frontiers in Blockchain

ORIGINAL RESEARCH
published: 07 April 2020
doi: 10.3389/fbloc.2020.00004

The Private Governance of Identity on the Silk Road

*Catalina Goanta**

Law & Tech Lab/Studio Europa, Maastricht University, Maastricht, Netherlands

Long before the creation of blockchain platforms, the rise of personal computing, and Internet connectivity brought with it a digital, online dimension of the material world, leading to the socio-technical construct known as "digital identity." After the online discussion boards and emailing lists of the early 1990s, individuals started socializing via the Internet more predominantly using social networks. One specific type of platform links this online socializing and transacting to blockchain-based spaces: dark web marketplaces. Identified as second-generation cryptocommunities, dark web marketplaces deployed cryptography for the use of pseudonymous identity, for communication, but also currency. This paper explores two questions in this fascinating space: what was the role of identity on the Silk Road, and what governance lessons can be drawn from this illustration for the purpose of applying them to more recent cybercommunities such as Ethereum? The paper is structured as follows. The first part describes the Silk Road and sketches its essential characteristics. The second part looks at how individuals could become platform users on the Silk Road, by analyzing the contractual relationship between the Silk Road and an individual user based on the rights and obligations enshrined in the Silk Road terms of service (ToS). The third part critically reflects on arbitrariness as the main pitfall arising out of the private regulatory framework created by the Silk Road, and contributes to existing narratives surrounding the regulatory nature of code by proposing a code-as-procedure perspective for analyzing this regulatory framework. Part four concludes.

Keywords: dark markets, private governance, code is law, Silk Road, procedural law

OPEN ACCESS

Edited by:
Oskar Josef Gstrein,
University of Groningen, Netherlands

Reviewed by:
Richard Tighe,
Oxfam, San Francisco,
United Kingdom
Jia (Carol) Xu,
Independent Researcher, San
Francisco, CA, United States

***Correspondence:**
Catalina Goanta
catalina.goanta@
maastrichtuniversity.nl

Specialty section:
This article was submitted to Blockchain for Good, a section of the journal Frontiers in Blockchain

Received: *25 September 2019*
Accepted: *28 January 2020*
Published: *07 April 2020*

Citation:
Goanta C (2020) The Private Governance of Identity on the Silk Road. Front. Blockchain 3:4. doi: 10.3389/fbloc.2020.00004

INTRODUCTION

The inescapable interest in blockchain technology seen in the past years has ignited a lot of debate surrounding the decentralization of established legal concepts and institutions. One such example reflects discussions around the concept of identity (e.g., nationality, citizenship, or broadly speaking membership to a legally defined group), as well as the institutions administrating various aspects of identity (e.g., state agencies conferring or depriving individuals of nationality). As decentralization is seen as empowering individuals to give up the use of or dependence on intermediation (be it private or public), it gave rise to the notion of self-sovereign identity systems which ought to preserve an individual's self-determination in providing, or even expanding, the benefits of record-keeping.

This discussion has prompted a lot of interdisciplinary literature, looking at the broader themes of e-government (Reijers et al., 2016; Augot et al., 2017; Hou, 2017; Sullivan and Burger, 2017) and

smart cities (McMillan, 2014; Biswas and Muthukkumarasamy, 2016; Ibba et al., 2017; Jaffe et al., 2017; Rivera et al., 2017; Sharma et al., 2017; Marsal-Llacuna, 2018) or particularly the use of self-sovereign identity systems in development aid [e.g., the United Nations High Commissioner for Refugees (UNHCR) using blockchain to manage the identity of refugees] (Biometric Technology Today, 2017; Mears, 2018), the privacy issues posed by the use of public blockchains in the management of identity (Zyskind et al., 2015; Zhang et al., 2017; Yang et al., 2018), or the use of decentralization as a means of breaking socio-legal constructs that lead to, for example, global inequality (Freund, 2017; Michaels and Homer, 2017). Most of this literature, whether reflecting legal, sociological, or economic analyses, focuses on recent platforms such as Pavilion.io, Mattereum, or Stampery (Casino et al., 2019). However, long before the creation of these blockchain platforms, the rise of personal computing and Internet connectivity brought with it a digital, online dimension of the material world, leading to the socio-technical construct known as "digital identity" (Lemieux, 2016; Dunphy, 2018). After the online discussion boards and emailing lists of the early 1990s, individuals started socializing via the Internet more predominantly using social networks (Can and Alatas, 2019). One specific type of platform links this online socializing and transacting to blockchain-based spaces: dark web marketplaces. Identified as second-generation cryptocommunities[1] (Goanta and Hopman) dark web marketplaces deployed cryptography for the use of pseudonymous identity, for communication, but also for currency[2].

