Chapter 3

Trust in Cryptomarkets for Illicit Drugs

Kim Moeller

Abstract

The growth in cryptomarkets has reinvigorated the research on illicit drug distribution due to the availability of large-scale data. This data has enabled researchers to ask new and detailed questions about how participants in these markets trust each other enough for the market not to collapse. This question deserves more attention because it has become a taken-for-granted notion that repeated transactions and social categories create trust. Whether online or on the street, economic exchanges under illegality are more uncertain than transactions in the legal economy. This puts higher demands on trust, as there is less information and the stakes are higher. In this chapter, the author presents definitions, typologies, and disciplinary contributions to the study of trust and examine how it has been operationalised in a sample of 13 peer-reviewed articles. These articles focus on three dimensions of trust: process-based trust that derives from repeated transactions with known partners; character-based trust measured by the networked reputation scores; and institutional-based trust in the platform and its administrators. In practice, the trust bases are intertwined. Drawing on the broader social science literature on trust, a mesolevel operationalisation that centres on networked reputation scores as embedded in processes and institutions can draw the research together in a multidisciplinary framework.

Keywords: Trust; cryptomarkets; drug markets; co-offending; uncertainty; anonymity

Digital Transformations of Illicit Drug Markets: Reconfiguration and Continuity, 29–43

doi:10.1108/978-1-80043-866-820231003

Introduction

The question of how co-offenders trust each other in the context of product illegality has attracted scholarly attention for decades (Gambetta, 1988). With the advent of cryptomarkets,[1] researchers now have a novel opportunity to observe drug markets in action on a large scale. The dramatic growth in the number of individuals who participate in these markets and the digital traces they leave has reinvigorated the field of drug market research and enabled new insight into the trade dynamics that stabilise and facilitate drug markets (Barratt and Aldridge, 2016; Décary-Hétu and Giommoni, 2017; Resnick and Zeckhauser, 2002; Van Buskirk et al., 2016). Research on cryptomarkets focusing on illicit drugs often notes that trust is a pivotal factor in enabling transactions. However, there is little agreement on what this trust actually entails. The ensuing lack of conceptual clarity is not exclusive to drug market research. Gambetta (1988, p. x) included a statement on this in the foreword to his anthology:

> Scholars tend to mention [trust] in passing, to allude to it as a fundamental ingredient or lubricant, an unavoidable dimension of social interaction, only to move on to deal with less intractable matters.

Cryptomarkets are a suitable empirical environment to examine theories of trust due to the high uncertainty and non-trivial risks for the actors involved (see Colman, 2023, Chapter 6, this volume; Norbutas et al., 2020a). The anonymity of online identities exacerbates the conventional trust problems in drug distribution and introduces three new sources of uncertainty. Firstly, untrustworthy sellers are able to mimic their reliable counterparts by generating false accounts and fake positive feedback (Holt et al., 2016; Norbutas et al., 2020b). Secondly, the past evidence, from reviews and the reputation system, does not eliminate the risk of future malfeasance (Bancroft et al., 2020). Thirdly, cryptomarket administrators compete on having a trustworthy infrastructure to create loyalty and encourage future purchases (Mao et al., 2020; McKnight and Chervany, 2001). Buyers have to trust not only the technical infrastructure but also the administrators themselves not to abscond with funds. Trust, especially under illegality, is hard to establish and remains fragile once achieved.

The purpose of this chapter is to describe how trust in cryptomarkets for illicit drugs has been examined in a sample of peer-reviewed articles.

To contextualise this quite recent research, I give various definitions and describe the dimensions of trust and highlight how they derive from economists' and sociologists' disciplinary modes of thinking. These discussions are relevant

[1]Note on terminology: I prefer the term 'cryptomarket' as it emphasises the use of encryption technology. The encryption of identities and payments has transformed the online trade in illicit drugs.

for achieving a more nuanced understanding of how cryptomarkets persist despite scamming vendors and law enforcement efforts to shut them down.

Trust Definitions

Several authors have noted how trust is a 'subtle, diffuse, and elusive' concept (Nooteboom, 1996, p. 990) with no a scholarly definition (Gambetta, 1988). For economic transactions, the central factors for trust are uncertainty, risk, and willingness to be vulnerable (Mayer et al., 1995; McKnight and Chervany, 2001; Rousseau et al., 1998). Granovetter (2018) suggested that trust can be represented as a continuum, ranging from the purely instrumental calculation of interest to non-rational normative commitments and emotional attachments, such as the trust a child can have in a parent (see also Lorenzo-Dus and Di Cristofaro, 2018; Swedberg, 2009). For the purpose of this chapter, I am most interested in the calculative types of trust that pertain to economic transactions. However, the illegality and associated uncertainty imply that normative elements are also relevant.

