Bitcoin Burglaries and The Theft Act 1968

Alex Taylor*
Dr. Micheál Ó Floinn**

Introduction

On 22nd January 2018, masked intruders kicked down the door to the Oxfordshire home of Danny Aston and Amy Jay, directors of Aston Digital Currencies Ltd.[1] After entering, they reportedly threatened the couple with a firearm, struck Mr Aston over the head, and issued their demands. They wanted payment in Bitcoin.[2]

Bitcoin is the best-known example of a type of virtual currency called a cryptocurrency. Since the release of its open-source code in 2009, thousands of alternative cryptocurrencies have been developed.[3] Some have become extremely valuable assets,[4] which can be traded for real-world goods and services or exchanged for traditional currencies. The significance of Bitcoin's underlying technology extends beyond its ability to sustain viable virtual currencies, and cryptocurrencies now form part of a broader class of 'cryptoassets'.

Although cryptoassets are used for both legitimate and illegitimate purposes, their unique characteristics have made them targets for criminals.[5] Cryptoasset transactions are generally irreversible, and relatively simple steps can be taken to make it difficult, if not impossible, to link them to a particular individual. It is therefore unsurprising that they have been the target of advanced cyber-attacks.[6]

However, it appears that a less sophisticated form of attack, exemplified by the Oxfordshire case, is emerging. As users employ tougher technological measures to protect their cryptoassets from remote threats, they render *themselves* the most vulnerable points of attack. Why should a criminal go to the trouble of orchestrating an expensive, time-consuming cyber-attack, which is increasingly unlikely to prove fruitful, when he could simply beat the victim with a rubber hose until he or she

* Pupil Barrister at 4 Pump Court, Temple, London.
** Lecturer in Criminal Law, University of Glasgow.
We would like to thank David Ormerod, Lindsay Farmer and the reviewer for their comments on an earlier draft.

[1] T Diver, 'Britain's first Bitcoin heist as trader forced at gunpoint to transfer cyber currency' *The Telegraph* (London, 28 January 2018) <https://www.telegraph.co.uk/news/2018/01/28/britains-first-bitcoin-heist-trader-forced-gunpoint-transfer/> accessed 28 November 2020.
[2] The heist was ultimately unsuccessful. See A French, 'Gang targeting bitcoin traders fled empty-handed' (Oxford, 30 January 2018) <https://www.oxfordmail.co.uk/news/15907000.gang-targeting-bitcoin-traders-fled-empty-handed/> accessed 28 November 2020.
[3] At the time of writing, CoinMarketCap.com lists almost 8000 cryptocurrencies in its index - see CoinMarketCap, 'All Cryptocurrencies' <https://coinmarketcap.com/all/views/all/> accessed 28 November 2020.
[4] The value of a single Bitcoin peaked on 17 December 2017 at £15,351.65, and the total value of all cryptocurrencies in circulation is estimated at the time of writing to be over half a trillion US dollars - see CoinMarketCap (fn. 3).
[5] CipherTrace values losses attributable to cryptoasset-related crime in 2019 at USD $4.5bn – see 'Q4 2019 Cryptocurrency Anti-Money Laundering Report' (CipherTrace, 11 February 2020) <https://ciphertrace.com/wp-content/uploads/2020/02/CipherTrace-CAML-2019-Q4-20200220.pdf> accessed 28 November 2020. One study estimates that around $76bn of illegal activity per year involves Bitcoin: see S Foley, J R Karlsen and T J Putniņš, 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed Through Cryptocurrencies?' (2019) 32(5) Review of Financial Studies 1798.
[6] See e.g. N Reiff, 'The Largest Cryptocurrency Hacks So Far' (Investopedia, 25 June 2019) <https://www.investopedia.com/news/largest-cryptocurrency-hacks-so-far-year/> accessed 28 November 2020.

provides the password?[7] The Oxfordshire attack was the first widely-reported 'rubber hose attack' targeting cryptoassets to take place in the UK, but similar incidents have been reported worldwide with increasing frequency since at least February 2015.

On the basis of the reported facts, there can be little doubt that the perpetrators of the Oxfordshire heist committed a firearms offence, as well as at least one offence against the person. However, it is less clear what crimes might have been committed specifically in relation to the cryptoassets. If the perpetrators had instead targeted a painting in the house, or the money in Mr Aston's wallet, they could clearly be charged with one or more property-based offences. Does the same hold true when cryptoassets are the target? This paper seeks to answer that question by examining the applicability of the offences of theft and burglary under the Theft Act 1968 ('TA 1968') in the context of 'rubber hose' attacks targeting cryptoassets. The thesis advanced is that the TA 1968 is capable of embracing wrongdoing in relation to this new asset class and, in particular, that cryptoassets are capable of being stolen. However, a number of interpretative challenges and uncertainties remain. We highlight these areas and suggest routes for the criminal courts to take when called to resolve them.

Cryptoassets: Background[8]

(1.1) From Virtual Currencies to Cryptoassets

Before Bitcoin, several attempts were made to create a virtual currency[9] capable of competing with traditional 'fiat' currencies.[10] A prominent obstacle faced by developers was the 'double spending problem'; since virtual tokens were nothing more than units of data, a mechanism was needed to prevent users from simply copying and pasting new 'coins'. Early implementations solved the problem by relying on trusted parties to issue tokens and clear transactions. However, this dependence on trust, combined with small user bases, meant that they failed to command widespread adoption.[11]

[7] The term 'rubber-hose cryptanalysis' is commonly used in the field of cryptography as a euphemism for extracting cryptographic secrets from a person by coercion, such as beating them with a rubber hose.

[8] The analysis in this section is necessarily brief. For more detail, see *inter alia* A Narayanan et al, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton University Press, 2016); A Judmayer et al, *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and their Consensus Mechanisms* (Morgan & Claypool, 2017); F Schar, *Bitcoin, Blockchain, and Cryptoassets: A Comprehensive Introduction* (MIT Press, 2020). For a briefer introduction targeted at "legal and other professional advisors", see J Bacon et al, 'Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers' (2018) 25 Rich. J.L. & Tech 1. Compelling analysis with a legal focus can be found in *inter alia* D Fox and S Green (eds), *Cryptocurrencies in Public and Private Law* (OUP, 2019); C Brummer (ed), *Cryptoassets: Legal, Regulatory, and Monetary Perspectives* (OUP, 2019); D Armstrong et al, *Blockchain and Cryptocurrency: International Legal and Regulatory Challenges* (Bloomsbury, 2019); L Sagar, *The Digital Estate* (Sweet & Maxwell, 2018).

[9] The term 'virtual currency' can be interpreted extremely broadly. See, for example, the definition given in Financial Action Task Force, 'Virtual Currencies: Key Definitions and Potential AML/CFT Risks' (2014) <http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf> accessed 28 November 2020. It is recognised that this will need to be further refined - see FATF, '12-month Review Virtual Assets and VASPs' (2020) <www.fatf-gafi.org/publications/fatfrecommendations/documents/12-month-review-virtual-assets-vasps.html> accessed 28 November 2020 (para 50).

[10] For more on the evolution of virtual currencies prior to Bitcoin, see B Geva, 'Cryptocurrencies and the Evolution of Banking, Money, and Payments' in Brummer (fn. 8); Narayanan (fn. 8) Chapter 1; Judmayer (fn. 8) 1-18.

[11] Judmayer (fn. 8) 16.

Bitcoin was announced in a white paper released by its pseudonymous creator, 'Satoshi Nakamoto', in October 2008.[12] Nakamoto outlined how cryptographic techniques, combined with incentive engineering and a distributed consensus mechanism, could be used to create a secure, pseudonymous,[13] decentralised virtual currency which solved the double-spending problem with minimal reliance on trust. Bitcoin launched in January 2009.

In simple terms, Bitcoin is a system that allows users to securely transfer monetary value, without any central entity, like a bank, overseeing or verifying the process. What is revolutionary is that it facilitates the remote peer-to-peer exchange of intangible virtual tokens in a way that mimics 'in-person' transactions involving tangible items.[14] At the click of a button, X can 'send' bitcoins to Y. Without the need for any intermediary or referee, both parties can be sure that X had sufficient bitcoins to spend, that they were not spent twice, and that the transaction has completed irreversibly. These characteristics allow bitcoins to be ascribed value by the community in which they are used, meaning that they can be used as payment for goods or services, or exchanged for fiat currency such as sterling.

The technology underpinning Bitcoin has facilitated the creation of numerous cryptography-based systems in which users can deal in a range of different 'cryptoassets'.[15] In crypto*currency* systems, like Bitcoin itself, the cryptoasset is an intangible token representing monetary value. In other systems, the things represented include access rights, equities and securities.[16] However, in all cryptoasset systems the tokens may be the subjects of dealings between users, and the underlying technology is, for present purposes, broadly similar.[17] Thus, cryptocurrencies are just one kind of cryptoasset, and the latter terminology is preferred herein.[18]

(1.2) How Cryptoasset Systems Work

For illustrative purposes, let us consider the hypothetical situation in which Alice has five cryptoassets – 'ExampleCoins' – and wants to send two to Bob.

A cryptoasset system is founded on a software protocol – a set of rules – to which all participating users, or rather the devices through which they interact with the system, must adhere. These rules prescribe *inter alia* the nature and specifications of the cryptoasset and the procedures for authenticating and verifying transactions. By running software that complies with the

---

[12] S Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' (The Bitcoin Project, first uploaded 31 October 2008) <https://bitcoin.org/bitcoin.pdf> accessed 28 November 2020.

[13] The majority of cryptoassets are not truly anonymous, as is sometimes suggested. The level of privacy afforded to users depends on "application requirements and associated technical design decisions" - see Bacon et al (fn. 8) 8. For a recent paper discussing the ways in which cryptoasset transactions may be de-anonymised, see Alex Biryukov and Sergei Tikhomirov, 'Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis' (2019) 2019 IEEE European Symposium on Security and Privacy (EuroS&P) 172-184.

[14] This point is helpfully illustrated by N Custodio, 'Still Don't Get Bitcoin? Here's an Explanation Even a Five-Year-Old Will Understand' (Coindesk, 20 March 2020) <https://www.coindesk.com/bitcoin-explained-five-year-old> accessed 28 November 2020.

[15] UK Jurisdiction Taskforce (UKJT), 'Legal Statement on Cryptoassets and Smart Contracts' (Lawtech Delivery Panel, 22/11/2019) available for download at <https://technation.io/about-us/lawtech-panel/> accessed 28 November 2020 (hereinafter 'LSCSC') paras 23-32; Brummer (fn. 8) 1-3.

[16] For an overview of the various types of cryptoassets, see A Haynes and P Yeoh (eds), *Cryptocurrencies and Cryptoassets: Regulatory and Legal Issues* (Routledge, 2020) paras 3.7.1-3.7.16.

[17] Ibid.

[18] It should be noted, however, that the terminology in this area is not standardised – see LSCSC (n15) para 26 and the citations at fn. 12 therein.

