Open Secrecy: How Police Crackdowns and Creative Problem-Solving Brought Illegal Markets out of the Shadows

Isak Ladegaard, *University of Illinois at Urbana-Champaign, Monash University*

Can organized illegal activities grow stronger and more advanced in response to legal pressure? In October 2013, the FBI shut down Silk Road, a thriving e-commerce market for illegal drugs. After the shock, market actors adopted a new identity verification method that enabled mass-migration to other markets, and created websites for information distribution that reduced post-shock uncertainties. The outcome was a decentralized market in which actors could operate in "open secrecy" across multiple websites. With verifiable pseudonyms and securely obfuscated real-world identities, actors could publicly discuss, plan, and participate in illegal activities. Threats from police and opportunistic criminals persisted but were no longer crippling concerns as buyers and sellers could reasonably expect that their exchange partners would be available for future business; the illegal market could operate more like a legal one. Drawing on quantitative and qualitative data, the author argues that advances in information technology have expanded the opportunity structure for cooperation and creative problem-solving in the underworld, and therefore that shocks did not hinder but rather stimulate development in digital drug markets. Data, collected in 2013–2017, include nearly one million transactions from three illicit e-commerce markets, three million messages from eight discussion forums, and website traffic from two market-independent websites.

Introduction

During an interview with a drug dealer from the infamous Silk Road, an anonymous e-commerce market for banned goods and services, I asked if he

I'm indebted to Stephen Pfohl, Juliet Schor, Sarah Babb, Diane Vaughan, and Junghyun Kim for reading and commenting on several drafts of this paper. I also thank the reviewers for offering constructive and encouraging feedback at various stages in the submission process. Their push to focus on market order was particularly helpful. I am also grateful to Nicholas Loeper, who was an excellent research assistant as I worked on this project. This work was funded by National Science Foundation, grant #1702919. Direct correspondence to Isak Ladegaard, The School of Social Sciences, Monash University, Victoria, Australia; e-mail: isak.ladegaard@gmail.com

Social Forces 1–28
doi:10.1093/sf/soz140

ever met his customers face-to-face. He did not. "I don't talk to anyone outside of the markets or the discussion forums [and] I sell nothing offline … I have no desire to risk exposure in milieus the police might know of." For this dealer and thousands more like him, information and communication technology has created unprecedented opportunities for illegal business. Drug dealing is no longer limited to shadowy trade within personal networks or dependent on the support of criminal syndicates, and can operate on a large scale, across time and space. I argue that efforts to rein in this realm have inadvertently strengthened it in ways that have broad implications for how anonymous activities are organized and controlled.

A central challenge for contemporary sociologists is to capture the complex ways in which information and communication technology produces social change (DiMaggio et al. 2001). Does technology transform social phenomena, such as people's ability to collaborate (Benkler 2006) and organize political activism (Earl and Kimport 2011), or does it simply reproduce existing conditions (Sassen 2002), such as structural inequality (Pasquale 2015) and precarious labor (Schor et al. 2018)? These studies and their findings present a paradox: information and communication technology is a source of liberation, but it also extends existing power structures. I study the clash between these two forces. I argue that when efforts are made to restrict digitally-mediated group activities, a combination of motivated resistance and new capabilities for cooperation and creative problem-solving will produce innovative and sophisticated reorganization. To build support for this argument, I explain how actors in illegal e-commerce markets overcame police crackdowns and other shocks.

In legal markets, people have built increasingly sophisticated systems for dispute resolution (Milgrom et al. 1990; Greif 1993; Greif, Milgrom, and Weingast 1994; Landa 1994; Fligstein and Calder 2015; Stringham 2003; Okazaki 2005). Uncertainty, a problem in all markets (Beckert 2009) is no longer solved by limiting trade to personal networks. Instead, expert systems such as contracts backed by the rule of law provide institutional trust (Williamson 2000; Giddens 2013 [1990]). The dynamics differ in illegal markets, where trade either remains dependent on personal networks (Dorn et al. 2002; Anderson 1999; Gambetta 2011) or require support from powerful crime syndicates such as the Italian mafia (Arlacchi 1986, 1998). Illegal markets often adapt to internal and external constraints, for example, as sellers move off the streets (May and Hough 2004) or crime "moves around the corner" (Cornish and Clarke 1987; Guerette and Bowers 2009), but market order is frequently disrupted by legal pressure, that is, the absence of legal safeguards, and direct police interventions (Arlacchi 1998). For these reasons, contemporary illegal markets resemble pre-modern markets (Beckert and Wehinger 2012). However, with the emergence of e-commerce sites such as Silk Road, this is changing. Digital and organizational innovations mitigate legal pressure's damage to market order and foreground more conventional coordination problems (Bakken, Moeller, and Sandberg 2018). Ironically, legal pressure was central in this development.

Fligstein and McAdam (2011) argue that when exogenous shocks create destabilizing change, affected (market) actors will typically identify threats and

central challenges, propose and trial solutions, and organize new courses of action. Uncertainty fosters innovation (Pemberton 1937, Rogers 2010) as actors evaluate existing arrangements and possible alternatives (McAdam and Scott 2005). Schumpeter (1961) noted that in pressing moments, entrepreneurs often make "new combinations" of ideas that existed in their minds but that they lacked the impetus to realize (Beckert 2014). I add that technology has vastly expanded the opportunity structure for creative and collaborative problem-solving as people can spread ideas quickly and efficiently across time and space, for example, during destabilizing change, when rapid action is required.

When the FBI shut down Silk Road in 2013, they created several challenges for market users. Would they relocate? If so, how could pseudonymous buyers and sellers maintain ties? How could Jane go to a different market and trust that the seller Jasmine is the "real" Jasmine she knows from Silk Road and not an imposter? And how did they figure out where to go? I find that actors created systems for identity verification and information distribution, which enabled them to operate as nomads in a decentralized economy. This exchange structure was fragmented, but stable. Diversification across multiple websites diminished the state's ability to stop transactions, rules of exchange were no longer dictated by a single marketplace, and identity verification systems supported trade based on crowd-sourced reputation scores.

Key to the post-shock transformation of digital drug trade was the emergence of what I call open secrecy. Actors remained anonymous, or pseudonymous, but operated publicly. With identity verification and systems for information sharing they discussed (illegal) plans in public discussion forums, contributed to collective ratings of (illegal) transactions, and moved openly between different (illegal) markets, for example, as market staff created and verified seller accounts. For any market to function, actors must be able to form expectations of stable reciprocity (Beckert 2009). Such expectations are typically absent in illegal markets (Beckert and Wehinger 2012), as order is difficult to maintain without state support (Fligstein 1996). This changed with open secrecy. The digital market for drugs appears chaotic, but with newfound solutions to common disruptions, buyers and sellers knew that their trusted exchange partners could participate in future transactions, even as individual markets dissolved following police crackdowns and sudden website closures. Trade emerged from the shadows, and could operate openly, and in order.

My findings suggest that efforts to rein in digitally organized activities will stimulate organizational innovation, as motivated actors can cooperate and communicate in open secrecy. This has implications for social change and social control. Organizational innovations spill over in industries (DiMaggio and Powell 1983) and between social movements (Meyer and Whittier 1994), and ideas are also likely to travel between contested activities in cyberspace, including activism in authoritarian states, file piracy, and extremist networks.

Following a brief literature review and an overview of my research methods, I explain how market actors adopted to exogenous shocks, and how their solutions enabled decentralized trade in open secrecy. I document how buyers and sellers adopted identity verification and information distribution systems

to overcome police crackdowns and other shocks, and how these developments also solved more conventional market problems.

Technologies of Trust in Legal and Illegal Markets

All markets face issues of trust. Over time, actors have created systems for interpersonal monitoring and sharing of reputational information to settle disputes, vet potential exchange partners, and ostracize untrustworthy actors (Milgrom et al. 1990; Greif 1993; Greif, Milgrom, and Weingast 1994; Landa 1994; Stringham 2003; Okazaki 2005). Traders assessed partners based on their social distance, for example, kinship, clanship, territory, and ethnicity (Landa 1995), or formed trading coalitions to monitor conduct and thus enable trade with vetted strangers (Greif 1993). Trust remains a problem and networks are still important (Granovetter 1985), especially in uncertain situations, when many prefer to buy from kin, friends, or acquaintances (DiMaggio and Louch 1998). However, rule of law have made exchange more predictable and conflicts easier to resolve (Fligstein and Calder 2001), as enforceable rules of exchange define trading conditions, for example, rules regarding insurance and payment (Fligstein 1996).

In e-commerce markets, the distance between exchange partners introduces risk and buyers and sellers thus want mechanisms to assess trustworthiness. Initially, this problem was mitigated by networks of frequent participants (Kollock 1999), but today, e-commerce is largely impersonal, and supported by a combination of dispute resolution systems (Katsh, Rifkin, and Gaitenby 1999) and crowd-sourced reputation scores (Resnick et al. 2006). Even in uncertain situations, for example, when sellers sell products of unknown quality and exchange partners only interact once, trust can be based on records of past behavior (Diekmann et al. 2014).

