LEGAL AND REGULATORY INTERVENTION IN THE CRYPTOCURRENCY SPACE

An Impossible Task?

It is often alleged that cryptocurrencies are "trustless", "immutable" and "decentralised" and that these traits not only make them "self-regulating", but also render legal and regulatory intervention in the cryptocurrency space impossible. The accuracy of such allegations is questionable. A closer examination of the mechanics behind several cryptocurrencies reveals that, while *some* cryptocurrencies display *degrees* of the aforementioned traits, cryptocurrencies are not *completely* "trustless", "immutable" or "decentralised" *in every case*. Furthermore, with reference to incidents like the 2016 hack of "The DAO", it will be shown that the *degree* of "immutability" possessed by *some* cryptocurrencies does not enable them to be "self-regulating", in the sense that they are able to police themselves against illegal conduct which may otherwise occur on such networks. Finally, it will be demonstrated that while the *degrees* of "trustlessness", "immutability" and "decentralisation" possessed by *some* cryptocurrencies undoubtedly generate challenges for legal and regulatory intervention in the cryptocurrency space, these challenges are *not* insurmountable. Substantiating this, several proposals are made which may enable courts and regulators to not only deal with the challenges presented by cryptocurrencies, but also to seize the opportunities presented by them.

LAU Chin Yang Joseph[1]
BA (Oxford), LLM (Intellectual Property and Technology Law) (National University of Singapore);
Teaching Assistant, Faculty of Law, National University of Singapore.

1 The author is grateful to Associate Professor Daniel Seng and the anonymous referee for the helpful comments. All errors and omissions remain the author's own.

I. Introduction

1 In 2008 "Satoshi Nakamoto" posted a whitepaper describing "Bitcoin",[2] the dominant cryptocurrency which laid the ground for all subsequent cryptocurrencies.[3] A "cryptocurrency" is a system which meets the following conditions:[4]

> (a) it is distributed and achieves consensus on its state;.
>
> (b) it keeps an overview of digital representations of value (referred to as "cryptocurrency units" in the interest of convenience) and their ownership;
>
> (c) it defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units; and
>
> (d) ownership of cryptocurrency units can be proved exclusively cryptographically;
>
> (e) it allows transactions to be performed in which ownership of the units of cryptocurrency is changed; and
>
> (f) if two different instructions for changing the ownership of the same units of cryptocurrency are simultaneously entered, it performs at most one of them.

The first commercial use of Bitcoin was a purchase of pizzas for 10,000 BTC.[5] At the time, 1 BTC was worth US$0.0025.[6] Bitcoin has since increased in value and usage. On 18 July 2020, 1 BTC was worth around US$9,122.11.[7] In terms of usage, whilst knowledge of Bitcoin was once confined to Internet forums,[8] it is now legal means of payment

2 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) <https://bitcoin.org/bitcoin.pdf> (accessed 9 December 2020).

3 Asress Adimi Gikay, "Regulating Decentralized Cryptocurrencies under Payment Services Law: Lessons from European Union Law" (2018) 9 *Journal of Law, Technology & the Internet* 1 at 4.

4 This definition is a modified version of the one proposed by Jan Lanksy. See Jan Lanksy "Possible State Approaches to Cryptocurrencies" (2018) 9(1) *Journal of Systems Integration* 19 at 19.

5 Julie Bort, "May 22 Is Bitcoin Pizza Day Thanks to These Two Pizzas Worth $5 Million Today" *Business Insider India* (22 May 2014).

6 BitcoinWiki, "Bitcoin History" <https://en.bitcoinwiki.org/wiki/Bitcoin_history#Bitcoin_in_2009> (accessed 17 July 2020).

7 CoinMarketCap, "Bitcoin" <https://coinmarketcap.com/currencies/bitcoin/> (accessed 9 December 2020).

8 Jerry Brito & Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Mercatus Center, 2013) at p 1.

in Japan.[9] Simultaneously, other cryptocurrencies like NEO and Ether have emerged.

2 While cryptocurrencies are increasingly ubiquitous and valuable, they are not without risks. In 2018, Europol estimated that 3–4% of illicit proceeds in Europe were laundered through cryptocurrencies and there are reports of terrorist groups soliciting support in Bitcoin.[10] These risks have not gone unnoticed: Singapore has passed the Payment Services Act 2019[11] ("PSA"), under which cryptocurrency dealing or exchange services are "digital payment token" services subject to anti-money laundering ("AML") and counter financing of terrorism ("CFT") requirements.[12]

3 However, some argue that legal and regulatory intervention in the cryptocurrency space is neither necessary nor feasible. In terms of *necessity*, these arguments focus on the data structure used by many cryptocurrencies, known as "blockchain":[13] a distributed digital ledger using cryptographic algorithms to verify the creation or transfer of digital records in a distributed network.[14] As the blockchain purports to create an "immutable" system safe from fraud, identity theft or tampering,[15] some therefore argue that no legal or regulatory intervention is required to

9 Luke Parker, "Bitcoin Regulation Overhaul in Japan" *Brave New Coin* (1 April 2017) <https://bravenewcoin.com/insights/bitcoin-regulation-overhaul-in-japan> (accessed 10 December 2020).

10 Zachary K Goldman *et al*, "Terrorist Use of Virtual Currencies: Containing the Potential Threat" (Centre for a New American Security, 2017) at p 4 <https://s3.amazonaws.com/files.cnas.org/documents/CNASReport-TerroristFinancing-Final.pdf?mtime=20170502033819> (accessed 9 December 2020); Shiroma Silva, "Criminals Hide 'Billions' in Crypto-cash – Europol" *BBC* (12 February 2018).

11 Act 2 of 2019.

12 *Singapore Parliamentary Debates, Official Report* (14 January 2019) vol 94 (Ong Ye Kung, Minister for Education).

13 Not all cryptocurrencies use blockchain. IOTA uses another data structure known as the "tangle": see Robby Houben & Alexander Snyers, "Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion" (European Union, 2018) at p 42 <http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf> (accessed 9 December 2020). However, since most cryptocurrencies, *eg*, Bitcoin, Ether and NEO, use blockchain, to the point that the popular conception of a cryptocurrency is that it *necessarily* entails the use of a blockchain, the focus of this article is on blockchain-based cryptocurrencies.

14 Michèle Finck, "Blockchains: Regulating the Unknown" (2018) 19(4) German LJ 665 at 667.

15 David E Fialkow, Jack S Brodsky & Edward Mikolinski, "Cryptocurrency 2018" *Harvard Law School Forum on Corporate Governance* (8 February 2018) <https://corpgov.law.harvard.edu/2018/02/08/cryptocurrency-2018/> (accessed 10 December 2020).

police cryptocurrency networks[16] that use blockchains against fraudulent conduct. Instead, such networks may rely on the "immutability" of blockchain to disincentivise abuse.[17]

4 As for the *feasibility* of intervention, four issues are commonly raised. Firstly, there is frequently no single entity controlling a cryptocurrency network,[18] seemingly presenting no target for intervention to ensure its compliance with laws and regulations. Secondly, users of some cryptocurrencies transact on these networks using pseudonyms, complicating the identification of the accused or defendant for the purposes of proceedings based on transactions on these networks.[19] Finally, cryptocurrency networks are distributed internationally, raising questions regarding the issues of jurisdiction[20] and governing law for

16 Cryptocurrency networks should not be confused with cryptocurrency exchanges. The former is a system of interconnected computing devices which build consensus to validate transactions on that system. The latter are online marketplaces in which *fiat* currency, cryptocurrencies, or goods and services may be exchanged.

17 Tatiana Cutts & David Goldstone, "Bitcoin Ownership and Its Impact on Fungibility" *Coindesk* (14 June 2015) <https://www.coindesk.com/bitcoin-ownership-impact-fungibility> (accessed 10 December 2020).

18 Eliza Mik, "Blockchains: A Technology for Decentralized Marketplaces" in The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms (Larry A DiMatteo, Michel Cannarsa & Cristina Poncibò eds) (Cambridge University Press, 2019) ch 9 at p 163.

19 Andrew Dickinson, "Cryptocurrencies and the Conflict of Laws" in *Cryptocurrencies in Public and Private Law* (David Fox & Sarah Green eds) (Oxford University Press, 2019) ch 5 at para 5.08.

20 Under public international law, "jurisdiction" primarily concerns *criminal* matters (see Xiaodong Yang, "Jurisdiction" *Oxford Bibliographies* (25 October 2012) <https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0030.xml> (accessed 10 December 2020)). It encompasses "prescriptive", "adjudicative" and "enforcement" jurisdiction. Prescriptive jurisdiction refers to the power of a State to create the legal rules which are valid within its system. Adjudicative jurisdiction refers to the power vested in the courts of the State to apply such rules in individual cases through judgments. Enforcement jurisdiction refers to the power of the State to use coercion to have its laws and judgments complied with. The approaches for assessing whether a State has prescriptive or adjudicative jurisdiction are similar (see Carlo Focarelli, *International Law* (Edward Elgar Publishing, 2019) at pp 283 and 285–292). Under private international law, "jurisdiction" is concerned with competence of national courts to adjudicate civil or commercial matters (see Jan Wouters *et al*, *International Law: A European Perspective* (Hart Publishing, 2019) at p 462). *Burgundy Global Exploration Corp v Transocean Offshore International Ventures Ltd* [2014] 3 SLR 381 at [79]–[80] clarifies that in private international law a distinction exists between "personal jurisdiction" and "subject-matter jurisdiction". The former refers to whether a person is amenable to the jurisdiction of the court in the sense of him being brought before the court. The latter demands a sufficient connection between the subject-matter of the dispute and the forum court (see Marcus Teo Wei Ren, "Service Out for Scandalising Contempt: An International Constitutional Jurisdiction?" [2019] Sing JLS 477 at 484–485).

proceedings based on transactions on such networks.[21] In addition to these issues, which stem from the allegedly "trustless" and "decentralised" nature of cryptocurrencies, the "immutability" of blockchain also poses challenges for legal and regulatory intervention. For instance, the General Data Protection Regulation[22] ("GDPR") and Singapore's Personal Data Protection Act 2012[23] ("PDPA") require rectification or erasure of data in certain circumstances. The "immutability" of blockchain therefore appears to render cryptocurrencies using it incapable of compliance with the GDPR or PDPA. Collectively, these challenges suggest that legal and regulatory intervention in the cryptocurrency space is impossible. This article queries the truth behind such claims, which can be broken down into three basic propositions:

(a) cryptocurrencies are "trustless", "immutable" and "decentralised";

(b) these traits render cryptocurrencies self-regulating; and

(c) cause cryptocurrencies to defy legal and regulatory intervention.

A deep dive is taken into the technology behind cryptocurrencies, with the accuracy of the above statements being tested against the capabilities and limitations of that technology. In discussing (c), this article goes one step further and makes proposals on how courts and regulators can address the challenges for legal and regulatory intervention posed by cryptocurrencies. In canvassing all the above, this article adopts the following structure. In part II of this article, the technology behind Bitcoin is explained to provide the requisite technical background; (a), (b) and (c) are discussed in Parts III, IV and V below respectively.

II. The technology behind Bitcoin

5 Many cryptocurrencies are based on Bitcoin, such that understanding the technology behind Bitcoin allows one to appreciate

21 Javier Sebastian Cermeño, "Blockchain in Financial Services: Regulatory Landscape and Future Challenges for its Commercial Application" 16/20 BBVA Research Working Paper (2016) at p 14 <www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf> (accessed 10 December 2020).

22 Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1.

23 Act 26 of 2012.

the mechanics of a wide range of cryptocurrencies.[24] Information on the Bitcoin network is stored on a network of nodes.[25] Copies of the "ledger" (the record of transactions on the network)[26] are stored on each full node,[27] with all copies of the ledger being continuously updated. The ledger takes the form of a blockchain, whose accuracy is maintained through a process of peer-validation.[28] Understanding how this works requires an explanation of "private" and "public" keys. "Private keys" are numerical identifiers unique to each user of the Bitcoin network and which are private to the user to whom they belong.[29] "Public keys" are generated from private keys[30] and, when run through hashing algorithms, produce "addresses"[31] (hashing algorithms convert input data into a "hash" which is unique to the input data from which it was derived – any change in that data produces a different hash).[32] "Addresses", analogised to bank account numbers, identify the "accounts" from which users of the network exchange BTC.[33] Public keys and their corresponding addresses can be shared with other users of the network[34] and are "pseudonymous", meaning that they do not, in and of themselves, reveal the identity of their owners, enabling parties to transact on the network without disclosing their identity.[35] However, it is inaccurate to say that users of the Bitcoin

24 Preston Miller, "The Cryptocurrency Enigma" in *Digital Forensics: Threatscape and Best Practices* (John Sammons ed) (Elsevier Inc, 2016) ch 1 at pp 1 and 4.

25 A "node" is a computer running the software enabling participation in a cryptocurrency network (see Andreas M Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* (O'Reilly Media, Inc, 2nd Ed, 2017) at p 50, as cited in Kelvin F K Low & Eliza Mik, "Pause the Blockchain Legal Revolution" (2019) 69(1) *International and Comparative Law Quarterly* 135 at 138).

26 Sarah Green, "Cryptocurrencies: The Underlying Technology" in *Cryptocurrencies in Public and Private Law* (David Fox & Sarah Green eds) (Oxford University Press, 2019) ch 1 at para 1.03.

27 Rebecca M Bratspies, "Cryptocurrency and the Myth of the Trustless Transaction" (2018) 25(1) Mich Telecomm & Tech L Rev 1 at 12.

28 Robleh Ali *et al*, "Innovations in Payment Technologies and the Emergence of Digital Currencies" (2014) Q3 *Bank of England Quarterly Bulletin* 262 at 268–269.

29 *An Introduction to Technology Law* (Lexis®PSL TMT Team eds) (LexisNexis, 1st Ed, 2018) at para 44.04.

30 Imran Bashir, *Mastering Blockchain: Distributed Ledgers, Decentralization and Smart Contracts Explained* (Packt Publishing, 2017) at p 117.

31 Chris Pacia, "Bitcoin Explained Like You're Five: Part 3 – Cryptography" *Escape Velocity* (7 September 2018) <https://chrispacia.wordpress.com/2013/09/07/bitcoin-cryptography-digital-signatures-explained/> (accessed 10 December 2020).

32 Niels Vandezande, *Virtual Currencies: A Legal Framework* (Intersentia, 2018) at p 59.

33 Kelvin F K Low & Ernie G S Teo, "Bitcoins and Other Cryptocurrencies As Property?" (2017) 9(2) *Law, Innovation and Technology* 235 at 238.

34 Robleh Ali *et al*, "Innovations in Payment Technologies and the Emergence of Digital Currencies" (2014) Q3 *Bank of England Quarterly Bulletin* 262 at 273.

