A Cryptocurrency Wallet:

IS IT 'RELEVANT MATERIAL' FOR TAX ADMINISTRATION PURPOSES?

FAREED MOOSA*

ABSTRACT

This article shows that wallets storing cryptocurrency are intangible property so that they ought to qualify as a 'thing' within the meaning of this term in section 1 of the Tax Administration Act 28 of 2011, read with the definition of 'relevant material' therein. This article shows further that cryptocurrency ownership is transferred electronically by way of the relevant encrypted ledger information being sent from one crypto user to another. It is argued that this ledger comprises data messages within the meaning of this term in section 1 of the Electronic Communications and Transactions Act 25 of 2002. Accordingly, it is also argued that the digital log of communication pertaining to the creation, storage and transfer of cryptocurrency ought to qualify as information as defined in section 1 of the Tax Administration Act read with the definition of 'relevant material'. If this contention is correct in law, then SARS's extensive investigative powers entitle it to access the contents of a taxpayer's e-wallet. If a taxpayer fails to comply with a lawful demand by a SARS official for access to data of a blockchain in a virtual wallet, then SARS may exercise its powers of search and seizure. If so, then it is argued that taxpayers' privacy rights entrenched in section 14 of the Constitution of the Republic of South Africa, 1996 ought to apply to all devices and databases on which digital information is stored related to cryptocurrency transactions. Consequently, a taxpayer ought to be entitled to challenge the validity of the investigative power utilised by SARS by seeking to have the relevant legislative provision declared unconstitutional on the basis that it does not pass muster under section 36 of the Constitution.

1. Introduction

In the global electronic ecosystem, conventional methods of payment (such as, bank transfers) are being replaced by alternative payment instruments. One such instrument is virtual currency (VC).[1] A VC is a pseudo-currency that is paperless and existing in digital form only within a computer network. The South African Reserve Bank (SARB) defines a VC as 'a digital representation of value that can be digitally traded and functions

* BProc LLB (UWC), LLM (Tax) (UCT), LLD (UWC).
Professor and Head of Department of Mercantile & Labour Law, University of the Western Cape.

[1] Nieman A 'A few South African cents' worth on Bitcoin' (2015) 18 *PELJ* 1979 at 1981.

as a medium of exchange, a unit of account and/or a store of value, but does not have legal tender status'.[2]

Conceptually, VCs are classified as centralised or decentralised, and convertible or non-convertible.[3] Convertible VCs are those which, potentially at least, have an equivalent value in real currency and may be exchanged for the latter. There are two subsets of convertible VCs, namely, centralised convertible and decentralised convertible VCs. The former has a single third-party administering authority which issues the digital unit, establishes rules for its use among principals in transactions, maintains a central payment ledger for the currency, and has authority to redeem it. Examples are Webmoney and PerfectMoney.

On the other hand, decentralised convertible virtual currencies (DCVC) are 'distributed, open-source, math-based peer-to-peer VCs that have no central administering authority and no central monitoring oversight.'[4] Examples are Bitcoin and Litecoin. A DCVC is a cryptocurrency, that is, a math-based VC protected by cryptography which is an encryption technique that secures digital information and protects its privacy from, *inter alia*, state institutions. Cryptocurrencies are an important technological innovation in the internet of things. In South Africa (SA), commercial transactions occurring behind their veil of encryption makes it challenging for the South African Revenue Service (SARS) to effectively track VC denominated transactions so as to collect taxes arising therefrom.

2. Aim of the article

The Tax Administration Act 28 of 2011 (TAA) confers a formidable arsenal of investigative powers on SARS that, when exercised, potentially results in an encroachment on taxpayers' rights to, *inter alia*, privacy and property. Section 46(1) permits SARS to require a taxpayer 'to, within a reasonable period, submit relevant material … that SARS requires'.[5] Section 47(2) permits a senior SARS official to require a taxpayer 'to produce relevant material' at an interview. During a search under section 61, a SARS official

[2] SARB *Position Paper on Virtual Currencies* Position Paper 2/2014 at 2, available at http://www.resbank.co.za, accessed on 2 July 2020.