ExampleCoin protocol on internet-enabled devices, Alice, Bob, and all other participants connect together to form a peer-to-peer (P2P) network[19] of 'nodes'.

At the heart of the P2P network is a master ledger recording every transaction to have taken place in the ExampleCoin system and their order. In ExampleCoin, like most cryptoasset systems, all users are free to store a copy of the ledger and inspect the information recorded in relation to each transaction 'address'. Addresses are simply unique alphanumeric identifiers generated by individual users, which serve as 'destinations' to which cryptoassets can be 'sent' in a transaction.[20] Thus, when we say that Alice 'has five ExampleCoins', we mean that the ExampleCoin ledger records, as the result of a transaction or series of transactions, a value of five in relation to an 'address' or addresses controlled by Alice. However, since no personal information is required to create an address, the fact that it is controlled by Alice will not be ascertainable without further information.[21] The data stored on the ledger may therefore be viewed as pseudonymous. [22]

Alice and Bob rely on 'wallet' software to make the process of managing, sending and receiving ExampleCoins more intuitive.[23] Despite its name in common parlance, this software is not a repository, but simply a tool for interacting with the cryptoasset system, and it could take the form of a mobile 'app' or a desktop computer program.[24] Before making a transaction, Alice and Bob will each have used their wallet software to generate mathematically-related pairs of cryptographic 'keys' – strings of data – one of which can be revealed publicly, and one of which must be kept private. The *private* key is used to initiate dealings with ExampleCoins, since it allows the holder to attach uniquely valid 'signatures' to outgoing transactions. The *public* key can be used:

(a) to generate the addresses referred to above, and

(b) to verify that a signature was made by the holder of its associated private key.

Once Alice and Bob have agreed to proceed with a transaction, Bob uses his wallet software and public key to generate an address, before providing it to Alice.

Cryptoasset transactions take the form of messages broadcast publicly throughout the P2P network. Alice uses her wallet software to create a transaction message specifying the quantity of ExampleCoins to be sent from her address or addresses, and the destination address provided by Bob.

---

[19] This is a network in which participants connect to one another directly, rather than via a central server.

[20] 'Addresses' are used in UTXO-based systems like Bitcoin, whereas 'accounts' are used in 'account-based' systems like Ethereum. The difference is not material to the legal discussion below, and the term 'address' is used for simplicity. However, the distinction is material from both a technological and an accounting perspective. See J Clifford, 'Intro to Blockchain: UTXO vs Account based' (Medium, 20 September 2019) <https://medium.com/@jcliff/intro-to-blockchain-utxo-vs-account-based-89b9a01cd4f5> accessed 28 November 2020.

[21] See above (fn. 13) and T Robinson, 'Bitcoin is not anonymous' (ResPublica, 24 March 2015) <https://www.respublica.org.uk/disraeli-room-post/2015/03/24/bitcoin-is-not-anonymous/> accessed 28 November 2020.

[22] Bitcoin addresses may be thought of as a 'transparent safe' – see 'How bitcoin transactions work' <https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/> accessed 28 November 2020. However, some ledgers are 'permissioned', meaning transaction details can only be inspected by certain authorised individuals, and new technology may allow for the verification of fully anonymous transactions - see 'How Is Blockchain Verifiable by the Public and yet Anonymous?' (ConsenSys, 13 January 2020) <https://consensys.net/blog/enterprise-blockchain/how-is-blockchain-verifiable-by-the-public-and-yet-anonymous/> accessed 28 November 2020.

[23] Wallet software is not essential; the various processes described below can be carried out manually by executing suitable computer code.

[24] There are many forms of wallet, but they are generally grouped as software, hardware or paper wallets.

Transaction messages need to be authenticated using a cryptographic process that generates a unique 'signature' derived from (but not including) the specific contents of the message[25] and the sender's private key. Accordingly, Alice uses her wallet software to sign the transaction message with her private key. She then initiates the transaction by broadcasting the signed message, along with her public key, throughout the P2P network. Each time the transaction message passes through a node, its authenticity is verified using Alice's public key. Only valid transactions are routed onward.

A crucial point to note is that the initiation of a transaction does *not* lead to ExampleCoins being 'deposited' into Bob's 'wallet'. This and similar terminology implying a close analogy with transactions involving traditional notes and coins, although common, is apt to confuse. Rather, cryptoasset transactions take effect by being recorded on the authoritative ordered ledger of transactions. This is necessary to prevent Alice from double-spending her ExampleCoins.

Rather than trusting a central entity to store and maintain the ledger, a cryptoasset system distributes responsibility for doing so throughout participants in the P2P network. Typically, the protocol prescribes a process in which users can partake in order to reach agreement on the validity and order of transactions, whilst simultaneously providing incentives for them to do so.[26] The effect of this 'distributed ledger technology' (DLT) is to create a system of 'rule by consensus', highly resistant to tampering by any individual,[27] "in which self-interest acts in favour of the collective interest, and the two are mutually reinforcing".[28]

Having initiated the transaction, Alice must wait for other users of the ExampleCoin network to reach consensus that it should be recorded on the ExampleCoin ledger. This may take anything from a few minutes to a few hours, depending on the nature of the 'consensus mechanism' built into the protocol. When such consensus is reached, it will be possible to consult the ledger and see a value of two recorded at the destination address provided by Bob. At this point, the transaction may be regarded as complete, and Bob is able to use his private key to initiate a further transaction with the ExampleCoins recorded at his address.

[25] Changing any element of the transaction message will yield a different signature. Thus, once a signature has been attached to a message, any subsequent modification of the message will invalidate it.
[26] Bitcoin, for example, introduced the most popular form of Distributed Ledger Technology (DLT), known as 'Blockchain', in which users recognise as authoritative the version of the ledger which has been subjected to the most computational effort. Users acting as 'miners' compile discrete lists – known as 'blocks' – of the transactions messages they receive, then compete to solve computationally-intensive cryptographic puzzles in relation to them. Solving a block confers an entitlement, under the protocol rules, to have it accepted by other users and added to a 'chain' of previously solved blocks, thus forming a single master ledger of transactions in an agreed order. The incentive to solve a block comes from the promise of a reward generated by the protocol and/or transaction fees.
[27] Cryptoasset systems are not completely immune in this regard. For example, a 'proof-of-work' system like Bitcoin could be manipulated by an entity which amasses more than 50% of the computational power in the network. A helpful summary of "51% attacks" and other cryptoasset vulnerabilities is provided by G Sugurdsson et al, 'Vulnerabilities and Security Breaches in Cryptocurrencies' in P Ciancarini et al (eds), *Proceedings of 6th International Conference in Software Engineering for Defence Applications* (Springer, 2019) 288-299.
[28] S Green, 'Cryptocurrencies: The Underlying Technology' in Fox and Green (fn. 8) 5.

(2) Prosecuting Rubber-Hose Attackers

(2.1) 'Rubber-Hose' Attacks

There is much in the nature of cryptoassets to attract criminality. Cryptoasset systems facilitate unmediated pseudonymous transfers of value, which can be harnessed by criminals in the commission of crimes like terrorist financing, money laundering and tax evasion. But the (speculative) value of these cryptoassets and the general irreversibility of transactions also make them the target of criminality in and of themselves. To date, the overwhelming majority of attacks targeting cryptoassets have been carried out remotely in relation to the victim. The use of viruses,[29] ransomware[30] and SIM swapping,[31] and deceptive practices like phishing are commonplace. However, in recent years there have been numerous reports of cases in which attackers have sought to obtain cryptoassets through direct contact with victims, including in their homes.[32] Some have apparently involved extreme violence, such as that of the Dutch trader tortured with a drill in front of his four-year-old daughter.[33]

Whilst the Oxfordshire heist[34] remains the only known case of its kind in the UK, it is possible that more have gone unreported.[35] In any event, it is reasonable to suppose that similar attacks will take place in the future.[36] Cryptoasset-related crime is on the rise in general,[37] and advances in cyber-security, along with heightened community awareness, are making successful remote attacks increasingly difficult and expensive.[38] For some criminals, 'beating the victim with a rubber hose' may come to be viewed as an economical mode of operation.

---

[29] E.g. E Lam, 'Hackers Steal $40m Worth of Bitcoin from Binance Exchange' (Bloomberg, 8 May 2019) <https://www.bloomberg.com/news/articles/2019-05-08/crypto-exchange-giant-binance-reports-a-hack-of-7-000-bitcoin> accessed 28 November 2020.

[30] Such as the infamous 'WannaCry' software that swept the world in 2017.

[31] E.g. B Winck, 'One cryptocurrency investor reportedly lost $24 million worth of bitcoin in a SIM swap attack' (Business Insider, 11 November 2019) <https://markets.businessinsider.com/currencies/news/bitcoin-investor-loses-24-million-of-crypto-sim-swap-hackers-2019-11-1028677818> accessed 28 November 2020.

[32] See N Popper, 'Bitcoin Thieves Threaten Real Violence for Virtual Currencies' (The New York Times, 2 February 2018) <https://www.nytimes.com/2018/02/18/technology/virtual-currency-extortion.html> accessed 28 November 2020. A list of known physical attacks targeting cryptoassets has been compiled by developer Jameson Lopp, although not all of the reports listed can be verified – see J Lopp, 'Known Physical Bitcoin Attacks' (Github) <https://github.com/jlopp/physical-bitcoin-attacks> accessed 28 November 2020.

[33] A Cuthbertson, 'Bitcoin Trader Brutally Tortured with Drill in Cryptocurrency Robbery' (The Independent, 5 March 2019) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-robbery-torture-cryptocurrency-netherlands-a8807986.html> accessed 28 November 2020. See also A Cuthbertson, 'Bitcoin Millionaire Jumps off Balcony After Being Threatened with Shotgun' (The Independent, 9 September 2019) <https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-cryptocurrency-robbery-norway-millionaire-gun-a9097576.html> accessed 28 November 2020.

[34] Diver (fn. 1).

[35] It has been suggested that victims around the world 'do not see the point' in reporting cryptoasset-related crime to the police - see G Chavez-Dreyfuss, 'RPT-Hacked, scammed and on your own: navigating cryptocurrency 'wild west'' (Reuters, 18 October 2018) <https://www.reuters.com/article/crypto-currency-crime/rpt-hacked-scammed-and-on-your-own-navigating-cryptocurrency-wild-west-idUSL2N1WX10G> accessed 28 November 2020.

[36] Unfortunately, there are no official statistics. The largest annual private-sector analysis of cryptoasset-related crime is provided by US-based company CipherTrace Inc (fn. 5), but its most recent report does not mention physical attacks, and it does not define the kinds of activity referred to as 'hacks and thefts'.

[37] CipherTrace (fn. 5).

[38] This may be evidenced by the fact that the number of hacks targeting cryptoassets decreased in 2019 compared to 2018, whereas cryptoasset-related crime in general increased significantly – see CipherTrace (fn. 5).