35 Jerry Brito & Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Mercatus Center, 2013) at p 8; "Is Bitcoin Anonymous?" *Bitcoin Magazine* <https://bitcoinmagazine.com/what-is-bitcoin/is-bitcoin-anonymous> (accessed 10 December 2020).

network are *incapable* of being identified and hence "anonymous" (*ie*, of unknown name),[36] as all transactions involving their public keys are recorded on the blockchain and it remains possible to use this information to tie public keys to their users.[37]

6 Equipped with this understanding, we follow a transfer of 5 BTC from Alice to Bob. To do this, Alice creates a transaction message containing, *inter alia*, her and Bob's addresses, the amount to be transferred to Bob's address and Alice's "digital signature".[38] Digital signatures prove that transactions originate from transferors, without transferors having to disclose their private keys.[39] They are generated by combining a user's private key with the transaction message in an algorithm and the user's public key can then be used to verify that the transaction message originated from that user.[40] Returning to the example of Alice and Bob, to affect the transfer, Alice first broadcasts the transaction message for verification by nodes known as "miners".[41] Miners bundle all unconfirmed transactions into "blocks" and compete to verify them in a way which other miners will accept.[42] Part of the verification

36 "anonymous, adj" *OED Online* (Oxford University Press, 2020) (accessed 10 December 2020).

37 Kelvin F K Low & Ernie G S Teo, "Bitcoins and Other Cryptocurrencies as Property?" (2017) 9(2) *Law, Innovation and Technology* 235 at 239.

38 Robleh Ali *et al*, "Innovations in Payment Technologies and the Emergence of Digital Currencies" (2014) Q3 *Bank of England Quarterly Bulletin* 262 at 268.

39 Jussila Jani-Pekka, *Reconciling the Conflict Between the "Immutability" of Public and Permissionless Blockchain Technology and the Right to Erasure under Article 17 of the General Data Protection Regulation* (unpublished Masters' thesis, University of Turku, 2018) at pp 13–14 <https://www.utupub.fi/handle/10024/146293> (accessed 10 December 2020).

40 Zibin Zheng *et al*, "An Overview of Blockchain Technology: Architecture, Consensus and Future Trends" 2017 Institute of Electrical and Electronics Engineers 6th International Congress on Big Data, Honolulu (25–30 June 2017) at p 558 <https://ieeexplore.ieee.org/document/8029379> (accessed 10 December 2018), as cited in Jussila Jani-Pekka, *Reconciling the Conflict between the "Immutability" of Public and Permissionless Blockchain Technology and the Right to Erasure under Article 17 of the General Data Protection Regulation* (unpublished Masters' thesis, University of Turku, 2018) at pp 13–14 <https://www.utupub.fi/handle/10024/146293> (accessed 10 December 2020).

41 Lam Pak Nian, *Bitcoin in Singapore: A Light-Touch Approach to Regulation* (unpublished LLB thesis, National University of Singapore, archived at the CJ Koh Law Library, National University of Singapore) (2014) at p 16 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427626> (accessed 10 December 2020).

42 Robleh Ali *et al*, "Innovations in Payment Technologies and the Emergence of Digital Currencies" (2014) Q3 *Bank of England Quarterly Bulletin* at p 268 <https://www.bankofengland.co.uk/quarterly-bulletin/2014/q3/innovations-in-payment-technologies-and-the-emergence-of-digital-currencies> (accessed 10 December 2020).

process involves checking that Alice's digital signature is correct[43] (see Figure 1 below).

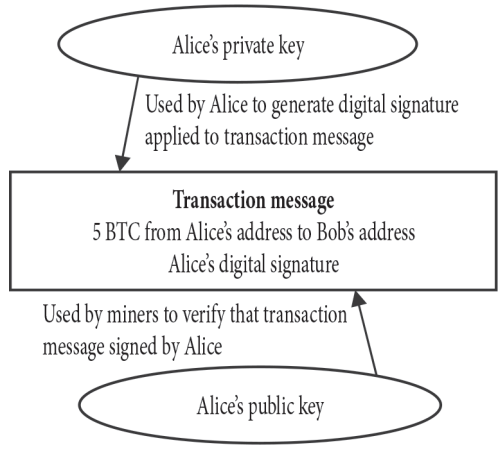

Figure 1

7 However, the correctness of Alice's digital signature only establishes that the transaction originated from her – it does not establish that she had 5 BTC to transfer to Bob.[44] To tackle this problem and ensure the veracity of transaction information, Bitcoin uses an algorithm known as "proof of work" ("PoW").[45] Explaining PoW, each unconfirmed transaction in a block is hashed and these hashes are organised into pairs, concatenated together and hashed again, with this process being repeated until a hash representing all the transactions in the block ("Merkle root") is obtained.[46] The following, *inter alia*, then comprise the "header" of the block of unconfirmed transactions ("Candidate Block"): the hash of the previous block in the blockchain, the Merkle root

43 Robleh Ali *et al*, "Innovations in Payment Technologies and the Emergence of Digital Currencies" (2014) Q3 *Bank of England Quarterly Bulletin* 262 at 269 <https://www.bankofengland.co.uk/quarterly-bulletin/2014/q3/innovations-in-payment-technologies-and-the-emergence-of-digital-currencies> (accessed 10 December 2020).

44 Yohan Yun, "Why Crypto Miners Are Sweating over the Imminent 'Bitcoin Halving'" *Forkast* (21 April 2020) <https://forkast.news/proof-of-work-what-is-it-bitcoin-halving/> (accessed 10 December2020).

45 Sarah Green, "Cryptocurrencies: The Underlying Technology" in *Cryptocurrencies in Public and Private Law* (David Fox & Sarah Green eds) (Oxford University Press, 2019) ch 1 at para 1.06.

46 Chris Pacia, "Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics" *Escape Velocity* (2 September 2018) <https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/> (accessed 10 December 2020).

of transactions in the Candidate Block and a "nonce".[47] The header of the Candidate Block is then hashed using Secure Hash Algorithm 256 ("SHA256"), producing an identifying hash for it.[48] The Bitcoin protocol requires identifying hashes to start with a certain number of zeroes and the "nonce" is a random number which, when hashed with other data in the header of a Candidate Block, produces a hash satisfying the Bitcoin protocol.[49] Finding the nonce is computationally intensive – generally it takes ten minutes for specialised computers to find the nonce.[50] Once a miner finds the nonce and generates the required hash for the Candidate Block, it broadcasts the Candidate Block to the network.[51] While finding the nonce is computationally intensive, it is easy for other miners to verify its accuracy and they express acceptance of the Candidate Block by using its identifying hash as input data for the header of the *next* block of unconfirmed transactions up for validation.[52] The network rewards the miner who found the nonce first with BTC and he may also earn transaction fees offered by the transferor.[53]

III. Cryptocurrencies are not completely "trustless", "immutable" and "decentralised" in every case

8 Although most cryptocurrencies work on essentially the same scheme as described for BTC, not all cryptocurrencies are the same:

47 Chris Pacia, "Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics" *Escape Velocity* (2 September 2018) <https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/> (accessed 10 December 2020).

48 Chris Pacia, "Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics" *Escape Velocity* (2 September 2018) <https://chrispacia.wordpress.com/201309/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/> (accessed 10 December 2020).

49 Chris Pacia, "Bitcoin Mining Explained Like You're Five: Part 2 – Mechanics" *Escape Velocity* (2 September 2018) <https://chrispacia.wordpress.com/2013/09/02/bitcoin-mining-explained-like-youre-five-part-2-mechanics/> (accessed 10 December 2020).

50 Peter Surda, *Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold* (unpublished thesis, W U Vienna University of Economics and Business) (2012) at pp 7–8 <https://nakamotoinstitute.org/static/docs/economics-of-bitcoin.pdf> (accessed 10 December 2020), as cited in Niels Vandezande, *Virtual Currencies: A Legal Framework* (Intersentia, 2018) at pp 59–60.

51 Samuel Elliott, "Bitcoin: The First Self-Regulating Currency?" (2018) 3 LSE Law Review 57 at 63.

52 Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) at p 2 <https://bitcoin.org/bitcoin.pdf> (accessed 9 December 2020), as cited in Samuel Elliott, "Bitcoin: The First Self-Regulating Currency?" (2018) 3 LSE Law Review 57 at 63–64.

53 Niels Vandezande, *Virtual Currencies: A Legal Framework* (Intersentia, 2018) at pp 56 and 68.

they all exhibit different *degrees* of "trustlessness", "immutability" and "decentralisation". Each concept is now defined and examined in turn. Table 1 below summarises the observations made regarding each of the cryptocurrencies examined in this section.

Name	Origins	Consensus algorithm	Decentralisation	Trustlessness	Immutability
Bitcoin	Mooted by Satoshi Nakamoto in 2008	PoW	Architecturally and politically decentralised,* but logically centralised * *Approximates a politically centralised system.*	Not trustless. Uses system of incentives to encourage validation of unconfirmed transactions and disincentives against tampering with records of past transactions.	Technically immutable at best.
Ethereum (Ether is the native token on the Ethereum network)	Envisioned by Vitalik Buterin in 2013[54]	PoW, but shifting to Proof of Stake ("PoS")[55]	Logically centralised (this article does not examine whether these cryptocurrencies are architecturally or politically decentralised)		
BlackCoin	Created in 2014, with sources crediting Pavel Vasin as its creator[56] and other sources crediting Joshua Bouw as its founder[57]	PoS			

54 Vitalik Buterin, "Ethereum Whitepaper" *Ethereum.org* <https://ethereum.org/en/whitepaper/> (accessed 10 December 2020).

55 Lin William Cong, Zhiguo He & Jiasun Li, "Decentralized Mining in Centralized Pools" George Mason University School of Business Research Paper No 18-9 (2018) at pp 38–39 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143724> (accessed 10 December 2020).

56 Alexander Weipprecht, "BlackCoin" *Coinreport* (12 February 2018) <https://www.coin-report.net/en/blackcoin/> (accessed 10 December 2020).

57 "What is BlackCoin (BLK)? Future of BLK Cryptocurrency and Know How to Buy BLK" *Coinswitch* <https://coinswitch.co/info/blackcoin/what-is-blackcoin> (accessed 10 December 2020).

NEO (note that the NEO network has *two* native tokens, NEO and GAS)[58]	Founded by Erik Zhang and Da Hongfei in 2014[59]	Delegated Byzantine Fault Tolerance	Politically and logically centralised (this article does not examine whether NEO is architecturally decentralised)	Not trustless. Users effectively trust in a single entity to validate unconfirmed transactions.	

Table 1

A. Decentralisation

9 "Decentralisation" refers to the distribution and dispersal of power away from a central authority.[60] In the context of cryptocurrencies, decentralisation has three aspects: architectural decentralisation, which examines how many computers comprise a system and whether there is a single point of failure, political decentralisation, which examines which entities are in control of the system, and logical decentralisation, which assesses whether the system behaves like a single monolithic object.[61] Applying the term "decentralised" to cryptocurrencies therefore suggests that they are architecturally, politically and logically decentralised. This is not always correct. For instance, the purpose of the consensus algorithms used by cryptocurrency networks is to achieve a *single* perspective on transaction validity throughout the network. As systems, cryptocurrency networks therefore *behave* like a single computer, reflecting one commonly agreed record of transactions,[62] with the consequence that they are logically *centralised*. However, the picture in terms of political decentralisation and architectural decentralisation respectively is more complicated and it is to these aspects of decentralisation that the discussion now turns.

58 Chris Wheal, "History of the NEO Cryptocurrency" *DEX* (5 June 2018) <https://dex.openledger.io/history-of-the-neo-cryptocurrency/> (accessed 11 December 2020).

59 Chris Wheal, "History of the NEO Cryptocurrency" *DEX* (5 June 2018) <https://dex.openledger.io/history-of-the-neo-cryptocurrency/> (accessed 11 December 2020).

60 "Decentralization News" *Cointelegraph* <https://cointelegraph.com/tags/decentralization> (accessed 10 December 2020).

61 Vitalik Buterin, "The Meaning of Decentralization" *Medium* (6 February 2017) <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274> (accessed 10 December 2020).

62 Vitalik Buterin, "The Meaning of Decentralization" *Medium* (6 February 2017) <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274> (accessed 10 December 2020).

(1) Political decentralisation

10 Keeping the definition of "decentralisation" in mind, a politically centralised system is one where a *single* entity has authority. One way of assessing "authority" in the context of a cryptocurrency network is to inquire whether its critical functions are controlled by a single entity. For instance, some cryptocurrencies need a constant allocation and distribution of new units of cryptocurrency or the validation of unconfirmed transactions to function. Accordingly, if a single entity controls these functions on a network, that network is politically centralised. Applying this test, Bitcoin (number one in terms of market capitalisation)[63] is not politically centralised, but NEO (number 17 in terms of market capitalisation)[64] is.

11 This is because the allocation and distribution of new BTC is not controlled by a single entity. Instead, new BTC is released by the network as a reward to the first miner to find the nonce for a given Candidate Block[65] as validation of unconfirmed transactions. Any participant operating a node on the network and who has installed the requisite software (which is free to download and run)[66] can be a miner to validate unconfirmed transactions, meaning that the issuance of BTC is not controlled by any *one single* entity. However, in practice, Bitcoin's use of PoW has caused this function to become controlled by a *handful* of entities,[67] thus *approximating* political centralisation. To understand this, some elaboration on how miners find the nonce is required. Miners experiment with potential nonces until the right one is found.[68] The more computational power a miner has, the faster it can try out potential nonces and the higher will be its chances of finding the nonce first.[69] The link between computational power and finding the nonce first has caused "mining pools", or arrangements under which computers share hash power in exchange for a portion of the rewards for successfully mined blocks,[70] to become popular. Chances of finding the nonce first are higher in a mining pool due to the combined computational power of members

63 CoinMarketCap website <https://coinmarketcap.com/coins/views/all/>.
64 CoinMarketCap website <https://coinmarketcap.com/coins/views/all/>.
65 See para 7 above.
66 Anthony Volastro, "CNBC Explains: How to Mine Bitcoins on Your Own" *CNBC* (23 January 2014).
67 Andreas M Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (O'Reilly Media Inc, 1st Ed, 2014) at pp 207–212, as cited in Angela Walch, "The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk" (2015) 18(4) NYUJ Legis & Pub Pol'y 837 at 847 and 861.
68 Niels Vandezande, *Virtual Currencies: A Legal Framework* (Intersentia, 2018) at p 59.
69 Amit Bhardwaj, *Crypto currency For Beginners* (Onlinegatha, 2017) at p 74.
70 Rebecca M Bratspies, "Cryptocurrency and the Myth of the Trustless Transaction" (2018) 25(1) Mich Telecomm & Tech L Rev 1 at 13–14.

being directed towards this.[71] A 2019 study indicated that 95.99% of the network's computational power was controlled by the top 25 mining pools and that from February 2016 to January 2019, the top four pools created *48.44%* of blocks on the network.[72] Based on these developments, it seems fair to conclude that though the Bitcoin network is politically decentralised, its use of PoW causes the *approximation* of political centralisation by allowing the validation of unconfirmed transactions on the network to become controlled by a handful of entities.

