The British Journal of Criminology, 2022, **62**, 1537–1552
https://doi.org/10.1093/bjc/azab118
Advance access publication 7 February 2022
Article

OXFORD

Criminology Towards the Metaverse: Cryptocurrency Scams, Grey Economy and the Technosocial

Simon Mackenzie

*Simon Mackenzie, School of Social & Cultural Studies, Te Herenga Waka–Victoria University of Wellington, Level 9 Murphy Building, Kelburn Parade, Wellington, New Zealand; simon.mackenzie@vuw.ac.nz.

Online markets in cryptocurrency represent a sprawling and eclectic alternative financial system, selling cutting edge techno-investment schemes that are complex and high risk. Crime control is almost entirely absent from this new crypto economy, and it is full of scams. This paper draws on an ethnography of crypto trading to review the main types of scam, suggesting that the grey economy of cryptocurrency trading is part of a wider evolution of society towards the technosocial, and beyond that perhaps towards the metaversal.

Key Words: cryptocurrency, scams, fraud, financial crime, cybercrime

METAVERSES, SHADOW ECONOMY AND THE TECHNOSOCIAL

This paper explores the intersection and overlap between two emerging themes in criminology: first, the shadow or 'grey' economy and second, the 'technosocial' (Brown 2006; Powell et al. 2018). It does this with a case study of scams in cryptocurrency. This is an online grey (i.e. practically unregulated) marketplace in financial investment speculation. Crypto exists on one of the leading edges of global technological development and around it, a 'degen' culture has developed: risky bets placed on volatile and uncertain assets by a society of traders who celebrate their 'degeneracy', as they see it, among the key motifs of which are to 'yolo' (you only live once) into 'moonshots' (risky bets on crypto with potentially huge upside).

In this introductory section, we will look at both of those ideas—grey economies and the technosocial—and suggest that as we move increasingly towards metaversal ways of living, an irreducible blend of online and offline life, criminology will need to continue to adapt its theory and method towards adequately recognising and appropriately analysing the new 'virtual/networked spaces' (Hayward 2012) in which some grey economies and the crimes associated with them exist.

On the spectrum of research on cybercrime, at one extreme we can place the discourse of 'novel threat' (Yar 2005). From this perspective, crime on the internet is a new frontier and demands a fundamentally different analysis from traditional offline crimes. At the other end of the spectrum we can put the 'old wine in new bottles' argument (O'Neill 2000; Grabosky 2001): that well-known criminal scripts may be moving online, but the basic social architecture

of crime remains the same. So, very basically, two poles of the argument about cybercrimes might be thought of as: 'it's a new problem' and 'it's an old problem'. Neither extreme can be sustained and this is increasingly apparent as technology continues to develop and to frame the experiences that make up our everyday lives (Lupton 2014). The hybridization (Brown 2006) or blending of on- and off-line life which continues to develop apace is one of the key reference points of social change in our time (Orton-Johnson and Prior 2013).

The term 'metaverse' was coined by sci-fi author Neal Stephenson in *Snow Crash* in 1992, referring to a 3D virtual world in which people lived, represented by avatars (Stephenson 1992; Laue 2011). Subsequent highlights in the cultural development of the idea of metaverses include Ernest Cline's 2011 novel *Ready Player One* (Cline 2011). Companies like FaceBook and Microsoft, who already mediate so much of our social and workplace lives, are now explicitly making moves towards building 'the metaverse'. In October 2021, FaceBook announced it was changing its name to Meta and declared the metaverse to be the future of the internet (Banerjee 2021). CEO Mark Zuckerberg intriguingly referred to his company's idea as an 'embodied internet that you are inside of rather than just looking at' (Wong and Duncan 2021). Microsoft wants to build the 'enterprise metaverse' (Banerjee 2021), where things like business meetings and education become avatar-based online experiences. Generally, the idea of a metaverse involves a computer-generated universe; a fully immersive online world 'where people gather to play games, socialize and work' (Palmer 2021). The metaverse is presently part aspirational dream, part hype and part real: the latter being identifiable in trends in online infrastructure development for virtual reality, gaming, socialising and economy (Palmer et al. 2000). The impression of a separation between online and offline life—the latter currently often referred to as IRL ('in real life') or more disparagingly 'the meatspace' (i.e. where our physical bodies actually are)—will become increasingly less well defined, and eventually, the line between the real and the simulated will no longer be a particularly relevant or helpful distinction to make for analysts of the social. While we currently talk of online advancements like 'virtual reality' or 'augmented reality', the future is said to be more likely to be 'mixed reality': a mix between on and offline, 'blending the digital and the real world together… ultimately this blend may be so good, and so pervasive, that the virtual and the real become indistinguishable' (Reid 2021).

We are still some way from that, but the on/offline distinction is blurring and will surely continue to do so. There is no longer, if there ever was, 'an exotic, esoteric or autonomous cyberspace' (Orton-Johnson and Prior 2013: 2). Instead, the internet develops towards 'Web 3.0', a decentralized online space run on blockchains promising, but not yet delivering, a new political, social and economic metaverse (Silver 2020). Cryptocurrencies are intricately tied into the prospect of the metaverse and its constituent technosocial scaffolding: they are variously the tokenized forms of governance used by blockchains (i.e. they give holders votes on future directions); they will likely be the currency used to transact in metaverses; and in their form of Non Fungible Tokens they represent ownership rights in digital goods, so they will be the title deeds to the property you own in these online universes. To that extent, a criminology of cryptocurrency is a formative step towards a criminology of the metaverse, and the online trading forums and routines we examine in this paper are key among the sociocultural, political and economic foundations on which metaverses are presently being built. The financial crimes in this space that we will examine here are, to that extent, the nascent scams of the metaverse.

Lately, writing on digital criminology has begun to recognize and explore our new technosocial lives, in some cases extending digital sociology analysis by arguing concomitantly for bringing more of the social back into academic discussion of cybercrime (Stratton et al. 2017). These writers are 'extending the practical and conceptual analyses of "cyber" or "e" crime beyond a focus foremost on the novelty, pathology and illegality of technology-enabled crimes, to understandings of online crime as inherently social' (Powell et al. 2018). With their concept

of digital society and the technosocial, these writers build on prior analyses which have variously considered the tightly woven mutual relationship between technology and society (e.g. Castells 1996; Lévy 2001; Lash 2002). This paper continues in that vein, examining the social and cultural aspects of contemporary scams in the rapidly developing online world of crypto markets. This investigation of crypto scams shows that there are elements of both novelty and tradition in the construction and practice of crypto scams. In the hybridization of the online and the offline, we see a 'vision of the crucial nature of the world as human/technical hybrid' (Brown 2006: 227).

