DRUG MARKETS AND ANONYMIZING TECHNOLOGIES

Panel overview

Meropi Tzanetakis
University of Oslo & University of Vienna

Silje A. Bakken
University of Copenhagen

Rasmus Munksgaard
University of Montréal

David Décary-Hétu
University of Montréal

The development and use of sophisticated networked technologies have contributed to the proliferation of drug markets on the Internet. These online drug markets take advantage of social media, encryption software (e.g. Tor network) and cryptocurrencies (e.g. Bitcoin, Monero) to conceal the identity and physical location of their users. Marketplaces that ensure the anonymity of their users by implementing these two technologies are commonly named cryptomarkets. Despite the variation of encryption in the online drug markets, the illegality of drugs and drug dealing makes technologically enabled anonymity an important factor among its participants. Anonymizing technologies allow to mitigate risks of vendors and customers when exchanging drugs while new risks emerge.

Research on online drug markets has demonstrated cryptomarkets are continually growing in terms of sales volumes generated despite law enforcement interventions. Moreover, previous studies have focused on the prevalence of drugs and drug users as well as implications for harm reduction policies. This series of papers proposes to

expand the exploration of platforms enabling the exchange of illicit drugs on the internet in a number of directions. Various papers propose different concepts for understanding cryptomarkets as social phenomena where social relationships and socio-technical practices enable economic transactions. It also sheds light on the tension between trust, anonymity and pseudonymity. The papers expand on reliability of data gathered via anonymous online interviews, drawing attention to participation of stigmatized communities. They also explore little-considered ways in which cryptomarkets govern themselves. The aim of this panel is to bring together different perspectives on online, anonymized and encryption-based markets for illegal drugs.

The first paper focuses on ways in which anonymous online drug platforms govern themselves through informal coordination practices. It applies Hofmann's et al. conceptual framework of governance as reflexive coordination to cryptomarkets. Thus, it addresses the processes, structures and actors that contribute to ordering these platforms. Based on a longitudinal ethnographic study, this paper examines governance by cryptomarkets as an evolving negotiation process in four dimensions. It explores how cryptomarkets perform relatively stable forms of ordering despite their lack of formal regulation which enable a flourishing e-commerce business that is based on informal norms, cognitive framings and technological design.

The second paper examines methodological challenges encountered when conducting encrypted online interviews with hard to reach populations. While the use of the encrypted application Wickr ensures interview participants anonymity, it raises questions regarding the relation of anonymity and data reliability. Doing textual based interviews also brings out multiple challenges affecting the quality of the interviews. Based on 110 semi-structured interviews with online drug dealers and buyers, the paper discusses advantages and disadvantages concerning the method of encrypted textual interviews.

The third paper investigates the buyer-vendor relationship from an economic sociological perspective. It argues that while mechanisms of informal social control and the reputation system reduce transactional uncertainty, a successful purchase more strongly reduces uncertainty. This situates the paper in an empirical and theoretical debate as to the antecedents of trust in illicit online markets. Empirically, the paper examines the relationship between vendor's reputation, previous transactional relations with the vendor, and buyers' willingness to subject themselves to risk using a dataset of cryptomarket transactions. Statistical analysis shows both transactional relations and reputation have strong effects on transaction values, suggesting that trust in vendors may initially be founded on public reputation and informal social control, but that ongoing dyadic transactional relations produce trust among those involved.

The final paper examines the relationship between reputation, trust and continued transactions between buyers and sellers in cryptomarkets. It outlines the importance of trust as trade partners do not know each other's motives and expectations which may include cheating or acting opportunistically, but also links the establishment of trust to technologically enabled anonymity features on illegal online markets. The paper goes on to explore how Gambetta's concept of interpreting signs and signals can produce process-based trust on anonymous market and therefore reduce uncertainties between

market participants. The model presented in this paper explains the impact of past experiences, the self-presentation and the community integration of online drug dealers on the creation of bonds of trusts. These bonds of trusts are measured through successful transactions.