12 On the other hand, the NEO network uses a consensus algorithm known as Delegated Byzantine Fault Tolerance ("DBFT"), under which the agreement of two-thirds of nodes known as "consensus nodes" is required for a record of transactions to be added to the blockchain.[73] Accordingly, if an entity controls more than two-thirds of the consensus nodes, the agreement of that entity to a record of transactions forms a *de facto* requirement for its addition to the blockchain. As of 11 December 2020, five of the seven consensus nodes supporting the NEO network are controlled by the NEO Foundation, which also controls the initial allocation and distribution of NEO.[74] Unlike Bitcoin, where new BTC is created through mining, the total supply of NEO was pre-mined,[75] with half being distributed to supporters of NEO and the distribution of the remainder being managed by the NEO Foundation.[76] The other native token on the NEO network, GAS, is generated every time a new block is added to the NEO blockchain and is distributed proportionally in accordance with the amount of NEO held in users' addresses on the

71 Preston Miller, "The Cryptocurrency Enigma" in *Digital Forensics: Threatscape and Best Practices* (John Sammons ed) (Elsevier Inc, 2016) ch 1 at p 11.

72 Canhui Wang, Xiaowen Chu & Qin Yang, "Measurement and Analysis of the Bitcoin Networks: A View from Mining Pools" (2019) at p 5 <https://arxiv.org/abs/1902.07549> (accessed 10 December 2020).

73 Marco Manoppo, "Delegated Byzantine Fault Tolerance Consensus Mechanism" *Medium* (16 June 2018) <https://medium.com/@cryptocohort/delegated-byzantine-fault-tolerance-consensus-mechanism-502f9586c358> (accessed 10 December 2020).

74 NEO website <https://neo.org/consensus>; "NEO White Paper" *neo.org* <https://docs.neo.org/docs/en-us/basic/whitepaper.html> (accessed 11 December 2020); NEO Foundation, "The Announcement of NEO Reorganization" *neo.org* (22 May 2018) <https://neo.org/blog/details/3083> (accessed 10 December 2020).

75 S Khatwani, "NEO Cryptocurrency: Everything You Need to Know about China Ethereum" *Coinsutra* (December 2017) <https://coinsutra.com/neo-cryptocurrency/> (accessed 10 December 2020).

76 "NEO White Paper" *neo.org* <https://docs.neo.org/docs/en-us/basicwhitepaper.html> (accessed 10 December 2020); NEO Foundation, "The Announcement of NEO Reorganization" *neo.org* (22 May 2018) <https://neo.org/blog/details/3083> (accessed 10 December 2020).

network.[77] Since the generation of GAS depends on possession of NEO, it is arguable that, by controlling the distribution of previously unissued NEO, the NEO Foundation also wields a great degree of indirect influence over the creation and supply of new units of GAS as well. With reference to the criteria above,[78] NEO is therefore arguably politically *centralised*.

(2) Architectural decentralisation

13 Cryptocurrency networks are comprised of multiple computing devices[79] and in that sense possess a degree of architectural decentralisation. However, architectural decentralisation also examines whether a system has a single point of failure.[80] Since the purpose of cryptocurrency networks is to process transactions, in this context "failure" ought to refer to the inability of a network to do so. Accordingly, an architecturally centralised cryptocurrency has a single point of failure, which if compromised, eliminates its ability to process transactions. Using Bitcoin as a case study, it was previously explained that the Bitcoin network relies on nodes known as "miners" to process transactions. As discussed above, anyone operating a node on the Bitcoin network can, with the requisite software, participate in the validation process as a miner. At one point, it was estimated that there were 100,000 miners supporting the Bitcoin network.[81] Miners generally operate full nodes (*ie*, a node maintaining a complete record of transactions on the Bitcoin network) and where they work together as part of a mining pool, the pool administrator maintains a full node.[82] While, as explained above, it is now common for mining nodes to pool their computational power together, this does not detract from the fact that mining nodes on the Bitcoin network may be operated by independent entities and the fact that no mining pool completely controls the validation process, such that if a single mining node (or for that matter, mining pool) fails, this will not compromise the ability of the network to process transactions, as other mining nodes will simply take its place. Bitcoin and similarly designed cryptocurrencies are therefore architecturally decentralised.

---

77 "NEO White Paper" *neo.org* <https://docs.neo.org/docs/en-us/basic/whitepaper.html > (accessed 11 December 2020).

78 See para 10 above.

79 See para 5 above.

80 See para 9 above.

81 "Neighbourhood Pool Watch" <http://organofcorti.blogspot.com/> (accessed 11 December 2020), as cited in Luke Parker, "Number of Bitcoin Miners Far Higher Than Popular Estimates" *Brave New Coin* (12 May 2015) <https://bravenewcoin.com/insights/number-of-bitcoin-miners-far-higher-than-popular-estimates> (accessed 11 December 2020).

82 ecurrencyhodler, "Let's Talk About Bitcoin Nodes" *Hackernoon* (11 November 2017) <https://hackernoon.com/lets-talk-about-bitcoin-nodes-e9502193198c> (accessed 11 December 2020).

B. Trustlessness

14 When used in relation to cryptocurrencies employing blockchain, it is claimed that the "trustlessness" nature of blockchains allows parties to transactions on such networks to trust *the blockchain*, rather than other *users* of the network, to do what a bank would do in transfers of *fiat* money, such as facilitating the transfer and ensuring sender authenticity.[83] To a degree, this claim seems well founded: in the real world, parties trust banks, as known entities with reputations, to handle transactions. However, users of the Bitcoin network and similarly designed cryptocurrencies are pseudonymous.[84] Their identities and any associated reputation therefore cannot be a factor which parties to transactions on these networks rely on as a reason to trust them to verify transactions. In addition, the cryptographic algorithms used by blockchains to verify the creation or transfer of digital records in a distributed network[85] neither eliminate the need for unconfirmed transactions on a cryptocurrency network to be validated by third parties, nor guarantee that its record of transactions will not be tampered with. However, they create a system of incentives for validating unconfirmed transactions and disincentives against tampering with past transactions which *enhances* the ability of parties to transactions on a cryptocurrency network to trust *other users* of the network, as a whole, to validate their transaction and refrain from tampering with past transactions,[86] notwithstanding the fact that these users might be pseudonymous entities, with no reputation which parties might be aware of and rely on as a basis for trusting them.

15 On the Bitcoin network, for instance, under the PoW concept, miners are incentivised to validate unconfirmed transactions through the rewards offered for doing so.[87] Simultaneously, the following features of the network disincentivise malicious actors against withdrawing transactions from a block:

> (a) Hashes are unique to the input data from which they are derived, so any change to that produces a different hash.[88]
>
> (b) The header of a Candidate Block contains the hash of the previous block in the blockchain and the Merkle root of

83 Rebecca M Bratspies, "Cryptocurrency and the Myth of the Trustless Transaction" (2018) 25(1) Mich Telecomm & Tech L Rev 1 at 19.

84 See para 6 above.

85 See para 3 above.

86 Preethi Kasireddy, "ELI5: What Do We Mean by 'Blockchains Are Trustless'?" *Medium* (4 February 2018) <https://medium.com/@preethikasireddy/eli5-what-do-we-mean-by-blockchains-are-trustless-aa420635d5f6> (accessed 11 December 2020).

87 See para 7 above.

88 See para 5 above.

transactions in the Candidate Block, with the Candidate Block's header being hashed to produce an identifying hash for it.[89]

(c) Miners must find the nonce for other miners to accept the Candidate Block, a computationally intensive task taking around ten minutes.[90]

(d) Where competing records of transactions are proposed on the network, it follows the longest chain of blocks.[91]

16 Bearing the above in mind, suppose Bob transfers to Alice 10 BTC for a car ("Transaction A"). Transaction A is validated and is recorded in Block 2 of the blockchain. However, Bob wants to reuse the 10 BTC to purchase a watch, "double-spending" it. To achieve this, Bob has been mining blocks of unconfirmed transactions, *without* broadcasting his solutions to the network, creating a private copy of the blockchain ("Bob's Blockchain") where Transaction A is *not* part of Block 2 (see Figure 2 below). The consequences of this become apparent comparing Bob's Blockchain against the original blockchain. Focusing on Block 1, since transactions in a block are hashed to produce a Merkle root for it[92] and hashes are unique to their input data,[93] removing Transaction A from Block 2 changes its Merkle root. This necessitates finding a new nonce for Block 2, as its existing nonce only produces an identifying hash for it satisfying the Bitcoin protocol when hashed with the information making up Block 2's header on the original blockchain.[94] If the Merkle root as part of the information in Block 2's header changes, the nonce for the block must be recalculated.

89 See para 7 above.
90 See para 7 above.
91 Lam Pak Nian, *Bitcoin in Singapore: A Light-Touch Approach to Regulation* (unpublished LLB thesis, National University of Singapore, archived at the CJ Koh Law Library, National University of Singapore) (2014) at p 20 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2427626> (accessed 10 December 2020).
92 See para 7 above.
93 See para 5 above.
94 See para 7 above.

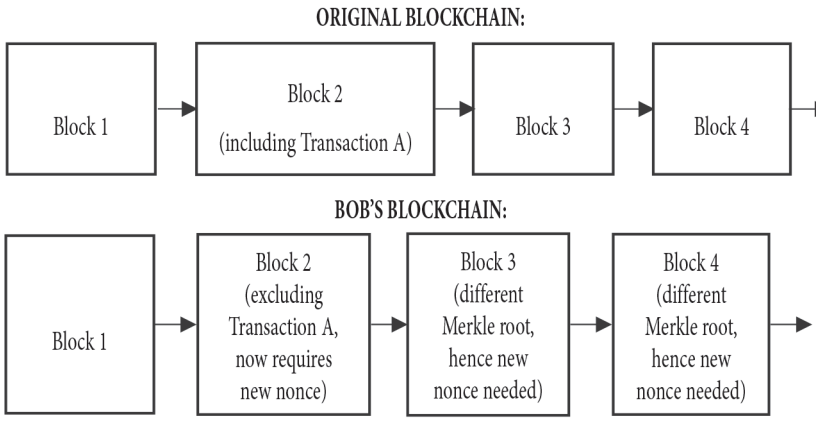

Figure 2

17 These changes in Block 2's Merkle root and nonce, as inputs fed into SHA256, produce a different identifying hash for Block 2. This affects subsequent blocks because each block uses the identifying hash of the previous block as part of the data hashed to produce its own identifying hash.[95] This means that for Block 3, one of the items of data which, when hashed with its existing nonce, produces an identifying hash for Block 3 which satisfies the Bitcoin protocol, is now different. Its existing nonce will not produce a hash satisfying the Bitcoin protocol when hashed with this modified set of data and a new nonce must be found for Block 3. As any change to inputs into a hashing algorithm produces a different result,[96] a change to Block 3's nonce as an input into SHA256 produces a different identifying hash for that block. This causes a similar process to occur in relation to Block 4, which in turn causes a similar process to occur for Block 5 and so on. Therefore, as a result of his alteration of the contents of Block 2, Bob cannot use the nonces of Block 2 and subsequent blocks on the *original* blockchain for the same blocks on Bob's Blockchain. He must find fresh nonces for those blocks. If Bob can do this and broadcast Bob's Blockchain to the network before another miner finds the nonce for the next block of the original blockchain, then since the network follows the longest chain of blocks,[97] Bob's Blockchain will be accepted by the network and Bob can double-spend 10 BTC. Bob has ten minutes to do so, since this is the amount of time another miner will take to find the nonce for the next block of the original blockchain.[98]

95 See para 7 above.
96 See para 5 above.
97 See para 15 above.
98 See para 7 above.

18 Therefore being the first to find the nonce is a matter of computational power.[99] Accordingly, to enable Bob to carry out his fraud, Bob has to find the nonces he requires before another miner finds the nonce for the next block on the original blockchain. Bob therefore needs more computational power than the rest of the network.[100] If malicious actors possess 51% of the computational power supporting the network, they are likely to be successful in altering the blockchain.[101] Such an attack is therefore known as a "51% attack".[102] Fortunately, the expense of amassing the computational power required disincentivises such attacks.[103] In July 2020, it was estimated that renting the computational power necessary to carry out a 51% attack against Bitcoin would cost $358,770 per hour.[104] This combination of incentives to the miners to validate transactions and disincentives against tampering allows parties to transactions on the network to trust the network *and* its pseudonymous users, as a whole, to process transactions and refrain from tampering with past transactions.

19 Cryptocurrencies using PoS, like BlackCoin,[105] also spread users' trust amongst the users of the network *as a whole*. Under PoS, nodes are selected by the algorithm to "mint", *ie*, validate, blocks of unconfirmed transactions.[106] To stand a chance of being selected, node operators "stake"[107] cryptocurrency. The more cryptocurrency "staked", the higher the chance of being selected.[108] Node operators who mint blocks are

99 See para 11 above.

100 Jimi S, "Blockchain Explained: How a 51% Attack Works (Double Spend Attack)" *Good Audience* (5 May 2018) <https://blog.goodaudience.com/what-is-a-51-attack-or-double-spend-attack-aa108db63474> (accessed 11 December 2020).

101 Andreas M Antonopoulos, *Mastering Bitcoin: Programming the Open Blockchain* (O'Reilly Media, Inc, 2nd Ed, 2017) at p 255.

102 Sarwar Sayeed & Hector Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms Against the 51% Attack" (2019) 9(9) Appl Sci 1788 at 4–5.

103 Kelvin F K Low & Ernie G S Teo, "Bitcoins and Other Cryptocurrencies as Property?" (2017) 9(2) *Law, Innovation and Technology* 235 at 251.

104 Crypto51, "PoW 51% Attack Cost" *Crypto51* <https://www.crypto51.app/> (accessed 19 July 2020).

105 Lin William Cong, Zhiguo He & Jiasun Li, "Decentralized Mining in Centralized Pools" George Mason University School of Business Research Paper No 18-9 (2018) at p 39 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143724> (accessed 10 December 2020).

106 Pedro Franco, *Understanding Bitcoin: Cryptography, Engineering and Economics* (Wiley, 2014) at p 234.

107 Generally, this is achieved through transferring cryptocurrency into a "staking wallet" on the relevant network (see Katalyse.io, "Earning Crypto without a Powerful Mining Rig – Stake Your Crypto Today!" *Hackernoon* (6 March 2018) <https://hackernoon.com/earning-crypto-without-a-powerful-mining-rig-stake-your-crypto-today-889df80c8641> (accessed 11 December 2020)).

108 Ameer Rosic, "Proof of Work vs Proof of Stake: Basic Mining Guide" *Blockgeeks* <https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake> (accessed

(cont'd on the next page)

called "forgers" and in return for minting transactions, forgers receive the transaction fees on offer for doing so.[109]

20 Simultaneously, PoS networks disincentivise malicious actors against tampering with records of transactions. Firstly, if transactions validated by a node are discovered to be fraudulent, the responsible node operator may lose its stake and its right to participate as a forger.[110] Secondly, while 51% attacks are still *possible* on PoS networks, the nature of PoS renders such attacks more expensive than they are on PoW networks.[111] In PoS, hashing power is determined by the quantum of cryptocurrency owned by a prospective forger.[112] Accordingly, for Bob to double spend ten BlackCoins, he would need 51% of the supply of BlackCoins. This is *much* more expensive than acquiring the computational power necessary to affect a 51% attack against a PoW cryptocurrency.[113] Furthermore, if an entity amassed 51% of the supply of a cryptocurrency using PoS, it would have no incentive to attack that cryptocurrency, as it would be the single largest holder of that cryptocurrency.[114] This combination of incentives to node operators to validate transactions and disincentives against tampering with past transactions allows parties to transactions on cryptocurrency networks using PoS to spread their trust amongst users of such networks *as a whole*.