If this is a fair short summary of current technosocial developments on the pathway to metaversal social and economic life, where traditional forms of crime develop into the social spaces created by the technological parameters of society and new forms also emerge, how might the research literature on grey economies assist us to see the potential magnitude of these developments for criminology? Grey economic activity refers to un- or under-regulated markets (Schneider and Enste 2002), where transactions take place to some extent outside officially sanctioned trade areas: 'hidden from public authorities for monetary, regulatory or institutional reasons' (Ohnsorge and Yu 2021: 49). The complexity of grey, or 'informal', markets can involve some uncertainty about whether what is going on is legal or not (Shapland and Ponsaers 2009). Grey economic activity might feel to participants like it is 'a bit legal, a bit illegal' (Galemba 2008: 21).

Cryptocurrency is one such grey economic activity: a booming online marketplace with an almost existentially defining uncertainty about its present and future legal status. Crypto is something like the economic equivalent of Stanley Cohen's 'public secret' (Cohen 2001): everyone knows about it, it is tolerated though not supported in most jurisdictions and it raises awkward policy questions. Among those awkward questions are big issues like the viability or desirability of global finance outside the purview of the state (Dodd 2018; Zook and Blankenship 2018), and more mundane issues like the considerable amount of crime that is known to trouble the space, but which is for the most part overlooked by the official agencies of criminal justice (Reddy and Minaar 2018; Kethineni and Cao 2019; Foley et al. 2019). The major institutional players in cryptocurrency jurisdiction-hop to avoid scrutiny, existing primarily online and individuals take part online, and anonymously if they wish.

At the time of writing the cryptocurrency market has a capitalization of almost three trillion US dollars. In this, it rivals the value of Apple, the world's largest publicly-traded company. At such a size, it is one of the most significant elephants in the room of global finance: while debates about its future regulatory status gather pace it remains 'out there in left field' as an economic area with very little official regulation or policing, and it is a new technosocial playground for fraud.

SCAMS: MYRIAD INVENTIVE VARIATIONS ON SOME BASIC UNDERLYING SCRIPTS

Scams have been around for a long time. The golden era of the so-called Big Con—the late 19th and early 20th century—has been recorded in popular and academic literature (Maurer 1940; Brannon 1948). While Short Cons aimed to 'take' (i.e. steal from) a prospective victim (a 'mark') for the money they happened to be carrying on their person, the Big Con was an elaborate construction designed ultimately to encourage the mark to drain their bank account in order to participate (the 'send'). Marks would be susceptible to the send because they would have been made to feel that they were betting on a sure thing: the essence of the Big Con was to offer up an illicit opportunity to the mark that looked like it was a sure-fire way to beat the system (Maurer 1940). Some Big Cons involved setting up fake betting shops, populated by paid 'shills' who were actors. The mark would be persuaded that his confidante, the con man, had access to race results before they became official, allowing bets to be placed which were guaranteed

to win. He would be allowed a few small wins at the fake bookmaker's shop to test the system and, duly persuaded, he would be sent to gather funds for the big one. This time, however, he would lose. The con man would declare it inexplicable—something unexpected must have gone wrong—and a process of conversational post-mortem would begin that Goffman called 'cooling the mark out' (Goffman 1959). Meantime, the fake betting shop was dismantled and the scammers would make their escape (Maurer 1940).

It would not have to be a sports betting set-up, of course. It could just as well be fake stock market investments, or any other get-rich-quick scheme. Scams are dressed in endless variety, and this is essential to their success: if they were all the same they would be easy to spot, and to avoid. The endless variety in scams is, however, layered over some core underlying common themes. The drama may always be slightly different but the source material is often essentially the same. The Big Con gives us an indication of what some of those common themes in scam routines are.

First, the scam architecture should appear indistinguishable from comparable legitimate entities or offerings (Doocy et al. 2001). If the betting shop looks obviously fake, the scam will not work and the same is true if the con artist appears 'out of place' rather than someone with an apparently reasonable explanation for being involved (Levi 2008: 394). For example, in contemporary terms, it was important that Bernie Madoff's investors believed they were sending their money to a conventional investment firm, and a conventional fund manager, not a scammer running a Ponzi enterprise (Balleisen 2017; Manning 2018).

Second, some scams work on the maxim 'you can't cheat an honest man' (Maurer 1940; Delord-Raynal 1983). In these versions, the attraction for the mark is the opportunity to make illicit gains (Edelson 2003; Holt and Graves 2007). A softer version of this, which does not require dishonesty on the part of the mark, is the presentation of a scheme that seems as though it is loaded in their favour, when in fact it is loaded against them (Mackenzie 2010): perhaps not an illegal opportunity then, but still one in which the mark sees a chance to get the better of others.

Third, there is the dynamic—well-known to consumer fraud awareness campaigners—of an offer seeming too good to be true (Titus and Gover 2001). For the victim in these circumstances, temptation may outweigh reticence and rationality; if the offer appears beneficial enough, some marks will persuade themselves it is legitimate and ignore evidence to the contrary simply because they feel so strongly that they would like it to be so (Leff 1976; Prus and Sharper 1977).

Fourth, the illicit nature of the opportunity presented (the second point above), and the retrospective appreciation that the offer was too good to be true (the third point), both assist in the cooling out process. In respect of illicit schemes, the mark may feel complicit and therefore less likely to go to the police because of the perception of self-incrimination involved (Titus and Gover 2001; Holt and Graves 2007). Where the scheme was not illicit, the cooling out strategy might involve drawing attention to the fact that the mark was taking a risk on an enterprise that, examined with a fresh rationality in hindsight, bore clear hallmarks of a potential scam—clearly too good to be true. So they may be encouraged to castigate themselves as having been so greedy as to blind themselves to an obvious reality, with the aim of leading them to conclude they were responsible in some measure for their own misfortune.

Fifth is the get-in-quick nature of the once-in-a-lifetime opportunity. The mark is given the idea that if they pass up the chance to get involved, someone else will surely take it up. This sense of time pressure makes full investigation of the scheme seem inopportune, and increases the chance the mark will push concerns to one side and jump in. Time-limited offers are, of course, widely used as persuasive devices in the conventional sales world too (Leff 1976) and this observation draws us back to the 'appearance of legitimacy' requirement in the first point above. Where manipulative but non-criminal sales techniques are such a widespread feature of contemporary consumer mar-

kets (Cialdini 2009), those edgy persuasion techniques become much more ambiguous signals; perhaps indicative of a scam, but perhaps not. As such, marks are left to the often very difficult task of trying to discern whether an illegal purpose lies behind the skilled emotion-management of the marketing racket (Santoro 1984; Pratankis and Aronson 1992; Doocy et al. 2001).