Moreover, trustworthiness and cooperation are two closely related concepts. Trustworthiness is the probability that a trustee 'will perform an action that is beneficial or at least not detrimental to us' and 'is high enough for us to consider engaging in some form of cooperation with him' (Gambetta, 1988, p. 217). It hinges on a perception of intentions and motives, and involves an assessment of integrity, benevolence, and ability (McEvily et al., 2003). Cooperation is occasionally used synonymously with trust, and the distinction may be unclear. Importantly, cooperation does not necessarily put any of the parties at risk and can also occur without trust (Mayer et al., 1995). What appears to be trust between co-offenders may actually be cooperation that involves testing trustworthiness, risking trust, or fatalistic attitudes (Von Lampe and Johansen, 2004). Trust is the underlying psychological condition that can cause or be the result of assessments of trustworthiness and the process of cooperation.

Dimensions of Trust

Several typologies highlight how to operationalise trust analytically. A few examples will illustrate this. From the legal online economy, Mao and colleagues (2020) study of the Airbnb platform departed from a distinction between personal trust (in the host) and institutional trust (in the platform) and concluded that a more comprehensive trust formation framework could include five overlapping dimensions: experience-, calculative-, cognition-, personality-, and institution-based trust. McKnight and Cervany (2001) proposed a typology for analysing e-commerce consisting of three elements: a dispositional element (trust in general others) inspired by psychology and economics, an institutional element (trust in platforms) from sociology, and interpersonal trust (trust in specific others) from social psychology and economics.

Rousseau and colleagues (1998) also applied an interdisciplinary approach. They identified four shared understandings across social science disciplines.

A *deterrence-based trust* relies on sanctions for breaches – for example by imposing switching costs. This means that if you cheat, you will have to find a new transaction partner, and that takes time and effort. A *calculus-based trust* applies not only deterrence but also credible information regarding the intentions of another. These are combined with a *relational trust*, derived from repeated interactions with known others, and an *institutional-based trust* that provides a critical mass that allows the other trust forms to exist in the first place. Von Lampe and Johanssen (2004) suggested a mesolevel network approach for analysing trust in organised crime, which consists of four elements: an individualised trust based on rational expectations of how the trustee reacts to sanctions and irrational affections; trust based on reputation and fear of losing this status; generalisations that indicate the person is a member of a delinquent subculture; and, lastly, an abstract individual characteristic of generalised trust in others.

These typologies have several considerations in common but have the most explanatory power when applied to their specific area of inquiry (e.g., the five elements identified by Mao et al., (2020), may be too detailed to apply to the cryptomarket context). For the purpose of this chapter, I will employ Wehinger's (2011) parsimonious typology of three broad ways to generate trust in cryptomarkets: process-based, characteristic-based, and institutional-based. I explain these in more detail later in the chapter.

Disciplinary Contributions

The lack of a unifying definition reflects variation in disciplinary contributions and levels of analysis (McKnight and Chervany, 2001; Rousseau et al., 1998). While psychologists were the first to study trust in the 1950s, with a focus on individuals and personality attributes (Resnick and Zeckhauser, 2002), contributions from economics and sociology are arguably more relevant for understanding the process of exchanging illegal drugs for money. However, economists and sociologists have notoriously different understandings of human agency and economic transactions (Moeller, 2018; Swedberg, 2009).

In economic terminology, cryptomarket buyers operate in a 'lemon' market where they are unable to differentiate between sellers offering quality products and those offering poor quality products (Holt et al., 2016). Economists tend to view trust as either calculative or institutional, focusing on asymmetric information – uncertainty, adverse selection, moral hazard, and choice mechanisms (McKnight and Chervany, 2001).

These issues are often analysed in a game theoretical framework, where participants estimate their transaction partners' propensity for cheating and decide on a course of action (Dixit, 2004). Game theory differs from the isolated transactions assumed in neoclassical economics because a repeated game implies that participants have an incentive not to cheat or act opportunistically. Cheating would damage their reputation and hinder future transactions. Having repeated transactions with the same partner builds trust over time and is economically rational because it reduces risks, information search time, and transaction costs

while increasing predictability and improving decision-making (Wang et al., 2014; McEvily et al., 2003).