21 Finally, it should be noted that if, under the rules of the consensus algorithm used by a cryptocurrency, a single entity is in a position to control the validation of transactions, *eg*, NEO,[115] parties to transactions on this network will effectively be trusting in a *single* entity to validate their transactions.

---

11 December 2020), as cited in Yeong Zee Kin, "Blockchain Records under the Personal Data Protection Act" [2019] PDP Digest 88 at 89.

109 Shaan Ray, "What Is Proof of Stake?" *Hackernoon* (7 October 2017) <https://hackernoon.com/what-is-proof-of-stake-8e0433018256> (accessed 11 December 2020).

110 Shaan Ray, "What Is Proof of Stake?" *Hackernoon* (7 October 2017) <https://hackernoon.com/what-is-proof-of-stake-8e0433018256> (accessed 11 December 2020).

111 Sarwar Sayeed & Hector Marco-Gisbert, "Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack" (2019) 9(9) Appl Sci 1788 at 6–7.

112 Muhammad Saad et al, "Exploring the Attack Surface of Blockchain: A Systematic Overview" (2019) at p 5 <https://arxiv.org/abs/1904.03487> (accessed 11 December 2020).

113 Dev Bharel, "How Proof of Stake Renders a 51% Attack Unlikely and Unappealing" *QTUM* (20 September 2018) <https://blog.qtum.org/how-proof-of-stake-renders-a-51-attack-unlikely-and-unappealing-ddebdc91a569> (accessed 11 December 2020).

114 Pedro Franco, *Understanding Bitcoin: Cryptography, Engineering and Economics* (Wiley, 2014) at p 234.

115 See para 12 above.

C. Immutability

22 There are two ways in which the concept of "immutability" is used. It could imply that once a transaction is appended to the blockchain, it cannot be changed or reversed ("transaction immutability") or it may relate to promises that the code behind the blockchain ("code immutability") is unchangeable.[116] Discussing transaction immutability first, for cryptocurrencies using PoW, altering blockchain records is *technically possible* if one amasses the computational power required.[117] While the cost of doing so may disincentivise 51% attacks,[118] a qualification is made. Some PoW-based cryptocurrencies are supported by a large amount of computational power, rendering it difficult and expensive to acquire 51% of the computational power supporting the network. However, other cryptocurrencies are supported by less computational power, reducing the cost of 51% attacks. For instance, in July 2020, while renting the computational power needed to mount a 51% attack on Bitcoin costs $358,770 per hour, it only costs $5,550 per hour to do the same against Ethereum Classic.[119] Therefore, 51% attacks against some cryptocurrencies utilising PoW are not beyond sufficiently resourced attackers. Evidencing this, Ethereum Classic suffered a 51% attack in 2019.[120] As for cryptocurrencies using PoS, 51% attacks are expensive and illogical but still *technically possible*.[121] Cryptocurrencies utilising PoS are therefore also only *technically* immutable.

23 Turning to code immutability, the code behind a cryptocurrency's blockchain is only as "immutable" as its users decide that it is.[122] The 2016 hack of "The DAO"[123] demonstrates this. The DAO was a smart contract on the Ethereum network, where in exchange for transferring Ether to an

116 Eliza Mik, "Blockchains: A Technology for Decentralized Marketplaces" in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Larry A DiMatteo, Michel Cannarsa & Cristina Poncibò eds) (Cambridge University Press, 2019) ch 9 at p 171.

117 See para 18 above.

118 See para 18 above.

119 Crypto51, "PoW 51% Attack Cost" *Crypto51* <https://www.crypto51.app/> (accessed 19 July 2020).

120 Gareth Jenkinson, "Ethereum Classic 51% Attack – The Reality of Proof-of-Work" *Cointelegraph* (10 January 2019) <https://cointelegraph.com/news/ethereum-classic-51-attack-the-reality-of-proof-of-work> (accessed 11 December 2020).

121 See para 20 above.

122 Rebecca M Bratspies, "Cryptocurrency and the Myth of the Trustless Transaction" (2018) 25(1) Mich Telecomm & Tech L Rev 1 at 36–37.

123 "DAO" stands for "Decentralised Autonomous Organization". See Kelvin F K Low & Eliza Mik, "Pause the Blockchain Legal Revolution" (2019) 69(1) *International and Comparative Law Quarterly* 135 at 170.

address, investors voted on investment proposals.[124] It attracted around US$168m worth of Ether as investment, but in 2016, a hacker exploited a weakness in its code and transferred US$50m of Ether[125] from The DAO to another address ("Dark DAO").[126] Most users of the network voted for a hard fork as the solution,[127] which modified *the code of the Ethereum protocol*[128] to move the misappropriated Ether from the Dark DAO to another address ("Recovery Contract") from which investors could recover their Ether.[129]

IV. The "immutability" of blockchain does not render cryptocurrencies using it "self-regulating"

24 The phrase "self-regulating" suggests that a system can police itself against illegal conduct. It is often argued that the "immutable" nature of blockchain ensures the veracity of transactions on cryptocurrency networks using it, obviating the need for legal or regulatory intervention to ensure this.[130] The discussion above[131] plainly indicates that the premise of this argument, that blockchain records are "immutable", is inaccurate. This argument also conflates the difficulty of altering blockchain records with the legal validity of the same. The consensus algorithms used to decide whether transactions are appended to the blockchain only confirm that *technical* parameters are satisfied (*eg*, for the DBFT algorithm used in NEO, that two-thirds of nodes responsible for validation agree that a proposed record of transactions is valid). It cannot confirm real-world events like whether the private key initiating

124 Antonio Madeira, "The Dao, the Hack, the Soft Fork and the Hard Fork" *CryptoCompare* (12 March 2019) <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/> (accessed 11 December 2020).

125 Klint Finley, "A $50 Million Hack Just Showed that the DAO Was All Too Human" *Wired* (18 June 2016), as cited in Kelvin F K Low & Eliza Mik, "Pause the Blockchain Legal Revolution" (2019) 69(1) *International and Comparative Law Quarterly* 135 at 171.

126 Phil Daian, "Analysis of the DAO Exploit" *Hacking, Distributed* (18 June 2016) <http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/> (accessed 11 December 2020).

127 Antonio Madeira, "The Dao, the Hack, the Soft Fork and the Hard Fork" *CryptoCompare* (12 March 2019) <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/> (accessed 11 December 2020).

128 Kelvin F K Low & Eliza Mik, "Pause the Blockchain Legal Revolution" (2019) 69(1) *International and Comparative Law Quarterly* 135 at 143–144.

129 Vitalik Buterin, "Hard Fork Completed" *Ethereum Blog* (20 July 2016) <https://blog.ethereum.org/2016/07/20/hard-fork-completed/> (accessed 11 December 2020).

130 See para 3 above.

131 See para 22 above.

the transfer was used by its rightful owner.[132] Accordingly, provided they satisfy the technical parameters of the consensus algorithm used by the network concerned, void or voidable transactions may be appended to that network's blockchain. One therefore should not conclude that just because a transaction has been recorded on a cryptocurrency network's blockchain, it is legally valid.

25 The 2016 hack of The DAO demonstrates this. Notwithstanding the use of PoW for Ether,[133] as noted above, the fraudulent transactions had been validated and appended to its blockchain. Users of the network were then confronted with competing philosophies: one camp argued that reversing the transactions was not an option, as this would compromise the "immutability" of the blockchain, while others argued that since it was morally wrong for the hackers to profit from their conduct, the transactions should be reversed.[134]

26 The hard fork chosen as a solution did not eliminate *the record* of the fraudulent transactions, but modified the code of the Ethereum protocol to pool the misappropriated Ether in the Recovery Contract.[135] Three observations are made. Firstly, the validation of the fraudulent transactions by the network demonstrates that blockchain is no safeguard against fraudulent transactions being validated on cryptocurrency networks. Secondly, since most users of Ethereum voted for the hard fork, implicit in their choice was the belief that the satisfaction of a consensus algorithm's technical parameters and the subsequent appending of transactions to a blockchain was insufficient to confer legal validity. Finally, the technical immutability of the Ethereum blockchain had to be *circumvented* for investors to obtain compensation. The technical immutability of the blockchain dictated that removing the record of the fraudulent transactions required 51% of the computational power supporting the network.[136] Yet instead of attempting to do so, most users of the network chose to erase *the effects* of the fraudulent transactions through modifications to the code of the Ethereum protocol. It thus appears that for cryptocurrencies to guard against illegitimate transfers

132 Kelvin F K Low & Eliza Mik, "Pause the Blockchain Legal Revolution" (2019) 69(1) *International and Comparative Law Quarterly* 135 at 141–142.

133 Plans are in place to shift it to Proof of Stake. See Lin William Cong, Zhiguo He & Jiasun Li, "Decentralized Mining in Centralized Pools" George Mason University School of Business Research Paper No 18-9 (2018) at p 39 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143724> (accessed 10 December 2020).

134 Antonio Madeira, "The Dao, the Hack, the Soft Fork and the Hard Fork" *CryptoCompare* (12 March 2019) <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/> (accessed 11 December 2020).

135 See para 23 above.

136 See para 18 above.

and provide their victims with relief, it is insufficient to rely upon the technically immutable nature of blockchain.

V. Legal and regulatory intervention in the cryptocurrency space is *not* impossible

A. A flawed premise

27 As observed above, cryptocurrencies are not *completely* "trustless", "immutable" or "decentralised" in *every case*. At best, *some* cryptocurrencies possess *degrees* of these traits. However, the *degrees* of these traits possessed by *some* cryptocurrencies produce challenges for legal and regulatory intervention in the cryptocurrency space.

28 The first is the identification of targets for regulatory and legal intervention. For instance, data protection legislation like the GDPR or PDPA require the identification of a "data controller" (in the case of the GDPR)[137] or an "organisation" (in the case of the PDPA)[138] for the purposes of regulation. The public keys used by natural persons to transact on cryptocurrency networks using blockchain may be "personal data" under the GDPR and the PDPA, rendering these laws applicable to the "processing" (in the language of the GDPR) or "collection, use or disclosure" (in the language of the PDPA, hereinafter referred to as "CUD") of individuals' public keys on cryptocurrency networks. This in turn raises questions over who the "data controller" (in the case of the GDPR) or "organisation" (in the case of the PDPA) is in relation to the processing or CUD (as the case may be) of individuals' public keys on cryptocurrency networks, whom authorities may hold responsible for compliance with the GDPR or PDPA (as the case may be) and against whom the owners of public keys may exercise their rights under the GDPR or PDPA (as the case may be).

29 Dealing first with the GDPR, Art 4(1) of the GDPR defines "personal data" as any information relating to an identified or identifiable natural person. Recital 26 of the GDPR also provides that data which has "undergone pseudonymisation, which could be attributed to a natural person by the use of additional information" is information on an identifiable natural person. Bearing these points in mind, the French data

137 Matthais Berberich & Malgorzata Steiner, "Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers" (2016) 2 Eur Data Prot L Rev 422 at 424.

138 *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, 2018) at para 2.68.

protection authority ("CNIL") opines that public keys (where these relate to natural persons) constitute "personal data".[139] Whilst it is generally impossible to identify users of cryptocurrency networks from their public keys *alone*, as these are merely alphanumeric strings, identification is possible when public keys are used with other information: users may have disclosed information to exchanges and wallet providers (entities which provide digital wallets which can be used to store and transfer units of cryptocurrency, like Coinbase or Jaxx),[140] where combining such records with public keys could reveal the identities of their users, and public keys can also be traced back to Internet Protocol addresses to identify their users.[141] Techniques like blockchain cluster analysis also allow users to be identified based on their public keys and transaction histories on the blockchain.[142] Keeping this in mind, Art 4(7) of the GDPR defines "data controller" as any natural or legal person that, alone or jointly with others, determines the purposes and means of the processing of personal data. In the absence of an identifiable data controller, the GDPR loses effectiveness, as the data controller is the entity addressed by data subjects[143] when enforcing rights under the GDPR.[144] In cryptocurrency networks, many actors influence the determination of the means and purposes of processing of personal data: in terms of means, miners decide

139 "Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data" *CNIL* (6 November 2018) <https://www.cnil.fr/enblockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data> (accessed 11 December 2020).

140 Financial Action Task Force, "Virtual Currencies – Key Definitions and Potential AML/CFT Risks" (FATF/OECD, 2014) at p 7 <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> (accessed 11 December 2020).

141 Alex Biryukov, Dmitry Khovratovich & Ivan Pustogarov, "Denonymisation of Clients in Bitcoin P2P Network" (2014) <https://arxiv.org/abs/1405.7418> (accessed 11 December 2020), as cited in Michèle Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?" *European Parliamentary Research Service* (July 2019) at pp 26–27 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> (accessed 11 December 2020).

142 Sarah Meiklejohn *et al*, "A Fistful of Bitcoins: Characterizing Payments among Men With No Names" (2013) <https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf> (accessed 11 December 2020), as cited in David Fox, "Cryptocurrencies in the Common Law of Property" in *Cryptocurrencies in Public and Private Law* (David Fox & Sarah Green eds) (Oxford University Press, 2019) ch 6 at para 6.73.

143 A "data subject" is an "identified or identifiable natural person". See Regulation (EU) 2016/679 of the European Parliament and Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, Art 4(1).

144 Matthais Berberich & Malgorzata Steiner, "Blockchain Technology and the GDPR – How to Reconcile Privacy and Distributed Ledgers" (2016) 2 Eur Data Prot L Rev 422 at 424.

what hardware to use for mining and developers and/or the users of the network[145] decide how software should be updated.[146] As for the purposes of processing, since influence over any purpose of processing suffices for an entity to be a "data controller",[147] many entities within cryptocurrency networks can qualify as such within a single transaction: the parties to the transaction who seek to transfer ownership over the cryptocurrency involved, and the miners who seek to claim incentives for processing transactions and/or to maintain the accuracy of the blockchain as a record.[148] In this scenario, it is unclear who the data controllers of the data subjects are under the GDPR.

30 As for the position under the PDPA, s 2(1) of the PDPA defines "personal data" as:

> … data, whether true or not, about an individual who can be identified —
>
> (*a*) from that data; or
>
> (*b*) *from that data and other information to which the organisation has or is likely to have access* …
>
> [emphasis added]

Accordingly, if the user of a public key can be identified using that public key and "other information" which an organisation has or is likely to have access to, that public key may constitute "personal data" under the PDPA. In this regard, it was mentioned earlier that users of public keys may have disclosed information to cryptocurrency exchanges or wallet providers which can be used with those users' public keys to

145 See para 23 above.

146 W Kuan Hon, Christopher Millard & Ian Walden, "Who is Responsible for 'Personal Data' in Cloud Computing? The Cloud of Unknowing, Part 2" Queen Mary School of Law Legal Studies Research Paper No 77 (2011) at p 10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1794130> (accessed 11 December 2020), as cited in Michèle Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?" *European Parliamentary Research Service* (July 2019) at pp 43–44 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> (accessed 11 December 2020).

147 Michèle Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?" *European Parliamentary Research Service* (July 2019) at p 44 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> (accessed 11 December 2020).

