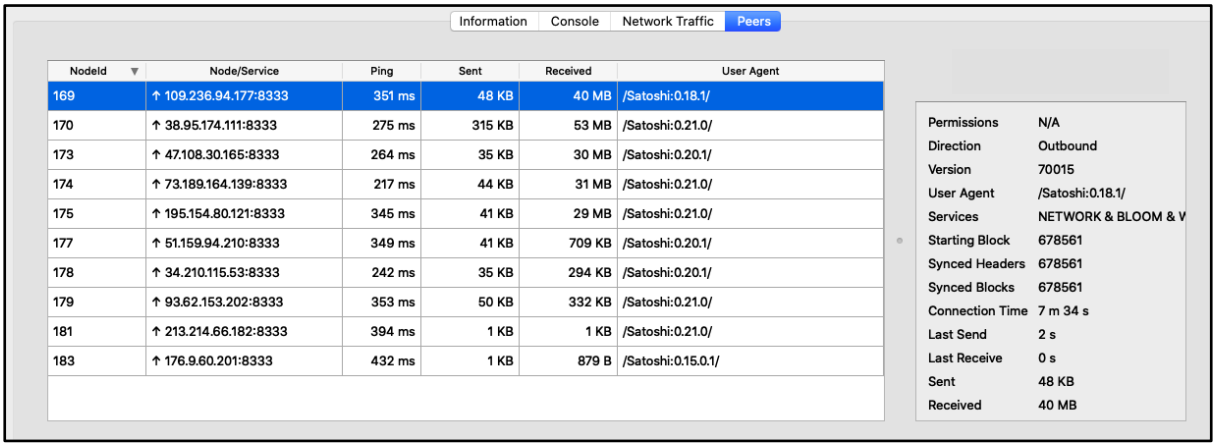
Diagram 2 – Bitcoin Core components and interactions[71]



Bitcoin Core contains several pre-programmed full nodes ('DNS seeds') to which the newly download full node may connect.[72] This is typically achieved by using the Internet to connect to the DNS seed's IP address. A full node is also capable of checking for peer nodes and storing their details for future reference. This is seen in Diagram 3 below.

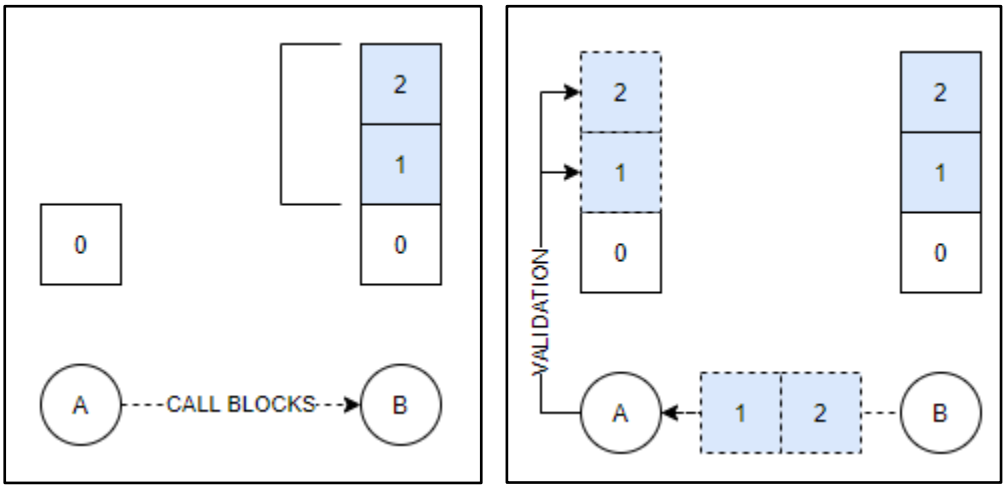
[70] See 'Software', *Bitcoin Wiki* (Documentation, 17 August 2021) <https://en.bitcoin.it/wiki/Software>.
[71] Image sourced from Andreas M Antonopoulos, 'Mastering Bitcoin' (2nd ed, 2017) O'Reilly Media, Inc. Ch 3. Some of the terms expressed in this image, such as 'RPC', 'Storage Engine', 'Connection Manager' and 'App', will not be explored in this dissertation.
[72] Bitcoin Project, 'Peer Discovery', *Developer Guides: P2P Network* (Documentation, 17 August 2021) <https://developer.bitcoin.org/devguide/p2p_network.html>.

Diagram 3 – Bitcoin Core Peer nodes display



When initially downloaded, Bitcoin Core contains only one block on its blockchain: the genesis block.[73] This means that the full node must contact a peer node and request all the blocks that follow that peer node's genesis block. This is seen in Diagram 4 below, where Node A transmits requests to Node B for blocks starting from the block after Node B's genesis block and ceasing when the final block in Node B's blockchain is received.

Diagram 4 – New full node calling for blocks and adding them to its Bitcoin blockchain



The peer node will transmit to the full node each block for validation and inclusion on that full node's own blockchain. Due to the current size of the Bitcoin blockchain,[74] this can take at least a week on a standard laptop computer. There are several methods to download and validate each block on the Bitcoin blockchain, however these methods will not be addressed by this dissertation.

Once this process is complete, the full node will possess an identical but separate version of the Bitcoin blockchain. This means that new peer nodes can request from that full node all blocks after its genesis block, in the same manner that the full node had originally acquired its version of the Bitcoin blockchain.

[73] Bitcoin Project, 'Initial Block Download', *Developer Guides: P2P Network* (Documentation, 2021) <https://developer.bitcoin.org/devguide/p2p_network.html>.
[74] As at 7:19PM AEST on 30 August 2021, there were 698,253 blocks on the Bitcoin blockchain.

As of 20 January 2021, the CoinTelegraph suggests that there are 11,558 reachable nodes currently active across Bitcoin.[75] Provided that these nodes are all full nodes, this could mean that there are 11,558 versions of the Bitcoin blockchain in existence. It is also worth noting that new full nodes can be introduced at any time, and existing full nodes can opt out of the Bitcoin network. Opting out of the Bitcoin network generally refers to deleting all software necessary to operate a full node. Therefore, the total number of Bitcoin blockchains maintained by full nodes fluctuates over time.

C *Memory pools store validated transactions*

The 'memory pool' is an overlooked Bitcoin mechanism as developers and authors focus more on transactions included in blocks and 'confirmations' of those blocks.[76] A mempool refers to the temporary, digital location where transactions that have been verified by the individual's full node as 'valid' are stored.[77] While the mempool is intended to be a temporary storage mechanism to house validated transactions prior to their addition to the blockchain, there are instances where these transactions – despite being validated – can fail to be added to the full node's Bitcoin blockchain. As highlighted by the Bitcoin Core website:

> When a [full node] shuts down, its memory pool is lost except for any transactions stored by its wallet. This means that never-mined unconfirmed transactions tend to slowly disappear from the network as [full nodes] restart or as they purge some transactions to make room in memory for others.[78]

'Unconfirmed' transactions refers to transactions that do not form part of a block on a full node's blockchain. If a full node shuts down, any validated but unconfirmed transactions held by that full node are deleted as the mempool ceases to store those transactions. However, this does not mean that the transactions are lost. There are circumstances where the transactions may have been validated by the individual's full node and subsequently broadcast to peer nodes. If the individual's full node is shut down after this time, the transactions may still be added into the mempool by a peer node. Where that peer node incorporates the transaction into a block, it may be added to the peer node's Bitcoin blockchain.

D *Full nodes 'gossip' with peer nodes*

An individual seeking to send bitcoin to another user will need to operate their own full node or use a lightweight client to connect to a full node that processes and validates the transaction on its behalf. If the transaction complies with the consensus rules of the full node, it will form part of the mempool. If the transaction does not comply with the consensus rules, it will be rejected. Consequently, the transaction will not pass into the mempool nor be transmitted to peer nodes.

---

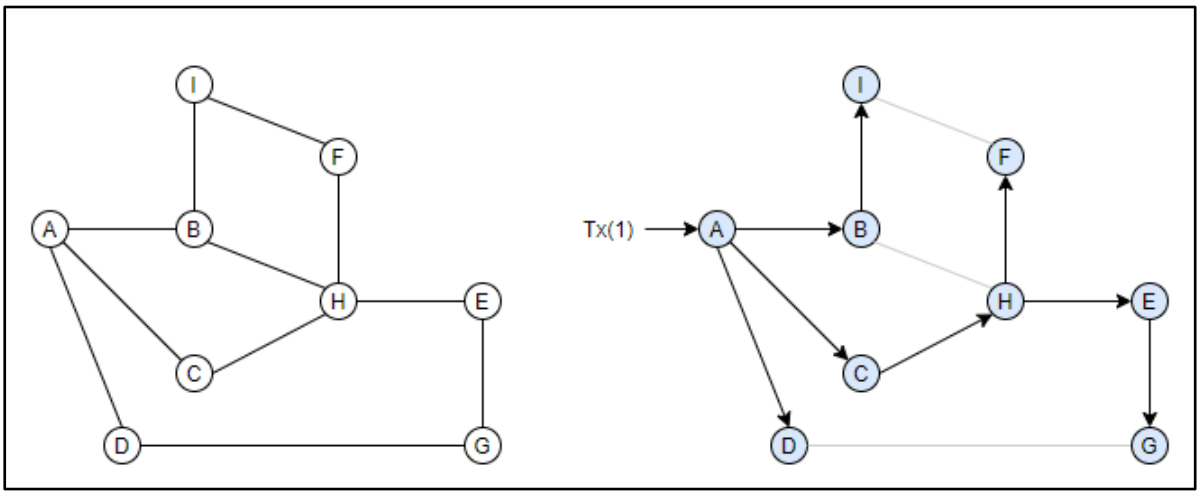
[75] Cyrus McNally, 'Bitcoin node count hits new all-time high' *CoinTelegraph* (online, 15 August 2021) <https://cointelegraph.com/news/bitcoin-node-count-hits-new-all-time-high>.
[76] See UK Jurisdiction Taskforce (n 61) [54].
[77] Bitcoin Project, 'Memory Pool', *Developer Guides: P2P Network* (Documentation, 2021) <https://developer.bitcoin.org/devguide/p2p_network.html>. See Antonopoulos (n 2) ch 8.
[78] Ibid.

A peer node connected to a full node may request the transactions that form part of the full node's mempool. Once transferred, this peer node seeks to validate the transactions using its own version of the consensus rules. In most cases, these consensus rules will be identical. As explained above, the transaction will only be added to the peer node's mempool if it complies with the peer node's version of the consensus rules. This process of validating and re-transmitting ('gossiping') a transaction is repeated until the transaction is communicated to as many connected full nodes as possible. As noted by Nakamoto:

> New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long.[79]

This transmission is best demonstrated by Diagram 5 below. In this example, each full node is represented by the letter 'A' through to 'I'. Each full node is also connected to a set number of peer nodes, represented by a solid, straight line between the nodes. 'Tx(1)', being a transaction initiated by a Bitcoin user, is transmitted to Node A for validation. Provided that the transaction is valid for each full node, the transaction could propagate through the network of full nodes as shown.

Diagram 5 – How a transaction may be propagated to other full nodes



E *Relevance of mining*

While it is possible for an individual to transact with an unspent transaction output ('UTXO') in a full node's mempool that has not been added to the full node's blockchain, proponents of Bitcoin recommend that individuals wait for the transaction to be added ('mined') to the full node's blockchain first.[80] This is on the assumption that a transaction becomes 'immutable' when it is added to the blockchain. For the reasons outlined in this Part, the notion that blocks added to a blockchain become 'immutable' is misleading, as a full node can undergo a 'chain reorganisation'.[81]

---

[79] Nakamoto (n 3) 4. Cf Bitcoin Project, 'Memory Pool', *Developer Guides: P2P Network* (Documentation, 2021) <https://developer.bitcoin.org/devguide/p2p_network.html>.
[80] See Nakamoto (n 3) 7. See also UK Jurisdiction Taskforce (n 61) [54].
[81] The statement that the blockchain is 'immutable' is frequently referenced by authors. See, eg, Emma Beechey, 'Blockchain and cryptocurrencies for barristers' (2018) *The Journal of the NSW Bar Association* 25, 26. Cf UK Jurisdiction Taskforce (n 61) [54].

Mining is the process of creating compatible 'blocks' containing validated transactions for addition to a full node's blockchain.[82] The process can be conducted by any full node that possesses a Bitcoin blockchain and sufficient hardware (such as a GPU) to run repetitive computations. Broadly, mining involves:

(a) collecting valid transactions from a full node's mempool,
(b) expressing those transactions in a set format (the 'block template'),[83]
(c) using hardware to iterate through hashes of the block's header to find a hash that satisfies a predefined pattern ('difficulty threshold'),[84] and
(d) where that hash is identified, communicating the newly created block to peer nodes.[85]

Nakamoto highlights that Bitcoin blocks contains two built-in incentives for full nodes to mine new blocks and distribute them to peer nodes: (a) the coinbase reward, and (b) transaction fees. Specifically:

> By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block ['the coinbase reward']. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them.[86]

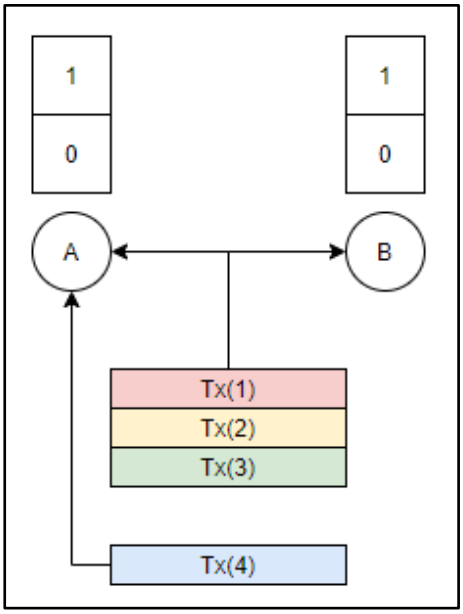
The coinbase reward is designed so that the bitcoin awarded to a successful miner is halved every 210,000 blocks.[87] This means that the total bitcoin that can ever be in circulation is BTC20,999,999.97690000 and is expected to occur in the year 2140.[88] Miners can also be rewarded with transactions fees, which is payable to the miner when the 'output value of a transaction is less than its input value'.[89] These incentives mean that, over time, it is expected that transactions will transition through the mempool and end up in a block on the full node's blockchain.

There are circumstances where a newly mined block will not form part of a full node's Bitcoin blockchain, such as a chain reorganisation.[90] A chain reorganisation refers to a process where a full node systematically activates and deactivates certain blocks on its Bitcoin blockchain to reflect a chain of blocks in its database with the most cumulative difficulty threshold.[91] This chain of blocks is called the 'main chain', and the blocks that have been deactivated are known as the 'secondary chains'. In Diagram 6, Node A and B possess identical Bitcoin blockchains. Each full node receives Tx(1), Tx(2), and Tx(3); however, only Node A receives Tx(4).

---

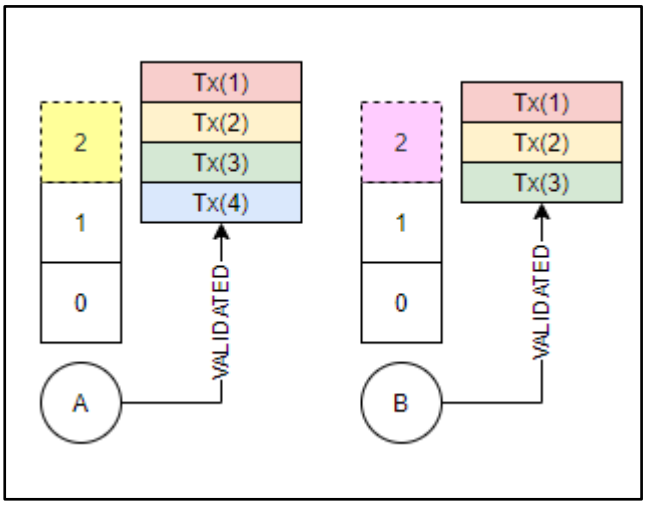
[82] Antonopoulos (n 2) ch 10.
[83] 'Block headers' will not be addressed by this paper. See Antonopoulos (n 2) ch 10.
[84] The concept of a 'difficulty threshold' will not be addressed by this paper. See Antonopoulos (n 2) ch 10.
[85] 'Solo Mining', *Mining* (Documentation, 2021) <https://developer.bitcoin.org/devguide/mining.html>.
[86] Nakamoto (n 3) 4.
[87] Antonopoulos (n 2) ch 10.
[88] Ibid.
[89] Nakamoto (n 3) 4.
[90] See Walker, Greg, 'Chain Reorganisation', *Learn me a bitcoin* (Web Page, 6 September 2019) <https://learnmeabitcoin.com/technical/chain-reorganisation>; Greg Walker, 'Longest Chain', *Learn me a bitcoin* (Web Page, 5 September 2019) <https://learnmeabitcoin.com/technical/longest-chain>; 'Bitcoin Core 0.11: Data Storage' (Documentation, 17 August 2021) <https://en.bitcoin.it/wiki/Bitcoin_Core_0.11_(ch_2):_Data_Storage>; 'Bitcoin Core 0.11: The Blockchain' (Documentation, 17 August 2021) <https://en.bitcoin.it/wiki/Bitcoin_Core_0.11_(ch_6):_The_Blockchain>; GR0KCHAIN, 'Understanding the data behind Bitcoin Core', *Bitcoin Developer Network* (Web Page, 25 September 2021) <https://bitcoindev.network/understanding-the-data/>; See also Antonopoulos (n 2) ch 10.
[91] Antonopoulos (n 2) ch 10.

Diagram 6 – Receiving different sets of transactions



Each transaction is validated by the full nodes that receive them. Assuming that Node A immediately commences mining rather than gossiping Tx(4), Node A will attempt to create a block containing Tx(1), Tx(2), Tx(3) and Tx(4), as those are the transactions it has received. Conversely, Node B attempts to create a block containing Tx(1), Tx(2) and Tx(3). This is shown in Diagram 7.

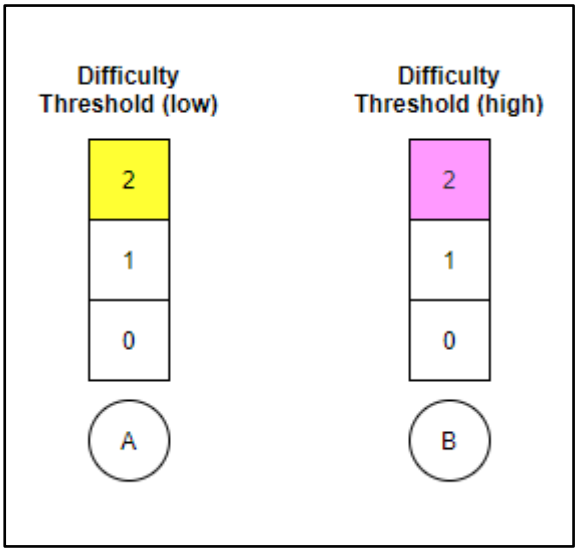
Diagram 7 – Validating different sets of transactions



Node A creates Block 2, which has a low difficulty threshold following the mining process. Node B also creates its own version of Block 2, which has a high difficulty threshold following the mining process. This is shown in Diagram 8. It is worth noting that the respective difficulty thresholds are not the result of the number of transactions contained in each block.[92]

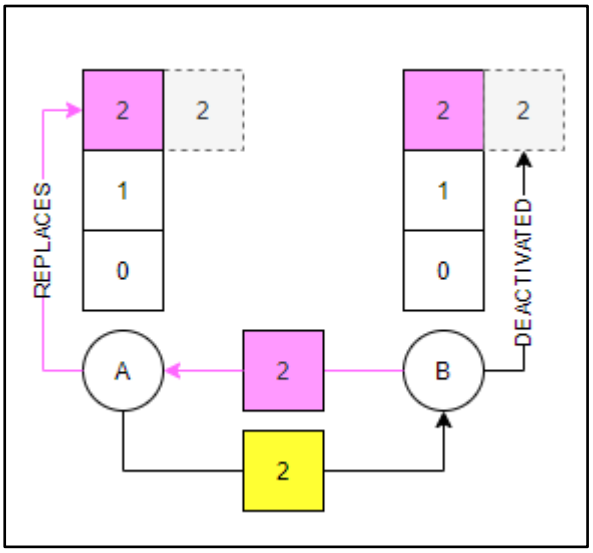
[92] The concept of a 'difficulty threshold' will not be addressed by this paper. See generally Antonopoulos (n 2) ch 10.

Diagram 8 – Two versions of Block 2 are created



Each node transmits its version of Block 2 to the other node for validation. Node B recognises that Node A's Block 2 continues the blockchain from Block 1. However, as Node B's Block 2 occupies this location, Node B compares the cumulative difficulty threshold from Block 0 to each version of Block 2. It determines that its version of Block 2 forms part of the main chain and deactivates Node A's Block 2. Similarly, Node A undertakes the same process but concludes that Node B's Block 2 forms part of the main chain. Consequently, it deactivates its own Block 2 in preference to Node B's Block 2. This is shown in Diagram 9.

