Chapter 4
Network Structure and Trust Formation in Cryptomarkets Based on Reputation

Introduction

A significant knowledge gap exists regarding the factors influencing a buyer's choice of vendor within the cryptomarket. The buyer's choice is of particular interest in contexts of information asymmetry, as highlighted by Akerlof (1970). Akerlof (1970) posits that the likelihood of market failure escalates when purchasers encounter difficulties in examining products prior to purchase. The result is the emergence of a market characterised as a "lemon market", in which the absence of accurate and trustworthy information regarding the quality of a product or service being sold leads to a cost being incurred in every transaction conducted within the market (Herley & Florencio, 2010). In addition, given the recognised significance of trust within cryptomarkets, it is reasonable to consider the specific circumstances in which transactions take place. This chapter attempts to address four primary research questions. First, what is the underlying network architecture of Abraxas? Second, how might the structure and composition of the buyers' and vendors' communities on the Abraxas network be described? Third, which market-level metrics and vendor characteristics can be used to predict the trustworthiness of a vendor, specifically in terms of their success (completed transactions), popularity (unique buyers) and affluence (revenue)? Finally, what is the developmental trajectory of vendors' market success, popularity and affluence on Abraxas?

The primary objective of this chapter is to analyse the intricate dynamics of trust within a dark web market. It aims to uncover the mechanisms involved in establishing and sustaining trust and explore the subsequent impact on the market's network structure. A better understanding of these components offers crucial insights for the design of law enforcement interventions.

To illustrate the issue of trust and network formation in a cryptomarket community, Abraxas, a cryptomarket active from 2014 to 2015, is used as the operative example. A conceptual (and often methodological) replication of previous research

V. Harinam, B. Ariel, *Law Enforcement Strategies for Disrupting Cryptomarkets*,
https://doi.org/10.1007/978-3-031-62821-4_4

conducted by Duxbury and Haynie (2017) and Norbutas (2018) is proposed. However, this chapter supplements their approach by looking at market-level indicators that effectively predict the selection of vendors, along with the trajectory of vendor performance over time. As will be shown, these analyses provide a deeper understanding of the influence of trust between buyers and vendors on the configuration of cryptomarkets.

This study applies social network analysis (SNA) to construct and analyse the transactional network, drawing upon the works of Papachristos (2009, 2014) and Duxbury and Haynie (2017). In recent years, a growing body of research has used SNA to gain insights into the operational dynamics of different clandestine networks (Holt et al., 2012; Kenney, 2007; Morselli, 2009; Malm & Bichler, 2011; Natarajan, 2006; Wood, 2017). This literature has shown SNA to be a valuable tool for studying criminal communities such as the cryptomarket environment. (This study will provide information on this analytical approach below. For now, it is simply noted that descriptive network analysis, community detection analysis and statistical and trajectory modelling enable a comprehensive investigation into the trust and network structure development within the Abraxas cryptomarket.) The analyses conducted in this chapter will guide the development and evaluation of simulation models discussed in subsequent chapters.

Trust and Criminal Networks

As shown in the previous chapters, the progress made in digital communication has given unparalleled rise to fresh avenues for criminal activities and deviant behaviour. One particular and fascinating area of tectonic change is how criminals work with other criminals. For example, the issue of proximity between offenders has transformed dramatically, given the nature of computer-facilitated crimes. Those with bad intentions can trade illicit goods and services by evading detection in ways considered impossible just 20 years ago; cybercriminals can exploit technological progress to facilitate collaborative engagement in criminal activities. They can collaborate in ways that no longer require one to assemble in a specific physical setting. They can now build criminal networks and cooperate remotely, adding layers of anonymity and self-protection that challenge law enforcement.

This study wishes to pay close attention to the issue of trust and how it is formed in cryptomarkets. Some level of trust—whether entirely momentary, selective, opportunistic or non-collegial—is required between two or more parties acting together. One must be assured that others will not cheat. One must also avoid dealing with a law enforcement officer, a competitor or someone who does not share a common cause. Therefore, trust remains an integral element of human behaviour, even among criminals. What does trust mean in these circumstances? How is trust affected when people cannot measure the trustworthiness of someone who is perhaps thousands of miles away? What psychosocial and environmental cues are markers of trust between people involved in delinquent acts? How do buyers choose

trustworthy vendors out of the hundreds, if not thousands, of drugs, arms or malicious software dealers on the dark web? How can a vendor perform basic know-your-client (KYC) procedures to ascertain that the buyer is not an undercover law enforcement agent?

Historically, Silk Road was not significantly different from Amazon, as the platform provided the necessary conditions to facilitate trust between vendors and buyers of illegal goods and services. As noted in Chap. 2, cryptomarkets can be understood as brokerage platforms that serve as intermediaries between vendors with the necessary capabilities and buyers willing to engage in transactions. Due to their relative success and ongoing expansion, these platforms replicate legitimate platforms' organisational structure, operational procedures and financial risk management capabilities, like eBay and Amazon. At the same time, cryptomarkets still raise clear concerns for all parties about the participants involved and their interrelationships. The dynamics of these transactional relationships and the subsequent impact on the overall configuration of the criminal network are unclear.

From psychological and sociological perspectives, understanding how the network operates and how trust is formed between parties is crucial. Understanding the network architecture of a cryptomarket can offer valuable insights into its inherent weaknesses. By mapping the cryptomarket and capitalising on the fundamental fact that people are often risk-averse and will do anything to avoid apprehension, there are practical ramifications for law enforcement agencies seeking to impede the operational efficiency of these unlawful entities (Bright et al., 2017).

It was noted earlier how law enforcement attempted to break the trust between buyers and sellers when AlphaBay and Hansa were taken down. Instead of issuing a formal notification that the website was down, the FBI and other agencies were able to disrupt both cryptomarkets and cause confusion and mistrust between the parties involved, who assumed technical difficulties, dishonesty (some buyers thought the vendors had disappeared with their cryptocurrency without delivering the goods) or both. Either way, the motivation was indeed to disrupt the fabric of the relationship between parties that already suffered from limited trust. Yet, as has been documented, this operation did not crack down on the entire ecosystem, which soon bounced back and has been operating since with even more enthusiasm.

The Criminal Underworld and Trust

Chapter 2 introduced the concept of trust in the context of cryptomarkets, but this chapter wishes to delve deeper into this concept, given its weight in network formation—and co-offending more broadly. Trust is crucial as an operational tool within criminal enterprises and associations. However, trusting others who are, by definition, "bad people" by their criminality poses significant challenges. How is one to trust someone that breaks the law? If previous markers of trustworthiness exist—via prior association, family ties, being part of the same organised crime group, etc.—then forming trust can be more straightforward (Baker & Piquero, 2010; Fader,

2016; von Lampe, 2016). Yet in the criminal world, when networks of two (or more) individuals are formed, co-offending is often based on short-term associations (Englefield & Ariel, 2017; Morselli et al., 2011; Sarnecki, 2001). Trust is, therefore, more fickle when offenders try to collaborate.

Trust, or rational reliance on others (Pettit, 2004), is fragile. Multiple factors contribute to its formation. Situational constraints, such as the possibility of harm, arrest or betrayal, frequently motivate criminals to disregard their previously expressed or perceived obligations (Serva et al., 2005). Furthermore, in criminal environments, there is typically a lack of a central governing body that can enforce contractual obligations and penalise those who refuse to comply, as is commonly observed in legitimate contexts (Smith & Papachristos, 2016). While it is true that specific criminal organisations, such as the Italian mafia or the Japanese Yakuza, do exert a degree of governance over the entities under their control, this phenomenon is relatively uncommon within the realm of criminal activity (Gambetta, 2000; Catino, 2014; von Lampe, 2016). However, trust can be viewed as a mechanism of coordination, facilitating collaboration among individuals involved in illicit activities, enabling them to work together towards a shared goal (Free & Murphy, 2015; Jaspers, 2017).

Therefore, trust among criminals is not too dissimilar to how normative networks are formed: Trust pertains to the reliance or confidence placed by individuals or entities in the integrity, credibility and dependability of others involved in criminal activities (Lantz & Ruback, 2017). Yet the definition of trust among offenders does have unique features. Gambetta (2000) suggests that trust can be defined as a specific degree of subjective probability that an individual assigns to the likelihood of another individual or group of individuals carrying out a particular action. This assessment is made before any observation of the action or even in situations where monitoring may not be possible, and it is made within a context that impacts the individual's actions (p. 217). This seems particularly pertinent to us: It appears that in an age when people who commit crimes can "check" with whom they partner before the initial contact with their co-offenders, then the reputation of an individual, their social media presence or how their associates perceive them form the foundation of trust between people. People thus "screen out" certain co-offenders—at least in criminal circumstances that require pre-planning rather than spur-of-a-moment criminal behaviours (Ashton & Bussu, 2022; Weerman, 2003).

Furthermore, trust serves as a mechanism through which individuals can effectively manage and navigate the inherent risks and uncertainties that arise in their interactions with others (von Lampe & Johansen, 2004, p. 103). Trust can be defined as an anticipation of the actions of another agent that is pertinent to the decision-making process (Dumouchel, 2005, p. 421). According to these scholars, trust encompasses the assumption of potential future uncertainty. Therefore, it is incumbent upon the individual to determine the inclinations and preferences of the individuals they aim to interact with to the best of their ability. This entails assessing the potential conduct of their soon-to-be collaborators within a specific scenario. Yet, in these circumstances, trust is less about the ability of the person we wish to trust to perform well (which would be an expectation of a certain level of capability);

instead, placing trust in another individual necessitates a rational evaluation of the likelihood that this person may betray or fail to fulfil their obligation (Gambetta, 1988).

For this reason, it becomes immediately apparent why establishing trust in the criminal realm poses a challenge. The co-offender, like oneself, is an individual with self-interested motives, who must suppress their desires (Williamson, 1993). According to Gambetta and Bacharach (2001), employing a game theory framework, it is evident that the most advantageous result is obtained by cheating (reneging) when a person chooses to cooperate (endow trust). However, repeating this result across multiple iterations would result in an exceptionally negative outcome for the person. Cheating is the most advantageous move in a one-off collaboration, but trust is more cost-effective in repeated games. The continuous display of deceitful behaviour by the individuals in question would serve as a deterrent for the person who trusts them, leading to a loss of potential collaborative efforts and prospects for the party charged with cheating. In this context, trust encompasses the ability to discern whether the individuals with whom one interacts are genuinely committed to collaboration or are merely pretending to cooperate while pursuing alternative objectives. The existing lack of trust is exacerbated by the need to establish a substantial level of trust to sustain enduring criminal partnerships. Therefore, partnerships will exhibit sudden and irregular patterns if trust cannot be consistently upheld.

However, trust is not the only factor in establishing co-offending partnerships. Establishing trust is not necessary in situations characterised by a negative-sum outcome, where both parties face potential losses. Gambetta (2000) asserts that cooperation can "come about independently of trust" (p. 213). In such circumstances, agents will behave based on their shared self-interest, as a failure to do so could potentially lead to the imposition of sanctions on all participating agents. Thus, it is unnecessary for an agent to explicitly place trust in another agent or make assumptions about future risks, as it is evident that the opposing agent is acting in alignment with one's interests. Nevertheless, establishing such a framework relies on two essential components: firstly, the assumption that all individuals possess knowledge of their interests and, secondly, the belief that all individuals can verify that their interests are in harmony with the interests of other individuals. While determining the first element can be relatively straightforward, as it involves identifying one's desired outcomes, establishing the second element can present challenges, as an agent may not always be able to discern the desired outcomes of other agents accurately. Thus, trust is not absent in these specific circumstances but takes on a distinct manifestation. While an agent may harbour doubts regarding the trustworthiness of a potential partner, they can still place reliance on the partner's underlying motivations.

The existing body of research (Gambetta, 2000; von Lampe & Johansen, 2004; Gambetta, 2009) has insisted on the lack of trust within criminal networks of different scales. However, it is essential to note that these findings primarily concern illegal activities occurring in conventional, terrestrial markets. It is reasonable to assert that trust dynamics may vary within cyberspace. Multiple academic studies (Holt & Lampke, 2010) have provided evidence suggesting the existence of market-driven dynamics within illicit online markets. Illegal online exchanges are perceived

and approached as voluntary economic transactions rather than simply illicit transactions. Décary-Hétu and Dupont (2013) conducted a study on a botnet forum. They discovered that trust in a vendor was frequently determined by straightforward indicators, such as the number of awards received, the duration of forum participation and the size of one's network. In this scenario, trust at a superficial level was established based on individual attributes and conduct rather than on shared experiences that foster a profound sense of trust.

