



# Gatekeeping in Online Markets: An Empirical Investigation of IT-based Self-regulation in Online Black Markets

Federica Ceci, Paolo Spagnoletti, and Andrea Prencipe

## ABSTRACT

This study examines how IT-based gatekeeping mechanisms influence platform survival in Online Black Markets (OBMs), anonymous, self-regulated marketplaces where buyers and vendors exchange illegal goods in absence of formal rules and regulatory bodies. In these high-conflict environments, platform owners rely on technological gatekeeping as a form of enhanced self-regulation, delegating specific control functions to IT-based intermediaries such as reputation systems, escrow services and access filters. Employing a sequential exploratory mixed-methods approach, we first conducted a qualitative case study of OBMs and then tested the impact of these mechanisms using quantitative survival analysis on a dataset of 56 OBMs spanning 54 months. Our findings reveal that controlling platform access enhances survival, whereas delegating transaction control to third parties increases failure risk. These insights advance the understanding of gatekeeping as a dynamic, IT-based self-regulation process to address conflicting practices in online markets and contributes to platform governance literature by highlighting the risks of decentralizing transaction control in high-conflict online environments.

## KEYWORDS AND PHRASES

Platform gatekeeping; platform governance; digital platforms; control mechanisms; darknet; crypto markets; online survival; black markets

## Introduction

Online markets (e.g., Alibaba, Airbnb, Amazon Marketplace) are based on matchmaking platforms that reduce transaction costs for the search, negotiation, and settlement of online transactions [27,41,85]. It is widely acknowledged that ensuring the existence and stability of online markets is a challenging task, since online interactions are performed by actors with diverse and often conflicting goals [34,97]. For example, some vendors may find it useful to establish long-term relationships with a large number of buyers, while others may be interested in maximizing the return on a single transaction. In the latter case, vendors may attempt to defraud buyers, damaging the reputation of the platform. Moreover, external actors may exploit platform vulnerabilities through fraudulent schemes and cyberattacks. Therefore, actors' self-interest can threaten the growth and survival of online markets [19,73].

To function successfully, online markets require rules to effectively govern the access of multiple participants, whose interests are seldom aligned [85,98]. Therefore, to regulate the behavior of buyers, vendors, and external actors, platform owners are called upon to establish, enact, and enforce rules that materialize into IT-based mechanisms. Various mechanisms are available to platform owners to regulate user behavior: owners decide who is allowed to connect through the platform, which rules users are required to

follow, and what positive or negative sanctions are imposed [27,50,85]. However, trade-offs emerge when platforms are opened to users, as platform owners need to monitor and contain behaviors through the implementation of IT-based gatekeeping mechanisms [16,49,87].

Gatekeeping is a set of rules, mechanisms and practices for regulating platform access and controlling what or who is admitted as a platform user according to some predetermined acceptance criteria [85,98]. It entails a dynamic interplay between rules, IT mechanisms, and user practices enacted by platform owners who operate as regulators of their ecosystems. Platform owners perform gatekeeping to find a “balance between bringing sellers and buyers together and keeping them apart” [3]. They decide on membership rules and implement mechanisms to grant access and devolve control, while limiting opportunistic user behavior [53]. Moreover, gatekeeping addresses challenges in online markets, such as network effects, information asymmetry, market failures, trust-building, reputation management, and stakeholder governance [16,41,57,69,73,74]. By performing effective gatekeeping, platform owners can create a secure, efficient, and thriving environment for market participants.

Previous studies on gatekeeping conceptualize it as a mechanism that reduces transaction costs for buyers and vendors and establishes long-term relationships in the market [39,52,81,98]. However, such view on gatekeeping fails in capturing the mutual and constitutive relationships between gatekeeping rules, IT mechanisms, and practices in online markets. We, instead, view gatekeeping as an IT-based regulation process where platform owners enact rules and delegate enforcement to technological artifacts that both shape and are shaped by the often-conflicting practices of market participants [15,90]. When gatekeeping is successfully performed, rules and practices dynamically propagate across time and space leading to the growth and stability of the online market. This aspect is of paramount importance when online markets are self-regulated by market participants, such as in the case of nonfungible tokens (NFT), crypto and gaming. In these settings, gatekeeping must regulate participants behaviors without any external rulemaking and control.

To explore how IT-based gatekeeping unfolds in self-regulated online markets, we focus on Online Black Markets (OBM), a distinct type of anonymous platform where buyers and vendors trade illicit goods and services [78]. While mimicking the user experience of legal marketplaces, OBMs operate in a context of radical decentralization: anonymity, lack of formal regulation and high exposure to fraudulent and opportunistic behaviors define their environment [10,77,78]. In the absence of legal oversight and formal enforcement mechanisms, platform owners in OBMs must rely solely on internal IT-based mechanisms to govern access, regulate transactions and preserve market order [30]. These features make OBMs particularly relevant to investigate gatekeeping as a process of IT-based self-regulation. Unlike legal marketplaces, where rule enforcement can rely on legal contracts or third-party arbitration, OBMs must balance openness and control through technical means alone. Conflicting practices among users—ranging from cooperative exchange to malicious exploitation—are endemic and can easily destabilize platforms. Yet, despite these fragilities, OBMs show remarkable patterns of resilience, where survival appears tightly linked to how gatekeeping is enacted and maintained over time.

Given the relevance of online markets and the limited understanding of how IT-based gatekeeping operates in self-regulated environments, we aim to answer the following

research question: How do IT-based gatekeeping mechanisms influence the survival of self-regulated online markets?

To address the research question, we adopted a mixed method approach [13,23,91]. We collected data from police operation reports and interviews, historical data through online forums, blogs, specialized web pages, public databases, data reported in previous research papers, and observations from hidden websites and these findings were corroborated by LEA experts [60]. We analyze three regulatory episodes to identify the conflicting practices, rules and IT mechanisms contributing to OBM survival and validated the relevance of such mechanisms by modelling a survival function of 56 OBMs over a 54-month period.

Our findings advance the understanding of gatekeeping as a fundamental process of IT-based regulation of conflicting practices in online marketplaces. We contribute to the literature on platform governance by shedding light on the relational dynamics among rules, IT mechanisms, and practices. Specifically, we identify these categories and show that involving third parties in gatekeeping increases the likelihood of platform failure in contexts characterized by self-regulation and high conflicting practices, such as the OBMs. We acknowledge that OBMs present unique characteristics, such as police intervention and frauds by platform owners, that limit direct comparability with regulated legal marketplaces. Therefore, while our findings provide insights into the relational dynamics of gatekeeping, we do not claim full generalizability to all online marketplaces. Instead, we argue that the mechanisms identified in OBMs can inform broader discussions of platform governance, particularly in self-regulated contexts where conflicting practices challenge regulatory frameworks. By theorizing gatekeeping as a process rather than a platform governance tool [90], we conceptualize enhanced self-regulation via technological intermediation, a form of IT-enabled governance especially relevant in high-risk digital environments. On a final note, we link to institutional and governance theories by showing how trust, behavioral control, and coordination can be sustained through informal rules and IT-based mechanisms, even in the absence of legal enforcement and stable identities.

The remainder of this paper is organized as follows. Section two reviews the literature on gatekeeping in online markets. Section three provides an overview of gatekeeping in the context of OBMs. Section four outlines the research strategy, presents case study findings, and reports the results of the survival regressions. Section five concludes the article by integrating insights from the qualitative and quantitative studies while also identifying avenues for further research.

## Theoretical Background

In online markets, platform owners—or decentralized communities acting as *de facto* regulators—must not only facilitate transactions, but also govern the conditions under which these transactions take place. This involves shaping rules, controlling access and enforcing norms, which are key to maintaining market integrity and user trust [16,41,53,85]. Particularly in peer-to-peer and self-regulated markets, platform owners convert loosely connected “peers” into accountable participants by establishing gatekeeping mechanisms and embedding governance practices in technical systems [3,26]. By carefully regulating access, they cultivate a pool of reputable vendors, and shape incentives to foster buyer loyalty. Delegating certain control functions to third parties contributes to platform governance [70,97]. Nevertheless, despite the imperative to grow rapidly, maintain low

overhead, operate flexibly, and maximize transaction fees, platform owners must carefully manage the trade-off between openness and control of platform boundaries [37,80,87]. Consequently, the expansion of membership, intended to boost transaction volumes, necessitates appropriate rules. Otherwise, the platform risks enabling noncompliant behaviors that could subvert the IT mechanisms designed to support an open environment, ultimately leading to systemic market failures.

### ***Gatekeeping in Self-regulated Platforms***

Drawing on Tiwana's [85] concept of platform control and extending it to the context of self-regulated platforms, we define gatekeeping as the set of processes, rules and tools—both technical and social—that regulate access, incentivize behaviors and deter misconduct in online markets [7,85]. Through gatekeeping, platform owners can oversee the activities of distinct and interdependent user groups [93] and set restrictions on their transactions [33,69]. These mechanisms are especially critical in markets where legal enforcement is absent, and market survival depends on the community's ability to maintain order and trust. In such contexts, misaligned or poorly calibrated gatekeeping may destabilize user expectations, discourage compliance, and accelerate market mortality [9,12,87,93]

Platform owners employ gatekeeping to regulate who can interact with the platform and in what manner [85]. This function is crucial, since opening or closing a platform directly shapes both the quantity and quality of its users, thereby influencing attractiveness and value creation [25,83,84]. Yet shifts in gatekeeping mechanisms can unsettle the ecosystem. Lenient input control may trigger coordination failures and quality issues, whereas strict control can suppress diversity and innovation [25,72,93].

Gatekeeping occurs at multiple stages, including user enrolment and transaction processing, and is typically enforced through IT-based tools such as algorithmic filters, automated reputation systems, and user feedback loops [31,39,48,51,81]. In self-regulated online markets, these mechanisms effectively substitute for formal regulation and are often maintained or even co-developed, by key community members acting as regulatory intermediaries. As a result, the layered gatekeeping infrastructure embodies a hybrid governance form in which technical artefacts and social norms co-evolve to regulate participation and behavior [31,39,48,51,81].

### ***Gatekeeping Mechanisms, Strategies, and Outcomes***

In self-regulated online markets, IT-based mechanisms are not just functional enablers—they operate as governance tools that define the regulatory architecture of the market itself. Algorithmic controls, protocols, and platform scripts embed enforceable rules, automate compliance, and shape the boundaries of acceptable behavior [53,79]. In doing so, they replace traditional contracts or institutional sanctions with code-based constraints that govern access, reputation, and transactions.

We refer to this regime as enhanced self-regulation: a system in which platform owners or community leaders exercise control through a mix of algorithmic enforcement, delegated authority, and embedded incentives. Here, decision rights are distributed. Owners retain control of core systems and strategic direction, while users contribute resources and maintain partial control over their offerings [50,53]. Gatekeeping mechanisms, in this

setting, help to mitigate opportunism and enable effective self-regulation. Yet this governance model is never static. Platforms must continually adapt to evolving threats like fraud, fake reviews, or coordinated attacks, choosing technological and organizational responses that preserve trust. Gatekeeping strategies range from laissez-faire approaches that rely on market incentives to tightly controlled regimes that restrict access and participation [1].