Diagram 9 – Node A undergoes a chain reorganisation



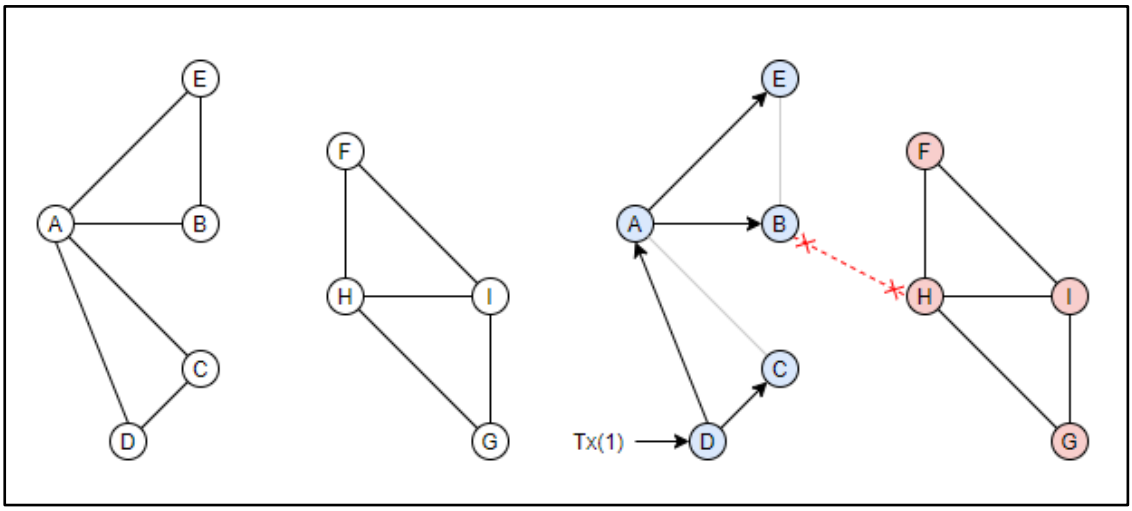
As Node A's Block 2 contained Tx(4), which does not appear in Node B's Block 2, Tx(4) will return to Node A's memory pool to be processed into a new block. While Node A and Node B did momentarily diverge in the blocks on their Bitcoin blockchains, this discrepancy (or 'fork') was resolved through chain reorganisation. The concept of a 'fork' will be explored next.

F *Forks cannot occur on a full node's blockchain*

Each full node maintains its own, discrete Bitcoin blockchain. By gossiping transactions and blocks with peer nodes, in conjunction with a full node's ability to reorganise its main chain, full nodes develop their blockchains and indirectly reach consensus with peer nodes on what forms a 'notional' main chain. As demonstrated by Diagram 8 above, there are instances where more than one full node may 'discover' a new block simultaneously. This means that full nodes, at various times, may possess a version of the Bitcoin blockchain that is not identical to other full nodes.[93] This type of comparison is referred to as a blockchain 'fork'.

It is never guaranteed that transactions or blocks will be transmitted to and adopted by every full node with a Bitcoin blockchain. This is because the consensus rules governing each full node may vary or some other factor may prevent the full nodes from accepting or transmitting information. For example, some full nodes may be operating on an upgraded version of the consensus rules which are incompatible with previous versions of those rules. There may also be technological issues that prevent a group of full nodes from contacting another group of full nodes. This is shown in Diagram 10 below.

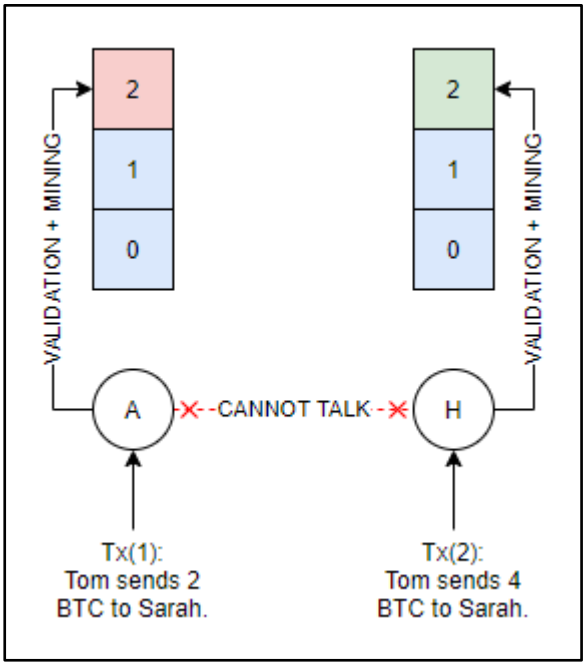
Diagram 10 – How a transaction may not propagate to all full nodes



In this example, all the full nodes possess a Bitcoin blockchain that is identical up to a set block. Due to an extreme weather event, Nodes A to E have no connection with Nodes F to I. If Tx(1) was transmitted to Node D (or any full node in the former group of full nodes), the transaction would not be transmitted to Node H (or any full node in the latter group of full nodes). This means that the two groups of full nodes could develop divergent Bitcoin blockchains despite possessing identical consensus rules. Consequently, a person who controlled a UTXO that was replicated by both groups of full nodes could redeem their UTXO twice. This is shown in Diagram 11 below.

[93] Antonopoulos (n 2) ch10.

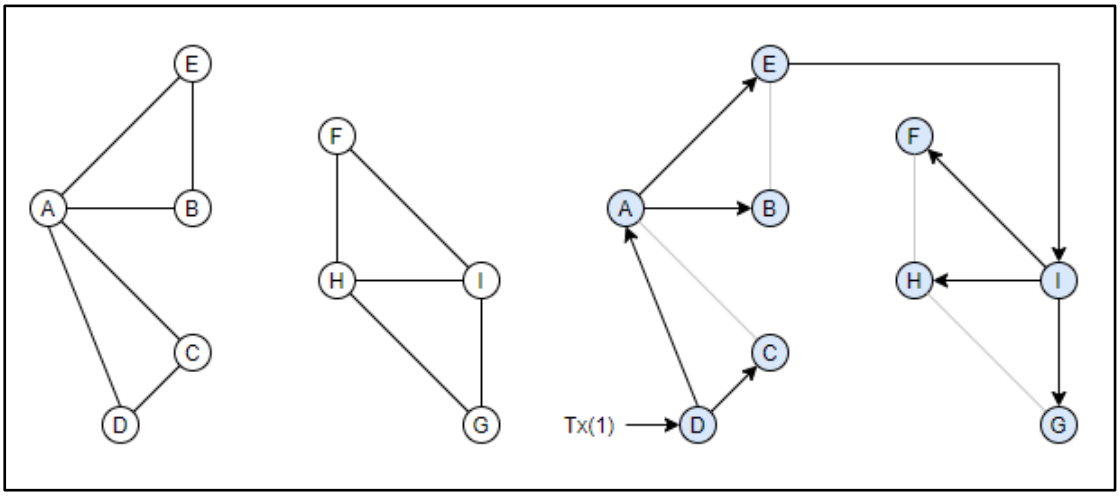
Diagram 11 – Double spending on separate full nodes



Tom controls a UTXO with BTC5. This UTXO is present on the Bitcoin blockchains maintained by Node A and Node H. Node A becomes unable to communicate with Node H and vice versa. Tom creates 'Tx(1)' to pay BTC2 to Sarah and transmits this to Node A. Later, Tom requests an update of the bitcoin associated with his private/public keypairs from Node H. Node H highlights that his UTXO of BTC5 remains unspent. Tom creates 'Tx(2)' to pay BTC4 to Sarah and transmits this to Node H. As highlighted in Diagram 11, each full node validates the separate transaction and seeks to add it on to their respective blockchains. Consequently, Sarah has control over two UTXOs: one on Node A (BTC2) and the other on Node H (BTC4).

Where the connection between the two groups of full nodes is re-established, the information exchange will recommence between both groups. This is shown in Diagram 12, where Node E re-establishes a connection with Node I.

Diagram 12 – Where groups of full nodes are reconnected



The full nodes share and identify those transactions and blocks that do not appear on their own Bitcoin blockchains before applying the concepts of chain reorganisation to determine which blocks form part of their respective main chains. This process may involve a full node abandoning one or more blocks on their own Bitcoin blockchain in favour of those blocks from a peer node.

Some forks are never resolved. For example, full nodes may adopt consensus rules that do not recognise the blocks from full nodes operating a different set of consensus rules. Like Diagram 11, one group of full nodes can develop blockchains that are not identical to the blockchains of other group of full nodes. Where the full nodes continue operating on different consensus rules, a distinct cryptocurrency may be recognised for commercial and practical purposes.[94]

[94] On 1 August 2017, a group of full nodes on the Bitcoin blockchain implemented a software upgrade that caused a fork. Blocks formed using the upgraded software were not recognised by un-upgraded full nodes. Ultimately, the led to the recognition of 'Bitcoin Cash' as a separate blockchain to Bitcoin: Joseph Young, 'Bitcoin Investors Should Not Fear August 1 Chain Split', *CoinTelegraph* (Article, 26 July 2017) <https://cointelegraph.com/news/bitcoin-investors-should-not-fear-august-1-chain-split>.

III BITCOIN: IS IT PROPERTY?

> *Much of our false thinking about property stems from the residual perception that 'property' is itself a thing or resource rather than a legally endorsed concentration of power over things and resources*.[95]
>
> **Gleeson CJ, Gaudron, Kirby and Hayne JJ, 1999**

A *Overview*

Starke J in *Minister of State for the Army v Dalziell* (1944)[96] explained that the ordinary meaning of 'property' refers to an expansive category of 'things'. Property law regulates the rights that a person has with respect to these things, the degree to which a person can interfere with another person's things (if at all), and the priority of rights where there are competing claims of ownership over a thing.[97] Dr Robert Chambers, author of *An Introduction to Property Law in Australia*,[98] also highlights that it is broadly accepted that individuals have property rights in most tangible objects, such as domesticated animals, vehicles and clothing; and Australian law recognises that individuals have property rights in intangible things, such as inventions and shares in a company.[99] Property rights and proprietary interests are synonymous expressions which refer to the legal relationships entities have with things.[100]

When faced with emerging technologies, the first question that must be asked is 'whether the thing can be an object of property rights'.[101]This Chapter examines precedential Anglo-Australian cases regarding what 'things' have amounted to a proprietary interest for Australian legal purposes. By applying the key indicia distilled from these cases, the Chapter concludes that unspent transaction outputs ('UTXOs') on most full nodes operating on the Bitcoin network amount to discrete proprietary interests. Following this analysis, the Chapter summarises the impact this view has on the Australian income tax treatment of Bitcoin.

B *Examples of property*

1 *Commercial value and recognition by commerce*

Potter v The Commissioner of Inland Revenue (1854)[102] (the Potter case) queried whether stamp

---

[95] *Yanner v Eaton* [1999] HCA 53, [18] (Gleeson CJ, Gaudron, Kirby and Hayne JJ), citing Kevin Gray, 'Property in Thin Air' (1991) 50 *Cambridge Law Journal* 252, 299.
[96] (1944) 68 CLR 261.
[97] Robert Chambers, *An Introduction to Property Law in Australia* (Thomson Reuters, 4th ed, 2018) 3; See Lyria Bennett Moses, 'The Applicability of Property Law in New Contexts: From Cells to Cyberspace' (2008) 30 *Sydney Law Review* 639, 639. But see Kyriaco Nikias and Paul Babie, 'Legislators, judges, and the content of property: Reflections on *Hocking v Director-General, National Archives of Australia*' (2020) 28 *Australian Property Law Journal* 195, 207.
[98] Chambers (n 97).
[99] Ibid 3.
[100] *Yanner v Eaton* [1999] HCA 53, [17] (Gleeson CJ, Gaudron, Kirby and Hayne JJ); Cf Lyria Bennett Moses, 'The Applicability of Property Law in New Contexts: From Cells to Cyberspace' (2008) 30 *Sydney Law Review* 639, 639.
[101] Lyria Bennett Moses, 'The Applicability of Property Law in New Contexts: From Cells to Cyberspace' (2008) 30 *Sydney Law Review* 639, 639.
[102] (1854) 156 ER 392 ('*Potter*').

duty was chargeable on a deed that assigned the goodwill of a business on the basis that the assignment was a conveyance of 'property'. Relevantly here, Pollock CB broadly explained that 'property' referred to 'that which belonged to another person exclusive of others, and which could be the subject of bargain and sale to another'.[103]

With respect to goodwill, his Honour highlighted how a frequented business will often sell for more than a less reputable business due to the rapport generated by that business with its regular patrons. The business's goodwill had no connection with the land on which it operated and, despite being intangible, conferred the benefits that come with the connections and reputation developed by the business over time.[104] Pollock CB concluded that goodwill was property as it was 'a valuable thing belonging' to the owner, could be sold 'to another for pecuniary consideration'.[105] The Potter case was approved by the High Court of Australia in *Commissioner of Taxation v Murry* [1998].[106]

In *Uniting Church in Australia Property Trust (NSW) v Immer (No 145) Pty Ltd* (1991) ('the Immer case'),[107] the Court of Appeal considered the extent to which a specific right conveyed by an agreement over 'air space' amounted to a proprietary right. The nature of 'air space' was a novel issue before the courts and was taken to mean a right to 'build higher than would normally be permitted by relevant council codes by acquiring from the owner of another building bonus floor site ratios'. Specifically, the 'air space' was the assignment of the right to prevent another person from building higher than a certain limit by an adjacent building owner.

In his concise judgment, Meagher JA saw no reason why these rights did not amount to a proprietary right like goodwill, patents or shares of a company.[108] His Honour stated that '[t]hey are transferable, and I assume transmissible', and 'they are of large commercial value'.[109] These factors were further considered in *Halwood Corporation Ltd v Chief Commissioner of Stamp Duties* (1992) ('the Halwood case'),[110] which is discussed below.

2 In personam *rights and fluctuating obligations*

In 1961, a woman deserted by her husband applied for and obtained a decree of judicial separation which required him to provide rent-free accommodation to her. At the time, the woman had been living in the matrimonial home acquired by the husband, subject to a charge in favour of National Provincial Bank Ltd. After defaulting on his obligations, the bank attempted to exercise its power to sell the home; however, the woman asserted that her right of accommodation was an 'overriding interest'. Consequently, the House of Lords in *National Provincial Bank Ltd v Ainsworth* [1965][111] ('the Ainsworth case') considered whether the wife possessed a proprietary right took priority over the bank's charge over the property.

---

[103] Ibid 396 (Pollock CB).
[104] Ibid.
[105] Ibid.
[106] [1998] HCA 42, [23] (Gaudron, McHugh, Gummow and Hayne JJ) ('*Murray*'); See also *Box v Commissioner of Taxation* (1952) 86 CLR 387.
[107] (1991) 24 NSWLR 510 ('*Immer*').
[108] Ibid 511.
[109] Ibid.
[110] (1992) 33 NSWLR 395 ('*Halwood*').
[111] [1965] AC 1175 ('*Ainsworth*').

In his judgment, Lord Wilberforce clarified that:

> Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability.[112]

Relevantly here, the wife's right to be provided accommodation arose from common law equity. Historically, courts recognised that the extent of a deserted wife's rights against her husband are based on the circumstances of the spouses.[113] They cannot be assumed by third parties because the rights are only enforceable by the wife against the husband.[114] Further, the nature of those rights could be reviewed at any time to reflect changing personal circumstances,[115] and the right of accommodation did not extend to occupy a particular property.[116] This meant the rights lacked permanence and stability because they fluctuated as the spouses' circumstances changed, and they were not capable of being defined. Consequently, the House of Lords held that this did not amount to a proprietary right.[117]

This approach was approved by Mason J in *Re Toohey; Ex parte Meneling Station Pty Ltd* (1982) (the Re Toohey case),[118] which is discussed next.

3 *Control and exclusivity*

The High Court of Australia in the Re Toohey case considered the extent to which grazing licences granted pursuant to the *Crown Lands Act 1931* (NT) were rights of a 'proprietary nature'.

Mason J, referencing Lord Wilberforce's description of property in the Ainsworth case, concluded that the grazing licences did not amount to a proprietary interest on the basis that the licences lacked permanency and were not capable of being assigned or transferred to another.[119] Specifically, his Honour highlighted that:

(a) Under the *Crown Land Regulations 1931* (Cth), the Minister could cancel the grazing licence without reason, provided that three months' written notice was given to the licencee.[120] This meant that the licencee had little to no control over the existence of the grazing licence into the future because the Minister could, in his absolute power under the regulations, terminate the licence.[121] Consequently, the licencee had no guarantee that its grazing licence was permanent nor stable beyond three months at any given time.

(b) The grazing licences could not be assigned, and licencees were required to obtain

[112] Ibid 1247—1248.
[113] Ibid 1247.
[114] *Ainsworth* (n 111) 1245.
[115] *Ainsworth* (n 111) 1247.
[116] Ibid.
[117] *Ainsworth* (n 111) 1248.
[118] (1982) 44 ALR 63, 74 ('*Re Toohey*'); See *Commonwealth of Australia v WMC Resources Ltd* [1998] HCA 8, 99 (Kirby J).
[119] *Re Toohey* (n 118) 74—75.
[120] *Re Toohey* (n 118) 74.
[121] Ibid.

> permission before any improvements could be made to the land to which their grazing licence related.[122] These characteristics reflect the notion that the licences were intended to be a form of personal right and did not convey a right to exclusive possession of the underlying land.[123] In relation to the inalienable nature of the licence, Mason J clarified that '[a]ssignability is not in all circumstances an essential characteristic of a right of property' but 'a proprietary right must be "capable in its nature of assumption by third parties".[124]

In *Yanner v Eaton* [1999] ('the Yanner case'),[125] an appellant harpooned two juvenile estuarine crocodiles and used the remains for domestic purposes under the assumption that the activity was an exercise of his rights under the *Native Title Act 1993* (Cth). Relevantly here, the High Court considered the extent that the Crown had 'property' in fauna pursuant to section 7 the then *Fauna Conservation Act 1974* (Qld) ('the Fauna Act').

Gleeson CJ, Gaudron, Kirby and Hayne JJ highlighted that 'property' has a dual meaning, referring to a thing belonging to another or the legal relationship with that thing.[126] Both meanings are comprehensive in scope and extend to tangible and intangible things. This includes a 'range of legal and equitable estates and interests' which may 'exist concurrently and be held by different parties'.[127]

With respect to crocodiles, their Honours discussed the history of the common law's approach to the limited proprietary rights exercisable in relation to wild animals. Specifically, they stated:

> …An action for trespass or conversion would lie against a person taking wild animals that had been tamed…, and a land owner had the exclusive right to hunt, take and kill wild animals on his own land. Otherwise no person had property in a wild animal.[128]

This demonstrates that an indicium of what makes a thing property relates to the degree of control exercisable over that thing. For the case of wild animals, they can become property through domestication as the animal is presumed to respond to the commands and control of a human. More broadly, their Honours also highlight that property refers to 'a legally endorsed concentration of power over things and resources' and 'consists primarily in control over access' to that thing.[129] This allows the owner to have, enjoy and dispose of the subject matter.[130] As the fauna described in the Fauna Act was always intended to refer to subject matter outside the possession or control of humans,[131] their Honours held that the Crown did not possess full beneficial, or absolute, ownership of that fauna.[132] Instead, the Fauna Act restricted the Crown to granting separate licences to entities for the 'taking or keeping of fauna'.[133]

---

[122] Ibid.
[123] Ibid.
[124] Ibid; See also *Commissioner of Stamp Duties (NSW) v Yeend* (1929) 43 CLR 235, 245 (Isaacs J); *Australian Capital Television Pty Ltd v Commonwealth (No 2)* (1992) 108 ALR 577, 615 (Brennan J).
[125] [1999] HCA 53 ('*Yanner*').
[126] *Yanner* (n 125) [17] (Gleeson CJ, Gaudron, Kirby and Hayne JJ).
[127] *Yanner* (n 125) [85] (Gummow J).
[128] *Yanner* (n 125) [24].
[129] *Yanner* (n 125) [17]—[18] (Gleeson CJ, Gaudron, Kirby and Hayne JJ).
[130] *Yanner* (n 125) [25] (Gleeson CJ, Gaudron, Kirby and Hayne JJ).
[131] Ibid [25] (Gleeson CJ, Gaudron, Kirby and Hayne JJ).
[132] *Yanner* (n 125) [30] (Gleeson CJ, Gaudron, Kirby and Hayne JJ).
[133] Ibid.

Gummow J also highlighted that protection afforded by the law can also mean that a thing that is not otherwise property may amount to a property because of the effect of the protection.[134] His Honour demonstrates how confidential information may not otherwise amount to property without the protection afforded to it under the equitable doctrine of confidential information.[135] In fact, it is by virtue of the effect of that protection that confidential information takes on a proprietary character.[136]

4 *Floor space and the notion of permanency*

Following the decision in the Immer case, Loveday J in the Halwood case determined whether 'a right… to have a development application considered by the city council taking into account the existence of … transferable floor space' amounted to property for the purposes of the *Stamp Duties Act 1920* (NSW).[137] His Honour highlighted that the opportunity for the existence of new proprietary rights was not closed.[138] New proprietary rights can be introduced by legislation, and courts have historically recognised new categories of proprietary rights 'created' by commerce.[139]

After citing Lord Wilberforce's test of property in the Ainsworth case, his Honour rejected the appellant's submission that the right failed the permanence and stability test on the basis that there was no guarantee that the city council would reach a decision favourable to the transferee of the right.[140] Rather:

> The fact that there may be some element of uncertainty as to the degree of enjoyment of transferable floor space does not mean that it is not a valuable right. Goodwill was recognised as a proprietary right even when it meant nothing more than the probability that customers would resort to the old place of business. Even in the modern wider view of "goodwill" the enjoyment of transferred goodwill is as much an "expectation" as transferable floor space.[141]

Like goodwill, commerce recognised the speculative value that attached to a transferee who was registered on the council's register of transferable floor space. This was on the basis that such a transferee would have an exclusive entitlement to that floor space if approved by the council. Further, this right to have an application considered by the council would not be possessed by another entity without that floor space. Loveday J therefore held that, as commerce regarded the right as a proprietary right, the 'courts should do likewise'.[142]

---

[134] *Yanner* (n 125) [85] (Gummow J).
[135] Ibid.
[136] Ibid.
[137] *Halwood* (n 110) 403 (Loveday J).
[138] *Halwood* (n 110) 402 (Loveday J).
[139] *Halwood* (n 110) 402 (Loveday J), citing *Keppell v Bailey* (1834) 2 My & K 517, 402 (per Lord Brougham). See *Colbeam Palmer Ltd v Stock Affiliates Pty Ltd* (1968) 122 CLR 255, [34] (per Windeyer J) in relation to the court's recognition of trade marks prior to their protection by legislation.
[140] *Halwood* (n 110) 402 (Loveday J), citing *Ainsworth* (n 111) 1247—1248 (Lord Wilberforce).
[141] *Halwood* (n 110) 402 (Loveday J); See also *Potter v The Commissioner of Inland Revenue* (1854) 156 ER 392; *Box v Commissioner of Taxation* (1952) 86 CLR 387.
[142] *Halwood* (n 110) 402 (Loveday J).