Estimating the Role of Trust and Network Structure in Cryptomarkets Through the Concept of Reputation

Trust and Reputation

Although it cannot be denied that duplicity and deception exist on these platforms, van Hout and Bingham (2013a) contend that successful connections among participants in cryptomarkets require trust and professionalism that likely surpass those that characterise terrestrial illicit markets (p. 387). The primary reason for this phenomenon can be attributed to the method of information dissemination within cryptomarkets in the form of product, vendor and transaction reputation. In this regard, vendors openly disclose information regarding the quality of their products and services, while buyers contribute publicly accessible feedback regarding their interactions with these vendors. Therefore, the quality of a product or service and a seller's reliability can be more readily determined in cryptomarkets compared to traditional offline markets.

Establishing vendor reputations depends on the frequency of transactions conducted with buyers, who subsequently evaluate their experiences with individual vendors. The evaluation process relies primarily on a numerical rating system ranging from 0 to 5 stars. Additionally, written feedback is solicited to provide more comprehensive information regarding the transaction. As far as can be determined, it is not within the vendor's capacity to modify the feedback publicly displayed on their cryptomarket page, regardless of whether it is positive or negative. Therefore, much like legitimate online markets, reputations cannot be artificially enhanced by vendors with self-serving intentions, as they are naturally formed through interactions with buyers.

According to Tzanetakis et al. (2016), providing customer feedback within cryptomarkets establishes trust within an environment that inherently lacks trust. The illegal drug trade frequently lacks guarantees regarding the actions and intentions of potential trading counterparts. To a certain degree, a vendor's reputation is considered common knowledge on these platforms, as potential buyers can easily consult it by visiting a vendor's page and reviewing the vendor's overall reputation score, along with the feedback provided by previous buyers.

However, does reputation affect the market and its dynamics? Hardy and Norgaard (2016) employed data on cannabis listings sourced from Silk Road to

examine the correlation between reputation and pricing. Their analysis demonstrates that reputation is an effective mechanism for self-enforcement, thereby facilitating transactions (p. 32). This implies that vendor reputation plays a significant role as a formal institution in establishing a stable trading environment, particularly among individuals who may not be perceived as inherently honest. Similarly, Janetos and Tilly (2017) found that mature cryptomarket vendors who receive high ratings tend to charge prices that are 20% higher compared to mature vendors with low ratings. This means that reputation is directly linked to the product price and can be monetised by "good" market players: Vendors with a more significant number of reviews tend to impose higher prices than sellers with a limited number of reviews, irrespective of their rating.

Batikas and Kretschmer (2018) studied data from the Agora marketplace. They found that sellers with lower rankings tended to leave the market rather than reduce their prices in response to negative feedback. This suggests that vendors in cryptomarkets are more inclined to discontinue their operations in response to negative feedback. Thus, feedback affects not only the price and the volume of transactions but also presence in the market: lLw scores tend to take out unreputable actors.

In their study, Duxbury and Haynie (2017) analysed the network structure of a transactional opioid network on the dark web, focusing on local and global aspects. The study revealed that the transactional network within the cryptomarket exhibited a diffuse and highly localised structure, wherein numerous buyers engaged in transactions with a limited number of vendors. The transactional network comprised multiple subgroups centred around well-established and successful vendors. The localised subgroups exhibited similar sizes. These findings led Duxbury and Haynie (2017) to conclude that the trustworthiness of vendors is more significant in the selection of vendors than product diversity or affordability. That is, buyers tend to engage in repeat transactions with vendors they trust (p. 23).

Felonious Few and Trust

The notion of the "felonious few" is not limited to cryptomarkets but has broader applicability across many networks and systems. The term "felonious few" essentially denotes a limited number of nodes (or players) inside a network that possesses a disproportionately elevated level of influence, connections or relevance compared to their counterparts. This concept resembles the Pareto principle, also known as the 80/20 rule, which posits that 80% of the effects may be attributed to 20% of the causes. Within cryptomarkets, the term "felonious few" may denote a select group of influential vendors, platforms or brokers who exercise control over a substantial number of market operations. It is argued that, to some degree, this concept is directly linked to trust.

Trust is frequently established based on reputation and historical records, particularly in dynamic and possibly hazardous contexts such as cryptomarkets. The limited number of influential participants in cryptomarkets—i.e. the "felonious few"—typically shows their standing through a gradual reputation-building

process. Newly registered users and those who have previously used the platform demonstrate a greater propensity to interact with these established vendors or platforms due to their proven history of successful transactions, positive evaluations and readily available feedback. As the concept of trust encompasses the reduction of uncertainty, alongside reduced search costs, interacting with the powerful few reduces the time and effort users must allocate to ensuring the trustworthiness of vendors or platforms. When a particular group establishes market dominance and maintains a continuous track record, customers tend to trust this group over lesser-known competitors. Consequently, these dominating vendors experience a surge in the reviews, feedback and transactions they receive. Enhanced visibility can improve their reputation, so establishing a feedback loop in which trust attracts a more extensive user base and the increased number of users further reinforces that trust.

Norbutas (2018) provided empirical evidence of this. His study on the Abraxas cryptomarket's transactional network identified low network density: A limited number of vendors were responsible for most transactions. This "power few" feature strongly characterises cryptomarkets more broadly, and it seems to be shaped, at least to some extent, by popularity linked to trust: Reputable vendors attract more clients and more transactions than other vendors. The power few vendors thrive on trust dynamics within the ecosystem: Placing trust in these prominent entities frequently appears to be the more secure option for users, despite the accompanying array of possible hazards.

Localisation and Trust

Directly linked to the issue of trust, Norbutas (2018) noticed that Abraxas' transactional network exhibited a significant degree of localisation, with segmentation occurring primarily along geographical lines: Vendors mainly ship to buyers within the same country. This finding challenges the prevailing notion that cryptomarkets are transnational platforms facilitating transactions among individuals from diverse geographical locations. Instead, cryptomarkets may potentially consolidate domestic trading by confining the circulation of illicit products to within a nation's boundaries.

Thus, buyers frequently prefer local dealers since they perceive them to offer a sense of familiarity, which they associate with decreased risk. This feature of cryptomarkets is linked to the concept of homophily, which suggests that people with comparable characteristics tend to connect and form affiliations more frequently than those with distinctive characteristics (Oksanen et al., 2020; see more broadly in McPherson et al., 2001). The preference for local merchants in cryptomarkets may be attributed to cultural homophily. The thinking is that if vendors and buyers who share a culture, place of living or background have previously engaged in successful transactions with a local vendor, then it is more probable that the buyer will also have a favourable experience. The apparent collective achievement among persons with cultural similarities enhances trust, increasing local businesses' attractiveness within cryptomarkets.

In addition to cultural homophily, practical considerations also influence the dynamics of trust within cryptomarkets. For example, international shipping is perceived as riskier than domestic shipment, due to intricate logistical processes and heightened visibility. The potential for customs checks, seizures or the participation of third-party businesses (Demant et al., 2018) increases the perceived risk for buyers. Transnational consignments depend on global shipping enterprises and are potentially subject to greater legal risks. These issues may prompt participants in cryptomarkets to prioritise local suppliers, perceiving them as more secure and reliable.

The Abraxas Network as a Case Study

In the following sections, the available literature and gathered evidence is used to respond to four overarching inquiries. While each of these questions is relevant to the broader academic debates over cryptomarkets, they will also be of interest to practitioners aiming to dismantle or mitigate the impact of cryptomarkets.

This study relies on data from the Abraxas network, a prominent clandestine online marketplace that could previously be accessed using the TOR network. Like its contemporaries, the platform functioned as a central point of exchange for a wide range of commodities and services, many of which were classified as unlawful or illicit. The offerings included (but were not limited to) drugs, counterfeit cash, fake documents and hacking tools. The life cycle of the Abraxas market exhibited the typical characteristics observed in other darknet platforms throughout the mid-2010s. The operational window of Abraxas was brief. Darknet markets are often ephemeral, either because of law enforcement interventions or internal disintegration.[1] Sufficient data from transactions and ratings of vendors are needed to understand the role of trust in cryptomarket transactions.

Research Questions

The first research inquiry aims to describe the overall framework of Abraxas' transactional network on a global scale. The phenomenon in question has been studied by Duxbury and Haynie (2017) in a different cryptomarket. However, there are gaps in our understanding of the orientation of vendors and buyers within the

[1] Speculation over the occurrence of an Abraxas "exit scam" was as a prominent topic of controversy. Within the clandestine recesses of the darknet, exit scams refer to instances wherein platform administrators abruptly terminate operations and embezzle customers' funds, leaving vendors and buyers in a state of uncertainty and disadvantage. Such scams have been a regular occurrence in darknet markets and have significantly influenced the dynamics of trust within these digital subcultures.

transactional network they are a part of. While it is evident that vendor reputations play a pivotal role in distinguishing vendors of superior quality from those of inferior quality, additional factors seem not to have been thoroughly examined. Additionally, there is a lack of clarity regarding the impact of trust on the overall network architecture of a cryptomarket and the potential implications for interventions. According to Barratt and Aldridge (2016), investigating the network structure of cryptomarkets can offer valuable insights into the concealed transactional dynamics that contribute to the stability of these illicit online marketplaces. If one can better understand these dynamics, it is possible to identify potential opportunities to cause destabilisation.

The second research question aims to gain insight into the attributes and makeup of discernible communities within the context of Abraxas. Duxbury and Haynie (2017) conducted analyses that reveal how users of cryptomarkets tend to form subgroups, wherein individual vendors engage in transactions with multiple buyers. The transactional network within the cryptomarket can be likened to small islands specific to certain products and countries. This characteristic is essential in designing law enforcement interventions with a potential focus on communities rather than individual users. Significantly, there has been no prior research that has applied community detection techniques to analyse a transactional network within a cryptomarket. Therefore, further investigation is necessary in this domain to comprehend its efficacy for professionals. Community detection analysis will facilitate a deeper comprehension of the network topology exhibited by cryptomarkets.

The third research inquiry aims to ascertain the attributes that most effectively forecast the choice of vendor. Although the existing study conducted by Décary-Hétu and Quessy-Doré (2017) provides insights into the popularity of various vendors, it does not explain the underlying reasons for buyers' choices. Gaining insight into buyers' decision-making process when selecting vendors is of utmost importance in comprehending the formation of the network structure within a cryptomarket. The central focus of this inquiry is the concept of trust. More specifically, the objective is to quantify the market-level metrics that serve as predictors for vendor selection across three proxy variables associated with trust. Gaining a comprehensive understanding of the nature and significance of these metrics and their operational implications can potentially enhance the effectiveness of law enforcement interventions. Furthermore, law enforcement must comprehend the significance of trust in cryptomarkets, as well as the factors that may undermine it.

According to Gambetta (2000), trust is operationalised in this chapter as "a specific degree of the subjective likelihood that an individual evaluates regarding the performance of a specific action by another individual or a collective of individuals" (p. 29). Therefore, the suggested metrics at the market level can be utilised as indicators or game-theoretic tools for buyers to evaluate the likelihood of a vendor fulfilling their obligations in a predetermined transactional agreement. A total of 14 predictors that span three distinct conceptualisations of vendor trustworthiness are employed. This endeavour can be considered the most comprehensive undertaking thus far.

The objective of the fourth research inquiry is to examine the developmental trajectory of vendors in cryptomarkets, focusing on whether vendors who are deemed most trustworthy continue to thrive as the market experiences growth. The level of continuity and potential growth or decline of vendors operating on these platforms is not thoroughly comprehended by practitioners in this field. This inquiry provides valuable insights into the reciprocal relationship between market and vendor growth. Suppose a scenario exists where a limited number of reputable vendors are responsible for most transactions in a cryptomarket. In this case, it can be inferred that the market's sustained functioning and expansion depend on the efficacy of a central group of vendors. For professionals in the field, understanding the developmental paths of individual vendors is essential in mitigating the impact of these actors and the overall expansion of the market. Law enforcement agencies can employ trajectory models to identify and mitigate potential threats within cryptomarkets.

Methods

Data

In this study, a dataset obtained from the Abraxas cryptomarket is utilised, as documented by Branwen et al. (2015). Other than the anonymous cryptomarket examined by Duxbury and Haynie (2017, 2019), this marketplace is the sole platform where distinctive identifiers are accessible to purchasers. Significantly, Norbutas (2018) employed Abraxas in a study investigating the spatial dispersion of transactions. To fulfil the objectives of this study, a bipartite buyer–seller trade network was built. This network encompasses a total of 5434 transactions involving illicit goods and services. The transactions occurred between 269 distinct sellers and 2794 unique buyers over 7 months, specifically from 2014 to 2015.