Sixth, and finally, the Big Con was often based around gambling and this draws our attention to evidence that some scams play off various types of 'gambler's fallacies' like the effects of near-wins. Near wins, like two cherries rather than three on a slot machine, may give the impression that it is worth another try since you came so close. This effect can be useful in keeping marks involved in scams where the 'take' occurs in tranches over time rather than in one hit. Titus and Gover (2001) summarize the technique:

> "once bitten twice shy" doesn't apply to many fraud victims … some scams are set up to appeal to tendencies that are similar to those that keep some people playing the one-armed bandits and lotteries to a point that can best be described as a "triumph of hope over experience" (Titus and Gover 2001: 145).

These six social mechanisms put to work in scam scripts are so old and well-used that we might even refer to them as among the 'classic' essences of a scam. It is therefore instructive to find that they are as evident in the new scams affecting cryptocurrency trading markets as they are in examples of scams taken from the era of the Big Con more than a hundred years ago. This turns a useful historical lens on the idea of new or emerging forms of crime and it might be tempting to conclude, as mentioned above, simply that the cutting edge of online crypto-finance can be seen to involve scams that are old criminal wine in new technological bottles. Those making that argument might suggest that the digital technology here is the 'tool' or 'instrument' of the crime rather than being fundamentally transformative of it (Grabosky and Walkley 2007), facilitating crime in terms of measures like speed, distance and volume (Wall 2015; Levi et al. 2015), but requiring only modest adaptations in the basic underlying scam routines. That line of argument would, however, not adequately capture the growth of crypto scams as a cultural form, integrated into and to a certain extent defining the economy of the space in question. A better interpretation is that crypto and its scams are part of the increasing hybridization of on/offline culture, economy and social life and so while of course old routines persist they adapt, mutate and expand to explore this new quasi-metaverse of financial speculation.

METHOD

The paper is based on ethnographic research in cryptocurrency trading and the online discussions around it. The aim of the research is to generate an accurate picture of financial crime as it is experienced in the crypto world, and to ask what this means for criminology in terms of the extension of current debates about cybercrime, grey economies and a critical cultural interpretation of social and financial lives increasingly lived in a blended on/offline way.

The methodological approach has been participant observation and this has two main aspects to it. First, it involves participating in discussion in online crypto trading chatrooms, which allows for a study of the discourse of the marketplace as well as gathering stories from traders about scams they have encountered (Hooley et al. 2012). Second, it involves participation in the economic side of the market through cryptocurrency trading. This second approach is important for various reasons. Without active participation in trading, the idea of ethnography would be significantly diluted here: the research would be relying only on reports from other traders about 'how it is' rather than obtaining any independent validation, which in this case is obtained by personal experience. As well as the verifiability of chatroom data, the other main

reason for participation in trading is that it helps to overcome the inherent difficulty of understanding the financial instruments that are the basis of the scams being researched. Crypto can be fiercely complicated, and the newcomer to the scene is faced with a very steep learning curve. Taking part in the market both through discussion and through trading has been, for me, in some cases the only way to unravel what is really going on.

The research was conducted over an intensive period of about a year, from late 2020 to late 2021. Prior to that there was a longer period of around three years where I was exploring the scene, initially 'lurking' (Ilan 2020), getting used to its routines, rhythms and jargon, and then slowly moving from more of an outsider or 'complete observer' role to an insider, and an active participant (Kozinets 2010). The study in this paper is focussed on scams as one of the defining features of crypto, but there are quite a few other defining features that would be rich grounds for future research. Demographics is one such area. The considerable majority of crypto traders seem to be young men, and the chatrooms are infused with language and attitudes that are sometimes aggressively right wing, individualist, hetero-normative, soft-pornographic and racist (cf. Golumbia 2016). In this paper, however, we will focus on the scams themselves rather than who the offenders and victims are. The timeframe for the research was guided by the aim of data saturation in respect of the main research questions: how the main types of scams in crypto work, and how these fit into, or alter, criminological theory about the hybrid technosocial development of cyber or digital crimes.

Several ethical considerations are raised by an ethnography of online economic crime. In the chatroom/discourse part of the study, the whole space is pseudonymous: everyone in crypto chatrooms uses an online alias. A very small minority of participants are 'doxed' (that is, they have revealed their real identity) while the vast majority are anonymous. The research is covert, and this is justified because (a) all data is gathered from publicly accessible online forums where there are no barriers to entry and everyone posting content knows it might be read by anyone, (b) almost everyone in the scene is similarly 'covert' in the sense that nobody other than the doxed minority mentioned is open about identity or purpose: anonymity is a fundamental premise in crypto, and (c) the research is in the public interest with no foreseeable harm to anyone involved. Considering the covert nature of the study and the lack of express consent this involves, I do not produce any direct quotes in this paper. This may dilute the reader's access to first-hand evidence but I do my best to overcome that by providing description that encapsulates an overall sense of what has been said.

THE GROWTH OF CRYPTO TRADING

A blockchain is a decentralized online ledger (Zook and Blankenship 2018). Blockchains are decentralized because transactions are verified automatically by computers working with algorithms (Baldwin 2018). Cryptocurrencies are tokens held on blockchains. In 2020 a trend called DeFi (decentralized finance) introduced decentralized exchanges ('dex'). These are web apps where users can perform token swaps. The dex does this automatically: there is no banker or middleman in the process. To enable these automatic token swaps, a dex needs liquidity. In other words, it will hold pools of the tokens that can be traded so that buyers can draw on those pools to get the tokens they want. Liquidity is usually initially deposited by the creators of the tokens, and then after that by the traders. Traders can deposit liquidity into a dex, i.e. lend it tokens, which it will use to fulfil other people's trades, and the lenders receive rewards in the form of a cut of the trading fees.

DeFi has opened up a whirlwind of opportunities for investment and return. In principle, DeFi is simply about removing the institutional constraints from financial product markets as we experience them in the 'centralized' economy. So in DeFi in addition to basic token

purchases on a dex you can also make or take out loans, invest for yield, make bets on future price movements and myriad other permutations of making your money work for you, without the barriers of credit checks, bank accounts, or character references (Härdle et al. 2020). But DeFi, and decentralization generally, can bring problems as well as opportunities. In a decentralized economy, you are completely in charge of your money and your trades. There is nobody else looking out for you. There is no pop up from your bank asking if you are sure you want to make a transfer. There is no customer service helpline. There is no daily limit on what you can transfer or who you can transfer it to, nor is there an age limit for participation. Youth, gambling addiction, mental instability, borderline bankruptcy—none of these are a barrier to entry. This is an investment market in which anyone with a computer and a reasonably high financial risk threshold (cf. Van Wyk and Benson 1997; Schoepfer and Piquero 2009) can participate directly. If you accidentally send money to the wrong address, it is gone. If you buy the wrong thing or panic sell at the bottom, too bad. If you lend your tokens to a dex as a liquidity provider, they will be lost if the platform goes bust or disappears for some other reason.