[3] SARB *Position Paper* op cit note 2 at 2.

[4] Nieman op cit note 1 at 1983. Also, see Ly MKM 'Coining Bitcoin's legal bits: examining the regulatory framework for Bitcoin and virtual currencies' (2014) 27 *Harvard J Law & Technology* 587.

[5] The provisions of s 46 are peremptory in nature. See *C:SARS v Brown* [2016] ZAECPEHC 17 para 39. For a discussion of a comparable provision in Canada, see *Minister of National Revenue v BP Canada Energy Company* 2015 FC 714, where the court held that the Canadian Revenue authorities could compel the production of unredacted working papers produced in the course of the compilation of a taxpayer's financial statements according to GAAP.

may 'seize any relevant material'[6] and 'seize and retain a computer or storage device in which relevant material is stored'.[7]

In the context of sections 46(1), 47(2) and 61(3)(*c*) of the TAA, 'relevant material'[8] bears its meaning in section 1 thereof, namely, 'any information,[9] document[10] or thing[11] that is foreseeably[12] relevant for tax risk assessment, assessing tax, collecting tax, showing non-compliance with an obligation under a tax Act or showing that a tax offence was committed'. Although this statutory definition is couched broadly, it is unclear therefrom whether cryptocurrency wallets qualify as 'relevant material'.

This article aims to hypothesise that a cryptocurrency wallet is relevant material in the sense that it is an incorporeal 'thing'. Moreover, it is argued that information stored in a cryptocurrency wallet is electronic data generated, recorded, sent, received and/or stored on a computer or other device so that it qualifies as 'information' within the ambit of the term relevant material for TAA purposes. Consequently, this article contends that SARS may, for tax assessment and general tax administration purposes, utilise sections 46(1), 47(2) and 61 of the TAA to access relevant information in a taxpayer's hands about his/her/its cryptocurrency dealings on the world wide web.

To fulfil this article's objective, the inner workings of cryptocurrency will first be explained. For this purpose, Bitcoin is used as a point of reference. It has been selected because Bitcoin is presently the most popular cryptocurrency used in South Africa. Consequently, this article is of importance to South African income-tax payers. However, the views expressed here apply with equal force to any other cryptocurrency traded by 'tech savvy' taxpayers. This is because cryptocurrencies are of the same nature and, generally speaking, operate in the same manner.

---

[6] Section 61(3)(*b*), TAA.

[7] Section 61(3)(*c*), TAA.

[8] For a discussion of 'relevant material', Vogelman A & Muller A'The extensive powers of SARS in requesting "relevant material"' (2014) 29(2) *Insurance & Tax J* 12. See also Seligson M 'Information-gathering by SARS under the TAA: Trumping the taxpayer's right to tax finality' (2016) 7(1) BTCLQ 1 at 6–8.

[9] The TAA (s 1) defines 'information' as including 'information generated, recorded, sent, received, stored or displayed by any means'.

[10] The TAA (s 1) defines 'document' to mean 'anything that contains a written, sound or pictorial record, or other record of information, whether in physical or electronic form'.

[11] The TAA (s 1) defines 'thing' as including 'a corporeal or incorporeal thing'.

[12] Clegg D *LexisNexis Concise Guide to Tax Administration* (2012) at 85 warns: '"Foreseeable" relevance is clearly in the eye of the beholder and may open the possibility of "fishing expeditions" being undertaken through requests for information of no direct relevance to a particular line of enquiry.'