GOVERNANCE BY CRYPTOMARKETS FOR DRUGS

Meropi Tzanetakis
University of Oslo & University of Vienna

Christian Katzenbach
Freie Universität Berlin & Alexander von Humboldt Institute for Internet and Society

The evolution of cryptomarkets
It was only seven years ago when Silk Road, the first drug distribution platform of its kind, started operating on the darknet – a subset of the internet which includes hidden services (Barratt, 2012). It pioneered the phenomenon of cryptomarkets by implementing the combination of anonymizing software and cryptocurrencies for making payments (Martin, 2014). Together both provide a basis for a socio-technical innovation with which the identity and physical location of its users are being concealed. At the same time, law enforcement (LE) interventions are increasingly complicated.
The term cryptomarkets refers to platforms for the sale of, among other products and services, licit and illicit drugs which can be accessed by using anonymizing software such as Tor (short for The Onion Router). The opening of Silk Road was accompanied by media attention, disapproval by government authorities and law enforcement, as well as the increasing interest of scholars. Only after Silk Road was taken down by the FBI in October 2013 did other marketplaces emerge in significant numbers, competing for market share (Soska & Christin, 2015). Moreover, whenever single cryptomarkets close voluntarily or enforced by LE, new cryptomarkets now reach similar sales levels within months. As of mid-2018, almost two dozen platforms of varying sizes and feature sets are online with vendors competing for a myriad of customers (DarkNet Stats 2018).

Governance as reflexive coordination
In this paper, we address governance by cryptomarkets, which is the processes, structures and actors that contribute to ordering cryptomarkets. In contrast to the governance of cryptomarkets, this is an underexplored issue in cryptomarket research and Internet governance (IG) scholarship alike. For this, the recent turn in IG literature to informal modes of coordination and governance is instructive as cryptomarkets cannot rely on formal institutions and law enforcement for their internal ordering. Instead of focusing on formal institutions such as the Internet Governance Forum (IGF) or ICANN, recent IG studies suggest to investigate how governance materializes in internet architecture, socio-technical practices, and private modes of ordering (DeNardis, 2012; Epstein et al., 2016). This paper builds on Hofmann et al. (2016)'s concept of reflexive coordination. Here, governance is grounded in mundane practices of coordination but is really set in motion in 'critical moments'. In these, the involved

parties begin to redefine the situation in question as routines are challenged, contested, and displaced through acts of articulation and justification.

Reflexive coordination on cryptomarkets
The analysis draws on a multi-sited digital ethnography conducted between 2014 and 2018. The longitudinal ethnography included eleven semi-structured face-to-face and seven encrypted online interviews with cryptomarket users, digital monitoring of cryptomarkets including AlphaBay, Agora, Dream Market, Nucleus and Outlaw, associated discussion forums (e.g., official market forums, Subreddit DarkNetMarkets) and scraping of market data on AlphaBay from September 2015 to August 2016 (described in Tzanetakis, 2018).

The results characterize governance by cryptomarkets as an evolving negotiation process in four dimensions (Katzenbach, 2018):
(1) The *regulative dimension* of governance addresses the provision and enforcement of formal rules. In contrast to legitimate platforms like eBay, Alibaba or Airbnb, actors on cryptomarkets cannot rely on formal institutions such as property rights provided by the state for formal legal economic exchange (Beckert & Wehinger, 2013). Nor can users sue each other for contractual infringement or violating standards for product quality. In addition, actors can be prosecuted for the exchange of illegal drugs. Despite these obstacles, cryptomarkets emerged as a 'transformative criminal innovation' on the darknet (Aldridge & Décary-Hétu, 2014).

(2) The *normative dimension* investigates prevalent assumptions about legitimate and illegitimate behavior in a given community. On cryptomarkets this dimension is expressed in the general terms of conditions by platform administrators stating which services or products are not allowed for sale. Interestingly, the distribution of child pornographic content is deemed unacceptable since the initial Silk Road and regularly affirmed by different community members ever since. Child pornography is negotiated as morally unacceptable as it harms innocent and vulnerable minors.

(3) The *technological dimension* takes into account the embodiment of affordances and rules in infrastructures, devices, and algorithms relevant to cryptomarkets. Similarly to legitimate e-commerce platforms, cryptomarkets need to resolve trust issues. This is achieved by implementing reputation systems (Resnick & Zeckhauser, 2002). They encourage consumers to rate each other, so that they can assess the quality of services and products before making buying decisions. Another architectural solution for trust issues is a centralized escrow service (Tzanetakis et al., 2016). It enables the administrator of a marketplace to retain the payment until all conditions of a transaction are complete. Escrow also allows for an arbitration process to resolve disputes between customers and vendors.