Trust issues are paramount in illegal markets. The high risk of participation and the absence of rule of law make it difficult to form reproducible role structures, that is, sets of recognizable participants who occupy certain positions and routinely interact over time (Fligstein and Calder 2001). Contemporary trade of banned goods and services therefore resemble trade in pre-modern markets (Beckert and Wehinger 2012), and is distinguished not just by its legal status but also by a lack of sophistication, that is, violence as a means of conflict resolution, the failure to adopt impersonal forms for communication and distribution, and dependency on networks (Arlacchi 1998). Actors typically vet their trading partners by seeking background information and signs of insider status, limit trade to people they know, or act through trusted intermediaries (Arlacchi 1998; Anderson 2000; Paoli 2004; Gambetta 2011). Successfully established networks remain vulnerable to disruption, for example, police interventions, which force actors to relocate and reorganize (Cornish and Clarke 1987; Hubbard 1997; May and Hough 2004; Hubbard 2004; Gootenberg 2008; Guerette and Bowers 2009). In some cases, trading partners proceed with such care that the exchange structure is too small to meet the market definition (Jenkins 2001). The fragile

state of illegal markets is in sum largely due to legal pressure. That is, while states are ultimately unable to eradicate crime (Garland 1996), as actors adapt to policing efforts like in a never-ending game of cat and mouse (Marx 2003), legal pressure does hinder market growth and the formation of order (Beckert and Wehinger 2012).

Recently, however, a new market type has emerged: anonymous e-commerce of banned goods and services. The pioneering market, Silk Road, was created in 2011 by a young Texan who combined sophisticated anonymization software and cryptocurrency to protect its users. Accessing the Silk Road required The Onion Router, a program that masks IP addresses by channeling internet traffic through randomly selected and globally dispersed hubs, and all transactions were made in bitcoin, a cryptocurrency that is easy to move around online without going through banks. Silk Road and other "cryptomarkets" (Martin 2014) like it resemble conventional e-commerce sites as trade were based on reputation scores rather than personal networks, and exchange partners or market staff resolved disputes (Bakken, Moeller, and Sandberg 2018). Payments were either immediately transferred to the seller, or kept in escrow until the shipment was received (Martin 2014). Notwithstanding their sophisticated mechanisms, individual cryptomarkets are vulnerable (Soska and Christin 2015), but this has, I argue, strengthened the larger economy.

Post-Shock Reorganization and Innovation in the Darknet Economy

The Silk Road was shut down by the FBI in 2013. This was a salient moment in the formation of what I call the Darknet Economy, which is composed of cryptomarkets, and associated communities and websites (figure 1). Two other destabilizing sources emerged in the ensuing years, and both relate to the absence of legal safeguards: hacks, and exit scams (figure 2). An example of the former category was the hacking of Silk Road 2 (created shortly after the original Silk Road was shut down): market staff said in February 2014 that digital intruders stole more than $2.7 million from customers and sellers, which was possible because cryptomarket payments are typically processed and thus temporarily stored in the markets (Martin 2014). In an exit scam, market operators first facilitate trade between buyers and sellers to earn their trust and then shut down, often without notice. Early exit scams were the market website Sheep, which shut down and stole $6 million user funds in late 2013 (Greenberg 2013), and the market Evolution, which closed in March 2015 with $12 million in the bag (Woolf 2015).

The shutdown of an electronic market destroys seller profiles and aggregated reputation data, and ties between exchange partners might be cut as they are suddenly unable to communicate in the marketplace. Therefore, one might argue that actors in the Darknet Economy were, like actors in other illegal markets, restrained in their ability to create order. My findings suggest otherwise. I argue that innovations in information and communication technology have changed

Figure 1. The Darknet Economy is made up of markets and their discussion forums, but also "information hubs": market-independent websites with practical information that help actors overcome market shocks.

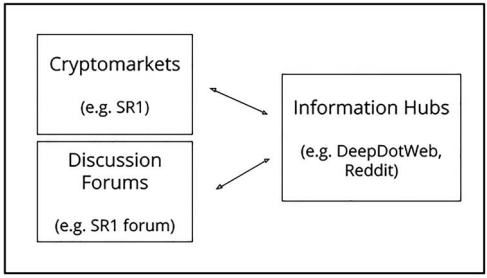
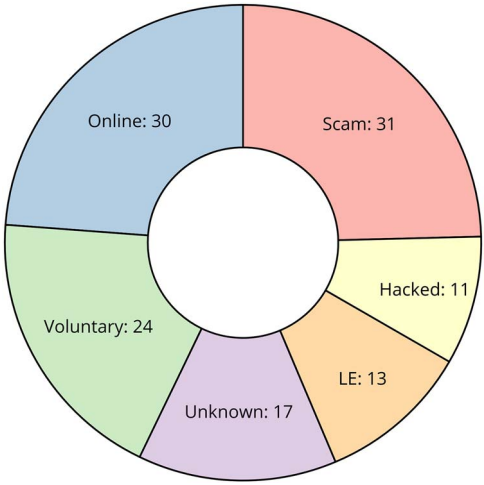


Figure 2. Markets in the Darnet Economy ($N = 126$) in the period 2011–2016. Thirty markets were online as of July 25, 2016. The rest have been closed down due to hacking, scam accusations, or following law enforcement interventions.



Note: LE = law enforcement operation. Data from Branwen (2017); DeepDotWeb (2017); and DNStats (2016).

the game for groups' ability to resist social control. Disruption stimulates creative action, and in the context of an expanded opportunity structure, market shocks will disseminate ideas and contribute to the creation of a new order.

I take three steps to build support for this argument. Drawing on qualitative and quantitative data from the Darknet Economy, I first document the emergence of a novel practice for identity verification, which enabled sellers to carry their reputation and customer base over to new websites and markets. Actors started using encryption-signing, which creates a unique link between a text phrase, an encryption code, and a username. This link can be validated by entering all data in an encryption program (any tinkering with the combination of text, code, and username and the confirmation check will fail) (for details,

see Appendix 1 in Supplementary Material). Second, I explain that people could make informed decisions about post-shock relocation due to the emergence of information hubs—independent websites that maintain detailed assessments of available cryptomarkets. Last, I will explain how these two solutions supported nomadic movement between markets, facilitated continued competition between sellers, and thus enabled a decentralized Darknet Economy to outlive individual markets.

Research Methods

Data Collection

To estimate the scale of encryption-signing, information hub activity, and seller migration, I downloaded and extracted data from key original sources using python and wget. For the encryption-signing analysis, I collected data from the discussion forums associated with five cryptomarkets: Silk Road and Silk Road 2; BlackMarket (another early cryptomarket); and the two largest cryptomarkets in 2014–2015: Agora and Evolution. I supplemented collected files with data from public archives (Branwen 2016). For the analysis of information hub activity, I collected data from three market-independent forums, and visitor data from two additional websites were shared with me by their operators. Last, I collected data on post-intervention trade and seller migration from the three largest markets after Silk Road was shut down: Silk Road 2, Evolution, and Agora. I collected these data daily, from October 2014 until September 2015. Agora lasted throughout the period, but Silk Road 2 was shut down in early November 2014, and Evolution closed in medio March 2015. (Most of these data are available at darkdata.bc.edu or upon request.)

Qualitative Analysis

To understand how and why encryption-signatures were first adopted, I monitored Silk Road and Silk Road 2's discussion forums shortly after the Silk Road marketplace was shut down (also, see Ladegaard 2019). Next, I systematically read all Silk Road and BlackMarket forum threads with an above-average frequency of encryption-signing before the same crackdown. In order to understand how actors decided which markets to relocate to before there were well-known options, I examined five information hubs: three discussion forums, and two websites with journalistic content for market users. I reviewed what information they offered, how cryptomarkets were assessed, and how forum users talked about these sites. Last, to understand how sellers were able to relocate after a crackdown, I returned to the discussion threads created immediately after the closure of Silk Road 1 and the creation of Silk Road 2. While these qualitative steps primarily preceded the quantitative steps described below, I criss-crossed between the two analytic approaches as important findings emerged.

Quantitative Analysis

I measured post-shock encryption-signing in the period 2011–2015 by counting the daily frequency of signing in the five above-mentioned discussion forums ("0" or "1" for all individual forum posts). In the Agora forum data, I removed machine-created threads that had posted hundreds of thousands of posts to promote links. I also removed two Silk Road threads devoted to encryption "training" rather than identity verification. To examine immediate and short-term effects of a shock in rates of encryption-signing, I forecasted daily rates of encryption-signing for the first four weeks after several shocks, and compared forecasted values to observed values. Following Studdert et al. (2017), I present the results as simple counts and percentages (table 1). Due to space constraints, each model covers two of the four periods I examined: (1) the first post-shock week, and (2) the first four post-shock weeks. I also measured post-shock activity in information hubs and compared observed and forecasted values.