However, as Williamson (1975) noted, in practice, trust is most important for non-calculative situations of minor economic significance. If the stakes are high enough, even transaction partners with whom one has had several exchanges may defect or exit the game. Some participants may be inclined towards such a pursuit to their own advantage and use guile and deceit to achieve it. To prevent opportunistic behaviour, contracts and deterrent controls at an institutional level are necessary complements to transactions. While controls may facilitate trust, they are costly and reduce efficiency.

A sociological conception of trust in economic exchanges can also focus on reducing uncertainty (Bancroft et al., 2020; Diekmann et al., 2014; Granovetter, 2018). Sociologists tend to analyse trust as interactions among people in groups and social structures such as organisations (McKnight and Chervany, 2001; Wang et al., 2014). Importantly, they emphasise that trust is not reducible to calculation and profit making (Swedberg, 2009).

Of particular relevance to this chapter is Granovetter's (1985) proposal that a focus on transactions embedded in social networks can overcome the over- and under-socialised conceptions of action, typically found in sociology and economics. He recommended analysing concrete patterns of social relations in networks instead of impersonal institutional arrangements that seek to deter malfeasance. This embeddedness perspective works at an intermediate level of analysis that seeks to integrate microlevel transactional processes with the macrolevel institutional arrangements (see also Diekmann et al., 2014; Rousseau et al., 1998). An example of an intermediate mechanism is the concept of 'networked reputation' (Glückler and Armbrüster, 2003). This networked reputation has practical applications in the analysis of the reputation scores used in both legal online marketplaces and cryptomarkets. The microlevel processes consist of personal experience with transactions involving that particular partner.

Method

To examine how trust has been analysed in research on cryptomarkets for illicit drugs, I retrieved peer-reviewed articles from the following academic databases: Sociological Abstracts, Academic Search Elite, and Google Scholar. Keywords used in the search were 'cryptomarket' and 'trust'. In the Google Scholar search, I added 'drugs' to delimit the number of hits. For Sociological Abstracts, an advanced search for the keywords anywhere in the text of peer-reviewed scholarly journals elicited five articles, while a similar search of Academic Search Elite elicited ten peer-reviewed studies. In Google Scholar, a whole text search for 'cryptomarket' and 'trust' and 'drugs' elicited 746 links. I first excluded all non-peer-reviewed articles. Next, to screen for relevance, I read the abstract for each article. If the abstract did not describe an analytical focus on 'trust' in cryptomarkets, the article was omitted from further analysis. Thereafter, a close reading was conducted to identify articles that were specifically related to trust in drug distribution on cryptomarkets. After sifting through all of the remaining articles

and removing duplicates from the three searches, 13 articles remained to be used in this study. Table 3.1 presents an overview of these articles.

This does not purport to be an exhaustive sample but is merely sufficient for the purpose at hand. Clearly, the selection criteria 'analytical focus' could mean different things to different researchers. Some studies examine 'cooperation' in cryptomarkets (e.g. Bakken et al., 2018) and could also have been included in a more comprehensive analysis. The retrieved articles were published between 2016 and 2020, with four from 2020 alone. All the studies examined trust empirically, drawing on conceptualisations from a variety of scholarly disciplines but mostly sociology. The articles used both qualitative and quantitative methods. In the following sections, I describe how their findings relate to Wehinger's (2011) tripartite typology.

Trust in Cryptomarkets

In the legal economy, institutional arrangements enforce rules of exchange and define trading conditions. Buyers expect that fraudulent conduct will be prosecuted and that they will be economically compensated – for instance, if they paid with a credit card (Ladegaard, 2020; Przepiorka et al., 2017). In contrast, exchanges on cryptomarkets take place against the state and between users who cannot easily trust one another. Here, transactions are anonymous, geographically dispersed, executed sequentially, plagued by problems of verifiability, and fraught with the constant risk of undercover law enforcement intervention or scamming (Childs et al., 2020; Duxbury and Haynie, 2018a; Norbutas et al., 2020b).