(4) The *discursive dimension* addresses the shared or contested understandings and framings of issues in certain contexts. In contrast to legitimate platforms, cryptomarkets face the danger of abruptly being taken down by LE agencies and, hence, their users loosing funds stored in centralized escrow. In a particular critical moment, the closure of Silk Road was followed by a negotiation process within the cryptomarket community leading to the implementation of multi-signature escrow. With this, funds do not

necessarily need to be stored centrally on any platform, but can be administrated decentralized. No central authority is required to process a payment, instead two of three public keys are required to finalize a transaction.

In sum, cryptomarkets perform relatively stable forms of ordering despite their lack of formal regulation. This enables a flourishing e-commerce business that is based on informal norms, cognitive framings and technological design. By foregrounding these often less visible forms of governance by cryptomarkets, this paper also contributes to the broader discussion of internet governance. Currents disputes around platform governance, privacy and copyright show that formal regulation always is complemented, challenged and substantiated by norms, discourses and technology. There's always more than law, not only in shadow areas such as cryptomarkets.

References
Aldridge, J., Décary-Hétu, D. (2014). Not an ebay for drugs: The cryptomarket silk road as a paradigm shifting criminal innovation. http://dx.doi.org/10.2139/ssrn.2436643.

Barratt, M. J. (2012). Silk Road: eBay for drugs. Letter to the editor. *Addiction*, 107: 683.

Beckert, J., F. Wehinger (2013). In the shadow: Illegal markets and economic sociology. *Socio-Economic Review*, 11: 5–30.

Darknet Stats (2018, July 20). https://dnstats.net/.

DeNardis, L. (2012). Hidden levers of internet control. An infrastructure-based theory of internet governance. *Information, Communication & Society*, 15:5, 720–738.

Epstein, D., Katzenbach, C. & Musiani, F. (Eds.). (2016). Doing internet governance: practices, controversies, infrastructures, and institutions. Special Issue. *Internet Policy Review*, 5(3).

Hofmann, J., Katzenbach, C., Gollatz, K. (2016). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society*, 19: 9, 1406–1423.

Katzenbach, C. (2018). There Is Always More Than Law! From Low IP Regimes To A Governance Perspective In Copyright Research. *Journal of Technology Law and Policy*, 22(1).

Martin, J. (2014). Drugs on the dark net. How cryptomarkets are transforming the global trade in illicit drugs. Basingstoke: Palgrave Macmillan.

Resnick, P., Zeckhauser, R. (2002). Trust among strangers in internet transactions: Empirical analysis of eBay' s reputation system, in M. R. Baye (ed.). The Economics of the Internet and E-commerce (pp.127–157), Emerald Group Publishing Limited.

Soska, K., Christin, N. (2015). Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. Paper presented at the 24th USENIX security symposium.

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.

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. *International Journal of Drug Policy*, 56, 176–186.

DOING QUALITATIVE RESEARCH IN ONLINE DRUG MARKETS: HOW TO BALANCE PARTICIPANT'S ANONYMITY AND DATA RELIABILITY?

Silje A. Bakken
University of Copenhagen

Jakob Demant
University of Copenhagen

Over the last few years, the Internet has become an important channel for drug dealing. It ranges from legal spice dealing on the clear web (Hillebrand, Olszewski, & Sedefov, 2010) to social media drug dealing (Demant & Bakken, 2018) to encrypted darknet markets (Martin, 2014). Despite the variation of encryption in these markets, the illegality of drug dealing does make anonymity an important factor among the participants. Complete anonymity would help avoid many of the risks when dealing with drugs, such as being discovered by the police or threatened by other market members. Participating in research would also mean engaging in risky behavior, especially if it includes face-to-face interviews or phone conversations. So how can we as researchers ensure participant anonymity in research, and by that make more people interested in joining? And how does the anonymity relate with data reliability?

Methods
This paper is based on 110 semi-structured interviews made with online drug dealers and buyers in 2017/2018. The interviews were part of a larger qualitative study of social media drug dealing in the Nordic countries (Denmark, Norway, Sweden, Finland and Iceland). The project also included extensive digital ethnographic research in each of the five countries. For this paper, the focus is on how we conducted the interviews and the challenges we met along the way, rather than the interview content itself. All interviewees in the social media study were offered a gift card of $40.