LAMBOS ON THE MOON: THE CULTURE OF CRYPTO

Around the economic side of crypto trading, a culture has emerged. Crypto traders form online communities to talk about purchasing opportunities, trading successes and failures and technical analysis. The core online discussion platforms are Telegram, Discord and Reddit. These host all kinds of discussions, from rational market analyses to shilling shitcoins. Shilling is talking up the chances of a token going to the moon. All of the tokens are relentlessly shilled by holders. The tokens with the lowest market capital, which are often also the newest, are 'shitcoins', seen as high-risk high-reward plays. There is a chance they will moon, but there is also a significant chance that they will either languish at the bottom of the pile forever, leaving the once-hopeful buyer 'holding the bags' as other speculative investors jump ship and move on; or alternatively vanish altogether, perhaps because they were part of one of the scams detailed below.

'Degen' traders who cannot resist FOMO (fear of missing out) will 'ape' or 'yolo' into shitcoin moonshots. FOMO in this context is an embodied internet experience. It is hard to describe or overemphasize the extraordinary thrill of placing a bet on a shitcoin and watching it shoot up in value by ten or one hundred times over a period of a few hours or a few days. The experience is visceral, and quite surreal. It is equally visceral and surreal to see your money disappear when the market goes the other way. To avoid being left holding bags, a trader should be careful of FOMO and must 'DYOR' (do your own research) to decide if the 'fundamentals' behind a token make it an attractive investment.

Working products are a rarity in crypto, many projects being at the ideas stage, perhaps full of promise but currently 'vapourware' as the market refers to technical solutions that do not yet exist. With such a dearth of real-world connection, the concept of fundamentals or FA in stock market speak (fundamental analysis) has become so diluted in crypto that traders looking for a quick flip refer instead to the 'pumpamentals' of a project, which is loosely translated as the prospects that a shitcoin will cause FOMO and moon.

The longest-running joke in the crypto forums is probably the Lambo. If you get into a shitcoin early enough, and if it moons hard enough, you might cash out with enough funds to buy a Lamborghini. Crypto forums are full of pictures of Lambos, a tongue in cheek aspiration. For its part, the car manufacturer apparently enjoys the attention (Pathak 2018).

As well as the absurdist and hyped reimagining of the high risk profit-chasing elements of stock market culture evident in the discourse of crypto trading and its Lambo dreams, three other important features of the socio-economic context of the market further set the tone for

scams to thrive. This is a context in which (a) market abuse is normalized, (b) you can lose money very quickly and you will come to expect that as part of the normal course of trading crypto and (c) the main method of crime control is trying to keep your wits about you. Let us briefly fill out those features of the landscape in which scams have emerged.

The normalization of market abuse

Price manipulation is normal in crypto. So-called 'whales' who own a lot of tokens can control pricing in the market. Whales can dump the price, setting off limit sell orders that other traders have set slightly below the current price of the token. These auto-sells dump the price even more. Then people start panic selling: they see the price dropping fast and want to exit. The result of all of this can be a very quick and severe sell-off, instigated by the whale, that drops the price dramatically and allows the whale to buy back in at the bottom. Whales frequently use this tactic to increase the number of tokens they hold. The result for 'minnow' traders whose fragile investments are thrown around in the economic waves created by whale price manipulation is a pervasive feeling that the market is not fair. This dilutes the outrage or surprise victims may otherwise feel when taken in by scams: it is simply to be expected that others are constantly deploying underhand tactics to manoeuvre you into losing trades.

The normalization of losing money in a flash

Sometimes crypto projects just give up. The developer and the marketing officers sell all their tokens and then announce that they are stopping the project. At this point, the price drops to near zero, and investors have no recourse other than to write it off to experience and try to make the investment back with a win on another project. Exchanges get hacked causing a massive and irrecoverable loss of user funds, and they sometimes collapse altogether. There are, in fact, a multitude of ways funds can disappear almost instantly in crypto, and this possibility hangs in one's mind over all investments made in the space. This adds a sense of caprice to the whole enterprise: you might try to be as safe as possible but to continue investing in crypto you have to accept catastrophic loss as a possible outcome. All such losses are irrecoverable in decentralized crypto markets. Having come to expect some instances of serious loss as part of the normal course of trading, when scams cause those losses their perceived importance fades somewhat into the overall tapestry of a high-risk environment.

There is no crime control in crypto: look out for yourself

As suggested in the discussion of decentralization above, crypto is a 'responsibilized' (O'Malley 2008) investment space. The general approach to taking a loss, whether due to crime, misjudgement or mishap, is to write it off. Most traders seem to think resort to law is futile, and this fits with the explanations for non-reporting of victimization in the fraud literature (Doig 2006); a leading reason—along with embarrassment at having been duped (King and Thomas 2009)—being that victims do not expect the police to catch the offender, and think restitution in respect of their loss is unlikely (Ross and Smith 2011). Levi observed more than a decade ago that 'formal social control—the police and the criminal courts—has not been particularly interested in frauds other than the more visibly harmful' (Levi 2008: 412) and scams are a field where awareness-raising and self-help avoidance techniques have been at the forefront of crime prevention (Shadel 2012). This is also the case in crypto scams today, where the police are only really interested in what they perceive to be the most major frauds (personal communication from specialist police, and see Levi 2017 for the same point made in relation to cybercrime fraud more generally). Although the police do not yet see it that way, I would argue that crypto is just such a major fraud scene. Data gathered by expert 'on-chain' analysts has identified that in the first half of 2021 some single addresses (i.e. probably solo individuals) have been making

over US$ 1 million *per day* from some of the scams outlined below (data on file with author). The large annual analytical crypto crime report conducted by Chainalysis found scams to be the majority of all crypto-related crime in 2020 (as was the case in 2019 too), with scams representing 54% of illicit activity, valued at roughly $2.6 billion (Grauer and Updegrave 2021). Despite these figures and what we might hope they would mean for policing, the fact remains that from the perspective of the trader this is for the moment an almost entirely unregulated zone and therefore protection from, or compensation and justice for, criminal losses experienced is not expected. The chances of crypto scammers being investigated, let alone pursued, by police or other regulators are not high (Warren 2020).

In summary, we find an aggregation of 'wild west' indicators in crypto. We are building a picture of a technosocial grey area, a cultural and economic space without many formal rules. Scammers find ideal victims here: people who ape into highly speculative investments with a risk radar that has fairly loose settings; people who know the market is seriously manipulated and who therefore are not expecting fairness or good behaviour from everyone else; people who are used to losing money and treat it as part of the risk of being involved; and people who are not thinking in terms of calling the police because decentralized trading has made them accustomed to the feeling that they are on their own and their best protection is their own judgement. This is a space where FOMO can really kick off, where people lust after Lambos on the moon, and where chat rooms are full of overheated bluster about pumpamentals and getting in quick so you do not get left behind. You could hardly ask for a better socio-economic structure within which to propagate scams. To cap it all off you have the anonymity and reach of the internet which makes it possible for scammers to talk simultaneously via chatrooms to hundreds—and in some cases thousands—of marks wherever they are in the world, receive their money through instantaneous transfers and leave without anyone ever knowing who or where they are (Grabosky et al. 2001; Wall 2007).