Seller migration I quantified in two ways. To estimate movement between Silk Road 2, Evolution, and Agora, I compiled lists of seller identities in the three markets. After I determined which sellers were active in multiple markets, I calculated and compared their respective earnings. False positives are in my judgment unlikely as seller identities are policed by market operators, sellers, and customers. To estimate capital movement, I used market reviews as proxies for purchases. Because the user interface of the market websites required customers to leave reviews for their orders (Soska and Christin 2015), most trade-focused cryptomarket studies use this method (e.g., Christin 2013; Aldridge and Décary-Hétu 2014).

Forecasting with Autoregressive Integrated Moving Average

Autoregressive integrated moving average (ARIMA) forecasting models do not make causal inferences but are powerful tools for assessing interventions (Cook and Campbell 1979), for example, policy impact on firearm sales (Studdert et al. 2017) and drug use (e.g., Cunningham et al. 2008). ARIMA models forecast equally spaced univariate time series data as a linear combination of past values and errors, and adjust data for trend and seasonality if necessary, which it was in this case. I adjusted Model 1, 8, 9, and 10 for a trend of gradual, long-term increase of activity in the observation periods. I also adjusted Model 2, 7, 8, and 10 for seasonality, as website activity was high on early weekdays and low on the weekend, likely because orders were placed in time for weekend consumption. I used the R package auto.arima, which selects the most appropriate models by minimizing the AICc values (Hyndman and Khandakar 2008; Hyndman and Athanasopoulos 2018; for model details, see Appendices 2–4 in Supplementary Material.

ARIMA models typically include prediction intervals (often confused with confidence intervals), which estimate a probability range for values that are currently unknown but will be observed in the future. For example, a forecast of expected sales with an 80 percent prediction interval means that the probability

Table 1. Changes in encryption-signing after market shocks

			Post-shock encryption-signing in market forums							
			Seven days after shock (daily mean)				Twenty-eight days after shock (daily mean)			
Model #	Description	Shock	Forecast (95% PI)	Actual count	Difference, n	Difference, %	Forecast (95% PI)	Actual count	Difference, n	Difference, %
1	Silk Road forum: daily encryption-signing after Silk Road market is shut down	LE OP	7.91 (−1.12 to 16.93)	103.57	95.67	1,210.04	7.37 (−1.92 to 16.66)	31.36	23.99	325.51
2	BlackMarket forum: daily encryption-signing after Silk Road is shut down	LE OP	0.22 (−0.77 to 1.20)	29.86	29.64	13,602.38	0.15 (−0.85 to 1.14)	16.46	16.32	11,189.80
3	Agora forum: daily encryption-signing after Silk Road 2 is hacked	Hack	1.76 (−2.39 to 5.91)	15.71	13.95	894.28	1.75 (−2.43 to 5.92)	15.50	13.75	887.78
4	Evolution forum: daily encryption-signing after Silk Road 2 is shut down	LE OP	0.90 (−1.61 to 3.40)	7.29	6.39	713.43	0.89 (−1.62 to 3.40)	7.54	6.65	746.52
5	Silk Road 2 forum: daily encryption-signing after Sheep scam	Scam	31.30 (−1.52 to 64.12)	75.14	43.84	240.06	28.45 (−5.56 to 62.46)	60.33	31.88	212.06

that the actual sales will fall somewhere between the higher and lower points of the range is 0.8. Prediction intervals thus express the uncertainty of a forecast model (Hyndman 2013; Hyndman and Athanasopoulos 2018).

Findings

Valuation and Cooperation in the Darknet Economy

Buyers assess the worth of a good as a category (for example, cocaine) and in relation to other goods (A's cocaine vs. B's cocaine) (Beckert 2009). In most illegal markets, information scarcity muddles such judgments (Beckert and Wehinger 2012), but in cryptomarkets, buyers can share experiences and discuss value, while sellers can describe their products in detail (Bakken, Moeller, and Sandberg 2018) and even advertise their worth (Ladegaard 2018). In the cryptomarkets I examined, sellers labeled goods by purity ("1 g MDMA crystals purity 84%+"), origin ("0.2 g Uncut Quality Peruvian Cocaine"), corporate brand ("Oxycontin 30 mg/10 tabs Teva"), and even alleged lab test results ("5 g Pure Crystal Happiness! Lab-Tested 80% + Europe's Finest MDMA"). Quality markers were not backed by legal guarantees, however, and buyers had to have faith in market actors' intent to cooperate by reporting accurate information and by fulfilling contracts. The asymmetric information distribution also posed safety risks. Diligent buyers encrypted communication, but still had to share delivery addresses with sellers. If law enforcement somehow obtained postal addresses, for example, following the arrest of a seller, police would have to prove that the addressee was also the person who placed the order, but details on a shipment could be actionable information, for example, to obtain a warrant. Buyers were thus bound to be concerned with a seller's past conduct and seek evidence of both product value and market cooperation in customer reviews. It follows that reputable sellers had strong incentives to preserve their pseudonyms. Actors discussed various means of identity verification long before the crackdown on Silk Road, but there was no consensus on potential solutions, in part because actors believed they could depend on the market infrastructure. When the Silk Road was shut down, however, relocating actors had to establish a way to verify identities across multiple markets, and that they did.

Before the Crackdown: Identity Verification in Silk Road

Silk Road resembled conventional e-commerce platforms. A reputation system with customer feedback mitigated information asymmetry and market design reduced risk. For example, Silk Road claimed to protect buyers and sellers by encrypting and deleting their correspondences: "from the moment you submit your order, to the moment it is displayed to your vendor, the information is fully encrypted and unreadable. Then, as soon as your vendor … confirms shipment, the address is deleted forever and is irretrievable" (from Silk Road's user guide, accessed on May 13, 2013). Market staff governed cooperation between buyers and sellers by resolving disputes, enforcing rules, and responding to practical

requests. However, a discussion from June 2011 suggests that Silk Road had no system for identity verification:

> Bungalow: What prevents a scammer/law enforcement to just make a new user with some already-established name? I think there should be some form of verification.
>
> K1ngk0ng: Totally agreed! I'd think of a quick solution like: make this forum invite only.
>
> Asdf90: 100% agree. When Silk Road was temporarily down [BlackMarket] was loaded with scams using Silk Road usernames.
>
> Dread: they could use [encryption] signatures.
>
> Zen862: If you're not sure of the identity of someone here, you can always PM them on the [market] site to double check.
>
> Egoa: Some sort of code generated from Silk Road to verify a forum account sounds like a good idea.
>
> Listentothemusic: Someone stole my name on BlackMarket to scam people … I just put in [a link to] my Silk Road profile which is where I have my feedback [and] a list of all my current legitimate accounts.
>
> DigitalAlch: Well, I think this thread could solve this problem … If any one seems sketchy on here and out of character we can write it here and have another known legit vendor can verify them via encrypted msg over the PM, then post results here.
>
> G4bb3r: [encryption signature] This message verifies that I am the true g4bb3r. You can check this signature with my public key that's [on my] Silk Road profile.
>
> [Silk Road founder]: if someone is impersonating you on the forums, just let us know on the [market] site and we'll do a password reset.
>
> Alternity: Beat me to it. I was gonna reiterate, just ask the member on the other site if they're the same on the forums.

In this thread and others like it, actors noted their inability to verify identities. Two suggested encryption-signing as a potential solution, but to others, this complicated method was unnecessary because one could simply "ask the member on the other site" if they have the same username across multiple sites. Silk Road's founder agreed that adequate solutions existed, such as his own ability to delete imposters ("just let us know"). Others requested the implementation of "some sort of verification" or "screening process" in the market website, for example, "some sort of code generated from Silk Road." Encryption-signing for identity verification was just one of many options; there was no system in place.

In 2012, similar discussions were held in the forum for BlackMarket, Silk Road's sole competitor at the time. Below is an excerpt from a thread titled "Why do you need pgp [encryption]?":

> Dutchy: I don't really get it.
>
> Backopy [BlackMarket's operator]: [PGP is] used to encrypt sensitive data … so even if the server gets compromised and is sized your data remains safe.
>
> Dutchy: Aaah alright now I get it!
>
> 0xy: I'd say the main importance … is when you buy drugs and you send the seller a message containing the pick-up address along with the other details. If that's compromised, it can be used against you.

BlackMarket's operator stated that the purpose of encryption is to protect "sensitive" communication such as postal addresses, and not verifying identities.

In another BlackMarket thread, posted in late 2012, several Silk Road sellers have temporarily moved to BlackMarket due to technical problems:

> Farmer1: I am here now. Top 12% of vendors on the Silk Road, 200+ transactions, perfect feedback … Silk Road forum review thread: [url redacted]. Alternate contact info: [e-mail redacted].
>
> Deltablues: Switching from Silk Road to BlackMarket.
>
> Koltbiz: Looking forward to do great business here too!
>
> Cindelle: I too have come from Silk Road … I have no stats on here. Guess I'll have to build them!
>
> Koltbiz: I post [ed] an update … in Silk Road['s forum], just to give you guys peace of mind that I'm the real Koltbiz … [url redacted].