148 Michèle Finck, "Blockchain and the General Data Protection Regulation: Can Distributed Ledgers be Squared with European Data Protection Law?" *European Parliamentary Research Service* (July 2019) at pp 43–44 <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf> (accessed 11 December 2020).

identify them.[149] Furthermore, other categories of information which can be used with public keys to identify their users, like the transaction history of a particular public key on a cryptocurrency network,[150] may be information which an organisation is "likely to have access" to. On cryptocurrency networks using blockchain, the record of transactions on the network, from which one can extract the transaction history of a specific public key, is not private information: copies of the ledger are distributed amongst multiple nodes and any user can see the record of transactions on the network. Essentially, it is not implausible that organisations have, or are likely to have, access to information which can be used with individuals' public keys to identify them.

31 However, the classification of public keys of natural persons as "personal data" under the PDPA is complicated by the *Advisory Guidelines on the Personal Data Protection Act for Selected Topics*[151] ("STAG") issued by Singapore's Personal Data Protection Commission ("PDPC"). The STAG indicates that *anonymised* data is not "personal data", where "anonymisation" refers to "the process of removing identifying information such that the remaining data cannot be used to identify any particular individual".[152] In and of itself, this does not complicate the classification of public keys as "personal data" under the PDPA. However, after defining "pseudonymisation" as the replacement of personal identifiers with other references (*eg*, the replacement of an individual's name with a reference number),[153] the STAG lists "pseudonymisation" as an *anonymisation technique* and provides an illustration of the use of anonymised data within an organisation which suggests that pseudonymised data will be considered *anonymised* if an organisation implements controls to prevent one department from using pseudonymised data from another department to re-identify individuals.[154] This would appear to preclude the classification of public keys as "personal data" under the PDPA. Public keys, as alphanumeric strings functioning as personal identifiers for users

149 See para 29 above.

150 See para 29 above.

151 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (24 September 2013; revised 9 October 2019).

152 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (24 September 2013; revised 9 October 2019) at paras 2.6, 3.1 and 3.4.

153 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (24 September 2013; revised 9 October 2019) at para 3.9.

154 Personal Data Protection Commission, *Advisory Guidelines on the Personal Data Protection Act for Selected Topics* (24 September 2013; revised 9 October 2019) at para 3.40, as cited in Benjamin Wong, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012" (2017) 7(4) *International Data Privacy Law* 287 at 297.

of cryptocurrency networks based on blockchain, would be considered "pseudonymised data". If "pseudonymised data" is then considered *anonymised* data, outside the definition of "personal data" under the PDPA, public keys would not constitute "personal data" under the PDPA, such that the PDPA would not apply to the CUD of individuals' public keys on cryptocurrency networks.

32 However, a close reading of the STAG reveals that the PDPC does not *automatically* consider "pseudonymised data" to be anonymised. Paragraph 3.3 of the STAG indicates that:

> 3.3 Data would *not* be considered anonymised if there is *a serious possibility that an individual could be re-identified*, taking into consideration both:
>
> a) the data itself, or *the data combined with other information to which the organisation has or is likely to have access*; and
>
> b) the measures and safeguards (or lack thereof) implemented by the organisation to mitigate the risk of identification.
>
> [emphasis added]

This holds open the possibility that in certain circumstances, "pseudonymised data" may not be *anonymised* data which falls outside the definition of "personal data" under the PDPA. Whether pseudonymised data is anonymised depends on two factors, the first being whether there is a serious possibility that an individual can be re-identified if the data is used with other information which an organisation has or is likely to have access to. With reference to para 30 above, there is a serious possibility that the user of a public key could be identified using that public key and other information which an organisation has or may have access to (*eg*, information provided to cryptocurrency exchanges or wallet providers, transaction histories on the blockchain). The second factor looks at whether there is a serious possibility that an individual can be re-identified having regard to measures and safeguards implemented by an organisation to mitigate the risk of re-identification, leaving open the possibility that where an organisation has not implemented such measures or safeguards, or has implemented *inadequate* measures or safeguards, the public key under consideration should not be considered anonymised data. What emerges is that in some cases, pseudonymised data like public keys on cryptocurrency networks will not be considered anonymised, instead continuing to be treated as "personal data" under the PDPA.

33 The question is then which "organisation" owes obligations under the PDPA in relation to the CUD of public keys. If this is not clear, owners of public keys will be at a loss in terms of whom they should enforce their rights under the PDPA against and the PDPC will have no clear target

which it can hold responsible for PDPA compliance. Unfortunately, the identification of the "organisation" bearing responsibility for PDPA compliance in relation to the CUD of public keys is complicated by two factors: firstly, the range of actors collecting, using or disclosing public keys on cryptocurrency networks, and secondly, the definition of "organisation" under the PDPA. Using a transfer of BTC from Alice to Bob to illustrate this, Alice may have disclosed her public key to Bob to facilitate the transaction. If Alice uses cryptocurrency exchanges or wallet providers, she may also have disclosed her public key to these entities, who may use it to comply with AML and CFT requirements. Alice's public key will also be used by miners to verify her digital signature and when Alice's transaction has been validated and the successful miner broadcasts its solution to the network, the information relating to the transaction, including the public keys involved, forms part of the ledger, which is visible to the entire network. Alice is thus faced with a confusing variety of candidates against whom she might enforce her rights under the PDPA. It is unclear whether she should enforce her rights against one, two, or *all* the parties engaged in the CUD of her public key. The definition of "organisation" under s 2(1) of the PDPA does little to thin the herd. Section 2(1) defines "organisation" as including

> … any individual, company, association or body of persons, corporate or unincorporated, whether or not —
>
> (*a*) formed or recognised under the law of Singapore; or
>
> (*b*) resident, or having an office or place of business in Singapore.

This definition is so expansive that it could apply to *all* the actors in the above example. Fortunately, the PDPC has clarified that Parts III to VI of the PDPA (containing the PDPA's data protection obligations) do not impose obligations on the following:

> (a) individuals acting in a personal or domestic capacity;
>
> (b) employees acting in the course of their employment with an organisation; and
>
> (c) public agencies[155] and organisations in the course of acting on behalf of a public agency in relation to the CUD of personal data.[156]

155 "[P]ublic agency" is defined by s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) to include the Singapore government and its constituent ministries, departments, *etc*.

156 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (23 September 2013; revised 2 June 2020) at paras 2.2 and 6.5. The Personal Data Protection (Amendment) Act 2020 ("2020 Amendment Act"), which amends s 4 of the Personal Data Protection Act 2012 (Act 26 of 2012)

(cont'd on the next page)

These guidelines are somewhat helpful, in that they may assist Alice to eliminate a *few* actors from the running when deciding whom she should enforce her rights under the PDPA against. Should Bob be acting in a personal or domestic capacity, or in the course of his employment with an organisation, Alice can rule him out as the "organisation" against whom she should enforce her rights under the PDPA. She can also rule out public agencies or entities acting on behalf of public agencies in relation to the CUD of her public key.[157] However, the list of categories of individuals and entities excluded from the PDPA's data protection obligations ultimately does not go far enough in clarifying what, in the context of transactions on a cryptocurrency network, is an "organisation" to which the PDPA's data protection obligations apply. Illustrating this, in the fairly common scenario where Alice transfers BTC to an address on a cryptocurrency network controlled by a business, as payment for goods or services, none of the categories of individuals or entities excluded from the application of the PDPA's data protection obligations appear to be relevant, leaving Alice without any meaningful guidance which could otherwise enable her to identify the actor against whom she should enforce her rights under the PDPA.

34 The degree of "trustlessness" possessed by some cryptocurrencies also contributes to the challenge of identifying targets for legal and regulatory intervention. It was explained how the pseudonymous nature of users of the Bitcoin network and similarly designed cryptocurrencies plays a role in granting these cryptocurrencies a degree of "trustlessness".[158] However, the ability of users of these networks to transact without disclosing their identities also complicates the identification of the accused or defendant for the purposes of legal proceedings based on transactions on cryptocurrency networks.

35 The second challenge relates to the issues of jurisdiction and governing law for such proceedings. Questions are raised in this area as cryptocurrency networks are distributed internationally.[159] The problem is compounded by the frequent absence of a central authority administering cryptocurrency networks, whose location might serve as

("PDPA") to impose obligations under Pts III to VI of the PDPA upon entities in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data, has been passed by Singapore's Parliament. When the 2020 Amendment Act comes into effect (on a date to be specified by notification in the Gazette), the range of "organisations" upon which the PDPA imposes obligations will widen further, worsening Alice's confusion in the example above.

157 Though see n 156 above.

158 See para 14 above.

159 See para 4 above.

an "anchor" for the assumption of jurisdiction.[160] This challenge is linked to the issue of identifying targets for regulatory and legal intervention, as it is pointless to discuss jurisdiction or governing law if the accused or defendant cannot be identified.

36 Finally, the "immutability" of blockchain is detrimental where amendment or deletion of the record is required.[161] Article 17 of the GDPR creates a "right to be forgotten", empowering data subjects to require data controllers to erase personal data concerning them. This right, like the right to rectification under Art 16 of the GDPR, requires the medium on which personal data is stored to allow for rectification and erasure of information. A tension therefore exists between the GDPR and the "immutable" nature of the blockchains used by many cryptocurrencies.[162] Similarly, a tension exists between the PDPA and the "immutable" nature of blockchain, as the PDPA also requires the medium on which personal data is stored to allow for rectification and erasure of that data. Section 22 of the PDPA empowers an individual to request an organisation to correct personal data about him which is in the possession or under the control of that organisation, while s 25 of the PDPA requires organisations to cease to retain or anonymise personal data, as soon as it is reasonable to assume that the purpose for which it was collected is no longer served by retention and retention is no longer necessary for legal or business purposes. While s 25 of the PDPA differs from Art 17 of the GDPR as it does not *expressly* confer on individuals the right to have their personal data deleted upon request, Wong suggests that *in practice* the PDPA offers a "right to be forgotten".[163] Wong argues that where the CUD of personal data is based on an individual's consent and that individual withdraws his consent, the conditions triggering an organisation's obligations under s 25 are satisfied.[164] The organisation must then cease to retain the individual's personal data, or anonymise it, despite the absence of an *express* "right to be forgotten" under the PDPA. Regardless of whether Wong's theory is

160 Javier Sebastian Cermeño, "Blockchain in Financial Services: Regulatory Landscape and Future Challenges for Its Commercial Application" 16/20 BBVA Research Working Paper (2016) at p 14 <www.bbvaresearch.com/wp-content/uploads/2016/12/WP_16-20.pdf> (accessed 10 December 2020).

161 Eliza Mik, "Blockchains: A Technology for Decentralized Marketplaces" in *The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms* (Larry A DiMatteo, Michel Cannarsa & Cristina Poncibò eds) (Cambridge University Press, 2019) ch 9 at p 173.

162 Michèle Finck, "Blockchains and Data Protection in the European Union" 18-01 Max Planck Institute for Innovation & Competition Research Paper (2017) at pp 21–24 <https://ssrn.com/abstract=3080322> (accessed 11 December 2020).

163 Benjamin Wong, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012" (2017) 7(4) *International Data Privacy Law* 287 at 295.

164 Benjamin Wong, "Data Privacy Law in Singapore: The Personal Data Protection Act 2012" (2017) 7(4) *International Data Privacy Law* 287 at 295.

correct, what is more significant for organisations storing personal data on blockchains is that regardless of *how* their obligations under s 25 are triggered, if they are triggered in circumstances where it is impossible to anonymise the personal data concerned, these organisations will have to grapple with the difficulties generated by the "immutability" of blockchain when attempting to remove personal data from such data structures.

B. Proposals addressing these challenges

(1) Identifying targets for legal and regulatory intervention

37 This article advances three solutions to address these challenges. The first solution is the use of the identification techniques discussed earlier.[165] The second solution is the introduction of incentives for the use of more "regulable" varieties of cryptocurrencies. Regulatory goals can be achieved through sticks or carrots. The absence of a centralised authority controlling a cryptocurrency only complicates finding parties upon whom to use sticks and does not prevent authorities from offering carrots to the cryptocurrency ecosystem, leaving it to those who wish to enjoy these incentives to identify themselves. While this method of regulation is admittedly uneven, in that only entities in the cryptocurrency ecosystem who wish to benefit from the incentives offered will come forward to identify themselves, cryptocurrencies seem uniquely suited for this method of regulation. A programmer can modify the source code of Bitcoin to create a hard fork and competition then occurs between offshoots of Bitcoin, with preferred platforms prevailing over less efficient competitors.[166] Because Bitcoin is mined using the computational power of its users, the success of an offshoot depends on acquiring and maintaining a user base.[167] This creates an opportunity for regulatory intervention: regulators could offer incentives for the use of Bitcoin variants that abandon or mitigate algorithmic or technical features that complicate regulation, such as the absence of a centralised authority responsible for compliance of the network with laws and regulations, or the pseudonymous nature of its users.

38 This approach is particularly useful in overcoming the challenges posed by the latter feature. Identification techniques are a temporary solution to the problem of user identification, as new technologies for obscuring the identity of users of cryptocurrency networks ("obfuscation

165 See para 29 above.

166 Samuel Elliott, "Bitcoin: The First Self-Regulating Currency?" (2018) 3 LSE Law Review 57 at 67.

167 Samuel Elliott, "Bitcoin: The First Self-Regulating Currency?" (2018) 3 LSE Law Review 57 at 67.

technologies") emerge. For example, the cryptocurrency Monero uses ring signatures for transaction authorisation.[168] A ring signature is a digital signature in which a group of possible signers are grouped together to produce a signature to authorise transactions.[169] It is not possible to determine which person within the group created the ring signature, thereby masking the origin of the transaction.[170]

39 Obfuscation technologies do not necessarily have dishonest objectives[171] and, as will be elaborated upon later, might be exploited to satisfy requests for erasure of personal data. However, a tension exists between data protection and privacy and access to information for the purposes of law enforcement.[172] If obfuscation technologies become the norm, rather than exceptional tools relied upon to give effect to legal rights, the balance tips too far in favour of data protection and privacy, compromising the identification of targets for legal and regulatory intervention. Obfuscation technologies should therefore be contained within reasonable limits. Incentivising the use of more "regulable" varieties of cryptocurrencies is half the equation here, with "chokepoint" regulation[173] (addressed below) being the other.

40 Returning to the use of incentives, the arms race between identification and obfuscation technologies means that user identification is never certain. A longer-term solution to the problem of user identification is therefore stimulating the development of technologies promoting user identification by incentivising their use. Incentives could be offered for the use of cryptocurrency variants designed to *promote*

168 Monero website <https://monero.org/> (accessed 11 December 2020), as cited in Cagla Salmensuu, "The General Data Protection Regulation and Blockchains" *Liikejuridiikka* (2018) at p 10 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143992> (accessed 11 December 2020).

169 Mark, "Monero Ring Signature Explained" *Mycryptopedia* (1 November 2018) <https://www.mycryptopedia.com/monero-ring-signature-explained/> (accessed 11 December 2020).

170 Bill Buchanan, "Ring Signatures and Anonymisation" *Coinmonks* (13 August 2018) <https://medium.com/coinmonks/ring-signatures-and-anonymisation-c9640f08a193> (accessed 11 December 2020).