(2.2) Three Working Scenarios

It is illustrative to conduct the legal analysis below with reference to three hypothetical scenarios. Although it is possible to conceive of others, these will help to highlight some of the key issues that arise in the areas considered.

(1) An attacker, D, points a gun at the victim, V, and demands that V transfer cryptoassets to a cryptoasset address controlled by D. V initiates the transaction using his private key.

(2) D points a gun at V and demands that V reveal his private key. V provides the key, and D uses it to initiate a transfer of cryptoassets to a cryptoasset address controlled by D.

(3) V holds an account with a centralised online exchange platform, Xchange, which allows V to exchange cryptoassets for other cryptoassets, as well as fiat currency for cryptoassets and vice versa. V can instruct Xchange to initiate transactions on his behalf. D points a gun at V and orders V to use the Xchange platform to request a transfer of cryptoassets to a cryptoasset address controlled by D. Xchange carries out this transaction request.

(2.3) Why consider property offences?

It seems intuitive to view D's conduct in the above scenarios as giving rise to a property-based offence.[39] This would certainly be the case if, rather than targeting cryptoassets, D demanded cash from V's wallet, or a bank transfer. However, the unique nature of cryptoassets makes the above scenarios harder to square with the offences that might, at first glance, appear to have been committed. This gives rise to a risk that the legal significance of D's actions may not properly be characterised and/or presented to the jury.

The murkiness of this area may even lead prosecutors to avoid charging rubber-hose attackers with seemingly 'trickier' offences in the first place, and instead select charges which fail to "reflect the seriousness and extent of the offending".[40]

For example, let us assume that the facts of Scenario (2) are capable of supporting *inter alia* charges of robbery and an offence under s. 1 of the Computer Misuse Act 1990 (CMA 1990).[41] The latter might seem tempting, since its *actus reus* is exceptionally wide,[42] and the CMA 1990 has been relied on in cases where the defendant has 'taken' the victim's virtual assets.[43] However, this charge will clearly not, by itself, reflect the true nature of D's wrongdoing, and this remains the case even if the CMA 1990 offence is charged in conjunction with an offence against the person. Only a charge

[39] It is common to see references to cryptoasset 'theft' and 'stealing' not only in the media, but also by law enforcement agencies. See for example: 'Oxford man arrested over £8.7m cryptocurrency theft' (BBC News, 23 January 2019) <https://www.bbc.co.uk/news/uk-england-oxfordshire-46980658> accessed 28 November 2020; 'Victims of cryptocurrency theft urged to contact regional cyber crime unit' (Avon and Somerset Police, 1 October 2019) <https://www.avonandsomerset.police.uk/news/2019/06/victims-of-cryptocurrency-theft-urged-to-contact-regional-cyber-crime-unit/> accessed 28 November 2020.

[40] Crown Prosecution Service, *The Code for Crown Prosecutors* (8th edn, 2018) para 6.1. There is evidence to suggest that this has already happened in the United States – see G Bischoping, 'Prosecuting Cryptocurrency Theft with the Defend Trade Secrets Act of 2016' (2018) 167 U. Pa. L. Rev. 239, 243-246.

[41] These facts could also sustain a charge of assault, but this is not immediately relevant.

[42] It is established if D 'causes a computer to perform any function'.

[43] See e.g. *R v Ashley Mitchell* (Exeter Crown Court, 3 February 2011) (virtual poker chips); *R v Stephen Burrell* (Northampton Magistrates Court, 28 Nov 2018) (Runescape coins).

of robbery reflects the fact that D acted dishonestly, 'took' something which did not belong to him, and threatened force in order to do so.

The selection of charges which accurately reflect the defendant's conduct is itself important for at least two reasons. The first is that this is necessary to equip the court with adequate sentencing powers.[44] In the above example, a charge of robbery would expose D to the possibility of life imprisonment,[45] but under s. 1 CMA 1990 he would face a maximum of two years (or five years if charged under s. 2). The second reason relates to the principle of fair labelling.[46] All offences, by their names and descriptions, act as labels communicating information about the conduct of those by whom they are committed.[47] Failure adequately to label D's offending could result in improper decisions being taken regarding D's future treatment within the criminal justice system, as well as deprive external parties of information necessary to evaluate D's character.[48]

(3) The Basic Offence of Theft

According to s. 1(1) of the Theft Act 1968 (TA 1968):

> *A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it […]*

(3.1) What is the 'Property'?

Property is defined in s. 4(1) TA 1968 as including "money and all other property, real or personal, including things in action and other intangible property". What could be property in the scenarios outlined above? One candidate common to all three is the cryptoassets themselves. In Scenario (2), an additional possibility is V's private key. In Scenario (3), V's rights against Xchange may constitute choses in action capable of being stolen.

(3.1.1) The Cryptoassets

Whether cryptoassets constitute property has been the subject of much literature, and the issue has been considered by courts around the world. In England, the issue has arisen primarily in interim civil proceedings, although it has also been relevant in a small number of cases under the Proceeds of Crime Act 2002 (POCA). It technically remains the case that no reported English decision has *conclusively* resolved the issue, though they all strongly indicate that cryptoassets are properly characterised as property.

(3.1.1.1) Cryptoassets as property

[44] As prosecutors are required to do in the selection of charges – see CPS Code (fn. 40) para 6.1.
[45] Theft Act 1968, s 8(2).
[46] This was famously defined as the principle that "widely felt distinctions between kinds of offences and degrees of wrongdoing are respected and signaled by the law, and that offences should be divided and labeled so as to represent fairly the nature and magnitude of the law-breaking" – A Ashworth, *Principles of Criminal Law*, (4th edn, OUP, 2003) 89–90.
[47] J Chalmers and F Leverick, 'Fair Labelling in Criminal Law' (2008) 71(2) M.L.R 217.
[48] ibid 224-239.

Before considering whether cryptoassets qualify as property, it is sensible first to consider precisely what it is that might be said to constitute the locus of any proprietary rights. It will be seen from explanation in Section 1.2 above that a cryptoasset comes to be *represented* by data recorded on a distributed transaction ledger. However, this data cannot be equated with the cryptoasset itself.[49] The data is of no value, and it may be replicated infinitely and by anyone. Even if a user were to modify a data entry in a copy of the ledger, this would not have the effect of increasing the quantity of cryptoassets associated with it.

The distribution of decision-making power throughout a cryptoasset system means that the data representing a cryptoasset is only capable of being used as the basis for an effective transaction when agreement is reached within the network that this is permitted by the rules of the protocol. Thus, a cryptoasset *itself* – as distinct from the data by which it is represented – is properly conceptualised as an intangible construct that arises from this interplay between public and private data, system rules and network consensus.[50]

(3.1.1.2) Arguments for Viewing Cryptoassets as Property

Academics and practitioners appear to speak with one voice on the characterisation of cryptoassets as property.[51] Probably the most authoritative extrajudicial assessment is the 'Legal Statement on Cryptoassets and Smart Contracts' (hereinafter 'LSCSC'), published in November 2019 by the LawTech Delivery Panel's UK Jurisdiction Taskforce,[52] in which the authors conclude:[53]

> *(a) cryptoassets have all of the indicia of property;*
>
> *(b) the novel or distinctive features possessed by some cryptoassets—intangibility, cryptographic authentication, use of a distributed transaction ledger, decentralisation, rule by consensus—do not disqualify them from being property;*
>
> *(c) nor are cryptoassets disqualified from being property as pure information, or because they might not be classifiable either as things in possession or as things in action;*
>
> *(d) cryptoassets are therefore to be treated in principle as property.*

[49] See LSCSC (fn. 15) paras 26, 60, 63 and 65. The LSCSC is cited on this point with approval by Gendall J in *Ruscoe and Moore v Cryptopia Ltd* [2020] NZHC 728 [120]-[121]. This view is also recognised by David Fox, however, he reserves judgment on the extent to which they should be, or indeed need to be, separated for purposes of analysis – see D Fox, 'Cryptocurrencies in the Common Law of Property' in Fox and Green (fn. 8) 154-155.
[50] See LSCSC (fn. 15) para 65 and Sagar (fn. 8) paras 4-86-4-90 and 4-95.
[51] See, for example, the arguments put forward in: Fox (fn. 8); Sagar (fn. 8); Bacon et al (fn. 8); J Perkins & J Enwezor, "The Legal Aspect of Virtual Currencies" (2016) 31 Butterworths J. Int'l Banking & Fin. L. 569; N McGrath, 'Transacting in a Vacuum of Property Law' (TLI Think! Paper 22/2016, 25 April 2016). <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2786206> accessed 1 October 2020.
[52] The LawTech Delivery Panel describes itself as an "industry-led, government-backed initiative, established to support the transformation of the UK legal sector through tech". As was observed by Bryan J in *AA v Persons Unknown* [2019] EWHC 3556 (Comm) [56]: "The UKJT is chaired by Sir Geoffrey Vos, and Sir Antony Zacaroli is also a member. However, neither in their judicial capacity was responsible for the drafting of the legal statement, nor have either in their judicial capacities endorsed that legal statement". The Legal Statement was prepared by Laurence Akka QC, David Quest QC, Matthew Lavy and Sam Goodman.
[53] UKJT Legal Statement (fn. 15) para 15.

Although the LSCSC is not a binding precedent, it has been cited with approval by courts in England[54] and New Zealand.[55]

Drawing broadly from the literature, the case for recognising cryptoassets as a species of property may be summarised as follows.[56] First, it is said that cryptoassets are theoretically capable of being the objects of proprietary rights, as they exhibit characteristics commonly identified as hallmarks of property.[57] Most importantly for the purposes of English law, cryptoassets satisfy the criteria identified in *Ainsworth,*[58] and applied in subsequent decisions.[59] In *Ainsworth*, Lord Wilberforce stated:[60]

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

Cryptoassets are "definable" and "identifiable by third parties" because it is possible to determine, with reference to the rules of the protocol and the values recorded on the ledger in relation to a particular public key, both the specifications of the cryptoasset, and how many are controlled by the holder of the corresponding private key. Cryptoassets are, by their nature, "capable of assumption by third parties", and they possess at least the same degree of "permanence" and "stability" as other recognised forms of property.[61]

Secondly, it is said that cryptoassets can be accommodated within English common law's taxonomy of property rights, even though they cannot be physically possessed, nor characterised as enforceable rights of action.[62] This argument takes two forms. The strongest is that the common law does not *only* recognise as property those things which can be classified as either "things in possession" and "things in action"; rather, the distinction is material only where classification under one of these headings is determinative of the applicability of a particular statute, cause of