Out of dozens of posters in the same thread, several Silk Road sellers confirmed their identities by sharing e-mail addresses and updating their forum pages. Only one used encryption-signing. Like Silk Road, BlackMarket had no established system for identity verification. Encryption-signing was introduced in the 1990s (Zimmermann 1995), so the point is not that the technology was unavailable. The point is that new ideas can take years to be adopted, even if the advantages are obvious, and it is only when they are adopted they are consequential. Innovation is not just eureka-moments in which new ideas are conceived, innovation is also about disseminating and putting existing ideas to work (Rogers 2010). Encryption-signing did not converge with illegal e-commerce until the Silk Road was shut down by the FBI in 2013.

Identity Verification after the Crackdown on Silk Road

When the Silk Road was shut down, persevering actors had to relocate. Sellers could sign up for alternative cryptomarkets with their Silk Road usernames and hope that customers would follow them and remember them, but how would customers know that they were really dealing with reputable sellers from Silk Road, and not opportunistic imposters or undercover police?

Immediately after the market shutdown, identity verification was one of several pressing problems under discussion in Silk Road's forum, which remained

online for several months (presumably because it was hosted on different servers). One of the most active threads on the day of the shutdown was titled "Vendors post your contact info here," which was created by a buyer who tried to get in touch with sellers. A total of thirteen sellers shared their contact information in that thread on the same day, and eight encryption-signed their messages. This suggests that market actors needed an impetus to start using encryption-signing. One of the signees was "Al Capone": "Well established vendor with 100% satisfaction … Contact me through PM or [email redacted]. Long live Silk Road! [encryption signature redacted]." Because he posted his encryption signature, customers could verify his identity and email address.

In the excerpt below, "Technohippy," a former Silk Road seller, was verified as the "real" Technohippy in a newly created Silk Road 2 marketplace.

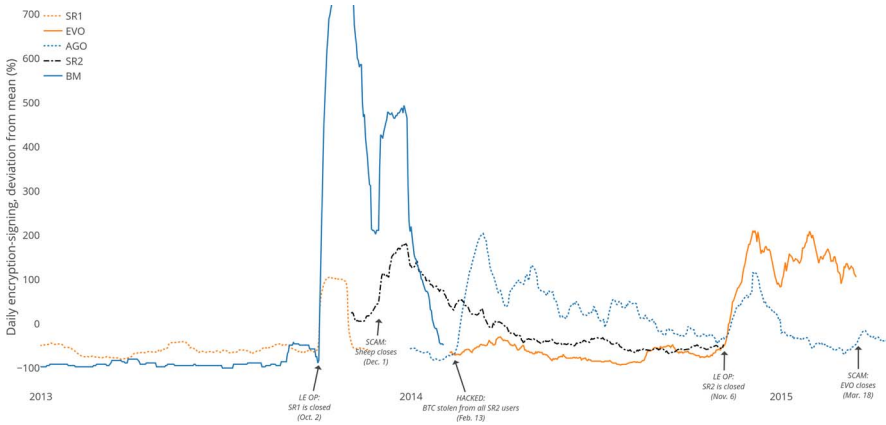
> Technohippy2.0: Just to let everyone know, technohippy username on the [forum] has been stolen I will be putting in a request for it to be retrieved however I am on there at the moment as technohippy2.0. I am not verified yet but as soon as we are we will be back with even more products than before. I have also seen a few posts popping up claiming that we were the other UK guys arrested … we have not been arrested we have just remained under the radar.
>
> Knuckles: Welcome back! Glad to hear you didn't get busted!
>
> Charliesheen1080: Technohippy you motherfucking legend!!!!! So glad to see you back.
>
> Rocknessie: I am SO FUCKING DELIGHTED you weren't busted.
>
> LevelHead: Very happy to see you back Technohippy.
>
> Sarge [market staff]: [posts encrypted message using Technohippy's public PGP key].
>
> ILTC: Welcome back Technohippy. Sarge, please let us know when he has been verified.
>
> Sarge [market staff]: Yes verified. He decrypted the PGP message I sent him.

Technohippy reclaimed the original username, disproved rumors, and gained customer trust. He/she/they continued to sell in at least three other cryptomarkets with the old Silk Road username, and earned at least $447,500 in Silk Road 2, $191,500 in Evolution, and $118,300 in Agora.

Shortly after Silk Road 2 launched, market staff conducted a similar but systematic encryption-verification of sellers from the original Silk Road. Below are excerpts from two threads titled "Accessing the vendor roundtable."

> [Market staff 1]: To all former Silk Road vendors, we will be providing you free vendor accounts on the new marketplace … users can message me in either a private message or post below, signing a message with their [encryption] key and I will fully reinstate your access … Please note you must … sign using the same [encryption] key as published on the previous Silk Road forums as we will be using this to verify you are who you claim to be for security purposes.

Figure 3. Daily encryption-signing in five cryptomarket forums.



Note: LE OP = law enforcement operation. "Deviation from mean" refers to the percent difference between the daily and mean frequency of encryption-signing in the source (e.g., Silk Road's forum) for all available time points, which enables easy visual comparison of encryption-signing in different forums.

> . . . [232 replies in the period Oct. 7-Dec. 2 2013, excluding posts from market staff].
>
> [Market staff 2]: If you do not have access to the old Silk Road forums, or did not post your [encryption key] on the old forums, don't bother PMing me asking for verification . . . We can not open the door to everybody.

Silk Road 2 staff verified at least 138 sellers from the original Silk Road market in the two threads, and possibly far more in private communications.

I counted encryption-signing in five cryptomarket forums in the period 2011–2016 and found that it surged after three types of shocks—police interventions, hacks, and scams—and particularly after the FBI shut down Silk Road in October 2013 (figure 3). A reversion to the mean in the weeks and months following each type of shock suggests that identity verification was typically a one-time event, for example, as a sellers requested to join a new market, and were asked to verify their reputable usernames.

ARIMA models confirm the pattern in figure 3: encryption-signing surged after major shocks in the economy (table 1; Appendices 2–4 in Supplementary Material), most notably in the Silk Road forum and BlackMarket forum, shortly after Silk Road was shut down by the FBI (Models 1 and 2). The forecasted rate of encryption-signing in the Silk Road forum, for the first seven days after the crackdown, was 7.91 per day. Observed encryption-signing in the same seven-day period was much higher at 103.57 per day in the first week and 31.36 per day in the first four weeks. The drop suggests that buyers and sellers acted quickly. The post-crackdown increase in encryption-signing was even steeper in the BlackMarket forum, most likely because BlackMarket was, at the time,

the only established alternative market to Silk Road. The forecasted rate of encryption-signing for the first week after the crackdown was 0.22 per day, while the observed rate was 29.86 per day. For the first four weeks, the tally was 16.46 per day. Encryption-signing also increased in the Agora forum after the hack of Silk Road 2 in medio February 2014 (Model 3). Forecasted rates of encryption-signing for the first post-hack week was 1.76 per day, while observed encryption-signings was 15.71 per day for the first week, and 15.50 per day for the first four weeks. One possible reason the two spikes were smaller than in Models 1 and 2 is that Silk Road 2 continued to operate despite the hack, and therefore gave users time to consider their options. The Silk Road 2 shutdown was also followed by a surge in encryption-signing in Evolution's forum (Model 4), which suggests some movement between the markets. The forecasted rate of encryption-signing was 0.90 per day for the first week, while the observed rate was 7.29 per day for the first week and 7.54 per day for the first four weeks. When the cryptomarket, Sheep exit-scammed in early December 2013, encryption-signing increased in the forum associated with Silk Road 2 (Model 5). Encryption-signing for the first week was forecasted at 31.30 per day, while the observed rate was 75.14 per day for the same period, and 28.45 per day for the first four weeks. The drop after week 1 suggests that Sheep users reacted quickly, just as Silk Road and BlackMarket users did (Models 1 and 2). In sum, the ARIMA models show that encryption-signing spiked after market shocks.