Our ethnographic research showed that Wickr was the most trusted application among online drug dealing participants. We therefore chose to let the interviewees choose how they preferred doing the interviews, which could have been face-to-face, over the phone or other messaging applications. Still, about 90% chose Wickr, which proved to be more flexible, similar to other online messaging interviews (Barratt, 2011). Wickr is an

encrypted messaging application where the messages have a chosen time limit, which the recipient activates when opening the text. The messages then disappear and cannot be retrieved afterwards. It is similar to SnapChat, except for the encryption and that the messages are not accessible to the company owning the application (as far as we know). Wickr ensured both participant anonymity and researcher protection.

Findings
We found Wickr to work well as a tool when interviewing participants of illegal activities. One advantage was that the majority of participants already knew the application from using it when dealing/buying drugs. In social media drug markets, it is common for sellers to post their Wickr-username when advertising their drugs, so that people can contact them directly in a safer application than where the post is, e.g. on Facebook and Instagram. The participants therefore trusted Wickr as it offers full anonymity and easily allows sharing their experiences with drugs and drug markets. Wickr was also our main gateway to contacting dealers for interviews, which gave us valuable one-on-one communication from start.

Additionally, the encryption created a physical distance between the interviewee and the interviewer, offering full anonymity if the interviewee wanted to. Not only did the encryption protect the interviewee from the researcher, but it also protected them against the potential risk of having legal institutions accessing the information. Compared to other encrypted applications, e.g. Telegram and Signal, Wickr does not demand a phone number or any other personal information.

Wickr is a messaging application people have on their phones, something that made the interview situation highly flexible. Interviewees were often occupied with other activities at the time of the interview. This resulted in some interviews taking several weeks, while most lasted 3-7 hours. To ensure as many full interviews as possible, the interviewers were told to be available on Wickr almost at all times when they had made initial contact with a potential participant. Another successful strategy was to schedule a time for the interview, trying to do it intensively in a few hours.

Despite the positive sides of full anonymity in interview situations, we also met several challenges. As with any other asynchronous communication in space, one could easily be misunderstood since the tone of the voice and facial expression is not visible (Opdenakker, 2006). It did, however, seem like the interviewees were used to this communication form, and the conversations went well. On the other hand, full encryption and anonymity makes it difficult to assure traditional reliability of the data collected. Problems such as multiple participation and sincerity were perceived as more challenging under full anonymity than in physical or oral interviews. The interviewer had no facial expressions or tone of voice to watch out for, and the interviewees had a lot of time to rethink their answers. Additionally, it was impossible to ensure a good interview situation for the interviewee, despite encouraging them to be alone and without larger distractions.

Conclusion
Using encrypted applications for interviews might be very useful, especially when interviewing on illegal or sensitive topics. It ensures anonymity and protection for both

the interviewee and the interviewer. However, there are quite a few challenges that should be well thought through before starting such interviews. It is therefore necessary to do more research on these types of methods and reflect on how to make sure to conduct fruitful interviews and to reach the wanted number of interviews while maintain a good research reliability.

References
Barratt, M. J. (202) The efficacy of interviewing young drug users through online chat. *Drug and Alcohol Review*, 31(4), 566-572.

Barratt, M. J. & 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.

Demant, J. & S. Bakken (*Unpublished*) Social media drug dealing in the Nordic countries.

Hillebrand, J., Olszewski, D. & R. Sedefov (2010) Legal Highs on the Internet. *Substance Use & Misuse*, 45(3), 330-340.

Martin, J. (2014) *Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade In Illicit Drugs*. Palgrave Macmillian, UK.

Opdenakker, R. (2006) Advantages and Disadvantages of Four Interviewing Techniques in Qualitative Research. *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 7(4).

BEYOND REPUTATION: THE EFFECTS OF SOCIAL RELATIONS ON CRYPTOMARKET TRANSACTION VALUES AND RISK-TAKING

Rasmus Munksgaard
University of Montréal

Cryptomarkets and the problem of trust

Illicit online markets for drugs, cryptomarkets, have become increasingly integrated components of 21st century drug distribution and -consumption (Aldridge & Décary-Hétu, 2016; Barratt et al., 2014, 2016; Cunliffe et al., 2017). Although the ecosystem constitutes a fraction of the international drug economy, cryptomarkets have shown continual growth despite law enforcement intervention (Décary-Hétu & Giommoni, 2016; Soska & Christin, 2015).