---

[54] *AA v Persons Unknown* [2019] EWHC 3556 (Comm), [2020] 4 WLR 35.
[55] *Ruscoe* (fn. 49).
[56] This summary draws on the literature citated at fn. 51 and the LSCSC (fn. 15). However, it should be noted that an alternative methodology has been put forward by Low and Teo, who suggest that the property relating to a cryptoasset may be conceptualized as a right to have one's address appear as the last entry on the ledger in relation to a particular cryptoasset – see Kelvin FK Low and Ernie GS Teo, 'Bitcoins and Other Cryptocurrencies as Property?' (2017) 9(2) Law, Innovation and Technology 235.
[57] Fairfield considers that cryptoassets possess the characteristics of transferability, persistence, rivalry, scarcity, and delineation – see JAT Fairfield, 'BitProperty' (2015) 88(4) Southern California Law Review 805. For the identification of other proprietary characteristics, see McGrath (fn. 51) Section IV; G Ishmaev, 'Blockchain Technology as an Institution of Property' (2017) 48(5) Metaphilosophy 666; R Sarel, 'Your Bitcoin is Mine: What does Law and Economics Have to Say About Property Rights in Cryptocurrencies?' (21 February 2020) available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542545> accessed 28 November 2020, p.31; Fox (fn. 49) paras 6.12-6.27.
[58] *National Provincial Bank v Ainsworth* [1965] AC 1175 (HL).
[59] *Armstrong DLW GmbH v Winnington Networks Ltd* [2012] EWHC 10 (Ch), [2013] Ch 156; *Re Celtic Extraction Ltd* [2001] Ch 475 (CA). For extrajudicial application of the *Ainsworth* test to cryptoassets, see LSCSC (fn. 15) paras 49-57; Fox (fn. 49) para 6.39; Sagar (fn. 8) para 4-93; Bacon (fn. 8) paras 179-183; Perkins and Enwezor (fn. 51) 569-570; McGrath (fn. 51). For judicial application, see *AA* (fn. 54) [59] and *Ruscoe* (fn. 49). Cryptoassets were also found to satisfy the *Ainsworth* test by the Singapore International Commercial Court in *B2C2 Ltd v Quoine Pte Ltd* [2019] SGHC(I) 03 [142], but it was decided on appeal ([2020] SGCA(I) 02 [144]) that the issue did not need to be decided as it was immaterial to the case.
[60] *Ainsworth* (fn. 58) 1247-1248
[61] On this last point, however, see LSCSC (fn. 15) paras 53-56 and the discussion of 'unstable cryptoassets' below.
[62] The traditional view that English law only recognises two types of property derives from the judgment of Fry LJ in *Colonial Bank v Whinney* (1885) 30 Ch. D. 261 (CA) 285-286.

action or remedy.[63] The less far-reaching form of the argument is that, even if the common law *does* demand such binary classification, the term "thing in action" is capable of encompassing intangible property other than enforceable rights of action.[64] Both lines of argument draw on a series of cases in which it was held that tradable permissions and quotas, granted pursuant to various statutory regimes, constituted property, even though they were intangible and conferred no enforceable rights.[65] It is also noted that various statutes, including the TA 1968, specifically refer to intangible property "other" than things in action.[66]

Finally, it is said that cryptoassets are not to be disqualified from proprietary status on the basis that information cannot be property.[67] Arguments to this effect are examined in greater detail below.

(3.1.1.2) Civil Cases

In three civil cases, the High Court has been prepared to treat cryptoassets as property for the purposes of granting interim injunctions.[68] The third of these cases, *AA v Persons Unknown,*[69] gives greatest consideration to the property issue. Granting an application for an interim proprietary injunction in respect of 96 bitcoins, Bryan J endorsed the LSCSC,[70] applied the *Ainsworth* criteria, and concluded that bitcoins were property, even if they could not be described as things in action "on a narrow definition of that term".[71]

These cases cannot be regarded as *conclusively* settling the proprietary status of cryptoassets. In none was the issue the subject of full argument before the court,[72] and it was only necessary for the judges to be persuaded to the standard required in an interim injunction application.[73] It is also possible that a different conclusion could be reached beyond the context of injunctive relief. Nonetheless, these decisions amount to persuasive authority. The judgment in *AA* clearly endorses the theoretical arguments in favour of recognising cryptoassets as property, and all three cases demonstrate a willingness on the part of the judiciary to do so.

Reasoned decisions of the courts of Singapore[74] and New Zealand provide additional support for the notion that cryptoassets qualify as property for the purposes of English law. The most extensive treatment of the subject is to be found in *Ruscoe,* a decision of the High Court of New

---

[63] This version of the argument is put forward by the authors of the LSCSC (fn. 15) paras 66-84 and endorsed in both *AA* (fn. 54) [58]-[59] and *Ruscoe* (fn. 49) [123]-[125]. It is also recognized by Fox (fn. 49) paras 6.28-6.44.
[64] In *Armstrong* (fn. 59) [61], Stephen Morris QC, sitting as a deputy High Court Judge, stated that the concept of a chose in action could potentially encompass "wider matters of property" beyond enforceable rights of action. This version of the argument is also put forward by the LSCSC (fn. 15) paras 66-84, and McGrath (fn. 51).
[65] *Attorney General of Hong Kong v Nai-Keung* [1987] 1 WLR 1339 (PC), *In re Rae* [1995] BCC 102 (Ch); *Swift v Dairywise Farms Ltd* [2000] 1 WLR 1177 (Ch); *In re Celtic Extraction Ltd* [2001] Ch 475 (CA); *Armstrong* (fn. 59).
[66] LSCSC (fn. 15) para 83.
[67] ibid paras 59-65.
[68] *Robertson v Persons Unknown* (Commercial Court, 15th July, 2019) (asset preservation order); *Elena Vorotyntseva v Money-4 Limited t/a Nebeus.Com* [2018] EWHC 2596 (Ch) (freezing order with proprietary component); *AA* (fn. 54) (proprietary injunction). A useful note of *Robertson* is provided by M Jones, 'Time to clarify the legal status of cryptocurrencies?' (Practical Law, 31 October 2019).
[69] *AA* (fn. 54).
[70] ibid [57].
[71] ibid [58]-[61].
[72] *Roberton* was an urgent *ex parte* application, and the proprietary status of cryptoassets was not disputed in *Vorotyntseva*. In *AA,* only the applicant attended the hearing and filed submissions.
[73] Accordingly, in AA (fn. 54) [63], Bryan J stated that he was "satisfied at least to the level required for the purposes of this application for interim relief that Bitcoins constitute property".
[74] See the Singaporean decisions in *B2C2* (fn. 59).

Zealand.[75] In that case, Gendall J cited relevant English cases[76] and the LSCSC with approval, applied the *Ainsworth* test, and held that cryptoassets were property for the purposes of the Companies Act 2006 "and also probably more generally".[77] Gendall J also noted that his conclusion aligned with public policy considerations.[78]

(3.1.1.3) Proceeds of Crime Cases

In two cases the Crown Court has granted orders which presuppose the proprietary status of cryptocurrencies. In *Teresko,*[79] Surrey Police succeeded in obtaining a restraint order, pursuant to s. 41 POCA, over 295 bitcoins. Restraint orders are only available in respect of "realisable property" held by the defendant,[80] but whether the bitcoins satisfied this requirement was not an issue before the Crown Court.[81]

In *West,*[82] a confiscation order was made against a defendant from whom 82 bitcoins had been seized by police. The quantum of the order included the value of the bitcoins at a rate of roughly £8,500 each.[83] By s. 7(2)(a) POCA, the amount payable under a confiscation order is capped at the 'available amount', which is defined as "the total of the values … of all the *free property* then held by the defendant". However, the order in *West* was agreed, and HHJ Korner was not asked to decide whether the bitcoins constituted "free property".[84]

Teresko and *West* cannot be said to provide *strong* support for the notion that cryptoassets constitute property. The issue was not disputed in either case, and it is arguable that a wide conception of 'property' is justified by the purpose of the PoCA regime, especially the provisions on investigatory seizure and restraint.[85] Nonetheless, they provide examples of judicial willingness to treat cryptoassets as property in the context of criminal proceedings.

(3.1.1.4) The position under the Theft Act 1968

Although the matter has not yet been finally decided, there is a persuasive case in principle for the recognition of cryptoassets as property at common law, and the caselaw points in favour of this conclusion. The best view, it is submitted, is that cryptoassets qualify as intangible property in English civil law, and it should follow that they also amount to property for the purposes of the TA 1968.[86] This conclusion is fortified by the fact that the definition of property in s. 4 is extremely wide and expressly includes "other intangible property".[87] Moreover, the Supreme Court has

---

[75] *Ruscoe* (fn. 49)
[76] Including those referred to at fns.59 and 65 above.
[77] *Ruscoe* (fn. 49) [133].
[78] ibid [129]-[132].
[79] *R v Teresko (Sergejs)* (Kingston Crown Court, 11 October 2017), noted by J Hall [2018] 1 Crim LR 81
[80] s 41(1).
[81] Hall (fn. 79).
[82] *R v West (Grant)* (Southwark Crown Court, 23 August 2019).
[83] S Rahman, 'The hacker, bitcoin, the Proceeds of Crime Act and the Criminal Courts (Sentencing) Act' (Lexology, 10 September 2009) <https://www.lexology.com/library/detail.aspx?g=f5712142-8200-4a8f-97b6-c228c1c7e733> accessed 28 November 2020.
[84] We are grateful to HHJ Korner for confirming this and for her comments on the case.
[85] See Hall (fn. 79) 83.
[86] "In terms of the recognition and protection of property, the criminal law is dependent upon and posterior to the civil law" – AP Simester and GR Sullivan, 'On the Nature and Rationale of Property Offences' in RA Duff and SP Green (eds), *Defining Crimes* (2005) 178; D Ormerod and K Laird, *Smith, Hogan, and Ormerod's Criminal Law* (15th edn, OUP 2018) para 18.3.2. Though cf. S Green, 'Theft and conversion – tangibly different?' (2012) 128(4) LQR 564.
[87] *Nai-Keung* (fn. 65) 1342 (Lord Bridge).

recently[88] stressed the importance of avoiding unprincipled divergences between civil and criminal concepts.[89] However, three issues require further consideration. The first concerns the aforementioned information objection to recognising cryptoassets as property; if cryptoassets are viewed as mere information, their proprietary status will be ruled out on the basis of established authority under the TA 1968. We argue below that this objection mischaracterises the nature of cryptoassets. The second and third considerations, on the other hand, suggest that courts should be wary of treating cryptoassets and other virtual assets as a homogenous class for the purposes of the TA 1968.

The Relevance of Oxford v Moss

In *Oxford*,[90] the Divisional Court held that information contained in an examination paper was not capable of being stolen. A number of civil cases have also refused to treat information as property,[91] but *Oxford* is the leading case addressing the issue in the context of the TA 1968.[92] The judgment of the Divisional Court in *Oxford* is short, and its reasoning is not clear, but various justifications have been advanced elsewhere for the law's reluctance to treat information as property.[93]

Perhaps the most common argument is that information is non-rivalrous; one person's knowledge of something does not diminish anybody else's knowledge of the same.[94] Relatedly, information is inalienable and unassignable; a fact cannot be (deliberately) 'unknown'. The question of who 'owns' a piece of information is nebulous,[95] and there are concerns about the use of criminal[96] and/or property[97] law to regulate the dissemination of information. Leaving aside the limited circumstances in which individuals are afforded rights to control the *use* of certain information,[98] affording exclusive rights of ownership could have adverse social and economic consequences.