Understanding gatekeeping in this context requires a shift in perspective—from seeing it as a fixed set of controls—to recognizing it as a dynamic governance function. It is this dynamic quality that allows platforms to sustain credibility, order, and adaptability even in the absence of formal oversight [56]. In this sense, platforms emerge as regulatory actors in their own right [90], embedding rules in IT systems, empowering key intermediaries, and actively shaping user interactions, market structure, and ultimately, their own survival [90].

### ***Gatekeeping in OBMs***

To illustrate these dynamics in an extreme self-regulated setting, we turn to Online Black Markets (OBMs). OBMs are anonymous marketplaces that connect buyers and vendors for the exchange of illegal products and services, relying on technologies such as cryptocurrencies and the Tor network. Their scale has expanded rapidly: transaction volumes grew from an estimated \$220 million in 2015 on Silk Road [77] to over \$790 million in 2019 [17]. Often referred to as darknet marketplaces or crypto markets, these platforms mirror legal marketplaces by offering product listings, vendor ratings, forums, and customer support [4,10,18,36,55].

Anonymity and illegality make survival especially challenging. In the absence of formal rules or regulatory bodies, opportunistic behaviors threaten platform growth and viability. Conflicts frequently arise when vendors deliver substandard products or when platform owners exploit their position. While fraud cannot be prosecuted in conventional ways, law enforcement agencies actively target OBMs to disrupt their operations. Yet despite repeated shutdowns, the ecosystem as a whole persists and expands [30,78].

Like legal online marketplaces, OBMs are owned and controlled by platform owners (or a group of owners) who define the rules and embed technical functions into the platform architecture [37,79]. These systems integrate core modules and complementary technologies to enable anonymous browsing, conceal financial transactions, and build vendor reputation, even under conditions of anonymity [43,47,78].

Operating without legal protection, OBMs face constant threats from Law Enforcement Agencies (LEAs), which heighten risks for vendors, buyers, and owners [8,18,30,67,68,78]. Strategic responses therefore center on gatekeeping, securing platform access and protecting transactions in adverse conditions [32,46,61,89]. OBMs mitigate risks such as moral hazard or undercover police operations by regulating exchanges through vendor ratings, banning deceptive users, and providing escrow services [6,66].

While OBMs share structural features with legal marketplaces—such as user interactions, reputation systems, and transaction processes—they operate under extreme constraints, including the absence of formal enforcement, the risk of police intervention, and potential fraud by owners. Lacking official governance, they rely on IT-based mechanisms to counter opportunistic behavior and preserve stability. Despite these pressures, the resilience and growth of OBMs underscore the adaptive and robust nature of gatekeeping in self-regulated platforms. Although OBMs represent a distinct market

type, they share with legal marketplaces fundamental governance challenges, such as balancing access control, enforcing trust, and sustaining market activity. Examining OBMs therefore helps to highlight the specific ways in which gatekeeping regulates participation under conditions of anonymity and illegality, while also pointing to broader dynamics observable across online markets.

Building on this comparison, we structure our analysis of gatekeeping across three dimensions—IT mechanisms, rules, and practices—contrasting legal marketplaces and OBMs (Table 1). IT mechanisms denote technology-driven solutions that enforce gatekeeping rules and shape user interactions; rules are the explicit policies and enforcement measures that regulate behavior and mitigate risks; and practices are the observable practices of participants, shaped by the interaction of IT mechanisms and rules.

Research Design

To address our research question, we adopted a sequential exploratory mixed-methods approach [23–25,91]. A sequential exploratory strategy requires the collection and analysis of qualitative data in a first research phase followed by the collection and analysis of quantitative data in a second phase to test and explain the relationships found in qualitative data. In the qualitative study, we explore OBM functioning, to shed light on how platform owners develop and apply gatekeeping mechanisms to operate the market while being protected by malicious users. In the quantitative study, we modelled a survival function of the 56 OBMs operating between October 2013 and March 2018 to understand the influence of the previously identified gatekeeping mechanisms on platform survival. The adoption of mixed-methods research provided an opportunity for a complementary view on the phenomenon [82]: it allowed us to obtain a complete picture, which was required by the hidden nature of the empirical context, and to further elaborate the findings from the qualitative study by immediately using the identifies variables [94]. In fact, as suggested by Venkatesh et al. [91], a mixed-methods approach is a powerful mechanism to interject context into a research inquiry. In the specific case of this research, we are grounding the study in a context where the initial qualitative study unearths factors that are not typically common in a legal online market [58,62]. The objective of the research is to identify such factors through a qualitative study and then assess their impact on platforms survival using a quantitative study. In this process, both quantitative and qualitative data are analyzed in accordance with the established guidelines for each methodology.

Table 1. Gatekeeping in Legal Marketplaces and OBMs (based on [93]).

Gatekeeping	Legal Marketplaces	Online Black Markets	Examples
IT mechanisms	IT tools that enforce platform rules, streamline transactions, and provide security	IT tools that materialize rules under anonymity, ensuring access, transaction safety, and reputation	Access control; escrow; crypto-wallets
Rules	Formal rules embedded in Terms of Service, liability frameworks, and customer protection policies	Informal or self-imposed rules that constrain misbehavior and align incentives in the absence of legal enforcement	Platform policies; incentives; sanctions
Practices	User practices shaped by platform design, customer service, and formal regulation	User practices that reflect navigation of constraints imposed by IT mechanisms and platform rules, often under risk of surveillance and fraud	User buys goods; vendor adds item; LEA undercover operations



### Qualitative Analysis

The qualitative analysis aims to investigate the functioning of OBM and examine how platform owners develop and implement gatekeeping mechanisms to effectively operate within the market. We need this phase to ground our study in the OBM specific context where this initial qualitative investigation will reveal factors that are uncommon or atypical in legal online markets. By acknowledging these unique elements, we aim to provide a comprehensive understanding of the dynamics at play in this setting. This contextual grounding allows us to identify and analyze the distinctive factors influencing the development and application of gatekeeping mechanisms by platform owners in the face of malicious users.

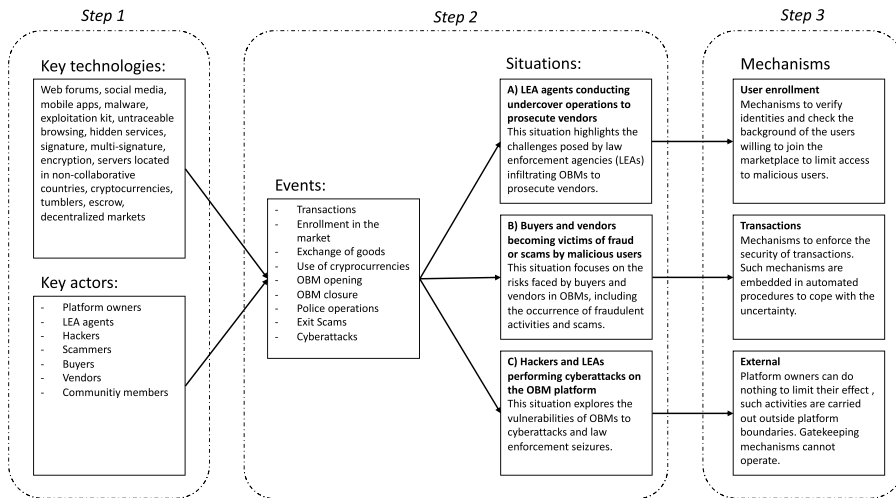
To do so, we conducted a case study to examine the evolution of OBMs operating on the Tor network, over a period of 4.5 years (from October 2013 to March 2018). This case study has a revelatory nature [96] because it provides an opportunity to observe a phenomenon that is otherwise inaccessible: specifically, the gatekeeping mechanisms employed in online marketplaces operating under conditions of highly conflicting goals. By following case study research guidelines [96], we adopted an embedded case study design; we identified multiple units of analysis within the case, such as transactions, actors and platforms.

We collected empirical data from multiple sources. Due to the anonymity and secrecy characteristics of the analyzed OBMs and users, we triangulated our data, as one single source would not have provided a complete picture of the phenomenon [36]. More specifically, we collected qualitative data from the following sources: (i) reports from police operations (e.g., EUROPOL); (ii) open source data on the Internet, i.e., historical data obtained by accessing online forums, blogs, specialized web pages, and public databases; (iii) data reported in previous research papers; and (iv) observations from hidden websites. To improve replicability, we provide an overview of our qualitative data sources in Table 2.

The data analysis procedure is articulated in three steps, that reflect the open coding, axial coding, and selective coding approach [20,75]. A summary of the data analysis process is presented in Figure 1.

**Table 2.** Overview of the collected data.

Sources of Data	Details of the source of data	Volume
Reports from police operations	Strategy briefs and reports from government, LEAs, and professional associations	15 national cybersecurity strategies 6 ENISA threat landscape reports 5 EUROPOL IOCTA reports 7 FBI IC3 reports 6 CLUSIT reports
Open sources data on the Internet	Articles and posts published on websites, blogs; trade journals, newspapers Longitudinal analysis of Deepdotweb.com accessed through Internet Archive Posts published on reddit.com Darknet market archives	215 articles (52 newspapers; 55 trade journals; 69 wire feeds, 39 other) 277 webpages captured 1800+ posts Online collection covering 89 DNMs and 37+ related forums
Data reported in previous research papers	Scientific papers on criminology, drug trafficking, security, and regulation	78 papers (49 in criminology journals, 22 in information systems journals, 7 other)
Observations from hidden websites	Terms and conditions, FAQ and buyers guidelines and vendor services list. List of offerings related to credit cards and identity theft on sales in major OBMs	36 GB of data, up to 18,831 pages/images per each OBM



**Figure 1.** Data Analysis Process

- (1) *Key Technologies and Key Actors.* We used coding techniques to categorize and organize the collected data; the coding process involved two researchers who independently coded the data and then engaged in iterative discussions to resolve discrepancies. We started with an open coding to identify key technologies and actors involved in those actions. Coding reliability was ensured through intercoder agreement, with discrepancies resolved through consensus discussions.
- (2) *Events and Situations.* On the basis of the open coding, we proceed with axial coding to establish relationships among themes, and we grouped technologies and actors by events observable in OBMs, such as users involvement in the platforms, transactions and exchanges, law enforcement operations, fraud, scams. This process was guided by an iterative approach where events were identified inductively and validated against prior literature on digital marketplaces and OBMs. On the basis on the inferred events, we identified three specific situations that represented three different moments where conflicting goals in OBMs should be managed. These situations were chosen since they summarize how OBMs operate and how actors navigate the challenges posed by conflicting user behaviors.
- (3) *Mechanisms.* We performed selective coding to refine key constructs related to gatekeeping in OBMs and we identified the gatekeeping mechanisms implemented by platform owners. We examined the strategies and practices used to regulate user behavior, mitigate risks, and manage conflicting goals. This step involved synthesizing the final categories into overarching themes representing gatekeeping mechanisms. The final constructs were validated by cross-referencing with existing platform governance literature and assessing coherence across multiple data sources.