The most prominent example of such a marketplace is the Silk Road, a space only reachable through the use of The Onion Router browser (TOR) (AlQahtani and El-Alfy, 2015), where an administrator with cyberlibertarian views by the name of Ross Ulbricht managed the first iteration of a multimillion dollar illegal marketplace. While dark web user identity is not as such self-sovereign, understanding how Ross Ulbricht's platform managed the identity of registered users can provide useful insights into blockchain governance problems. Just like many well-known "idols" of the contemporary blockchain space, Ross Ulbricht's libertarian views made him especially allergic to the notion of state law limiting individual freedoms and argued not only for the reduction of government interventionism but also for the potential replacement of state law with the private rules of a community that took individual freedom as the most important value in determining its own functioning[3] (Greenberg, 2012; Bartlett, 2015).

This paper explores two questions in this fascinating space: what was the role of identity on the Silk Road[4] and what governance lessons can be drawn from this illustration for the purpose of applying them to more recent cybercommunities such as Ethereum? The paper is structured as follows. The first part describes the Silk Road and sketches its essential characteristics. The second part looks at how individuals could become platform users on the Silk Road, by analyzing the contractual relationship between the Silk Road and an individual user based on the rights and obligations enshrined in the Silk Road terms of service (ToS). The third part critically reflects on arbitrariness as the main pitfall arising out of the private regulatory framework created by the Silk Road and contributes to existing narratives surrounding the regulatory nature of code by proposing a code-as-procedure perspective for analyzing this regulatory framework. Part 4 concludes. From a methodological perspective, this paper is based on the qualitative analysis of all the documents identified by the Government of the United States as the Silk Road ToS in Ulbricht's initial indictment from 2014[5].

FEATURES OF THE SILK ROAD AS A CRYPTOCOMMUNITY

According to the United States government, the Silk Road was a dark web marketplace created by a United States citizen (Ross Ulbricht) in order to facilitate the transacting of illegal (and legal) items such as drugs[6]. The first iteration of the Silk Road was online between 2011 and 2013 (Christin, 2012), when Ulbricht started popularizing the nascent platform on various web forums to facilitate the sale of self-produced hallucinogenic mushrooms[7]. At the height of its popularity, the Silk Road managed to bring together up to 150,000 active users, mostly from the United States (see **Figure 1**). The most commonly sold product on the Silk Road was, by far, weed (see **Figure 2**).

[1] A cryptocommunity is a virtual community where cryptography is used to ensure the "security of identity, communication, currency, or more recently, value" and for the creation and/or support of political ideologies. See C. Goanta and M. Hopman, "Cryptocommunities as legal orders" 3.

[2] *Ibid.*

[3] For a general overview of the Silk Road, see A. Greenberg, *This Machine Kills Secrets: How Wikileakers, Cypherpunks, and Hacktivists Aim to Free the World's Information* (Dutton 2012); J. Bartlett, *The Dark Net* (Melville House 2015).

[4] It is important to mention that all references to Silk Road in this paper are used to designate the first iteration of this dark web marketplace. There were at least three more iterations.

[5] *United States of America v Ross William Ulbricht*, Indictment, District Court, Southern District of New York, 21 August 2014, 14 Cr. 68.

[6] *Ibid.*, Government exhibit 226D.

[7] Bartlett, fn 12, at 137.