According to Norbutas (2018, p. 93), the dataset compiled by the independent researchers Branwen et al. (2015) encompasses data from various cryptomarkets and is acknowledged to have limitations in terms of its comprehensiveness. To clarify, it is possible that the Abraxas marketplace was not comprehensively captured during the routine data extraction processes conducted by Branwen et al. in 2015. Norbutas (2018) compared the number of crawled item pages in the data and the observed number of items presented on Abraxas' home page at various dates. The analysis revealed evident inconsistencies. More broadly, Norbutas (2018) noted that the mean proportion of retrieved items in Branwen's crawls was 92.4%, though it ranged from 26% to 100% depending on the specific crawl (p. 93). Moreover, a significant number of scraped webpages were found to be nonfunctional, resulting in incomplete documentation of market transactions. This limitation is evident as the analysis was restricted to a subset of the Abraxas cryptomarket. To a certain

degree, it can be argued that this transactional network lacks completeness, as not all transactions were documented or recorded. Using Norbutas' (2018) methodology, data from multiple daily crawls of item pages were compiled. Consequently, duplicate transactions were identified and removed. The resulting dataset comprises 269 distinct sellers, 2794 distinct buyers and 5434 transactions.

To establish a two-mode transactional network comprising exchanges between individual buyers and sellers, it was necessary to assign each feedback message to a specific buyer. In a broad sense, feedback functions as tangible evidence that a transaction has occurred. According to Martin (2014), customer feedback encompasses a diverse range of expressions, including elaborate remarks regarding the duration of shipping, discreet packaging methods, the perceived effectiveness of illegal substances and a straightforward rating system using five stars (p. 41). It is worth noting that although all cryptomarkets rely on a feedback system, there may be variations in their policies regarding the obligatory nature of buyer feedback. Certain cryptomarkets require buyers to provide feedback following each transaction, whereas others do not impose such a requirement. Abraxas belongs to the former category: All transactions carried out during the market's operational period were meticulously recorded through buyer feedback.

The presence of feedback data in network-based cryptomarket datasets is typically challenging because of partially or fully anonymised buyer usernames. However, Abraxas included distinct buyer profile identifiers for each feedback message. These identifiers were found within the HTML code of item pages. The buyer identifiers were used to consolidate the feedback messages provided by individual buyer accounts. After eliminating duplicate entries, a two-mode transactional network was built for vendors and buyers on Abraxas from 15 January 2015 to 4 July 2015.

Although these analyses successfully identified the purchases made by individual buyer accounts, the dataset lacked information regarding the buyers' country of residence. While direct observation of buyers' geographic location was not possible, making inferences about the clustering of buyers in the marketplace by analysing their choice of vendors located in specific countries was possible. The transactions were systematically classified into different categories to facilitate analysis. The categorisation system consisted of a broad category encompassing all types of items, a subcategory that divided the items into more specific categories and a secondary subcategory that offered more detailed information about each item. Every individual item was manually coded. Regarding pricing, all transactions were converted from Bitcoin to USD using a dynamic exchange rate from the United States. Although this approach may potentially yield less precise pricing information due to the inherent volatility of cryptocurrencies, it also leads to alterations in the listed prices. Implementing a stable exchange rate rather than a fluctuating one would inadequately reflect fluctuations in listed prices.

Statistical Analyses

Descriptive statistics were employed to provide a concise and accessible summary of the 5434 transactions. The aim of this summary was to provide a comprehensive understanding of the characteristics and constituents of illegal transactions occurring on the Abraxas platform. Descriptive statistics, as a whole, offer a simple, transparent and comprehensive means of viewing the data. Social network analysis was performed to investigate Abraxas' network structure. Four distinct analytical approaches are utilised: descriptive network analysis, community detection analysis, statistical modelling and trajectory modelling. The network statistics, modelling and visualisations were performed using R and Microsoft Excel software programmes.

Descriptive Network Analysis

The network structure of Abraxas is summarised at a preliminary level using standard network measures based on social network analysis. It is of utmost significance to ascertain the existence of a connection between two actors by examining whether feedback has been provided following a transaction. The existence of feedback serves as tangible proof that a transaction has taken place. Bichler et al. (2017) have argued that researchers must elucidate the methodology employed in constructing the networks utilised for social network analysis. A network comprising vendors and buyers was created based on the 5434 illicit transactions. The network was built using only transactions involving a known vendor and a buyer. Vendors were identified by their distinct vendor names, whereas the identification of buyers was accomplished using their HTML code. The transactional network comprised 5434 transactions involving 269 distinct vendors and 2794 distinct buyers. A correlation can be established between acting professionals if they have participated in a joint transaction (McGloin & Kirk, 2011).

Network Analysis

In this study, four network measures were employed: network density, in-degree centralisation, out-degree centralisation and eccentricity. The concept of density was used to quantify the level of interconnectedness within a network. To clarify, this metric calculates the ratio of the actual number of connections between actors to the maximum potential number of connections that could exist. The measurement is represented by a coefficient between 0 and 1. In the context of this dataset, a score close to 1 signifies a high level of buyer engagement with multiple vendors, reflecting the extensive interconnections within the network. On the contrary, density scores closer to 0 suggest that buyers engage in transactions with a limited number of vendors, resulting in a dispersed network.

According to Duxbury and Haynie (2017), centralisation refers to the extent to which a few actors possess significant control over the overall network structure (p. 23). In this study, the concept of centralisation is used to represent the extent to which vendors (out-degree centralisation) or buyers (in-degree centralisation) exert influence over the network structure of the Abraxas transactional network. Centralisation was calculated using the degree of centrality of each node. According to Duxbury and Haynie (2018), the calculation determines the total disparities between the actor with the highest centrality score and all other actors within the network. This total is then divided by the maximum possible number of disparities obtained from a hypothetical matrix of equivalent dimensions (p. 929). The outcome of this calculation yields a numerical value that falls within the range of 0 to 1. A higher value on this scale signifies a stronger indication of central tendency within a network, as described by Wasserman and Faust in 1994. In network analysis, eccentricity is a metric that quantifies the maximum distance between a given node and any other node within the network. The eccentricity of a node in a connected network is defined as the maximum distance between that particular node and all other nodes in the network.

Each of these measurements was chosen to assess the interconnectedness of Abraxas' global network structure and the significance of individual nodes within the network. Alternative measurements, such as closeness and betweenness centrality, could have been used in this analysis. However, these measurements would not have yielded meaningful insights due to the rigid categorisation of nodes as either buyers or vendors.

Community Detection

Although standard network measures offer valuable information about the overall characteristics of a network, they have limited ability to reveal the underlying structural features of the network. However, this objective can be accomplished by employing community detection analysis. According to Yang et al. (2013), community detection identifies groups of interconnected vertices, also known as nodes, within a network based on their structural characteristics (p. 15). In brief, community detection algorithms aim to partition nodes into separate communities by considering the extent of their connections with other nodes within the network. While there may be occasional deviations, networks typically comprise individuals who interact more frequently with certain individuals than with others.

In this study, the Walktrap community detection algorithm is used (Pons & Latapy, 2005; Newman, 2003, 2006) to ascertain the subgroup configuration of the Abraxas transactional network. According to Pons and Latapy (2005), the Walktrap algorithm detects various potential community structures by employing a random sequence of walks. According to the source, the graph is divided into distinct communities at each stage, with the merging of communities occurring when the distance between them is deemed sufficiently small (p. 6). The Walktrap method is well suited for analysing extensive, directed networks like the Abraxas network.

The metric Q, the modularity score, was employed to assess the degree of congruence between the communities generated by the Walktrap community detection algorithm. A community is commonly defined as a group of nodes within a network that exhibit stronger connections among themselves than with other nodes. Modularity is a statistical measure that accounts for chance, with values ranging from −0.5 to 1. According to Blondel et al. (2008, p. 43), the term "modularity" refers to the difference between the actual proportion of connections within specific groups and the expected proportion of randomly distributed connections.

The calculation of modularity is defined as:

$$Q = \Sigma\left(e_{bd} - a_b^2\right)$$

According to Duxbury and Haynie (2018, p. 930), the variable "e" represents the proportion of ties that connect community b and community d, while the variable "a" represents the proportion of ties that are connected to community b. A network's level of segmentation increases as its modularity score increases. Values exceeding 0.3 are indicative of a substantial community structure.

Model Estimation

To address the third research question, three regression models were formulated. In all models, identical explanatory and control variables were employed, except for one variable. In the evaluated model that assessed cumulative revenue generated, the inclusion of cumulative purchase price as an explanatory variable was not considered due to its role as the dependent variable.

Estimating Trustworthiness

To assess the trustworthiness of vendors, three proxy variables were generated: success, popularity and affluence. The various manifestations of trust are reflected in these dependent variables, each representing a crucial aspect of trust. Success was defined in this context as the total number of transactions conducted by a vendor, explicitly referring to the number of sales made. The quantity of sales generated by a vendor serves as an indicator of the enduring quality of their service provision. Trust is established and sustained through the consistent display of professionalism by both the truster and the trustee, as noted by Gambetta (2009) and Przepiorka et al. (2017). Consequently, it can be inferred that vendors who generate higher sales volumes, including both new and repeat customers, are perceived as more trustworthy by buyers who have made an initial purchase and are likely to engage in future transactions. The operationalisation of popularity in this study was defined as the cumulative count of distinct purchasers with whom a vendor has engaged in business transactions. The number of distinct clients in a vendor's client list is a

more comprehensive and widespread manifestation of trust. Affluence in this context referred to the vendor's total profit during their period of activity on the Abraxas platform. The sum of the purchase price, denominated in USD, for every transaction a vendor effectively executed was calculated. In this context, trust is represented by the financial benefits esteemed vendors stand to gain from the confidence buyers place in their services. Collectively, these dependent variables provide three distinct yet interconnected indicators for trust. Furthermore, the use of three regression models allowed us to carry out a comparative analysis of the effectiveness of each explanatory variable in accounting for the variability observed in vendor trustworthiness.

Fourteen explanatory variables were formulated and are presented in Table 4.1. Each of the concepts discussed in the scholarly literature on cryptomarket vendors is characterised by a quantifiable attribute (Christin, 2013; Décary-Hétu, 2016; Przepiorka et al., 2017; Norbutas et al., 2020). The explanatory variables can be categorised into six distinct concepts: reputation, affordability, product diversity, openness, risk-taking and accessibility. Each of these concepts contributes, to varying degrees, to the understanding of vendor favourability.

The initial explanatory variable is a cumulative reputation score. Based on the research by Décary-Hétu and Quessy-Doré (2017), the cumulative reputation score is determined by aggregating the ratings assigned to all documented transactions a vendor has successfully carried out. Affordability pertains to the degree of expense associated with a particular vendor. Similar to sellers in legitimate markets, vendors in cryptomarkets must establish prices that are deemed reasonable to incentivise

Table 4.1 Descriptive statistics of variables used in analysis

Variable name	Mean or total	SD	Median	Range
Dependent variables				
Number of transactions	20.2	38.95	7	1–330
Number of unique buyers	14.64	23.24	6	1–179
Cumulative revenue generated	2210.10	5931.95	473.25	0.23–68812.96
Reputation, price and risk				
Cumulative reputation	98.76	191.46	35	0–1628
Average purchase price	105.33	165.72	66.98	0.23–2025.04
Cumulative risk score	42.9	92.41	11	1–929
Items and information				
Unique item listings	5.49	7.42	3	1–58
Unique item categories	1.1	0.46	1	1–5
Unique item subcategories	1.12	0.38	1	1–4
Number of words in item description	2773	7468.18	592	0–73,267
Location shipped from				
Domestic only	1700 (31.3%)	–	–	–
Regional/continental	893 (16.4%)	–	–	–
Worldwide	2374 (43.7%)	–	–	–
Unknown	467 (8.6%)	–	–	–

potential buyers to engage in transactions with them. The concept of affordability was measured by employing two variables: cumulative purchase price and average purchase price. The cumulative purchase price was determined by aggregating the purchase prices of all transactions conducted by a vendor. The average purchase price refers to the mean price at which a vendor sells a product.

Product diversity is a measure of the range of distinct items a vendor provides to customers. The explanatory variable in question implicitly compares the profitability of focusing on a specific product with the profitability of diversifying across multiple products. The understanding of the impact of specialisation and diversification on vendor trustworthiness remains incomplete. Three variables were used to operationalise the concept of product diversity: the number of distinct product listings, the number of product categories and the number of product subcategories. The calculation of each variable involved the aggregate of distinct items or item categories within the respective categories. As proposed by Akerlof (1970), the notion of information asymmetry is mirrored in the concept of openness, which refers to the degree to which vendors divulge product information in a listing. Within each listing, there was a dedicated section for further information about the product being offered for sale. The operationalisation of openness was therefore achieved using a cumulative word count. This metric represents the quantity of words supplied by the seller in the description segment of the listing. The total number of words was determined by aggregating the word count for each transaction completed by a vendor.