Trust is a precondition for a transaction to be completed, and is in an exchange context a question of the other's future honesty (Beckert, 2009; Lewis & Weigert, 1985). The cryptomarket literature identifies social control as the main mechanism that reduces this uncertainty and specifies two institutional mechanisms: The mediating role of marketplace administrations, providing dispute resolution and escrow services (Martin,

2014), and the reputation system which allows buyer to rate vendors (Hardy & Norgaard, 2015; Przepiorka et al., 2017). In offline drug markets, transactions are often embedded in contexts of friendship, reciprocity or community (e.g. Hughes et al., 2017; Jacques & Wright, 2015; Sandberg, 2012). Recent studies have shown cryptomarket buyers tend to be repeat customers (Décary-Hétu & Quessy-Doré, 2017), and that the network structure of the cryptomarkets reflects *'buyers' desire for trustworthy […] vendors'* (Duxbury & Haynie, 2017, p. 247). Thus, while reputation seems predictive of economic action, the latter is still embedded in transactional-dyadic relations. However, scholars arguing that reputation is the foundation of trust on cryptomarkets have rejected trust-building through social embeddedness and institutional control in cryptomarkets (Przepiorka et al., 2017). This paper empirically examines the tension between this theoretical disagreement and the new empirical findings on the social embeddedness of cryptomarket transactions.

Analysis, method and data
The analysis is based on a dataset of cryptomarket transactions collected through webscraping, an established methodology in cryptomarket studies (e.g. Aldridge & Décary-Hétu, 2016; Christin, 2013; Soska & Christin, 2015; Tzanetakis, 2018). The transaction is treated as the behavioral manifestation of trust which implies a risk of harm, specifically the risk of a transaction failure (Morselli et al., 2017; Lewis & Weigert, 1985). The willingness to undertake financial risk by purchasing a more expensive product is considered an expression of trust and estimated as the outcome of three sources of trust: Social/economic ties with the seller, institutional approval and reputation using multilevel linear regression controlling for between-vendor variance, product category and origin.

Findings
Modeling the value of cryptomarket transactions as a function of the three sources of trust yields a model with superior explanatory power to one based solely on either, as in previous research. Further, as institutional approval and economic relations are included in statistical modelling, the effect of reputation lessens. This suggests that trust is a function of multiple sources, contrary to what the literature argues (Przepiorka et al., 2017).

Discussion
The findings demonstrate that neither reputation nor institutional approval are satisfactory explanations for why cryptomarket actors trust each other. Rather, trust is contingent upon the availability of multiple sources of trust. This provides evidence for the central thesis of *new economic sociology*, that economic action is socially embedded in both social and economic relations and institutional contexts (Granovetter, 2017; Swedberg, 1997; Swedberg & Granovetter, 1992), despite the appearance of cryptomarket transactions being between atomized anonymous individuals. The finding that the effect of reputation diminishes as other sources of trust are included in modelling suggests that previous studies which have argued that reputation is what creates social order in online markets, both licit and illicit, have omitted key theoretical explanations with possible empirical implications (Przepiorka et al., 2017; Tadelis, 2016).

References

Aldridge, J., & Décary-Hétu, D. (2016). Hidden Wholesale: The drug diffusing capacity of online drug cryptomarkets. International Journal of Drug Policy, 35, 7–15.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2014). Use of Silk Road, the online drug marketplace, in the United Kingdom, Australia and the United States. Addiction, 109(5), 774–783.

Barratt, M. J., Ferris, J. A., & Winstock, A. R. (2016). Safer scoring? Cryptomarkets, social supply and drug market violence. International Journal of Drug Policy, 35, 24–31.

Beckert, J., & Wehinger, F. (2013, 1). In the shadow: illegal markets and economic sociology. Socio-Economic Review, 11(1), 5–30.

Cunliffe, J., Martin, J., Décary-Hétu, D., & Aldridge, J. (2017). An island apart? Risks and prices in the Australian cryptomarket drug trade. International Journal of Drug Policy, 50, 64–73.

Christin, N. (2013). Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. Proceedings of the 22nd International Conference on World Wide Web, 213–224.

Décary-Hétu, D., & Giommoni, L. (2016, 10). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime, Law and Social Change, 1–21.

Décary-Hétu, D., & Quessy-Doré, O. (2017, 10). Are Repeat Buyers in Cryptomarkets Loyal Customers? Repeat Business Between Dyads of Cryptomarket Vendors and Users. American Behavioral Scientist, 61(11).