171 David Fox, "Cryptocurrencies in the Common Law of Property" in *Cryptocurrencies in Public and Private Law* (David Fox & Sarah Green eds) (Oxford University Press, 2019) ch 6 at para 6.70.

172 Robby Houben & Alexander Syners, "Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion" (European Union, 2018) at p 55 <http://www.europarl.europa.eu/supporting-analyses> (accessed 9 December 2020).

173 Dion Blummont, "Blocking the Future? The Regulation of Distributed Ledgers" Victoria University of Wellington Legal Research Paper, Student/Alumni Paper No 37/2017 (2017) at p 37 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3016210> (accessed 12 December 2020).

user identification, *eg*, by avoiding the use of ring signatures. Regulators might offer "official status as a legal means of payment" as an incentive, rendering a cryptocurrency variant more valuable and hence more attractive to mine,[174] driving more users to support it. The attractiveness of this incentive should not be underestimated. Bitcoin started 2017 at below US$1,000, but after the announcement that Bitcoin was a legal means of payment in Japan, Bitcoin surged to over US$1,000.[175] Since one of the key reasons for mining cryptocurrencies is their market value, the grant of status as a legal means of payment can thus be a powerful incentive encouraging mining of more "regulable" variants of cryptocurrencies.

41 Coming to "chokepoint" regulation, most cryptocurrencies cannot function without exchanges and wallet providers[176] and most individuals interact with the blockchains utilised by cryptocurrencies through such intermediaries[177] (the term "intermediaries" is used to refer to cryptocurrency exchanges and wallet providers because of their use as "middle men" to facilitate individuals' interactions with the blockchains employed by cryptocurrency networks – the use of this term as a reference to cryptocurrency exchanges and wallet providers is *not* intended to suggest that, in *every case*, these entities are "data intermediaries", as this term is used in the PDPA),[178] which can be the target of legal and

174 Recall that when a miner is the first to find the nonce for a given Candidate Block, he obtains a reward of BTC. See para 7 above.

175 Chrisjan Pauw, "How Cryptocurrency Prices Work, Explained" *Cointelegraph* (24 July 2018) <https://cointelegraph.com/explained/how-cryptocurrency-prices-work-explained> (accessed 12 December 2020).

176 Asress Adimi Gikay, "Regulating Decentralized Cryptocurrencies under Payment Services Law: Lessons from European Union Law" (2018) 9 Case W Res J L Tech & Internet 1 at 7.

177 Rebecca M Bratspies, "Cryptocurrency and the Myth of the Trustless Transaction" (2018) 25(1) Mich Telecomm & Tech L Rev 1 at 39.

178 According to s 2(1) of the Personal Data Protection Act 2012 (Act 26 of 2012) ("PDPA"), "data intermediary" ("DI") means "an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation". Unlike mere "organisations", when processing personal data on behalf of and for the purposes of another organisation, pursuant to a contract evidenced or made in writing, DIs are not subject to the full range of obligations under the PDPA and only possess responsibilities in relation to the protection and retention of personal data (see s 4(2) of the PDPA). An entity can be a mere "organisation" for some aspects of its operations and a "data intermediary" in relation to other aspects of its operations, with the yardstick for classification being whether the entity, alone or with others, *controls* the collection, processing, use or disclosure of the personal data (see Daniel Seng, "Data Intermediaries and Data Breaches" in *Data Protection Law in Singapore: Privacy and Sovereignty in an Interconnected World* (Simon Chesterman ed) (Academy Publishing, 2nd Ed, 2018) ch 7 at para 7.18 and 7.28 (citing Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"* (00264/1/EN WP 169, 16 February 2010) at p 25)). Building on this, it is suggested that in *some* aspects of their operations,

(cont'd on the next page)

regulatory intervention. Examples of this approach include the PSA and the GDPR. Under the PSA, exchanges are classified as "digital payment token" services subject to AML and CFT requirements.[179] As for the GDPR, CNIL clarifies that users of cryptocurrency networks which "have the right to write on the chain and who decide to send data for validation by the miners", could be "data controllers" where the user is a natural person and the transactions carried out by him are carried out as part of a professional or commercial activity on behalf of other persons, or where the user is a legal entity registering personal data on the blockchain.[180] Where intermediaries do so (*eg*, when a cryptocurrency exchange or wallet provider executes transactions on behalf of a user on the blockchain of the relevant cryptocurrency network, using a public key and address assigned to that user),[181] this appears to put intermediaries within the definition of "data controller".[182] Two points suggest that intermediaries might also be the best candidate when it comes to designating an actor within the cryptocurrency ecosystem as being responsible for PDPA compliance in relation to the CUD of individuals' public keys. Firstly, it was explained above[183] that the definition of "organisation" under the PDPA is broad enough to apply to intermediaries. Furthermore, none of the organisations excluded from the data protection obligations of the PDPA (*eg*, individuals acting in a personal or domestic capacity, public agencies, *etc*)[184] seem to apply to the CUD of public keys by intermediaries. As a matter of law, it is therefore possible to consider intermediaries "organisations" responsible for PDPA compliance. Secondly, in contrast to other actors in the cryptocurrency ecosystem which may qualify as

eg, the collection of individuals' public keys and the use of this information for anti-money laundering and counter financing of terrorism compliance, "organisations" like cryptocurrency exchanges and/or wallets exercise *control* over the collection, processing, use or disclosure of their users' public keys and therefore are not "data intermediaries". This does not rule out the possibility that cryptocurrency exchanges and wallets may not possess such control in relation to other aspects of their operations, being "data intermediaries" in so far as those aspects of their operations are concerned.

179 See para 2 above.

180 CNIL, "Blockchain – Solutions for a Responsible Use of the Blockchain in the Context of Personal Data" *CNIL* (September 2018) <https://www.cnil.fr/sites/default/files/atoms/files/blockchain_en.pdf> (accessed 12 December 2020).

181 See Jiménez-Gomez Briseida Sofia, "Risks of Blockchain for Data Protection: A European Approach" (2020) 36(3) *Santa Clara High Technology Law Journal* 281 at 296 for an example of how cryptocurrency exchanges and/or wallet providers function.

182 Laura Jehl, Robert Muisala & Stephanie Malaska, "Op Ed: 10 Takeaways from Recent French Guidance on Blockchain and the GDPR" *Bitcoin Magazine* (1 November 2018) <https://bitcoinmagazine.com/articles/op-ed-10-takeaways-recent-french-guidance-blockchain-and-gdpr/?utm> (accessed 12 December 2020).

183 See para 33 above.

184 See para 33 above.

"organisations", like miners, intermediaries have an identity which, if not known by individuals and authorities, is easily discoverable and not obscured by the use of a pseudonymous identifier. It is therefore easier to pursue enforcement of the PDPA against intermediaries, rather than other actors in the cryptocurrency ecosystem.

42 Chokepoint regulation complements the introduction of incentives for more "regulable" cryptocurrency variants in addressing the challenge of user identification, such as the use of obfuscation technologies within the cryptocurrency, *eg*, Monero, or by intermediaries. For example, Dark Wallet offers "mix services" for transactions on the Bitcoin network.[185] Suppose Alice wants to transfer 5 BTC to Bob but does not wish to disclose her public key.[186] She can transfer the BTC to an address controlled by a mix service, which then pays 5 BTC to Bob from *another address* it controls and which was paid in by another client, breaking the connection between Alice's public key and the output at Bob's address,[187] making it difficult to use transaction histories to identify users behind public keys. The fact that intermediaries can deploy obfuscation technologies and the fact that most individuals interact with the blockchains used by cryptocurrencies through such intermediaries render it insufficient to rely on incentivising the use of more "regulable" cryptocurrency variants to address the challenge of user identification. Chokepoint regulation supplements this approach, with regulators targeting intermediaries, as *known* entities, to limit their deployment of obfuscation technologies to scenarios where this is justified by law, *eg*, to satisfy erasure requests.[188]

43 A clarification is required. The assumption that, where obfuscation technologies are used, public keys are no longer "personal data", is unwarranted. Where obfuscation technologies are used, whether a public key constitutes "personal data" depends on the technology used

185 Perri Reynolds & Angela S M Irwin, "Tracking Digital Footprints: Anonymity Within the Bitcoin System" (2017) 20(2) *Journal of Money Laundering Control* 172 at 182.

186 Malte Möser, "Anonymity of Bitcoin Transactions" Munster Bitcoin Conference, University of Munster (2013) <https://www.semanticscholar.org/paper/Anonymity-of-Bitcoin-Transactions-An-Analysis-of-M%C3%B6ser/e1aed9296c3af9139f48d15e043e2e8beab55409> (accessed 13 December 2020), as cited in David Fox, "Cryptocurrencies in the Common Law of Property" in *Cryptocurrencies in Public and Private Law* (David Fox & Sarah Green eds) (Oxford University Press, 2019) ch 6 at para 6.70.

187 David Fox, "Cryptocurrencies in the Common Law of Property" in *Cryptocurrencies in Public and Private Law* (David Fox & Sarah Green eds) (Oxford University Press, 2019) ch 6 at para 6.70.

188 See paras 61–62 below, which elaborate on how obfuscation technologies may help address legal obligations to delete personal data from blockchains.

and whether, in the arms race between obfuscation and identification technologies, the obfuscation technology employed can be overcome. If, considering these two factors, identification is possible using the public key and other information, by legal means and without requiring a disproportionate effort,[189] then the public key constitutes "personal data" and questions of identifying data controllers and how rectification and erasure may be affected remain pertinent. Mix services, for example, may not eliminate the possibility of user identification. Mix services need to keep records linking the input of 5 BTC from Alice to the output of 5 BTC at Bob's address and although they usually undertake to destroy these records, if this information is legally obtained it can be used to identify users of public keys.[190]

44 On a smaller scale, "chokepoint *litigation*" might be utilised by victims of wrongful transactions on cryptocurrency networks. The pseudonymous nature of the users of many cryptocurrencies complicates the identification of counterparties to such transactions. Where this proves impossible and victims have dealt through intermediaries, then depending on the facts and circumstances of the case, they may at least proceed against these intermediaries, *as known entities*, to obtain compensation.

(2) Jurisdiction and proper law for prosecutions

45 Prosecutions and civil claims are canvassed separately because of a difference between these types of proceedings. While under private international law a distinction exists between issues of governing law and jurisdiction, for prosecutions the two issues are inseparable: once a State exercises adjudicative jurisdiction,[191] it will apply *its* criminal laws.[192]

46 The first issue is the identification of the accused, which has been dealt with above.[193] Bearing para 45 above in mind, the remaining issue is establishing jurisdiction. This is complicated by the international distribution of cryptocurrency networks and the frequent absence of central authorities administering cryptocurrencies, whose nationality might serve as an "anchor" for the assumption of jurisdiction.[194]

189 *Patrick Breyer v Bundesrepublik Deutschland* [2016] EU:C:2016:779 at paras 45–46.
190 David Fox, "Cryptocurrencies in the Common Law of Property" in *Cryptocurrencies in Public and Private Law* (David Fox & Sarah Green eds) (Oxford University Press, 2019) ch 6 at para 6.71.
191 See n 20 above.
192 Paul Arnell, "The Proper Law of the Crime in International Law Revisited" (2000) 9(1) Nottingham LJ 39 at 42.
193 See paras 37–42 above.
194 See para 35 above.

Extraterritorial jurisdiction may therefore be required for States to exercise jurisdiction over prosecutions based on transactions on cryptocurrency networks, presenting problems under public international law, as the primary basis for exercising prescriptive and adjudicatory jurisdiction is the "territorial principle" which requires the offence to occur within a State and enforcement jurisdiction is strictly territorial.[195]

47 Several proposals address these problems. The territorial nature of enforcement jurisdiction can be overcome through appropriately worded extradition treaties. A State can enforce its laws abroad under the terms of a treaty.[196] Attention must be paid to how the treaty defines extraditable offences: the "enumerative approach" of listing them, or the "eliminative" approach of requiring them to be subject to *a minimum level of punishment* under the laws of each party to the treaty.[197] If the former approach is used, care must be taken to ensure that wrongdoing likely to involve transactions on cryptocurrency networks, such as hacking, is listed as extraditable. Where the eliminative approach is used and a State penalises, for instance, hacking with *less* than the minimum level of punishment required for this offence to be extraditable, it will not be an extraditable offence. To secure the extradition of accused persons for offences based on transactions on cryptocurrency networks, States entering into extradition treaties using the eliminative approach should scrutinise the penalties for offences likely to involve transactions on cryptocurrency networks under the laws of their negotiating partners, ensuring that the relevant offences possess the level of punishment required for them to be extraditable.

48 As for prescriptive and adjudicatory jurisdiction, two arguments are made. Firstly, under the dominant approach to territorial jurisdiction over cross-border offences, the "constituent elements" theory, a State has territorial jurisdiction if a constituent element of a crime occurs within it.[198] Furthermore, the territorial principle has two manifestations: "subjective territoriality", which allows a State to exercise territorial jurisdiction over an act which originated within its territory but was

195 Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at pp 9 and 49.

196 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 479.

197 M Cherif Bassiouni, *International Extradition: United States Law and Practice* (Oceana Publications, 2nd Ed, 1987) at pp 330–331, as cited in John T Soma, Thomas F Jr Muther & Heidi M L Brissette, "Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?" (1997) 34 Harv J on Legis 317 at 324–325.

198 Cedric Ryngaert, "Territorial Jurisdiction over Cross-Frontier Offences: Revisiting a Classic Problem of International Criminal Law" (2009) 9 Int'l Crim L Rev 187 at 187.

completed abroad, and "objective territoriality", which allows a State to do so where an act initiated abroad is completed within it.[199] Considering these points, a State may have territorial jurisdiction over offences based on transactions on cryptocurrency networks where an act which is a constitutive element of the offence originates in the State, but whose effects are consummated outside the State's territory, or the effects felt in the State of conduct that form a constitutive element of the offence originates from outside it.[200]

49 For example, s 378 of Singapore's Penal Code[201] provides that "[w]hoever, intending to take dishonestly any movable property out of the possession of any person without that person's consent, moves that property in order to such taking" commits theft. With movement of property being a constitutive element of theft,[202] the Singapore courts may have territorial jurisdiction to prosecute an accused for theft if, after dishonestly obtaining the private keys of users of the Bitcoin network resident in the US, he uses his computer in Singapore to fraudulently authorise transfers of BTC from those users' addresses to his own. The movement of BTC to effect the dishonest taking, as a constitutive element of theft, originates in Singapore, but its effects are felt elsewhere. The constituent elements theory and the subjective manifestation of territoriality will together enable the Singapore courts to exercise territorial jurisdiction in this case.[203]

---

199 Diane Rowland, Uta Kohl & Andrew Charlesworth, *Information Technology Law* (Routledge, 4th Ed, 2012) at p 30; James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 458; Malcolm Shaw, *International Law* (Cambridge University Press, 7th Ed, 2014) at p 684; Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press, 2nd Ed, 2015) at p 52, as cited in Chia Chen Wei, "Sketching the Margins of a Borderless World: Examining the Relevance of Territoriality for Internet Jurisdiction" (2018) 30 SAcLJ 833 at 845–846.