Origin		Acceptable destinations	
Country	**Pct.**	**Country/Region**	**Pct.**
U.S.A.	43.83%	Worldwide	49.67%
Undeclared	16.29%	U.S.A.	35.15%
U.K.	10.15%	European Union	6.19%
Netherlands	6.52%	Canada	6.05%
Canada	5.89%	U.K.	3.66%
Germany	4.51%	Australia	2.87%
Australia	3.19%	World. excpt. U.S.A.	1.39%
India	1.23%	Germany	1.03%
Italy	1.03%	Norway	0.70%
China	0.98%	Switzerland	0.62%
Spain	0.94%	New Zealand	0.56%
France	0.82%	Undeclared	0.26%

FIGURE 1 | Shipping origin and destination (Christin, fn 14, at 9).

Category	#. items	Pct.
Weed	3338	13.7%
Drugs	2194	9.0%
Prescription	1784	7.3%
Benzos	1193	4.9%
Books	955	3.9%
Cannabis	877	3.6%
Hash	820	3.4%
Cocaine	630	2.6%
Pills	473	1.9%
Blotter (LSD)	440	1.8%
Money	405	1.7%
MDMA (ecstasy)	393	1.6%
Erotica	385	1.6%
Steroids, PEDs	376	1.5%
Seeds	374	1.5%
Heroin	370	1.5%
DMT	343	1.4%
Opioids	342	1.4%
Stimulants	291	1.2%
Digital goods	260	1.1%

FIGURE 2 | Top 20 product categories of items available (Ibid).

The Silk Road was partially fueled by a revolutionary vision. For the cypherpunks of the late 1980s who were the first to set libertarian ideals in cyberspace (May, 1992), the libertarian vision of freedom entailed removing the state from the affairs of its citizens. This very idea was taken over by the Silk Road, where it further developed in the wake of new tools (e.g., cryptocurrencies and hidden network services). Using those tools, Ulbricht and his helpers managed to usher in a new expression of libertarianism, where the community was mostly free to enter into transactions that states would not otherwise recognize as lawful. Still, not all members of the community shared the revolutionary vision. Given the behavioral diversity of the Silk Road's members, it comes as no surprise that not all of them believed in the platform's core philosophy. Some members show abundant support for the movement behind the platform; yet others see it as a one-stop-shop for drug commerce, and nothing more[8].

The Silk Road's effectiveness was primarily based on trust. The essential "technology" that made transactions possible between strangers who did not know or trust each other was not necessarily the cryptocurrency they were paying with—although this did make their interactions possible—but rather the reputational mechanisms that created behavioral incentives for users, both sellers and buyers, to conduct business within the parameters set by the creator of the system.

In addition, the Silk Road operated in a very intense adversarial environment. Cryptocommunities are innately built on the premise that there is a malicious entity trying to prevent the system from achieving its functions, and this is expressed in a cat-and-mouse setup between the actors of the system. For every solution an actor comes up with, there will be others trying to undermine it. For cypherpunks, the adversary was the arm of the state, which at times was real and frightening and threatened the livelihood of the group's members[9]. This tension also extended to dark markets, with one difference: because dark markets started gathering and trading in wealth, in the form of cryptocurrencies, this drew the interest of a new type of adversary—individuals or groups, with no allegiance to the state, who either were direct competitors or simply followed personal purposes (whether for entertainment, financial gain, or both) in hacking market participants, including platforms[10]. These attacks often took place in the form of phishing, where hackers would for instance make mirrors of the Silk Road website and ask users to log in, gaining access to their accounts, as well as any information seen by that user's account. This feature was further consolidated into decentralized platforms as well. At the moment, Ethereum's main adversary is not the state, but the overabundance of similar platforms and developers who might have a stake in bringing the platform down or simply drying it of its funds, as was the case with the decentralized autonomous organization (DAO) attack in 2016 (Metjahic, 2018).