In *Federal Commissioner of Taxation v United Aircraft Corporation* [1943] ('the UAC case'),[143] Latham CJ addressed whether the ongoing exchange of information between two parties for a set period amounted to a transfer of 'property'. Specifically, the information transferred was not the subject of a patent, copyright licence, nor was it a trade secret sufficient for protection under existing legal frameworks (eg, patent law, copyright law, or confidential information). Instead, Latham CJ highlighted that the information itself was not property for the following reasons:

(a) Anyone can acquire knowledge freely even though that knowledge may be known to another entity subject to an agreement to keep that knowledge secret.[144]

(b) Anyone can use knowledge in any way they please, provided they are not subject to contractual obligations, patent laws or copyright laws.[145]

(c) While knowledge on a subject matter would be valuable where there is a monopoly, this assumes that the knowledge would remain a secret.[146] In this instance, the transferor of the information retained the knowledge in their mind after imparting it to another.[147]

Naturally, the more times the information is 'transferred', the more well-known that information becomes and, by extension, the less valuable it is. This judgment reflects notions that, in order for a thing to amount to property, the thing must be valuable, capable of being transferred rather than duplicated in the mind or control of another (ie, the person relinquishes control over the thing), and that the owner can effectively exclude others from acquiring the thing in some other manner unrelated to the owner.

C *Indicia of property*

From the cases outlined above, several factors are considered when determining whether a thing amounts to a proprietary right. These factors include whether:

(a) It is definable;[148]
(b) It is identifiable by third parties;[149]
(c) It is transferrable or capable of assumption by third parties;[150]
(d) It can be controlled, or others can be excluded from controlling it;[151]
(e) It has commercial value;[152]

[143] [1943] HCA 50 ('*UAC*').
[144] *UAC* (n 143) [535] (per Latham CJ).
[145] Ibid.
[146] Ibid.
[147] *UAC* (n 143) [534] (per Latham CJ).
[148] See *Ainsworth* (n 111) 1247—1248.
[149] Ibid.
[150] See *Potter* (n 102) 396; *Immer* (n 107) 511. Cf *Re Toohey* (n 118) 74.
[151] See *Potter* (n 102) 396; *Murry* (n 106) [23]; *Ainsworth* (n 111) 1247—1248; *Box v Commissioner of Taxation* (1952) 86 CLR 387; *Yanner* (n 125) [17]—[18]. Cf *Re Toohey* (n 118) 74.
[152] See *Potter* (n 102) 396; *Halwood* (n 110) 402 (Loveday J); *Immer* (n 107) 511.

(f) It has some degree of stability or permanence;[153] and,
(g) Existing common law principles afford the thing 'property-like' rights.[154]

As historical cases have selected which of these factors apply (if any), it is likely that no single factor is determinative nor is it necessary for each factor to be present. However, greater emphasis appears to be placed on the ability of an entity to control or exclude others from the thing.[155] It is a precursor characteristic from which other factors likely arise. For example, control and the ability to exclude others from a thing can generate scarcity for that thing. Restricted access to the thing may, respectively, increase its speculative value.

D *Application to Bitcoin concepts*

This dissertation will now apply each factor outlined above to Bitcoin.

1 *Definable*

The Oxford English Dictionary states that 'definable' means 'capable of being defined'.[156] To 'define' a thing means to state the essential characteristics of that thing and identify its boundaries.[157] Therefore, this dissertation will highlight how an individual's right to access or redeem an unspent transaction output ('UTXO') on a full node's Bitcoin blockchain is the relevant 'thing' to be considered. For this dissertation, 'redeem' means to recover or claim the value associated with a UTXO by presenting the corresponding private/public keypair in a valid transaction.[158]

Firstly, there are no physical 'bitcoin' that are physically delivered from person to person. Even at a digital level, there is no distinguishable piece of data that identifies or 'earmarks' a particular bitcoin.[159] This is because a UTXO is an encoded alphanumeric string containing details such as output information, which specifies the value (in bitcoin) to be associated with a particular private/public keypair. As discussed in Chapter 2, one must fully redeem a UTXO as an input for a new transaction in order to use the bitcoin associated with their UTXO. This generates new UTXOs whose value is equal to the inputs of the transaction and ensures that the chain of ownership can be tracked through each transaction.[160] Comparatively, Australian regulators and authors mistakenly claim that bitcoin are 'held' in Bitcoin wallets.[161]

Secondly, an individual's right to redeem a UTXO associated with their private/public keypair is typically present on every version of the Bitcoin blockchain. Chapter 2 highlights that there

[153] See *Ainsworth* (n 111) 1247—1248; *Re Toohey* (n 118) 74—75; *Halwood* (n 110) 402 (Loveday J).
[154] See *Yanner v Eaton* [1999] HCA 53; *Halwood* (n 110) 402 (Loveday J), citing *Keppell v Bailey* (1834) 2 My & K 517, 402 (per Lord Brougham). Cf *UAC* (n 143) [535] (per Latham CJ).
[155] See Kyriaco Nikias and Paul Babie, 'Legislators, judges, and the content of property: Reflections on *Hocking v Director-General, National Archives of Australia*' (2020) 28 *Australian Property Law Journal* 195, 213.
[156] *Oxford English Dictionary* (online at 11 September 2021) 'definable'.
[157] *Oxford English Dictionary* (online at 11 September 2021) 'define' (def 3, 6).
[158] *Macquarie Dictionary* (online at 13 October 2021) 'redeem' (def 3, 5a).
[159] See Antonopoulos (n 2) ch 6.
[160] See David Fox, 'Cryptocurrencies in the Common Law of Property' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019) [6.18]—[6.19].
[161] See paragraph 9 of Taxation Determination TD 2014/26 *Income tax: is bitcoin a 'CGT asset' for the purposes of subsection 108-5(1) of the Income Tax Assessment Act 1997?*; Reuben Grinberg, 'Bitcoin: An Innovative Alternative Digital Currency' (2012) 4 *Hastings Science & Technology Law Journal* 159, 163; Sarah A Hinchcliffe, 'Bitcoins – a bit of this and a bit of that' (2016) 19(1) *Internet Law Bulletin* 259.

is no central version of the Bitcoin blockchain. Each full node maintains an independent (although typically identical) version of the Bitcoin blockchain. Consequently, for each full node that possesses a record of a particular UTXO, the owner of the private/public keypair will possess the right to access, redeem and use that UTXO. This means that if there are 11,000 full nodes that possess the record of that UTXO, the holder of the private/public keypair will possess 11,000 rights to redeem the UTXO even though they may need only authorise a single transaction to use a UTXO once. This is explored in Part 2 below.

International case law on bitcoin as property, such as *Ruscoe v Cryptopia Limited (in liq)* [2020] ('the Ruscoe case'),[162] disregards this critical fact. Instead, Gendall J in the Ruscoe case treats the Bitcoin blockchain like a centralised source of truth, with copies of this 'ultimate' ledger replicated across full nodes. For the reasons outlined throughout this Chapter, this dissertation respectfully disagrees with that proposition.

Finally, as this test has established that the 'things' to be considered are UTXOs and not bitcoin, the remainder of this Chapter will apply the common law tests to UTXOs.

2 *Identifiable by third parties*

The Oxford English Dictionary states that 'identifiable' means 'able to be identified'.[163] As 'identify' possesses several meanings, this dissertation regards 'identifiable' as a reference to the capability of third parties in locating, recognising, and distinguishing a thing from other things.[164]

As highlighted in Chapter 2, each full node possesses a separate version of the Bitcoin blockchain despite these versions being almost (if not completely) identical with peer nodes. A full node can run functions to identify all UTXOs relating to a set of known private/public keypairs. Similarly, third parties can request all UTXOs associated with known bitcoin addresses. Consequently, third parties can readily identify potential rights to redeem UTXOs even where the actual identity of the owner is not known.[165]

Gendall J in the Ruscoe case conversely suggests that 'identifiable' refers to the idea that the owner of a thing is 'capable of being recognised as such by third parties', demonstrated by their ability to exclude others from the thing.[166] These concepts are explored next.

3 *Transferable, control and exclusivity*

Transferability, control, and exclusivity are related concepts. A thing is 'transferable' if it is 'capable of being transferred or legally made over to another';[167] a person 'controls' a thing where they possess the power or can act to control, regulate, dominate, or command that

[162] [2020] NZHC 728, [106] (Gendall J) ('*Ruscoe*').
[163] *Oxford English Dictionary* (online at 12 September 2021) 'identifiable'.
[164] *Oxford English Dictionary* (online at 12 September 2021) 'identify' (def 6).
[165] For an example of the information that can be viewed on a full node's blockchain, see Blockchain.com, 'Bitcoin Explorer' (Web Page, 23 September 2021) <https://www.blockchain.com/btc/blocks?page=1>. This website displays the information received by a full node operated by Blockchain Luxembourg S.A.
[166] *Ruscoe* (n 162) [109]—[110] (Gendall J).
[167] *Oxford English Dictionary* (online at 12 September 2021) 'transferable'.

thing;[168] and, excluding others from a thing necessarily requires that the person has the power to preclude others from using the thing.[169] Lyria Moses states that the 'excludability test suggests that something can only be property if it is conceptually, physically or legally possible to prevent others from using that thing.'[170]

There are several degrees of control that are relevant for UTXOs.

Firstly, a person can control a UTXO if they know (or possess the means to know or access)[171] the private/public keypair that is required to redeem that UTXO. This is because the UTXO can only be redeemed if the individual presents:

(a) The public key that matches the hash ('fingerprint') of the UTXO, and
(b) A signature from the private key associated with the public key used in (a).[172]

The private key is an alphanumeric number that is generated at random. This is kept secret from third parties. Using a cryptographic function, the public key is derived from the private key. From the public key, and using a different cryptographic function, a bitcoin address can be generated. Importantly, it is computationally difficult (if not near improbable) to reverse these processes and identify from a bitcoin address or public key, the private key. Some authors suggest that the private/public keypair is like a PIN to a bank account,[173] which is not correct. The private/public keypair is used as a digital signature to prevent the unauthorised access, redemption and use of a UTXO. It is this mechanism that allows owners of UTXOs to preclude others, including full nodes, from using their UTXOs without authorisation.

When the owner authorises the redemption and use of the UTXO in a transaction, the UTXO becomes unspendable and functionless.[174] This is because the full node recognises that the UTXO has been 'spent' in the transaction. After this transaction, new UTXOs are associated with the same or different private/public keypairs. This is the mechanism through which value is transferred through the Bitcoin blockchain.[175] However, imparting the knowledge of a private/public keypair to another can also change or dilute the control of a UTXO. No transaction will appear on any Bitcoin blockchain because the UTXO has not been redeemed, but a change in the control of the UTXO nonetheless occurs because another person now possesses the means to redeem that UTXO.[176] Similarly, this method also enables an owner to transfer or dilute their control over the UTXO.

---

[168] *Macquarie Dictionary* (online at 23 September 2021) 'control' (def 1, 4).
[169] *Oxford English Dictionary* (online at 23 September 2021) 'exclude' (def 2b, 3a).
[170] Lyria Bennett Moses, 'The Applicability of Property Law in New Contexts: From Cells to Cyberspace' (2008) 30 *Sydney Law Review* 639, 651.
[171] For example, the person can access a Bitcoin wallet, which stores the relevant private/public keypair.
[172] Bitcoin Project, 'Unlocking a P2PKH Output for Spending', *Developer Guides: Transactions* (Documentation, 18 August 2021) <https://developer.bitcoin.org/devguide/transactions.html>.
[173] See Paul Babie et al, 'Cryptocurrency as property: *Ruscoe v Cryptopia Ltd (in liq)* [2020] NZHC 728'(2020) 28 *Australian Property Law Journal* 106, 114, discussing *Ruscoe v Cryptopia Ltd (in liq)* [2020] NZHC 728.
[174] While the UTXO may become functionless, it can still be used for evidentiary purposes, such as supporting a claim of ownership or redemption: UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smart contracts* (Legal Statement, November 2019) [43], [45]. This Legal Statement was drafted by four barristers: Lawrence Akka QC, David Quest QC, Matthew Lavy, and Sam Goodman.
[175] See David Fox, 'Cryptocurrencies in the Common Law of Property' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019) [6.18]—[6.19].
[176] This is also true where a person provides access to software that itself provides access to a person's private/public keypair. For example, sharing access to a Bitcoin wallet allows the user to control connected private/public keypairs.

Secondly, even though a person can attempt to exercise the right to redeem UTXOs, the transaction must be accepted as valid and be maintained by a full node into the future. This factor is completely disregarded in existing literature.[177] A person cannot redeem a UTXO if they construct an invalid transaction or their UTXO is not recognised by that full node. It is also worth noting that consensus rules are applied automatically and impartially by full nodes. Broadly, this means that a person may still have a proprietary interest in a UTXO even though anyone operating a full node could manually reject the redemption of the UTXO at any time.[178] Where a full node routinely rejects or ignores transactions, it cannot be said that the person exercised any control over UTXOs on that full node's Bitcoin blockchain.[179]

While a person's right to access, redeem and use a UTXO extends to each UTXO recognised by a full node, practically, a person need only exercise their right once by constructing a valid transaction for a connected full node. This dissertation asserts that the holder implicitly authorises the recipient full node to re-transmit the transaction (and therefore the exercise of the right) on the holder's behalf to peer nodes.

Therefore, a person's ability to control bitcoin associated with their UTXOs is restricted to those full nodes that they can communicate with directly (or operate themselves) or indirectly, through the peer nodes with which their full node communicates and so on.

4 *Commercial value*

There is no doubt that bitcoin are valuable and recognised as property by commercial parties. Price-tracking websites, like 'CoinMarketCap', estimate that there are approximately BTC18,850,000 currently in circulation on the Bitcoin blockchain, with a market capitalisation of roughly AUD1.5 trillion.[180]

The concern, however, is whether the right recognised by commercial parties must be the same right as outlined by this dissertation. Existing literature, which reflects the general commercial understanding of bitcoin, disregards the duplication of UTXOs across full nodes and instead treats this consensus as evidence of one, universal blockchain.[181] There is an assumption that an individual's right to redeem this notional UTXO, which appears on the 'universal' blockchain, is the right that is attributed value.

This issue is reminiscent of the 'single publication rule', historically raised in relation to the tort of defamation. As stated by Gaudron J, the single publication rule is a legal fiction that deems widely disseminated information as forming 'a single communication regardless of the number of people to whom…it is circulated.'[182] Gleeson CJ, McHugh, Gummow and Hayne JJ

[177] See UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smart contracts* (Legal Statement, November 2019) [85].
[178] Cf *Re Toohey* (n 118) 74.
[179] See *Re Toohey* (n 118) 74.
[180] Ibid. See also Taxation Determination TD 2014/26 *Income tax: is bitcoin a 'CGT asset' for the purposes of subsection 108-5(1) of the Income Tax Assessment Act 1997?* [10].
[181] See Terence Wong, 'Bitcoin deconstructed: Part 1 – Concepts and signposts' (2014) 30(4) *Australian Banking & Finance Law Bulletin* 70; UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smart contracts* (Legal Statement, November 2019) [85].
[182] *Dow Jones & Company Inc v Gutnik* [2002] HCA 56, [57] (Gaudron J) ('*Dow Jones*').

further highlight that:

> …those who post information on the World Wide Web do so knowing that the information they make available is available to all and sundry without any geographic restriction.[183]

Focusing on the fact that the publication arose from a singular event ignores the function and reach of the Internet, which made the simultaneous and widespread dissemination of information through electronic means easier.[184]

Similarly, the notion of a universal Bitcoin blockchain is a legal fiction. One of two scenarios arise when an individual redeems a UTXO. Where parties are transacting through the same full node, the consideration provided in exchange for the redemption of the UTXO is directly related to the UTXO on that full node. One view is that commercial parties recognises only this UTXO as a valuable 'thing', and duplicate UTXOs are disregarded. Alternatively, commercial parties may apportion the consideration across all UTXOs.

The second scenario arises where the parties transact through different full nodes. For example, Person A redeems a UTXO on Node A in exchange for AUD10 from Person B. Person B is not connected to Node A, as Person B solely uses Node B. Node A validates the transaction and relays it to Node B. Node B accepts the transaction as valid, allowing Person B to access, redeem, and use the new UTXO in subsequent transactions. How does the attribution of value operate in this instance? The consideration paid to Person A directly relates to the redemption of a UTXO on Node A in favour of Person B's private/public keypairs, which are recognised on Node A and Node B. Yet Person B chose to transact only with Node B. Does this mean that the parties only recognise the UTXO being redeemed on Node A, or as discussed earlier, is there an assumption that the value is apportioned across the Bitcoin full nodes?

It could be argued that a high-level recognition of bitcoin as valuable, despite being misguided, is sufficient for common law purposes because commerce still recognises that an individual with control over a UTXO possesses a valuable right.

5 *Stability and permanence*

The test relating to stability and permanence considers the degree to which a UTXO continues to exist and persist without change.[185] As demonstrated in the Ainsworth case, rights that fluctuate and can be reviewed at any time to reflect changing personal circumstances may not amount to a proprietary right.[186] This is distinguished from cases where there may be some degree of uncertainty about whether an owner can enjoy their right over a thing. In these instances, the rights are still regarded as proprietary in nature.[187]

Like goodwill and transferable floor space, the right to redeem a UTXO is an intangible right

[183] *Dow Jones* (n 182) [39] (Gleeson CJ, McHugh, Gummow, and Hayne JJ).
[184] See *Dow Jones* (n 182) [38], [40] (Gleeson CJ, McHugh, Gummow, and Hayne JJ).
[185] *Macquarie Dictionary* (online at 23 September 2021) 'stability' (def 2); *Macquarie Dictionary* (online at 23 September 2021) 'permanence'.
[186] *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175, 1248.
[187] See *Halwood Corporation Ltd v Chief Commissioner of Stamp Duties* (1992) 33 NSWLR 395, 402 (Loveday J); See also *Potter v The Commissioner of Inland Revenue* (1854) 156 ER 392; *Box v Commissioner of Taxation* (1952) 86 CLR 387; Cf *Re Toohey; Ex parte Meneling Station Pty Ltd* (1982) 44 ALR 63, 74.

that confers on the person the probability or expectation that the UTXO can be redeemed at some future point in time for value (the bitcoin associated with the UTXO).[188] This right continues to exist, unchanged, on a full node's Bitcoin blockchain until it is redeemed by that person. Even where a chain reorganisation occurs, the UTXO typically persists on the full node's Bitcoin blockchain. Specifically, when a valid transaction (and the subsequent creation of a right to a UTXO) is received by a full node, it is recognised, validated, and stored in the mempool.[189] If a chain reorganisation occurs at this time, the existing chainstate changes and blocks are activated and deactivated to reflect the new chainstate. As the new UTXO was not included in any block, it remains validated in the mempool pending confirmation by the mining process. Where the UTXO did form part of a block that was deactivated following a chain reorganisation, two situations may arise:

(a) The UTXO could be duplicated in one of the new blocks that triggered the chain reorganisation. In this case, the holder retains the right to redeem the UTXO in the new block despite the chain reorganisation.

(b) Alternatively, where none of the new active blocks contain the UTXO, the deactivated transaction would be re-added to the mempool pending confirmation by the mining process.

In both circumstances, the right to redeem the UTXO has in substance persisted. In practice, risk-adverse commercial parties wait approximately an hour to confirm that the transaction has been recognised by most full nodes.[190] Waiting for this period allows further blocks to be added to full nodes' blockchains, reducing the probability that a fork may cause a chain reorganisation and remove the parties' transaction from a valid block. [191]

However, there are several circumstances that can bring a person's right to a UTXO to an end. Firstly, a full node may decide to adopt new consensus rules that interfere with the UTXOs in several blocks.[192] Secondly, the permanence of a UTXO also depends on the full node's intention to continue maintaining its Bitcoin blockchain into the future. For example, a person may only download the Bitcoin blockchain or its software for educational purposes.[193] That person may choose to disable the full node's ability to receive transactions or blocks. Alternatively, the person may decide to delete the software and data necessary to operate the full node. In both cases, the full node's actions fetters a person's ability to redeem a UTXO recognised by that full node. In the latter case, the full node destroys the UTXO and the accompanying right of the person to access, redeem, and use it. For that full node, the UTXO would not exist, but it may persist on other full nodes' Bitcoin blockchains.

Therefore, this dissertation further submits that UTXOs are sufficiently stable and permanent

[188] See *Potter v The Commissioner of Inland Revenue* (1854) 156 ER 392, 396 (Pollock CB); *Halwood Corporation Ltd v Chief Commissioner of Stamp Duties* (1992) 33 NSWLR 395, 402 (Loveday J).
[189] See Part C of Chapter 2.
[190] UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smart contracts* (Legal Statement, November 2019) [54].
[191] Ibid.
[192] See for example the software update 'EIP-779: Hardfork Meta: DAO Fork' on the Ethereum blockchain. This was implemented to 'undo' the exploitation of an event known as the DAO hack on 17 June 2016. Broadly, the update had the effect of transferring all Ether from specific Ethereum accounts (used by the hacker) to a smart contract for redistribution to wronged participants. This is an unusual and rare occurrence.
[193] This applies for the author of this dissertation, who subsequently deleted software necessary to run a full node.

except in circumstances where the full node directly interferes with a person's UTXOs, disables its ability to receive transactions, or removes all files necessary to operate on the Bitcoin network.[194]

6 '*Property-like' protections under common law*

There are currently no Australian cases that consider the extent to which a UTXO may be afforded property-like protections under common law similar to confidential information, trade secrets, trade marks. UTXOs are not imparted in confidence nor possesses a necessary quality of confidence.[195] They are strings of encoded information that are read and decoded by full nodes when processing subsequent transactions. The transaction that gives rise to the UTXO is also in the public domain. Full nodes are not restricted from publishing the encoded transactions that form part of their Bitcoin blockchains, and full nodes re-transmit these transactions throughout the Bitcoin network. This is distinguished from the secrecy afforded to the *mechanism* to access, redeem and use a UTXO, the private/public keypair. The nature of a private key as a proprietary right will not be considered by this dissertation.