The underlying problem lies in the incentive structure of a trust dilemma: the seller has an incentive not to honour a buyer's trust but rather to maximise profit by keeping the goods or sending goods of lower quality than promised (Norbutas et al., 2020b). This entails a paradox where anonymity is required for access to the marketplace, but this simultaneously increases the risk of fraud (Tzanetakis et al., 2016). Unlike the two-party, seller–buyer relationships in traditional offline drug markets, selling and buying drugs on cryptomarkets is a configuration of at least three parties: administrators/moderators, vendors, and buyers (Kamphausen and Werse, 2019; Tzanetakis et al., 2016). Both individual vendors and market operators can scam buyers by earning their trust and then leaving without completing the transaction (Ladegaard, 2020; Moeller et al., 2016; Norbutas et al., 2020b). In addition, law enforcement agencies can intervene and confiscate the drugs during the shipping stage, but buyers cannot be certain that sellers are not responsible for these events (Aldridge and Askew, 2017; Décary-Hétu et al., 2016). This causes 'noise', as the available information on transactions may be affected by uncontrollable exogenous events (Norbutas et al., 2020b).

In the following sections, I examine how these problems have been analysed in the 13 peer-reviewed articles. I begin each section with a brief description of Wehinger's (2011) conceptualisation of three trust bases – process, character, and institutional. I conclude by discussing how they are associated and how this may inspire future analyses of trust in cryptomarkets.

Table 3.1. Sample Description.

Authors	Date	Title, short	Data	Methods	Marketplace
Tzanetakis, Kamphausen, Werse, von Laufenberg	2016	The Transparency Paradox	32 Vendor interviews, 4 vendor case studies	Qualitative interviews, case studies	Agora
Przepiorka, Norbutas, Corten	2017	Order Without Law	5,675 Item prices	Regression	Silk Road 1.0
Décary-Hétu, Giommoni	2017	Do Police Crackdowns Disrupt Drug Cryptomarkets?	226,297 Listings, 7,280 dealers	Interrupted time series analysis	Agora, Cloud-Nine, Evolution, Hydra, SR2
Masson, Bancroft	2018	Nice People Doing Shady Things	9 Interviews,	Qualitative interviews, ethnography	NA
Lorenzo-Dus, Di Cristofaro	2018	'I Know This Whole Market is Based on the Trust You Put in Me …'	~250 Million words	Corpus Assisted Discourse Studies	Silk Road
Ladegaard	2018	Instantly Hooked?	2,218 Forum posts, 2,116 vendors	Ethnography, regression	Agora
Duxbury, Haynie	2018a	The Network Structure of Opioid Distribution	763 Actors	Social network analysis	Cryptomarket

(*Continued*)

Table 3.1. (*Continued*)

Authors	Date	Title, short	Data	Methods	Marketplace
Kamphausen, Werse	2019	Digital Figurations	Forum posts	Qualitative content analysis	Abraxas, Agora, Dream Market, Nucleus, Outlaw
Bancroft, Squirrell, Zaunseder, Rafanell	2019	Producing Trust Among Illicit Actors	Forum posts	Ethnography	PFM
Norbutas, Ruiter, Corten	2020	Believe It When You See It	6,374 Items, 9,244 feedback messages, 390 seller profiles, 3,192 buyer profiles	Logistic regression	Abraxas
Norbutas, Ruiter, Corten	2020	Reputation Transferability Across Contexts	7,500 Seller accounts, ~2.5 million feedback messages	Longitudinal multilevel regression	Abraxas, Agora, AlphaBay
Ladegaard	2020	Open Secrecy	~1,000,000 Transactions, ~3,000,000 messages	Ethnography, interrupted time series analysis	Silk Road, Silk Road 2.0, BlackMarket, Agora, Evolution
Childs, Coomber, Bull, Barratt	2020	Evolving and Diversifying Selling Practices	965 Forum posts	Thematic analysis	NA

Process-based Trust

In Wehinger's (2011) typology, the production of trust can be process-based, relying on information collected during past exchanges. This is a common element in trust typologies, where, for example, Mao and colleagues (2020) conceptualised the idea of experience-based trust, consistent with the economic understanding of trust as derived from a 'repeated game'. Repeated exchanges with the same others are preferred because information about them is cheap, detailed, and accurate (Reuter and Caulkins, 2004; Rousseau et al., 1998). Both the vendor and the buyer have an interest in maintaining a good relationship and ensuring ongoing business (Beckert and Wehinger, 2013). This form of trust is common in conventional drug markets where interpersonal relationships evolve over time (Tzanetakis et al., 2016). The temporal dimension implies that a more sociologically inspired analysis can include both the rational expectations of sanctions and an element of irrational affection (Von Lampe and Johansen, 2004).