On the Silk Road, only a small community had high technology literacy. Whether it entailed knowing how to operate the different cryptographic tools available on the hidden network (e.g., not falling prey to phishing attacks on TOR) or understanding the algorithms calculating the seller reputation rate or the Silk Road's fees, it becomes very clear from the forum posts of the Silk Road's first iteration that the overwhelming majority of users are in the dark[11]. This effect was most likely worsened by the operation of constant changes by the platform, as well as by the high volatility of the Bitcoin market. All these features together divided the community into two categories: the core users who understood the infrastructure of the system and its components and the users who gave up trying to understand these matters and simply relied on the user-friendly interface to get their business done. The more sophisticated these tools get in different iterations of cryptocommunities, the bigger the gap between those who know how to work with and around them and those who remain illiterate, because the cost of becoming educated on this matter might be too high, thus leading to an indirect knowledge centralization creep. In addition, as a direct result of their high behavioral heterogeneity, cryptocommunities based on decentralized platforms have been developing a fuzzy jargon that frustrates the process of gaining technological literacy (Walch, 2017).

Although a lot of the activity on the Silk Road was based on human decision making, the platform developed strong technocratic institutions. The Silk Road administrators made an effort to develop an elaborate set of legal rules to keep order in the community. By October 2011, Ulbricht had between a team of two and five administrators to run the platform, deal with complaints, resolve disputes, moderate the forum, and

[8]Goanta and Hopman, fn 9.

[9]May, fn 19.

[10]Bartlett, fn 12, at 138.

[11]Goanta and Hopman, fn 9.

track down law enforcement infiltration[12]. However, given that this team was running a website, its policy implementations were fundamentally technocratic. This led to the development of technocratic institutions, such as the algorithmic reputational mechanisms. The community was based on a set of rules, but the procedural implementation of these rules in the form of enforcement mechanisms such as algorithmic reputation systems and account management was inconsistent, as clear procedures were absent.

THE PRIVATE GOVERNANCE OF USER TRANSACTIONS ON THE SILK ROAD: RULES

That the Silk Road has libertarian roots is undeniable. Given that no recognized state in the world currently in existence can be described as a libertarian legal system, the principles behind it retain a highly philosophical dimension. In the light of this characteristic, one would expect whatever system of rules was created by the platform's operators and adhered to by the community to be a set of social and legal norms consistent with this core libertarian vision. Yet a large part of the rules applicable to the Silk Road are rules that are currently in force in national and supranational legal orders and are not just philosophical in nature. For this reason, some rules might conflict with the libertarian order, which raises the question of whether this confusion was a result of misunderstanding the role and infrastructure of legal systems in the first place. This part looks into the nature of the rules found at the core of the Silk Road operations, which can be entirely found in the Supplementary Annex 1–5 to this paper.

Charter

The Silk Road Charter is the equivalent of the platform's constitution, as it lays down its purpose and fundamental values. The purpose of the Silk Road is to provide "systems and platforms" to "customers," in order to empower them to "live as free individuals[13]." The Charter also mentions that in doing so, the Silk Road engages in the protection of "basic human rights," although these rights are not defined any further. What is, however, defined, is a set of five fundamental values.

Self-Ownership

This value revolves around the property rights cast upon individuals, which include their bodies, thoughts, and will but also "anything they create with their property or obtain without coercion." The concept of owning one's person echoes Locke's writing: "though the earth, and all inferior creatures, be common to all men, yet every man has a property in his own person: this nobody has any right to but himself. The labor of his body, and the work of his hands, we may say, are properly his" (Locke, 1821). The same ideas are also reflected in the work of Nozick and Rothbard (Nozick, 1977; Rothbard, 1978; Cohen, 1995; Van Parijs, 1995). There are however, no legal systems that embraced the idea of a right of self-ownership as described by libertarian philosophical literature, partially because the libertarian ideal of self-ownership has been labeled as a "self-defeating theory when we consider the operability and usefulness of the rights it bestows upon those who have no original resources to trade" (Cleaver, 2011). In the context of the Charter, self-ownership is an expression of an absolute personal freedom.

Responsibility

The Charter clarified the notion of responsibility by placing it in the context of accountability: "If one infringes on another's rights, they should be held accountable." The Silk Road system thus acknowledges that an infringement of rights created in this order must lead to punishment. What is unclear, however, is how the punishment is determined and who establishes and enforces it. In formal legal orders, the state holds the monopoly over the exercise or threat of violence, which it implements through, for instance, access to justice. As formal legal orders are not acknowledged in the Charter, there are two ways in which this fundamental value can be interpreted. It can first be interpreted to say that users do have access to justice, albeit private justice. In this reading, accountability takes place through a right of retribution of the wronged party. Another option is to interpret this value as authorizing the operators of the platform to act as the guardians of these values and thus penalize behavior going outside of its mandated limitations.