[88] *Compare R v Hinks* [2000] UKHL 53; [2000] 3 WLR 1590, where the House of Lords found there could be an appropriation for the purposes of the offence of theft, even in the absence of any civil wrong.
[89] See *Ivey v Genting Casinos (UK) Ltd t/a Crockfords* [2017] UKSC 67, [57] and [63]. For critique, see M Dyson and P Jarvis 'Poison Ivey or herbal tea leaf' (2018) 134 LQR 198, 200.
[90] *Oxford v Moss* (1979) 68 Cr. App. R. 183.
[91] See CM Phipps, W Harman and S Teasdale, *Toulson & Phipps on Confidentiality* (Sweet & Maxwell, 2020) paras 2-006-2-036 and the cases cited therein.
[92] *Oxford* was followed in *R v Absolom* (The Times, 14 September 1983). See further the decision of the Canadian Supreme Court in *R v Stewart* [1988] 1 S.C.R. 963, in which it was also held that confidential information was not property for the purposes of s. 322 of the Canadian Criminal Code. Neither is theft of confidential information a crime in Scotland – see *Grant v Allan* [1987] JC 71.
[93] A useful summary of some of the issues is given by RG Hammond, 'Quantum Physics, Econometric Models and Property Rights to Information' (1981) 27 McGill L Rev. 47, 53-56. See also *Toulson & Phipps* (fn. 91) paras 2-015-2-036.
[94] See e.g. *Stewart* (fn. 92) 980 (Lamer J); *Federal Commissioner of Taxation v United Aircraft Corp* (1943) 68 C.L.R. 525, 534-535 (Latham CJ); *Boardman v Phipps* [1967] 2 AC 46 (HL), 127 (Lord Upjohn). For discussion of the concept of rivalrousness, see SP Green, *Thirteen Ways to Steal a Bicycle: Theft Law in the Information Age* (Harvard University Press, 2012) 208-210 and *Hammond* (fn. 93).
[95] Hammond (fn. 93) 54. See, relatedly, *Boardman* (fn. 94) 127 (Lord Upjohn).
[96] See *Stewart* (fn. 92) 977-978 (Lamer J); F R Moskoff, 'The Theft of Thoughts: The Realities of 1984' (1984–85) 27 Crim LQ 226; E Griew, *The Theft Acts 1968 and 1978* (7th edn, Sweet & Maxwell, 1995) para 2.25.
[97] See Hammond (fn. 93) 69-70; JT Cross, 'Trade Secrets, Confidential Information, and the Criminal Law' (1991) 36 McGill LJ 524, 534-535; TF Aplin, 'Confidential Information as Property?' (2013) 24 KLJ 172-201; KFK Low and D Llewelyn, 'Digital files as property in the New Zealand Supreme Court: innovation or confusion?' (2016) 132 LQR 394.
[98] For example, intellectual property rights and the equitable action to restrain breaches of confidence.

The application of the various 'information' objections to cryptoassets is rejected in both the LSCSC[99] and *Ruscoe*[100] on the overarching basis that this involves a mischaracterisation of the nature of cryptoassets. Crucially, it is wrong to equate the data *representing* a cryptoasset, which may be characterised as pure information, with the cryptoasset itself, which cannot. Rather, a cryptoasset is an intangible deriving from the interplay between data, consensus and system rules.[101]

A cryptoasset, properly conceived, *is* rivalrous, since the protocol's consensus mechanisms ensure that it can only be 'spent' once, and only by the holder of its associated private key. Thus, cryptoassets are capable of being assigned, alienated and otherwise dealt with in ways that pure information, such as trade secrets, cannot be. Determining the owner of a cryptoasset does not give rise to the difficulties that arise in relation to pure information, and affording them proprietary status does not represent an impediment to the free flow of information.

Even if they are viewed as a type of information – which it is submitted herein that they should not be – a functional assessment reveals that cryptoassets are simply not amenable to any of the arguments put forward against the recognition of property rights in information.[102] In these circumstances, it should be open to a criminal court to distinguish *Oxford* and hold that cryptoassets are not excluded from s. 4 TA 1968.

'Unstable' cryptoassets

The proprietary status of cryptoassets turns, in part, on whether they satisfy the *Ainsworth* criteria.[103] Whilst it is probable that all cryptoassets are, by their nature, definable, identifiable and alienable, and that they are "as permanent as other conventional financial assets",[104] not all cryptoassets possess the same degree of "stability".[105]

The authors of the LSCSC identify two issues with regard to stability – the fact that the immutability of transactions increases with time, and the potential for "forks" – and restrict their conclusion as follows:

> *Cryptoassets are in our view sufficiently permanent and stable to be treated as property, at least for a commercial cryptoasset system with a significant number of participants, an established history of transactions, and a generally stable set of rules.*[106]

This leaves room for an argument that certain newly-created and/or niche cryptoassets do not qualify as property. This contention could cause difficulties in criminal proceedings because it is not clear precisely what 'degree' of stability is required, to what standard this would need to be proven, nor whether this is an issue for the tribunal of fact or law, or both.

---

[99] LSCSC (fn. 15) paras 59-65.
[100] *Ruscoe* (fn. 49) [128].
[101] See Section 1.2 above, including footnotes and citations.
[102] David Fox is less certain of the extent to which cryptoassets should be distinguished from the information by which they are represented. However, he nonetheless argues that "the real objection to treating information as property should depend on the functions it is used for rather than on the plain fact that it is information". See Fox (fn. 49) 142-155.
[103] *Ainsworth* (fn. 58) 1247-1248.
[104] LSCSC (fn. 15) para 52.
[105] ibid paras 49-58.
[106] ibid para 56.

In reality, this issue is unlikely to arise, since the degree of stability required by the *Ainsworth* test must necessarily be minimal if it is to have any meaning,[107] and it is reasonable to suppose that most cases will involve cryptoassets that are sufficiently well-established as to have some appreciable value. It is also arguable that, in the context of the TA 1968,[108] a more important factor informing proprietary status is the tradability of an asset, its conferral of a benefit on the owner, and its susceptibility to dishonest dealing at the time of appropriation.[109] Nonetheless, the stability criterion has the potential to cause difficulties in fringe cases.

The Limits of Virtual Property

The difficulty of squaring cryptoassets with the final limb of the *Ainsworth* test highlights a broader problem in bundling cryptoassets together for the purposes of analysis. The characteristics capable of allowing cryptoassets to qualify as property and avoid the various information objections are a function of their design, but not all cryptoasset systems are created equally; they exhibit differing degrees of rule-by-consensus, security and immutability.

In this paper, 'cryptoasset' is used to refer to those intangibles – of which bitcoins are an example – which align substantially with the description in section 1.2 above. Whilst there is a clear case for recognising *these* cryptoassets as property, doing so raises difficult questions about the law's treatment of other 'virtual' assets.

Consider tradable items in online multiplayer games. Such games allow users to simultaneously connect and play in a virtual environment, and some facilitate the trading of items within the games, such as clothes or weapons. These items are capable of amassing significant value in the real world.[110] They are typically linked to an account accessible with a unique password, and they 'exist' in a framework of rules that govern their specifications, assignability and duration, and prevent double-spending. It is at least arguable that they satisfy the *Ainsworth* criteria. However, such items are not widely regarded as property capable of being stolen,[111] and treating them as such could have undesirable consequences.[112]

If it is thought that in-game items should not constitute property,[113] then they should be clearly distinguishable from those cryptoassets, like bitcoins, which do. One difference is that the existence of the latter depends, in part, on a distribution of decision-making power, which justifies

---

[107] "Ownership of a thing is not a guarantee against deterioration in or destruction of the thing" – see Fox (fn. 49) 153. Vos J has stated extrajudicially that permanence or stability can be "ephemeral" - Sir Geoffrey Vos, 'Cryptoassets as property: how can English law boost the confidence of would-be parties to smart legal contracts?' (Joint Northern Chancery Bar Association and University of Liverpool Lecture, 2 May 2019) <https://www.judiciary.uk/wp-content/uploads/2019/05/Sir-Geoffrey-Vos-Chancellor-of-the-High-Court-speech-on-cryptoassets.pdf> accessed 28 November 2020, para 26. The criterion of stability has been described as "radical and obscurantist nonsense" – see K Gray, 'Property in Thin Air' (1991) 50 CLJ 252, 293.

[108] The meaning of 'property' varies with context - *Nokes v Doncaster Amalgamated Colliers Ltd* [1940] 1 AC 1014 (HL), 1051 (Lord Porter).

[109] In *Nai-Keung* (fn. 65) it was held that intangible textile export quotas were capable of being stolen, even though they were only valid for a limited period. Delivering judgment on behalf of the Privy Council, Lord Bridge stated at 1342 that "the definition of 'property' in the English Theft Act 1968 and the Hong Kong Theft Ordinance was intended to have the widest ambit. It would be strange indeed if something which is freely bought and sold and which may clearly be the subject of dishonest dealing which deprives the owner of the benefit it confers were not capable of being stolen".

[110] W Rumbles, 'Theft in the digital: Can you steal virtual property?' (2011) 17(2) Canta LR 354, 358-360.

[111] This probably explains why e.g. Stephen Burrell (fn. 43) was charged under the CMA 1990, rather than theft, when he obtained access to other players' Runescape accounts and sold their in-game items for money.

[112] See AA Gillespie, *Cybercrime: Key Issues and Debates* (2nd edn, Routledge, 2019) 151-152.

[113] For discussion of this issue, see Gillespie (ibid) 137-152; Rumbles (fn. 110); JAT Fairfield, 'Virtual Property' (2005) 85 B.U. L. Rev. 1047.

treating bitcoins as more than just the data by which they are represented. But what then of cryptoasset systems that are highly-centralised, meaning that overall control is concentrated in only a few entities, or even just one?[114]

This is certainly not to say that cryptoassets cannot be distinguished from in-game tokens or items. The point is rather that distinctions between different cryptoassets, and between cryptoassets and other kinds of virtual asset, can only be viewed as shades of grey. In these circumstances, more work is needed to delineate *precisely* which virtual assets qualify as property, and for which statutory regimes.[115] Without this, there is a risk that property – and, by extension, criminal – law, will creep beyond justifiable limits.[116] Such an inquiry goes beyond the scope of this article. For present purposes, it should be noted that, whilst many cryptoassets can be regarded as property with little difficulty, this may not always be the case.[117] Similarly, the conclusion that certain cryptoassets qualify as property does not mean that the same can be said of all commodifiable intangibles.

(3.1.2) The Private Key

Scenario (2) gives rise to the question whether V's private key is property capable of being stolen. The answer is that it is not,[118] although it would of course be possible for D to steal a physical device or document on which V's private key is recorded.[119] A private key is simply a string of alphanumeric digits and thus pure information. Unlike cryptoassets themselves, a private key is amenable to the various objections levelled against treating information as property, and its proprietary status is ruled out by *Oxford*.