So the scene is set for scams to flourish. Let us now take a look at some of them. For analysis we can split these scams up into three categories: advanced fee frauds; 'first in best dressed' scams; and rug pulls.

ADVANCE FEE FRAUDS

The giveaway scam is a form of advance fee fraud, a category of crime that covers myriad versions of the same basic premise: I have something valuable to give you; to release it, send me a payment (Grabosky et al. 2001: 105 et seq). Giveaway scams plague naïve crypto investors on twitter and other platforms. The scammers set up impersonation accounts, pretending to be one of the big names in crypto and expressing the desire to reward followers. Send them some of your crypto 'to confirm your address', and they will return, say, ten times the amount to the address you have sent it from. Those who send crypto never see it again and, as mentioned, in the decentralized world of crypto if you send someone your tokens whether in error or by duplicity there is no way to undo the transaction.

A prominent example of the giveaway scam happened around Elon Musk's appearance on Saturday Night Live in May 2021. While the show was being live-streamed, scammers set up fake SNL social media accounts directing readers to a giveaway page where Musk apparently wanted to incentivize widespread crypto adoption by returning in multiples the bitcoins that his followers might send in. One UK victim lost £400,000 to the scam, sending in 10 bitcoins (Tidy 2021). We can see several 'classic' scam mechanics operating here: the giveaway scam is time-limited, it has the appearance of legitimacy, and it is too good to be true. Victims afterwards report feeling stupid for having fallen for it, placing some of the blame on themselves for allowing greed to cloud their judgement.

Another example of advance fee fraud in crypto is the cry for help scam. This particular scam leverages the adage 'you can't cheat an honest man'. Investors hold crypto in online apps referred to as wallets. Each wallet has a backup mechanism, a seed phrase. The first thing every newcomer to crypto learns is to never tell anyone your seed phrase. If you do, they can re-create your wallet on their computer, and have access to and control of your crypto. It would be like giving someone your online banking password. In the cry for help scam, the scammer posts his seed phrase in an online chat forum in an apparently innocent plea for someone to help him with his broken wallet that is full of crypto. The wallet does not contain any of the particular crypto that is needed to pay the transaction fee for moving tokens, called a gas fee. So in order to steal the scammer's tokens, as well as using the seed to make his wallet on their computers, other users will have to send a little gas into the wallet. The scammer has, however, set up a bot to monitor the wallet, and whenever any gas arrives it is instantly automatically sent out again by the bot, directed to the scammer. As the blockchain is public, once these scams identified it is possible to view the transactions that have gone through the honeypot wallet, which are simply a long and depressing list of gas payments in and out: depressing because of the length of the list, representing the high number of people who have tried to steal the purported-newcomer's tokens. You can't cheat an honest man (in some scams); and had they been honest they would not have fallen victim to the cry for help scam.

FIRST IN BEST DRESSED SCAMS

There are two main types of these scams in crypto: pump and dumps (Kamps and Kleinberg 2018); and ponzi schemes. Telegram groups are rife with crypto pump and dump (PnD). Well known in the stock markets (Stevenson 2000; Shover et al. 2003), this scam is even easier to achieve in crypto. Again, there are many variants, but the central script begins with a PnD group accumulating coins in a crypto project they have expertise. The PnD group will have established a Telegram channel on the promise of their expertize in making good calls, and when they are ready they will 'call' this coin as next to pump. Their followers on Telegram will jump in, ramping the price up with their purchases. These pumps can happen incredibly quickly in crypto; the price can be manipulated upwards ten times and more in a matter of hours. At the crescendo of the FOMO, with naïve marks still piling in, the core group will sell the tokens they accumulated before the call, resulting in a massive dump in the price.

The thing that makes the PnD so successful is the difficulty marks have in identifying whether they have been the victim of a scam, or whether they were just perhaps a little too slow and learned a lesson about FOMO from ape-ing in too high. The routine is a self-fulfilling prophecy since the PnD 'experts' can take credit in their Telegram for being right in their moon prediction, and indeed some of their followers who were early buyers will have made some money on the coat-tails of their scheme, provided they sold before the dump. So the scene is set for the next PnD with the same group of marks, who now believe the hype. In this way, the crypto PnD is similar in format to many other types of long-running scam which seek to extract money from marks in tranches (often the case in romance fraud, see Carter 2021; Rege 2009; and sometimes in the 419 email scam, see Smith et al. 1999). It also leverages near-win psychology: you almost made it, you just need to try to get in a little earlier next time.

There are so many of these scams happening in crypto that it is sometimes difficult to tell an orchestrated PnD scam from the price effects of a 'genuine' influencer who tells her followers on twitter about a token she has just bought and then enjoys the inevitable pump this creates. In the end, both of these PnD types of price manipulation and investor exploitation are so prevalent that they have become like wallpaper to the day-to-day trading of the market. The only practical regulation of these scams is for individual traders to be wary of them; to treat every 'call' or pump of a coin with suspicion, and to resist the FOMO impulse that would tend to make

them want to jump in. This echoes the more general advice in the crime prevention literature on scams that 'consumers are their own best defence against scams' (Smith 2007; and see also Schulte 1995; and Shadel 2012 for two among many examples of approaches grounded in a 'how to avoid scams' approach to prevention).

We can therefore see that permutations of the PnD can be organized around all six of the classic scam themes mentioned. It can have the appearance of legitimacy, where the calls may seem genuine and influencers who are not outright pump and dumpers have comparable price effects through their calls. Often though, PnD groups are explicit in their methods so it is no secret to investors that the leaders are pumping and dumping. Here, the invitation is to join the pump and to dump on other unwitting investors outside the group, although the real underlying intent of the leaders is to dump on their followers. In these cases, what is on offer is an illicit deal that appears to be loaded in the victim's favour when in fact it is loaded against. It is too good to be true and for victims their complicity in the scheme and their shame at the risk their greed has caused them to take can bring a cooling out effect. The opportunity to make gains is clearly a time-limited offer, more so even than the victims will realize given that the odds are so heavily stacked against them. And the scheme enjoys longevity, often preying on the same victims repeatedly, thanks to the impression of a near-win.