However, this does not prevent a UTXO from amounting to a proprietary interest under other indicia.

E *Conclusion*

After a careful weighing of the tests outlined above, this dissertation propounds that the relationship a person has with respect to a UTXO amounts to a proprietary interest for Australian legal purposes.

The relationship can be defined as the right to access, redeem and use a UTXO on a full node's Bitcoin blockchain. This right is present across all full nodes that maintain identical (or nearly identical) Bitcoin blockchains, meaning that the owner of the private/public keypair for a UTXO will have as many rights to redeem that UTXO as there are full nodes that recognise that UTXO on their Bitcoin blockchain. Third parties can readily identify a person's right to redeem a particular UTXO, which is distinguished from other UTXOs recorded on a full node's Bitcoin blockchain. This is the case even though the actual identity of the owner may not be known.

A person exercises recognised control over a UTXO by virtue of its encoded nature. A UTXO is cryptographically secured to prevent its redemption unless the corresponding private/public keypair is presented to 'unlock' it for use in a subsequent transaction. A person who knows (or possesses the means to know or use)[196] the private/public keypair associated with the UTXO controls that UTXO. Consequently, third parties without this knowledge are restricted from interfering with this right. For practical purposes, a person need only exercise their right once by constructing a valid transaction for a connected full node. The holder implicitly authorises the recipient full node to re-transmit the transaction (and therefore exercise of the right) on the owner's behalf to peer nodes. This mechanism also reflects the ability of the inherent value of

[194] *Re Toohey; Ex parte Meneling Station Pty Ltd* (1982) 44 ALR 63, 74.
[195] See *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* [1963] 3 All ER 413; *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41.
[196] For example, the person can access a Bitcoin wallet, which stores the relevant private/public keypair.

the UTXO to be re-associated with new private/public keypairs. It is this restricted control over the bitcoin associated with a UTXO that has value, which is recognised as a valuable, intangible right.

However, a UTXO will not amount to property where a full node directly interferes with the owner's UTXO, disables its ability to receive transactions, and/or removes all files necessary to operate on the Bitcoin network.

While bitcoin is broadly treated as property in several Australian cases,[197] this dissertation has detailed the precise nature of that proprietary right, which is absent from these cases. From this position, the next Part will identify the impacts this conclusion has on Australia's taxation of bitcoin transactions.

F *Further considerations*

The concept of property permeates several areas of Australian law. While this dissertation cannot evaluate the impact across every area of Australia law, it will briefly address the consequences for taxation purposes.

In taxation law, a thing that satisfies the definition of a 'CGT asset' under paragraph 108-5(1)(a) of the *Income Tax Assessment Act 1997* (Cth) would be captured by the Australian capital gains tax (CGT) regime.[198] A capital gain (typically the difference between the proceeds from the sale of the CGT asset less the original acquisition price) is included in a person's assessable income for Australian taxation purposes.

The Australian Taxation Office (ATO) in Taxation Determination TD 2014/26 *Income tax: is bitcoin a 'CGT asset' for the purposes of subsection 108-5(1) of the Income Tax Assessment Act 1997?* (TD 2014/26) adopts the view that bitcoin is property according to Australian common law and a CGT asset. However, there are several interpretive issues with the ATO view.

Firstly, the ATO claims that there is a change of ownership when a transaction is effected on the Bitcoin blockchain. As an act or event involving a change in ownership of a CGT asset triggers a 'CGT event A1', the ATO concludes that this CGT event governs when an individual makes a capital gain for income tax purposes.[199] This dissertation respectfully disagrees with that claim. A change in the ownership of a UTXO is not recorded on the Bitcoin blockchain. This is because, to effect a change in ownership without redeeming a UTXO, a person would need to impart the knowledge of a private/public keypair relating to a UTXO to a third party.[200] This is because a change in ownership of the UTXO can only occur where the mechanism to access, redeem and use the UTXO is rendered onto another.

---

[197] See *Australian Securities and Investments Commission v Ostrava Equities Pty Ltd* [2015] FCA 425, [17] (per Davies J); *Balsam & Lackner* [2020] FCCA 1115, [186], [200] (per Burchardt J); *Powell v Christensen* [2020] FamCA 944, [44].
[198] See Part 1-3 of the *Income Tax Assessment Act 1997* (Cth).
[199] See paragraph 15 of Taxation Determination TD 2014/26 *Income tax: is bitcoin a 'CGT asset' for the purposes of subsection 108-5(1) of the Income Tax Assessment Act 1997?*
[200] See subsection 104-10(1) of the *Income Tax Assessment Act 1997* (Cth).

All transactions on the Bitcoin blockchain necessarily involve a UTXO being redeemed, which causes the creation of new UTXOs associated with the private/public keypairs identified in the transaction. The individual retains control of the original UTXO, however that UTXO becomes unspendable and functionless.

Secondly, the redemption of a UTXO in constructing a valid transaction for a full node triggers a different CGT event. A CGT event C2 applies to circumstances where an individual's ownership of an intangible CGT asset ends where the asset is 'redeemed or cancelled'.[201] As a UTXO becomes unspendable once it has been redeemed in a transaction, it is arguable that this CGT event occurs with each transaction. Where that transaction (and therefore the redemption of the UTXO) is re-transmitted to peer nodes, each validation by a separate peer node will also trigger a CGT event C2. Consequently, every time a transaction is validated and re-transmitted, an individual would trigger as many CGT events are there are versions of the validated UTXO. As CoinTelegraph suggests that there are 11,558 reachable nodes currently active across Bitcoin,[202] each redemption of a UTXO may trigger 11,558 CGT events.

Alternatively, as ownership of the UTXO is not lost when it is redeemed in a transaction, it is also arguable that a CGT event H2 occurs. This CGT event arises where no other CGT event applies, and the act or event that affects your CGT asset does not adjust the asset's cost base (broadly, the amounts considered to form the costs of acquiring the asset).[203] Where CGT event C2 is not applicable, this dissertation claims that a CGT event H2 occurs with each direct and re-transmitted transaction.

Depending on the applicable CGT event, the general rules about what forms part of an asset's initial value or proceeds received from a CGT event can be displaced by special modifications. Therefore, knowing which CGT event has occurred is relevant when calculating the correct net capital gain from CGT assets. For example, where a CGT event A1 occurs and no consideration is received, the market value of the asset at the time of the disposal can be substituted as the proceeds when calculating the capital gain or loss of that CGT event.[204] This is known as the market value substitution rule ('MVSR'). Conversely, where a CGT event H2 occurs, the MVSR does not apply.[205]

Finally, the ATO claims that a new CGT asset may be received by an individual following a chain split.[206] For example, on 1 August 2017, some full nodes on the Bitcoin blockchain adopted a different set of consensus rules to those that existed previously. These changes were not compatible with the previous consensus rules, and the blocks created using these rules were not accepted by the un-upgraded full nodes. Consequently, one group of full nodes re-branded their Bitcoin blockchain to 'Bitcoin Cash', and the Bitcoin community accepted that this re-branding represented a separate cryptocurrency.

---

[201] See paragraph 104-25(1)(a) of the *Income Tax Assessment Act 1997*(Cth).
[202] Cyrus McNally, 'Bitcoin node count hits new all-time high' *CoinTelegraph* (online, 15 August 2021) <https://cointelegraph.com/news/bitcoin-node-count-hits-new-all-time-high>.
[203] R L Deutsch, et al, *The Australian Tax Handbook* (Thomson Reuters, 1st ed, 2018) 530.
[204] *Income Tax Assessment Act 1997* (Cth) s 116-30.
[205] See *Income Tax Assessment Act 1997* (Cth) s 116-25.
[206] Australian Taxation Office, 'Chain splits', *Transacting with cryptocurrency* (Web Page, 20 August 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?page=2#Chain_splits>.

The ATO states that this chain split resulted in the creation of a new asset – Bitcoin Cash.[207] However, this dissertation suggests that this view is incorrect. A chain split occurs when the Bitcoin blockchains of two or more full nodes are compared, where it is identified that the blocks on each blockchain permanently diverge from one another from a point in time. This typically occurs because of changes to a full node's consensus rules, which makes the full node validate transactions and blocks in different ways. However, no new assets are created. UTXOs that existed prior to the chain split persist through the chain split unless the change to the consensus rules have the effect of rendering historical UTXOs invalid. Instead, commercial parties and the Bitcoin community treat this divergence as the creation of a secondary, separate asset, but this does not reflect the facts above.

These consequences highlight the significant administrative burden faced by individuals and the ATO when applying Australian taxation law to Bitcoin concepts. This dissertation proposes that the Australian government should consider implementing administrative concessions or targeted legislation to curtail the burden arising from Bitcoin transactions.

[207] Australian Taxation Office, 'Chain splits', *Transacting with cryptocurrency* (Web Page, 20 August 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?page=2#Chain_splits>.

IV BITCOIN: 'MONEY', 'CURRENCY' OR 'LEGAL TENDER'?

A frequently asked question is whether bitcoin … can be defined as 'money'. The short answer is that bitcoin is not a form of money.[208]

Reserve Bank of Australia, 2018

A *Overview*

The Reserve Bank of Australia highlights that '[t]hroughout history and around the world, money has taken diverse forms'.[209] While coins, such as pound sterling or the Australian dollar, are well-known examples of money, many other objects and instruments have acted as media of exchange (see Diagram 13 below).

In ancient Egypt, grain was the preferred medium of internal exchange and formed part of the nation's accounting system.[210] In fact, Glyn Davies, author of *History of Money*, claims that the concept of transfer payments originated from the centralisation of harvested grain into local warehouses ('grain banks'). Once farmers deposited their harvest into these grain banks, compulsory payments to the king could be settled by adjusting the grain's allocation in favour of the king.[211] Eventually this expanded so that debts owed to other people could also be settled through grain banks.[212]

As early as 1535, 'wampums' (a string of beads made from the shells of predominantly white clams) were widely used as Native American currency.[213] Like gold excavated for coinage, wampums were harvested from the rivers towards the north-east of North America.[214] Davies also highlights that wampums played an influential role in the monetary policy of early American colonies such that 'Massachusetts declared white wampum legal tender at six beads a penny and black at three a penny'.[215]

Prior to the adoption of decimal currency in Australia in 1966, colonies also exchanged peculiar objects despite the existence of prescribed coinage. Deputy President Bernard McCabe in *Seribu Pty Ltd v Commissioner of Taxation* [2020][216] detailed how, even though a mandate dictated that the pound sterling was the official currency of Australia, the lack of supply of that currency into Australia forced early settlors to adopt rum and promissory notes as alternative media of exchange.[217] Rum persisted as currency from 1792 until the end of the infamous Rum

---

[208] Reserve Bank of Australia, 'What are cryptocurrencies', *Cryptocurrencies* (Web Page, 19 September 2021) <https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html>.
[209] Reserve Bank of Australia, 'What is Money?', *Explainers* (Web Page, 17 October 2021) <https://www.rba.gov.au/education/resources/explainers/what-is-money.html>.
[210] Glyn Davies, 'History of Money' (University of Wales Press, 3rd ed, 2002) 52; Seth Litwack, 'Bitcoin: Currency or Fool's Gold?: A Comparative Analysis of the Legal Classification of Bitcoin' (2015) 29(2) *Temple International & Comparative Law Journal* 309, 311.
[211] Davies (n 210) 52.
[212] Ibid.
[213] Davies (n 210) 40.
[214] Ibid.
[215] Davies (n 210) 41.
[216] AATA 1840.
[217] *Seribu Pty Ltd v Commissioner of Taxation* [2020] AATA 1840, [2]—[4] (Deputy President McCabe) ('*Seribu*'); See also National Museum of Australia, 'Governor William Bligh is deposed in the Rum Rebellion', *Defining Moments* (Web Page, 17 October 2021) <https://www.nma.gov.au/defining-moments/resources/rum-rebellion>.

Rebellion in 1810 when Governor Macquarie imported and converted Spanish coins into a new local currency, the 'holey dollar'.[218] By 1829, the holey dollar was abandoned and Britain required Australian colonies conduct transactions in British coins.[219] The National Museum of Australia highlights how

> [i]t wasn't until 1910, nine years after Federation, that Australia again created its own currency – the Australian pound. Even then, its coins were minted by branches of Britain's Royal Mint in Sydney, Melbourne and Perth.[220]

Over time, this too changed; and, in 1966, Australia transitioned to the decimal currency now circulating today, the Australian dollar.[221]

Diagram 13 – Forms of money: cowrie shells, rum bottles and the 'holey dollar'[222]

Given the range of objects that have been accepted as money historically, this Chapter examines the decisions of judicial officers in determining when a 'thing' meets the definition of 'money' or 'currency' for Australian legal purposes. Charles Proctor, author of *Mann on the Legal Aspect of Money*, is often cited in Australian case law due to the comprehensive nature of his analysis into money and monetary obligations. He affirms how the term 'money' is so pervasive and frequently used in legislation and case law that even lawyers forget the meanings it possesses in different legal scenarios.[223] Therefore, this dissertation outlines several propositions about the nature of money, currency, and legal tender, and considers whether concepts relating to Bitcoin satisfy these definitions.

It concludes that unspent transaction outputs (UTXOs) meet the functional and common law definition of the term 'money', and, due to the widespread circulation of UTXOs as a means of

---

[218] *Seribu Pty Ltd v Commissioner of Taxation* [2020] AATA 1840, [6] (Deputy President McCabe); See also National Museum of Australia, 'Governor William Bligh is deposed in the Rum Rebellion', *Defining Moments* (Web Page, 17 October 2021) <https://www.nma.gov.au/defining-moments/resources/rum-rebellion>; National Museum of Australia, 'Holey dollar', *Collection Highlights* (Web Page, 17 October 2021) <https://www.nma.gov.au/explore/collection/highlights/holey-dollar>.

[219] National Museum of Australia, 'Decimal Currency', *Defining Moments* (Web Page, 17 October 2021) <https://www.nma.gov.au/defining-moments/resources/decimal-currency>.

[220] Ibid.

[221] Ibid. The naming of the Australian dollar was made a public event, and Australians suggested the following names for the decimal currency: 'Austral, Oz, Boomer, Roo, Kanga, Emu, Koala, Digger, Zac, Kwid, and Dinkum'.

[222] Images sourced from Reserve Bank of Australia, 'What is Money?', *Explainers* (Web Page, 17 October 2021) <https://www.rba.gov.au/education/resources/explainers/what-is-money.html>; National Museum of Australia, 'Holey dollar', *Collection Highlights* (Web Page, 17 October 2021) <https://www.nma.gov.au/explore/collection/highlights/holey-dollar>.

[223] Charles Proctor, *Mann on the Legal Aspects of Money* (Oxford University Press, 7th ed, 2012) 6.

payment, it also satisfies the broadest definition of 'currency'. Comparatively, 'legal tender' is a statutory term referring to the prescribed, 'lawful money' of a nation. UTXOs are not legal tender in Australia as the lawful money of Australia is prescribed by the *Currency Act 1965* (Cth) and *Reserve Bank Act 1959* (Cth). However, due to the decree recently issued by the Legislative Assembly of the Republic of El Salvador, Bitcoin has been adopted as the legal tender of El Salvador.[224]

B *Examples of money and currency*

1 *Bank notes*

In *Miller v Race* (1758) ('the Miller case'),[225] Lord Mansfield considered whether a plaintiff, who had been robbed of a bank note sent by post, could bring an action of trover against the defendant to recover the note itself rather than seek compensatory damages.[226] Relevantly here, the defendant who was found in possession of the note had acquired it from a third party without notice that it had been illegally obtained.[227]

Lord Mansfield established that bank notes are 'not goods, not securities, nor documents for debts'.[228] Even where the bank notes pass under a will, they are not treated as securities for money due to the prescribed value of the note.[229] Rather, they:

> …are treated as money, as cash, in the ordinary course and transaction of business, by the general consent of mankind; which gives them the credit and currency of money, to all intents and purposes.[230]

As an action of trover had historically been brought before money had been passed in currency, his Lordship considered whether the bank note had passed into the defendant's hands as money in currency.[231] If the note had passed as money in currency, the action of trover would fail. Ultimately, the court held that the bank notes had passed as money in currency as the notes were universally treated as money by commerce, such that 'their currency should be established and secured'.[232] This decision was considered and approved in *Moss v Hancock* [1899] ('the Moss case'),[233] which is discussed next.

2 *Stolen gold pieces*

In the Moss case, an appellant stole a gold five-pound piece from his employer, the respondent, and exchanged it as 'a curiosity' for five sovereigns.[234] The appellant was charged, plead guilty to the theft, and the court ordered that the five-pound piece be restored to the respondent

---

[224] *Ley Bitcoin* [Bitcoin Law] (El Salvador), Decree No. 57, 8 June 2021 <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf>.
[225] (1758) 1 Burrow 452 ('*Miller*').
[226] Action of trover is similar to modern day actions for restitution.
[227] *Miller* (n 225).
[228] *Miller* (n 225) 457 (per Lord Mansfield).
[229] Ibid.
[230] Ibid.
[231] *Miller* (n 225) 458 (per Lord Mansfield).
[232] *Miller* (n 225) 459 (per Lord Mansfield).
[233] [1899] 2 QB 111 ('*Moss*').
[234] *Moss* (n 233) 111.

pursuant to section 100 of the *Larceny Act 1861*. According to the *Coinage Act 1870*, however, a gold, five-pound piece was deemed to be currency and legal tender. Counsel for the appellant argued that restitution of the piece could not be made once it had entered circulation as money.[235] Similar to the bank note from the Miller case, the Queen's Bench Division considered whether the gold piece had passed as 'money'.

Darling J highlighted how exchanging gold pieces does not necessarily mean that the parties were transacting in money as currency.[236] Some coins, despite being current, are more valuable as antiques or rare items. In those instances, they are money as 'medals'.[237] Money as currency, however, means:

> that which passes freely from hand to hand throughout the community in final discharge of debts and full payment for commodities, being accepted equally without reference to the character or credit of the person who offers it and without the intention of the person who receives it to consume it or apply it to any other use than in turn to tender it to others in discharge of debts or payments for commodities.[238]

Consequently, Darling J concluded that the gold piece did not pass as currency.[239] The transaction occurred because the appellant secured a buyer of rare items, seeking to redeem the value of the piece as a rarity rather than its denomination. This highlights that the term 'money' possesses a dual meaning that is characterised by its use. Specifically, even though property may constitute 'money', one must also consider whether it also passes as currency. Given the length of time that has passed since this case, it is also unclear whether money as currency means the same thing as modern notions of 'currency'.

3 *Deposits at the bank, inter-bank transfers and exchange settlement accounts*

In *Re Collings* [1933] ('the Collings case'),[240] the executor of a testator's estate approached the Chancery Division for a determination regarding whether 'money' for the purpose of testator's will included money in a deposit account at a bank. At this point in time, it had been accepted that 'cash in hand and money on drawing account' was money on the basis that it was readily available.[241]

Farwell J reflected on the ordinary use of the term 'money' and highlighted how a person, when describing what they consider to be all their money, treats funds held in a deposit account as their money. While such funds were not money in the strict legal sense of the term, Farwell J preferred an approach based on the substance of the transaction. Therefore, even though the proper form of those funds were a debt, his Honour held that the ordinary usage by mankind regarded deposits at a bank as money.

Subsequently, the ordinary usage of the term 'money' was also considered by Rich and Williams JJ in *Bank of New South Wales v Commonwealth* [1948] (the Bank Nationalisation

---

[235] *Moss* (n 233) 113, citing *Miller v Race* (1791) 1 Burrow 452, 447.
[236] *Moss* (n 233) 116 (Darling J).
[237] Ibid.
[238] Ibid.
[239] *Moss* (n 233) 117 (Darling J).
[240] [1933] Ch 920 ('*Collings*').
[241] *Collings* (n 240) 922 (per Farwell J).

case)[242] while addressing whether banks were engaged in 'trade and commerce' under the Australian Constitution.

Their Honours explored the evolution of the banking industry and highlighted how the transfer of funds between banks in different States no longer involved the physical transfer of bank notes or coins.[243] Instead, the parties would negotiate over the phone how a customer's liabilities could be adjusted to reflect a notional payment of funds interstate. Citing Lord Wright in the Privy Council case *Trinidad Lake Asphalt Operating Co Ltd v Commissioners of Income Tax for Trinidad* (1945),[244] their Honours stated that:

> …the transmission of funds has become still more divorced in the minds of business men, and even of lawyers, from the idea of any material embodiment. No document is necessary. Two companies separated by the ocean may orally agree over the wireless telephone that the debt of one may be set against a debt of the other and both cancelled. The only evidence or material embodiment of the transaction may consist of entries in the books on each side made in pursuance of their agreement, but what has happened is, if so intended, equivalent to a receipt of money…[245]

Therefore, 'any medium which by practice fulfills the function of money and which everybody will accept in payment of a debt is money in the ordinary sense of the word.'[246] Most importantly, their Honours noted that money (and 'bank money' as described above) need not be legal tender.[247]

4 *Currency, coinage, and legal tender under the Australian Constitution*

Section 51(xii) of the *Commonwealth of Australia Constitution Act 1901* (Cth) ('the Constitution') confers on the Parliament of Australia the power to make laws 'for the peace, order, and good government of the Commonwealth' with respect to 'currency, coinage and legal tender'. In 1979, an action for declaratory relief was sought in the High Court of Australia on several constitutional grounds. This included clarifying the terms 'currency, coinage, and legal tender' under the Constitution.