200 An example is a gun being fired from State A to kill somebody in State B. Where the constituent element relates to the initiation of the crime (the firing of the gun) a State can exercise subjective territorial jurisdiction. Where the constituent element relates to the completion of the crime (the bullet striking the victim), a State can exercise objective territorial jurisdiction. See Jan Wouters *et al*, *International Law: A European Perspective* (Hart Publishing, 2019) at p 443.

201 Cap 224, 2008 Rev Ed.

202 Stanley Yeo, Neil Morgan & Chan Wing Cheong, *Criminal Law in Malaysia and Singapore* (LexisNexis, 3rd Ed, 2018) at paras 13.41–13.42.

203 Section 4B of the Penal Code (Cap 224, 2008 Rev Ed) makes this even clearer. Under s 4B(1)(*a*), "specified offences" will be deemed to have occurred in Singapore, enabling the Singapore courts to exercise territorial jurisdiction, where a physical element of the specified offence has occurred in Singapore. This remains the case even if other physical elements of the specified offence occur outside Singapore. This is consistent with the constituent elements theory. Under s 4B(1)(*b*), a specified offence will be deemed to have occurred in Singapore if a physical element of the specified offence occurs partly in Singapore and partly outside Singapore, whether

(cont'd on the next page)

50 Secondly, aside from the territorial principle, public international law recognises other justifications for the extraterritorial exercise of prescriptive and adjudicatory jurisdiction.[204] The "effects doctrine" gives States jurisdiction over extraterritorial conduct whose effects are felt within the State,[205] even where no constituent element of the offence has taken place within the State.[206] The utility of this doctrine in enabling states to exercise jurisdiction over criminal conduct which, through the use of technology, occurs on a transnational level, was recognised in *Public Prosecutor v Taw Cheng Kong*[207] ("*Taw*"), where the court held that:[208]

> As Singapore becomes increasingly cosmopolitan in the modern age of technology, electronics and communications, it may well be more compelling and effective for Parliament to adopt the effects doctrine as the foundation of our extraterritorial laws in addressing potential mischief.

51 Having regard to *Taw*, it is unsurprising that s 4B(1)(*c*) of the Penal Code allows "specified offences" to be deemed to be committed in Singapore where they "involved an intention to make a gain or cause a loss or exposure to a risk of loss or to cause harm to any person in body, mind, reputation or property, and that gain, loss or harm occurs in Singapore". With "specified offences" covering wrongdoing which may be based on transactions on cryptocurrency networks, such as theft,[209] s 4B(1)(*c*) provides the Singapore courts with a powerful tool to exercise prescriptive and adjudicatory jurisdiction over prosecutions based on transactions on cryptocurrency networks, even where the territorial principle does not ground the exercise of such jurisdiction.

(3) Jurisdiction and proper law for civil claims

52 If the defendant cannot be identified, it is pointless to discuss jurisdiction or governing law. Fortunately, the difficulties posed by the

---

or not other physical elements of the specified offence occur in Singapore. This is consistent with the constituent elements theory and the manifestations of the territoriality principle.

204 M Sornarajah, "Globalisation and Crime: The Challenges to Jurisdictional Principles" [1999] Sing JLS 409 at 411.

205 Danielle Ireland-Piper, *Accountability in Extraterritoriality: A Comparative and International Law Perspective* (Edward Elgar Publishing, 2017) at p 34.

206 Roger O' Keefe, "Universal Jurisdiction: Clarifying the Basic Concept" (2004) 2(3) *Journal of International Criminal Justice* 735 at 739, as cited in Danielle Ireland-Piper, *Accountability in Extraterritoriality: A Comparative and International Law Perspective* (Edward Elgar Publishing, 2017) at p 35.

207 [1998] 2 SLR(R) 489.

208 *Public Prosecutor v Taw Cheng Kong* [1998] 2 SLR(R) 489 at [88].

209 Penal Code (Cap 224, 2008 Rev Ed) s 4B(1)(2), read with para 3 of the Schedule. See para 49 above.

pseudonymous nature of users of the Bitcoin network and similarly designed cryptocurrencies in this regard are surmountable.[210] This subsection therefore focuses on issues of jurisdiction and governing law for claims based on transactions on cryptocurrency networks where the defendant and his location are *known*.

53 Starting with jurisdiction, in common law jurisdictions the basis for exercising personal jurisdiction[211] is service of originating process.[212] Since parties to transactions on cryptocurrency networks can be anywhere and may have dealt through intermediaries located outside the jurisdiction, service out of jurisdiction ("SOJ") will likely be needed for claims based on such transactions. This complicates matters, as leave of court is generally required for SOJ.[213] Under Singapore law, obtaining leave requires the plaintiff to establish, *inter alia*, that the claim comes under one or more grounds for SOJ prescribed by the Rules of Court[214] ("ROC") and that Singapore is the more appropriate forum for the dispute.[215] This demands a substantial connection between the claim and Singapore, which can be difficult to establish for claims based on transactions on cryptocurrency networks due to the transnational elements involved: neither party to a transaction on the Bitcoin network may have been in Singapore at the material time and this transaction will have been validated on an international network lacking any centralised authority in Singapore.

54 Fortunately for parties bringing contract and tort claims based on transactions on cryptocurrency networks, several developments may help. The first is the Singapore International Commercial Court ("SICC"), which has a liberal approach to the assumption of jurisdiction and conservative approach toward declining it. Section 18D(1) of the Supreme Court of Judicature Act[216] provides that, *inter alia*, the SICC has jurisdiction where the action is "international" and "commercial" and satisfies such other conditions as the ROC provides. There is scope for parties to pre-emptively subject disputes to the SICC's jurisdiction. Parties may agree that a claim is "international" and "commercial"

210 See paras 37–44 above.

211 See n 20 above. The focus is put on personal jurisdiction as, at least in Singapore, the court's exercise of its *in rem* jurisdiction is generally viewed as being limited to its admiralty jurisdiction. See *Sunseap Group Pte Ltd v Sun Electric Pte Ltd* [2019] 1 SLR 645 at [95].

212 James Crawford, *Brownlie's Principles of Public International Law* (Oxford University Press, 8th Ed, 2012) at p 472.

213 *Singapore Civil Procedure 2020* vol 1 (Chua Lee Ming & Paul Quan eds) (Sweet & Maxwell, 2019) at para 11/1/1.

214 Cap 322, R 5, 2014 Rev Ed.

215 *Man Diesel & Turbo SE v IM Skaugen SE* [2020] 1 SLR 327 at [27].

216 Cap 322, 2007 Rev Ed.

and under the ROC the SICC has jurisdiction where parties submit to its jurisdiction under a written jurisdiction agreement.[217] The latter is particularly interesting for parties bringing claims based on transactions on cryptocurrency networks as O 110 r 6(2) of the ROC provides that leave is not required for the service of originating process outside of Singapore on a party to a written jurisdiction agreement,[218] benefiting plaintiffs in such claims, as it would otherwise be difficult for them to obtain leave because of the transnational elements involved in transactions on cryptocurrency networks.

55 Since most cryptocurrency users use intermediaries to interact with the blockchains,[219] this, coupled with the difficulties of identification posed by the pseudonymous nature of cryptocurrency users,[220] incentivises victims of fraudulent cryptocurrency transactions to proceed against intermediaries, as *known* entities with (presumably) deep pockets, rather than the counterparties in such transactions, whose identities may not be known. Consequently, in most claims based on transactions on cryptocurrency networks, the user agreements under which intermediaries provide their services will be significant. This provides an opportunity for intermediaries and their users, as likely parties to disputes based on transactions on cryptocurrency networks, to exploit the liberal approach of the SICC towards assumption of jurisdiction to pre-emptively clarify this issue for disputes between them.[221] If in the user agreement parties agree that disputes arising under or in connection with the provision of the intermediary's services are "international" and "commercial" and submit to the exclusive jurisdiction of the SICC, *ie*, inserting an exclusive jurisdiction clause ("EJC"), the SICC will have jurisdiction over disputes between the parties arising under or in connection with the intermediary's services, *without the plaintiff in such disputes having to obtain leave for SOJ*, where the requirements for obtaining leave might otherwise be difficult to satisfy due to the transnational elements involved in transactions on cryptocurrency networks. Regulators may, for instance, tie incentives for the use of a cryptocurrency to the creation of a centralised authority administering that cryptocurrency and condition these incentives on a contract stipulating that disputes arising under or in connection with the use of that cryptocurrency are "international" and "commercial" and containing an EJC in favour of the SICC. This extends the utility of

217 Rules of Court (Cap 322, R 5, 2014 Rev Ed) O 110 rr 1(2)(*a*)(iv), 1(2)(*b*)(iii) and 7.

218 Adeline Chong & Man Yip, "Singapore As a Centre for International Commercial Litigation: Party Autonomy to the Fore" (2019) 15(1) *Journal of Private International Law* 97 at 106.

219 See para 41 above.

220 See para 34 above.

221 This was how the Singapore International Commercial Court had jurisdiction in *B2C2 Ltd v Quoine Pte Ltd* [2019] 4 SLR 17 (see the judgment at [23]).

the SICC's liberal approach towards assumption of jurisdiction beyond claims between intermediaries and their users.

56 The SICC's conservative approach towards declining jurisdiction also merits discussion. To obtain leave for SOJ, Singapore must be the more appropriate forum for the dispute.[222] Under the *Spiliada* test,[223] a comparison is required between Singapore and competing *fora*, assessing the connections each jurisdiction has, to identify the most appropriate forum. This poses difficulties for claims based on transactions on cryptocurrency networks, whose transnational elements render it unlikely that strong connections can be established between Singapore and the dispute. However, O 110 r 8(1) of the ROC provides that the SICC may decline jurisdiction "if it is not appropriate" for the action to be heard by it and r 8(2) provides that the SICC cannot decline jurisdiction "solely on the ground that the dispute between the parties is connected to a jurisdiction other than Singapore, if there is a written jurisdiction agreement between the parties". While it has been held that the "not appropriate" standard in r 8(1) replaces the *Spiliada* test with the *Voth* test[224] of whether Singapore is a clearly inappropriate forum, this has been critiqued on the basis that both tests rely on foreign connections and are thus inconsistent with r 8(2), which precludes relying solely on foreign connections as the basis for the SICC declining jurisdiction.[225] Commentators suggest that it is more consistent with r 8(2) for the "not appropriate" standard to be interpreted in a manner which *does not require comparative evaluation of Singapore with competing fora*.[226] If this is correct, then where an intermediary and one of its users have an EJC in favour of the SICC, the mere fact that the dispute is connected to other jurisdictions apart from Singapore – which is likely, given the transnational elements involved in transactions on cryptocurrency networks – will not be grounds for the SICC to decline jurisdiction.

57 A qualification is required. EJCs can be overridden by rules conferring exclusive jurisdiction over a dispute to the courts of a particular State, based on the subject-matter of the dispute.[227] An example is the

222 See para 53 above.
223 *Spiliada Maritime Corp v Cansulex Ltd* [1987] AC 460.
224 *Voth v Manildra Flour Mills Pty Ltd* (1990) 171 CLR 538.
225 Chng Wei Yao Kenny, "Exploring a New Frontier in Singapore Private International Law: *IM Skaugen SE v MAN Diesel & Turbo SE* [2016] SGHCR 6" (2016) 28 SAcLJ 649 at 661–662, referring to *IM Skaugen SE v MAN Diesel & Turbo SE* [2016] SGHCR 6 at [145].
226 Adeline Chong & Man Yip, "Singapore As a Centre for International Commercial Litigation: Party Autonomy to the Fore" (2019) 15(1) *Journal of Private International Law* 97 at 108.
227 Alex Mills, *Party Autonomy in Private International Law* (Cambridge University Press, 2018) at p 209.

Moçambique rule that a court has no jurisdiction to determine the title to, or the right to possession of, any immovable property situated outside the forum.[228] While the fact that a claim is based on transactions on a cryptocurrency network, *without more*, does not appear to trigger these rules (indeed, even where cryptocurrency is transferred as consideration for title to immovable property situated outside Singapore, while the *Moçambique* rule prevents Singapore courts from trying questions of title to the land, it does not prevent them from adjudicating on and enforcing equitable obligations between and binding on the parties),[229] plaintiffs seeking to exploit the above approach should ensure that the other facts and circumstances of their claim do not trigger these rules, preventing the SICC from exercising jurisdiction.[230]

58 A second development assists plaintiffs to extend the "subject-matter scope"[231] of the EJCs described earlier to *tort* actions. In *The Jian He*[232] ("*Jian*"), the court endorsed a "close connection" test to assess whether tort claims fell within the scope of an EJC covering "all disputes arising under or in connection with" a bill of lading.[233] Under this approach, where the parties' EJC is similarly drafted and the tort claim has a close connection with concurrent claims based on the contract containing the EJC, the tort claim comes within the EJC.[234] Accordingly, where a contract between an intermediary and one of its users contains an EJC in favour of the SICC, whose interpretation is governed by Singapore law[235] and *Jian* is satisfied, the EJC may encompass tort claims between the parties.

59 Two proposals are made regarding the issue of governing law. Firstly, governing law clauses ("GLCs") may address this issue for contractual claims. Most claims based on transactions on cryptocurrency

228 *Murakami Takako v Wiryadi Louise Maria* [2009] 1 SLR(R) 508 at [5] and [9], indicating that this rule – and its exceptions – are part of Singapore law.

229 See n 228 above.

230 Section 18D(1)(*b*) of the Supreme Court of Judicature Act (Cap 322, 2007 Rev Ed) provides that the Singapore International Commercial Court ("SICC") has jurisdiction only where the action is one which the Singapore High Court may hear and try in its original civil jurisdiction. Accordingly, if the Singapore High Court cannot hear a dispute because it transgresses a rule of exclusive subject-matter jurisdiction, the SICC will also be unable to do so.

231 Alex Mills, *Party Autonomy in Private International Law* (Cambridge University Press, 2019) at p 176.

232 [1999] 3 SLR(R) 432.

233 *The Jian He* [1999] 3 SLR(R) 432 at [13] and [15].

234 *The Jian He* [1999] 3 SLR(R) 432 at [14]–[15].

235 The law governing the interpretation of an exclusive jurisdiction clause will usually, but not always, be the governing law of the contract (see *The Jian He* [1999] 3 SLR(R) 432 at [10]; Adrian Briggs, "The Subtle Variety of Jurisdiction Agreements" [2012] LMCLQ 364 at 365).

networks will be between intermediaries and their users.[236] Where these are contractual, a GLC in the user agreement will generally dispose of the issue of governing law, as under Singapore law, in the absence of exceptional circumstances, GLCs render the governing law of the claim that specified by the parties.[237] The utility of GLCs in clarifying the governing law may also extend to *tort* claims between intermediaries and their users if Singapore law governs the interpretation of the GLC. In *Ong Ghee Soon Kevin v Ho Yong Chong*[238] ("*Ong*"), Belinda Ang Saw Ean J held that the issue of whether Singapore law would extend the scope of GLCs to encompass tort claims was still open.[239] Ang J referred to developments which suggest that the scope of GLCs ought to be so extended where disputes between intermediaries and their users are concerned.[240] Firstly, Ang J cited Yeo's argument that extending the scope of GLCs to cover tort claims supports the development of Singapore as a hub for cross-border litigation, with cases having given weight to contractual relationships between parties when dealing with non-contractual obligations.[241] Ang J also cited V K Rajah JA's view (expressed extra-judicially) that where the relationship between parties is primarily contractual, causes of action relating to the contract should be governed by the proper law of the contract.[242] The relationship between an intermediary and its users is primarily contractual, engaging this logic. Finally, Ang J referenced reforms abroad giving effect to party autonomy in choice of law for non-contractual obligations, demonstrating that the extension of the scope of GLCs to encompass tort claims is not unprecedented. Having regard to these developments and pending further judicial analysis of *Ong*, intermediaries and their users might argue that where the interpretation of the GLC in their contract is governed by Singapore law, it may encompass tort claims between them.