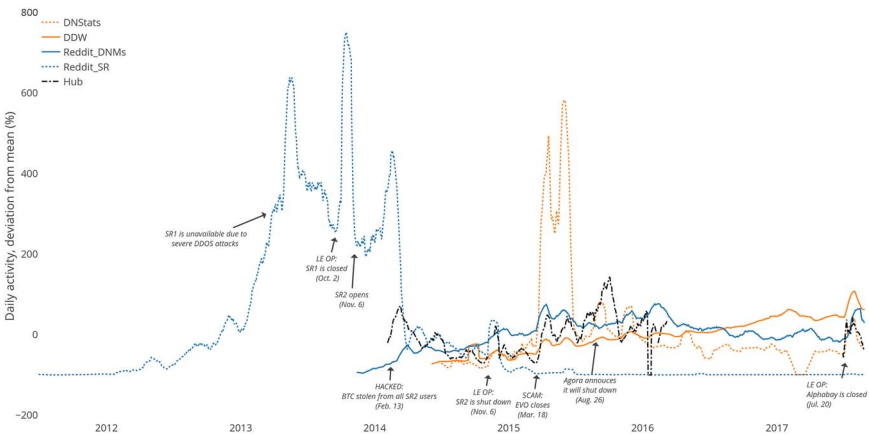
Competition: Information Hubs

Competition is typically inefficient in banned and opaque markets (Beckert and Wehinger 2012). In the Darknet Economy, however, competition is structured by information hubs, that is, independent websites that provide detailed assessments of available cryptomarkets and related information. Evidence suggests that information hubs were created to assuage post-shock uncertainties. The blog DeepDotWeb, created in 2013 "in the wake of our friend being arrested by local authorities," aimed to make "the dark net safer." The site produced more than 2,500 articles (August 2017), and had in the period May 2014 to September 2017 more than 23,000 unique daily visitors. Another information hub, DNStats, specialized in automated testing of market uptime. It was created because the founder "was always seeing people wanting to know when a site went down, how long has it been down and when did it come back up." DNStats had in the period June 2014 to September 2017 more than 5,500 daily visitors. Reddit's section for Silk Road and Silk Road 2 had more than 24,000 subscribers who wrote more than 122,000 comments, mostly in the years 2013–2015. A Reddit page for all cryptomarkets was created about two weeks after Silk Road was shut down. It maintained a FAQ page, an oft-updated list of available cryptomarkets, had nearly 160,000 subscribers, and more than 1.1 million public comments (October 2017). The Hub, an "Unbiased Forum for Users of Every Marketplace," was introduced a little more than three months after Silk Road was closed. "We've had it rough, and we've seen it all," explained staff in their introduction to the site. "From falling victim to scams and dishonesty,

to seeing our brothers arrested and our digital homes torn apart. With all of this happening, we felt the need to build something that would bring stability, continuity and guided decision-making to our community." Between 2014 and 2017, users of the Hub wrote 190 posts per day.[1] Activity in these information hubs surged after market shocks (figure 4). Cryptomarket actors also shared information in market-specific forums, and in the period 2011–2015, users in the forums for Silk Road, BlackMarket, Silk Road 2, Evolution, and Agora wrote nearly three million posts.

Post-shock traffic in information hubs surpassed all ARIMA forecasts (table 2; Appendices 2–4 in Supplementary Material), especially following the Silk Road 2 shutdown and Evolution's exit scam (many of the examined information hubs were not available when the FBI shut down the original Silk Road). For DeepDotWeb, the forecasted number of unique visitors surged after Silk Road 2 was shut down by the FBI (Model 6). In the first post-shock week, the forecasted tally of unique visitors was 8,480 per day, while the observed number of visitors was 16,699 per day for the same week, and 12,888 per day for the first four weeks after the crackdown. DNStats also had more visitors after the Silk Road 2 shutdown (Model 7). The forecasted number of visitors for the first week was 1,299 per day, while the observed values for the same period were 6,336 per day, and for the first four weeks, 3,635 per day. Activity on Reddit's page for Silk Road users increased after the market was shut down (Model 8). The logged per-day forecast for the first week after the shutdown was 5, but the observed tally of posts for the same week was 7. In the four weeks following the shutdown, the activity decreased drastically, likely because users had an alternative Reddit page to go to. The forecasted number of Reddit posts for the first week was 225 per

Figure 4. User activity in five Information Hubs.



Note: "Deviation from mean" refers to the difference, in percent, between the daily activity score and mean activity score for the entire time period, for each individual website. Data are presented this way to visualize a comparison of encryption-signing in different forums. In the ARIMA models, raw data are used instead of mean scores.

day, while the observed number of posts was 287 per day in the first week, and 407 per day in the first four weeks. The increase in activity after the first week is possibly due to post-hack developments as Silk Road 2 staff struggled to pacify market actors, for example, by pledging to repay lost funds. Reddit activity also increased after Evolution's exit scam was confirmed (Model 10). For the first week, the forecast was 876 posts per day, while the number of actual posts was 1,769 per day in the first week and 1,335 in the first four weeks.

Shocks frequently interrupted trade in the Darknet Economy, but with information hubs, relocating actors could make informed decisions. They could look up market lists and compare market features, and observe or partake in relevant forum discussions. With encryption-signing and access to information, actors could migrate—with intact pseudonyms—to the "best" cryptomarkets currently available. The clustering of established sellers enabled competition, and the emergence of new "top" markets created order.

Post-Shock Trade and Nomadic Seller Movement

The Darknet economy continued to grow in its early years, despite being hit by shocks. Silk Road's monthly revenue was $1.22 million in 2012 (Christin 2013) and $7.48 million a year later (Aldridge and Décary-Hétu 2014). I estimate that in the fall of 2014, about a year after the FBI crackdown on Silk Road, combined seller revenue in Silk Road 2 was $6.37 million per month. After another FBI operation shut down Silk Road 2, trade continued in Evolution and Agora, where combined monthly seller revenue was $8.49 million and $10.45 million (figure 5). Media attention might explain some of the increase (Ladegaard 2017). For this study, it is important to note that sellers who overcame the crackdowns by operating across multiple markets drove most of the trade. Newfound systems for identity verification and information sharing created a market order that survived multiple shocks.

Multi-market sellers—sellers who maintained accounts in both Evolution and Agora throughout the data-collection period—accounted for a majority of trade in the two markets and earned notably more than single-market sellers (figure 6), even though there were fewer of them (909 vs. 2,843). Movement after Silk Road 2 shut down illustrates how cryptomarket sellers relocated: migrating Silk Road 2 sellers remained active for a mean of 105 days in Evolution, which shut down in March 2015, and 167 days in Agora, which shut down in September 2015 (many sellers likely continued in other cryptomarkets). The mean monthly revenue for each Silk Road 2 seller who continued in Evolution was $4,600, while Silk Road 2 sellers who continued in Agora earned $8,900 per month (in part because the market lasted longer). In total, about a quarter of all Silk Road 2 sellers continued in two or more markets (figure 7).

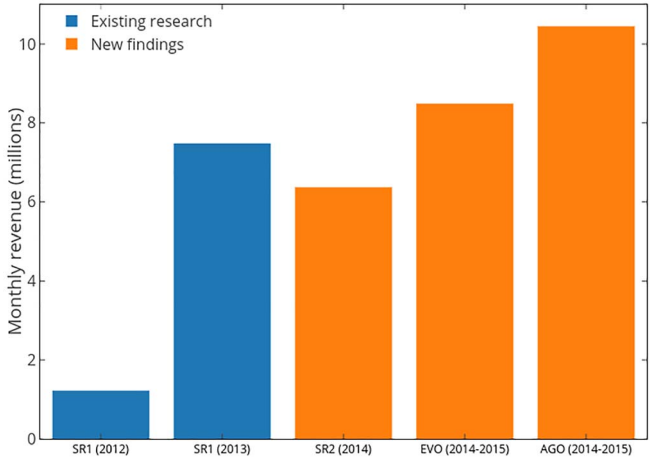
Shocks likely incurred substantial costs for sellers, as payments were canceled and future earnings reduced. Technohippy, for example, decided to "lay low" for several weeks after the FBI shut down Silk Road, a period that could have generated income. However, Technohippy and many other sellers learned to operate nomadically and were no longer dependent on individual markets. In

Table 2. Information hub activity after market shocks

			Post-shock activity in information hubs							
			Seven days after shock (daily mean)				Twenty-eight days after shock (daily mean)			
Model #	Description	Shock	Forecast (95% PI)	Actual count	Difference, n	Difference, %	Forecast (95% PI)	Actual count	Difference, n	Difference, %
6	DeepDotWeb: daily visitors after Silk Road 2 is shut down	LE OP	8,480.21 (−17,026.61 to 33,987.03)	16,698.86	8,218.65	96.92	8,481.35 (−17,069.84 to 34,032.54)	12,887.68	4,406.33	51.95
7	DNStats: daily visitors after Silk Road 2 is shut down	LE OP	1,298.96 (−651.03 to 3,248.94)	6,336.00	5,037.04	387.78	1,390.23 (−648.25 to 3,428.71)	3,635.32	2,245.09	161.49
8	Silk Road subreddit: daily posts after the Silk Road is shut down[a]	LE OP	5.48 (4.40 to 6.56)	6.72	1.24	22.54	5.57 (4.37 to 6.77)	5.67	0.10	1.88
9	DNMs subreddit: daily posts after Silk Road 2 hack	Hack	225.01 (117.84 to 332.19)	287.14	62.13	27.61	220.04 (89.81 to 350.28)	406.79	186.74	84.87
10	DNMs subreddit: daily posts after Evo exit-scams	Scam	876.41 (629.41 to 1,123.41)	1,769.00	892.59	101.85	883.86 (609.37 to 1,158.36)	1,334.71	450.85	51.01

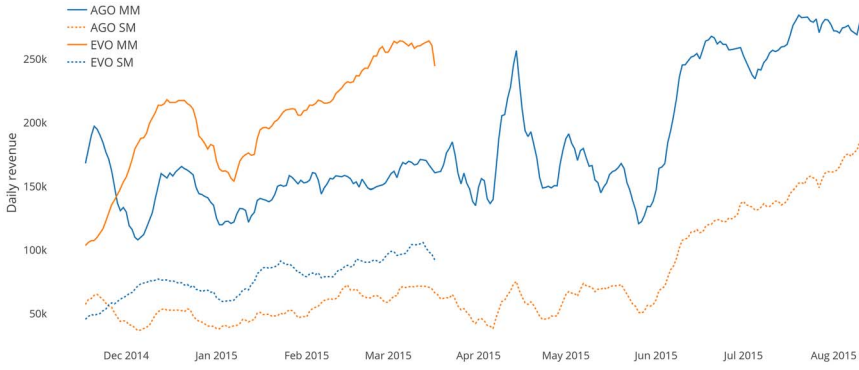
Note: PI = prediction interval; LE OP = law enforcement operation.
[a]Logged.