Concept refinement was conducted through iterative discussions, where emergent themes were reviewed against existing literature and additional data sources, including follow-up interviews with LEA experts [60]. These interviews provided further validation and



contextual insights. Convergence was assessed by examining coding saturation, ensuring that no new themes emerged in the final coding iterations.

### ***Risks of Failure and the Management of Conflicting Goals in OBM***

Following the procedure described above, we identified three regulatory episodes that illustrate how gatekeeping ensures market survival despite users' conflicting behaviors. For each situation, we provide empirical evidence from the data collected, in order to highlight where such mechanisms have been observed. In each episode, we observe that some users threaten market functioning, and we identify the gatekeeping rules, IT mechanisms and practices that regulate user behavior and their conflicting goals.

### ***LEA Agents Conducting Undercover Operations to Prosecute Vendors***

Activities in OBMs are carried out in a anonymous way using the Tor network and cryptography tools. However, the use of such tools requires some expertise in order to preserve anonymity. Moreover, buyers and vendors need to exchange and convert their cryptocurrencies, which gives LEAs the opportunity to monitor suspicious transactions on exchange markets and prosecute buyers and vendors.

We observe two different and contrasting situations: on the one hand, expanding the overall number of users can be beneficial to the success of the platform; on the other hand, to protect the platform, it is best to focus and retain users that are already members of the community. These users, in fact, are more experienced in conducting anonymous transactions and therefore aware of how to minimize risks.

OBM owners can decide to select buyers and vendors by controlling their access in the following ways. To limit the access of buyers, OBM owners can implement a registration mechanism called "invite only": to access the OBM and interact with its users, existing platform members must issue a referral link. This restricts access to the OBM to people already in contact with community members. Another option is to facilitate access for buyers by enabling open registration (i.e., no invitation from other users is required to join the market). In this case, it is possible to sign up with an OBM platform as a buyer and interact with its users with a simple registration, decreasing search costs and facilitating access.

To limit the access of vendors, several mechanisms can be implemented. Some specialized websites refer to "vendor bond" as the requirement by the OBM owner to pay a fee to start selling in the marketplace. The amount of money can be requested by the OBM owner in US dollars or cryptocurrency, such as Bitcoin. Once a vendor's application is approved, his or her products are listed in the e-catalogue. Vendor bond is paid back when vendor status is revoked. The second mechanism refers to the possibility for OBM owners to request a "PGP key" from registered vendors to certify their identity. PGP is an acronym that stands for Pretty Good Privacy and refers to an encryption solution that provides cryptographic privacy and authentication. PGP is used to sign, encrypt, and decrypt text, e-mail, files, directories, and to increase the security of communications. Some OBM administrators check the authenticity of vendors and then allow them to post their offerings on the OBM. Moreover, some markets require vendors to follow special rules, instructing them, for example, to share their public key, "avoid self-rating, do not ask to "finalize early"

for escrow offers and do not have order too long in status accepted” (Dream Market Vendors Guidelines accessed on Tor October 2nd, 2018).

Here we observe how gatekeeping mechanisms implement procedures to verify identities and check the background of the users willing to join the marketplace to limit the success of LEA undercover operations.

### ***Buyers and Vendors Becoming Victims of Fraud or Scams by Malicious Users***

Specific characteristics of anonymous trade (i.e., anonymity, untraceability, and illegality of traded goods) lead to sudden and frequent interruptions in the normal functioning of OBM, which can be caused by sudden and unpredictable events such as an exit scam. In this case, malicious users (e.g., hackers) exploit the opportunity created by the presence of substantial amounts of money in the escrow system: the hacker can simply transfer the cryptocurrencies to his or her own wallet, and remove the account to conceal his or her tracks from both admins and buyers.

Two mechanisms can be implemented at this stage to manage control over transactions: (i) the use of multi-signature and (ii) the possibility to finalize early the transaction. These elements allow external users (in addition to vendors and buyers) to check transactions occurring in the OBM. More specifically, the control can be performed by a third party: if multi-signature is adopted, the OBM requires a multi-signature procedure, i.e., transactions must be validated by multiple parties before funds can be unlocked. In the event of opportunistic behavior by one of the two users involved in the transaction, the wallet can be opened through the key belonging to a predetermined trusted third party. The second possibility is to include or exclude the option to “finalize early” the transaction. By “finalize early”, we refer to the release of escrow funds before the seller knows that the conditions of the contract have been met. This is used to reduce the vendor’s risk of currency price fluctuation and market shutdown.

In this case, gatekeeping mechanisms operate when transactions occur, and platform owner implements procedures that enforce rules for transaction security. The implementation of standardized processes embedded in technical interfaces makes possible to cope with the uncertainty and manifold options for activity by malicious actors.

### ***Hackers and LEAs Performing Cyberattacks on the OBM Platform***

The most relevant failures generally occur in the final stage of an OBM’s life, when OBM operation is disrupted by LEA’s seizure, a denial-of-service attack, or admins performing an exit scam or officially announcing the closure on the website.

These shutdowns are often unexpected, such as in the case of police operations that are announced by LEAs after the operations have ended or after the exit scam. The closure of an OBM can be anticipated by some flaws in its functioning, due to the increasing number of extortion attempts made by hackers through cyberattacks. An operation can be checked by monitoring the uptime status (also called business continuity, that is the percentage of time during which the platform is successfully operating) of the platform, which usually decreases significantly in the final part of its life. In parallel with the growth of vendors and offers and the increase of its popularity, the size of the platform attracts the interest of malicious actors seeking to misappropriate value. Constant feedback on the functioning of the platform, consisting of ratings and comments, is constantly reported by users in specialized websites (i.e., Deepdotweb.com, seized by the FBI on May 7, 2019). However,

we note that there is not much that platform owners can do to limit the effect of such malicious actors, as these activities are not carried out by platform users. Business continuity, size, and ratings are performance measures of an OBM status that cannot be directly controlled by the OBM admin, therefore, we identified an area when gatekeeping mechanisms cannot operate in ensuring the survival of the platform.

We selected the above regulatory episodes for our analysis based on their relevance to understand how conflicting goals are managed in OBMs when the risk of failure is high. By examining these episodes, we gain insights on the gatekeeping rules, IT mechanisms and practices emerging in OBMs.

### Bridging Qualitative and Quantitative Study

Bridging is the process of developing a link between qualitative and quantitative findings, it is important to understand boundary conditions related to the research context and it is particularly suitable for sequential mixed methods research in which researchers seek to provide a developmental or expanded view of a phenomenon of interest [91]. The qualitative study leads us to identify variables that explain how gatekeeping operates in OBMs. For each episode we report the threat, observed variables, and the type of control exercised by the IT-based gatekeeping mechanisms (if any) implemented by the platform owner (Table 3).

### Quantitative Analysis

In the quantitative study, we modeled a survival function of the 56 OBMs operating between October 2013 and March 2018 in the Tor network to understand the influence of gatekeeping mechanisms on platform survival. Based on the results of our qualitative analysis, we gained a comprehensive understanding of the various forms of gatekeeping mechanisms within the context of OBM. However, their impact on platform survival is still unknown. With the survival analysis, we shed light on the effects of such mechanisms on the survival of OBM platforms. In contrast to conventional online marketplaces, where performance is typically measured through user growth, transaction volume, or engagement, OBMs operate under extreme conditions of uncertainty, where the primary concern for platform owners is remaining operational over time. We adopt platform survival as the dependent

**Table 3.** A Summary of the Qualitative Analysis.

Regulatory episodes	Variables	Control	Description
LEA agents conducting undercover operations to prosecute vendors	<i>Invite only</i> <i>Vendor bond</i> <i>PGP</i>	User enrollment	Mechanisms to verify identities and check the background of the users willing to join the marketplace to limit access to malicious users.
Buyers and vendors becoming victims of fraud or scams by malicious users	<i>Multi-signature</i> <i>Finalize early</i>	Transactions	Mechanisms to enforce the security of transactions. Such mechanisms are embedded in automated procedures to cope with the uncertainty brought by the activities performed by the users.
Hackers and LEAs performing cyberattacks on the OBM platform	<i>Police operations</i> <i>Size</i> <i>Ratings</i> <i>Business continuity</i>	External	Platform owners can do nothing to limit the effect of malicious actions, as some activities are carried out outside platform boundaries. In this area gatekeeping mechanisms cannot operate.

variable: survival captures the effectiveness of governance mechanisms in sustaining platform functionality under adverse conditions, and thus offers a robust and context-appropriate indicator of gatekeeping performance in self-regulated digital markets.

To conduct the quantitative analysis, we collected historical data by accessing specialized web pages through the Internet Archive (IA) website monthly to reconstruct for each of the first ranked OBMs the gatekeeping mechanisms implemented and status over time. We then complemented these data with a public database, the Darknet Market Archive [11], used in previous research papers [31,67,80,81]. Our dataset refers to the period from October 2013 until March 2018, covering 4.5 years of OBM evolution. Based on these data, we tracked the evolution of OBMs after the closure of Silk Road 1 (i.e., the first OBM, closed by the FBI in October 2013). In October 2013 there were five active OBMs and since then, we have recorded the existence of 81 anonymous marketplaces in the deep web. We integrated the data from multiple sources and we obtained a database composed by 56 OBMs. The database reports, for each OBM, the entry date, exit date, and the technological and operational characteristics of the platform. Collected data offer a complete overview on the policies, technologies, and procedures adopted by OBM owners to develop their platforms, improve security, and facilitate access. In the process of constructing the database, 25 OBMs have been excluded from the analysis due to missing information. We tested the equality of means of survival among the two groups of OBMs and we do not find a statistically significant difference in the means ( $\Pr(|T| > |t|) = 0.1100$ ). The database is available upon request.

Operationalization of Key and Control Variables

The independent variables employed in this study to explain the exit hazard for OBMs has been identified with the qualitative study, as reported in Table 2. A graphical representation of the model is shown in Figure 2.

To model the function, we used two sets of independent variables and five control variables, described as follows. To operationalize the “control over membership” decisions on the platform, we used: *Invite only*, *Vendor bond*, and *Forced vendor PGP*. *Invite only* is

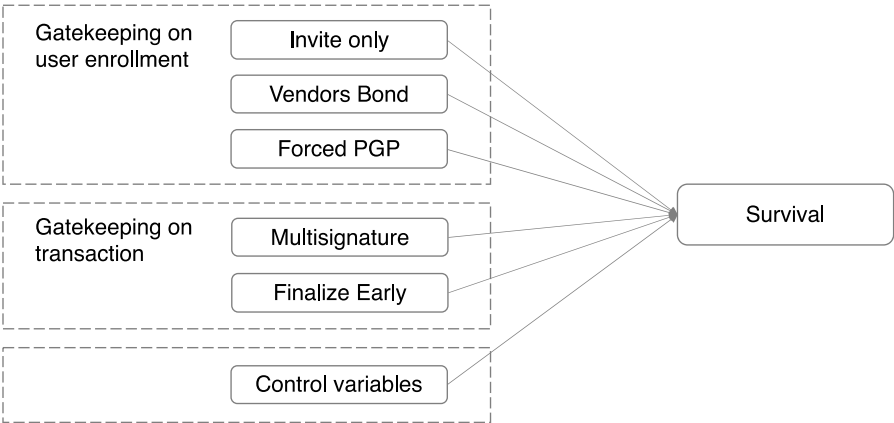


Figure 2. Analytical Model

a dummy variable and it takes the value 1. To access the OBM and interact with its users, subscribers are required to use a referral link issued by existing platform members. The variable takes the value 0 if it is possible to register to the OBM as buyers without any invitation by existing users. The variable *Vendor bond* measures the OBM owner's requirement to pay a fee to start selling in the market. *Vendor bond* is a categorical variable that indicates the amount of money required from the vendor. The variable takes the value 1 if no money is required, 2 if the bond is up to 50 USD, 3 if it is between 51 and 100 USD, 4 if it is between 101 and 200 USD, 5 if it is over 201 USD. The amount of money can be demanded by the OBM owner in USD or Bitcoin; we converted Bitcoins into USD, using the exchange rate at the time of market birth. The *Forced vendor PGP* is a dummy variable taking the value 1 if the OBM requires vendors to be authenticated through their PGP key.