Five of the selected studies empirically examine process-based trust by quantitatively measuring the popularity of individual vendors and counting transactions. Norbutas et al. (2020a, p. 2) found that buyers' previous exchanges with sellers affect their subsequent decisions on whom to buy from. Repeated exchanges 'between the same dyads of buyers and sellers play a crucial role in maintaining trust over time'. It was very rare that buyers 'came back to a seller after posting negative feedback'. Less than 0.5% of all exchanges were made with vendors with whom buyers reported having a 'negative experience … in the past'. Conversely, 'cooperative sellers get awarded by repeated exchanges' (Norbutas et al., 2020b, p. 150). This preference for repeated transactions with the same partner affects the cryptomarket as a whole. Décary-Hétu and Giommoni (2017) and Duxbury and Haynie (2018a, p. 936) found that 'buyers rarely make purchases outside of their own community of 1–3 established vendors'. A small fraction of dealers is responsible for a large portion of total sales. Duxbury and Haynie (2018a) concluded that vendors' process-based trust is more important than the price of their products or the variety of products they offer. These vendors increase the overall activity on the cryptomarket and make it more difficult for scamming vendors to impact the overall network structure.

Décary-Hétu and Giommoni (2017) noted that the concentration of sales on a few vendors also has implications for the potential effectiveness of law enforcement interventions (Warren and Ryan, 2023, Chapter 4, this volume). Police crackdowns on individual cryptomarkets reduce activity but displace transactions to other markets. Central to this adaptive capability is the concentration of transactions with fewer but trusted dealers. Crackdowns have not hitherto been able to limit the scope of total cryptomarket activity (Décary-Hétu and Giommoni, 2017). These effects of crackdowns represent both continuity and change in the adaptive capacity of drug markets. It has always been difficult for law enforcement to disrupt drug markets. Buyers and sellers invent strategies to avoid and mitigate arrest risks and crackdowns (Moeller et al., 2016). On cryptomarkets, technological innovations can support these adaptive strategies and make law enforcement efforts less efficient. Ladegaard (2020) examined this aspect and found that when

an individual market suddenly closed down, users were aware that their trusted exchange partner could participate in future transactions on another cryptomarket platform. Targeting the most popular dealers, and not market administrators, may therefore be a more efficient strategy for law enforcement.

Childs et al. (2020) analysed the practice of direct dealing where vendors and buyers do not rely on the cryptomarket infrastructure but rather move communications to encrypted messaging applications after contact has been made via the cryptomarket. They found that direct dealing is more likely to occur between vendors and buyers that have established sufficient process-based trust, perhaps related to the number of prior transactions (Childs et al., 2020). The advantage of direct dealing is to avoid administration fees. This is an example of the trade-off, also known from conventional drug markets, between operational security and economic efficiency (Moeller and Sandberg, 2015). Trust reduces costs.

To be successful in competition with other cryptomarkets, a platform needs to have some trustworthy vendors who will attract buyers. A process-based trust may be the key component in stabilising cryptomarkets generally, as it strengthens the structure of individual marketplaces. Over time, the process-based trust increases the reputation scores of vendors, which may have the result of them achieving verified status granted by site administrators. In this way, the process-based trust affects the other dimensions of trust, both the characteristic-based trust as well as the institutional-based trust of the cryptomarket infrastructure.

Characteristic-based Trust

Characteristic-based trust is known from research on organised crime, where trust is commonly ascribed to family members, those with a common ethnicity, or a local community (Wehinger, 2011; Von Lampe and Johansen, 2004). Knowledge about common backgrounds enhances the willingness to work together and be vulnerable, as based on expectations and generalisations (Von Lampe and Johansson, 2004; Mayer et al., 1995; Mao et al., 2020). This type of information is not readily available online. However, the reputation systems substitute for the characteristic-based generalisations. In the legal online economy, more than two dozen studies have analysed the effect of sellers' reputations on the probability of product sale and selling price using eBay auction data (for a review, see Diekmann et al., 2014).

Sellers do not cheat, because it might ruin their good reputation and hinder future business. In economic terminology, a reputation system deters moral hazard and adverse selection because a good reputation has a market value (McKnight and Chervany, 2001; Resnick and Zeckhauser, 2002). However, Przepiorka et al. (2017) noted that much of this research is based on small-scale laboratory and field experiments or from online markets embedded in functioning legal systems. We therefore cannot assume that the cryptomarket reputation systems are as efficient in reducing fraud as in the legal online economy. In cryptomarkets, the systems are compromised by problems with manipulation and transferability issues (Moeller et al., 2017), and eventual economic losses are not protected by credit card insurance or police investigation and legal proceedings.