The act of shipping goods across international borders is commonly perceived as a hazardous endeavour due to the heightened likelihood of detection, particularly in the case of drug trafficking. Branwen et al.'s (2015) study showed that most cryptomarket vendors arrested (precisely 62%) were apprehended due to their involvement in international shipments. This finding was based on data collected as of May 2015. Therefore, a vendor's readiness to ship internationally can be seen as an indicator of risk-taking. The operationalisation of risk-taking was achieved by utilising a cumulative risk score. A risk score was assigned to each transaction based on the shipping locations specified by the vendor. To minimise the number of control variables, the shipping locations were initially consolidated and represented by four dummy variables, which were used to indicate the distinct shipping categories. Subsequently, risk scores were assigned to each category as follows: unknown or N/A denoted missing data, domestic only was assigned a score of 1 to indicate low risk, continental/regional was assigned a score of 2 to indicate medium risk and worldwide was assigned a score of 3 to indicate high risk. The cumulative risk score was determined by aggregating the risk scores associated with each transaction conducted by a vendor.

The final explanatory factor, accessibility, is closely associated with risk propensity regarding the geographical areas where vendors are willing to deliver their products. The broader the range of shipping destinations a vendor is ready to accommodate, the greater the dilution of exclusivity and the enhanced accessibility of their services to a broader clientele. In contrast to the concept of risk-taking, the variable representing the locations to which items are shipped is categorical. However,

similar to risk-taking, the shipping locations were grouped into four dummy variables to accommodate the various shipping categories. The categories encompassed in this classification were domestic only, continental/regional, worldwide with exceptions and worldwide. Significantly, the reference category was established as domestic only.

Trajectory Modelling

In this study, k-means longitudinal modelling was used to ascertain the developmental trajectory of active vendors on the Abraxas platform. Group-based trajectory modelling (GBTM) is a statistical technique introduced by Nagin and Land (1993) to identify distinct subgroups within longitudinal data by examining homogeneous trajectories. Similarly, k-means longitudinal analysis also seeks to identify homogeneous trajectories by grouping data into subgroups. The k-means algorithm, a hill-climbing algorithm, is classified within the expectation–maximisation class. According to Genolini and Falissard (2010), the algorithm initially assigns data points to a particular cluster and then iteratively recalculates each cluster to ensure that each data point is moved closer to the cluster that it most accurately belongs to. The concept of "expectation" entails the identification of the centroid of each cluster, while "maximisation" involves allocating each observation to the closest proximity cluster. The two phases mentioned above are iterated until the clusters reach a state where no additional modifications occur.

The trajectory models were developed using the KmL package in the R programming language, as described by Genolini et al. (2016). Significantly, to address the challenge of determining the precise number of clusters (or trajectories) in advance, and so facilitate the grouping of the data, the Calinski–Harabasz Index was used to ascertain the most suitable number of trajectory groups for each proxy variable, based solely on the clustering results. Andresen et al. (2017) assert that the Calinski–Harabasz Index criterion is a relative metric for comparing various group solutions (p. 434). A trajectory model was developed for each proxy variable mentioned above, representing vendor trustworthiness. These variables included success (measured by completed transactions), popularity (measured by unique buyers) and affluence (measured by revenue).

Results

Descriptive Statistics

Table 4.2 provides a comprehensive set of descriptive statistics about the Abraxas marketplace. When considering the prevalence of drugs, Abraxas exhibits similarities to other cryptomarkets, such as Silk Road 1 (Aldridge & Décary-Hétu, 2016;

Table 4.2 Descriptive statistics on the Abraxas cryptomarket

Descriptive statistics	Mean (SD) or total	Range
Vendor reputation		
Cumulative reputation	98.76 (191.46)	0–1628
Average reputation	4.85 (0.54)	0–5
Cumulative positive reputation	97.43 (189.7)	0–1625
Cumulative negative reputation	1.327 (4.67)	0–59
Ratings		
0	1.4% (74)	–
1	0.4% (23)	–
2	0.2% (10)	–
3	0.5% (26)	–
4	1.1% (59)	–
5	96.5% (5242)	–
Listing categories		
Drugs	92.9% (5050)	–
Digital goods	5.9% (321)	–
Services	0.4% (21)	–
Drug paraphernalia	0.3% (17)	–
Others	0.3% (14)	–
Custom listing	0.2% (11)	–
Listing subcategories		
Cannabis	34.21% (1859)	–
Stimulants	19.38% (1053)	–
Ecstasy	13.8% (750)	–
Opioids	10.8% (587)	–
Psychedelics	6.75% (367)	–
Benzos	3.7% (201)	–
N/A	2.72% (148)	–
Prescription	2.19% (119)	–
Dissociatives	1.25% (68)	–
Information	1.03% (56)	–
E-books	0.98% (53)	–
Erotica	0.9% (49)	–
Fraud	0.59% (32)	–
Steroids	0.35% (19)	–
RCs	0.22% (12)	–
Data	0.2% (11)	–
Drugs (cyber)	0.17% (9)	–
Hacking	0.15% (8)	–
Money	0.11% (6)	–
Weapons	0.11% (6)	–
Electronics	0.09% (5)	–
IDs and passports	0.07% (4)	–

(continued)

Table 4.2 (continued)

Descriptive statistics	Mean (SD) or total	Range
Others	0.06% (3)	–
Software	0.06% (3)	–
Miscellaneous	0.04% (2)	–
Security	0.04% (2)	–
Drug paraphernalia	0.02% (1)	–
Services	0.02% (1)	–
Purchase price (in USD)		
All purchases	109.41 (173.51)	0.23–2800.03
<$1	2.2% (121)	–
$1–$4.99	3.3% (178)	–
$5–$9.99	3.1% (168)	–
$10–$19.99	8.7% (472)	–
$20–$49.99	24.7% (1344)	–
$50–$99.99	28.2% (1532)	–
$100–$199.99	16.3% (884)	–
$200–$499.99	10.8% (589)	–
$500–$999.99	1.9% (201)	–
>$1000	0.8% (44)	–
Locations shipped from		
Australia	8.74% (475)	–
Belgium	0.83% (45)	–
Belize	0.02% (1)	–
Bulgaria	0.64% (35)	–
Canada	0.61% (33)	–
China	0.02% (1)	–
Colombia	0.02% (1)	–
Czech Republic	0.09% (5)	–
Denmark	0.81% (44)	–
Europe/EU	7.19% (391)	–
France	0.74% (40)	–
Germany	25.10% (1364)	–
Hungary	0.06% (3)	–
India	0.18% (10)	–
Italy	0.99% (54)	–
Mexico	0.02% (1)	–
Netherlands	9.22% (501)	–
Norway	0.29% (16)	–
Poland	0.11% (6)	–
South Africa	0.2% (11)	–
Spain	2.37% (129)	–
Switzerland	0.39% (21)	–
UK	13.78% (749)	–

(continued)

Table 4.2 (continued)

Descriptive statistics	Mean (SD) or total	Range
United States	19.34% (1051)	–
Unknown or N/A	8.23% (447)	–
Locations shipped to		
Australia	8.19% (445)	–
Europe	15.73% (855)	–
Europe and United States	0.07% (4)	–
Europe except Italy	0.18% (10)	–
Europe except United Kingdom	0.48% (26)	–
Germany	1.23% (67)	–
Switzerland	0.13% (7)	–
United Kingdom	4.42% (240)	–
United States	17.32% (941)	–
United States and Canada	0.04% (2)	–
Worldwide	36.53% (1985)	–
Worldwide with exceptions	7.16% (389)	–
Unknown or N/A	8.60% (463)	–

Christin, 2013) and Agora (Van Buskirk et al., 2016). Among the various categories of listings, 92.9% (5050) involve drug-related products. In comparison, digital goods account for only 5.9% (321) of the total products sold. A more detailed analysis of the various categories reveals that cannabis comprises the most significant proportion (34.21%), followed by stimulants (19.38%), ecstasy (13.8%), opioids (10.8%) and psychedelics (6.75%). These five categories collectively represent the most prominent products in terms of sales. The pattern above is evident, too, in the monetary value of transactions involving the various substances: Cannabis accounts for $198,745.16, stimulants for $149,078.46, ecstasy for $95,949.28, opioids for $94,480.70 and psychedelics for $19,952.46. In total, the monetary value of transactions in the cryptomarket under investigation amounted to $594,517.50 during the designated research period. Compared to well-established platforms, such as Silk Road 1, Evolution, AlphaBay, Hansa and Wall Street, the total value of transactions in this particular cryptomarket can be considered relatively modest.

In terms of pricing, it is observed that 28.2%, 24.7% and 16.3% of the products were sold at price points falling within the intervals of $50–99.99, $20–49.99 and $100–199.99, respectively. This finding implies that purchasers of Abraxas products generally did not allocate a disproportionately high sum of money towards their purchases. On the contrary, most of the items acquired were moderately priced. However, there were a total of 44 transactions that surpassed the threshold of $1000. Following the trend mentioned earlier, these particular acquisitions involved cannabis (18), opioids (11), ecstasy (8) and stimulants (7). In the context of transaction ratings, the mean rating observed was 4.85, with a substantial majority of transactions (96.5%) receiving a rating of 5. This observation suggests that a significant proportion of purchasers express a high level of satisfaction with the services

provided by vendors. However, it is crucial to consider the possibility that the Abraxas rating system may be influenced by the Pollyanna principle, which suggests a tendency towards a positive bias. The top five shipping nations, in terms of origin of the goods shipped, are Germany, the United States, the United Kingdom, the Netherlands and Australia. These countries account for 25.1%, 19.34%, 13.78%, 9.22% and 8.74% of the total number of shipments made, respectively. In addition, it is worth noting that the global distribution of shipped locations was as follows: the world accounted for 36.52%, the United States for 17.32% and Europe for 17.73%. Significantly, this showcases the vendors' inclination to ship without discrimination to all destinations.

Network Structure of Abraxas, Interconnectedness and Organisational Framework

The Abraxas transactional network consists of a total of 2794 distinct actors who are involved in 5434 transactions. Among these actors, there are 269 unique vendors and 2525 unique buyers. In addition, a total of 3935 distinct dyadic pairings exist. Moreover, it is worth noting that the network does not contain any isolates as every buyer is connected to at least one vendor. Importantly, the inability to match unique URL tags for buyers with unique vendor IDs prevented the identification of buyers who also operated as vendors. Due to this constraint, the computation of reciprocity or transitivity metrics was impossible. The network composition and characteristics are presented in Fig. 4.1 and Table 4.3, respectively.

The Abraxas transactional network exhibits low network density, precisely measured at 0.0007. Therefore, a mere 0.07% of the total potential transactions took place. In a comparative analysis, the study conducted by Duxbury and Haynie (2018) revealed that the cryptomarket transactional network for opioid distribution exhibited a density of 0.002. The complete network comprises 29 components. It is worth noting that one specific component contains the majority of nodes within the network, accounting for 97.6% (2726) of the total nodes. This information can be found in Table 4.4. The remaining connected components comprised 19 dyads, seven triads and individual assortments of components of varying sizes. This study's findings indicate that buyers consistently purchase from a limited number of vendors. This behaviour gives rise to a substantial cluster of users with sparse connections, with only a few isolated cliques of buyers and sellers. In the Abraxas transactional network context, nodes exhibit an average maximum distance of 11.23 units from each other, as determined by the eccentricity measurement. Similar mean values can also be observed for vendors (10.32) and buyers (11.33).