To operationalize decisions about the “control over transaction”, we used *Multi-signature* and *Finalize early*. *Multi-signature* is a dummy variable taking the value 1 if the OBM requires a multi-signature procedure, i.e., transactions must be validated by multiple parties before funds can be unlocked. *Finalize early* is a categorical variable taking the value 2 if it is not permitted, 1 if it is permitted under specific conditions, 0 if it is always permitted. By *Finalize early*, we refer to the release of escrow funds before the seller knows that the conditions of the contract have been met.

Along with the key explanatory variables, we used five control variables: *business continuity*, *size*, *ratings*, *police operations*, and *cryptocurrencies*. The variable *business continuity* is measured by recording the value of the OBM uptime status monthly for the whole survival period of the OBM [95]. This variable is a proxy for the ease of access and reliability of OBMs for users involved in the transactions. The *size* of the OBMs is calculated as the ln of the number of offerings (i.e. the products or services provided by the platform to its users) at the time of exit from the market. This variable is a proxy for the dimension of the OBM. The variable *ratings* has been constructed calculating the mean of the ratings (measured monthly for the whole life of the DNM) received by the platform and collected from the website Deepdotweb.com accessed through Internet Archive. *Police operations* specifies if the OBM was up and running at the time when one of the two main operations that closed a high number of OBMs, i.e., when Onymous and Bayonet, took place [2,14,92]. This is a dummy variable taking the value 1 if the OBM was running, 0 otherwise. Finally, *cryptocurrencies* indicates if the OBM accepts any type of cryptocurrencies (e.g. Bitcoin and Monero among the others). The variable assumes the value 1 if accepted and 0 otherwise. Table 4 reports an overview of the variables used and the source used to construct those variables. Figure A1 reports some descriptive statistics for the variables used in the models.

### **Empirical Specifications**

In our analysis, we focus on the survival time of the platform, which is a duration variable that measures the number of months in which the platform has been online. Survival analysis provides information regarding the amount of time necessary before the occurrence of an event (e.g., platform closure) and the role of different causes in explaining the occurrence of the event. In our case, the survival function measures the probability that a platform would remain online and active  $t$  months. To select the most appropriate modelling technique, we tested for the proportionality of hazard rates for the covariates introduced in the model [42]. Regarding our data, we found that the proportionality

**Table 4.** Variables Construction.

Variable		Definition	Source
<i>Survival</i>	Dependent	Number of months in which the platform has been online	Reports from police operations, Deepdotweb.com accessed through Internet Archive, Darknet market archives
<i>Invite only</i>	Independent	To access the OBM and interact with its users, subscribers are required to use a referral link issued by existing platform members.	Deepdotweb.com accessed through Internet Archive and articles and posts published on websites
<i>Vendor bond</i>	Independent	OBM owner's requirement to pay a fee to start selling in the market	Deepdotweb.com accessed through Internet Archive and Darknet market archives
<i>Forced vendor PGP</i>	Independent	OBM requires vendors to be authenticated through their own PGP key	Deepdotweb.com accessed through Internet archive
<i>Multi-signature</i>	Independent	OBM requires a multi-signature procedure, i.e., transactions must be validated by multiple parties before funds can be unlocked	Deepdotweb.com accessed through Internet archive and Darknet market archives
<i>Finalize early</i>	Independent	Release of escrow funds before the seller knows that the conditions of the contract have been met	Deepdotweb.com accessed through Internet archive
<i>Business continuity</i>	Control	Ease of access and reliability of OBM's for users involved in the transactions	Deepdotweb.com accessed through Internet archive
<i>Size</i>	Control	Dimension of the OBM, i.e. number of offerings at the time of exit from the market	Deepdotweb.com accessed through Internet archive and articles and posts published on websites
<i>Ratings</i>	Control	Ratings received by the platform and collected from a specialized website	Deepdotweb.com accessed through Internet Archive
<i>Police operation</i>	Control	OBM was up and running at the time when one of the two main police operations took place	Reports from police operations and Darknet market archives
<i>Cryptocurrencies</i>	Control	The market accepts cryptocurrencies	Deepdotweb.com accessed through Internet archive and Darknet market archives

assumption is violated. Therefore, we selected a parametric survivor function; more specifically, we selected a proportional hazards (PH) model. In the PH model, the concomitant covariates have a multiplicative effect on the hazard function:

$$h(t_j) = h_0(t)g(x_j)$$

In our case, the function  $h_0(t)$  takes the parametric form specific to the Gompertz model [59]. This distribution is suitable for modeling data with monotone hazard rates that either increase or decrease exponentially with time. The coefficients relating the predictors to the hazard function are conceptually similar to the odds ratios found in logistic regression.

## Empirical Results

The results of the Gompertz hazard regressions are presented in Table 5. Model 1 estimates variables that operationalize control over membership, Model 2 estimates variables that operationalize control over transactions, Model 3 estimates all variables simultaneously. All the models include control variables. The main results will be summarized as follows: first, broadening the buyer base has a positive effect on survival. As shown in the models [1, 3] in Table 5, the coefficients of *Invite only* are positive and statistically significant, therefore implementing an “invite only” policy leads to an increased hazard rate. The coefficient of



**Table 5.** Results of the Gompertz Hazard Regression.

	Model 1			Model 2			Model 3		
	Coef.	SE.	$P> z $	Coef.	SE	$P> z $	Coef.	SE	$P> z $
<i>Invite only</i>	0.88	0.42	0.037				1.00	0.42	0.018
<i>Vendor bond</i>	−0.03	0.14	0.823				−0.03	0.14	0.812
<i>Forced vendor PGP</i>	−0.02	0.31	0.952				−1.30	0.45	0.004
<i>Multi-signature</i>				0.73	0.33	0.030	1.47	0.48	0.001
<i>Finalize early</i>				0.43	0.22	0.049	0.49	0.22	0.031
<i>Business continuity</i>	−0.02	0.01	0.061	−0.01	0.03	0.278	−0.03	0.01	0.061
<i>Size</i>	0.07	0.09	0.426	0.08	0.08	0.352	0.14	0.09	0.132
<i>Ratings</i>	0.36	0.29	0.217	0.15	0.27	0.566	0.43	0.32	0.183
<i>Police operation</i>	1.89	0.37	0.000	1.87	0.37	0.000	2.19	0.40	0.000
<i>Cryptocurrencies</i>									
Gamma	0.051	0.015	0.001	0.066	0.017	0.000	0.08	0.019	0.000
Log likelihood	−66.041			−64.25			−58.20		
LR $\chi^2(7)$	29.86								
LR $\chi^2(6)$				33.44					
LR $\chi^2(9)$							41.99		
AIC	150.08			144.49			138.40		
BIC	168.30			144.49			160.48		
N	56			56			56		

*Forced vendor PGP* is negative and statistically significant in Model 3, while being not significant in Model 1. These results show that increasing control when accepting new vendors in the platform decreases the hazard rate, therefore expanding the vendor base has a negative effect on survival.

Second, when transactions are controlled directly by the OBM owners, the chances of survival are higher. In fact, as shown in Models 2 and 3, the variables that operationalize the control performed by third parties (i.e., *Multi-signature* and *Finalize early*) are positively associated with the hazard rate. These results suggest that the involvement of third parties in transaction control and guarantee has a negative effect on OBM survival.

Finally, among the control variables, only the *police operations* variable is significant and positively associated an increase in the hazard rate. It is worth noting that the coefficients of *size* and *ratings* are not statistically significant, while *business continuity* is negative and significant in Models 1 and 3. These results suggest that the classical leverages of platforms strategy are not important in our empirical context. In fact, due to the role of external threats, OBMs cannot obtain the winner-takes-all outcome, and the usual performance indicators (*size* and *ratings*) do not impact platform survival. Only platform availability (measured via the *business continuity* variable) is significant and negatively associated with an increase in the hazard rate. Finally, it is important to mention that the gamma coefficient ( $\gamma$ ) is positive and statistically significant at the 1% level, indicating that the baseline hazard of the Gompertz model increases with time.

## Discussion

Previous research focusing on platform governance has emphasized the role of gatekeeping mechanisms in enabling online marketplaces to function efficiently and underlined the role they play in shaping actors' behaviors [7,25,85,98]. We contribute to this debate by offering an empirical investigation of gatekeeping in the OBM context, a high-risk and extreme setting characterized by hidden identities, value misappropriation, absence of formal rules

and regulatory bodies, and highly conflicting goals among actors. Understanding gatekeeping in OBM is significant because these marketplaces operate under conditions of mutual distrust and anonymity, which hampers the delegation of responsibilities and complicates the design of effective self-regulation mechanisms. At the same time, comparing these dynamics with legitimate marketplaces helps clarify both shared governance logics and the unique constraints that shape OBMs. In so doing, we identified a set of gatekeeping mechanisms that can be used to balance openness and platform protection by selecting users and regulating their behavior with the help of technical tools. We then analyzed how these mechanisms affect marketplace survival, finding that platforms relying on third-party control in transactions show a higher likelihood of failure.

### ***From Gatekeeping to Enhanced Self-regulation***

Our findings contribute to the literature on platform governance by shedding light on the different gatekeeping mechanisms and how they operate in self-regulated online markets. Rather than overgeneralizing to all online marketplaces, we emphasize the relevance of our findings for high-conflict and weakly regulated environments, where traditional governance structures are absent. The gatekeeping mechanisms we identify, particularly their relational dynamics, offer insights into how platforms manage conflicting behaviors and regulatory challenges more broadly. We highlight the unique strategies that emerge when governance relies primarily on IT-based control rather than external legal frameworks. Moreover, while survival is not commonly adopted as a primary performance metric in regulated online marketplaces, it emerges as a critical outcome in high-risk environments such as OBMs, where platform viability is continuously threatened both by internal disruptions and external. In these settings, remaining operational over time constitutes a core strategic goal and a concrete indicator of governance effectiveness. Consequently, platform owners prioritize mechanisms aimed at preserving stability, mitigating systemic risks, and enforcing trust, rather than maximizing growth or transaction volumes. This orientation is reflected in the design of gatekeeping strategies, which are geared more toward containment than expansion. Mechanisms such as invite-only registration, vendor authentication through PGP, and restrictions on third-party intervention in transaction management are deliberately employed to ensure tighter control and limit exposure to malicious actors. Although context-specific, these practices illuminate how gatekeeping mechanisms may be adapted to support platform resilience in self-regulated or weakly governed digital ecosystems.