Stephen J in *Watson v Lee* (1979) ('the Watson case')[248] highlighted that the provision contained very clear overlapping terms.[249] Coinage, which refers to coins as money, is an example of currency.[250] Legal tender, on the other hand, refers to the 'lawful mode of payment within a polity' at any given time.[251]

His Honour also highlights that this head of power is not restricted to Australian coinage, as this would ultimately limit the Commonwealth's ability to legislate with respect to foreign

[242] [1948] HCA 7 ('*Bank Nationalisation*').
[243] Cf the concept that money is a physical thing 'passing freely from hand to hand': *Moss* (n 233) 116 (Darling J).
[244] (1945) AC 1.
[245] *Bank Nationalisation* (n 242) 100, citing *Trinidad Lake Asphalt Operating Co Ltd v Commissioners of Income Tax for Trinidad* (1945) AC 1, 10—12 (per Lord Wright).
[246] *Bank Nationalisation* (n 242) 100.
[247] Ibid.
[248] (1979) 26 ALR 461 ('*Watson*').
[249] *Watson* (n 248) 480 (Stephen J), citing *Bank Nationalisation* (n 242) 193 (Latham CJ).
[250] *Watson* (n 248) 480 (Stephen J).
[251] Ibid.

coinage.[252] For example, adopting a narrow interpretation of 'coinage' would have curtailed the Commonwealth's ability to domestically address foreign coinage counterfeiting.[253] The same principles apply with respect to 'currency', which include paper money and counterfeit paper money.[254]

After exploring the history of the currencies used throughout the British colonies (including Australia), his Honour clarified that 'currency' was not limited to 'the money of a particular nation nor to that which is one nation's legal tender'.[255] This is because, prior to and for some time after the Federation of Australia, there was no particular currency formally adopted by any one of the Australian colonies.[256] To restrict the meaning of 'currency' under the Constitution would have resulted in a significant reduction of the Commonwealth's ability to 'regulate and control…[what was] the everyday currency of the country'.[257] Therefore, Stephen J concluded that 'currency' under the Constitution was not limited to Australian currency.[258]

Following this decision, the meaning of the provision was again considered by the High Court of Australia in *Leask v Commonwealth of Australia* (1996) ('the Leask case').[259] The judgments of two Justices are relevant here. Firstly, Brennan CJ reflected on the Watson case before stating that:

> 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.[260]

This paragraph could be interpreted in two ways as 'consists of', which means 'to be made up or composed of', can refer to a list that is exhaustive or non-exhaustive.[261] Either Brennan CJ's passage above provides that currency means only those notes and coins issued under the law of a country used as a medium of exchange, or his Honour is merely outlining examples of currency.

Comparatively, Gummow J stated that 'currency is a universal means of exchange, designated by a particular unit of account'.[262] His Honour did not reference the need for currency to be expressed in notes or coins nor held that it had to be issued by any particular nation.[263] Instead, his Honour highlighted that:

> …while "coinage" and "legal tender" involved quite specific and narrow concepts, the former being concerned with coins as money and the latter with the prescription of that which at any particular time may be a lawful mode of payment, **"currency" was a**

[252] *Watson* (n 248) 481 (Stephen J).
[253] *Watson* (n 248) 481 (Stephen J), discussing *Crimes Act 1990* (NSW) ss 318—324.
[254] *Watson* (n 248) 481 (Stephen J).
[255] Ibid.
[256] *Watson* (n 248) 482 (Stephen J).
[257] Ibid.
[258] Ibid.
[259] (1996) 140 ALR 1 ('*Leask*').
[260] *Leask* (n 259) 10 (Brennan CJ).
[261] *Oxford English Dictionary* (online at 3 October 2021) 'consist' (def 7 'to consist of').
[262] *Leask* (n 259) 31 (Gummow J).
[263] *Leask* (n 259) 31 (Gummow J), discussing *Jolley v Mainka* (1933) 49 CLR 242, 259-61, 266-9.

> **broader expression**.[264] (emphasis added)

The critical point to be extracted from this passage is that currency is a broader expression than legal tender. If legal tender is concerned with prescribed mode of payment within a nation, then currency must extend to non-prescribed payments, as highlighted by the Watson case.

These cases represent the most definitive definitions of 'currency' and 'legal tender' available in Australia, given the broad scope of the Constitution. The judgments from Stephen J in the Watson case and Gummow J in the Leask case demonstrate that the broadest definition of currency is any money designated in a unit of account that is presently circulating,[265] regardless of whether it is legal tender.[266]

5 *Promissory notes and exchanging liabilities*

In *Messenger Press Proprietary Ltd v Federal Commissioner of Taxation* [2012] (the Messenger case),[267] a large group of related companies (the appellants) agreed to reorganise the group's assets to increase the profitability of their Australian-based companies.[268] By a series of complex transactions, this reorganisation was effected through the exchange of promissory notes denominated in foreign currencies for liabilities denominated in Australian dollars.[269] For taxation purposes, the appellants claimed that the exchange of the promissory notes gave rise to foreign currency losses under the former Division 3B of the *Income Tax Assessment Act 1936* (Cth) ('ITAA 1936'). Former Division 3B of the ITAA 1936 allowed taxpayers to treat capital losses arising from the fluctuations in foreign currency exchanges rates as an expense that could be used to offset their assessable income for income tax purposes.

Perram J considered whether the provision was limited to those losses from the exchange of foreign and Australian 'money' or if it extended to fluctuations in exchanging liabilities.[270]

While the promissory notes had the effect of exchanging liabilities between the entities in the group, his Honour stated that non-bank promissory notes and intra-group debts did not constitute money.[271] Firstly, no evidence was produced that demonstrated that the group's promissory notes were used throughout a community to discharge monetary obligations, nor did it form part of a payment system.[272] Secondly, if such evidence was produced, the recipient would necessarily need to enquire into the character and credibility of the issuer to ascertain whether the issuer was capable of fulfilling the obligation.[273] Finally:

> [n]or, where the promissory notes were not presented for payment, is it possible to identify another flow of funds which might usefully be seen as 'money' (i.e. that which might have occurred if a bank account had been credited on presentation of each note).[274]

---

[264] *Leask* (n 259) 31 (Gummow J).
[265] *Macquarie Dictionary* (online at 2 October 2021) 'current' (def 2).
[266] *Watson* (n 248) 481 (Stephen J); *Leask* (n 259) 31 (Gummow J).
[267] [2012] FCA 756 ('*Messenger*').
[268] *Messenger* (n 267) [60].
[269] *Messenger* (n 267) [61] and [67].
[270] *Messenger* (n 267) [117].
[271] *Messenger* (n 267) [155].
[272] *Messenger* (n 267) [196].
[273] Ibid.
[274] *Messenger* (n 267) [196].

This final statement appears to reflect further the notion that promissory notes did not form part of an established payment system, which would credit the financial institution account of the recipient who had presented the promissory note. Crediting the recipient's account, in turn, allows the recipient to tender on the value associated with the credit. Hence, intra-group promissory notes could not be freely tendered on to others to satisfy monetary obligations.

6 *Foreign currency and bank deposits denominated in foreign currency*

In *Deputy Commissioner of Taxation v Conley and Others* (1998) (the Conley Case),[275] a respondent failed to pay the Australian Taxation Office ('ATO') approximately AUD52m in tax-related liabilities. To recover this liability, the Deputy Commissioner of Taxation issued two garnishee notices pursuant to former section 218 of the ITAA 1936 ('the garnishee notices') to a bank with which the respondent held accounts. Garnishee notices require recipients pay to the ATO any 'money' the recipient may otherwise owe to a taxpayer. In response, the respondent sought declaratory relief from the Federal Court of Australia to confirm whether foreign currency satisfied the meaning of 'money' for the purpose of the garnishee notices.

While Emmett J considered whether 'money' meant Australian currency or 'money as a medium of exchange, irrespective of the currency involved',[276] his Honour did not address any historical cases outlined above. Instead, his Honour relied on the publication *The Legal Aspect of Money*, authored by Francis Mann.[277]

Mann distinguished between two forms of money: the concrete form and abstract form.[278] The concrete form concerns the legal tender of a country. Specifically, it refers to the chattels issued by a legal authority, denominated in a unit of account, and used as the medium of exchange in that country.[279] Comparatively, money in the abstract form looks at the 'purchasing power in terms of wealth in general'.[280]

In the context of garnishee notices, the term money extended beyond legal tender and included money obligations, such as credit balances at a bank. Emmett J further held that:

> …money in that sense must still be expressed in an accepted unit of account. That unit of account will vary from country to country. Within a particular country, money will generally refer to the medium of exchange within that country, namely, the currency of the country.

The *Currency Act 1965* (Cth) and predecessor legislation relevantly define the unit of currency of Australia.[281] The first denomination of this currency is the 'Australian dollar'.[282] It is equivalent to one hundred 'cents', the second denomination of the currency of Australia.[283] His Honour also highlighted how the *Currency Act 1965* (Cth) requires all payments and

[275] (1998) 158 ALR 229 ('*Conley*').
[276] *Conley* (n 275) 234 (per Emmett J).
[277] *Conley* (n 275) 235 (per Emmett J).
[278] Francis Mann, *The Legal Aspects of Money* (Oxford University Press, 5th ed, 1992) 5.
[279] *Conley* (n 275) 235 (per Emmett J), citing Mann (n 278) 5.
[280] *Conley* (n 275) 235 (per Emmett J), citing Mann (n 278) 28.
[281] See *Currency Act 1965* (Cth) s8; *Coinage Act 1909* (Cth) s 2; *Coinage Act 1936* (Cth) sch 1; *Coinage Act 1947* (Cth) sch 1.
[282] *Currency Act 1965* (Cth) subs 8(1).
[283] *Currency Act 1965* (Cth) subs 8(3).

transactions (and other matters or things relating to money) to be made in the currency of Australia unless it was made according to the currency of some country other than Australia.[284] This, in conjunction with the fact that the ITAA 1936 broadly uses the expression 'currency of Australia' in its provisions,[285] meant that the payment of money under garnishee notices did not extend to money denominated in foreign currency.[286]

Unfortunately, Emmett J's judgment is ambiguous. The only inferences that can be drawn from this reasoning are that bank deposits denominated in foreign currency may be money generally but are not money for the purpose of a garnishee notice. This is on the basis that his Honour continued to refer to these bank deposits as 'money denominated in foreign currency'. It is also unclear whether sections 9 and 11 of the *Currency Act 1965* (Cth) create an interpretive presumption that all references to 'money' in Australian legislation is, in the first instance, restricted to the currency of Australia or the currency of some country other than Australia.

In *Travelex Limited v Commissioner of Taxation* [2008] (the Travelex case),[287] an applicant sought declaratory relief against the Commissioner of Taxation regarding the sale of foreign currency in light of the *A New Tax System (Goods and Services Tax) Act 1999* (Cth) ('the GST Act'). Emmett J considered the legal relationship between foreign currency as a 'good' versus 'money'.

This judgment is significantly clearer than his Honour's earlier judgment in the Conley case. Specifically, his Honour reiterated the definition provided by Darling J in the Moss case and said that:

> Money is any generally accepted medium of exchange for goods and services and for the payment of debts… Currency and legal tender are examples of money. However, a thing can be money and can operate as a generally accepted medium and means of exchange, without being legal tender… It is common consent and conduct that gives a thing the character of money…[288]

In relation to currency, Emmett J states that the term is synonymous with the physical form of the medium of exchange circulating in a nation (e.g., coinage and bank notes).[289] This is because each nation can implement whatever legislation it desires to govern its monetary system, including details about the lawful mode of payments, money specifications and authority to issue that money.[290] However, currency can also be used to refer to the feature that the right to the currency of a nation passes on delivery irrespective of the title of the transferor and 'is inseparable from the possession of it'.[291] That is, currency is exempt from the maxim of *nemo dat quod non habet*.[292]

Turning to legal tender, his Honour reiterated that this term describes the nation's lawful mode

[284] *Conley* (n 275) 235 (per Emmett J), citing *Currency Act 1965* (Cth) ss 9, 11.
[285] *Conley* (n 275) 235 (per Emmett J).
[286] *Conley* (n 275) 240 (per Emmett J).
[287] [2008] FCA 1961 ('*Travelex*').
[288] *Travelex* (n 287) [25] (per Emmett J).
[289] *Travelex* (n 287) [23]—[24] (per Emmett J).
[290] *Travelex* (n 287) [26] (per Emmett J).
[291] *Travelex* (n 287) [24] (per Emmett J).
[292] *Travelex* (n 287) [24] (per Emmett J).

of payment,[293] which necessarily has money-like qualities.[294] To effectively discharge a debt in a nation, there must be payment of currency that is recognised as legal tender in that nation.[295] Therefore, revisiting his Honour's earlier statements on money, a generally accepted medium of exchange can still be money even though it is not the lawful mode of discharging a debt. This is because parties to a transaction can consent to its use even though there is no formal obligation to do so.[296]

Emmett J also clarified that 'the mere fact that foreign currency might be legal tender in another polity does not make it legal tender in Australia'.[297] This means that, even if Bitcoin concepts were recognised as legal tender in another nation, such as El Salvador,[298] it would not make it legal tender in Australia.

Relevantly here, the GST Act defines money as including foreign currency.[299] Consequently, his Honour held that the sale of foreign currency was a supply of money rather than a supply of goods.[300]

C *Observations about money, currency, and legal tender*

It is clear from historical Anglo-Australian cases that the meaning of money and currency involves a significant degree of overlap. The following six propositions explain the conceptual meaning of and relationships between the terms money, currency, and legal tender. They also form the basis of the conclusions reached in Part D, which considers the extent to which Bitcoin satisfies those definitions.

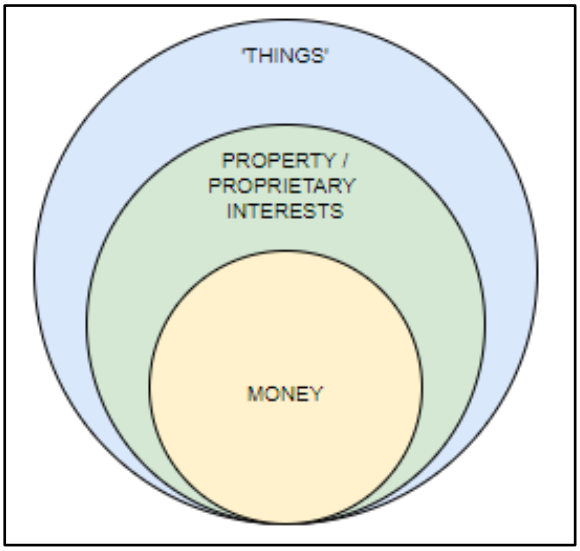
Proposition 1: All money is a form of property.[301] If a thing does not amount to property by virtue of its own characteristics or by a deeming provision under legislation,[302] it cannot be money. However, not all property is money.

Proposition 2: As currency and legal tender are examples of money,[303] they too must be property. If a thing satisfies the meaning of currency or legal tender, it will be both money and property. Therefore, where a UTXO is currency or legal tender, it must also be money.

---

[293] *Travelex* (n 287) [24] (per Emmett J), citing *Watson v Lee* (1979) 144 CLR 374, 398.
[294] *Travelex* (n 287) [27] (per Emmett J).
[295] *Travelex* (n 287) [28] (per Emmett J).
[296] *Travelex* (n 287) [33] (per Emmett J).
[297] Ibid.
[298] *Ley Bitcoin* [Bitcoin Law] (El Salvador), Decree No. 57, 8 June 2021 <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf>.
[299] See *A New Tax System (Goods and Services Tax) Act 1999* (Cth) s 195-1.
[300] *Travelex* (n 287) [35] (per Emmett J).
[301] See *Moss* (n 233) 116 (Darling J).
[302] For example, Australian notes or coinage.
[303] *Travelex* (n 287) [25] (per Emmett J).

Diagram 14 – Money as property



Proposition 3: Money does not need to be the legal tender of any nation.[304] Historical case law reflects the adoption of 'Societary theory', which considers that broad community acceptance determines when an object amounts to money.[305] Conversely, 'State theory', introduced by Georg Knapp, regards money as a thing that can only be created by a State.[306] This dissertation applies Societary theory further to the precedential case law outlined above.

Provided that a thing fulfills the function of money and meets the definition provided Australian common law, that thing will be money under the broadest meaning of the term. This is true even where the thing has no tangible form.[307] The 'function of money' refers to the ability of money to act as:

(a) a measure of value or unit of account,
(b) a means of payment,
(c) a medium of exchange, and
(d) a store of value.[308]

Where Australian legislation includes the term 'money', standard principles regarding statutory interpretation apply, and the meaning of 'money' may be narrowed.

Proposition 4: Money exists in two forms: circulating and non-circulating money.[309] This distinction is relevant when considering whether an action for restitution would succeed in relation to the money. For example, as highlighted in the Miller and Moss cases, where a thing that satisfies the broad definition of money is not passed as circulating money (ie, it passes like

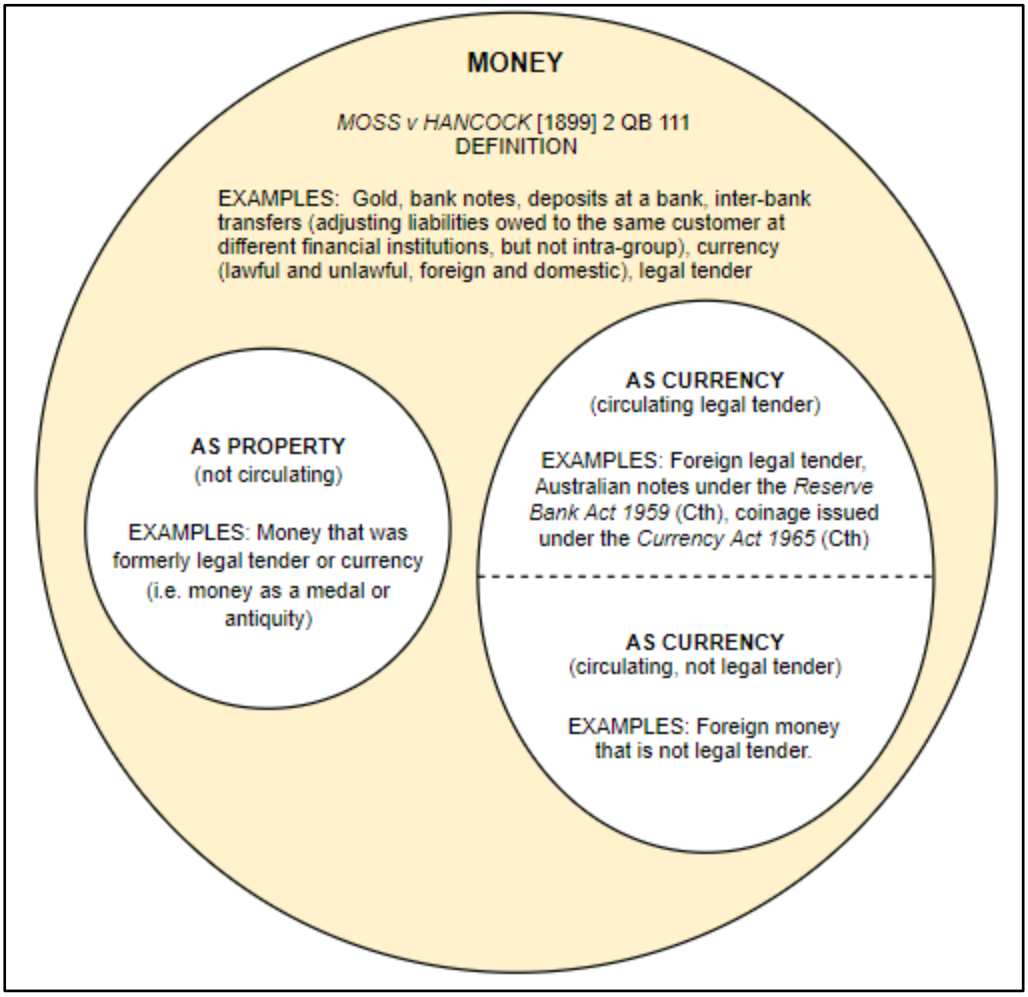
[304] See *Travelex* (n 287) [25] (per Emmett J); *Bank Nationalisation* (n 242) 100. See also Terence Wong, 'Bitcoin deconstructed: Part 2 – Real and virtual worlds' (2014) 30(6) *Australian Banking & Finance Law Bulletin* 122, 123. Cf Charles Proctor, 'Cryptocurrencies in International and Public Law Conceptions of Money' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019) [3.07].
[305] Proctor (n 104) [3.07].
[306] Proctor (n 104) [3.06].
[307] See *Bank Nationalisation* (n 242) 100.
[308] Georgios Zekos, 'Economics and Legal Understanding of Virtual Currencies' (2019) 38(8) *Banking & Finance Services Policy Report* 1; Geoffrey Ingham, *Money* (Polity Press, 1st ed, 2020) 11.
[309] See *Miller* (n 225) 458 (per Lord Mansfield); *Moss* (n 233) 116 (Darling J).

a medal or antiquity) it is capable of being recovered by the common law action of restitution.[310]

Proposition 5: Currency, or current money, is circulating money denominated in a unit of account.[311] Similarly, currency does not need to be legal tender of any nation; however, the Australian legislature may limit the meaning of currency in its legislation.[312] If currency did possess a meaning similar to legal tender, the legislature would struggle to regulate and control money other than Australian currency (money issued under the *Currency Act 1965* (Cth) and the *Reserve Bank Act 1959* (Cth)).[313]

Proposition 6: Legal tender is a nation's prescribed currency.[314] It is normally created, issued, and regulated by legislation and a government entity, typically as a Central Bank.

Diagram 15 – Categories of money, currency, and legal tender



From these propositions, this dissertation will examine whether UTXOs amount to 'money', 'currency', or 'legal tender' for Australian legal purposes.