Not unlike the PnD in underlying intent, a Ponzi scheme is an investment vehicle that pays out existing subscribers using the proceeds obtained from new recruits (Balleisen 2017). In Spring 2021, a rash of tokens launched which 'tax' new buyers and redistribute it to existing holders. This mechanism is usually all there is to the project: the only aim is to generate more and more participants. Early examples of this kind of token proved outrageously popular, giving early investors massive returns on their entries. There followed hundreds upon hundreds of imitators of these first few projects. The first few Ponzi tokens took weeks to grow, but now the timeline has accelerated as investors have become wise to what is at stake. Most of these tokens now pump violently in the first few hours and then dump calamitously, giving very early entrants—among them the scheme organizers—returns at the expense of those later who lose everything. To that extent, these Ponzi tokens are often comparable to PnD schemes in their themes and mechanics.

RUG PULLS

A 'rug pull' is an exit scam; so like Ponzi's, PnD's and advance fee frauds, it is yet another type of criminal routine with a long history. In crytpo, rug pulls can be slow or fast.

In a slow rug, the developer will have reserved a large amount of the project's tokens for themselves, and after launch as people buy tokens on the market, thus giving them value, the developer will sell theirs in tranches. The price might pump in the first few hours or even days but ultimately, like a slow puncture in a tyre, the volume of tokens the developer is selling will gradually suppress the price until the project ultimately dies (Levine 2021).

The slow rug puller is likely to be in the project's telegram group chatting with new buyers while he is stealing their money by dumping coins. In Goffman's example, cooling the mark out was the process of staying with the victim during and after the scam to make sure they did not call the police. The way con artists would do this was through what Goffman referred to as helping them to 'adapt to failure' and giving them 'instruction in the philosophy of taking a loss' (Goffman 1959: 459).

Some crypto scammers have become quite expert in cooling out. They will be in the chat telling you that the dip is just early buyers selling, that it pumped a lot at the beginning and it is natural for people to take some profits, that other crypto tokens that went on to valuations in the millions had dips just like this at the start, the beginning is always a bit rocky (the 'appear-

ance of legitimacy' by comparison). They will tell you that actually you should see this ongoing dip as a great buying opportunity, so you should buy up some more because it will take off soon and you don't want to be left behind (the FOMO-inducing 'time-limited appeal'). They will say things like scared money doesn't make money, and that you should have 'diamond hands, not paper hands', in other words that you will be ultimately rewarded for holding on through tough times. And all the time they are selling the ground from underneath your feet. Eventually when it becomes clear that the price is not going to recover they might say that crypto is risky and everyone knows that; not everything succeeds despite the best intentions; that they were heavily invested too and they have lost more than anyone; and that there will always be other opportunities so let's all just focus on the next moonshot and try to make it all back.

The idea of cooling out marks is therefore just as relevant to crypto crimes in 2021 as it was to con games a hundred years ago. Some of the detail of what exactly is being said has been updated to meet the new fintech context, and while the overall technique remains the same in basic psycho-social structure it is being made in a new context. Since they can (and will) simply delete their telegram account, close the chat group and disappear once the fraud is complete, the main purpose of cooling out in crypto rugs is to keep marks on the hook until the scammer has managed to sell all their tokens. The cooling out discourse is therefore a tactic of prevarication and delay here, concerned with framing perceptions of the crime as it is ongoing more than a reconceptualization of prior events. There are elements of the technosocial scene that render this an easier thing to do in crypto than IRL. The mediated nature of the chatroom and the relatively inscrutable investment opportunities being offered mean that it is very difficult to discern the truth of what is happening, and this allows dissembling discourse to achieve more purchase than it otherwise might. Events tend to become more clear in hindsight, but a slow rug can be hard to differentiate from any other kind of underperforming investment at the time, especially if someone is making great efforts to persuade you it is the latter.

While a slow rug is usually a developer token-selling scheme, a fast rug is a liquidity pull. Recall the discussion of DeFi dex's above, and that the pools of tokens they need to execute trades come from liquidity provision from developers and traders. In a fast rug pull, a scammer will make a new token, add liquidity to a dex to allow traders to buy it and then when a suitable amount of buying has happened so that the liquidity pool has become inflated on the dex, the scammer will remove it. As they abscond with all the money, investors are left with worthless tokens that could not be traded even if there was any remaining sense of value because there is now no marketplace to do so.

Both types of rug, slow and fast, are common in crypto. The number of projects pulling the rug every day is incredible. One analyst found more than 3,000 instances of total liquidity removal in just one day (data on file with author). Most, but not all, of those will have been rugs; there are occasional legitimate reasons for pulling liquidity, such as project restarts. The result of this ubiquity of exit scams is that they have become normalized as risk-events. How can they be so successful? Surely traders could be more adept at avoiding them? Traders may be able to see some of the tell-tale signs, some of the time, but the temptation to get in early on a project that lacks much verifiable information can be too great. It is not unusual for speculative crypto traders in their thousands to enter projects fully aware that they might be a rug pull, protecting themselves only by not investing more than they are willing to lose and just hoping for the best.

TOWARDS THE METAVERSE: BLENDING FAMILIAR CRIMINAL ROUTINES WITH THE TECHNOSOCIAL GREY CRYPTO ECONOMY

The unregulated wild west of crypto trading is rife with market manipulation and lucrative opportunities of dubious moral and legal standing, and scams are so prevalent as to be normalized

as an experience and as such diminished as a legitimate source of grievance. Responsibilized traders work on the basis of *caveat emptor* in a zone that is still largely ungoverned by legal regulation while scammers make hay with endless variations on old themes of deception. Fraud here is endlessly repeated in a vortex of permutations of some common basic roots.

Traders who send bitcoin to an address in the hope of getting more back, attempt to exploit a cry for help, are pumped and dumped, rug pulled, or ape too late into a ponzi token, all have in common in the end the sense that they should have known better and that they are in part to blame for their own misfortune. Each of these scams takes on the appearance of a legitimate, albeit sometimes illicit or prejudicial, offer. Several of them leverage the maxim 'you can't cheat an honest man' or its diluted variant, the scheme that appears loaded in the mark's favour at the expense of some other prospective victim. All of them lure marks with invitations to profit that, viewed ex post facto, victims will agree were too good to be true. They all have elements of time-sensitivity, geared to encourage quick action, leaving little time for reflection. In some cases like giveaway scams this will likely be an explicitly time-limited offer; in others simply a sense that getting in ahead of the crowd is the key to success. They all employ techniques widely used in the gaming industry to encourage gambling: setting up the temptation of a risk worth taking, a potentially big payoff for a relatively small stake, and in some cases the psychology of the near win that can encourage another roll of the dice.

So isn't this just a case of old wine in new bottles? A grey market context that is new and emerging but a crime that is not? It is not that simple. Like our social lives, our financial lives are increasingly moving online, and crypto is a good example of an 'embodied internet': an online experience that involves not only financial decision making but also hanging out in chat rooms, often for most of your waking hours, making online friends and sometimes enemies, sharing jokes, memes and stories, feeling the joys, the pains and the excitement of investing and generally stepping further towards a life lived in a metaverse, having a presence and an identity that straddles dichotomies like on/offline, local/global, simulation/real life. To ask whether this grey technosocial economy and the crimes that have developed with it are 'new' or 'old' is perhaps not a helpful question when so many of us are increasingly cyber-real, living online and offline in ways that are twisted together and cannot now be separated. Tradition and novelty are part of that mix, as they will have to be in any criminology that looks towards the metaverse.