Figure 5. Monthly cryptomarket revenue (U.S. dollars). Trade continued after SR1 was shut down in October 2013, and after SR2 was shut down in November 2014. Year of data collection in brackets.



Note: *Christin (2013). **Aldridge and Décary-Hétu (2014).

Figure 6. Daily vendor revenue (14-day moving average). Agora and Evolution's multi-market vendors (full lines) outperform single-market vendors (dotted lines), both after the FBI shut down Silk Road 2 (November 2014) and after Evolution's "exit scam" (March 2014).

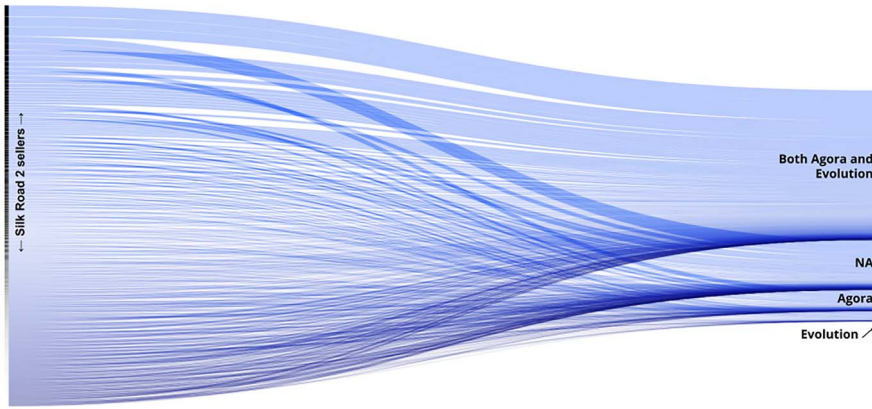


fact, many of the cryptomarkets and information hubs discussed in this study have been shut down, but they have been replaced, and trade continues (Popper 2019).

Discussion

In 2017, following another cryptomarket crackdown, the FBI's deputy director stated: "Our critics will say as we shut down one site another site emerges. And they may be right. But that is the nature of criminal work. It never goes away,

Figure 7. Silk Road 2 sellers continued trade in other markets. Each line represents a seller who was active in Silk Road 2 in the 19 days preceding its shutdown. Most of the 573 sellers continued in Agora (85) or Evolution (36), or both (267). The "NA" category includes sellers who did not relocate to Agora or Evolution under the same name (185). Line thickness reflects sellers' revenue in Silk Road 2 in the 19-day period.



Note: Sellers are ordered by their Silk Road 2 revenue in the 19 days preceding the crackdown (high revenue = thick line). For reference, the top seller earned $71,500 in the 19-day period, the seller at the bottom earned $1.

you have to constantly keep at it" (Farivar 2017). The remarks align with the classical argument that although law enforcement is unable to eradicate crime (Garland 1996), police pressure lowers incidence rates, pushes crime "around the corner" (Guerette and Bowers 2009), and most importantly, restricts market development (Arlacchi 1998). Beckert and Wehinger (2012) observe that while all markets are fundamentally alike in that buyers and sellers strive to coordinate their activities, illegal markets are shackled because they must operate "in the shadow." Product valuation is difficult to establish due to information scarcity, "competition is deficient," and cooperation problems "inhibit efficient organizational size and information flows." These issues "impair enlargement," in part because trust between exchange partners can only be established in "limited locations and cannot be easily extended" (p. 21). Trade in the Darknet Economy is undoubtedly affected by legal pressure. Exogenous shocks burden market actors with liabilities of newness (Stinchcombe 2000): attempts to reorganize trade in new ways risk failure because structures are unstable, legitimacy is low, and better-known alternatives—for example, offline trade—might seem more reliable. Moreover, sophisticated anonymization technology will not prevent human error, which preceded several police crackdowns, including the one that brought down the original Silk Road (Ladegaard 2017). However, newfound means for collaboration and innovation have unsettled the longstanding whack-a-mole dynamic of crime and control, which the FBI deputy alluded to. In the

Darknet Economy, individual buyers and sellers learned to solve coordination problems on their own, at the expense of law enforcement, and thus trade circumvented many of the obstacles observed by Beckert and Wehinger (2012). Digital drug trade transformed into a decentralized economy with effective information flows and nomadic actors; not despite legal pressure, but because of it.

Information and communication technology has expanded the opportunity structure for creative problem-solving and rapid mass-communication of ideas, and in this context, exogenous shocks such as law enforcement crackdowns on motivated actors will stimulate innovation, movement, and action. Uncertainty diffuses ideas (Pemberton 1937; Rao, Morrill, and Zald 2000) as people are in such moments more receptive to alternative ways of doing things, especially when threats to group interests mobilize individual action and organizational resources (Fligstein and McAdam 2011). The three-step process of threats, uncertainty, and change was evident when actors in the Darknet Economy scrambled to establish systems for identity verification in the aftermath of the crackdown on Silk Road, and when they figured out how they could operate nomadically. Actors made "new combinations" of existing ideas, and such combinations often exist solely in the minds of entrepreneurs and remain there, unrealized, until people are enticed away from risk aversion and inactivity (Schumpeter 1961; Beckert 2014), such as in moments of destabilizing change, when action is required. In a reminder of how purposeful social action can have unintended consequences (Merton 1936), legal pressure inadvertently created an illegal market that could operate more like a legal market. Shocks became predictable and manageable, and thus not that shocking, and actors could expect stability as trade would continue even in the face of major market shutdowns. Buyers and sellers gained the capacity to protect themselves and solve their own coordination problems. They no longer traded in the shadows, but in open secrecy.

An organization's capacity for deviance is typically dependent on its opportunities for "structural secrecy," that is, the way information patterns, organizational structure, processes, and transactions "systematically undermine the attempt to know and interpret situations" (Vaughan 1996: 238). Open secrecy is a paradoxical variant. In the Darknet Economy, actors are pseudonymous and thus secret, but they could coordinate trade, in public, across time and space. With identity verification and information hubs in place, actors openly discussed their practical problems in forums, their illegal transactions were documented by customer reviews, and their movements were also hidden in plain sight, for example, as pseudonymous sellers advertised their intentions to relocate, and verified themselves in new markets. When markets were shut down, users could read up on alternatives, or simply ask their forum peers, "where are you guys going now?" Collective post-shock mobilization and reorganization in anonymity was possible because of open secrecy.

Organizational innovations spread, for example, as entrepreneurs bring already-existing ideas to untapped markets (Schumpeter 1961) or as firms innovate in response to emerging challengers (Fligstein and McAdam 2011). The Darknet Economy resembles in certain respects the file piracy sector,

which also decentralized and transformed in response to legal pressure (e.g., from Napster to BitTorrent). Like sellers in the Darknet Economy, prominent providers of stolen media content earned community reputation (e.g., for audio quality), and often operated with consistent pseudonyms or team identities (Witt 2015). Moreover, research on file piracy has argued that actors adopted advanced anonymization tools in response to increased policing efforts (Larsson and Svensson 2010), much like the Silk Road shutdown triggered organizational change in the Darknet Economy. One key difference between the two worlds is that file piracy users do not risk much by downloading from unverified providers, and thus providers rarely required the kind of identity verification that is essential in the Darknet Economy. My point here is that the "new combination" of anonymity and verifiable identity is a powerful and liberating force that might be adopted by other groups and actors who operate in secrecy and require verification methods for public communication. For example, a central problem for social movements in authoritarian states is the vulnerability of key organizers. If organizers are anonymous, and use verifiable pseudonyms to spread messages across multiple platforms, their communications will be hard to stop. Certainly, encryption software has already been used to protect communication within groups that operate in the shadows, but to my knowledge, mass-communication in open secrecy is rare, probably in part because few know of the possibility, and because of the learning curve (Appendix 1 in Supplementary Material). However, my findings suggest that if motivated actors are pressed to act, mass-adoption of innovative tools may follow.