3. The Bitcoin ecosystem: receiving, storing and transferring 'bits'

Bitcoin is a nascent e-currency generally believed to be the first innovation of its kind.[13] It is a currency comprising entirely of digital 0s and 1s.[14] As a currency, Bitcoin is not produced by any issuing body, nor does its use require the involvement of an intermediary (such as, a bank, central government, institutional regulator, or network operator).[15] The absence of a central administrator or other point of control allows for self-regulation by the Bitcoin community. Since Bitcoin users deal directly with one another, transactional costs are lower than those attendant upon payments in the virtual and real world which are reliant on the intervention of an intermediary.[16]

Bitcoin is an open-sourced scheme. As such, taxpayers using Bitcoin can convert fiat currency (such as rands and dollars) into Bitcoin and vice versa.[17] The Bitcoin system uses a digital ledger in which each participant, called a 'node', has an operating account. Every Bitcoin denominated transaction is posted to this ledger. A collection of these entries or postings is called a 'block'.[18] Every block is distributed to every node on the Bitcoin peer-to-peer (P2P) network. In this way, every block is made public within the Bitcoin community only. This would exclude SARS. Bitcoin members are able to verify the authenticity of a block within the Bitcoin chain.[19] A historical record or log of all past, verified transactions in the Bitcoin ledger is called a 'blockchain'.

Authentication of a block is crucial to ensuring the integrity and, hence, continued viability of Bitcoin as a medium of exchange. Verification ensures that users do not double-spend Bitcoin, nor alter Bitcoin balances. This is similar to the maintenance of the integrity of the payment system facilitated by banks which ensures, for example, that customers do not spend more than their available credit balances reflected in the bank's accounting records.

Bitcoin, or any sub-unit of value therein called a 'bit', may be obtained either through a process called 'mining',[20] or purchasing it from an exchange

---

[13] See Nakamoto S *Bitcoin: A Peer-to-Peer Electronic Cash System* 2008 (unpublished white paper) available at http://bitcoin.org/bitcoin.pdf, accessed on 20 July 2020.

[14] Jeans ED 'Funny money or the fall of fiat: Bitcoin and forward-facing virtual currency regulation' 2015 *Colorado Technology LJ* 99 at 104.

[15] See *US v Petix* WL 7017919 (Western Division of New York, 1 December 2016) 5.

[16] Leidel D 'The taxation of Bitcoin: How the IRS views cryptocurrencies' 2018 *Drake LR* 107 at 113.

[17] Akins BW, Chapman JL & Gordon JM 'A whole new world: Income tax considerations of the Bitcoin Economy' 2014 *Pittsburgh Tax Review* 25 at 27–28.

[18] The original 'block' in a chain of electronic transactions is referred to as the 'genesis block'. See Akins, Chapman & Gordon op cit note 17 at 30.

[19] SARB *Position Paper* op cit note 2 at 3.

[20] In this context, 'mining' refers to a process involving, on the one hand, a digital currency miner spending competitive computing power of specialised hardware to validate cryptocurrency transactions on a Bitcoin network, and, on the other,

(such as, Luno), or accepting it directly from a transferor as payment for goods sold or services, or receiving it as an award, or by exchanging legal tender for a Bitcoin or bit. Each of these methods of acquiring Bitcoin or a bit ought, it is submitted, to qualify as a 'transaction' within the meaning of this term in section 1 of the Electronic Communications and Transactions Act 25 of 2002 (ECTA), namely, 'a transaction of either a commercial or non-commercial nature'.

To receive, store and transmit encrypted Bitcoin, a user must install the required management software which enables the user's computer to be connected to the P2P network within the Bitcoin system.[21] Without this connectivity, a person cannot be a node in the Bitcoin ledger, or participant in a block. Taxpayers and other holders of Bitcoin store it in a virtual wallet.[22] This is a computer-generated file, also called a 'software wallet' (or crypto wallet), located, for example, in the hard drive of a computer, laptop or tablet, or in an electronic device,[23] or in an online database.[24] The storing of Bitcoin in a computer file is called 'cold storage'.[25]