Whilst this conclusion presently seems unassailable as a matter of English law, it may become necessary to revisit it in light of developments at the international level. In particular, EU Directive 2019/713 seeks to harmonise the domestic criminal laws of member states with regard to fraud and counterfeiting of 'non-cash means of payment'. [120] Article 5(a) requires that member states impose criminal penalties for *inter alia* the intentional "unlawful obtainment" or "misappropriation" of a "non-corporeal non-cash payment instrument". The definition of the

---

[114] It has been alleged that the company behind Ripple, the fourth-largest cryptocurrency by market capitalisation at the time of writing, possesses substantial control over it - see G Thompson, 'Ripple (XRP) isn't a Real Cryptocurrency, Claims Exchange that Just Listed the 'Heavily Centralized' Token' (CCN, 13 February 2019) <https://www.ccn.com/ripple-xrp-centralized-not-cryptocurrency-coinmotion/> accessed 28 November 2020.

[115] For example, even if cryptoassets are capable of being stolen for the purposes of the TA 1968, that does not necessarily mean that they should be treated as such for the purposes of the Criminal Damage Act (CDA) 1971. Indeed, the definition of 'property' in s. 10(1) of the CDA 1971 – as property of a tangible nature – rules out treating cryptoassets as property capable of being criminally damaged. The position under *R v Whiteley* (1991) 93 Cr. App. R. 25, in which the deletion of information on computer discs was found to constitute criminal damage, even without any physical damage to the discs, has since been superseded by s. 10(5) CDA 1971 and the Computer Misuse Act 1990.

[116] This risk is exemplified by *Dixon v R* [2015] NZSC 147, [2016] 1 NZLR 678, in which the Supreme Court of New Zealand held that computer data *in general* – in that case, digital CCTV video files – can be property capable of being stolen. Both the reasoning and decision in *Dixon* have been powerfully criticised, particularly on the basis that unjustified leaps of logic were employed to ascribe to digital information the qualities of tangible property – see Low and Llewellyn (fn. 97) above and D Harvey, 'Case note: Digital property - Dixon v R [2017]' [2017] NZCLR 31.

[117] For an interesting take on this issue from a law and economics perspective, see Sarel (fn. 57), who argues that the decision whether to protect a given cryptoasset via either a liability rule or a property rule should depend on whether transaction costs are likely to be high or low. This, Sarel argues, could provide a conceptual framework for determining which types of cryptoassets should be treated as property.

[118] LSCSC (fn. 15) para 65.

[119] This would include a computer, a purpose-built 'hardware wallet', or even just a piece of paper.

[120] Directive (EU) 2019/713 of 17 April 2019 on combating fraud and counterfeiting of non-cash means of payment and replacing Council Framework Decision 2001/413/JHA, article 1.

latter term plainly applies to private keys used in cryptocurrency transactions,[121] meaning they may come to be protected by theft or theft-like offences in EU member states. Although the directive is not binding on the UK,[122] it is conceivable that parallel changes may be required for the purposes of future EU-UK cooperation in criminal investigations and proceedings.

(3.1.3) V's rights against Xchange

In Scenarios (1) and (2), V holds the private keys to his cryptoassets. In Scenario (3), the position is different due to the involvement of a cryptocurrency exchange. Although the precise mechanics of the exchange-customer relationship will vary between platforms, the important point to note is that the customer will often have nothing more than contractual rights against the exchange.[123]

When, in Scenario (3), V deposits money with Xchange, V acquires a contractual right to repayment. However, V can also use it to buy an amount of cryptoassets at the going rate. Typically, exchanges satisfy orders by finding another customer,[124] Y, who is looking to sell cryptoassets.[125] Xchange will give two new undertakings: to pay V the requested quantity of cryptoassets, and to pay Y the agreed value of those cryptoassets in an agreed currency.[126] Crucially, Xchange will often retain control of the private keys until called upon to transfer the cryptoassets to an address provided by V.

For the purposes of the TA 1968, "property" includes "things in action". This term "… is now used to describe all personal rights of property which can only be claimed or enforced by action, and not by taking physical possession".[127] Both the benefit of a contract,[128] as well as rights of action arising thereunder,[129] have been held to constitute things in action. It follows that both are property capable of being stolen. Support for this can be drawn from *Marshall,* in which it was stated, *obiter,* that selling partially-used train tickets might constitute theft of a chose in action.[130]

Although it has been argued that the inclusion of contractual rights within the scope of s. 4 renders the offence of theft too broad,[131] it is submitted this is not so. Indeed, the paradigm example of a thing in action capable of being stolen – the debt created when money is deposited with a bank[132] – is contractual in nature.[133] Similarly, a bank's obligation to honour cheques within an agreed overdraft limit can be enforced via an action for breach of contract, and therefore constitutes a thing in action capable of being stolen.[134]

---

[121] See ibid article 2(a) and recitals 6, 8, 10 and 15.
[122] See ibid recital 38.
[123] See Narayanan (fn. 8) 4.4.
[124] In practice, this might be many other customers.
[125] Narayanan (fn. 8) 4.4.
[126] Ibid.
[127] This definition is given in *Halsbury's Laws* (5th edn, 2009) volume 13, para 1, and was cited with approval in *Armstrong* (fn. 59), [45]. See also *Torkington v Magee* [1902] 2 KB 427 (Channell J).
[128] See *Halsbury's Laws* (5th edn, 2009) volume 13, para 6 and the cases cited therein.
[129] See ibid para 7 and the cases cited therein.
[130] *R v Marshall* [1998] 2 Cr. App. R. 282, 288.
[131] A Steel, 'Problematic and Unnecessary? Issues with the Use of the Theft Offence to Protect Intangible Property' (2008) 30 Sydney Law Review 575 and JC Smith, 'Stealing Tickets' [1998] Criminal Law Review 723.
[132] See *R v Kohn* (1979) 69 Cr. App. R. 395.
[133] *Foley v Hill* (1848) 9 E.R. 1002, 1006 (Lord Cottenham CJ).
[134] *Kohn* (fn. 132) 407-408. See also E Griew, 'Stealing and Obtaining Bank Credits' [1986] CLR 356, 359.

V's contractual rights against Xchange, as well as the benefit of any such contract, are clearly property for the purposes of s. 4 TA 1968.[135] However, the precise nature of the thing in action will depend on the present state of Xchange's contractual undertakings to V.

(3.2) Belonging to another

Theft requires that property belongs to another at the time of appropriation. By s. 5(1) TA 1968:

> *Property shall be regarded as belonging to any person having possession or control of it, or having in it any proprietary right or interest (not being an equitable interest arising only from an agreement to transfer or grant an interest).*

It is possible for one item of property to 'belong to' multiple people for the purposes of s. 5.[136]

(3.2.1) Cryptoassets

Being intangible, cryptoassets cannot be "possessed".[137] However, it is fair to say that they are "controlled" by any person with access to their associated private key.[138] On this basis, the cryptoassets in Scenarios (1) and (2) can be said to belong to V until they are transferred to D's address.

Although it has yet to be seen how title to cryptoassets may be established and transferred, the authors of the LSCSC suggest that:

> *The starting point, in our view, is that a person who has acquired knowledge and control of a private key by some lawful means would generally be treated as the owner of the associated cryptoasset, in much the same way that a person lawfully in possession of a tangible asset is presumed to be the owner.*[139]

On this basis, it may be presumed that V also has a "proprietary right or interest" in the cryptoassets in Scenarios (1) and (2).

In Scenario (3), it is equally clear that the cryptoassets "belong to another". Less clear is whether they belong to V or Xchange, or both. If Xchange alone holds the private key, they probably cannot be said to "belong to" V on the control basis.

Whether the cryptoassets in Scenario (3) can be said to belong to V on the basis of a proprietary right or interest will depend on the precise nature of V's relationship with Xchange. If Xchange holds a quantity of cryptoassets on trust for V, V will have an equitable proprietary interest in

---

[135] The same view is taken in Fox & Green (fn. 8).
[136] *R v Turner (No 2)* [1971] 1 WLR 901 (CA).
[137] At least not to the extent that the law demands physical possession – see *OBG Ltd v Allan* [2007] 2 WLR 920, *Your Response Ltd v Datateam Business Media Ltd* [2014] EWCA Civ 281. Cf. Green (fn. 86).
[138] The holder of a private key has an exclusive ability to transact with its associated cryptoassets, and this is 'control' in the ordinary sense of the word. Section 5(1) TA 1968 cannot sensibly be read as imposing any requirement of *physical* control, given that the offence of theft extends to intangibles. Moreover, the Court of Appeal has refused to add qualifications to the terms 'possession' and 'control', suggesting they should be interpreted broadly - see *Turner* (fn. 136).
[139] LSCSC (fn.15) para 43.

them.[140] However, if V's relationship with Xchange is purely contractual, V will either have no proprietary interest in the cryptoassets held by Xchange, or V will have at most "an equitable interest arising only from an agreement to transfer or grant an interest", which is excluded from s. 5.[141]

To summarise, the cryptoassets in Scenario (3) can only be said to belong to V if they are held on trust for V by Xchange. However, the existence of such a trust may be difficult to establish,[142] and the safest option is probably to regard the cryptoassets as 'belonging to' Xchange only.

(3.2.2) V's rights against Xchange

In Scenario (3), the benefit of the contract with Xchange, and any enforceable rights arising thereunder, plainly belong to V.

(3.3) Appropriation

By s. 3(1) of the TA 1968:

> *Any assumption by a person of the rights of an owner amounts to an appropriation, and this includes, where he has come by the property (innocently or not) without stealing it, any later assumption of a right to it by keeping or dealing with it as owner.*

(3.3.1) Scenario (1)

For an appropriation to take place in Scenario (1), D must assume one[143] of the rights of an owner of a cryptoasset. The precise scope of these rights is not yet clear, but it is nevertheless possible to identify certain core rights inherent in the notion of 'ownership'.[144]

Although cryptoassets cannot be *physically* held and guarded, the owner of a cryptoasset can be said to have a right to *possess* it in the sense that he is entitled to exclude others from its "use and other benefits".[145] The owner of a cryptoasset also has rights to *use*,[146] *manage*[147] and *derive income*[148] from

---

[140] This issue was central in both *B2C2* (fn. 59) and *Ruscoe* (fn. 49).
[141] See TA 1968, s 5(1).
[142] In *B2C2* (fn. 59), for example, the Singapore Court of Appeal reversed the lower court's finding that a trust had been created, holding instead that there had been insufficient certainty of intention.
[143] *Morris* [1983] 3 WLR 697 (HL).
[144] The best-known account of these rights was given by AM Honoré in a 1961 essay entitled 'Ownership', reprinted in Tony Honoré, *Making Law Bind: Essays Legal and Philosophical*' (Clarendon Press, 1987), 161. Honoré's 'standard incidents of ownership' were compiled into a widely-cited list by LC Becker in 1977, reprinted as LC Becker, *Property Rights (Routledge Revivals): Philosophic Foundations* (Routledge, 2014) 18-20.
[145] Becker (fn. 144) 19. See also Honoré (fn. 144) 166-168 and 179-184.
[146] Honoré (fn. 144) 168.
[147] This is "the right to decide how and by whom the thing owned shall be used" – see Honoré (fn. 144) 168.
[148] Honoré (fn. 144) 169-170.

it, as well as the right to its *capital*. The latter consists "in the power to alienate the thing and the liberty to consume, waste or destroy the whole or part of it".[149]

By forcing V to initiate a cryptoasset transaction, it is arguable that D assumes the rights to exclude, possess, and use the cryptoassets, but it is clear that D assumes the right to the capital of the cryptoassets, specifically the right to "consume, waste or destroy" them. This is because a cryptoasset transaction does not technically involve a 'transfer', but rather the destruction of the sender's cryptoassets and the corresponding creation of new ones linked to the recipient's private key.[150] It is well-established that the destruction of intangible property is sufficient to establish appropriation.[151]

(3.3.2) Scenario (2)

In Scenario (2), D orders V to disclose his private key before using it to make a transaction at some later time. In cases of this type, it is possible that D will take some physical thing of V's on which the private key is recorded, and appropriation will be easily established in relation to that thing. In any event, when D initiates the transaction, appropriation of V's cryptoassets will be established on the same bases as in Scenario (1).