[310] Ibid.
[311] See *Leask* (n 259) 31 (Gummow J); Cf *Leask* (n 259) 10 (Brennan CJ).
[312] See *Leask* (n 259) 10 (Brennan CJ).
[313] *Watson* (n 248) 482 (Stephen J).
[314] *Leask* (n 259) 31 (Gummow J); *Travelex* (n 287) [33] (per Emmett J).

D *Application to Bitcoin concepts*

Chapter 3 demonstrates that unspent transaction outputs ('UTXOs') on most full nodes amount to separate proprietary interests. Following from Proposition 1 above, UTXOs are not prima facie excluded from being money, currency, or legal tender.

1 *UTXOs are money*

Proposition 2 states that a 'thing' that fulfills the function of money and meets the definition provided in the Moss case will be money under the broadest meaning of the term. The 'functional approach' to money refers to the ability of money to act as:

(a) a measure of value or unit of account,
(b) a means of payment,
(c) a medium of exchange, and
(d) a store of value.[315]

(a) Measure of value or unit of account

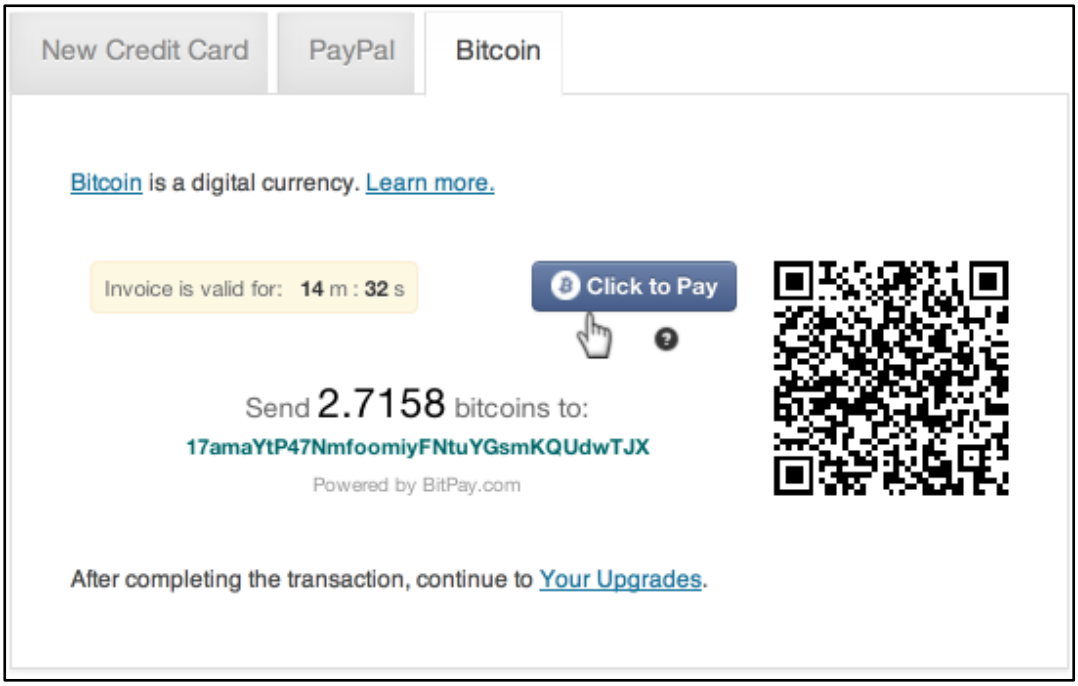
Money as a unit of account refers to the 'numerical measure of value' used to record income or wealth, and price goods, services, or debts.[316] The unit of account for UTXOs is 'bitcoin', however there is no distinguishable piece of data that identifies a particular 'bitcoin' as a discrete digital 'coin'.[317] This is because a UTXO is an encoded alphanumeric string containing details such as output information, which specifies the 'value' in bitcoin to be associated with a particular public key.[318] If the output information indicates that a UTXO is attributed with a set number of bitcoin, the measure of the UTXO's value is that number of bitcoin.

Mooning Market is an example of one of over a hundred of thousand businesses that accepts bitcoin in exchange for goods and services.[319] Like other online marketplaces,[320] Mooning Market offers a range of items that are priced in bitcoin, such as laptops, furniture, clothing, and real estate. As early as 2015, there has been a growing trend where, even though established businesses may price goods and services in Australian dollars, they also accept bitcoin payments through bitcoin payment processors.[321] Some of the companies that use these

[315] Georgios Zekos, 'Economics and Legal Understanding of Virtual Currencies' (2019) 38(8) *Banking & Finance Services Policy Report* 1; Geoffrey Ingham, *Money* (Polity Press, 1st ed, 2020) 11.
[316] Ingham (n 315) 11.
[317] See Nakamoto (n 3) 5; Antonopoulos (n 2) ch 6.
[318] See Antonopoulos (n 2) ch 6.
[319] Online Blockchain PLC, 'The Crypto Marketplace', *Mooning Market* (Web Page, 19 September 2021) <https://mooningmarket.com/>; See *United States v Harmon*, 474 F Supp 3d 76 (D Wash, 2020) 88-9.
[320] Such as Amazon and eBay.
[321] *United States v Harmon*, 474 F Supp 3d 76 (D Wash, 2020) 88-9. The integration of the bitcoin payment processor, Payfast, in South Africa is also discussed in Annamart Nieman, 'A Few South African Cents' Worth On Bitcoin' (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979, 1993. See also the uptake of Bitpay and other Bitcoin merchant service providers in: Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Report, 3 May 2016) <https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf> 11-2.

payment processors include Dell,[322] Microsoft,[323] WordPress,[324] Virgin Galactic,[325]and the largest American telecommunications company, AT&T.[326] An example of the WordPress payment options is shown in Diagram 16.

Diagram 16 – WordPress subscription denominated in bitcoin[327]



While the Reserve Bank of Australia ('RBA') acknowledges that some businesses accept bitcoin, the regulator observes that Australian dollars are the primary method to price goods and services.[328] As bitcoin is not the primary unit of account for goods and services in Australia, the RBA does not regard that bitcoin displays key characteristics of money.[329] However, this strict interpretation – that a thing is only money in Australia if it is the primary unit of account – would mean that foreign currency is also not regarded as money.

This dissertation disagrees with that statement as it would conflict with Proposition 3 ('Money does not need to be the legal tender of any nation'). Consequently, a UTXO's output information (the value in bitcoin) is a unit of account as bitcoin is used to price goods, services,

---

[322] Mike Flacy, 'Dell, Newegg start accepting Bitcoin as payment', *digitaltrends.com* (Blog Post, 19 July 2014) <https://www.digitaltrends.com/web/dell-newegg-start-accepting-bitcoin-payment/>.
[323] As early as 2014, Microsoft accepted bitcoin as a means of payment: Jonathan Vanian, 'Microsoft Welcomes Back Bitcoin', *Fortune* (online, 11 January 2018) <https://fortune.com/2018/01/10/microsoft-bitcoin-temporary-halt/>.
[324] Andy Skelton, 'Pay Another Way: Bitcoin', *WordPress.com* (Blog Post, 15 November 2012) <https://wordpress.com/blog/2012/11/15/pay-another-way-bitcoin/>.
[325] @richardbranson (Richard Branson) (Twitter, 22 November 2013, 11:20pm AEST) <https://twitter.com/richardbranson/status/403875534339203073>; Matthew Belvedere, 'Richard Branson: Buy your space flight with bitcoin', *CNBC* (online, 22 November 2013) <https://www.cnbc.com/2013/11/22/virgin-galactic-to-accept-bitcoin-branson.html?&qsearchterm=bitcoin%20virgin>.
[326] AT&T, 'AT&T Now Accepts BitPay', *About* (Web Page, 23 May 2019) <https://about.att.com/story/2019/att_bitpay.html>.
[327] Image sourced from Andy Skelton, 'Pay Another Way: Bitcoin', *WordPress.com* (Blog Post, 15 November 2012) <https://wordpress.com/blog/2012/11/15/pay-another-way-bitcoin/>.
[328] Reserve Bank of Australia, 'What are cryptocurrencies', *Cryptocurrencies* (Web Page, 19 September 2021) <https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html>.
[329] Ibid.

and debts.

(b) Means of payment and medium of exchange

Money as a means of payment refers to the ability of a thing to be accepted as a method for settling a debt denominated in that unit of account.[330] Money as a medium of exchange refers to the thing providing a 'convenient proxy or method to facilitate the effective exchanges of goods and services'.[331]

UTXOs are intangible property, like bank deposits denominated in hard currencies, shares or debts. A person who controls a UTXO may access, redeem, and use it for several reasons, including paying for goods and services, settling monetary obligations, investing, or conducting a business. Australian case law does not indicate that there is any requirement for a thing to be solely used as a method for settling monetary obligations. Rather, the thing only needs to be accepted as a method for settling monetary obligations.

Given that many transactions on the Bitcoin network are private, it is difficult to identify the extent to which a UTXO is accepted as a means of payment. This is because the information recorded on each Bitcoin blockchain outlines the time of the transaction, the transferor bitcoin address, transaction value (in bitcoin), and the recipient bitcoin address. It does not record the purpose for the transaction. However, there are companies that have conducted quantitative and qualitative analysis into this information and cross-referenced the data with entities connected with particular bitcoin addresses. On 30 March 2020, for example, Chainalysis published its insights into the value of bitcoin being sent to merchant services between 19 July 2019 and 19 March 2020.[332]

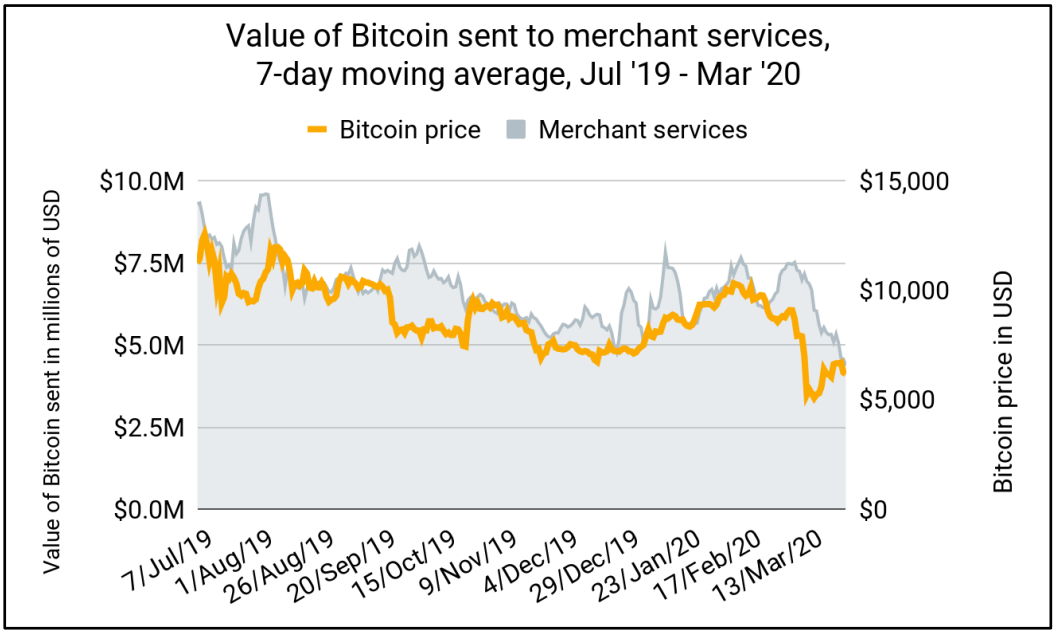
The company derives insights by applying clustering techniques to a version of the Bitcoin blockchain and other public-source information to identify patterns of behaviour, types of users on the network, and other observable groupings. 'Clustering' is the established 'multivariate statistical procedure' through which datasets are partitioned and reorganised so that classifications for highly similar entities can be created.[333] It is a procedure fundamental to almost every field of study. For example, in biology the taxonomy of living creatures is based on observable differences and similarities that give rise to discrete groupings and provide insights into each group's potential evolutionary process.[334]

Similarly, for the purpose of Chainalysis's analysis, clustering was used to distinguish between individuals who retained bitcoin as an investment versus those who redeemed their bitcoin

[330] Ingham (n 315) 11.
[331] Charles Proctor, *Mann on the Legal Aspects of Money* (Oxford University Press, 7th ed, 2012) 10; See also Geoffrey Ingham, *Money* (Polity Press, 1st ed, 2020) 12. Other proxies for value include 'air miles, credit card points, retail loyalty or reward points, [and] coupons': Annamart Nieman, 'A Few South African Cents' Worth On Bitcoin' (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979, 1981.
[332] Chainalysis Team, 'Covid-19 is Changing the Relationship Between Bitcoin Price and Bitcoin Spending', *Insights* (Web Page, 30 March 2020) <https://blog.chainalysis.com/reports/covid-19-bitcoin-price-bitcoin-spending>. Chainalysis is a blockchain analysis company that provides 'data, software, services, and research to government agencies, exchanges, financial institutions, and insurance and cybersecurity companies in over 60 countries. Our data platform powers investigation, compliance, and risk management tools that have been used to solve some of the world's most high-profile cyber criminal cases and grow consumer access to cryptocurrency safely': https://www.chainalysis.com/.
[333] Brian Everitt et al, *Cluster Analysis* (John Wiley & Sons Ltd, 5th ed, 2011) 5.
[334] Everitt et al (n 333) 2; See also Mark Aldenderfer and Roger Blashfield, *Cluster Analysis* (SAGE, 1984) 8.

through merchant services for goods and services.[335] As highlighted by Diagram 17 below, the seven day moving average value of bitcoin redeemed through merchant services over the period 7 July 2019 to 13 March 2020 fluctuated between USD3,000,000 and USD9,000,000.[336] This demonstrates that there are businesses routinely accepting bitcoin as a means of payment.

Diagram 17 – Redemption of bitcoin through merchant services[337]



Chainalysis also suggests that 'users are buying essentials via merchant services that they [cannot] get elsewhere with fiat currency'.[338] In the wake of COVID-19:

> The need for merchant services could be augmented by local business closures in areas hit especially hard by Covid-19. Business services such as web hosting, which tend to have recurring payment plans, are also widely available via merchant services — spending on those services from pre-existing contracts could also be backstopping the category as a whole.[339]

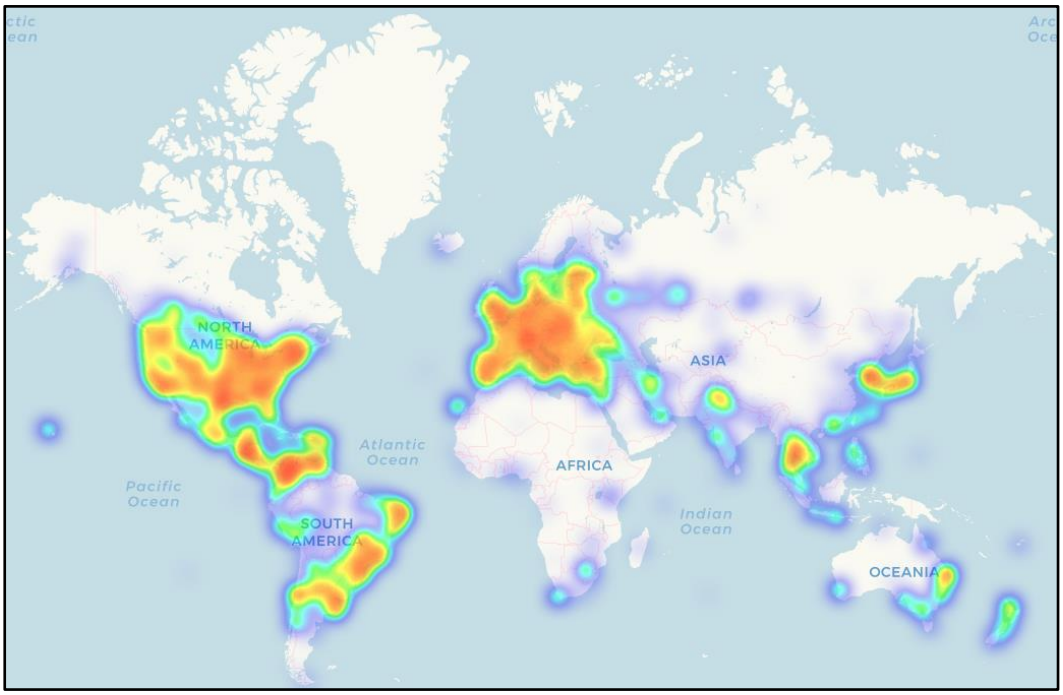
Several authors highlight that the increase in online marketplaces and global business has meant that currencies issued by nations are not as necessary to conduct those businesses. Bitcoin offers a cost-effective means of transacting beyond any one nation's borders, accessing capital, and escaping oppressive financial regimes.[340]

Many Venezuelans are desperately adopting bitcoin in their businesses to protect their savings following record-high inflation rates that threaten to render their local currency, the bolivar,

[335] Chainalysis Team, 'Covid-19 is Changing the Relationship Between Bitcoin Price and Bitcoin Spending', *Insights* (Web Page, 30 March 2020) <https://blog.chainalysis.com/reports/covid-19-bitcoin-price-bitcoin-spending>.
[336] Ibid.
[337] Image sourced from Chainalysis Team (n 335).
[338] Chainalysis Team (n 335).
[339] Ibid.
[340] Annamart Nieman, 'A Few South African Cents' Worth On Bitcoin' (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979, 1988; Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Report, 3 May 2016) 10—11, 14—5 <https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf>.

worthless.[341] Kevin Rand, commentator at *Forbes*, highlights how 'cash-strapped governments are taking notice' of Bitcoin and implementing measures to promote the use of Bitcoin in struggling economies.[342] As demonstrated by Diagram 18, the uptake of bitcoin by businesses globally is not insignificant.[343] Coinbase, a well-known bitcoin payment processor, purports that it services over 8,000 merchants around the world.[344]

Diagram 18 – Heatmap of Bitcoin retailers by Coinmap.org on 4 October 2021[345]



The RBA, on the other hand, claims that its survey research indicates 'that only a small fraction of bitcoin holders use them regularly for payments'.[346] Based on the evidence outlined above, this dissertation questions the accuracy of this research. While the details of this survey have not been published, there is inherent bias that may arise using this methodology due to the sample size, individuals sampled, and response rate. For example, if the individuals sampled are only from a particular geographical region, the data captured will not reflect global usage trends. For a borderless payment system like Bitcoin, this bias could be the difference between its treatment as money or not. Without knowing the parameters of the survey, it is impossible to determine whether the results are biased. Therefore, this dissertation uses the cryptocurrency data outlined above. From this, more accurate representations of behaviours on the Bitcoin blockchain can be achieved even where the users are not identified.

---

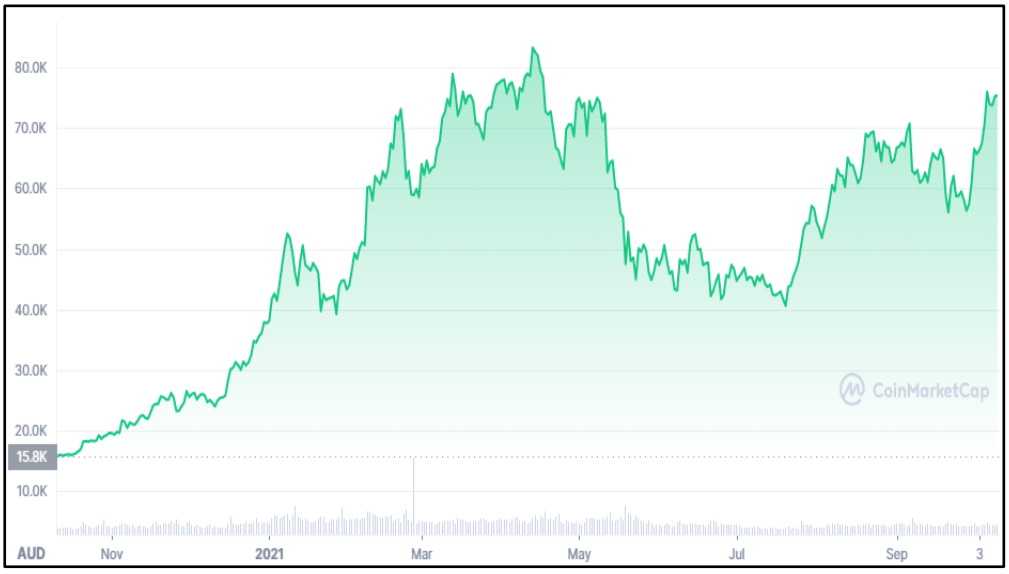
[341] Kevin Rand, 'Why Venezuela's Currency Crisis Is A Case Study For Bitcoin', *Forbes* (online, 17 October 2021) <https://www.forbes.com/sites/realspin/2017/02/03/why-venezuelas-currency-crisis-is-a-case-study-for-bitcoin/?sh=717efd7419b2>. See also Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Report, 3 May 2016) 16 <https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf>.
[342] Ibid; See also Brian Ellsworth, 'As Venezuela's economy regresses, crypto fills the gaps', *Thomson Reuters* (online, 17 October 2021) <https://www.reuters.com/technology/venezuelas-economy-regresses-crypto-fills-gaps-2021-06-22/>.
[343] As of 27 October 2021, there are 27,918 businesses registered with Coinmap: Coinmap, *Coinmap.org* (Web Page, 27 October 2021) <https://coinmap.org/view/#/world/20.79720143/25.66406250/2>.
[344] Coinbase, 'Commerce', *Business* (Web Page, 27 October 2021) <https://commerce.coinbase.com/>.
[345] Coinmap, *Coinmap.org* (Web Page, 27 October 2021) <https://coinmap.org/view/#/world/20.79720143/25.66406250/2>.
[346] Reserve Bank of Australia, 'What are cryptocurrencies', *Cryptocurrencies* (Web Page, 19 September 2021) <https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html>.