Due to the limited network density observed in Abraxas, buyers exhibited a tendency to restrict their interactions to a select few vendors, relying primarily on those they deemed trustworthy or with whom they had established a sense of comfort. According to the data presented in Table 4.5, it is evident that a significant

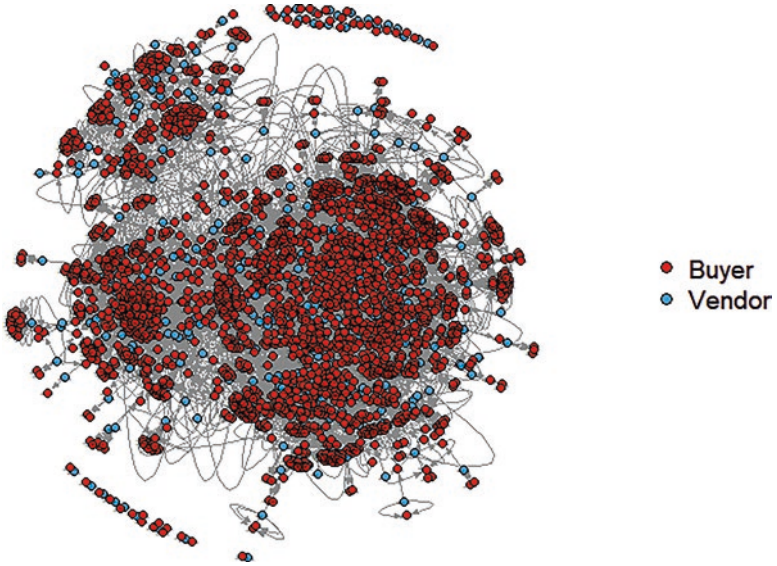

Fig. 4.1 Abraxas transactional network

Table 4.3 Network characteristic

Network characteristics	Mean (SD) or total	Range
Unique actors/nodes	2794	–
Unique vendors	269	–
Unique buyers	2525	–
Isolates	0	–
Total unique edges	3935	–
Density	0.0007	–
In-degree	2.15 (2.2)	1–34
Out-degree	20.2 (39)	1–330
In-degree centralisation	0.01	–
Out-degree centralisation	0.12	–
Eccentricity (All)	11.23 (1.9)	1–16
Eccentricity (vendors)	10.32 (3.38)	1–15
Eccentricity (buyers)	11.33 (1.64)	1–16

proportion of buyers, specifically 34.1% or 860 individuals, made purchases exclusively from two vendors. Indeed, most buyers (67.5% or 1702 individuals) purchased solely from a single vendor. It is clear that purchasers exhibit a preference for engaging in transactions with a limited number of suppliers rather than a diverse range of options. This preference results in a market imbalance characterised by a concentration of transactions among a limited number of vendors. This information can also be inferred from the out- and in-degree centrality measures. On average, buyers engaged in transactions with 2.15 vendors, whereas vendors had an average

Table 4.4 Distribution of network components

Component size	Frequency	Percentage (%)	Node total	Percentage (%)
2	19	66	38	1.4
3	7	24	21	0.8
4	1	3	4	0.1
5	1	3	5	0.2
1000+	1	3	2726	97.6
Total	**29**	**100**	**2794**	**100**

Table 4.5 Frequency of unique vendors purchased from by number of transactions

Transactions per buyer													
Unique vendors purchased from		**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10–14**	**15–19**	**20+**	**Total**
	1	1350	249	59	18	15	3	1	3	0	3	1	0	**1702**
	2	0	313	107	45	15	11	7	2	3	5	0	0	**508**
	3	0	0	79	50	17	11	5	4	2	3	0	0	**171**
	4	0	0	0	36	21	7	11	0	4	3	0	0	**82**
	5	0	0	0	0	9	5	5	3	3	5	0	0	**30**
	6	0	0	0	0	0	3	7	4	3	0	1	3	**21**
	7	0	0	0	0	0	0	0	1	0	0	1	1	**3**
	8	0	0	0	0	0	0	0	0	1	0	1	0	**2**
	9	0	0	0	0	0	0	0	0	0	3	0	0	**3**
	10	0	0	0	0	0	0	0	0	0	1	0	1	**2**
	11+	0	0	0	0	0	0	0	0	0	0	0	1	**1**
	Total	**1350**	**562**	**245**	**149**	**77**	**40**	**36**	**17**	**16**	**23**	**4**	**6**	**2525**

of 20.2 buyers (refer to Table 4.6). As mentioned earlier, the findings are consistent with the research conducted by Duxbury and Haynie (2017) and Norbutas (2018).

A more precise representation of the distribution of in- and out-degree centrality can be observed in Table 4.6. A significant proportion of purchasers (53.47%) engaged in transactions exclusively with a single vendor. In the context of Abraxas, it is essential to note that transactions typically involve multiple participants, with 19 dyads being observed. However, it is commonly observed that buyers tend to exhibit a preference for engaging with a single vendor. Furthermore, a notable percentage of buyers, precisely 22.6%, have been involved in transactions with two distinct vendors. The lack of selectivity observed among vendors, with 84.4% having multiple buyers, is comprehensible. Undoubtedly, vendors engage in transactions with a diverse range of buyers.

The out-degree centralisation of Abraxas is 0.12. Once more, this observation serves as evidence that a significant proportion of purchasers tended to engage in transactions with a limited selection of highly influential suppliers. However, specific buyers exhibited higher enthusiasm in their purchasing behaviours than others. In contrast to the average buyer who purchased from only two vendors, the most enthusiastic buyers engaged in transactions with a significantly higher number of vendors, ranging from 1 to 34. Many buyers exhibited infrequent purchasing

Table 4.6 Distribution of in- and out-degree

Degree centrality	Out-degree total (vendor) (%)	In-degree total (buyer) (%)
1	42 (15.6)	1350 (53.47)
2	30 (11.2)	562 (22.26)
3	21 (7.8)	245 (9.7)
4	19 (7.1)	149 (5.9)
5	8 (3)	77 (3.05)
6	11 (4.1)	40 (1.58)
7	7 (2.6)	36 (1.43)
8	10 (3.7)	17 (0.67)
9	7 (2.6)	16 (0.63)
10–14	27 (10)	23 (0.91)
15–19	18 (6.7)	4 (0.16)
20–29	15 (5.6)	5 (0.2)
30–49	25 (9.3)	1 (0.04)
50–99	22 (8.2)	–
100+	7 (2.6)	–
Total	**269 (100)**	**2525 (100)**

behaviour as the in-degree centralisation of Abraxas was 0.001. Determining the underlying factors driving a buyer's purchasing pattern is a complex task due to the many potential reasons that may influence the decision-making process. These buyers may have transitioned to an alternative cryptomarket or ceased their activities on the dark web entirely due to the inherent risks involved.

Notably, although a minority of vendors were responsible for the majority of sales, the vendors beyond this dominant group encountered challenges in sustaining their livelihoods on Abraxas. As mentioned earlier, the phenomenon can potentially be ascribed to the influence of trust and reputation. Vendors possessing superior reputations consistently generate sales, thereby intensifying the obstacles new vendors face when entering the market. A vendor's average cumulative reputation score is 98.76, with a standard deviation of 191.46. The observed scores exhibited a wide range from 0 to 1628. Vendors with a strong reputation tend to attract more buyers as they leverage their established track record of reliable service as a significant factor in their sales strategy. This information can be inferred from the results of the community detection analysis below.

Community Detection Analysis

Community detection analysis allows us to identify significant attributes that help improve our understanding of the fundamental organisation of the Abraxas transactional network. Abraxas exhibited a total of 158 distinct communities established based on the preferences of the most prominent vendors (see Fig. 4.2). Furthermore,

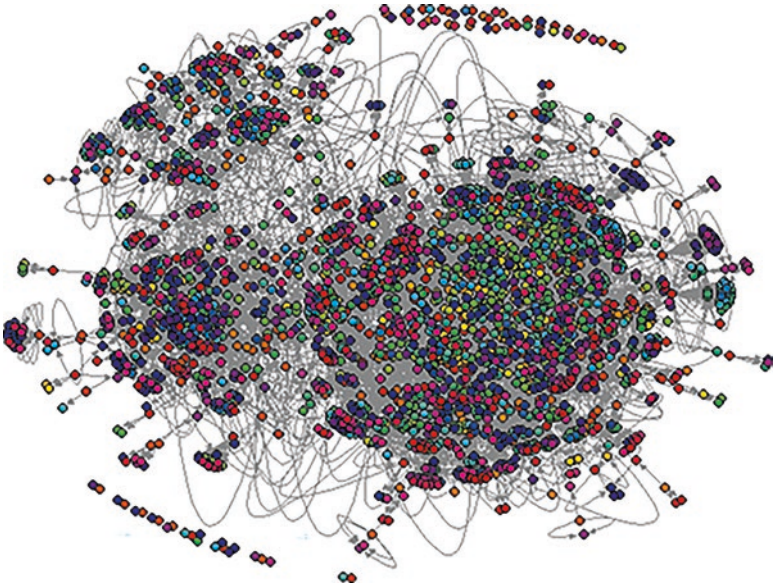

Fig. 4.2 Abraxas transactional network by community

Table 4.7 Community network characteristics

Network characteristics	Mean (SD)	Range
Community size	17.7 (44.7)	2–390
Community density	0.26 (0.19)	0.01–1
Edges	26.96 (85.81)	1–810
Within community transactions	34.39 (103.03)	1–921
Average cumulative vendor reputation	66.09 (87.97)	1–550
Avg. outdeg (vendor)	10.33 (12.72)	1–85
Avg. indeg (buyer)	1.29 (0.31)	1–2.17
Number of vendors	1.7 (2.87)	1–29
Number of buyers	15.98 (42.03)	1–373

the community detection analysis yielded a modularity score of 0.72, indicating a relatively high Q value. This observation suggests that the network exhibited significant segmentation, with numerous distinct communities. The largest community comprised 390 members, while the smallest 111 communities had less than ten members each (refer to Table 4.7). In this regard, it is noteworthy that 35 communities were classified as dyads, consisting of two members, while 20 communities were categorised as triads, comprising three members. The top 20 communities were responsible for a significant portion of activity in the market, accounting for 63% (1763) of the total number of actors and 71.9% (3909) of the transactions. Furthermore, it is worth noting that the typical community exhibited an average of 1.7 vendors and 15.98 buyers. To clarify, it can be stated that each vendor, along with their corresponding buyers, formed distinct communities.

In terms of community composition, communities with larger membership exhibited higher average vendor reputation scores, as depicted in Table 4.8. These communities also revealed the highest concentration of vendors. Most transactions conducted on Abraxas can be attributed to these communities, as many buyers were drawn to a limited number of reliable vendors. Nevertheless, it is plausible that the size of these communities influences this phenomenon, as larger communities tend to have a more significant number of engaged participants. In this sense, Abraxas can be described as a collection of transactional entities that revolve around multiple widely recognised vendors, attracting numerous purchasers. The average ratio of vendors to buyers in these communities is 1:19, with a range from 1:6.5 to 1:57. Indeed, there are three communities that a single vendor completely controls. As expected, the network density of a community tends to increase as its size grows.

In addition, these communities are limited to specific countries and products, as indicated in Table 4.9. Communities, on average, exhibit significant concentration (96.7%) in terms of the origin country from which the traded items were shipped. Furthermore, within a community, the items shipped tended to be classified within the same category, exhibiting an average rating of 97.6%. Hence, the transactional communities within Abraxas are characterised by their specific geographical locations and limited to a particular category of items. As an illustration, a community may engage primarily in the exchange of drug paraphernalia that is exclusively

Table 4.8 Community network measures (top 20 based on community size)

Community size	Community density	Edges	Within community transactions	Cumulative reputation (M)	Vendors	Buyers
390	0.01	810	921	266.06	17	373
337	0.01	574	748	126.69	29	308
139	0.02	331	373	153.58	12	127
129	0.01	202	247	135.78	9	120
96	0.02	151	210	166.33	6	90
91	0.02	149	176	109.5	8	83
82	0.02	117	196	294.67	3	79
58	0.03	97	105	510	1	57
53	0.03	71	111	550	1	52
52	0.02	66	89	109.75	4	48
52	0.02	65	99	246	2	50
44	0.04	85	97	121.25	4	40
38	0.04	55	71	106.67	3	35
38	0.06	80	95	237	2	36
38	0.03	45	55	251	1	37
32	0.04	36	52	82	3	29
32	0.05	53	62	102.67	3	29
32	0.04	40	64	156.5	2	30
30	0.05	40	58	72.25	4	26
30	0.05	41	74	119	3	27

Table 4.9 Communities by item categories and country shipped from (top 20 based on community size)

Community size	Custom listing (%)	Digital goods (%)	Drug paraphernalia (%)	Drugs (%)	Others (%)	Services (%)	Shipping cou ntry 1 (%)	Shipping country 2 (%)	Shipping country 3 (%)	Shipping country 4 (%)	Shipping country 5 (%)	Shipping country 6 (%)	Shipping country 7 (%)
390	0	0	0	100	0	0	93.16	2.71	1.95	1.74	0.33	0.11	–
337	0	85.45	0	14.55	0	0	36.10	28.74	6.42	5.88	5.35	4.95	3.07
139	0	0	0	100	0	0	92.76	6.97	0.27	–	–	–	–
129	0.40	0.27	0	99.33	0	0	96.36	3.24	0.40	–	–	–	–
96	0	0	0	100	0	0	68.10	23.33	5.71	1.90	0.95	–	–
91	1.72	0	0	98.28	0	0	99.43	0.57	–	–	–	–	–
82	0	0	0	100	0	0	100	–	–	–	–	–	–
58	0	0	0	100	0	0	100	–	–	–	–	–	–
53	0.80	6.97	0.27	90.08	0	1.88	100	–	–	–	–	–	–
52	0.11	1.95	0	97.94	0	0	96.63	3.37	–	–	–	–	–
52	0	0	0	95.77	0	4.23	83.84	13.13	1.01	1.01	1.01	–	–
44	1.02	0	0	98.98	0	0	100	–	–	–	–	–	–
38	0	0	0	100	0	0	92.96	4.23	2.82	–	–	–	–
38	0	0	0	100	0	0	100	–	–	–	–	–	–
38	0	0	0	100	0	0	100	–	–	–	–	–	–
32	0	0	0	100	0	0	100	–	–	–	–	–	–
32	0	0	0	100	0	0	100	–	–	–	–	–	–
32	0	0	0	96.91	3.09	0	79.69	18.75	1.56	–	–	–	–
30	0	0	0	100	0	0	65.52	22.41	12.07	–	–	–	–
30	0	0	0	100	0	0	97.30	2.70	–	–	–	–	–

imported from Canada. This implies that trust in Abraxas is potentially influenced by factors beyond a vendor's reputation, such as the country of origin for shipping and the specific product(s) being sold. This observation indicates a bias towards a particular vendor and contradicts the argument set out in Barratt and Aldridge (2016) that cryptomarkets operate as a globally interconnected network for transactions. According to Norbutas (2018), the transactional network of Abraxas exhibits a significant degree of localisation in its structure. These findings provide more comprehensive documentation of this particular trend.