### ***Gatekeeping Mechanisms and Platform Survival***

The results of our survival analysis suggest that gatekeeping over transactions, operationalized through IT tools (i.e., *Multi-signature* and *Finalize early*), are likely to lead to platform failure when third-party control is introduced, highlighting the vulnerabilities of decentralized governance in high-risk environments. If control rights are assigned to third parties. Tiwana [85] studied a similar type of control and defined it as “relational control”. He described it as control that occurs through clan control, achieved by including third parties in the governance and promoting common values, shared beliefs, and norms [87]. However, enforcing norms, fostering values, and controlling buyers and vendors can be particularly

difficult in contexts characterized by anonymous users with conflicting interests and in the absence of regulatory bodies. Our results show that the inclusion of third parties in the process leads to a higher probability of platform failure. Typically, assigning rights to third parties is intended to increase trust both in the transactions and in the process, however, our results suggest that platforms that exclude external actors from control increase their chances of survival. This finding challenges the assumption that third-party involvement is a universally effective trust-enhancing mechanism [40,63,70,86,87], instead suggesting that in some marketplaces, decentralization can exacerbate risks rather than mitigate them. In conflict-laden contexts, delegating the role of guarantor to external actors introduces vulnerabilities rather than increasing security. Our analysis suggests that the involvement of third parties in transaction control introduces vulnerabilities in environments characterized by anonymity and high conflict. These actors, often lacking persistent identities and clear enforcement capacity, may be unable to reliably mediate disputes or prevent fraud. Unlike legal platforms, where third-party actors can be certified and supported by enforceable contracts, OBMs lack such institutional scaffolding and must rely on technical substitutes. As a result, delegating control to third parties may reduce the platform's ability to maintain consistent and enforceable standards, thereby increasing uncertainty and undermining trust. These qualitative insights are supported by our regression results, which show a consistent and statistically significant association between third-party mechanisms and increased hazard rates. While causality cannot be definitively established, the converging evidence supports our interpretation that decentralization, under certain conditions, weakens governance.

This observation emphasizes the complexity in environments with high conflict or anonymity: in settings like OBMs, where users often have conflicting interests and anonymity prevails, the effectiveness of this approach diminishes. The anonymity and lack of accountability make it harder for third parties to effectively enforce rules or norms. This is because their role as unbiased arbiters or enforcers becomes significantly more challenging without clear, consistent interaction histories or identities. In such contexts, the introduction of external guarantors might introduce additional layers of complexity and risk, potentially leading to increased skepticism among users rather than the intended trust. Therefore, while third-party involvement is a common trust-building mechanism, its efficacy is context-dependent, and in some settings, platforms might benefit from retaining control internally.

### ***The Role of Access Control in Platform Survival***

Beyond the effect of third-party mechanisms, our findings highlight the critical role of access control in platform survival. The invite-only mechanism, which restricts platform entry to users guaranteed by existing members, is significantly associated with lower hazard rates. This stands in contrast with legal marketplaces, where access is typically open but safeguarded by formal identity checks, Terms of Service, and liability frameworks. This suggests that controlled access serves as an effective gatekeeping strategy, likely due to improved user quality, increased social accountability, and reduced exposure to external threats such as undercover enforcement agents. Similarly, the finalize early mechanism reveals a nuanced dynamic: platforms that allow early finalization under specific conditions tend to experience lower failure rates compared to those where early finalization is either

fully allowed or entirely prohibited. This suggests that selectively granting discretion to trusted vendors, while maintaining general control, can enhance transactional fluidity without compromising platform integrity. These findings reinforce the importance of balancing control and flexibility in the design of gatekeeping mechanisms.

### ***Contributions to Theory***

Our findings lead to relevant contributions that shed new light on gatekeeping. First, although the academic community agrees that openness leads to experimentation, reduced innovation costs, and a greater variety of features, services, and products offered [44,45,76,94], other contributors pointed out that a more closed approach prevents appropriation by external participants, reduces uncertainty in the technical evolution of the platform, increases security, and avoids the inclusion of actors with misaligned goals [35,38,69]. Our findings reinforce the latter view on platform openness. However, rather than advocating for closure in all online marketplaces, we highlight that in high-risk environments like OBMs, restricting external participation is critical for maintaining platform stability. By contrast, legal marketplaces can afford greater openness because external enforcement mechanisms (e.g. legal liability, customer protection, payment processors) mitigate the risks of opportunism.

Second, since gatekeeping over transactions conducted including third parties is the main source of failure in contexts characterized by conflicting actors' goals, we contribute to the understanding of the limits of decentralized governance in online marketplaces, while centralized control is more effective. This result also goes in the direction of algorithmic bureaucracy [54], according to which deviant behavior can be substantially contained by the technical infrastructure. Instead of leveraging actors' motivations, successful strategies for platform protection apply a regime of rules that standardize processes through technological (algorithmic) interfaces. Such interfaces are impersonal entities that constrain user behaviors and replace the efforts made by platform owners during platform construction. Future studies may further investigate these aspects [15].

This study offers new insights into OBM governance and gatekeeping mechanisms in extreme digital environments. Understanding the relations between rules, conflicting behaviors, and IT-based mechanisms in OBM helps in designing effective countermeasures to new forms of crimes and activates a virtuous cycle to contrast malicious cyber activities. Surprisingly, the preliminary findings of this study were reported on a post on the website Deepdotweb.com, a website known for its focus on darknet market matters (see Figure B1). However, this site, which served as a significant information source on darknet activities, was seized by law enforcement agencies shortly after our findings were published. This event underscores the relevance and impact of our research in real-world contexts, bridging the gap between academic investigation and practical implications in the realm of cyber governance and law enforcement [5,64].

Our findings can be further interpreted through the lens of governance and institutional theories that examine informal regulation and trust-building in digital environments. As already noted, the OBM context provides a relevant setting to explore how control can emerge in the absence of formal rules. As suggested by relational control theories [71,85], platform coordination may rely on norms, shared practices, and reputational mechanisms rather than on contractual obligations. We observe that OBMs activate such relational

forms of coordination through gatekeeping IT tools, rules and practices (e.g., vendor vetting, reputation thresholds, user reviews, vendor forums), even in the absence of persistent identities. These practices reflect a relational logic that substitutes formal contracting with community enforcement.

Our findings also resonate with studies on trust in digital platforms [70], which highlight how IT-based solutions can compensate for the lack of identifiable actors and external certification. Consistent with this view, our analysis shows that OBM rely heavily on algorithmic and reputation-based controls to manage trust. However, we also demonstrate that some widely used IT-based trust mechanisms may undermine platform survival in high-conflict environments. This suggests that while IT tools can foster trust, their effectiveness is contingent on governance design and context-specific constraints.

Furthermore, this study aligns with recent contributions questioning the viability of self-regulation in digital ecosystems [28, 29], by illustrating how OBMs, in the absence of formal control, develop alternative mechanisms that balance openness, trust, and risk mitigation. However, our findings nuance this debate by showing that the viability of self-regulation depends not only on the presence of IT-based controls, but also on their alignment with the platform's strategic priorities and risk exposure. In this sense, OBMs illustrate how enhanced self-regulation can be understood as an emergent governance mode, combining technical enforcement with decentralized relational dynamics. While specific to high-risk environments, these mechanisms offer insights into how platforms operating without institutional safeguards may still achieve stability and coordination.

### ***Managerial Implications***

Our study also has managerial implications. The gatekeeping mechanisms identified in OBMs provide insights relevant to other digital marketplaces where governance is complex and external regulation is weak. Our findings highlight governance strategies that may be relevant in environments where anonymity and limited oversight pose similar challenges. This contribution is relevant to privacy-preserving online markets, decentralized platforms, and peer-to-peer marketplaces, in which platform owners must regulate the behavior of sellers with no specific qualifications to offer services using their own resources. We foresee the application of these findings in the sharing economy (e.g., Airbnb, Uber). In addition, the application of these mechanisms can be extended to online markets where users trade hiding behind pseudonyms and without a trusted identity provider. Such marketplaces are spreading with novel blockchain applications [88]. Future research may assess the validity of our results in the context of NFT markets [21, 22], such as digital art marketplaces. Moreover, the study of gatekeeping in self-regulated online markets is important not only because of the raise of such markets in the bright web, but also to shed light on OBM dynamics. In fact, understanding the relations between rules, conflicting behaviors and IT-based mechanisms in OBM helps in designing regulatory approaches that balance control and autonomy in various digital environments. While some dynamics may be unique to OBMs, others can provide useful lessons for legal marketplaces dealing with unregulated or semi-regulated transactions. This knowledge can contribute to planning effective countermeasures to new forms of crimes and activates a virtuous cycle to contrast black hat phenomena [65].

While our findings are grounded in the context of OBMs, a comparison with legal marketplaces can help clarify generalizability and specificity of the observed dynamics. OBMs and regulated platforms share several structural features, such as the need to coordinate buyers and sellers, manage reputation, and secure transactions. However, the mechanisms through which these goals are achieved differ substantially. In legal marketplaces, access and transactional governance are typically supported by formal institutions, including identity verification, legal contracts, and customer service channels. These differences underscore how gatekeeping in OBMs serves as a fully endogenous governance solution, substituting for institutional trust with technical constraints and peer-based accountability. [Table 1](#) summarizes these parallels and divergences across OBMs and legal marketplaces, clarifying both the scope of our findings and the limits of their generalizability.

## Conclusions

Based on the analysis of an extreme case, this study sheds light on gatekeeping in online marketplaces operating under conditions of conflicting goals among users in the absence of formal rules and regulatory bodies. These conditions can be easily encountered in other blockchain-based platforms where the anonymity of users is guaranteed by decentralized data governance systems. While our findings highlight generalizable dynamics of gatekeeping in self-regulated environments, we do not claim full applicability to all online markets. Instead, we propose that the relational mechanisms of gatekeeping identified in this study offer relevant insights for other decentralized and lightly regulated platforms, particularly regarding the challenges of balancing openness with security. Balancing platform openness and protection in these settings may be a challenge for platform owners dealing with new users and fraudulent actors. Our study offers a nuanced view of gatekeeping mechanisms that can be used to address these challenges. We found that the involvement of third parties in gatekeeping may pose new threats to platform business.

Nevertheless, this study has certain limitations arising from the characteristics of the context and the quality of the available data. The study is based on archival and secondary data, due to the difficulty in obtaining OBM access data and the ethical implications of interviewing criminals and hackers. In addition, the quality of data collected is largely affected by the volatility of data sources due to police interventions. For example, the website that contained our main source of data was seized by a LEA on May 7, 2019.