To ensure that a secure, trustworthy and reliable Bitcoin ecosystem is maintained, all users on the Bitcoin network must have a public and private key that is protected by the math-based cryptography product utilised in the Bitcoin system. Therefore, the Bitcoin computer programme ought, it is submitted, to qualify as a 'cryptographic product' as defined in section 1 of the ECTA, namely, 'any product that makes use of cryptographic techniques and is used by a sender or recipient of data messages for the purposes of ensuring—(*a*) that such data can be accessed only by relevant persons; (*b*) the authenticity of the data; (*c*) the integrity of the data; or (*d*) that the source of the data can be correctly ascertained'. A private key is the secret password that identifies the sender's right to spend Bitcoin stored in a software wallet. The private key also protects holders of Bitcoin against loss through unauthorised access to their Bitcoin accounts by third parties on the network (such as, computer hackers).[26] The public

to secure the network using encryption techniques and keep all peers thereon duly synchronised so that they have a complete, immutable historical record of all confirmed transactions relating to Bitcoin. For performing this verification service, a miner is rewarded with a small number of newly mined Bitcoin. See Akins, Chapman & Gordon op cit note 17 at 33–35.

[21] Nakamoto op cit note 13 at 3.

[22] A remote server storing Bitcoin is called a 'web wallet'. See https://bitcoin.org/en/vocabulary#mining, accessed on 8 July 2020. Unlike bank accounts, e-wallets do not contain a user's personal information (such as, name, identity number and address). This fosters high levels of anonymity when Bitcoin is traded. See Jeans op cit note 14 at 105.

[23] Such as a USB memory stick or portable modem.

[24] Such as an i-cloud or dropbox.

[25] Leidel op cit note 16 at 111.

[26] Baker ED 'Trustless property systems and anarchy: how trustless transfer technology will shape the future of property exchange' 2015 *Southwestern LR* 351 at 355 states that the public ledger system through which Bitcoin is traded is advan-

key of a recipient is a once-off transaction address (or user account number) that is made available on the Bitcoin network and by which the recipient may be authenticated for purposes of a Bitcoin transaction.

Once a sender has authenticated the intended recipient, the former will electronically send the Bitcoin or bit file, as the case may be, after signing off the transaction using the sender's private cryptographic signature.[27] The information is then available to all users on the decentralised Bitcoin network. The transaction is only added as a new, irreversible block in the electronic chain once it is confirmed by individuals, so- called miners, using a hashing algorithm that aids in solving a complex set of incorruptible mathematical verification puzzles or proofs.[28] It is only when such verification occurs that a transfer of rights to Bitcoin or a bit, as the case may be, occurs so that a potential liability for income tax may ensue.[29] Transfers of this nature take place regularly in SA where technology, both digital and non-digital alike, is the new frontier where social interaction (such as, on Facebook, Twitter, Instagram, Whatsapp) occurs, and commerce too.

4. Conclusion

On the basis of the explanation above in 3, it is submitted that a software wallet is intangible in nature. This virtual wallet exists in electronic form only. As such, it is an incorporeal which may qualify as a 'thing' within the meaning of this term in section 1 of the TAA read with the definition of 'relevant material', both of which terms are discussed above in 2. This article shows further that ownership rights in Bitcoin and, by extension, cryptocurrency generally, is transferred electronically within the digital ecosystem. This involves sending the relevant encrypted ledger information from one cryptocurrency user to another.[30] The electronic communication related to this transfer is then shared within the relevant cryptocurrency community for verification purposes.

The cryptocurrency ledger recording a blockchain comprises a series of 'data message[s]' within the meaning of this term in section 1 of the ECTA, namely, 'data generated, sent, received or stored by electronic means and includes … a stored record'. In this context, 'data' is defined in section 1

tageous because it 'thwarts the efforts of identity thieves and protects individuals from the numerous types of fraud that are common when relying on third-party intermediaries' (e g, banks).

[27] For a discussion of the requirements for electronic signatures under the ECTA, see *Spring Forest Trading 599 CC v Wilberry (Pty) Ltd t/a Ecowash* 2015 (2) SA 118 (SCA) paras 15–28.

[28] Simonite T 'What Bitcoin is, and why it matters: Can a booming "cryptocurrency" really compete with conventional cash?' *MIT Technology Review* (25 May 2011) available at *https://www.technologyreview.com/s/424091/what-bitcoin-is-and-why-it-matters*, accessed on 27 July 2020.