Based on the transaction values, pervasive uptake by payment processors, and integration with businesses globally, this dissertation concludes that a UTXO is a means of payment. Consequently, UTXOs are also an effective method through which goods and services can be exchanged between individuals, akin to promissory notes and bank transfers.

(c) Store of value

Money as a store of value means that the thing's 'purchasing and debt settling power' is retained between its original receipt and later use as a means of payment.[347] Like global currency exchange rates, the value of bitcoin is dictated by the global market and fluctuates in response to market demand.[348] The RBA highlights that 'large fluctuations in the price of bitcoin reduce its effectiveness as a store of value'.[349] As expressed above, it is unclear on what data this statement is based. One view may be that the value of bitcoin when compared to Australian dollars varies by a degree which may render a UTXO ineffective in maintaining value over time. These fluctuations can be seen in Diagram 19, which highlights how the value of bitcoin in Australian dollars steadily rose to AUD80,000 per bitcoin followed by a drop to AUD40,000 and a resurgence back to AUD75,000.[350]

Diagram 19 – AUD/BTC (bitcoin): 9 October 2020 to 10 October 2021[351]



When Australian dollars are compared to the United States dollar, one can see significantly less variation. For example, in Diagram 20 below, the value of an Australian dollar fluctuates by 8 cents over the same period.

[347] Geoffrey Ingham, *Money* (Polity Press, 1st ed, 2020) 12.
[348] Russ Marshall, 'Bitcoin: Where Two Worlds Collide' (2015) 27(1) *Bond Law Review* 89, 94.
[349] Reserve Bank of Australia, 'What are cryptocurrencies', *Cryptocurrencies* (Web Page, 19 September 2021) <https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html>.
[350] CoinMarketCap OpCo, LLC, 'Bitcoin', *CoinMarketCap* (Web Page, 19 September 2021) <https://coinmarketcap.com/currencies/bitcoin/>.
[351] Ibid.

Diagram 20 – AUD/USD (United States dollar): 9 October 2020 to 10 October 2021[352]

However, this approach only reflects the exchange rate between bitcoin and a hard currency. As highlighted in Diagram 21 below, the Icelandic krona experienced significant fluctuations in its exchange rate when compared to the Australian dollar. Between November 2020 and April 2021, the value of AUD1 fluctuated between IDR10,300 and IDR11,300.

Diagram 21 – AUD/IDR (Icelandic krona): 9 October 2020 to 10 October 2021[353]

Exchange rates are not the only means to measure whether a thing is an effective store of value.

[352] Thomson Reuters, 'Currencies' *Markets* (Web Page, 10 October 2021) <https://www.reuters.com/markets/currencies>.
[353] Ibid.

Inflation occurs when there is an 'undue expansion or increase of the currency of a country' which forces 'a substantial rise of prices' due to the expectation that the currency is now worth less than before.[354] The extreme form of this expansion, hyperinflation, occurs when 'general price rises reach such unusually high levels that the currency tends to become no longer able to perform its normal functions in part or wholly'.[355]

For example, throughout the 1913 civil war in Mexico, the government issued additional paper notes to fund its war campaigns. Liping He, author of *Hyperinflation: A World History*, notes '[i]n a period of 47 months to December 1916, general prices rose 107-fold, with the annual increase rate reaching as high as 7,716,100 percent at one point'.[356] Mexico is one of many nations that have been subject to hyperinflation. As highlighted in Diagram 22, during the 1920s alone, developed nations such as Germany and Russia experienced significant devaluation to their local currencies.

Diagram 22 – Table 3.1 from *Hyperinflation: A World History*[357]

Table 3.1 Hyperinflations in Germany, Russia, and CEE countries during the 1920s[4]

	Start date	*End date*	*Highest monthly inflation rate*	*Month with highest inflation rate*	*Currency*	*Indicator of inflation*
Germany	Jan 1920	Jan 1920	56.9 percent	Jan 1920	Papiermark	WPI
	Aug 1922	Dec 1923	29,500 percent	Oct 1923	Papiermark	WPI
Russia/USSR	Jan 1922	Feb 1924	212 percent	Feb 1924	Ruble	CPI
Austria	Oct 1921	Sep 1922	129 percent	Aug 1922	Crown	CPI
Hungary	Mar 1923	Feb 1924	97.9 percent	Jul 1923	Crown	CPI
Poland	Jan 1923	Jan 1924	275 percent	Oct 1923	Marka	WPI

As addressed earlier, Venezuela is experiencing record-high inflation rates which threaten to render the bolivar worthless, forcing its citizens to identify and adopt alternative forms of payment, like Bitcoin.[358]

Therefore, this dissertation concludes that no single indicator (such as exchange rates or inflation) determines whether something is an effective store of value. While the AUD/BTC exchange rate fluctuates more than the AUD/USD exchange rate, the uptake and pervasive use of bitcoin by merchant services indicates that bitcoin demonstrates some ability to act as a store of value even if that value is subject to speculation.[359]

(d) Money as defined by Australian common law

Australian common law indicates that a thing may be money if it is:

[354] *Macquarie Dictionary* (online at 17 October 2021) 'inflation' (def 1, 2a).
[355] Liping He, *Hyperinflation: A World History* (Routledge, 1st ed, 2018) 1.
[356] Liping He (n 355) 52.
[357] Ibid.
[358] Kevin Rand, 'Why Venezuela's Currency Crisis Is A Case Study For Bitcoin', *Forbes* (online, 17 October 2021) <https://www.forbes.com/sites/realspin/2017/02/03/why-venezuelas-currency-crisis-is-a-case-study-for-bitcoin/?sh=717efd7419b2>.
[359] Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Report, 3 May 2016) 21 <https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf>.

(a) passed freely from hand to hand or is a medium of exchange,[360]
(b) accepted throughout a community as a means of payment,[361]
(c) accepted without reference to the character or credit of the offeror,[362] and
(d) tendered on to others as a means of payment by recipients.[363]

Earlier paragraphs have examined the extent to which a UTXO is a medium of exchange and concluded that a UTXO facilitates the exchange of goods and services.

The nature of a UTXO as a means of payment has been considered above, however Australian common law dictates that money must be 'accepted throughout a community'. The meaning of 'community' is not defined in Australian legislation, and its definition for common law purposes has not been explored.

On one view, it may refer to 'a body of people who live in the same place', locality or country.[364] From as early as 2015 onwards, Bitcoin has been accepted in some geographical communities, such as Venezuela,[365] Cape Town,[366] and the United States.[367] An alternative view is that 'community' has changed over time to mean 'a group of people who share the same interests, pursuits, or occupation, [which is] distinct from those of the society in which they live'.[368] It may also refer to a group of individuals on an online facility.[369] Under this interpretation, the global use of UTXOs would be captured as the individual users would form part of the online Bitcoin community, which is distinct from their geographical community. This approach to the meaning of 'community' is also consistent with Proposition 3, that money need not be the legal tender of any nation. Therefore, under either interpretation, UTXOs are accepted throughout a community.

The Moss and Messenger cases also require that evidence be produced that a thing is accepted by recipients without enquiring into the character or credibility of the issuer.[370] Due to the structure of Bitcoin transactions, the only information known to a recipient is: the time of the transaction, the transferor bitcoin address, the transaction value (in bitcoin), and the recipient bitcoin address.[371] The transaction does not require the issuer to provide their name, address, or other personal identifiers. Consequently, this element of the Australian common law test for money is satisfied.

---

[360] *Moss* (n 233) 116; *Bank Nationalisation* (n 242) 100.
[361] *Miller* (n 225) 457 (per Lord Mansfield); *Moss* (n 233) 116; *Bank Nationalisation* (n 242) 100; *Messenger* (n 267) [196]; *Travelex* (n 287) [25] (per Emmett J).
[362] *Messenger* (n 267) [196].
[363] *Moss* (n 233) 116.
[364] *Oxford English Dictionary* (online at 10 October 2021) 'community' (def 2b).
[365] Kevin Rand, 'Why Venezuela's Currency Crisis Is A Case Study For Bitcoin', *Forbes* (online, 17 October 2021) <https://www.forbes.com/sites/realspin/2017/02/03/why-venezuelas-currency-crisis-is-a-case-study-for-bitcoin/?sh=717efd7419b2>. See also Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Report, 3 May 2016) 16 <https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf>.
[366] See Annamart Nieman, 'A Few South African Cents' Worth On Bitcoin' (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979, 1988.
[367] *United States v Harmon*, 474 F Supp 3d 76 (D Wash, 2020) 88-9.
[368] *Oxford English Dictionary* (online at 10 October 2021) 'community' (def 5b, 8).
[369] *Oxford English Dictionary* (online at 10 October 2021) 'community' (def 5b, 8).
[370] *Moss* (n 233) 116 (Darling J); *Messenger* (n 267) [196].
[371] Antonopoulos (n 2) ch 9.

This dissertation therefore concludes that UTXOs are money for Australian legal purposes.

2 *UTXOs are currency*

On 8 June 2021, the Legislative Assembly of the Republic of El Salvador approved the introduction of the 'Bitcoin Law',[372] which decrees that El Salvador accepts bitcoin as legal tender.[373] As Proposition 6 proposes that legal tender is a nation's prescribed currency, UTXOs denominated in bitcoin must be currency. For completeness, this dissertation also considers that UTXOs satisfied the broadest definition of currency prior to this decree. As outlined by Proposition 5, UTXOs are a form of circulating money denominated in a recognised unit of account. Therefore, it must have been currency prior to the Bitcoin Law.

3 *UTXOs are not Australian legal tender*

Legal tender for Australian legal purposes is governed by the *Currency Act 1965* (Cth) and the *Reserve Bank Act 1959* (Cth) (and each Act's statutory predecessors).

Subsection 16(1) of the *Currency Act 1965* (Cth) states that 'a tender of payment of money is a legal tender if it is made in coins that are made and issued under this Act and are of current weight'. Under section 8 and Part 3 of the *Currency Act 1965* (Cth), the Treasurer is granted the power to make and issue coins of a specified composition and in denominations of the currency of Australia (ie, the dollar and cent). As UTXOs are not issued by the Treasurer under this Act nor meet the specified composition requirements under Part 3 and the Schedule of the *Currency Act 1965* (Cth), UTXOs are not legal tender under the *Currency Act 1965* (Cth).

Similarly, subsection 36(1) of the *Reserve Bank Act 1959* (Cth) states that 'Australian notes are a legal tender throughout Australia'. An 'Australian note' means a note issued under the *Australian Notes Act 1910* (Cth), Part VII of the *Commonwealth Bank Act 1911* (Cth), Part VI of the *Commonwealth Bank Act 1945* (Cth), or under Part V of the *Reserve Bank Act 1959* (Cth). As sections 34, 43 and 44 of the *Reserve Bank Act 1959* (Cth) restrict the making and issuing of Australian notes to the Reserve Bank of Australia, UTXOs will also not fall under this definition of legal tender for Australian legal purposes.

Perhaps the simplest conclusion in this Chapter is the determination that UTXOs are not Australian legal tender.

E *Conclusion*

While most nations currently use a form of coinage or note as their prescribed currency, historically, an array of tangible and intangible things have been adopted to facilitate the exchange of goods and services, settle monetary obligations and measure wealth. Even Australia, which introduced the 'Australian dollar' in 1966, has adopted objects one would not typically consider money, such as rum bottles.

---

[372] *Ley Bitcoin* [Bitcoin Law] (El Salvador), Decree No. 57, 8 June 2021 <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf>.

[373] Ibid. See also @Nayibbukele, 'I've just sent the #BitcoinLaw to Congress' (Twitter, 9 June 2021, 11:49AM) <https://twitter.com/nayibbukele/status/1402442597235310596>.

Despite this rich evolution where money has taken many forms, Australian courts have been reluctant to define 'money' and 'currency'. A review of Anglo-Australian case law indicates that money must be a form of property, but it need not be the legal tender of any nation. Provided that the thing, as tangible or intangible property, fulfills the function of money throughout a community and meets other bespoke qualities, Australian courts appear to regard it as such. For example, while bank notes, bank deposits, and inter-bank transfers are not legal tender, they are recognised as money by commerce and accepted as a means of payment throughout communities.

Like bank transfers, unspent transaction outputs ('UTXOs') perform all the functions of money, and there is quantitative analysis from recognised blockchain analysis companies that affirm the widespread acceptance of bitcoin in everyday business globally. While there is ongoing speculation regarding bitcoin's ability to retain its value over time, citizens from countries with currencies suffering from hyperinflation are converting to bitcoin to prevent their wealth from depreciating. These factors suggest that, despite such criticisms, UTXOs are treated as money in geographical and online communities.

The term 'currency' refers to circulating money, as opposed to money passing as antiquity, and must be denominated in a unit of account. This dissertation explored how bitcoin, the unit of account associated with UTXOs, widely circulate through different communities. It concludes that UTXOs clearly satisfy the definition of 'money' and 'currency'. Comparatively, 'legal tender' is a narrow tender referring to the prescribed money of a nation. Legal tender for Australian legal purposes is governed by the *Currency Act 1965* (Cth) and the *Reserve Bank Act 1959* (Cth). Neither of these Acts regard bitcoin or UTXOs as Australian legal tender.

F *Further considerations*

The nature of UTXOs as currency is a contentious issue for Australian taxation purposes.

Division 775 of the *Income Tax Assessment Act 1997* (Cth) ('ITAA 1997') ('the forex rules') outlines when and how foreign currency gains or losses are recognised for income tax purposes. Broadly, a foreign currency gain or loss is brought to account when the gain or loss is 'realised'. For example, if an entity acquires a foreign currency for AUD100 and sells it for AUD200, the sale of the foreign currency would be regarded as the time of realisation, and the Australian dollar value of the gain made would be declared in the entity's income tax return. Conversely, where a loss is made, the entity could claim a deduction.[374]

While foreign currency is regarded as a CGT asset for the purpose of the capital gains tax (CGT) regime,[375] and may therefore give rise to a capital gain or capital loss following a CGT event, the forex rules override the application of the CGT regime.[376] This means that any double taxation that may arise as a result of the application of the CGT regime and forex rules is negated so that only the gain or loss arising from the forex rules is considered for income tax purposes.[377]

[374] *Income Tax Assessment Act 1997* (Cth) s 775-30.
[375] *Income Tax Assessment Act 1997* (Cth) Note 1 in s 108-5.
[376] *Income Tax Assessment Act 1997* (Cth) sub-s 775-15(4).
[377] Ibid.

This is a critical distinction as an entity that makes a capital loss under the CGT regime can only use that loss to offset capital gains.[378] Specifically, if an entity derives ordinary income (such as salary and wages), any capital losses made from a CGT asset cannot be used to reduce that income.[379] The forex rules, however, treat foreign currency losses as allowable deductions.[380] Consequently, if an entity makes a loss on foreign currency, this loss could be used to reduce their taxable income.[381]

While the Australian Taxation Office (ATO) regards bitcoin as a CGT asset, it also published Taxation Determination TD 2014/25 *Income tax: is bitcoin a 'foreign currency' for the purposes of Division 775 of the Income Tax Assessment Act 1997?* (TD 2014/25), which outlines that the regulator does not regard bitcoin as foreign currency for the purpose of the forex rules. 'Foreign currency' under the ITAA 1997 means 'a currency other than Australian currency'.[382] Paragraphs 27 of TD 2014/25 propounds that:

> Parliament chose to define 'foreign currency' as the antithesis of 'Australian currency'. Therefore it is necessary to consider what the ITAA 1997 means by 'Australian currency' in order to determine in what sense the term 'currency' is being used within the definition of foreign currency.[383]

According to the ATO, 'Australian currency' refers to the 'currency of Australia' as prescribed by subsection 8(1) of the *Currency Act 1965* (Cth): the Australian dollar.[384] Following the Leask case and Proctor,[385] the ATO regarded 'currency' for the purpose of the forex rules as 'a currency legally recognised and adopted under the laws of a country as the monetary unit and means of discharging monetary obligations for all transactions and payments in that country'.[386]

This view was recently considered and approved by the Administrative Appeals Tribunal in *Seribu Pty Ltd v Commissioner of Taxation* [2020] (the Seribu case).[387] Deputy President McCabe, however, incorrectly stated that 'foreign currency' under the ITAA 1997 meant 'a currency other than **an** [sic] Australian currency'.[388] After considering the Leask case, the Deputy President concluded that:

> the reference to "an Australian currency" is plainly a reference to the unit of exchange established in the Currency Act, and the reference to "[an]other currency" must be interpreted in light of that comparator. It follows the "other currency" in question must be an official currency issued or recognised by a sovereign state.
> [389]

---

[378] See *Income Tax Assessment Act 1997* (Cth) sub-ss 8-1(2)(a), 102-10(2).
[379] *Income Tax Assessment Act 1997* (Cth) sub-ss 8-1(2)(a), 102-10(2).
[380] *Income Tax Assessment Act 1997* (Cth) s 775-30.
[381] *Income Tax Assessment Act 1997* (Cth) ss 8-5, 12-5, 775-30.
[382] *Income Tax Assessment Act 1997* (Cth) sub-s 995-1(1).
[383] Taxation Determination TD 2014/25 *Income tax: is bitcoin a 'foreign currency' for the purposes of Division 775 of the Income Tax Assessment Act 1997?* ('*TD 2014/25*')
[384] *TD 2014/25* (n 383) [31].
[385] *TD 2014/25* (n 383) [23].
[386] *TD 2014/25* (n 383) [32].
[387] [2020] AATA 1840 ('*Seribu*').
[388] *Seribu* (n 387) [22] (emphasis added). The Deputy President included the word 'an', which does not appear in the definition provided in subsection 995-1(1) of the ITAA 1997.
[389] *Seribu* (n 387) [29].

There are several issues with this judgment.

Firstly, Deputy President McCabe introduced the word 'an', which does not appear in the definition of a foreign currency under subsection 995-1(1) of the ITAA 1997. This additional term influences the interpretation of the provision as emphasis is now placed on a currency other than '*an Australian* currency' rather than currency 'other than Australian currency'. 'Other than' means 'different from in nature or kind',[390] or 'besides, except, apart from'.[391] Therefore, 'foreign currency' must mean 'a currency apart from Australian currency'.

Secondly, the Deputy President has reached a conclusion based on the fallacy of composition. This fallacy occurs when one mistakenly reasons that the 'attributes of an individual member of some collection' represent the 'attributes of the totality of that collection'.[392] Deputy President McCabe states that, as Australian currency refers to the legal tender of Australia, the term 'currency' must refer to the legal tender of other nations.[393] This dissertation respectfully disagrees with this statement. A 'currency other than Australian currency' unambiguously means any other currency (prescribed or un-prescribed) except for Australian currency. Under this interpretation, bitcoin would meet the definition of a 'foreign currency' for the purpose of the forex rules.

Finally, on 8 June 2021, the Legislative Assembly of the Republic of El Salvador approved the introduction of the 'Bitcoin Law',[394] which decrees that El Salvador accepts bitcoin as legal tender.[395] Consequently, even under TD 2014/25 and the Seribu case, bitcoin satisfies the definition of a 'foreign currency' from the date that the decree takes effect.

---

[390] *Macquarie Dictionary* (online at 19 October 2021) 'other' (def 15).
[391] *Oxford English Dictionary* (online at 19 October 2021) 'other' (def 5e).
[392] Siu-Fan Lee, *Logic: A complete introduction* (Hodder & Stoughton, 1st ed, 2017) 74.
[393] *Seribu* (n 387) [29].
[394] *Ley Bitcoin* [Bitcoin Law] (El Salvador), Decree No. 57, 8 June 2021 <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf>.
[395] *Ley Bitcoin* [Bitcoin Law] (El Salvador), Decree No. 57, 8 June 2021, art 1 <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf>; See also @Nayibbukele, 'I've just sent the #BitcoinLaw to Congress' (Twitter, 9 June 2021, 11:49AM) <https://twitter.com/nayibbukele/status/1402442597235310596>].

V CONCLUSION

The law, lawyers, and regulators are struggling to keep pace with new financial technologies, namely Bitcoin. While several publications purport to provide concise, holistic explanations of Bitcoin, this dissertation highlights how these Bitcoin primers mislead communities and nations into adopting measures (such as tax policy) that disregard critical features of the Bitcoin network.

By exploring the mechanics that enable Bitcoin to function as a trustless, distributed payment system, this dissertation highlights that the unit of account, bitcoin, is associated with unspent transaction outputs ('UTXOs'). As each full node maintains its own version of the Bitcoin blockchain, multiple versions of a UTXO exist. By presenting the corresponding private/public keypair, an individual can access, redeem, and use the value attributed to that UTXO.

Under Australian law, an individual's right to redeem the value associated with a UXTO on a full node amounts to a proprietary interest. Consequently, an individual possesses duplicate UTXOs across all full nodes, and a separate proprietary right exists in relation to each of these UTXOs. For practical purposes, when an individual accesses, redeems and uses a UTXO on a full node, that person implicitly authorises the full node to re-transmit the transaction (and therefore exercise the right) on the individual's behalf to peer nodes. When redeemed and used in a transaction, the UTXO becomes functionless and new UTXOs are created.

An examination of the history of money, currency, and legal tender also demonstrates how flexible communities have been when accepting 'things' as media of exchange. Given that UTXOs meet the functional and Australian common law definition of the term 'money' and are widely circulating as a means of payment, UTXOs also satisfy the broadest definition of 'currency'. Comparatively, 'legal tender' is a statutory term referring to the prescribed, 'lawful money' of a nation. UTXOs are not legal tender in Australia as the lawful money of Australia is prescribed by the *Currency Act 1965* (Cth) and *Reserve Bank Act 1959* (Cth). However, due to the decree recently issued by the Legislative Assembly of the Republic of El Salvador, Bitcoin has been adopted as the legal tender of El Salvador.

As this dissertation departs from the views expressed by regulators such as the Australian Taxation Office ('ATO') and Reserve Bank of Australia ('RBA'), there are several taxation implications that are explored. This includes the significant administrative burdens faced by Australian taxpayers in applying the income tax laws to each redemption of a UTXO (and its duplications across the Bitcoin network); however, it is proposed that the legislature should seek to enact amendments to alleviate this burden.