FUNDING

This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement number 804851).

REFERENCES

Baldwin, J. (2018), 'In Digital We Trust: Bitcoin Discourse, Digital Currencies, and Decentralised Network Fetishism', *Palgrave Communications,* 4(14): 1–10.

Balleisen, E. (2017), *Fraud: An American history from Barnum to Madoff*. Princeton University Press.

Banerjee, P. (2021), *Microsoft details plans for building a metaverse for enterprises*, Mint [Online]. Available at: https://www.livemint.com/industry/infotech/microsoft-reveals-metaverse-plans-for-the-enterprise-11635897733673.html [accessed 15 November 2021].

Brannon, W.T. (1948), *The Con Game and Yellow Kid Weil*. Dover Publications Inc.

Brown, S. (2006), 'The Criminology of Hybrids: Rethinking Crime and Law in Technosocial Networks', *Theoretical Criminology,* 10(2): 223–44.

Carter, E. (2021), 'Distort, Extort, Deceive and Exploit: Exploring the Inner Workings of a Romance Fraud', *The British Journal of Criminology*, 61(2): 283–302.

Castells, M. (1996), *The Rise of the Network Society*. Blackwell.

Cialdini, R.B. (2009), *Influence: The Psychology of Persuasion (Revised edn)*. Harper Collins.
Cline, E. (2011), *Ready Player One*. Arrow Books.
Cohen, S. (2001), *States of Denial: Knowing about Atrocities and Suffering*. Polity.
Delord-Raynal, Y. (1983), 'Les Victimes de la Delinquance d'Affaires', *Victimology: An International Journal,* 8: 68–79.
Dodd, N. (2018), 'The Social Life of Bitcoin', *Theory, Culture & Society,* 35(3): 35–56.
Doig, A. (2006), *Fraud*. Willan.
Doocy, J., Shichor, D., Sechrest, D. and Geis, G. (2001), 'Telemarketing Fraud: Who Are the Tricksters and What Makes Them Trick?', *Securities Journal,* 14: 7–26.
Edelson, E. (2003), 'The 419 Scam: Information Warfare on the Spam Front and a Proposal for Local Filtering', *Computers & Security,* 22(5): 392–401.
Foley, S., Karlsen, J.R. and Putniņš, T.J. (2019), 'Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?', *The Review of Financial Studies*, 32(5): 1798–853.
Galemba, R.B. (2008), 'Informal and Illicit Entrepreneurs: Fighting for a Place in the Neoliberal Economic Order', *Anthropology of Work Review,* XXIX(2): 19–24.
Goffman, E. (1959), 'On Cooling the Mark Out: Some Aspects of Adaptation to Failure', *Psychiatry,* 15: 451–63.
Golumbia, D. (2016), *The Politics of Bitcoin: Software as Right-wing Extremism*. University of Minnesota Press.
Grabosky, P. (2001), 'Virtual Criminality: Old Wine in New Bottles?', *Social & Legal Studies*, 10: 243–9.
Grabosky, P.N., Smith, R.G. and Dempsey, G. (2001), *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge University Press.
Grabosky, P. and Walkley, S. (2007), 'Computer Crime and White-Collar Crime', in H.N. Pontell and G. Geis, eds, *International Handbook of White-Collar and Corporate Crime*. Springer.
Grauer, K. and Updegrave, H. (2021), *The 2021 Crypto Crime Report*, Chainalysis [Online]. Available at: https://go.chainalysis.com/2021-Crypto-Crime-Report.html [accessed 14 July 2021].
Härdle, W.K., Harvey, C.R. and Reule, R.C.G. (2020), 'Understanding Cryptocurrencies*', *Journal of Financial Econometrics,* 18(2): 181–208.
Hayward, K.J. (2012), 'Five Spaces of Cultural Criminology', *British Journal of Criminology,* 52(3): 441–62.
Holt, T.J. and Graves, D.C. (2007), 'A Qualitative Analysis of Advance Fee Fraud E-mail Schemes', *International Journal of Cyber Criminology,* 1(1): 137–54.
Hooley, T., Marriott, J. and Wellens, J. (2012), 'Online Ethnographies', in Bloomsbury Collections (ed) *What is Online Research? Using the Internet for Social Science Research*, 73–90. Bloomsbury Academic.
Ilan, J. (2020), 'Digital Street Culture Decoded: Why criminalizing drill music is Street Illiterate and Counterproductive', *The British Journal of Criminology,* 60(4): 994–1013.
Kamps, J. and Kleinberg, B. (2018), 'To the Moon: Defining and Detecting Cryptocurrency Pump-and-Dumps', *Crime Science,* 7(18): 1–18.
Kethineni, S. and Cao, Y. (2019), 'The Rise in Popularity of Cryptocurrency and Associated Criminal Activity', *International Criminal Justice Review,* 30(3): 325–44.
King, A. and Thomas, J. (2009), 'You Can't Cheat an Honest Man: Making ($$$s and) Sense of the Nigerian E-mail Scams', in F. Schmallegar and M. Pittaro, eds, *Crimes of the Internet*. Pearson Education.
Kozinets, R. (2010), *Netnography: Doing Ethnographic Research Online*. Sage.
Lash, S. (2002), *Critique of Information*. Sage.
Laue, C. (2011), 'Crime Potential of Metaverses', in K. Cornelius and D. Hermann, eds, *Virtual Worlds and Criminality*. 19–31. Springer.
Leff, A.A. (1976), *Swindling and Selling: The Story of Legal and Illegal Congames*. The Free Press.
Levi, M. (2008), 'Organized Fraud and Organizing Fraud: Unpacking Research on Networks and Organization', *Criminology and Criminal Justice,* 8(4): 379–409.
Levi, M. (2017), 'Assessing the Trends, Scale and Nature of Economic Cybercrimes: Overview and Issues', *Crime, Law and Social Change,* 67: 3–20.
Levi, M., Doig, A., Gundur, R., Wall, D. and Williams, M. (2015), *The Implications of Economic Cybercrime for Policing*. City of London Corporation.
Levine, M. (2021), *Pump and Dump and Pull the Rug*, Bloomberg [Online]. Available at: https://www.bloomberg.com/opinion/articles/2021-07-01/pump-and-dump-and-pull-the-rug [accessed 16 July 2021].
Lévy, P. (2001), *Cyberculture*. University of Minnesota Press.
Lupton, D. (2014), *Digital Sociology*. Routledge.
Mackenzie, S. (2010), 'Scams', in F. Brookman, M. Maguire, H. Pierpoint and T. Bennett , eds, *Handbook on Crime*. Willan.
Manning, P. (2018), 'Madoff's Ponzi Investment Fraud: A Social Capital Analysis', *Journal of Financial Crime*, 25(2): 320–36.