Another potential spillover area is organized crime. Evidence from the "El Chapo" trial suggests that cartels already embrace encryption technology (Feuer 2019), and if criminal syndicates create cryptomarkets that are maintained by professional developers and maybe even backed by state actors in the manner Afghan opiate crops are taxed by the Taliban (UNOCD 2017), commissions will generate substantial profits, and thus indirectly add to their political and military capital. This is a sobering paradox: innovations that enable illegal market trade without the backing of criminal syndicates might end up largely benefiting such groups.

Currently, the Darknet Economy is a drop in the ocean in the overall market for banned drugs. Why? Possibly because few are aware of cryptomarkets, or because they are framed as failing projects, or because they are considered too complicated for most. However, evidence suggests that the economy is growing, and trade might expand to other profitable products and services, and thus might create other types of harm. Rare animal parts are sold (Wright 2019) in the darknet, and so are hacker services, pirated software, stolen credit card information, firearms, social media "likes" and "followers," identity documents, and even forged discount coupons. Drug trade dominates in the Darknet Economy, partly due to demand and practical matters, but the social harm of illegal goods and services is not a purely quantitative measure. A forged passport and an automated rifle can be far more destructive than 10,000 shipments of cannabis.

Conclusion

Encryption-signing for identity verification has been freely available since the early 1990s, and information hubs draw on existing opportunity structures such as web-hosting services, web-design templates, and presumed free speech protection. It seems improbable that Silk Road would have continued indefinitely, even if law enforcement was evaded, considering the frequency of other shocks, and actors might have developed identity verification systems and information hubs for market migration even if Silk Road remained online, for example, if overwhelming demand limited access. However, evidence suggests that mass-adoption of encryption-signing was triggered by the FBI's intervention in the Darknet Economy in October 2013, when Silk Road's buyers, sellers, and staff members were evicted. Information hubs were also, in the words of their founders, created in response to law enforcement interventions and related uncertainties.

Actors in the Darknet Economy created sophisticated solutions for common coordination problems. These efforts in turn supported a surprisingly stable environment that enabled trade to operate more like it does in legal markets. But this is not an evolution: illegal markets are unlikely to ever catch up with legal markets, in which participants and the state work together to create stable worlds of exchange. Rather, attempts to create orderly conditions for illegal trade are likely to go in novel directions, as actors face unique organizational challenges. Consider, for example, that all trade measured in this study was conducted in bitcoin, which until recently was an unknown digital commodity and certainly has not been implemented on a similar scale in legal e-commerce. That is not to say that illegal markets offer glimpses of the future, but we should abandon the view that illegal markets are unsophisticated and most resemble pre-modern trade.

Illegal markets are alternative worlds of economic exchange, and studying them might generate theoretical insights (Beckert and Wehinger 2012). One insight from this study is that legal pressure creates a distinct impetus for creative action. In legal markets, innovation primarily stems from entrepreneurs and firms who try to fend off competition, but in illegal markets, legal pressure compels operators, buyers, sellers, and all other market actors to contribute to reorganization, by participating in problem-solving, by disseminating ideas, or by adopting newfound solutions (e.g., learning encryption). That is, illegal markets require a degree of commitment that is unusual in legal markets, and this is the central difference between them. Navigating illegal trade has always demanded particular forms of cultural capital, and this undoubtedly discourages casual buyers and sellers and encumbers collective action. However, committed market actors can now communicate and cooperate across time and space, in open secrecy, and in the case of the Darknet Economy, their combined innovative force overcame legal pressure and created a new market order. Drawing on this finding, I have argued that information and communication technology has changed the game for illegal markets, and at large, organized illegal activities. Shocks such as police crackdowns will under certain circumstances not impair

development, but rather challenge actors to make new combinations that will disseminate quickly and widely, in open secrecy.

Notes

1. Excluding periods with downtime.

About the Author

Isak Ladegaard is Assistant Professor of Sociology at the University of Illinois at Urbana-Champaign. He obtained a Ph.D. in sociology at Boston College, and prior to joining University of Illinois in 2020, was a Lecturer at Monash University, Australia. His research interests include technology and social change, economic sociology, and crime and deviance.

Supplementary Material

Supplementary material is available at *Social Forces* online, http://sf.oxfordjournals.org/.

Acknowledgements

I'm indebted to Stephen Pfohl, Juliet Schor, Sarah Babb, Diane Vaughan, and Junghyun Kim for reading and commenting on several drafts of this paper. I also thank the reviewers for offering constructive and encouraging feedback at various stages in the submission process. Their push to focus on market order was particularly helpful. I am also grateful to Nick Loeper, who was an excellent research assistant as I worked on this project.

Funding

National Science Foundation, grant #1702919.

References

Aldridge, Judith and David Décary-Hétu. 2014. "Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation." Available at SSRN 2436643.

Anderson, Elijah 2000. *Code of the street: Decency, violence, and the moral life of the inner city*: WW Norton & Company.

Arlacchi, Pino 1986. *Mafia Business: The Mafia Ethic and the Spirit of Capitalism* Vol. 3. London: Verso.

Arlacchi, Pino 1998. "Some Observations on Illegal Markets." *The New European Criminology: Crime and Social Order in Europe* 203–15.

Bakken, Silje A., Kim Moeller, and Sveinung Sandberg. 2018. "Coordination Problems in Cryptomarkets: Changes in Cooperation, Competition and Valuation." *European Journal of Criminology* 15 (4): 442–60.

Beckert, Jens. 2009. "The Social Order of Markets." *Theory and Society* 38 (3): 245–69.

Beckert, Jens. 2014. "Capitalist Dynamics: Fictional Expectations and the Openness of the Future." Available at SSRN 2463995.

Beckert, Jens and Frank Wehinger. 2012. "In the Shadow: Illegal Markets and Economic Sociology." *Socio-Economic Review* 11 (1): 5–30.

Benkler, Yochai 2006. *The wealth of networks: How social production transforms markets and freedom*: Yale University Press.

Branwen, Gwern. 2016. "Dark Net Market Archives, 2011-2015." Accessed June 10. https://www.gwern.net/DNM%20archives.

Branwen, Gwern. 2017. "Darknet Market Mortality Risks." gwern.net/DNM%20survival.

Campbell, Donald Thomas and Thomas D. Cook 1979. *Quasi-experimentation: Design & analysis issues for field settings*. Chicago: Rand McNally College Publishing Company.

Christin, Nicolas. 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*. ACM, 213–224.

Cornish, Derek B., and Ronald V. Clarke. 1987. "Understanding crime Displacement: An Application of Rational Choice Theory." *Criminology* 25 (4): 933–948.

Cunningham, James K., Lon-Mu Liu, and Myra Muramoto. 2008. "Methamphetamine Suppression and Route of Administration: Precursor Regulation Impacts on Snorting, Smoking, Swallowing and Injecting." *Addiction* 103 (7): 1174–1186.

DeepDotWeb. 2017. "Updated List of Dark Net Markets." Accessed August 7. https://bit.ly/2YTlh0y.

Diekmann, Andreas, Ben Jann, Wojtek Przepiorka, and Stefan Wehrli. 2014. "Reputation Formation and the Evolution of Cooperation in Anonymous Online Markets." *American Sociological Review* 79 (1): 65–85.

DiMaggio, Paul and Hugh Louch 1998. "Socially Embedded Consumer Transactions: For What Kinds of Purchases do People Most Often use Networks?" *American Sociological Review* 619–37.

DiMaggio, Paul J. and Walter W. Powell 1983. "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." *American sociological review* 147–60.

DiMaggio, Paul, Eszter Hargittai, W. Russell Neuman, and John P. Robinson. "Social Implications of the Internet." *Annual review of sociology* 27, no. 1 (2001): 307–336.

Dorn, Nicholas, Karim Murji and Nigel South 2002. *Traffickers: Drug markets and law enforcement*: Routledge.

DNStats, Market Comparison n.d. Web. 03 Apr. 2016. dnstats.net/market-comparison.

Earl, Jennifer and Katrina Kimport 2011. *Digitally Enabled Social Change: Activism in the Internet Age*: MIT Press.

Farivar, Masood 2017. "International Sting Hits Dark Web's Promise of Anonymity." VOA." Accessed September 20. https://bit.ly/2f6C8Mr.

Feuer, Alan. 2019. *Drug Kingpin Used Spyware to Monitor His Wife and Mistress, Jurors Told*. The New York Times. https://nyti.ms/2H6s57y.

Fligstein, Neil, and Doug McAdam. "Toward a general theory of strategic action fields." *Sociological theory* 29, no. 1 (2011): 1–26.

Fligstein, Neil 1996. "Markets as Politics: A Political-Cultural Approach to Market Institutions." *American Sociological Review* 656–73.

Fligstein, Neil and Ryan Calder 2015. "Architecture of Markets. Emerging Trends in the Social and Behavioral Sciences: An Interdisciplinary, Searchable, and Linkable." *Resource* 1–14.

Fligstein, Neil, and Doug McAdam. "Toward a General Theory of Strategic Action Fields." *Sociological theory* 29, no. 1 (2011): 1–26.