Finally, this study also points to avenues for future research. In fact, although our main focus is not related to ecosystem effects, we observe that the OBM ecosystem persists over time in the absence of a central sponsor and with loosely interconnected complementors. An ecosystem sponsor is the organization that supports and benefits from the success of the ecosystem. The success of sponsors depends on their approach in aligning the interests of different players and building coalitions, internal actions such as managing their own commitment and creating an organizational design that supports engagement. Therefore, we believe that our empirical context can shed further light on the governance of unsponsored ecosystems. Moreover, online marketplaces also innovate by integrating technical tools developed by open-source communities (e.g., PGP, wallets in our case) that are loosely interconnected complementors in the OBM ecosystem. Therefore, a study on OBMs can be useful to gain further insight into the dynamics and functioning of innovation platforms whose value proposition is to create a shared space for the misappropriation of value.



## Disclosure statement

No potential conflict of interest was reported by the author(s).

## Notes on contributors

**FedericaCeci** (federica.ceci@unich.it) is Full Professor of Innovation and Organizational Design at the University G. d'Annunzio, Italy, where she coordinates the Ph.D. Program in Accounting, Management and Business Economics. She holds a Ph.D. in Management Engineering from the University of San Marino. Dr Ceci's research interests include digital transformation, data ecosystems, and the organizational dynamics of innovation. Her work has appeared in leading journals such as *Research Policy*, *European Journal of Information Systems*, *Industrial and Corporate Change*, *Journal of International Management*, *Industry & Innovation*, and *Information Systems Frontiers*.

**Paolo Spagnoletti** (pspagnoletti@luiss.it) is Full Professor of Organization Studies at Luiss University, Italy, where he holds the Fastweb+Vodafone Chair in Cybersecurity and Digital Transformation. He is also an adjunct professor at the University of Agder, Norway, and President of Cyber 4.0, the Italian Competence Center for cybersecurity. He holds a Ph.D. in Information Systems from Luiss University. Dr Spagnoletti's research interests include digital innovation, information infrastructures, and cybersecurity. His work has appeared in leading journals such as the *Journal of the AIS*, *Journal of Information Technology*, *Journal of Strategic Information Systems*, *Information & Management*, and *Information Systems Frontiers*.

**Andrea Prencipe** (aprencipe@luiss.it) is an academic leader with nearly 30 years of experience driving innovation in both university and corporate settings. Dr Prencipe's international career spans multiple countries, including Belgium, France, Italy, the Netherlands, Norway, the UK, the USA, and Vietnam. He began his career at SPRU (University of Sussex, UK), gaining recognition as a leading scholar in the innovation studies community, with publications in such prestigious academic journals as *Administrative Science Quarterly* and *Organization Science* and top-tier practitioner journals such as *California Management Review*. He has been Associate Editor of the *Journal of Management Studies*.

## References

1. Adam, M.; Croitor, E.; Werner, D.; Benlian, A.; and Wiener, M. Input control and its signalling effects for complementors' intention to join digital platforms. *Information Systems Journal*, 33, 3 (2023), 437–466. [10.1111/isj.12408](https://doi.org/10.1111/isj.12408)
2. Afilipoaie, A., and Shortis P. (2015). International law enforcement agencies target the Dark Net in November (2014), Global Drug Policy Observatory
3. Ahrne, G.; Aspers, P.; and Brunsson, N. The organization of markets. *Organization Studies*, 36, 1 (2015), 7–27. [10.1177/0170840614544557](https://doi.org/10.1177/0170840614544557)
4. Aldridge, J.; and Décary-Héту, D. Hidden wholesale: The drug diffusing capacity of online drug cryptomarkets, *International Journal of Drug Policy*, 35, 9 (2016), 7–15. [10.1016/j.drugpo.2016.04.020](https://doi.org/10.1016/j.drugpo.2016.04.020)
5. Bachura, E.; Valecha, R.; Chen, R.; and Rao, HR. The OPM data breach: an investigation of shared emotional reactions on Twitter. *MIS Quarterly*, 46, 2 (2022) 881–910. [10.25300/MISQ/2022/15596](https://doi.org/10.25300/MISQ/2022/15596)
6. Bakken, S.; Moeller, K.; and Sandberg, S. Coordination problems in cryptomarkets: Changes in cooperation, competition and valuation. *European Journal of Criminology*, 15, 4 (2017), 442–460. [10.1177/1477370817749177](https://doi.org/10.1177/1477370817749177)
7. Barzilai-Nahon, K. Toward a theory of network gatekeeping: A framework for exploring information control. *Journal of the American Society for Information Science and Technology*, 59, 9 (2017), 1493–1512. [10.1002/asi.20857](https://doi.org/10.1002/asi.20857)

8. Beckert, J.; and Wehinger, F. In the shadow: Illegal markets and economic sociology. *Socioeconomical Review*, 11, 1 (2013), 5–30. [10.1093/ser/mws020](https://doi.org/10.1093/ser/mws020)
9. Benlian, A.; Hilkert, D.; and Hess, T. How open is this platform? The meaning and measurement of platform openness from the complementors' perspective. *Journal of Information Technology*, 30, 3 (2015), 209–228. [10.1057/jit.2015.6](https://doi.org/10.1057/jit.2015.6)
10. Bhaskar, V.; Linacre, R.; and Machin, S. The economic functioning of online drugs markets. *Journal of Economic Behavior & Organization*, 159, (2019), 426–441.
11. Branwen, G.; Christin, N.; Decary-Hetu, D.; and Andersen RM. Dark Net Market Archives 2015. <http://www.gwern.net/Black-maretarchives> (accessed on August 23, 2022).
12. Broekhuizen, T.; Emrich, O.; Gijzenberg M.; Broekhuis, M.; Donkers, B.; and Sloot L.M. Digital platform openness: Drivers, dimensions and outcomes. *Journal of Business Research*, 122, (2021), 902–914. [10.1016/j.jbusres.2019.07.001](https://doi.org/10.1016/j.jbusres.2019.07.001)
13. Bullough, A.; Renko, M.; and Abdelzaher, D. Women's business ownership: Operating within the context of institutional and in-group collectivism. *Journal of Management*, 43, 7 (2017), 2037–2064. [10.2139/ssrn.3460206](https://doi.org/10.2139/ssrn.3460206)
14. Buskirk, J. van; Roxburgh, A.; Bruno, R.; Naicker, S.; Lenton, S.; Sutherland, R.; et al. Characterising dark net marketplace purchasers in a sample of regular psychostimulant users. *International Journal of Drug Policy*, 35, (2016), 32–37. [10.1016/j.drugpo.2016.01.010](https://doi.org/10.1016/j.drugpo.2016.01.010)
15. Butler, T.; Gozman, D.; and Lyytinen, K. The regulation of and through information technology: Towards a conceptual ontology for IS research. *Journal of Information Technology*, 38, 8 (2023), 86–107. [10.1177/02683962231181147](https://doi.org/10.1177/02683962231181147)
16. Cennamo, C.; and Santalo, J. Platform competition: Strategic trade-offs in platform markets. *Strategic Management Journal*, 34, 11 (2013), 1331–1350. [10.1002/smj.2066](https://doi.org/10.1002/smj.2066)
17. Chainalysis. *The 2020 state of Crypto-Crime*. 2020. <https://go.chainalysis.com/2020-state-of-crypto-crime-Part1.html> (accessed on)
18. Chaudhry, P.E. The looming shadow of illicit trade on the internet. *Business Horizons*, 60, 1 (2017), 77–89. [10.1016/j.bushor.2016.09.002](https://doi.org/10.1016/j.bushor.2016.09.002)
19. Chen, Y.; Chen, L.; Zou, S.; and Hou, H. Easy to start, hard to persist: Antecedents and outcomes of entrepreneurial persistence in online marketplaces. *International Journal of Electronic Commerce*, 25, 4, (2021), 469–496. [10.1080/10864415.2021.1967003](https://doi.org/10.1080/10864415.2021.1967003)
20. Conboy, K.; Fitzgerald, G.; and Mathiassen, L. Qualitative methods research in information systems: Motivations, themes, and contributions. *European Journal of Information Systems*, 21, (2012), 113–118. [10.1057/ejis.2011.57](https://doi.org/10.1057/ejis.2011.57)
21. Craig, K.; Sadovykh, V.; Sundaram, D.; and Peko, G. Introduction to the Special Section: Blockchain and nonfungible tokens in electronic commerce. *International Journal of Electronic Commerce*, 28, 1 (2024), 31–32. [10.1080/10864415.2023.2295069](https://doi.org/10.1080/10864415.2023.2295069)
22. Creswell, J.W. *Research Design: Qualitative, Quantitative, and Mixed Methods*. Thousand Oaks: SAGE, 2003.
23. Creswell, J.W.; and Clark, VLP. *Designing and Conducting Mixed Methods Research*. Thousand Oaks: SAGE, 2017.
24. Croitor, E.; Adam, M.; and Benlian, A. Perceived input control on digital platforms: a mixed-methods investigation of web-browser platforms. *Journal of Decision Systems*, 30, 1 (2021), 50–71. [10.1080/12460125.2020.1815440](https://doi.org/10.1080/12460125.2020.1815440)
25. Croitor, E.; and Benlian, A. Perceived input control on online platforms from the application developer perspective: Conceptualisation and scale development. *Journal of Decision Systems*, 28, 1 (2019), 19–40. [10.1080/12460125.2019.1616977](https://doi.org/10.1080/12460125.2019.1616977)
26. Cuel, R.; Ceci, F.; Pappas, I.; and Senyo, PK. Transformation and Sustainability of Digital Platforms and Ecosystems: A Multidisciplinary Exploration. *International Journal of Electronic Commerce*, 28, 2 (2024), 148–155. [10.1080/10864415.2024.2332045](https://doi.org/10.1080/10864415.2024.2332045)
27. Cusumano, M.; Gawer, A.; and Yoffie, D. *The Business of Platforms: Strategy in the Age of Digital Competition, Innovation, and Power*. New York: Harper Business, 2019.
28. Cusumano, M.; Gawer, A.; and Yoffie, D. Can self-regulation save digital platforms? *Industrial and Corporate Change*, 30, 5 (2021), 1259–1285. [10.1093/icc/dtab052](https://doi.org/10.1093/icc/dtab052)