Finally, Bitcoin is one of over ten thousand cryptocurrencies in existence. This dissertation highlights the consequences where the mechanics of *one* cryptocurrency are misconstrued. There is still more work to be done in understanding how the law applies to other unique forms of cryptocurrencies.

BIBLIOGRAPHY

A *Articles/Books/Reports*

Aldenderfer, Mark and Roger Blashfield, *Cluster Analysis* (SAGE, 1984)

Antonopoulos, Andreas M, *Mastering Bitcoin* (O'Reilly Media, Inc., 2nd ed, 2017)

Babie, Paul et al, 'Cryptocurrency as property: *Ruscoe v Cryptopia Ltd (in liq)* [2020] NZHC 728'(2020) 28 *Australian Property Law Journal* 106

Bambrough, Billy, '"$500,000 In Five Years" – Elon Musk and Tesla Devotee Cathie Wood Reveals Huge Bitcoin and Ethereum Price Predictions' *Forbes* (online, 15 September 2021) <https://www.forbes.com/sites/billybambrough/2021/09/15/500000-in-five-years-elon-musk-and-tesla-devotee-cathie-wood-reveals-her-huge-bitcoin-and-ethereum-price-prediction/?sh=670dadb35630>

Beechey, Emma, 'Blockchain and cryptocurrencies for barristers' (2018) *The Journal of the NSW Bar Association* 25

Belvedere, Matthew, 'Richard Branson: Buy your space flight with bitcoin', *CNBC* (online, 22 November 2013) <https://www.cnbc.com/2013/11/22/virgin-galactic-to-accept-bitcoin-branson.html?&qsearchterm=bitcoin%20virgin>

Brito, Jerry, and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Report, 3 May 2016) <https://www.mercatus.org/system/files/gmu_bitcoin_042516_webv3_0.pdf>

Cardozo, Benjamin, '"Ev'ry American Experiment Sets a Precedent": Why One Florida State Court's Bitcoin Opinion is Everyone's Business' (2016) 16 *Journal of International Business and Law* 6

Chambers, Robert, *An Introduction to Property Law in Australia* (Thomson Reuters, 4th ed, 2018)

Cohen, Bram, 'The BitTorrent Protocol Specification', *BitTorrent.org* (Technical Standard, 10 January 2008) <https://www.bittorrent.org/beps/bep_0003.html>

Council of Australian Law Deans, 'CALD Statement on the Nature of Research' (May and October 2005)

Davies, Glyn, 'History of Money' (University of Wales Press, 3rd ed, 2002)

Deutsch, R L, et al, *The Australian Tax Handbook* (Thomson Reuters, 1st ed, 2018)

Ellsworth, Brian, 'As Venezuela's economy regresses, crypto fills the gaps', *Thomson Reuters* (online, 17 October 2021) <https://www.reuters.com/technology/venezuelas-economy-regresses-crypto-fills-gaps-2021-06-22/>

Everitt, Brian et al, *Cluster Analysis* (John Wiley & Sons Ltd, 5th ed, 2011)

Garewal, Karan Singh, 'Practical Blockchains and Cryptocurrencies' (1st ed, 2020) Apress Media LLC

Feitelson, Dror G, Eitan Frachtenberg and Kent L. Beck, 'Development and Deployment at Facebook' (2013) 17(4) *IEEE Internet Computing* 1 <https://research.fb.com/wp-content/uploads/2016/11/development-and-deployment-at-facebook.pdf>

Fox, David, 'Cryptocurrencies in the Common Law of Property' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019)

Franco, Pedro, *Understanding Bitcoin*: *Cryptography, engineering, and economics* (Wiley, 1st ed, 2015)

Gray, Kevin, 'Property in Thin Air' (1991) 50 *Cambridge Law Journal* 252

Green, Sarah, 'Cryptocurrencies: the underlying technology' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019)

Green, Sarah, 'It's Virtual Money' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019)

Grinberg, Reuben, 'Bitcoin: An Innovative Alternative Digital Currency' (2012) 4 *Hastings Science & Technology Law Journal* 159

Hinchcliffe, Sarah A, 'Bitcoins – a bit of this and a bit of that' (2016) 19(1) *Internet Law Bulletin* 259

Hutchinson, Terry, and Nigel Duncan, 'Defining and describing what we do: doctrinal legal research' (2012) 17(1) *Deakin Law Review* 83

Ingham, Geoffrey, *Money* (Polity Press, 1st ed, 2020)

Kien-Meng Ly, Matthew, 'Coining Bitcoin's "Legal Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies' (2014) 27 *Harvard Journal of Law & Technology* 587

Kirby, Michael, 'Medical Technology and New Frontiers of Family Law' (1987) 1 *Australian Journal of Family Law* 196

Kreltszheim, David, 'The Legal Nature of "Electronic Money": Part 1' (2003) 14 *Journal of Banking and Finance Law and Practice* 161

Kreltszheim, David, 'Taking and enforcing security over cryptocurrency' (2018) 34(6) *Australian Banking & Finance Law Bulletin* 105

Kuroda, Akinobu, 'A Global History of Money' (Routledge, 1st ed, 2020)

Lee,Siu-Fan, *Logic: A complete introduction* (Hodder & Stoughton, 1st ed, 2017)

Liping He, *Hyperinflation: A World History* (Routledge, 1st ed, 2018)

Litwack, Seth, 'Bitcoin: Currency or Fool's Gold: A Comparative Analysis of the Legal Classification of Bitcoin' (2015) 29(2) *Temple International & Comparative Law Journal* 309

Ly, Matthew Kien-Meng, 'Coining Bitcoin's "Legal-Bits": Examining the Regulatory Framework for Bitcoin and Virtual Currencies' (2014) 27 *Harvard Journal of Law & Technology* 588

Mann, Francis, *The Legal Aspects of Money* (Oxford University Press, 5th ed, 1992)

Marshall, Russ, 'Bitcoin: Where Two Worlds Collide' (2015) 27(1) *Bond Law Review* 89

McGinnis, John O, 'Bitcoin's nature and its future' (2020) 43 *Harvard Journal of Law & Public Policy* 59

McNally, Cyrus, 'Bitcoin node count hits new all-time high' *CoinTelegraph* (online, 15 August 2021) <https://cointelegraph.com/news/bitcoin-node-count-hits-new-all-time-high>

Moses, Lyria Bennett, 'The Applicability of Property Law in New Contexts: From Cells to Cyberspace' (2008) 30 *Sydney Law Review* 639

Nakamoto, Satoshi, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Whitepaper, October 2008), <https://bitcoin.org/bitcoin.pdf>

Nieman, Annamart, 'A Few South African Cents' Worth On Bitcoin' (2015) 18(5) *Potchefstroom Electronic Law Journal* 1979

Nikias, Kyriaco, and Paul Babie, 'Legislators, judges, and the content of property: Reflections on *Hocking v Director-General, National Archives of Australia*' (2020) 28 *Australian Property Law Journal* 195

Proctor, Charles, 'Cryptocurrencies in International and Public Law Conceptions of Money' in David Fox and Sarah Green (eds), *Cryptocurrencies in Public and Private Law* (Oxford University Press, 2019)

Proctor, Charles, 'Mann on the Legal Aspects of Money' (Oxford University Press, 7th ed, 2012)

Rand, Kevin, 'Why Venezuela's Currency Crisis Is A Case Study For Bitcoin', *Forbes* (online, 17 October 2021) <https://www.forbes.com/sites/realspin/2017/02/03/why-venezuelas-currency-crisis-is-a-case-study-for-bitcoin/?sh=717efd7419b2>

Rountree, David, 'Champing at the Bitcoin: Bitcoin, Regulators and the Law' (2013) 32(4) *Communications Law Bulletin* 5

Rountree, David, 'The Taxing Business of Taxing Bitcoin' (2014) 33(4) *Communications Law Bulletin* 17

Smithin, John, *What is Money?* (Routledge, 1st ed, 2000)

UK Jurisdiction Taskforce, *Legal statement on cryptoassets and smart contracts* (Legal Statement, November 2019)

Vanian, Jonathan, 'Microsoft Welcomes Back Bitcoin', *Fortune* (online, 11 January 2018) <https://fortune.com/2018/01/10/microsoft-bitcoin-temporary-halt/>

Wong, Terence, 'Bitcoin deconstructed: Part 1 – Concepts and signposts' (2014) 30(4) *Australian Banking & Finance Law Bulletin* 70

Wong, Terence, 'Bitcoin deconstructed: Part 2 – Real and virtual worlds' (2014) 30(6) *Australian Banking & Finance Law Bulletin* 122

Wong, Terence, 'Bitcoin deconstructed: Part 3 – Market rollercoaster' (2014) 30(7) *Australian Banking & Finance Law Bulletin* 136

Wong, Terence, 'Bitcoin deconstructed: Part 4 – Underground dealings' (2014) 30(10) *Australian Banking & Finance Law Bulletin* 239

Young, Joseph, 'Bitcoin Investors Should Not Fear August 1 Chain Split', *CoinTelegraph* (Article, 26 July 2017) <https://cointelegraph.com/news/bitcoin-investors-should-not-fear-august-1-chain-split>

Zekos, Georgios, 'Economics and Legal Understanding of Virtual Currencies' (2019) 38(8) *Banking & Finance Services Policy Report* 1

B *Cases*

Australian Capital Television Pty Ltd v Commonwealth (No 2) (1992) 108 ALR 577

Australian Securities and Investments Commission v Ostrava Equities Pty Ltd [2015] FCA 425

B2C2 Ltd v Quoine Pte Ltd [2019] 4 SLR 17

Balsam & Lackner [2020] FCCA 1115

Bank of New South Wales v Commonwealth (1948) 76 CLR 1

BDI Capital LLC v Bulbul Investments LLC, 446 F Supp 3d 1127 (ND Ga, 2020)

Box v Commissioner of Taxation (1952) 86 CLR 387

Coco v AN Clark (Engineers) Ltd [1969] RPC 41

Colbeam Palmer Ltd v Stock Affiliates Pty Ltd (1968) 122 CLR 255

Commissioner of Stamp Duties (NSW) v Yeend (1929) 43 CLR 235

Commissioner of the Australian Federal Police v Bigatton [2020] NSWSC 245

Commonwealth of Australia v WMC Resources Ltd [1998] HCA 8

Conley & Anor v Commissioner of Taxation & Anor (1998) 81 FCR 24

Deputy Commissioner of Taxation v Conley and Others (1998) 158 ALR 229

Dow Jones & Company Inc v Gutnik [2002] HCA 56

Elsinora Global Ltd v Healthscope Ltd (No 2) [2006] FCA 18

Federal Commissioner of Taxation v United Aircraft Corporation (1943) 68 CLR 525

Halwood Corporation Ltd v Chief Commissioner of Stamp Duties (1992) 33 NSWLR 395

Keppell v Bailey (1834) 2 My & K 517

Messenger Press Proprietary Ltd v Federal Commissioner of Taxation [2012] FCA 756

Miller v Race (1758) 1 Burrow 452

Minister of State for the Army v Dalziell (1944) 68 CLR 261

Moss v Hancock [1899] 2 QB 111

National Provincial Bank Ltd v Ainsworth [1965] AC 1175

Potter v The Commissioner of Inland Revenue (1854) 156 ER 392

Powell v Christensen [2020] FamCA 944

Re Alberta Statutes [1938] SCR 100

Re Collings [1933] Ch 920

Re Toohey; Ex parte Meneling Station Pty Ltd (1982) 44 ALR 63

Ruscoe v Cryptopia Limited (in liq) [2020] NZHC 728

Saltman Engineering Co Ltd v Campbell Engineering Co Ltd [1963] 3 All ER 413

Securities and Exchange Commissioner v Shavers, (D Tex, No 4:13–CV–416, 18 September 2014)

Seribu Pty Ltd v Commissioner of Taxation [2020] AATA 1840

Skatteverket v David Hedqvist (Court of Justice of the European Union, C-264/14, 22 October 2015)

Travelex Limited v Commissioner of Taxation [2008] FCA 1961
Trinidad Lake Asphalt Operating Co Ltd v Commissioners of Income Tax for Trinidad (1945) AC 1

United States v Faiella, 39 F. Supp. 3d 544 (SD NY, 2014)

United States v Harmon, 474 F Supp 3d 76 (D Wash, 2020)

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

Uniting Church in Australia Property Trust (NSW) v Immer (No 145) Pty Ltd (1991) 24 NSWLR 510

Watson v Lee (1979) 144 CLR 374

Yanner v Eaton [1999] HCA 53

C *Legislation*

A New Tax System (Goods and Services Tax) Act 1999 (Cth)

Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth)

Auction Sales Act 1973 (WA)

Australian Notes Act 1910 (Cth)

Coinage Act 1909 (Cth)

Coinage Act 1936 (Cth)

Coinage Act 1947 (Cth)

Commonwealth Bank Act 1911 (Cth)

Commonwealth Bank Act 1945 (Cth)

Commonwealth of Australia Constitution Act 1901 (Cth)

Criminal Code Act 1995 (Cth)

Currency Act 1965 (Cth)

Fauna Conservation Act 1974 (Qld)

Financial Accountability Act 2009 (Qld)

Income Tax Assessment Act 1936 (Cth)

Income Tax Assessment Act 1997 (Cth)

Ley Bitcoin [Bitcoin Law] (El Salvador), Decree No. 57, 8 June 2021 <https://www.asamblea.gob.sv/sites/default/files/documents/decretos/8EE85A5B-A420-4826-ABD0-463380E2603B.pdf>

Native Title Act 1993 (Cth)

Reserve Bank Act 1959 (Cth)

Stamp Duties Act 1920 (NSW)

D *Treaties*

E *Other*

@Nayibbukele, 'I've just sent the #BitcoinLaw to Congress' (Twitter, 9 June 2021, 11:49AM) <https://twitter.com/nayibbukele/status/1402442597235310596>

@richardbranson (Richard Branson) (Twitter, 22 November 2013, 11:20pm AEST) <https://twitter.com/richardbranson/status/403875534339203073>

AT&T, 'AT&T Now Accepts BitPay', *About* (Web Page, 23 May 2019) <https://about.att.com/story/2019/att_bitpay.html>

Australian Taxation Office, 'Chain splits', *Transacting with cryptocurrency* (Web Page, 20 August 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?page=2#Chain_splits>

Australian Taxation Office, 'Cryptocurrency as an investment', *Transacting with cryptocurrency* (Web Page, 21 September 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?page=2#Cryptocurrency_as_an_investment>

Australian Taxation Office, 'Paying salary or wages in cryptocurrency', *Cryptocurrency used in business* (Web Page, 21 September 2021) <https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?page=3#Paying_salary_or_wages_in_cryptocurrency>

Australian Taxation Office, ‘Transacting with cryptocurrency’, *Tax treatment of cryptocurrencies* (Web Page, 19 September 2021) < https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/?anchor=Transactingwithcryptocurrency#Transactingwithcryptocurrency>

‘Bitcoin Core 0.11: Data Storage’ (Documentation, 17 August 2021) <https://en.bitcoin.it/wiki/Bitcoin_Core_0.11_(ch_2):_Data_Storage>

‘Bitcoin Core 0.11: The Blockchain’ (Documentation, 17 August 2021) <https://en.bitcoin.it/wiki/Bitcoin_Core_0.11_(ch_6):_The_Blockchain>

‘Bitcoin Core version history’, *BitcoinCore* (Web Page, 20 August 2021) <https://bitcoin.org/en/version-history>

Bitcoin Project, ‘Initial Block Download’, *Developer Guides: P2P Network* (Documentation, 2021) <https://developer.bitcoin.org/devguide/p2p_network.html>

Bitcoin Project, ‘Introduction’, *Developer Guides: Transactions* (Documentation, 18 August 2021) <https://developer.bitcoin.org/devguide/transactions.html>

Bitcoin Project, ‘Memory Pool’, *Developer Guides: P2P Network* (Documentation, 2021) <https://developer.bitcoin.org/devguide/p2p_network.html>

Bitcoin Project, ‘Peer Discovery’, *Developer Guides: P2P Network* (Documentation, 17 August 2021) <https://developer.bitcoin.org/devguide/p2p_network.html>

Bitcoin Project, ‘Unlocking a P2PKH Output for Spending’, *Developer Guides: Transactions* (Documentation, 18 August 2021) <https://developer.bitcoin.org/devguide/transactions.html>

Blockchain.com, ‘Bitcoin Explorer’ (Web Page, 23 September 2021) <https://www.blockchain.com/btc/blocks?page=1>

Blockchain.com, Inc., ‘Block 0’ *Blockchain.com* (Web Page, 30 August 2021) <https://www.blockchain.com/btc/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>

Blockchain.com, Inc., ‘Blocks’ *Blockchain.com* (Web Page, 20 August 2021) <https://www.blockchain.com/btc/blocks?page=1>

Chainalysis Team, ‘Covid-19 is Changing the Relationship Between Bitcoin Price and Bitcoin Spending’, *Insights* (Web Page, 30 March 2020) <https://blog.chainalysis.com/reports/covid-19-bitcoin-price-bitcoin-spending>

Coinbase, ‘Commerce’, *Business* (Web Page, 27 October 2021) <https://commerce.coinbase.com/>

Coinmap, *Coinmap.org* (Web Page, 27 October 2021) <https://coinmap.org/view/#/world/20.79720143/25.66406250/2>

CoinMarketCap OpCo, LLC, 'Bitcoin', *CoinMarketCap* (Web Page, 19 September 2021) <https://coinmarketcap.com/currencies/bitcoin/>

Flacy, Mike, 'Dell, Newegg start accepting Bitcoin as payment', *digitaltrends.com* (Blog Post, 19 July 2014) <https://www.digitaltrends.com/web/dell-newegg-start-accepting-bitcoin-payment/>

GR0KCHAIN, 'Understanding the data behind Bitcoin Core', *Bitcoin Developer Network* (Web Page, 25 September 2021) <https://bitcoindev.network/understanding-the-data/>

Macquarie Dictionary (online at 20 August 2021) 'blockchain' (def 1)

Macquarie Dictionary (online at 23 September 2021) 'control' (def 1, 4)

Macquarie Dictionary (online at 2 October 2021) 'current' (def 2)

Macquarie Dictionary (online at 20 August 2021) 'encode' (def 1)

Macquarie Dictionary (online at 17 October 2021) 'inflation' (def 1, 2a)

Macquarie Dictionary (online at 18 August 2021) 'open-source' (def 1)

Macquarie Dictionary (online at 23 September 2021) 'permanence'

Macquarie Dictionary (online at 18 August 2021) 'software' (def 1)

Macquarie Dictionary (online at 23 September 2021) 'stability' (def 2)

National Museum of Australia, 'Decimal Currency', *Defining Moments* (Web Page, 17 October 2021) <https://www.nma.gov.au/defining-moments/resources/decimal-currency>

National Museum of Australia, 'Governor William Bligh is deposed in the Rum Rebellion', *Defining Moments* (Web Page, 17 October 2021) <https://www.nma.gov.au/defining-moments/resources/rum-rebellion>

National Museum of Australia, 'Holey dollar', *Collection Highlights* (Web Page, 17 October 2021) <https://www.nma.gov.au/explore/collection/highlights/holey-dollar>

Online Blockchain PLC, 'The Crypto Marketplace', *Mooning Market* (Web Page, 19 September 2021) <https://mooningmarket.com/>

Oxford English Dictionary (online at 10 October 2021) 'community' (def 2b)

Oxford English Dictionary (online at 10 October 2021) 'community' (def 5b, 8)

Oxford English Dictionary (online at 11 September 2021) ‘definable’

Oxford English Dictionary (online at 11 September 2021) ‘define’ (def 3, 6)

Oxford English Dictionary (online at 3 October 2021) ‘consist’ (def 7 ‘to consist of’)

Oxford English Dictionary (online at 23 September 2021) ‘exclude’ (def 2b, 3a)

Oxford English Dictionary (online at 12 September 2021) ‘identifiable’

Oxford English Dictionary (online at 12 September 2021) ‘identify’ (def 6)

Oxford English Dictionary (online at 12 September 2021) ‘transferable’

Reserve Bank of Australia, ‘What are cryptocurrencies’, *Cryptocurrencies* (Web Page, 19 September 2021)
<https://www.rba.gov.au/education/resources/explainers/cryptocurrencies.html>.

Reserve Bank of Australia, ‘What is Money?’, *Explainers* (Web Page, 17 October 2021)
<https://www.rba.gov.au/education/resources/explainers/what-is-money.html>

‘Running A Full Node’ *What Is A Full Node?* (Documentation, 2021)
<https://bitcoin.org/en/full-node#what-is-a-full-node>

Skelton, Andy, ‘Pay Another Way: Bitcoin’, *WordPress.com* (Blog Post, 15 November 2012)
<https://wordpress.com/blog/2012/11/15/pay-another-way-bitcoin/>

‘Software’, *Bitcoin Wiki* (Documentation, 17 August 2021)
<https://en.bitcoin.it/wiki/Software>

‘Solo Mining’, *Mining* (Documentation, 2021)
<https://developer.bitcoin.org/devguide/mining.html>

Taxation Determination TD 2014/25 *Income tax: is bitcoin a ‘foreign currency’ for the purposes of Division 775 of the Income Tax Assessment Act 1997?*

Taxation Determination TD 2014/26 *Income tax: is bitcoin a 'CGT asset' for the purposes of subsection 108-5(1) of the Income Tax Assessment Act 1997?*

Thomson Reuters, ‘Currencies’ *Markets* (Web Page, 10 October 2021)
<https://www.reuters.com/markets/currencies>

Walker, Greg, ‘Chain Reorganisation’, *Learn me a bitcoin* (Web Page, 6 September 2019)
<https://learnmeabitcoin.com/technical/chain-reorganisation>

Walker, Greg, ‘Longest Chain’, *Learn me a bitcoin* (Web Page, 5 September 2019)
<https://learnmeabitcoin.com/technical/longest-chain>