Duxbury, S. W., & Haynie, D. L. (2017). The Network Structure of Opioid Distribution on a Darknet Cryptomarket. Journal of Quantitative Criminology, In print.

Granovetter, M. (2017). Society and economy: Framework and principles (1st ed.). Cambridge: Harvard University Press.

Hardy, R. A., & Norgaard, J. R. (2015, 9). Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. Journal of Institutional Economics, 12, 1–25.

Hughes, C. E., Bright, D. A., & Chalmers, J. (2017). Social network analysis of Australian poly-drug trafficking networks: How do drug traffickers manage multiple illicit drugs? Social Networks, 51, 135– 147.

Jacques, S., & Wright, R. (2015). Code of the suburb: Inside the world of young middle-class drug dealers. Unversity of Chicago Press.

Lewis, J., & Weigert, A. (1985). Trust as a Social Reality. Social forces, 63(4), 967–985.

Martin, J. (2014). Drugs on the dark net: how cryptomarkets are transforming the global trade in illicit drugs. Palgrave Macmillan.

Morselli, C., Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2017). Conflict Management in Illicit Drug Cryptomarkets. International Criminal Justice Review, 27(4).

Przepiorka, W., Norbutas, L., & Corten, R. (2017). Order without Law: Reputation Promotes Cooperation in a Cryptomarket for Illegal Drugs. European Sociological Review.

Sandberg, S. (2012). The Importance of Culture for Cannabis Markets: Towards an Economic Sociology of Illegal Drug Markets. British Journal of Criminology, 52, 1133–1151.

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. 24th USENIX Security Symposium (USENIX Security 15), 33–48.

Swedberg, R. (1997). New Economic Sociology: What Has Been Accomplished, What Is Ahead? Acta Sociologica, 40.

Swedberg, R., & Granovetter, M. (1992). Introduction. In M. Granovetter & R. Swedberg (Eds.), The Sociology of Economic Life (1st ed., pp. 1–26). Oxford: Westview Press.

Tadelis, S. (2016). Reputation and Feedback Systems in Online Platform Markets. Annual Review of Economics, 8(1), 321–340.

Tzanetakis, M. (2018). Comparing cryptomarkets for drugs. A characterisation of sellers and buyers over time. International Journal of Drug Policy, 56(0), 176–186.

TRADE, UNCERTAINTY AND TRUST PRODUCTION

David Décary-Hétu
University of Montréal

Masarah Paquet-Clouston
GoSecure

Laurin Weissinger
Oxford University

Trade, defined as the exchange of products and services, is an important building block of human interactions and yet, often also a risky undertaking for the parties involved. While a trade itself can be risky (Topalli et al., 2002), a variety of other concerns exist due to the non ad-hoc nature of many trades. These concerns can be summed up in one crucial question: can the other party be trusted (Schelling, 1984)?

Parties involved in a trade can seldom know their alter's motives and expectations with absolute certainty. The literature distinguishes between the "good" and "bad" types of trade parties (Gambetta, 2000). A good party is one that does not cheat or act opportunistically while a bad one does. This "good vs bad" dichotomy is a hidden property (Spence, 1974) but its veil of secrecy can sometimes be lifted to some extent by interpreting the signs and signals that trade parties showcase or broadcast. Signs are "dormant potential signals", such as tattoos and signals are intentionally displayed by an actor, such as showing the tattoo to another party (Gambetta, 2009). Usually, the greater the perceived risk, the more trust (or precautions) through reading is required.

Trust is a concept that takes different meanings depending on the author and the context. For this paper, we adopt the definition by Gambetta (1998, p.217) that is particularly functional in our case as we will be dealing with market interactions: *"a particular level of the subjective probability with which an agent assesses that another agent or group of agents will perform a particular action, both before he can monitor such action and in a context in which it affects his own actions"*

The Trust Game in an Online Setting
Economic transactions are taking place more frequently in online settings. Unsurprisingly, illicit transactions have followed the trend with online illegal markets emerging as well. Products or services such as financial fraud, spamming services, computer hacking services or identity fraud products and even drugs can now be purchased through online channels.

Yet, although offering some interesting characteristics, the anonymity feature of online illicit markets creates a high level of uncertainty for market participants. Trust is not easily produced, since any participant can act opportunistically and deceive others with high impunity (Yip et al., 2013). Moreover, the risk of unsuccessful transactions is increased by the lack of means to enforce agreements and the absence of quality control of products bought. Uncertainty underlies each trade to the point where being a victim of a fraud or a scam is a bigger threat for illicit market participants than the threat of being arrested by law enforcement (Wehinger, 2011).