The reputation systems and written feedback in cryptomarkets are arguably the key benefit over conventional drug distribution (Décary-Hétu and Giommoni, 2017). Most of the articles in the sample examined characteristic-based trust in one way or another. Some focused on communicative signalling, but the majority concerned the reputation systems and their vulnerabilities.

Signalling. Given that actual personal characteristics are impossible to ascertain online, signalling is pivotal. Both buyers and sellers have an interest in pretending that something is true (Lusthaus, 2012), and in Gambetta's (1988) approach, signalling theory is concerned with authenticity. The first source of information for buyers is the profile page of a vendor, but vendors can also signal authentic characteristics in the customer feedback system and the discussion forums. Giving written feedback is not usually mandatory, but it is strongly encouraged and a large majority of customers do so (Tzanetakis et al., 2016). Kamphausen and Werse (2019, p. 281) referred to these conversations as the 'communicative constellations' surrounding the logistics of the trade. They noted that buyers preferred vendors to be polite and responsive, to include information about the products and terms of trade, and to be able to handle a quick shipment of the goods.

The reviews concern not only the quality of the product but also the service involved in the transaction. This service includes vendors participating in conversations in an 'earnest, friendly, and respectful' tone (Ladegaard, 2018, p. 241). Lorenzo-Dus and Di Cristofaro (2018) noted that this discursive performance of identity is about signalling integrity and benevolence. The signals are carefully selected performances often concerning technical competence and personal identity (Masson and Bancroft, 2018). Bancroft et al. (2020) described them as being cultivated, mediated, and negotiated between the three parties to the transaction: vendors, buyers, and administrators. Lastly, sellers can perform this discursive signalling by participating on discussions forums. While this could be considered cheap talk because it is not associated with transactions or services; Norbutas et al. (2020b) found that it actually improved vendors' market outcomes. Buyers know that the reputation scores may be compromised. Vendors can add credibility to their scores, their characteristic-based trust, by signalling credibility.

Reputation System. Reputation scores are used to assess potential exchange partners and ostracise untrustworthy actors (Ladegaard, 2020). They reflect multiple dimensions of a seller's trustworthiness, operational security practices, product quality, and communication (Norbutas et al., 2020b; Przepiorka et al., 2017). Regarding trust, Tzanetakis et al. (2016) note that reputation systems constitute arguably the most important difference between conventional and virtual dealing. Online vendors try to establish trust proactively by building a good reputation score, as opposed to relying on repeated transactions and process-based trust.

Reputation scores also attract buyers. Duxbury and Haynie (2018a, p. 936) found that reputation scores better predict buyer preference compared to price levels and selection of products: 'One unit increase in vendors' reputation score is associated with a 0.3% increase in the odds of selecting a given vendor for a drug purchase'. Przepiorka et al. (2017) also found that this was the case and that vendors with better reputation scores sell their products faster compared

to sellers with no rating history or a bad rating history. Norbutas et al. (2020b) tested the external validity of findings from legal online platforms concerning the association between high reputation scores and higher prices. The key difference is that the reputation information is less reliable, user identities are unstable, and exchanges are not insured. They found that the association between reputation and prices also held in the uninsured and anonymous context (but see Munksgaard, 2020, for a critique).

Importantly, the perceived level of trust that a vendor had established via the reputation score is transferable between cryptomarkets. Law enforcement crackdowns used to ruin the reputation scores that vendor built up, destabilising the cryptomarket as a whole. However, Ladegaard (2020) noted that technologies for identity verification and information distribution enable the scores to be transferred between cryptomarkets. This bolsters the reputation systems and enables vendors to operate as nomads in a decentralised economy. He concludes that cryptomarket innovation is driven by external pressure from law enforcement. Childs et al. (2020b) also found that reputation scores are maintained across multiple platforms. However, Norbutas et al. (2020a) emphasised that buyers perceive the transferred scores as incomplete and unreliable information. Despite this reduced reliability, reputation transferability embeds trust relations between buyers and sellers beyond a single cryptomarket's boundaries. In this way, buyers can now use feedback messages and reputation scores to punish opportunistic sellers even in future markets. This technological innovation increases the deterrent capacity, promotes compliance, and pushes out untrustworthy sellers from the market.