Leaving aside the case in which V hands over a physical thing, it does not appear that appropriation takes place when D forces V to reveal his private key. The private key is not itself property, and it does not seem likely that compelling V to disclose it could amount to an appropriation of V's cryptoassets, even though the two are closely linked.[152] On the facts of Scenario (2), appropriation is established when D takes a physical thing from V and/or when D initiates a transaction using V's private key. This is important, because the timing and location of appropriation are significant where D is charged with robbery under s. 8(1)[153] or theft-based burglary under s. 9(1)(b) TA 1968[154] respectively.

(3.3.3) Scenario (3)

Scenario (3) involves two types of property. With regards to the thing in action, it should not be difficult to establish appropriation. A right to request a transfer by Xchange of cryptoassets to a specified address is a thing in action belonging to V. D assumes this right if he uses V's account to request a transfer to his own address. Even if V does not have an immediate right to a transfer

---

[149] Honoré, (fn. 144) 170-171.
[150] LSCSC (fn. 15), paras 44-47.
[151] The lack of any 'transfer' would have been fatal under the repealed offence of 'obtaining' property by deception – see s 15(1) TA 1968 and *Preddy* [1996] AC 815. However, it is settled law that a transfer of property is merely sufficient, but not necessary, to establish theft, and that the destruction of intangible property constitutes an act of appropriation – see *Kohn* (fn. 132), *Hilton* [1997] 2 Cr. App. R. 445 (CA) and the addendum to Lord Bingham's judgment in *Graham* [1997] 1 Cr App R 302, 334. Although these cases refer to choses in action, there is no reason why the same reasoning should not apply in the case of 'other intangible property'.
[152] It could be argued that the owner of a cryptoasset has a right to maintain confidentiality in its associated private key, and that V appropriates this right by compelling disclosure. However, this seems incompatible with *Oxford* (fn. 90), in which the Divisional Court rejected a similar argument.
[153] See Section 4 below.
[154] See Section 4.1 below.

of cryptoassets, appropriation will take place if D purchases cryptoassets using money previously deposited by V. Here, D interferes with V's right to repayment of the deposited sum.[155]

The second type of property is the cryptoassets themselves which, absent a trust relationship between Xchange and V, belong to Xchange only. In a series of cases, the Court of Appeal has considered whether there is an appropriation when D causes payment to be made from a bank account.[156] The effect of these decisions – although not free from ambiguity – is to draw a distinction between two situations:

(a) Where D sets in motion a process which will lead more or less automatically to the diminution or extinguishment of a thing in action, with the role of any human actors limited to that of innocent agents, there is an appropriation by D.[157]

(b) Where D deceives V or V's agent into making a conscious decision to diminish or extinguish a thing in action, there is not normally an appropriation by D.[158]

Although cryptoassets may not be classified as a chose in action for the purposes of s. 4 TA 1968, there is no reason why the same principles should not apply to them as 'other intangible property'. By posing as V, and thus supplying a valid transaction request from a valid Xchange user account, D supplies the "key" necessary to set the transaction process in motion, and may therefore be viewed as assuming a right to destroy cryptoassets owned by Xchange.[159]

(3.4) *Mens rea*: Dishonesty and Intention Permanently to Deprive

None of the above scenarios give rise to any unique issues with regards to the *mens rea* elements of theft. In all three, it is clear that D intends to appropriate property belonging to another. D also acts dishonestly according to the *Ivey* test,[160] and none of the exceptions in s. 2(1) TA 1968 apply. D's intention permanently to deprive the victim of the relevant property would probably not be difficult to prove.[161]

(3.5) Theft: Conclusion

There is no reason why D could not be charged with theft in all three scenarios. In Scenarios (1) and (2), D steals V's cryptoassets when he initiates the transaction. If, in Scenario (2), D takes a

---

[155] See *Kohn* (fn. 132).
[156] See Blackstone's Criminal Practice 2020, paras B4.48-4.50
[157] See e.g. *R v Williams (Roy)* [2001] 1 Cr App R 23 (CA) and *R v Hilton* [1997] 2 Cr App R 445 (CA).
[158] See e.g. *R v Naviede* [1997] Crim LR 662 (CA) and *Darroux* [2018] EWCA Crim 1009, [2019] QB 33. In *Darroux* paras 61-64, it was stated that cases of this description should, other than in certain unspecified circumstances, be charged as fraud rather than theft.
[159] See *Hilton* (fn. 157) 453-456 and Blackstone's Criminal Practice 2020, para B4.50. The position might be more complicated if Xchange conducted a manual review of transaction requests and/or retains a discretion not to satisfy them. This would be analogous to the situation in *Darroux* (ibid), in which it was held that the active role played by payroll staff in assessing the defendant's dishonestly exagerated timesheets created a degree of separation between the defendant's conduct and the eventual reduction in her employer's credit balance. In circumstances like this, it may not be possible to view the *defendant* as having assumed any right to destroy or diminish V's intangible property. However, it seems more likely that a cryptoasset exchange would process transaction requests in a more or less automatic way.
[160] *Ivey* (fn. 89). The Court of Appeal has recently confirmed that this should be followed in the criminal courts. See *R v Barton and Booth* [2020] EWCA Crim 575 [1].
[161] s 6(1) TA 1968.

physical thing on which V's private key is recorded, D also steals that thing. In Scenario (3), D steals a chose in action belonging to V or cryptoassets belonging to Xchange.[162]

(4) Other Offences Under the Theft Act 1968

Theft involves both a primary and secondary wrong. The primary wrong is a violation of the norm against stealing, whereas the secondary wrong relates to the manner in which stealing is effected.[163] The analysis above shows that the primary wrong of theft is established in all three working scenarios. However, the way in which D steals in each clearly reflects a secondary wrong beyond mere dishonesty; D threatens V with physical violence, and the events are likely to take place in a building – possibly V's home – in which D is trespassing.

Distinctions between the secondary wrongs of theft are reflected not only in substantive law and sentencing, but also society's understanding of the moral culpability of theft-based offences.[164] Empirical research suggests that individuals consider robbery involving deadly threat to be the most blameworthy form of theft, closely followed by extortion, then burglary involving housebreaking, then simple robbery.[165] In the types of scenarios considered in this article, and for the reasons outlined above,[166] prosecutors will want and expect these more serious charges to be available.

If it is accepted that cryptoassets constitute property capable of being stolen, there will be little difficulty in charging robbery[167] in Scenarios (1)-(3). In each case D steals cryptoassets or a chose in action, and immediately before and/or at the time of stealing, D intentionally seeks to put V "in fear of being then and there subjected to force", in order to steal.[168] There would equally be little difficulty in charging blackmail in cases of this kind, even if cryptoassets are held *not* to constitute property for the purposes of the TA 1968.[169]

However, in relation to the offence of burglary, there is some interpretative legwork to be done. Some of the questions raised by the attempted Oxfordshire cryptoasset heist are not new and could equally arise in a situation where D burgles and initiates a bank transfer from V's bank account while in V's house. However, 'bitcoin burglaries' are likely to prove much more attractive to criminals. Unlike bank transfers, which can be reversed or at least readily traced through co-operation with banks, P2P cryptoasset transactions are significantly more immutable and censorship-resistant, and through use of technologies such as decentralised exchanges and/or 'coin mixing' services, it can be exceedingly difficult to identify wrongdoers. It is for this reason that some of the hitherto unaddressed issues relating to the interpretation of s. 9 TA 1968, may soon be brought into sharp focus in the criminal courts.

---

[162] He could not be charged with stealing both, as it would constitute double charging - see *R v Harris* (1969) 53 Cr. App. R. 376, 379; *R v Nelson and another* [2016] EWCA Crim 1517 [34].
[163] SP Green (fn. 94) 91-131.
[164] ibid 54.
[165] ibid 54-68. The study involved 172 participants.
[166] See the discussion at Section 2.3.
[167] s 8(1) TA 1968.
[168] Complications could arise in scenario 2 if D does not initiate the transaction immediately, but this is unlikely to happen in practice as it would give V an opportunity to protect the cryptoassets.
[169] Blackmail may be committed where D makes an unwarranted demand accompanied by menaces, 'with a view to' gaining money or other property – see s 21 TA 1968. The phrase 'with a view' imports a weak causative requirement, such that blackmail may be committed where gaining money or property "is one of several objects which D has in mind in making the demand" – see Ormerod & Williams, *Smith's Law of Theft* (OUP, 2007) para 12.21. Accordingly, even if cryptoassets *themselves* do not qualify as property, it is arguable that D commits blackmail where his plan is to exchange them for money or property.

(4.1) Burglary and Aggravated Burglary

S.9 TA 1968 creates two separate burglary offences. The s. 9(1)(a) offence involves entering a building as a trespasser with intent to commit an ulterior offence specified in s. 9(2). The s. 9(1)(b) offence is established when D, having entered a building as a trespasser, commits an ulterior offence specified in that subsection. D commits the aggravated form of the offence if he is in possession of an offensive weapon at the time of the burglary.[170]

It is uncontroversial that, if the facts of Scenarios (1)-(3) unfold in a building which D has entered as a trespasser, D may face a charge under s. 9(1)(a) on the basis that he entered with an intention to inflict grievous bodily harm on V.[171] Similarly, if D does in fact inflict such harm, he may be guilty of burglary under s. 9(1)(b). However, if D is alleged to have committed burglary on the basis that he either intended to, attempted to, or did in fact, steal, then a problem arises.[172]

Where the offence of burglary is alleged to be founded on the ulterior offence of intended, attempted or actual theft, ss. 9(1)(a) and (b) are ambiguous as to the required location of both the defendant's actions and the relevant property. Specifically, s. 9(1)(a) refers, via ss. 9(2), to 'stealing anything in the building or part of a building in question', and s. 9(1)(b) requires that D 'steals or attempts to steal anything in the building or that part of it'.