Gambetta, Diego 2011. *Codes of the Underworld: How Criminals Communicate*: Princeton University Press.

Garland, David. 1996. "The Limits of the Sovereign State Strategies of Crime Control in Contemporary Society." *The British Journal of Criminology* 36 (4): 445–471.

Giddens, Anthony 2013. *The Consequences of Modernity*: John Wiley & Sons.

Gootenberg, Paul 2008. *Andean Cocaine: The Making of a Global Drug*: University of North Carolina Press.

Greenberg, A. 2013. Silk Road Competitor Shuts Down And Another Plans To Go Offline After Claimed $6 Million Theft. Retrieved from https://www.forbes.com/sites/andygreenberg/2013/12/01/silk-road-competitor-shuts-down-and-another-plans-to-go-offline-after-6-million-theft/#42958c407e08.

Greif, Avner 1993. "Contract Enforceability and Economic Institutions in Early Trade: The Maghribi Traders' Coalition." *The American Economic Review* 525–48.

Greif, Avner, Paul Milgrom, and Barry R. Weingast. 1994. "Coordination, Commitment, and Enforcement: The Case of the Merchant Guild." *Journal of Political Economy* 102 (4): 745–776.

Granovetter, Mark. "Economic Action and Social Structure: The Problem of Embeddedness." *American journal of sociology* 91, no. 3 (1985): 481–510.

Guerette, Rob T., and Kate J. Bowers. 2009. "Assessing the Extent of crime Displacement and Diffusion of Benefits: A Review of Situational Crime Prevention Evaluations." *Criminology* 47 (4): 1331–1368.

Hubbard, Phil. 1997. "Red-Light Districts and Toleration Zones: Geographies of Female Street Prostitution in England and Wales." *Area* 29 (2): 129–140.

Hubbard, Phil. 2004. "Cleansing the Metropolis: Sex Work and the Politics of Zero Tolerance." *Urban Studies* 41 (9): 1687–1702.

Hyndman, Rob J. 2013. "The Difference Between Prediction Intervals and Confidence Intervals." *Hyndsight*. Accessed January 17. https://bit.ly/2xKO9gz.

Hyndman, Rob J. and George Athanasopoulos 2018. *Forecasting: Principles and Practice*: OTexts.

Hyndman, Rob J. and Yeasmin Khandakar 2008. "Automatic Time Series Forecasting: The Forecast Package for R." *Journal of Statistical Software* 26:1–22.

Jenkins, Philip 2001. *Beyond Tolerance: Child Pornography on the Internet*: New York City, NY: NYU Press.

Katsh, Ethan, Janet Rifkin and Alan Gaitenby 1999. "E-commerce, E-disputes, and E-dispute Resolution: In the Shadow of eBay Law." *Ohio St. J. on Disp. Resol.* 15:705.

Kollock, Peter. 1999. "The Production of Trust in Online Markets." *Advances in Group Processes* 16 (1): 99–123.

Ladegaard, Isak. 2017. "We Know Where You Are, What You Are Doing and We Will Catch You: Testing Deterrence Theory in Digital Drug Markets." *The British Journal of Criminology* 58 (2): 414–433.

Ladegaard, Isak. 2018. "Instantly Hooked? Freebies and Samples of Opioids, Cannabis, MDMA, and Other Drugs in an Illicit E-commerce Market." *Journal of Drug Issues* 48 (2): 226–245.

Ladegaard, Isak. 2019 "I Pray That We Will Find a Way to Carry on This Dream: How a law Enforcement Crackdown United an Online Community." *Critical Sociology* 45 (4–5): 631–646.

Landa, Janet T. 1994. *Trust, ethnicity, and identity: beyond the new institutional economics of ethnic trading networks, contract law, and gift-exchange*: Ann Arbor, MI: University of Michigan Press.

Larsson, Stefan, and Måns Svensson. 2010. "Compliance or Obscurity? Online Anonymity as a Consequence of Fighting Unauthorised File-sharing." *Policy & Internet* 2 (4): 77–105.

Martin, James. 2014. *Drugs on the Dark Net: How Cryptomarkets are Transforming the Global Trade in Illicit Drugs*. New York City, NY: Springer.

Marx, Gary T. 2003. "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance." *Journal of Social Issues* 59 (2): 369–390.

May, Tiggey, and Mike Hough. 2004. "Drug Markets and Distribution Systems." *Addiction Research & Theory* 12 (6): 549–563.

McAdam, Doug and William Richard Scott 2005, "Organizations and Movements". In *Social Movements and Organization Th eory*, edited by Davis, Gerald, McAdam, Doug, Scott, William Richard, Zald, Mayer Nathan, pp. 4–40. Cambridge, UK: Cambridge University Press.

Merton, Robert K. 1936. "The Unanticipated Consequences of Purposive Social Action." *American Sociological Review* 1 (6): 894–904.

Meyer, David S., and Nancy Whittier. "Social Movement Spillover." *Social problems* 41, no. 2 (1994): 277–298.

Milgrom, Paul R., Douglass C. North, and Barry R. Weingast. 1990. "The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges, and the Champagne Fairs." *Economics & Politics* 2 (1): 1–23.

MIT PGP Public Key Server. 2017. Accessed March 30. https://pgp.mit.edu/.

Okazaki, Tetsuji. 2005. "The Role of the Merchant Coalition in Pre-modern Japanese Economic Development: An Historical Institutional Analysis." *Explorations in Economic History* 42 (2): 184–201.

Paoli, Letizia. 2004. "The Illegal Drugs Market." *Journal of Modern Italian Studies* 9 (2): 186–207.

Pasquale, Frank 2015. *The Black Box Society*. Cambridge, MA: Harvard University Press.

Pemberton, H. Earl. 1937. "The Effect of a Social Crisis on the Curve of Diffusion." *American Sociological Review* 2 (1): 55–61.

Popper, Nathaniel. "*Dark Web Drug Sellers Dodge Police Crackdowns*." *The New York Times*. New York City, NY: The New York Times, June 11, 2019. https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html.

Rao, Hayagreeva, Calvin Morrill and Mayer N. Zald 2000. "Power Plays: How Social Movements and Collective Action Create New Organizational Forms." *Research in Organizational Behavior* 22:237–81.

Resnick, Paul, Ko Kuwabara, Richard Zeckhauser, and Eric Friedman. "Reputation Systems." *Communications of the ACM* 43, no. 12 (2000): 45–48.

Rogers, Everett M. 2010. *Diffusion of Innovations*: Simon and Schuster.

Schumpeter, Joseph 1961. *Theory of Economic Development: An Inquiry into Profits, Capital, Credit, Interest, and the Business Cycle*. Cambridge, MA: Harvard University Press.

Sassen, Saskia. "Towards a Sociology of Information Technology." *Current Sociology* 50, no. 3 (2002): 365–388.

Soska, Kyle, and Nicolas Christin. 2015. "Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem." In *24th {USENIX} Security Symposium ({USENIX} Security 15)*, 33–48.

Schor, Juliet, B., William Attwood-Charles, Mehmet Cansoy, Isak Ladegaard, and Robert Wengronowitz. 2018. "Dependence and Precarity in the Platform Economy. Unpublished paper." Boston College.

Stinchcombe, Arthur L. 2000. "Social Structure and Organizations". In Baum, Joel AC, Dobbin, Frank, eds. *Economics Meets Sociology in Strategic Management*: Emerald Group Publishing Limited, 2000. Bingley, United Kingdom. pp. 229–59.

Stringham, Edward. 2003. "The Extralegal Development of Securities Trading in Seventeenth-century Amsterdam." *The Quarterly Review of Economics and Finance* 43 (2): 321–344.

Studdert, David M., Yifan Zhang, Jonathan A. Rodden, Rob J. Hyndman, and Garen J. Wintemute. 2017. "Handgun Acquisitions in California after Two Mass Shootings." *Annals of Internal Medicine* 166 (10): 698–706.

United Nations Office on Drugs, and Crime 2017. *World drug report*, p. 2017: United Nations Publications.

Vaughan, Diane 1996. *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA*: Chicago, IL: University of Chicago Press.

Williamson, Oliver E. 2000. "The New Institutional Economics: Taking Stock, Looking Ahead." *Journal of Economic Literature* 38 (3): 595–613.

Witt, S. 2015. The Man Who Broke the Music Business. [online] The New Yorker. Available at: https://www.newyorker.com/magazine/2015/04/27/the-man-who-broke-the-music-business [Accessed 30 Oct. 2017].

Woolf, Nicky 2015. ""Bitcoin 'Exit Scam': Deep-Web Market Operators Disappear with $12m." The Guardian." *Guardian News and Media*. https://bit.ly/2tyLF3x.

Zimmermann, Philip R. 2019. "Darknet Usage in the Illegal Wildlife Trade." *SocArXiv*. doi: 10.31235/osf.io/fgr9d.

Zimmermann, Philip R. 1995. "The O cial PGP User's Guide". 216 Cambridge, MA: MIT Press.