The problem with online reputation systems is that they can be gamed. Trustful actors can be impersonated and trust signals can be faked (Bancroft et al., 2020). Some sellers manipulate their scores by inhibiting negative reviews and promoting positive reviews (Bancroft et al., 2020; Bolton et al., 2013). An example is that vendors use free samples to rake up positive reviews, cultivate customers, and increase trade (Ladegaard, 2018). Kamphausen and Werse (2019) described a way of gaming the reputation system by 'shilling'. Vendors use secondary accounts to boost their own reputation or have friends vouch for them. They may also maliciously damage the reputations of competing vendors. Bancroft et al. (2020) referred to this practice as 'reputation fluffing' and noted that the reviews posted on forums are a better indicator of vendor quality, as the discursive signalling here is harder to fake (see also Holt et al., 2016).

While the reputation mechanisms are 'technically robust', they are simultaneously 'socially brittle' (Bancroft et al., 2020, p. 3). Vendors who are known as trustworthy can abscond with buyers' funds overnight in so-called exit scams (Moeller et al., 2017). Vendors also have a less ominous reason for exiting. Norbutas and colleagues (2020b) found that reputation scores in cryptomarkets are extremely skewed. Ratings below the maximum value are only posted in extraordinary cases. In their study, 96% of all feedback messages were 5-star ratings, while 0- to 4-star ratings accounted for about 1%. This gives new vendors an incentive to exit the cryptomarket if they receive a negative rating. It is less costly for them to re-enter with a new pseudonym compared to rebuilding a damaged reputation

(Norbutas et al., 2020b). This procedure exacerbates the unreliability of the reputation score information, and it illustrates Gambetta's (1988) statement that trust is not predicated on evidence but rather on the lack of contrary evidence.

Similar to process-based trust, characteristic-based trust is intertwined with the other dimensions of trust. A reputation score is going to be interpreted by buyers. Some of this interpretation concerns noisiness (i.e., whether the score has been transferred from elsewhere), and some of it concerns an assessment of the administrators (i.e., if they are perceived as efficient in vetting dishonest vendors). Lastly, the score will be interpreted against dyadic process-based experience. Norbutas et al. (2020) concluded that buyers consider negative ratings from other buyers before making their first purchase but that the weight of this information decreases as the number of transactions between a specific vendor and buyer increases. This finding echoes Granovetter's (1985, p. 489) sentiment that buyers are mostly concerned with how honest sellers will be in any exchange with them; in other words, they are 'less interested in *general* reputations than in whether a particular other may be expected to deal honestly with *them*'.

Institutional-based Trust

In the legal economy, trust in economic exchanges is supported through institutions such as courts, credit rating agencies, and other impersonal structures that reduce the negative effects of product uncertainty (Beckert and Wehinger, 2013; Glückler and Armbrüster, 2003). All of the trust typologies reviewed for this chapter include an institutional element – for example, Mao and colleagues (2020) 'trust-in-platform' and the observation that legal online transactions are protected by insurance from credit card companies.

Illicit transactions obviously lack this institutional protection, and cryptomarket administrators go to considerable lengths to demonstrate that users can trust that the marketplace is relatively safe. Lorenzo-Dus and Di Cristofaro (2018) specified that Silk Road users must trust that the marketplace can effectively mediate transactions, protect them from law enforcement surveillance, and will not defraud them intentionally. Deterrence mechanisms that sanction breaches and encourage cooperation through self-interest are examples of institutional measures to promote trust (Rousseau et al., 1998). Specifically, cryptomarket administrators can increase the costs of opportunistic behaviour by introducing fees for opening a seller account and monitoring and banning untrustworthy sellers (Norbutas et al., 2020b). A less repressive alternative is the dispute resolution mode where administrators adjudicate between the vendor and the buyers. Most cryptomarkets have in-built verification and validation methods to encourage users to trust the sites, while others rely on community validation over time, as vendors with no complaints can be awarded a verified status (Masson and Bancroft, 2018; Wehinger, 2011).