Regression Results and Power Few Distributions

The results of the multiple linear regression models for vendor success, popularity and affluence are displayed in Table 4.10. The cumulative reputation score exhibits a positive and statistically significant trend across all three models. It is evident that a vendor's reputation plays an essential role in determining trust levels across the three proxy variables. This is consistent with the findings of previous studies

Table 4.10 Results of regression models

	Number of transactions (success)		Number of unique buyers (popularity)		Cumulative revenue generated (affluence)	
Variable name	Coefficient	SE	Coefficient	SE	Coefficient	SE
Intercept	−0.79**	0.27	−0.33	1.03	2389.86***	657.76
Cumulative reputation	0.1949***	0.0016	0.077***	0.006	37.86***	3.04
Average purchase price	−0.0003	0.0005	−0.0001	0.001	5.58***	1.17
Cumulative purchase price	0.0001**	0.00002	−0.0001	0.0001	–	–
Cumulative risk score	0.02***	0.003	0.059***	0.011	−35.52***	7.099
Items and information						
Unique items listings	−0.079**	0.026	0.33***	0.098	−41.97	64.01
Item categories	0.67*	0.29	1.298	1.098	−3777.36***	675.32
Item subcategories	0.38***	0.11	0.831*	0.404	314.88	263.70
Number of words in item description	0.00004*	0.00002	0.0001	0.0001	0.18***	0.044
Shipped to locations						
Continent/region	0.118	0.2625	0.79	0.991	539.78	646.98
Worldwide	−0.228	0.1986	0.0022	0.75	592.76	488.63
AIC	832.8	–	1496.88	–	4737.46	–
BIC	878.5	–	1542.66	–	4779.71	–

AIC Akaike information criteria, *BIC* Bayesian information criteria
*$p < 0.05$; **$p < 0.01$; ***$p < 0.001$

(Décary-Hétu, 2016; Décary-Hétu & Quessy-Doré, 2017; Duxbury & Haynie, 2017), despite their broader scope. Furthermore, cumulative risk demonstrates statistical significance as a predictor in all three models. While the coefficient estimate displays a positive value for the number of transactions and the number of distinct buyers, it exhibits a negative value for the cumulative revenue generated. This intriguing development requires further analysis based on extensive qualitative data to provide a thorough explanation. The outcome aligns with logical reasoning concerning the number of transactions and the number of distinct buyers. The adage "no risk, no reward" remains applicable in Abraxas. The vendor's willingness to assume the risks associated with international shipping, especially on a global scale, enhances their capacity to engage in more transactions and expand their customer base. Therefore, the success and popularity of a vendor are enhanced when they possess the willingness and capability to access a broader market. A logical correlation could be postulated between the revenue generated and the measured variables in the model. However, the model suggests otherwise.

It is essential to note that each model exhibits variations in the specific estimates that account for the variability in vendor success, popularity and affluence. Regarding the achievement of a vendor, the combined purchase price, categories of items and subcategories of items also serve as positive indicators. The impact of the cumulative purchase price on a vendor's success is found to be insignificant. However, the vendor's probability of achieving success is positively influenced by the ability to provide customers with a greater variety of items (in terms of item category and subcategory). Unique item listings and subcategories also serve as positive indicators of the popularity of vendors. This concept is logically sound, as a vendor with a more comprehensive range of products is more likely to appeal to a broader group of buyers with varying purchasing preferences. Ultimately, the product description's mean acquisition cost and word count emerge as the sole indicators of vendor prosperity. This concept is logical to a certain extent, as there is a positive correlation between the average price of a product and the potential revenue a vendor can generate. Furthermore, when an excessively high price is associated with a product, the vendor must provide the buyer with a guarantee of the utmost quality of the purchased item. Therefore, it can be inferred that including additional words in product descriptions decreases information asymmetry, as suggested by Akerlof (1970).

Figure 4.3 illustrates the power law distributions of vendor success, popularity and affluence. The phenomenon observed in Abraxas can be characterised by a power law distribution, wherein a minority of vendors are responsible for most transactions, unique buyers and generated revenue. In this study, it was found that 9.3% of vendors were responsible for 50% of the total completed transactions. Additionally, 10% of vendors accounted for 47% of unique buyers, while a smaller group of 5.2% contributed to 50.1% of the total revenue generated. As with numerous natural (Zipf, 1949; Simon, 1955) and criminological phenomena, Abraxas is indeed influenced by a select group of individuals with significant authority. The significant degree of preferential attachment observed underscores trust's critical role in shaping Abraxas' transactional network.

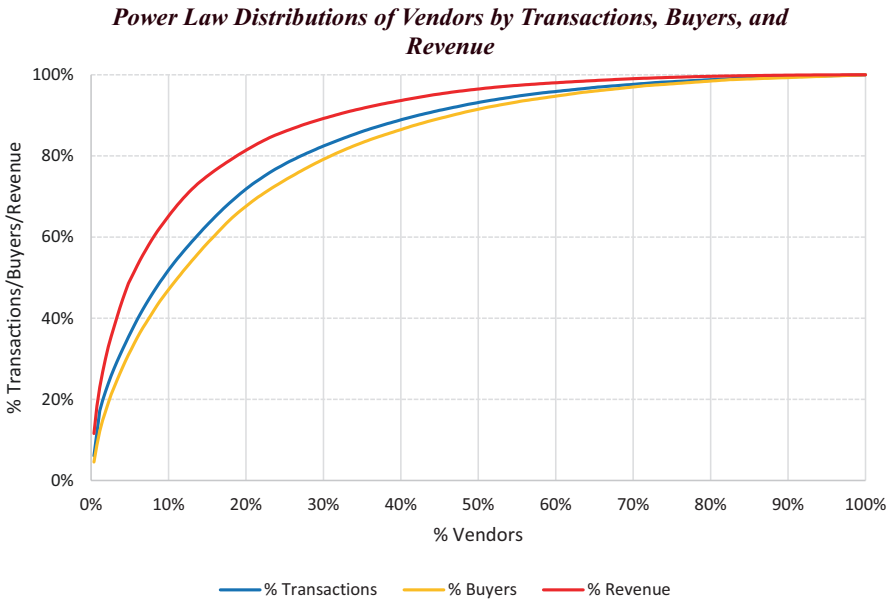

Fig. 4.3 Power law distributions of vendors by transactions, buyers and revenue

Trajectory Analyses

The results of the k-means trajectory models are presented in Table 4.11. The table provides information on three proxy variables, including the count of trajectories in each model, the relative level of each trajectory concerning the specific variable, the base crime count in January (the first month of Abraxas' operation), the trend and the percentage of vendors within each trajectory group. These trends are identified by applying regression analyses to the vendors' data over time, within each trajectory group. According to Andresen et al. (2017), a trajectory can be considered stable if the slope parameter falls within the range of −0.2 to 0.2. If the slope parameter is below −0.2, the trajectory is deemed to be decreasing, while if it is above 0.2, it is classified as increasing.

Utilising the Calinski criterion score, it was determined that a k-means partition of four groups is optimal for models assessing success, popularity and affluence. Importantly, the first trajectory in each model comprises over 80% of the total number of vendors on Abraxas. This finding suggests that a significant proportion of vendors did not engage in a high number of transactions, interact with many vendors or generate considerable revenue during their time in the market. In essence, most vendors had a negligible impact on market dynamics within the Abraxas platform, as they could not stimulate growth. Likewise, the second trajectories observed in both models indicate that moderately successful, popular and affluent vendors exhibited consistent growth within these respective categories. However, they did

Table 4.11 Summary of k-means trajectories

Variable	Trajectory	Level	Base, January	Trend	% of vendors
Number of transactions (success)	1	Low	0	Increasing	83.3
	2	Moderate	0.07	Increasing	15.6
	3	High	0	Increasing	0.7
	4	High	0	Increasing	0.4
Number of unique buyers (popularity)	1	Low	0	Increasing	82.2
	2	Moderate	0.07	Increasing	16
	3	High	0	Increasing	1.1
	4	High	0	Increasing	0.7
Cumulative revenue generated (affluence)	1	Low	0.3	Increasing	90.3
	2	Moderate	1.4	Increasing	8.6
	3	High	0	Increasing	0.7
	4	High	0	Increasing	0.4

not ultimately achieve high success, popularity and affluence. These vendors failed to reach a position among the top-performing vendors in the market. The vendors deemed the most successful, popular and financially prosperous consistently followed a similar trajectory in both the third and fourth models, maintaining this trend until the eventual closure of Abraxas. These vendors achieved significant prominence within the market and maintained their dominant position throughout their tenure in the market.

The trajectories of each model over Abraxas' operational timeline are depicted in Fig. 4.4. Each line in the regression output represents the average values of the results. In both models, the third and fourth trajectories demonstrate substantial growth as a limited number of vendors achieve significant success, popularity and affluence within a relatively brief timeframe. Interestingly, the vendors above displayed relatively low activity levels during the initial 2 months but experienced a notable surge in prominence during April, exhibiting exponential growth. Both the revenue and affluence models exhibit a comparable pattern. To provide further details, the fourth trajectory within the success model indicates a mean of zero transactions during January and February, followed by an increase to three transactions in March. Subsequently, the trajectory experienced a significant surge, reaching 41, 108 and 129 transactions in April, May and June, respectively. In a similar vein, the fourth trajectory within the revenue model exhibits an initial average cumulative revenue of $0 during January and February, followed by a substantial surge to $17,865.2, $30,276.7 and $18,024.6 in April, May and June, respectively. In the popularity model, the fourth trajectory exhibits an initial absence of unique buyers in January and February, followed by a subsequent increase to 68, 80.5 and 60.5 in April, May and June, respectively. Interestingly, a significant majority of trajectories in every model exhibit a downward trend after May. The reasons behind this phenomenon remain unclear, despite potential factors such as market competition and the unpredictable nature of the dark web.