29. E;Dattée, B.; Alexy, O.; and Autio, E. Maneuvering in poor visibility: How firms play the ecosystem game when uncertainty is high. *Academy of Management Journal*, 61, 2 (2018), 466–498. [10.5465/amj.2015.0869](https://doi.org/10.5465/amj.2015.0869)
30. Décary-Hétu, D.; and Giommoni, L. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, 67, (2017), 55–75. [10.1007/s10611-016-9644-4](https://doi.org/10.1007/s10611-016-9644-4)
31. Dijck, J. van; Poell, T.; and De Waal, M. *The Platform Society: Public Values in a Connective World*. New York: Oxford Academic, 2018. [10.1093/oso/9780190889760.001.0001](https://doi.org/10.1093/oso/9780190889760.001.0001)
32. Duxbury, S.; and Haynie, D. Building them up, breaking them down: Topology, vendor selection patterns, and a digital drug market's robustness to disruption. *Social Networks*, 52, 1, (2018), 238–250. [10.1016/j.socnet.2017.09.002](https://doi.org/10.1016/j.socnet.2017.09.002)
33. Eisenmann, T.; Parker, G.; and Van Alstyne, M. Opening platforms: how, when and why? In: A. Gawer (ed.) *Platforms, Markets and Innovation*. Northampton, MA: Edward Elgar, 2009, pp. 131–162.
34. Eisenmann, T.; Parker, G., and van Alstyne, M. Strategies for two-sided markets. *Harvard Business Review*, 84, 10, (2005) 92. ()
35. Farrell, J.; and Simcoe, T. Four paths to compatibility. In M. Peitz and J. Waldfoegel (eds.) *The Oxford Handbook of the Digital Economy*. Oxford University Press, 2012, pp. 34–58. [10.1093/oxfordhb/9780195397840.013.0002](https://doi.org/10.1093/oxfordhb/9780195397840.013.0002)
36. Ferguson, R. Offline 'stranger' and online lurker: methods for an ethnography of illicit transactions on the darknet. *Qualitative Research*, 17, 6 (2017), 683–698. [10.1177/1468794117718894](https://doi.org/10.1177/1468794117718894)
37. Ghazawneh, A.; and Henfridsson, O. Balancing platform control and external contribution in third-party development: The boundary resources model. *Information Systems Journal*, 23, 2 (2013), 173–192. [10.1111/j.1365-2575.2012.00406.x](https://doi.org/10.1111/j.1365-2575.2012.00406.x)
38. Greenstein, S. Open platform development and the commercial Internet. *Platforms, markets and innovation*, (2009), pp. 219–248.
39. Gu, G.; and Zhu, F. Trust and disintermediation: Evidence from an online freelance marketplace. *Management Science*, 67, 2 (2021) 794–807. [10.1287/mnsc.2020.3583](https://doi.org/10.1287/mnsc.2020.3583)
40. Guo, W.; Straub, D.; Zhang, P.; and Cai, Z. How trust leads to commitment on micro-sourcing platforms: unraveling the effects of governance and third-party mechanisms on triadic micro-sourcing relationships. *MIS Quarterly*, 45, 3 (2021), 1309–1348. [10.25300/MISQ/2021/14349](https://doi.org/10.25300/MISQ/2021/14349)
41. Hagiu, A. Strategic decisions for multisided platforms. *MIT Sloan Management Review*, 55, 2 (2014), 71.
42. Han, A.; and Hausman, J. Flexible parametric estimation of duration and competing risk models. *Journal of Applied Econometrics*, 5, 1 (1990) 1–28. [10.1002/jae.3950050102](https://doi.org/10.1002/jae.3950050102)
43. He, B.; Patel, M.; Zhang, Z.; and Chang, K. Accessing the Deep Web. Attempting to locate and quantify material on the Web that is hidden from typical search techniques. *Communications of the ACM*, 50, 5 (2007), 94–101. [10.1145/1230819.1241670](https://doi.org/10.1145/1230819.1241670)
44. Hippel, E. von. *Democratizing Innovation*. Cambridge, MA: MIT Press, 2005.
45. Hippel, E. von; and Krogh, G. von. Open source software and the “private-collective” innovation model: Issues for organization science. *Organization Science*, 14, 2 (2003) 209–223. [10.1287/orsc.14.2.209.14992](https://doi.org/10.1287/orsc.14.2.209.14992)
46. Holt, T.; Smirnova, O.; and Hutchings, A. Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, 2, 2, (2016), 137–145. [10.1093/cybsec/tyw007](https://doi.org/10.1093/cybsec/tyw007)
47. Hout, M. van; and Bingham, T. Responsible vendors, intelligent consumers: Silk Road, the online revolution in drug trading. *International Journal of Drug Policy*, 25, 2 (2014), 183–189. [10.1016/j.drugpo.2013.10.009](https://doi.org/10.1016/j.drugpo.2013.10.009)
48. Hu, X.; Lin, Z.; Whinston, A.; and Zhang, H. Hope or hype: On the viability of escrow services as trusted third parties in online auction environments. *Information Systems Research*, 15, 3 (2004), 236–249. [10.1287/isre.1040.0027](https://doi.org/10.1287/isre.1040.0027)
49. Huber, T.; Kude, T.; and Dibbern, J. Governance practices in platform ecosystems: Navigating tensions between cocreated value and governance costs. *Information Systems Research*, 28, 3 (2017), 563–584. [10.1287/isre.2017.0701](https://doi.org/10.1287/isre.2017.0701)

50. Islam, H.; Farrell, M.; Nair, A.; and Zhang, J. Understanding transaction platform governance and conflicts: A configuration approach. *Technological Forecasting and Social Change* 189, (2023), 122382. [10.1016/j.techfore.2023.122382](https://doi.org/10.1016/j.techfore.2023.122382)
51. Jarrahi, M.; Sutherland, W.; Nelson, S.; and Sawyer, S. Platformic management, boundary resources for gig work, and worker autonomy. *Journal of Computer Supported Cooperative Work*, 29, (2020), 153–189. [10.1007/s10606-019-09368-7](https://doi.org/10.1007/s10606-019-09368-7)
52. Karunakaran, A. In Cloud we trust? Co-opting occupational gatekeepers to produce normalized trust in platform-mediated interorganizational relationships. *Organization Science*, 33, 3 (2020), 1188–1211. [10.1287/orsc.2021.1469](https://doi.org/10.1287/orsc.2021.1469)
53. Kirchner, S.; and Schüßler, E. The organization of digital marketplaces: Unmasking the role of internet platforms in the sharing economy. In G. Ahrne and N. Brunsson (eds.), *Organization Outside Organizations*. Cambridge: Cambridge University Press, 2019, pp. 131–154.
54. Kokshagina, O.; Reinecke, P.; and Karanasios, S. To regulate or not to regulate: Unravelling institutional tussles around the regulation of algorithmic control of digital platforms. *Journal of Information Technology*, 38, 2 (2023), 160–179. [10.1177/02683962221114408](https://doi.org/10.1177/02683962221114408)
55. Kraemer-Mbula, E.; Tang, P.; and Rush, H. The cybercrime ecosystem: Online innovation in the shadows? *Technological Forecasting and Social Change*, 80, 3 (2013), 541–555. [10.1016/j.techfore.2012.07.002](https://doi.org/10.1016/j.techfore.2012.07.002)
56. Kretschmer, T.; Leiponen, A.; Schilling, M.; and Vasudeva G. Platform ecosystems as meta-organizations: Implications for platform strategies. *Strategic Management Journal*, 43, 3 (2022), 405–424. [10.1002/smj.3250](https://doi.org/10.1002/smj.3250)
57. Kwon, K.; Oh, O.; Agrawal, M.; and Rao, H. Audience gatekeeping in the Twitter service: An investigation of tweets about the 2009 Gaza conflict. *AIS Transactions on Human-Computer Interaction*, 4, 4 (2012) 212–229. <https://aisel.aisnet.org/thci/vol4/iss4/1>
58. Lee, A.; and Baskerville, R. Generalizing generalizability in information systems research. *Information Systems Research*, 14, 3 (2003), 221–243. [10.1287/isre.14.3.221.16560](https://doi.org/10.1287/isre.14.3.221.16560)
59. Lee, E.; and Wang, J. *Statistical Methods for Survival Data Analysis*. John Wiley & Sons, 2003.
60. Lee, J.; Yoo, C.; Wang, J.; and Rao, H. Use of body worn camera (BWC) in gray scenarios: A law enforcement officers' perspective. *European Journal of Information Systems*, 33, 4 (2023) 597–616. [10.1080/0960085X.2023.2213450](https://doi.org/10.1080/0960085X.2023.2213450)
61. Linder, C. The entrepreneurial criminal: How trust coordinates illicit drug cryptomarkets. In B. Sergi and C. Scanlon (eds.), *Entrepreneurship and Development in the 21st Century*. Emerald Publishing Limited, 2019, pp. 171–89. [10.1108/978-1-78973-233-720191010](https://doi.org/10.1108/978-1-78973-233-720191010)
62. Locke, E. The case for inductive theory building. *Journal of Management*, 33, 6 (2007), 867–890. [10.1177/0149206307307636](https://doi.org/10.1177/0149206307307636)
63. Luo, W.; and Cook, D. An empirical study of trust of third party rating services. *Journal of Computer Information Systems*, 48, 2 (2008), 66–73. <https://www.tandfonline.com/doi/abs/10.1080/08874417.2008.11646010>
64. Mahmood, M.; Siponen, M.; Straub, D.; Rao, H.; and Raghu, T. Moving toward black hat research in information systems security: An editorial introduction to the special issue. *MIS Quarterly*, 34, 3 (2010), 431–433. [10.2307/25750685](https://doi.org/10.2307/25750685)
65. Munksgaard, R.; Demant, J.; and Branwen, G. A replication and methodological critique of the study “Evaluating drug trafficking on the Tor Network.” *International Journal of Drug Policy*, 35, (2016), 92–96. [10.1016/j.drugpo.2016.02.027](https://doi.org/10.1016/j.drugpo.2016.02.027)
66. Odaba, M.; Holt, T.; and Breiger, R. Governance in Online Stolen Data Markets. In: J. Beckert and M. Dewey (eds) *The Architecture of Illegal Markets: Towards an Economic Sociology of Illegality in the Economy*. Oxford University Press, 2017, pp. 87–107. [10.1093/oso/9780198794974.003.0005](https://doi.org/10.1093/oso/9780198794974.003.0005)
67. O'Mahony, S.; and Karp, R. From proprietary to collective governance: How do platform participation strategies evolve? *Strategic Management Journal*, 43, 3 (2022), 530–562. [10.1002/smj.3150](https://doi.org/10.1002/smj.3150)
68. Paquet-Clouston, M.; Décary-Héty, D.; and Morselli, C. Assessing market competition and vendors' size and scope on AlphaBay. *International Journal of Drug Policy*, 54, 4, (2018), 87–98. [10.1016/j.drugpo.2018.01.003](https://doi.org/10.1016/j.drugpo.2018.01.003)