A key example of a technology that simultaneously promotes and relies on institutional-based trust is the escrow payment system. Using escrow, the seller must provide the products to the buyer, who then allows the escrow agent to release the funds to the seller. Typically, a forum selects a single individual to

serve as an escrow agent, who has a position of trust in the market (Holt et al., 2016). With cryptomarkets, the escrow agent is usually the marketplace administrator. While not all cryptomarkets employ escrow models (Bancroft et al., 2020), they play an important function in building and drawing on trust where they are instated. Using escrow accounts requires that participants trusts that the administrator does not to steal the money. However, because the service includes a fee, a fixed percent for each transaction, some prefer to circumvent it. Vendors may offer a reduced price for trading directly without the escrow and finalising early, which opens numerous ways to defraud buyers (Moeller et al., 2017). Other than the agent absconding with funds, sellers could also falsely claim to use escrow but never actually follow through on the claim. It is an easy signal to fake for untrustworthy actors (Holt et al., 2016). Masson and Bancroft (2018) noted that only the most trustworthy of vendors are able to finalise early. Buyers can also abuse the escrow system by claiming they never received the item, which leads some sellers to require a direct transfer of money from the buyer (Norbutas et al., 2020b).

Administrators set up rules and moderate the forums, signal competence and trustworthiness, and sanction misconduct. In line with the discursive signalling of vendors, an important way for administrators to build institutional-based trust is to communicate with buyers through the forums, especially in times of crisis (Bancroft et al., 2020). They found that administrators communicated mistrust in the sense that they encouraged buyers to always be sceptical (e.g. act as if the forum is already compromised). To these administrators, this mode of thinking signifies a move away from relying on the technologies of escrow and identity verification. Accordingly, these artefacts were primarily used as '(the quote)' (Bancroft et al., 2020, p. 14).

Discussion

Several studies and typologies described in this chapter note that trust is a multidimensional phenomenon. Bancroft et al. (2020) explain this as lateral and vertical forms of trust. Solidarity between users on the forums and a recognition of common interest for all users of the cryptomarket constitute a lateral form of trust, while the reliance on administrators and owners is a vertical relation (Lorenzo-Dus and Di Cristofaro, 2018). The position of trust proposed by Rousseau et al. (1998) as an intermediate concept has some interesting implications for future research in this area. They argue that research on trust should integrate microlevel psychological and economic processes with a sociological analysis of character-based elements and macrolevel institutional arrangements.

From the legal online economy, McKnight and Chervany (2001) explained how trust in a platform over time translates into trust towards individual vendors. Rousseau et al. (1998) similarly noted that institutional factors support a critical mass of trust that encourages further trusting behaviour between actors. This is a top-down perspective on trust formation starting at the institutional level. Specifically for cryptomarkets that operate outside of the support of the legal economy, well-functioning deterrence mechanisms and conscientious administrators that ban scamming vendors are required to attract buyers and vendors and for

process- and character-based trust to develop. Similarly, there is also top-down diffusion of trust from reputation scores to the process-based repeated transactions between the same buyer and seller. Vendors with a better reputation attract more buyers and charge higher prices (Diekmann et al., 2014).

This vertical axis of trust also has a bottom-up facet. Vendors who cheat risk having this malfeasance conveyed to the broader group (Lusthaus, 2012). This effect appears to be relatively rare, as the majority of ratings are for the highest score, and vendors who receive low scores may choose to exit the market and re-enter with a new identity. While this could indicate that the reputation systems as a whole are less than reliable, they nevertheless serve an important function through their transferability. In combination with identity verification technology, the transferability of reputation scores reduces the effectiveness of law enforcement interventions, stabilising the cryptomarket system as a whole (Norbutas et al., 2020b). Following this notion of several cryptomarkets forming a landscape, it is noteworthy that the bottom-up trust towards the institutional arrangement also has a lateral component. While the vertical component consists of trust in anonymising technologies and deterrence mechanisms, the lateral component concerns the assessment of the technical competencies and honesty of individual administrators.

Bancroft et al. (2020) proposed that mistrust could be a guiding concept for understanding how the lateral aspects of trust influence behaviour. In their examination of how the process-based interactions between buyers and vendors combine with the technical infrastructure of the market, they concluded that the shared orientation to security in the specific cryptomarket was more important than the technological infrastructure alone. They referred to this mistrust as a building block for the generation of trust. Sztompka (2006) similarly proposed that mistrust should be given separate attention. Lack of trust does not immediately turn into mistrust, which is the belief that the partner has an interest in cheating. Mistrust stems from the high levels of uncertainty that persist because many vendors, administrators, and law enforcement officials have managed to circumvent these protections (Moeller et al., 2017). This is highly relevant for future cryptomarket research because mistrust shapes all the participants' behaviour and affects their readiness to trust.