Equality

Equality is used in this ecosystem to express its decentralized nature, or namely, the fact that the platform's sovereign is not considered to have the same authority as the state in a peer-to-peer platform. The value of equality is an example of internal inconsistency within the Charter, as it contradicts the notion of self-ownership. The latter is based on the consideration that you can own your own body, as well as what you make and what you conquer without using force. Applied to a reality of limited resources, this idea entails that at some point in time, all resources will have been conquered and that newcomers will not have anything to conquer anymore. However, this conflicts with the principle of equality, as it expressly envisages property rights.

Integrity

The Charter defines integrity as honoring one's word. Put differently, this fundamental value embodies the centuries-old contractual principle of *pacta sunt servanda* (Wehberg, 1959; Jeremy, 2000; Mazzacano, 2011), namely, that all promises made need to be kept. In the UNIDROIT Principles of International Commercial Contracts, for instance, this principle has led to the development of specific performance remedies (Gebhardt, 1947; Vlavianos, 1993; Dizgovin, 2016). In the context of the Silk Road, this entailed that buyers could have a right of replacement in case ordered products did not meet the buyer's expectations.

Virtue

The last fundamental value is phrased in a rather confusing way: "to improve one's self and the lives of others in all actions." On the

[12] Bartlett, fn 12, at 138.

[13] Supplementary Annex 1.

one hand, it seems to refer to personal development, but on the other hand, it also refers to development as communal progress.

Terms of Service

The Silk Road ToS comprise three different documents: the Seller's Contract (Supplementary Annex 2), the Seller's Guide (Supplementary Annex 3), and the Buyer's Guide (Supplementary Annex 4). These resources bring to light quite a considerable volume of contractual rules, primarily between the platform and the sellers, as well as between the sellers and the buyers.

Seller's Contract

The Seller's Contract was a nine-line piece of text displayed to a platform user when they registered as a seller and focused on essential obligations the seller was going to be held accountable for. Most prominently, data protection and information duties (e.g., packaging and product information) references can be found therein, as follows:

Data Protection

In a way, sellers can be considered the processors of buyers' personal data, such as the buyer's shipping address. This is referred to as client anonymity. While some buyers would give fake addresses, some would use their real ones, so this posed great risks for the whole operation. The seller's role was thus to safeguard this information, and they were under a strict obligation to destroy the client's shipping address "as soon as it is used to label the package[14]."

Information Duties

In their contract with the sellers, the platform mandated the latter to bear the burden of obtaining information on matters such as staying "up-to-date on the latest stealth shipping methods" or informing themselves of the further obligations outlined in the Seller's Guide (Eisenberg, 2003; Bar-Gill and Porat, 2017).In addition, not only did sellers bear the burden of obtaining information, but they were also subject to mandatory disclosures, since they were expected to "describe the items accurately and truthfully." In a way, this clause is reminiscent of an obligation of performing their contract with the Silk Road in good faith. This is seconded by a moral norm imposed on the sellers, that of treating customers with respect, so to "go above and beyond for them."

Failure to comply with these rules resulted in the vendor account being banned. The Silk Road seemed to have formalized this agreement with its sellers by retrieving consent in a very explicit manner: "By clicking 'I agree' at the bottom, you agree to abide by the guidelines and terms below when selling on Silk Road."

Seller's Guide

As mentioned in the Seller's Contract, sellers had to inform themselves of the obligations outlined in an additional document which was available on the Silk Road's wiki. The need for the centralization of rules and procedures used on the Silk Road was felt by the community as a whole, and the emergence of a wiki page was announced by Dread Pirate Roberts (DPR) at an early stage of the platform's existence: "Hey gang, I want to set up a Silk Road wiki so we can have all of the FAQ's answered in one spot and hopefully remove some of the clutter of repeated questions from the forum. Anyone who's set up a wiki before want to administer this? I could do it, but I want to get more community members involved and a wiki is a great community project anyway[15]."