Maurer, D.W. (1940) *The Big Con: the Story of the Confidence Man and the Confidence Game*. The Bobbs-Merrill Co.
Ohnsorge, F. and Yu, S., eds, (2021), *The Long Shadow of Informality: Challenges and Policies*. World Bank.
O'Malley, P. (2008), 'Neoliberalism and Risk in Criminology', in T. Anthony and C. Cunneen, eds, *The Critical Criminology Companion*. Federation Press.
O'Neill, M.E. (2000), 'Old Crimes in New Bottles: Sanctioning Cybercrime', *George Mason Law Review,* 9: 237-88.
Orton-Johnson, K. and Prior, N., eds, (2013), *Digital Sociology: Critical Perspectives*. Palgrave Macmillan.
Palmer, M. (2021), *A Beginner's Guide to the Metaverse (and Making Money In It)*, Sifted [Online]. Available at: https://sifted.eu/articles/metaverse-what-is-it-guide/ [accessed 15 November 2021].
Palmer, N., Addyman, P., Anderson, R., Browne, A., Somers Cocks, A., Davies, M., Ede, J., Van der Lande, J. and Renfrew, C. (2000), *'Ministerial Advisory Panel on Illicit Trade', December 2000*. Department for Culture, Media and Sport.
Pathak, S. (2018), *When Lambo? How Lamborghini became the status brand of the crypto boom*, Digiday [Online]. Available at: https://digiday.com/marketing/lambo-lamborghini-became-status-brand-crypto-boom/ [accessed 19 March 2021].
Powell, A., Stratton, G. and Cameron, R. (2018), *Digital Criminology: Crime and Justice in Digital Society*. Routledge.
Pratankis, A. and Aronson, E. (1992), *The Age of Propaganda: The Everyday Use and Abuse of Persuasion.* W.H. Freeman.
Prus, R. and Sharper, C.R.D. (1977), *Road Hustler: The Career Contingencies of Professional Card and Dice Hustlers*. Lexington Books.
Reddy, E. and Minaar, A. (2018), 'Cryptocurrency: A Tool and Target fro Cybercriminals', *Acta Criminologica: Southern African Journal of Criminology,* 31(3): 71–92.
Rege, A. (2009), 'What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud', *International Journal of Cyber Criminology,* 3(2): 494–512.
Reid, D. (2021), *Who is Going to Police the Metaverse?*, *Liverpool Hope University* [Online]. Available at: https://www.hope.ac.uk/news/allnews/who-is-going-to-police-the-metaverse.html [accessed 15 November 2021].
Ross, S. and Smith, R.G. (2011), 'Risk Factors for Advance fee Fraud Victimization', *Trends & Issues in Crime and Criminal Justice, No. 420*. Australian Institute of Criminology.
Santoro, V. (1984), *The Rip-Off Book: the Complete Guide to Frauds, Con Games, Swindles and Rackets*. Loompanics Unlimited.
Schneider, F. and Enste, D.H. (2002), *The Shadow Economy: An International Survey*. Cambridge University Press.
Schoepfer, A. and Piquero, N.L. (2009), 'Studying the Correlates of Fraud Victimization and Reporting', *Journal of Criminal Justice,* 37(2): 209–15.
Schulte, F. (1995), *Fleeced!: Telemarketing Rip-offs and How to Avoid Them*. Prometheus Books.
Shadel, D. (2012), *Outsmarting the Scam Artists: How to Protect Yourself From the Most Clever Cons*. John Wiley & Sons.
Shapland, J. and Ponsaers, P., eds, (2009), *The Informal Economy and Connections with Organised Crime: The Impact of National Social and Economic Policies*. Boom Juridische Uitgevers.
Shover, N., Coffey, G.S. and Hobbs, D. (2003), 'Crime on the Line: Telemarketing and the Changing Nature of Professional Crime', *British Journal of Criminology,* 43: 489–505.
Silver, C. (2020), *What is Web 3.0?*, Forbes [Online]. Available at: https://www.forbes.com/sites/forbestechcouncil/2020/01/06/what-is-web-3-0/?sh=6164d5ad58df [accessed 15 November 2021].
Smith, R.G. (2007), 'Consumer Scams in Australia: An Overview', *Trends & Issues in Crime and Criminal Justice No. 331*. Australian Institute of Criminology.
Smith, R.G., Holmes, M.N. and Kauffman, P. (1999), 'Nigerian Advance Fee Fraud', *Trends & Issues in Crime and Criminal Justice No. 121*. Australian Institute of Criminology.
Stephenson, N. (1992), *Snow Crash*. Penguin.
Stevenson, R.J. (2000), *The Boiler Room and other Telephone Scams*. University of Illinois Press.
Stratton, G., Powell, A. and Cameron, R. (2017), 'Crime and Justice in Digital Society: Towards a Digital Criminology?', *International Journal for Crime, Justice and Social Democracy,* 6(2): 17–33.
Tidy, J. (2021), *Bitcoin: Fake Elon Musk Giveaway Scam Cost Man £400,000*, BBC [Online]. Available at: https://www.bbc.com/news/technology-56402378 [accessed 16 July 2021].
Titus, R.M. and Gover, A.R. (2001), 'Personal Fraud: The Victims and the Scams', *Crime Prevention Studies,* 12: 133–52.

Van Wyk, J. and Benson, M.L. (1997), 'Fraud victimization: Risky business or Just Bad Luck?', *American Journal of Criminal Justice*, 21(2): 163–79.
Wall, D.S. (2007), *Cybercrime: The Transformation of Crime in the Information Age*. Polity.
Wall, D.S. (2015), 'The Internet as a Conduit for Criminal Activity', in A. Pattavina, eds, *Information Technology and the Criminal Justice System*. 77–98. Sage.
Warren, J.M. (2020), 'A Too Convenient Transaction: Bitcoin and Its Further Regulation', *Journal of Law & Cyber Warfare*, 8(1): 5–29.
Wong, W.H. and Duncan, J. (2021), *Facebook's metaverse won't be bound by physical borders—neither are human rights*, The Globe and Mail [Online]. Available at: https://www.theglobeandmail.com/opinion/article-facebooks-metaverse-wont-be-bound-by-physical-borders-neither-are/ [accessed 15 November 2021].
Yar, M. (2005), 'The Novely of Cybercrime', *European Journal of Criminology*, 2(4): 407–27.
Zook, M.A. and Blankenship, J. (2018), 'New Spaces of Disruption? The Failures of Bitcoin and the Rhetorical Power of Algorithmic Governance', *Geoforum*, 96: 248–55.