60 The second proposal deals with proprietary claims based on transactions on cryptocurrency networks. While the question of whether cryptocurrencies constitute property has been left open under Singapore law, it is clear that under English and New Zealand law respectively, they constitute a form of intangible property.[243] However, one encounters

236 See para 55 above.
237 Peh Teck Quee v Bayerische Landesbank Girozentrale [1999] 3 SLR(R) 842 at [12].
238 [2017] 3 SLR 711.
239 Ong Ghee Soon Kevin v Ho Yong Chong [2017] 3 SLR 711 at [107].
240 *Ong Ghee Soon Kevin v Ho Yong Chong* [2017] 3 SLR 711 at [108]–[109].
241 Yeo Tiong Min, "The Effective Reach of Choice of Law Agreements" (2008) 20 SAcLJ 723 at 742.
242 V K Rajah, "Judicial Dynamism in International Trade in Hong Kong and Singapore – An Indivisible Link" (2010) 40 HKLJ 815 at 822.
243 *Quoine Pte Ltd v B2C2 Ltd* [2020] 2 SLR 20 at [144]; *AA v Persons Unknown* [2020] 4 WLR 35 at [55]–[59]; *Ruscoe v Cryptopia Ltd* [2020] NZHC 728; [2020] 22 ITELR 925 at [69], [102], [120], [125], [128], [132] and [133].

problems applying the choice of law approaches for intangible property to cryptocurrencies. One approach ascribes a notional *situs* to intangible property,[244] with unique rules for each type of intangible property: intellectual property rights for example are situated in the jurisdiction whose law governs their existence,[245] whilst shares may be situated where the relevant company was incorporated.[246] These rules are inappropriate for cryptocurrency: cryptocurrencies do not depend on the law of any jurisdiction for their existence, and in so far as Bitcoin is concerned, there is no entity which "issues" BTC.[247] More generally, when notice is taken of the fact that cryptocurrency networks are distributed internationally and often lack a central authority located in any jurisdiction,[248] trying to pin down a *situs* for cryptocurrencies seems pointless. Accordingly, the UK Jurisdiction Taskforce ("UKJT") has abandoned the search for a notional *situs* for cryptocurrencies, instead proposing a multi-factorial approach for determining the governing law of proprietary claims relating to cryptocurrencies.[249] Building on this proposal, should the Singapore courts recognise cryptocurrency as property in the future, they should consider the following when determining the proper law for proprietary claims based on transactions on cryptocurrency networks:[250]

(a) where any relevant off-chain *physical* asset is located (should the cryptocurrency be used as asset tokens);

(b) whether there is any centralised control over the relevant network in a particular jurisdiction;

244 J M Carruthers, *The Transfer of Property in the Conflict of Laws* (Oxford University Press, 2005) at paras 1.31–1.34, as cited in Michael Ng, "Choice of Law for Property Issues Regarding Bitcoin under English Law" (2019) 15(2) *Journal of Private International Law* 315 at 326

245 *Dicey, Morris & Collins on the Conflict of Laws* (Lord Collins of Mapesbury & J Harris Eds) (Sweet & Maxwell, 15th Ed, 2017) at para 22-051, as cited in Michael Ng, "Choice of Law for Property Issues Regarding Bitcoin under English Law" (2019) 15(2) *Journal of Private International Law* 315 at 331.

246 Michael Ng, "Choice of Law for Property Issues Regarding Bitcoin under English Law" (2019) 15(2) *Journal of Private International Law* 315 at 328.

247 Michael Ng, "Choice of Law for Property Issues Regarding Bitcoin under English Law" (2019) 15(2) *Journal of Private International Law* 315 at 328 and 331–332.

248 See para 35 above.

249 UK Jurisdiction Taskforce, "Legal Statement on Cryptoassets and Smart Contracts" (November 2019) at para 99 <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> (accessed 14 December 2020).

250 UK Jurisdiction Taskforce, "Legal Statement on Cryptoassets and Smart Contracts" (November 2019) at para 99 <https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf> (accessed 14 December 2020).

(c) whether the particular units of cryptocurrency are controlled by a user of the relevant network in a particular jurisdiction (*eg*, because a private key is stored there); and

(d) the law applicable to the relevant transfer of cryptocurrency.

(4) Technical immutability of blockchain

61 The technical immutability of blockchain may not be anathema to the GDPR or the PDPA. Article 17 of the GDPR does not define "erasure", permitting interpretations which dispense with the need for deletion.[251] Some national laws implementing the GDPR take a "softer" interpretation of "erasure": under German law, in cases of non-automated processing, deletion is not insisted upon if this is impossible or requires a disproportionate amount of effort *due to the mode of storage used*, and in such scenarios an alternative solution of *limiting* processing of the relevant personal data is permitted.[252] Keeping this in mind and having regard to the fact that the technical immutability of blockchain renders it unrealistic to expect intermediaries, as data controllers,[253] to modify a blockchain to omit transactions involving specific public keys,[254] in the context of public keys as personal data stored on a cryptocurrency's blockchain, erasure requests ought to be satisfied where intermediaries *approximate* deletion, by employing obfuscation technologies to limit the extent to which cryptocurrency linked to a public key can continue to be associated with it and hence (through re-identification techniques) with its user. For example, assume an intermediary which creates key pairs for its users on the Bitcoin network receives an erasure request from Alice regarding her public key. The intermediary might satisfy this request by:

(a) transferring cryptocurrency under Alice's address to an address controlled by it ("A") and then transferring, from another address controlled by it ("B"), to a new address created for Alice ("C"), a corresponding amount of cryptocurrency which was transferred to B by another user (essentially, acting as a mix service); and

(b) once (a) is done and where permitted under applicable laws and regulations, deleting its records relating to such mixing.

251 Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press, 2018) at p 108.

252 Michèle Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press, 2018) at p 108.

253 See para 41 above.

254 See para 18 above.

With reference to the discussion on how user identification might be achieved notwithstanding the use of mix services,[255] this limits the possibility that cryptocurrency at C can be traced to Alice's public key and hence, using identification techniques, Alice. Admittedly, under this approach, transactions preceding the erasure request which involved Alice's public key remain on the blockchain and information relating to these transactions can be used with her public key to identify Alice as its user. However, the removal of these transactions from the blockchain ought not to be required to satisfy Alice's erasure request given the disproportionate effort required by the intermediary to do so,[256] leaving this approach as the closest *approximation* of deletion achievable in the circumstances. Users of intermediaries might try to abuse this approach to shield cryptocurrency, under the guise of erasure requests, from being traced to their public keys for the purposes of prosecutions or civil claims. Article 17(3)(e) of the GDPR guards against this, providing that erasure requests may be refused to the extent that processing of personal data is necessary for the establishment, exercise or defence of legal claims. Intermediaries can thus refuse erasure requests when notified that the public key in question contains the proceeds of criminal conduct.

62 It is also arguable that intermediaries need not remove transactions involving individuals' public keys from a cryptocurrency's blockchain to satisfy their obligations under s 25 of the PDPA. Section 25 provides that when the purpose for which personal data was collected by an organisation is no longer served by its retention and retention is no longer necessary for legal or business purposes, that organisation has two options, namely:

> (a) "cease to retain its documents containing personal data"; *or*
>
> (b) "remove the means by which the personal data can be associated with particular individuals".

PDPC guidelines regarding (b) suggest that intermediaries may satisfy their obligations under s 25 by deploying obfuscation technologies to limit the extent to which individuals can continue to be linked to their public keys. Paragraph 3.3 of the STAG indicates that the successful anonymisation of personal data depends on whether there is a "*serious* possibility that an individual could be re-identified" [emphasis added], having regard to the data, or the data combined with other information which the organisation has or is likely to have access to and measures and safeguards implemented by the organisation to mitigate the risk of

255 See para 43 above.
256 See para 18 above.

identification. It is worth noting that the test is not whether there is a *possibility* of re-identification, taking these factors into account, but is whether there is a ***serious*** *possibility* of re-identification, considering both factors. This suggests that, where intermediaries have mitigated the risk of identification by deploying obfuscation technologies to limit the extent to which individuals can be linked to their public keys, the fact that these technologies do not remove the *possibility* of those individuals being re-identified (*eg*, see the explanation above on how mix services can be beaten),[257] does not mean that the public keys have not been anonymised. Instead, if the obfuscation technologies used have the consequence that those individuals cannot be re-identified without great expense and effort, one might argue that the measures and safeguards implemented by the intermediary to mitigate the risk of identification are such that no *serious* possibility of re-identification exists. In this scenario, if the intermediary does not have and is not likely to have access to information which would enable it to re-identify those individuals (*ie*, the first factor in the test for whether personal data is anonymised), the intermediary will have satisfied its obligations under s 25 of the PDPA, notwithstanding its failure to remove transactions involving those individuals' public keys from the relevant cryptocurrency's blockchain.

63 Turning to the right of rectification under Art 16 of the GDPR, this provision has two dimensions: the completion of incomplete personal data and the rectification or deletion of inaccurate personal data.[258] Since public keys are generated from private keys using an algorithm,[259] it is mathematically impossible for a public key to be *incomplete*. However, if the person on whose behalf the public key was generated was not who he claimed to be, the public key is "inaccurate" because it fails to reflect reality and discloses untrue information.[260] So if Alice dishonestly uses personal information about Bob to open an account with a wallet provider, which generates a key pair for "Bob" on a cryptocurrency network, then insofar as that public key might be used with customer information possessed by the intermediary to identify *Bob* as its owner, the public key is "inaccurate".

257 See para 43 above.

258 Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International Publishing, 2017) at pp 154–156.

259 See para 5 above.

260 C Worms, "Art 16 DSGVO" in *Beck'scher Online-Kommentar Datenschutzrecht* (Heinrich Wolff & Stefan Brink eds) (C H Beck, 18th Ed, 2016) and Boris Paal, "Art 16 DSGVO" in *Beck'sche Kompaktkommentare Datenschutz-Grundverordnung* (Boris Paal & Daniel Pauly eds) (CH Beck, 1st Ed, 2017), as cited in Paul Voigt & Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide* (Springer International Publishing, 2017) at p 155.

64 Under Recital 39 of the GDPR, inaccurate personal data should be rectified or deleted. However, a public key cannot be "rectified" as it is the product of passing a private key through an algorithm. It therefore cannot be altered unless the private key passed through the algorithm is changed. Deletion is therefore the sole option. However, the technically immutable nature of blockchain renders it unrealistic to expect intermediaries to modify the relevant cryptocurrency's blockchain to omit transactions involving "Bob's" public key.[261] Fortunately, Art 5(1)(d) and Recital 39 of the GDPR provide that "reasonable" steps must be taken to erase inaccurate personal data. Technical limitations inherent in the mode of storage of personal data therefore should be acknowledged when addressing requests for the deletion of inaccurate public keys from blockchains,[262] such that deletion is not insisted upon. Instead, such requests should be satisfied where steps are taken to *limit* the possibility that the requesting user will continue to be associated with the public key. In the context of the above example and assuming the wallet provider manages its users' private keys, this may require it to:

(a) amend its records relating to "Bob's" public key to reflect the fact that Bob is not its user;

(b) freeze the account which Alice used on their platform as "Bob", so no further transactions involving "Bob's" public key can originate from that account; and

(c) publicise the fact that "Bob's" public key was fraudulently created and that cryptocurrency ought not to be transferred to the associated address.

65 The approach in the preceding paragraph may also satisfy the demands of s 22 of the PDPA, which empowers an individual to request organisations to correct inaccurate personal data about him in their possession or under their control. Unless the organisation is satisfied on reasonable grounds that the correction should not be made, it must correct the personal data as soon as practicable.[263] At this juncture, it is important to note that s 11(1) of the PDPA provides that in meeting their responsibilities under the PDPA, organisations "shall consider what a reasonable person would consider appropriate in the circumstances". Paragraph 9.4 of the PDPC's *Advisory Guidelines on Key Concepts in the*

261 See para 18 above.

262 Michèle Finck, "Blockchains and Data Protection in the European Union" Max Planck Institute for Innovation & Competition Research Paper No 18-01 (2017) at p 22 <https://ssrn.com/abstract=3080322> (accessed 11 December 2020).

263 Personal Data Protection Act 2012 (Act 26 of 2012) s 22(2).

Personal Data Protection Act[264] indicates that "[i]n determining what a reasonable person would consider appropriate in the circumstances, an organisation should consider *the particular circumstances it is facing*" [emphasis added]. Whether an organisation complies with its obligations under the PDPA therefore depends on the circumstances in which the organisation operates. Accordingly, when assessing whether an intermediary facilitating an individual's interactions with a blockchain-based cryptocurrency has satisfied its obligations under s 22 of the PDPA in relation to that individual's public key, the technical limitations of blockchain as a mode of storage of personal data must be considered. The expense and effort required to delete information stored on blockchain suggest that it is not realistic to demand that intermediaries remove transactions involving that individual's public key from the blockchain. Instead, an intermediary's obligations under s 22 should be considered satisfied where, in a manner akin to that described in the preceding paragraph, it has taken steps to *limit* the possibility that the individual making the s 22 request can continue to be associated with his public key.

VI. Conclusion

66 Looking at the proposals for cryptocurrency regulation canvassed in this article, it appears that while new and innovative laws or regulatory approaches are needed to address the challenges for legal and regulatory intervention posed by cryptocurrencies, *existing* legal tools and doctrines should not be ignored as a source of solutions to those challenges. On one hand, it was shown that choice of law approaches for proprietary claims relating to intangible property were inappropriate for proprietary claims relating to cryptocurrencies. In this context, the UKJT's proposed test for the proper law of proprietary claims relating to cryptocurrencies represents the sort of legal innovation necessary to adapt the law to the challenges posed by new technologies. On the other hand, the proposals dealing with the challenges posed by cryptocurrencies, in terms of the ability of courts to establish jurisdiction, demonstrate that *existing* legal tools and doctrines can address the problems posed by new technologies. Extradition treaties are not a novel legal tool and doctrines like the constituent elements theory and subjective territoriality are not new either. Yet these have been shown to be of use in addressing the challenges for legal and regulatory intervention posed by cryptocurrencies. The lesson for courts and regulators is therefore that addressing the challenges posed by new technologies is not only a matter of looking to the future and developing fresh legal solutions, but also requires drawing inspiration

264 Personal Data Protection Commission, *Advisory Guidelines on Key Concepts in the Personal Data Protection Act* (23 September 2013; revised 2 June 2020).

from the past by exploring whether existing legal tools and doctrines can address these challenges.