69. Parker, G.; and van Alstyne M. Innovation, openness, and platform control. *Management Science*, 64, 7 (2017), 3015–3032. [10.1287/mnsc.2017.2757](https://doi.org/10.1287/mnsc.2017.2757)
70. Pavlou, P.; and Gefen, D. Building effective online marketplaces with institution-based trust. *Information systems research*, 15, 1, (2004) 37–59. [10.1287/isre.1040.0015](https://doi.org/10.1287/isre.1040.0015)
71. Poppo, L.; and Zenger, T. Do formal contracts and relational governance function as substitutes or complements? *Strategic Management Journal*, 23, 8 (2002) 707–725. [10.1002/smj.249](https://doi.org/10.1002/smj.249)
72. de Reuver, M.; and Bouwman, H. Governance mechanisms for mobile service innovation in value networks. *Journal of Business Research*, 65, 3 (2012), 347–354. [10.1016/j.jbusres.2011.04.016](https://doi.org/10.1016/j.jbusres.2011.04.016)
73. de Reuver, M., Sørensen, C.; and Basole, R. The digital platform: A research agenda. *Journal of Information Technology*, 33, 2 (2018), 124–135. [10.1057/s41265-016-0033-3](https://doi.org/10.1057/s41265-016-0033-3)
74. Rietveld, J.; and Schilling, M. Platform competition: A systematic and interdisciplinary review of the literature. *Journal of Management*, 47, 6 (2021), 528–563. [10.1177/0149206320969791](https://doi.org/10.1177/0149206320969791)
75. Sarker, S.; Xiao, X.; and Beaulieu, T. Guest Editorial: Qualitative studies in information systems: A critical review and some guiding principles. *MIS Quarterly*, 37, 4 (2013), iii–xviii.
76. Sims, J.; and Seidel, V. Organizations coupled with communities: The strategic effects on firms engaged in community-coupled open innovation. *Industrial and Corporate Change*, 26, 4 (2016), 647–665. [10.1093/icc/dtw043](https://doi.org/10.1093/icc/dtw043)
77. Soska, K.; and Christin, N. Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. In SEC'15: Proceedings of the 24th USENIX Conference on Security Symposium. 2015, pp. 33–48.
78. Spagnoletti, P.; Ceci, F.; and Bygstad, B. Online Black-Markets: An investigation of a digital infrastructure in the dark. *Information Systems Frontiers*, 24, 6 (2022), 1811–1826. [10.1007/s10796-021-10187-9](https://doi.org/10.1007/s10796-021-10187-9)
79. Spagnoletti, P.; Resca, A.; and Lee, G. A design theory for digital platforms supporting online communities: A multiple case study. *Journal of Information Technology*, 30, 4 (2015), 364–380. [10.1057/jit.2014.37](https://doi.org/10.1057/jit.2014.37)
80. Spahiu, E.; Spagnoletti, P.; and Sposito, A. Building a blockchain-based platform for interbank collaboration. *International Journal of Electronic Commerce*, 28, 2, (2024), 269–291. [10.1080/10864415.2024.2332051](https://doi.org/10.1080/10864415.2024.2332051)
81. Steur, A.; and Seiter, M. Properties of feedback mechanisms on digital platforms: An exploratory study. *Journal of Business Economics*, 91, 4, (2021) 479–526. [10.1007/s11573-020-01009-6](https://doi.org/10.1007/s11573-020-01009-6)
82. Teddlie, C., and Tashakkori, A. Mixed methods research. In N. Denzin and Y. Lincoln (eds.), *The Sage Handbook of Qualitative Research* 2nd edition. London: SAGE 912, 2011.
83. Thies, F.; Wessel, M.; and Benlian, A. Effects of social interaction dynamics on platforms. *Journal of Management Information Systems*, 33, 3 (2016), 843–873. [10.1080/07421222.2016.1243967](https://doi.org/10.1080/07421222.2016.1243967)
84. Thies, F.; Wessel, M.; and Benlian, A. Network effects on crowdfunding platforms: Exploring the implications of relaxing input control. *Information Systems Journal*, 28, 6 (2018), 1239–1262. [10.1111/isj.12194](https://doi.org/10.1111/isj.12194)
85. Tiwana, A. *Platform ecosystems: Aligning architecture, governance, and strategy*. Platform Ecosystems: Aligning Architecture, Governance, and Strategy. Newnes. 2013.
86. Tiwana, A.; and Keil, M. Control in internal and outsourced software projects. *Journal of Management Information Systems*, 26, 3 (2009), 9–44. [10.2753/MIS0742-1222260301](https://doi.org/10.2753/MIS0742-1222260301)
87. Tiwana, A.; Konsynski, B.; and Bush A. Platform evolution: Coevolution of platform architecture, governance, and environmental dynamics. *Information Systems Research*, 21, 4 (2010) 675–687. [10.1287/isre.1100.0323](https://doi.org/10.1287/isre.1100.0323)
88. Treiblmaier, H.; and Sillaber, C. The impact of blockchain on e-commerce: A framework for salient research topics. *Electronic Commerce Research and Applications*, 48, (2021), 101054. [10.1016/j.elerap.2021.101054](https://doi.org/10.1016/j.elerap.2021.101054)
89. Tzanetakis, M.; Kamphausen, G.; Werse, B.; and von Laufenberg R. The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy*, 35, 9 (2016), 58–68. [10.1016/j.drugpo.2015.12.010](https://doi.org/10.1016/j.drugpo.2015.12.010)



90. De Vaujany, F.; Fomin, V.; Haeffliger, S.; and Lyytinen, K. Rules, practices, and information technology: A trifecta of organizational regulation. *Information Systems Research*, 29, 3 (2018), 755–773. [10.1287/isre.2017.0771](https://doi.org/10.1287/isre.2017.0771)
91. Venkatesh, V.; Brown, S.; and Bala, H. Bridging the qualitative-quantitative divide: Guidelines for conducting mixed methods research in information systems. *MIS Quarterly*, 37, 1 (2013), 21–54. [10.25300/MISQ/2013/37.1.02](https://doi.org/10.25300/MISQ/2013/37.1.02)
92. van Wegberg, R.; and Verburch, T. Lost in the dream? Measuring the effects of operation bayonet on vendors migrating to dream market. *Proceedings of the Evolution of the Darknet Workshop*, 9 (2018) 1–5.
93. Wessel, M.; Thies, F.; and Benlian, A. Opening the floodgates: The implications of increasing platform openness in crowdfunding. *Journal of Information Technology*, 32, 4 (2017), 344–360. [10.1057/s41265-017-0040-z](https://doi.org/10.1057/s41265-017-0040-z)
94. West, J. How Open is open enough? Melding proprietary and open source platform strategies. *Research Policy*, 32, 7 (2003) 1259–1285. [10.1016/S0048-7333\(03\)00052-0](https://doi.org/10.1016/S0048-7333(03)00052-0)
95. Yannikos, Y.; Schäfer, A.; and Steinebach, M. Monitoring Product Sales in Darknet Shops. *ARES '18: Proceedings of the 13th International Conference on Availability, Reliability and Security*, 2018, pp. 59. [10.1145/3230833.3233258](https://doi.org/10.1145/3230833.3233258)
96. Yin, R.K. *Case Study Research: Design and Methods*. Thousand Oaks, CA: SAGE, 2009. [10.33524/cjar.v14i1.73](https://doi.org/10.33524/cjar.v14i1.73)
97. Yoffie, D.; Gawer, A.; and Cusumano, M. A study of more than 250 platforms a reveal why most fail. *Harvard Business Review*, 2, 5 (2019). <https://hbr.org/2019/05/a-study-of-more-than-250-platforms-reveals-why-most-fail>
98. Zhang, Y.; Li, J.; and Tong, T. Platform governance matters: How platform gatekeeping affects knowledge sharing among complementors. *Strategic Management Journal*, 43, 3 (2022), 599–626. [10.1002/smj.3191](https://doi.org/10.1002/smj.3191)

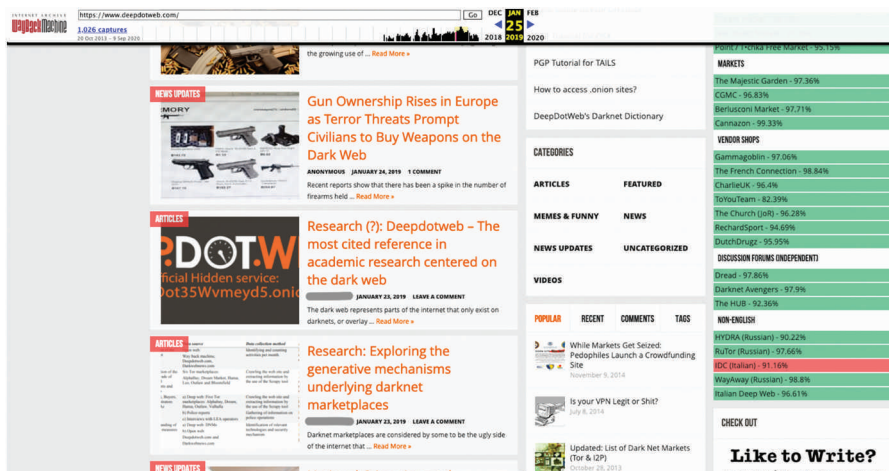


## Appendix A

**Table A1.** Descriptive Statistics of the Variables.

Variable	Type	Mean	SD	Min–Max
<i>Survival</i>	Dependent	14.844	11.745	1–45
<i>Business continuity</i>	Control	93.487	9.535	35.618–100
<i>Size</i>	Control	9.238	1.709	3.784–1.284
<i>Ratings</i>	Control	3.550	0.581	1.670–4.886
<i>Invite only</i>	Independent	0.827		0–1
<i>Forced vendor PGP</i>	Independent	0.551		0–1
<i>Multi-sSignature</i>	Independent	0.655		0–1
<i>Police operation</i>	Control	0.561		0–1
<i>Cryptocurrencies</i>	Control	0.379		0 – 1
		Value	Frequencies	Percentage
<i>Vendor bond</i>	Independent	1	25	43.10
		2	9	15.52
		3	15	25.86
		4	4	6.90
		5	5	8.62
<i>Finalize early</i>	Independent	0	39	67.24
		1	11	18.97
		2	8	13.79

## Appendix B



The screenshot displays the homepage of Deepdotweb, a platform reporting on darknet activities. The layout includes a top navigation bar with a search function and a calendar. The main content area is divided into several sections:

- News Updates:** Features articles such as "Gun Ownership Rises in Europe as Terror Threats Prompt Civilians to Buy Weapons on the Dark Web" and "Research (7): Deepdotweb – The most cited reference in academic research centered on the dark web".
- Markets:** A table listing various darknet markets and their market share percentages.
- Categories:** A list of different categories of darknet content, including "PGP Tutorial for TAILS", "How to access .onion sites?", and "DeepDotWeb's Darknet Dictionary".
- Articles:** A section for featured articles, including "Research: Exploring the generative mechanisms underlying darknet marketplaces".
- Videos:** A section for video content, including "While Markets Get Seized, Pedophiles Launch a Crowdfunding Site" and "Is your VPN Legit or Shit?".
- Popular:** A section for popular content, including "Updated: List of Dark Net Markets (Tor & I2P)".
- Check Out:** A section for recommended content, including "Like to Write?".

The right sidebar contains a "MARKETS" table with the following data:

Market	Market Share (%)
The Majestic Garden	97.36%
CGMC	96.83%
Berlusconi Market	97.71%
Canazon	99.33%

Below the markets table, there is a "VENDOR SHOPS" section with a list of vendors and their market share percentages:

Vendor	Market Share (%)
Gammagoblin	97.06%
The French Connection	98.84%
CharnelUK	98.4%
BoYouTeam	82.39%
The Church (I2P)	96.28%
ReichardtSport	94.69%
DutchDrugs	95.95%
DISCUSSION FORUMS (INDEPENDENT)	
Dread	97.86%
Darknet Avengers	97.9%
The HUB	92.36%

At the bottom, there is a "NON-ENGLISH" section with a list of non-English markets and their market share percentages:

Market	Market Share (%)
HYDRA (Russian)	90.22%
RuFor (Russian)	97.66%
IBC (Italian)	91.16%
Wayway (Russian)	98.8%
Italian Deep Web	96.61%

**Figure B1.** Screenshot of the Homepage of Deepdotweb Reporting Preliminary Findings