[29] For a discussion of the taxability of cryptocurrency, see Moosa F 'Cryptocurrencies: Do they qualify as "gross income"' (2019) 44(1) *Journal for Juridical Science* 1.

[30] Nakamoto op cit note 13 at 2.

of the ECTA to mean 'electronic representations of information in any form'.[31] Accordingly, the digital log of communication pertaining to crypto ownership ought, it is submitted, to qualify as 'information' within the meaning of this term as defined in section 1 of the TAA read with the definition of the term 'relevant material' as used therein.

If this view is correct, then SARS's investigative powers entitles it to call on taxpayers to disclose, *inter alia*, the content of a software wallet.[32] In this way, SARS would be able to detect undisclosed revenue in the hands of a taxpayer. Revenue from taxation is pivotal for all levels of government to achieve constitutional goals.[33] If a taxpayer fails to comply with a lawful demand by a SARS official during an audit or investigation in relation to accessing data in a blockchain, then SARS may exercise its powers of search and seizure granted by the TAA.[34] The exercise of these powers must, however, meet constitutional safeguards.[35]

If e-wallets storing Bitcoin and/or other cryptocurrency are 'relevant material' for tax administration purposes in the various senses hypothesised in this article, then taxpayers' rights to privacy of the digital information stored therein would be implicated whenever SARS seeks access thereto. In this context, taxpayers ought to be entitled to invoke the protection afforded by sections 14(*b*) and (*d*) of the Constitution of the Republic of South Africa, 1996.[36] This is particularly so because, in SA's constitutional democracy, 'the substantive enjoyment of rights has a high premium'.[37] Taxpayers ought therefore to be accorded constitutional protection in cases where, for example, SARS seeks to search and seize a taxpayer's computer or other device on which digital information related to the creation, storage and/or transfer of cryptocurrency may be found.

To overcome an encroachment on privacy, a taxpayer ought, pursuant to section 36 of the Constitution, to be able to challenge the validity of the relevant investigative power exercised by SARS. Such challenge would be predicated on the basis that it constitutes an unreasonable and unjustifiable

[31] Fairfield JAT 'Bitproperty' (2015) 88 *Southern California LR* 805 at 811 describes 'property' as 'the law of lists and ledgers'. Thus, he characterises Bitcoin and digital property generally as information or data.

[32] Smith J, in *CSARS v Brown* (561/2016) [2016] ZAECPEHC 17 paras 50–51, held that a request for 'relevant material' under the TAA is not administrative in nature because it entails a preliminary investigation that does not adversely affect the taxpayer's rights.

[33] *Kalil NO v Mangaung Metropolitan Municipality* 2014 (5) SA 123 (SCA) para 6.

[34] Fabricius J, in *Moyane v Ramaphosa* [2018] ZAGPPHC 835 para 29 refers to the crucial role that SARS plays because 'South Africa is staring at a fiscal cliff—the expenditure is higher than the income, growth is low, investment is plunging and poverty is rife'.

[35] *Huang v C:SARS: In re C:SARS v Huang* 2015 (1) SA 602 (GP) paras 13–16.

[36] Section 14 reads: 'Everyone has the right to privacy, which includes the right not to have—(*a*) their person or home searched; (*b*) their property searched; (*c*) their possessions seized; or (*d*) the privacy of their communications infringed.'

[37] *Koyabe v Minister for Home Affairs* 2010 (4) SA 327 (CC) para 44.

limitation on a taxpayer's privacy. In such a limitation's enquiry, a fair balance must be struck between the competing interests at play, namely, a taxpayer's privacy, on the one hand, and SARS's aim to access relevant financial information that may uncover undisclosed taxable income, on the other. The outcome would usually depend on the particular factual scenario, including SARS's grounds for the investigation and whether or not the taxpayer is being unfairly subjected to a 'fishing expedition'.