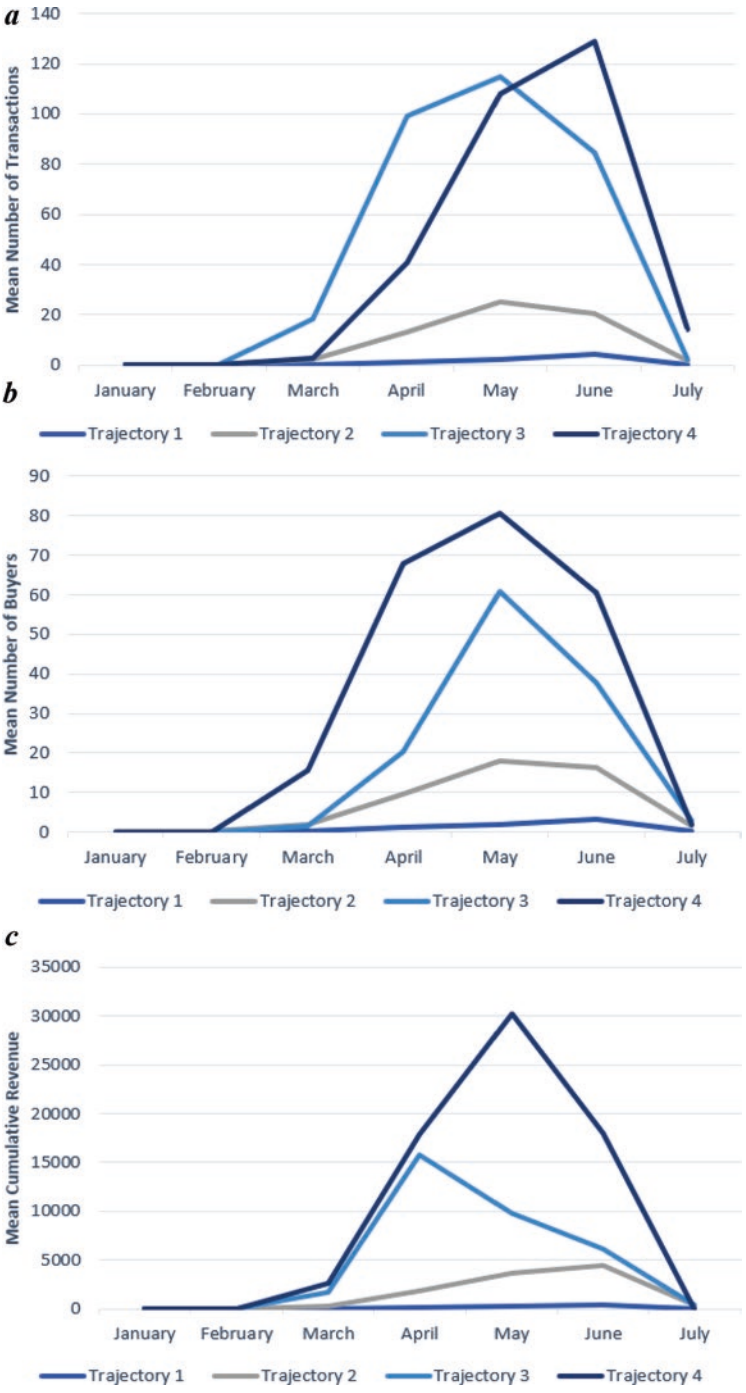

Fig. 4.4 K-means trajectories

Discussion

The examination of the Abraxas cryptomarket indicates the existence of a vast and dispersed network, wherein a significant proportion of buyers engage in transactions with a small group of vendors. The average number of vendors buyers engaged with was 2.15, as indicated by the distribution of out-degree centrality. Conversely, vendors were observed to have an average of 20.2 buyers, as evidenced by the distribution of in-degree centrality. To a significant degree, Abraxas shows a concentration of power with a limited number of vendors responsible for most completed transactions, unique buyers and revenue generated. The development of trust in a cryptomarket is significantly influenced by the ability of vendors to establish a reputation for trustworthy behaviour, which in turn enhances their chances of success. Moreover, this established reputation extends to subsequent transactions, because prospective buyers are inclined to engage in business with the most reputable vendors. This observation can be deduced from the outcomes of trajectory models, in which vendors exhibiting low and moderate levels of success, popularity and affluence demonstrate a lack of upward mobility. In contrast, vendors characterised by high levels in each dimension experience rapid and substantial growth within a brief timeframe. The results presented in this study align with the findings reported by Duxbury and Haynie (2017) and Norbutas (2018). Therefore, these collective studies provide insights into the underlying structure and dynamics of trust that support the transactional network of cryptomarkets.

The present study examines the interplay between trust, reputation and network structure within the context of Abraxas. The configuration of a clandestine market's network frequently relies on the fundamental dynamics of trust (Morselli et al., 2007; Wood, 2017). The distribution of trust within an illegal market presents a paradox, considering the significant unpredictability involved. Trust dynamics, a crucial aspect that supports market dynamics and structure, have received limited attention in the existing literature on the cryptomarket. Several studies (Duxbury & Haynie, 2017; Lacson & Jones, 2016; Janetos & Tilly, 2017) have researched and provided insights into the allocation of trust in cryptomarkets. However, a more comprehensive understanding of this phenomenon can only be achieved by examining it within the context of a transactional network. This approach allows one to quantify vendor–buyer relations over an extended period and apply statistical and trajectory models to the data.

Based on the empirical findings, it can be inferred that reputation and, to some extent, risk-taking behaviour are influential factors in the network structure of Abraxas. The power few analysis and the distribution of in-degree centrality indicate that a limited number of vendors are responsible for a significant portion of market activity. Buyers tend to engage primarily with these vendors. Therefore, the configuration of the global network results from the initial and subsequent interactions between buyers and vendors. Furthermore, this distribution occurs within the framework of the local network structure of this cryptomarket. Within the Abraxas ecosystem, each vendor and their corresponding buyers form distinct communities.

As mentioned earlier, the communities also tend to be geographically situated and focused on specific products, indicating the significance of geographic proximity and specialised markets in shaping the network structure. It was observed that, on average, approximately 96.7% of the commodities exchanged within a given community originate from a single nation. Moreover, these items were classified under the same product category in 97.6% of cases.

Therefore, the transactional communities within Abraxas are geographically bound and limited to a specific category of products. This contradicts the argument made by Barratt and Aldridge (2016), who suggest that cryptomarkets operate as globally interconnected trading networks, facilitating transactions between buyers and vendors across various nations and involving a diverse range of products and services. In essence, trust in Abraxas is intricately linked to multiple factors, such as the vendor's reputation, the country of origin for shipping and the nature of the product(s) being sold. However, this observation may indicate buyer preferences rather than an accurate measure of vendor trustworthiness. Purchasers may prefer to engage in transactions with vendors who specialise in a particular product and operate from a specific geographical location, driven by subjective inclinations or the desire for ease and convenience. This is of central importance since the fact that illicit transactions are guided by the specific preferences of buyers, in addition to the trust they place in vendors, is frequently overlooked. While the primary focus of this chapter has been on the dynamics of trust, buyer preferences cannot be disregarded.

Summary and Conclusion

This chapter has examined the allocation of trust on the platform known as Abraxas. Significantly, a notable prevalence or consolidation of trust among buyers towards a limited group of vendors exists. Although the available data does not provide conclusive evidence on the finite nature of trust within Abraxas, there are indications that it follows a Pareto distribution. However, buyers depend on data concerning vendors' previous actions when deciding which vendor to choose. The data presented herein is derived from feedback voluntarily submitted by previous clients. Vendors who are new to the market and lack a proven track record of ethical behaviour can enhance their reputation by offering price discounts to buyers. By accruing a growing number of favourable ratings, individuals or businesses can offset their initial investment by commanding a higher price based on their reputation.

Trust in Abraxas is a coordination mechanism facilitated by the established feedback and reputation system. The feedback provided by a buyer serves as an indicator of their level of trust, or lack thereof, in a vendor. Prospective buyers can subsequently access this data to assess the reliability of the vendor in question. Akerlof (1970) was one of the early scholars to highlight the potential for market failure when buyers cannot examine products before purchase and are left with uncertainty regarding the quality of the products. The negative experiences of

buyers who transact with sellers of low-quality products lead to a decline in quality standards and a diminishing willingness to pay the appropriate price for high-quality products. According to Shapiro (1983), one potential solution to address the information asymmetry between buyers and sellers that hinders trade is for sellers of high-quality products to establish a reputation upon entering the market.

The regression models indicate that vendor reputations serve as a form of brand name, conveying to buyers the reliability and excellence of a vendor. According to Akerlof's seminal work in 1970, the adverse consequences of a market characterised by information asymmetry can be alleviated if a buyer can determine the quality of the goods being sold. In the context of Abraxas, reputation plays a crucial role in distinguishing the quality of goods and mitigating uncertainty in a volatile setting. In this scenario, prospective and existing consumers will decline to engage in future transactions with a vendor of substandard quality.

In summary, reputation scores serve as a predictive indicator of consumer behaviour. Acknowledging that reputation scores indicate a seller's overall performance and dependability is essential. However, it is plausible that sellers with solid credibility and high-quality products may occasionally deceive buyers by overemphasising the product's quality or misrepresenting its attributes. With this in mind, it is plausible that a purchaser may experience heightened apprehension when evaluating a vendor with a less established reputation, as the overall perception of said vendor relies heavily on a limited number of concluded transactions. In contrast, buyers are reassured by vendors who have completed numerous transactions, as observed. Therefore, satisfactorily completed transactions may help reduce information asymmetry and address a buyer's apprehensions. Buyers may seek certain information regarding a vendor's transactional history to facilitate their decision-making process when purchasing. This observation provides insights into the mechanisms employed to address information asymmetry within cryptomarkets, such as Abraxas. Regardless of whether the feedback is positive or negative, vendors gain more recognition as their feedback increases. Consequently, the network architecture of Abraxas may potentially result from this particular dynamic.

Ultimately, drawing from the outcomes of the trajectory models, a limited subset of vendors emerges as remarkably prosperous, renowned and financially well-off within a relatively brief timeframe. This phenomenon may be attributed to how trust is established and disseminated within a cryptomarket. As stated earlier, the extent to which trust can be considered a finite resource in cryptomarkets remains uncertain. However, trust is not evenly distributed among a limited number of vendors who disproportionately benefit from it. Furthermore, this level of trust, or the absence thereof, persists over time. In this particular scenario, it appears probable that trust in Abraxas is based on a "winner-takes-all" framework, wherein certain vendors who successfully establish trust with buyers gradually assume market dominance throughout its operation. In terms of functionality, vendors who are unable to establish rapport with buyers will experience limited transactional activity and subsequently generate minimal revenue. Consequently, once trust has been established with certain vendors, it becomes challenging for new vendors to displace them. From a certain perspective, trust can be perceived as a metaphorical moat,

serving as a strategic advantage that distinguishes a select group of vendors from the remaining competitors in the market.

Moreover, the trajectory models illustrate that the initial stages of the market did not witness the presence or activity of the leading vendors on Abraxas. However, these vendors eventually emerged as dominant market players upon their engagement with buyers. This phenomenon may be indicative of a transactional cascade. Undoubtedly, upon the entrance of particular vendors into a market and their initiation of transactions with novel buyers, their engagement rapidly intensifies, resulting in a substantial share of market activity within a relatively brief timeframe. However, there remains ambiguity regarding whether these particular vendors were previously successful sellers on other platforms before transitioning to Abraxas, or if their success was primarily derived from this specific market. Therefore, it is indeterminate whether their achievement on Abraxas was a result of organic development or if it was transferred from another market. On the other hand, the vendors in the initial trajectories exhibited limited growth concerning each proxy variable over time. Furthermore, it should be noted that these vendors were involved from the beginning of Abraxas, engaging in a limited number of transactions during January. This suggests that the absence of a first mover principle on Abraxas results in early entrants' eventual dominance of market activity.

In conclusion, the points mentioned above suggest that trust is an inherent component of any network that engages in the transportation, exchange and commerce of goods and services, irrespective of their legal status. The network structure of cryptomarkets such as Abraxas and the one investigated by Duxbury and Haynie (2017) is based on the trust buyers place in the vendors they engage in transactions with. Trust plays a crucial role in facilitating the smooth functioning of transactional networks; however, it can also introduce disruptions to their operational efficiency. In the present scenario, trust emerges as a fragile component of the Abraxas transactional network. Suppose law enforcement agencies were to formulate a strategy to impede trade on Abraxas. It is plausible that they would prioritise targeting vendors with high credibility and trustworthiness among buyers. After all, this select group of individuals is responsible for propelling market activity on the Abraxas platform. It is highly probable that the elimination of these actors would result in a cessation of market activity or, at the very least, a reduction in its pace to some extent.

The practical implications of this study are apparent in this context. In order to effectively mitigate the activities of these illicit entities, law enforcement agencies should prioritise gaining a comprehensive understanding of their underlying dynamics of trust. This would entail identifying the vendors that are most responsible for market activity. Law enforcement officers might then compile a roster of appropriate subjects for apprehension. The primary objective of this strategy is to disrupt a criminal network by focusing specifically on those individuals with the highest level of trust within the network. The hypothetical elimination of these actors would potentially deprive a transactional network of its most crucial economic resources, compelling buyers to transition to an unfamiliar supplier or withdraw from the market entirely.

Although the rationale behind this specific strategy aligns with the present study's findings, the adverse consequences of such targeted interventions are inadequately understood. What might be the impact on the overall level of trust in the market if a reliable vendor were to be eliminated? What methods might be employed to quantify this phenomenon? Would purchasers opt for an alternative vendor within the same market, or would they transition to an entirely different market to conduct their business? The upcoming chapters will address these questions, simulating and evaluating the effectiveness of eliminating trusted cryptomarket users as a comprehensive law enforcement strategy.