The words 'in the building' may be read as circumscribing either the location of the thing actually or intended to be stolen, *or* the location of the act of stealing – appropriation. However, intangible property, such as cryptoassets and choses in action, cannot be said to exist in any particular location.[173] Thus, if it is necessary that the property be located in the building, then D cannot be guilty of burglary in any of the three hypothetical scenarios unless he also steals, or intends to steal, a physical thing located in the building.

The most thorough examination of the ambiguity in s. 9 can be found in a 1986 article by Steven White, which focuses primarily on the (now repealed) ulterior offence of rape.[174] White powerfully demonstrates how each of the techniques traditionally employed to resolve ambiguity in statutory language lead to different and contradictory conclusions in the context of s. 9. White does not reach a conclusion on the interpretation of s. 9 as a whole, though he suggests that, in relation to theft, the words 'in the building' should probably be read as circumscribing the location of the property.[175] This is probably the most natural reading from a purely textual perspective, and it also achieves consistency with the ulterior offence of criminal damage in s. 9(2), which refers to damaging the building or 'anything therein'.[176] Other writers appear to support this 'object location' interpretation.[177] However, it is submitted that there is a strong case for reading s. 9 as circumscribing the location of the *act* of stealing, at least in a case involving intangible property.

---

[170] TA 1968 s 10.
[171] This is an ulterior offence under both ss 9(2) and 9(1)(a).
[172] It might be necessary or preferable to frame the charge of burglary around the ulterior offence of theft if, for example, it cannot be proven that D intended to inflict GBH, rather than merely to scare V.
[173] Even though it might be possible to tie intangible property to a particular jurisdiction e.g. for the purposes of taxation, it is quite another thing to say that they are located 'in a building'.
[174] S White, 'Lurkers, draggers and kidnappers: the further offence in burglary' (1986) 1500 JP 37-39 and 56-59 (the article is separated into two parts within the same publication).
[175] ibid 56-57.
[176] Ibid.
[177] *Smith, Hogan, and Ormerod* (fn. 86), p.1019; R Card and J Molloy (eds), *Card, Cross & Jones: Criminal Law* (22nd edn, OUP 2016) 452.

As a starting point, it should be noted that an 'act location' interpretation is compatible with one of the most persuasive purposes of the offence of burglary.[178] This, White argues, is reduction of the incidence of violence attendant upon the commission of offences.[179] The argument is that both D and V are more likely to encounter violence in a situation where D commits or intends to commit a crime whilst trespassing in a building, compared to the situation in which D acts 'out in the open'.[180] On this basis, it is logical to adopt an interpretation of s. 9 which focuses on the location of D's actions.

Second, it is unlikely that s. 9 was intended to exclude an entire class of property from the remit of burglary. Intangible property is plainly capable of being stolen, and it may be stolen through acts of a trespasser in a building which give rise to precisely the same risks and harms that arise when tangible property is targeted. Given that the TA 1968 was enacted at a time when intangible property was significantly less prevalent in society, and the ways in which it could be stolen were even more limited, the issue was probably not even considered.[181] In 1968, it would have been difficult to conceive of a burglary involving the intended or actual theft of intangible property, and there is no mention of intangible property in the CLRC's report, [182] or the debates in Hansard.

Third, it does not appear that the drafters of the TA 1968 intended that it should alter the position under the Larceny Act 1916 ('LA 1916'), whereby the location of the act of offending was paramount.[183] The LA 1916 contained four predecessors to the modern burglary offence. The three offences of burglary[184] and housebreaking[185] all required that D committed, or intended to commit, a felony in a building. The other offence – larceny in dwelling-houses[186] – similarly required that D 'steals in any dwelling house'. Although the latter offence was qualified by a common law rule that property had to be 'under the protection of the house', this qualification was only necessary to distinguish the offence of larceny 'in a dwelling-house' from the distinct offence of larceny 'from the person'; D committed the former offence where he took money from the pocket of a coat V had hung in his hallway, but not if he pickpocketed V inside the same dwelling-house (since here the property was under the protection of the *person*).[187] The purpose of the qualification was *not* to limit the scope of larceny in dwelling-houses to property located inside the dwelling-house; this would have been superfluous, since such a limitation already followed necessarily from the ingredients of larceny. Since larceny required a taking and carrying away of tangible property, the location of the act of larceny and that of the stolen property would always have coincided.[188]

All of the predecessors to the modern offence of burglary can be interpreted as adopting an 'act location' approach, save to the extent that unique characteristics of the offence of larceny

[178] The rationale behind the law of burglary is "not entirely clear" – see White (fn. 174) 38.
[179] This justification was originally put forward in a note entitled 'A Rationale of the Law of Burglary' (1951) 51(8) Columbia Law Review 1009, 1022-1024.
[180] ibid; White (fn. 174) 38-39.
[181] For discussion of the Criminal Law Revision Committee's recommendation to include 'things in action' within the definition of 'property' in the new offence of theft, see JC Smith 'Obtaining cheques by deception or theft' (1997) Crim. LR 396, 397-399. As Smith notes, "[t]he consequences of extending … [theft] to cover things in action does not seem to have been considered in any detail by the Committee".
[182] See Criminal Law Revision Committee, *Eighth Report: Theft and Related Offences* (Cmnd. 2977, 1967).
[183] See ss 26 and 27 LA 1916 and White (fn. 174) 57. See also Criminal Law Revision Committee, ibid, paras 73 and 77, where the authors refer only to the location of offending, not that of the victim or property.
[184] s 25 LA 1916.
[185] ss 26-27 LA 1916.
[186] s 13 LA 1916.
[187] JC Smith and B Hogan, *Criminal Law* (1st edn, Butterworths, 1965) 406-407.
[188] See ibid 371.

necessitated a different interpretation.[189] However, these same characteristics are not present in the modern offences of theft or burglary. Under s. 9 TA 1968, no distinction can be drawn between the two types of pocket theft described above; both are capable of amounting to burglary. Under the modern offence of theft – which imports a wide requirement of appropriation and expressly extends to intangible property – there is no necessary correspondence between the location of the act of appropriation and that of the stolen property. Thus, the reasons that compelled an 'object location' interpretation in certain cases under the Larceny Act 1916 are simply inapplicable in the context of s .9 TA 1968.

Fourth, even if s. 9 is read as circumscribing the location of *tangible* property, it does not necessarily follow that it does so with respect to intangible property. This is because it is simply nonsensical to speak of intangible property being located either inside or outside a building.

Fifth, reading s. 9 as circumscribing only the location of appropriation is consistent with the decision in *Attorney-General's References (Nos. 1 and 2 of 1979).*[190] In that case, the Court of Appeal affirmed its earlier decision in *Walkington*[191] and held that a defendant may be convicted of burglary under s. 9(1)(a) on an indictment alleging trespassory entry into a building "with intent to steal therein". This is so even if he does not have a specific thing in mind, or if he only intends to steal if there is something 'worth stealing". This decision can be read as attaching greater significance to the location of the intended appropriation than that of the property. Reading the case in this way not only helps to explain why a conditional intent to "steal therein" is sufficient for a conviction under s. 9(1)(a), but also avoids an absurdity that could arise in a case involving intangible property. If the actual or intended location of the property were crucial, the same D could face a burglary conviction for intending to steal something which was not in fact in the building, but escape a conviction for actually stealing something which *cannot* be located there.

One possible objection to an 'act location' interpretation is that it goes against the principle that ambiguous penal statutes should be construed in favour of the defendant.[192] However, it is submitted that this objection lacks force. To the extent that the principle of strict construction exists to ensure that criminal statutes provide 'fair warning' to individuals, it cannot realistically be said to rule out an act location interpretation of s. 9; it is difficult to imagine the D in Scenarios (1)-(3) arguing that he had no reason to believe his actions might amount to burglary. Moreover, the principle of strict construction is not absolute; it is one of several factors a court should take into account as part of a broader contextual and purposive inquiry.[193] Since the principle of strict construction bears little weight in the instant context, it should give way to the principled arguments for favouring an act location interpretation, at least in a case involving intangible property.

There is a strong case for adopting an act location interpretation and concluding that the facts of Scenarios (1) and (3) are capable, in principle, of sustaining a charge of theft-based burglary, provided the other elements of the offence are made out. However, the ambiguity in s. 9 means this cannot be asserted with certainty.

---

[189] This interpretation is strengthened by the fact that, in contrast to ss 13 and 25-27 LA 1916, s 15 (larceny from ships and docks) unambiguously circumscribes the location of the stolen property, rather than the act of stealing. The wording of the latter provision differs notably from the others, suggesting that a conscious decision was taken to distinguish it from other offences for which location was a significant consideration.
[190] (1979) 69 Cr. App. R. 266 (CA).
[191] *Walkington* [1979] 1 WLR 1169 (CA).
[192] White (fn. 174) 39.
[193] J Horder (ed), *Ashworth's Principles of Criminal Law* (9th edn, OUP, 2019) 85; *Bogdanic v Home Office* [2014] EWHC 2872; *R v Z (Attorney General for Northern Ireland's Reference)* [2005] UKHL 35.

As with robbery, Scenario (2) may be more difficult.[194] Theft-based robbery is plainly capable of being established where D takes a tangible thing belonging to D, and, provided D initiates a transaction before leaving the building, the position is materially identical to Scenario (1). However, if D does not take a tangible thing and initiates the transaction only *after* leaving the building, neither the act nor the object of theft will have been in the building. In these circumstances, a charge of theft-based burglary will not be available.

Conclusion

There is nothing new about intangible property being valuable and of interest to criminals. 'Bank money' has and always will be the object of criminal activity. There is equally nothing new about information, like a password, being sought by criminals, often as a means to an end for further criminal activity. What is relatively novel is the way that cryptoassets appears to be incentivising the convergence of these activities. Beating someone with a rubber hose for an account password or a bank transfer is not a very attractive *modus operandi* if transactions can be reversed, cancelled or readily traced. Cryptoassets, on the other hand, offer new opportunities for those with such predilections.

The fundamental question that this raises for the criminal law is whether cryptoassets are capable of being stolen. We argue that due to their unique technical characteristics there will in most instances be little difficulty in defining cryptoassets as property, although on the edges of these technologies, challenging questions remain as to how cryptoassets can and should be distinguished from other (centralised) forms of virtual tokens or credits, both from the perspective of the TA 1968, but also more generally. Moreover, we have illustrated with the three scenarios addressed in this article how 'rubber-hose' cryptoasset heists will also raise many further questions of the TA 1968, with the complexity of the underlying blockchain architecture apt to cause confusion in the interpretation of many elements of property offences such as theft and burglary. Nevertheless, we have argued that these should normally be viable charges for cryptoasset heists, and the above analysis charts the path for framing and understanding such heists as property offences in these forms.

[194] See fn. 168.