Trust Production on Cryptomarkets
A cryptomarket is "a marketplace that hosts multiple sellers or 'vendors', provides participants with anonymity via its location on the hidden web and use of cryptocurrencies for payment, and aggregates and displays customer feedback ratings and comments" (Barratt & Aldridge, 2016: p.1). Anonymity is a necessary feature and is ensured with two technologies: the Tor network and the use of cryptocurrencies. In terms of trade, just like their other online illicit market counterparts, cryptomarkets have developed sophisticated features to produce trust among trading parties. These features allow vendors to broadcast trust signs and signals and consequently facilitate the transaction process while reducing its associated costs. Cryptomarket administrators have set up features that produce institution-based trust, providing information to support buyers' decision with whom to trade with (Martin, 2014). Such features are set up around the vendor's profile and provide information on the vendor's history and proven track-record. One last interesting feature that can help trust-

production on cryptomarkets are the discussion forums associated to the trading platforms. Many studies found that these forums host a living community of individuals who share a marginal sub-culture and discuss openly on drug-related subjects (Maddox et al., 2016).

Current study

For this study, the Alphabay cryptomarket, the largest market at the time of the data collection, was selected. To ensure the best model fit, we decided to limit this research to a single type of drug product sold: cocaine. We chose this product because cocaine is one of the most popular products bought on cryptomarkets, according to Soska and Christin (2015) and, contrary to cannabis, it is considered illegal at the global level.

For this study, three data collection strategies were needed to gather information from the different features offered by cryptomarkets. An automated data collection on the AlphaBay cryptomarket allowed us to gather information on vendors' past experiences. A qualitative strategy in which all listings and vendor's profiles were analyzed manually was used to assess how vendors design their online personas was used. Finally, we considered the official Alphabay forum to assess whether vendors in our sample interacted in the official forums.

The different data collection strategies allowed us to gather a diversified set of variables with the number of transactions as the outcome of our model. Each transaction is treated as a bond of trust between a vendor and a buyer. Our dependent variable is the number of cocaine sales conducted by vendors in the last month. As about 42% of the sampled vendors did not conduct any sale in the past month, our dependent variable is highly skewed to the left and follows a poisson distribution. Also, the dependent variable is overdispersed: the mean (xbar = 11.19) is much smaller than the variance (Var=602.28). Thus, the negative binomial regression is the best model, as it considers dependent variable poisson distribution while controlling for the overdispersion since the distribution parameter is a random variable. This study improves on past literature by expanding the number of variables taken into account to predict trust in online illicit markets. Most important is the vendors' profile design which was believed to play an important role in trust building but fails to reach significance in our final model.

References

Barratt, M. J., & 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.

Gambetta, D. (1998). Trust, the Social Virtues and the Creation of Prosperity.

Gambetta, D. (2000). Can we trust trust. Trust: Making and breaking cooperative relations, 13, 213-237.

Gambetta, D. (2009). Signaling. The Oxford handbook of analytical sociology, 168-194.

Maddox, A., Barratt, M. J., Allen, M., & Lenton, S. (2016). Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital 'demimonde'. Information, Communication & Society, 19(1), 111-126.

Martin, J. (2014). Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs. New York, USA: Springer.

Schelling, T. C. 1984: Strategic analysis and social problems. In Choice and Consequence, Cambridge, Mass.: Harvard University Press.

Soska, K. and N. Christin (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. Proceedings of the 23rd USENIX Security Symposium (USENIX Security'14). Washington DC: 33 - 48.

Spence, A.M. (1974). Market Signaling: Informational Transfer in Hiring and Related Screening Processes, Harvard University Press.

Topalli, V., Wright, R., & Fornango, R. (2002). Drug dealers, robbery and retaliation. Vulnerability, deterrence and the contagion of violence. British Journal of Criminology, 42(2), 337-351.

Wehinger, F. (2011, September). The Dark Net: Self-regulation dynamics of illegal online markets for identities and related services. In Intelligence and Security Informatics Conference (EISIC), 2011 European (pp. 209-213). IEEE.

Yip, M., Webber, C., & Shadbolt, N. (2013). Trust among cybercriminals? Carding forums, uncertainty and implications for policing. Policing and Society, 23(4), 516-539.