References

Akerlof, G. A. (1970). The market for lemons: Qualitative uncertainty and the market mechanism. *Quarterly Journal of Economics, 84*, 488–500.

Aldridge, J. & Décary-Hétu, D. (2016). Cryptomarkets and the future of illicit drug markets. In European Monitoring Centre for Drugs and Drug Addiction, J. Mounteney, A. Bo, & A. Oteo (Eds.), *The internet and drug markets (EMCDDA Insights 21)* (pp. 23–30). Publications Office of the European Union. https://data.europa.eu/doi/10.2810/324608

Andresen, M. A., Curman, A. S., & Linning, S. J. (2017). The trajectories of crime at places: Understanding the patterns of disaggregated crime types. *Journal of Quantitative Criminology, 33*, 427–449.

Ashton, S. A., & Bussu, A. (2022). The social dynamics of adolescent co-offending. *Youth Justice, 23*(3), 350–371. https://doi.org/10.1177/14732254221136044

Baker, T., & Piquero, A. R. (2010). Assessing the perceived benefits—Criminal offending relationship. *Journal of Criminal Justice, 38*(5), 981–987.

Barratt, M., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy, 35*, 1–6.

Batikas, M., & Kretschmer, T. (2018). Entrepreneurs on the darknet: Reaction to negative feedback (Unpublished paper). https://doi.org/10.2139/ssrn.3238141.

Bichler, G., Malm, A., & Cooper, T. (2017). Drug supply networks: A systematic review of the organizational structure of illicit drug trade. *Crime Science, 6*(2), 63–73.

Blondel, V., Guillaume, J., Lambiotte, R., & Lefebvre, E. (2008). Fast unfolding of communities in large networks. *Journal of Statistical Mechanics: Theory and Experiment, 2008*, P10008. https://doi.org/10.1088/1742-5468/2008/10/P10008

Branwen, G., Christin, N., Décary-Hétu, D., Andersen, R. M., StExo, E. P., Anonymous, L., Sohhlz, D., Kratunov, D., Cakic, V., Buskirk, V., Whom, M., Goode, S. (2015, July 12). *Dark net market archives, 2011–2015*. https://www.gwern.net/DNM-archives

Bright, D. A., Koskinen, J., & Malm, A. (2017). Illicit network dynamics: The formation and evolution of a drug trafficking network. *Journal of Quantitative Criminology, 35*(2), 237–258.

Catino, M. (2014). How do mafias organize? Conflict and violence in three mafia organizations. *European Journal of Sociology, 55*(2), 177–220.

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213–224). Association for Computing Machinery. https://doi.org/10.1145/2488388.2488408.

Décary-Hétu, D. (2016). Policing cybercrime and cyberterror. *Global Crime, 17*(1), 123–125.

Décary-Hétu, D., & Dupont, B. (2013). The social network of hackers. *Global Crime, 13*(3), 1–16.

Décary-Hétu, D., & Quessy-Doré, O. (2017). Are repeat buyers in cryptomarkets loyal customers? Repeat business between dyads of cryptomarket vendors and users. *The American Behavioral Scientist, 61*(11), 1341–1357.

Demant, J., Munksgaard, R., Décary-Hétu, D., & Aldridge, J. (2018). Going local on a global platform: A critical analysis of the transformative potential of cryptomarkets for organised illicit drug crime. *International Criminal Justice Review, 28*(3), 255–274.

Dumouchel, P. (2005). Trust as an action. *European Journal of Sociology, 46*(3), 417–428.

Duxbury, S., & Haynie, D. (2017). The network structure of opioid distribution on a darknet cryptomarket. *Journal of Quantitative Criminology, 34*(4), 921–941.

Duxbury, S., & Haynie, D. (2018). Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social Networks, 52*, 238–250.

Duxbury, S., & Haynie, D. (2019). Criminal network security: An agent-based approach to evaluating network resilience. *Criminology, 57*(2), 314–342.

Englefield, A., & Ariel, B. (2017). Searching for influencing actors in co-offending networks: The recruiter. *International Journal of Social Science Studies, 5*(5), 24–45.

Fader, J. J. (2016). Criminal family networks: Criminal capital and cost avoidance among urban drug sellers. *Deviant Behavior, 37*(11), 1325–1340.

Free, C., & Murphy, P. R. (2015). The ties that bind: The decision to co-offend in fraud. *Contemporary Accounting Research, 32*(1), 18–54.

Gambetta, D. (Ed.). (1988). Trust: Making and breaking cooperative relations. .

Gambetta, D. (2000). Can we trust trust? In D. Gambetta (Ed.), *Trust: Making and breaking cooperative relations* (pp. 213–237). University of Oxford.

Gambetta, D. (2009). *Codes of the underworld: How criminals communicate*. Princeton University Press.

Gambetta, D., & Bacharach, M. (2001). Trust in signs. In K. Cook (Ed.), *Trust and society* (pp. 148–184). Russell Sage Foundation.

Genolini, C., & Falissard, B. (2010). KmL: k-means for longitudinal data. *Computational Statistics, 25*(2), 317–328.

Genolini, C., Ecochard, R., Benghezal, M., Driss, T., Andrieu, S., & Subtil, F. (2016). kmlShape: An efficient method to cluster longitudinal data (time-series) according to their shapes. *PLoS One, 11*(6), e0150738. https://doi.org/10.1371/journal.pone.0150738

Hardy, R., & Norgaard, J. (2016). Reputation in the Internet black market: An empirical and theoretical analysis of the Deep Web. *Journal of Institutional Economics, 12*(3), 515–539.

Herley, C., & Florencio, D. (2010). Nobody sells gold for the price of silver: Dishonesty, uncertainty and the underground economy. In T. Moore, D. Pym, & C. Ioannidis (Eds.), *Economics of information security and privacy* (pp. 35–53). Springer.

Holt, T., & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*(1), 33–50.

Holt, T., Strumsky, D., Smirnova, O., & Kilger, M. (2012). Examining the social networks of malware writers and hackers. *International Journal of Cyber Criminology, 6*(1), 891–903.

Janetos, N., & Tilly, J. (2017). Reputation dynamics in a market for illicit drugs (Unpublished paper).

Jaspers, J. D. (2017). Managing cartels: How cartel participants create stability in the absence of law. *European Journal on Criminal Policy and Research, 23*, 319–335.

Kenney, M. (2007). The architecture of drug trafficking: Network forms of organisation in the Colombian cocaine trade. *Global Crime, 8*(3), 233–259.

Lacson, W., & Jones, B. (2016). The 21st century darknet market: Lessons from the fall of Silk Road. *International Journal of Cyber Criminology, 10*(1), 40–61.

Lantz, B., & Ruback, R. B. (2017). The relationship between co-offending, age, and experience using a sample of adult burglary offenders. *Journal of Developmental and Life-Course Criminology, 3*, 76–97. https://doi.org/10.1007/s40865-016-0047-0

Malm, A., & Bichler, G. (2011). Networks of collaborating criminals: Assessing the structural vulnerability of drug markets. *Journal of Research in Crime and Delinquency, 48*(2), 271–297.

Martin, J. (2014). *Drugs on the dark net*. Palgrave Macmillan.
McGloin, J. M., & Kirk, D. (2011). An overview of social network analysis. *Journal of Criminal Justice Education, 2*(2), 169–181.
McPherson, M., Smith-Lovin, L., & Cook, J. M. (2001). Birds of a feather: Homophily in social networks. *Annual Review of Sociology, 27*(1), 415–444.
Morselli, C. (2009). *Inside criminal networks*. Springer.
Morselli, C., Giguere, C., & Petit, K. (2007). The efficiency/security trade-off in criminal networks. *Social Networks, 29*(1), 143–153.
Morselli, C., Turcotte, M., & Tenti, V. (2011). The mobility of criminal groups. *Global Crime, 12*(3), 165–188.
Nagin, D., & Land, K. (1993). Age, criminal careers and population heterogeneity: Specification and estimation of a nonparametric, mixed Poisson model. *Criminology, 31*(3), 327–362.
Natarajan, M. (2006). Understanding the structure of a large heroin distribution network: A quantitative analysis of qualitative data. *Journal of Quantitative Criminology, 22*(2), 171–192.
Newman, M. E. J. (2003). The structure and function of complex networks. *SIAM Review, 45*(2), 167–256. https://doi.org/10.1137/S003614450342480
Newman, M. E. J. (2006). Modularity and community structure in networks. *Proceedings of the National Academy of Sciences, 103*(23), 8577–8582.
Norbutas, L. (2018). Offline constraints in online drug marketplaces: An exploratory analysis of a cryptomarket trade network. *International Journal of Drug Policy, 56*, 92–100. https://doi.org/10.1016/j.drugpo.2018.03.016
Norbutas, L., Ruiter, S., & Corten, R. (2020). Believe it when you see it: Dyadic embeddedness and reputation effects on trust in cryptomarkets for illegal drugs. *Social Networks, 63*, 150–161.
Oksanen, A., Miller, B. L., Savolainen, I., Sirola, A., Demant, J., Kaakinen, M., & Zych, I. (2020, July). Illicit drug purchases via social media among American young people. In G. Meiselwitz (Ed.), *Social computing and social media. Design, ethics, user behavior, and social network analysis. HCII 2020. Lecture Notes in Computer Science: Vol. 12194* (pp. 278–288). Springer.
Papachristos, A. V. (2009). Murder by structure: Dominance relations and the social structure of gang homicide. *American Journal of Sociology, 115*, 74–128.
Papachristos, A. V. (2014). The network structure of crime. *Sociology Compass, 8*, 347–357.
Pettit, P. (2004). Trust, reliance and the internet. *Analyse & Kritik, 26*(1), 108–121.
Pons, P., & Latapy, M. (2005). Computing communities in large networks using random walks. In P. Yolum, T. Güngör, F.Gürgen, & C. Özturan (Eds.), *Computer and Information Sciences—ISCIS 2005. Lecture Notes in Computer Science: Vol. 3733* (pp. 284–293). Springer.
Przepiorka, W., Norbutas, L., & Corten, R. (2017). Order without law: Reputation promotes cooperation in a cryptomarket for illegal drugs. *European Sociological Review, 33*(6), 752–764.
Sarnecki, J. (2001). *Delinquent networks: Youth co-offending in Stockholm*. Cambridge University Press.
Serva, M. A., Fuller, M. A., & Mayer, R. C. (2005). The reciprocal nature of trust: A longitudinal study of interacting teams. *Journal of Organizational Behavior, 26*(6), 625–648.
Shapiro, C. (1983). Premiums for high quality products as return to reputation. *Quarterly Journal of Economics, 98*, 659–680.
Simon, H. (1955). On a class of skew distribution functions. *Biometrika, 42*, 425–440.
Smith, C. M., & Papachristos, A. V. (2016). Trust thy crooked neighbour: Multiplexity in Chicago organized crime networks. *American Sociological Review, 81*(4), 644–667.
Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2016). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy, 35*, 58–68. https://doi.org/10.1016/j.drugpo.2015.12.010
Van Buskirk, J., Naicker, S., Roxburgh, A., Bruno, R., & Burns, R. (2016). Who sells what? Country specific differences in substance availability on the Agora cryptomarket. *International Journal of Drug Policy, 35*, 16–23. https://doi.org/10.1016/j.drugpo.2016.07.004

van Hout, M., & Bingham, T. (2013a). 'Surfing the Silk Road': A study of users' experiences. *International Journal of Drug Policy, 24*(6), 524–529. https://doi.org/10.1016/j.drugpo.2013.08.011

von Lampe, K. (2016). The ties that bind: A taxonomy of associational criminal structures. In G. A. Antonopoulos (Ed.), *Illegal entrepreneurship, organized crime and social control: Essays in Honor of Professor Dick Hobbs* (pp. 19–35). Springer.

von Lampe, K., & Johansen, P. (2004). Organized crime and trust: On the conceptualization and empirical relevance of trust in the context of criminal networks. *Global Crime, 6*(2), 159–184.

Wasserman, S., & Faust, K. (1994). *Social network analysis: Methods and applications*. Cambridge University Press.

Weerman, F. M. (2003). Co-offending as social exchange: Explaining characteristics of co-offending. *British Journal of Criminology, 43*(2), 398–416.

Williamson, O. (1993). Calculativeness, trust, and economic organization. *Journal of Law and Economics, 36*(1), 453–486.

Wood, G. (2017). The structure and vulnerability of a drug trafficking collaboration network. *Social Network, 48*, 1–9.

Yang, S., Keller, F., & Zheng, L. (2013). *Social network analysis: Methods and examples*. Sage Publications.

Zipf, G. (1949). *Human behavior and the principle of least effort: An introduction to human ecology*. Addison-Wesley Press.