The final wiki was ready by November[16], and it served as an information management resource users could inspect to understand how different aspects of the platform worked. At the same time, the administrators who had been appointed by DPR to compile the wiki also added—most likely with his permission—the Seller's and the Buyer's Guides.

As far as the seemingly legal obligations in the Seller's Guide are concerned, they were not few.

Data Protection

The obligation of destroying any shipping address information once the package was shipped is complemented with the prohibition of obtaining any personal information from the buyers. The action of saving customer addresses could lead to the revocation of seller privileges.

Obligations Relating to Payment

The processing of payment was the Silk Road's monopoly, expressed in the escrow system, which entailed that any payment had to be held by the platform until the buyer notified the receipt of the goods, at which point the payment would be released to the seller. The Seller's Guide makes it clear that if payments do not go through the escrow system, this can cost sellers their accounts. There were two exceptions to when party agreement overruled this principle: (i) the website being down and (ii) "closing early," namely, releasing funds from escrow before the arrival of the goods.

Fiscal Policies

The Silk Road's success was based on the possibility of using Bitcoin. However, Bitcoin was a highly volatile currency, and the platform came up with two options for its sellers: (i) the possibility to pegging listings to either the dollar or Bitcoin and (ii) the possibility to use "escrow hedging," namely, to reduce the losses of fiscal depreciation for payments that were placed in escrow.

Restricted Items

The Seller's Guide specifies that any items that serve to "harm or defraud, such as stolen items or info, stolen credit cards, counterfeit currency, personal info, assassinations, and weapons of any kind" were indirectly considered to be immoral and therefore not permitted.

Customer Service

Sellers are encouraged to behave in good faith; otherwise, they are warned that the platform's reputational mechanisms will not

[14]Supplementary Annex 2.

[15]https://antilop.cc/sr/users/dpr/threads/20110826-0208-Silk_Road_wiki.html

[16]https://antilop.cc/sr/users/dpr/threads/20111110-1711-Announcing_the_official_Silk_Road_Wiki.html

help their business goals. Tampering with these systems (e.g., leaving feedback for yourself as a seller from a dummy account) would be sanctioned with the revocation of privileges. The same goes for threatening customers "even if it is a veiled threat" and lying about shipping out goods. In other terms, defects of consent equivalent to misrepresentation or fraud would result in the harshest punishment, namely, killing the account.

Buyer Statistics

This is a reference to the algorithmic reputational mechanism used to determine the reliability of the buyer (Resnick and Zeckhauser, 2002; Mudambi and Schuff, 2010; Motoyama et al., 2011). The role of these systems is to remedy the trust issues arising out of the context of concluding pseudonymous transactions.

Seller Pages

An example of a mandated disclosure identified in the documents was the reputation system created by the platform. Available in different versions throughout the life span of the Silk Road, an algorithm would calculate consumer feedback, leading to a score (e.g., 100% positive feedback), which also allowed the seller to be ranked vis-à-vis the other sellers on the platform. Sellers could not opt out of this system, and as such, it would not lead to any consumer rights, because its role was to flag bad actors. Voluntary disclosures related to transaction details such as guarantees for seized orders, pricing, and shipping; office hours for incoming orders; shipping options; or the payment and escrow policy. Voluntary disclosures were made at the seller's discretion. However, interestingly, these disclosures did not only include transactional limitations (e.g., "I only accept payment through the Silk Road") but also generated rights. This is an example of a consumer right of replacement arising out of the "Seized Orders Guarantee" practices by the seller going by the name Variety Jones: "Any orders stolen by customs will be replaced and re-shipped at absolutely no charge to you. It's not your fault if the thieving bastards intercepted your order, and I believe it is my responsibility to package your order stealthily enough to make it to your door. If they steal it again, I will replace it again, once again at absolutely no charge to you. I will not stop until you get your order. I may request that you use a different mailing address for replacement orders. I fucking hate those goddam customs wankers, and want you to be confident you will receive what you pay for[17]."

Buyer's Guide

As we have seen above, the Seller's Guide includes a number of obligations the seller is bound to by agreeing to the Seller's Contract. The Buyer's Guide reproduces a lot of information from the Seller's Guide (e.g., escrow hedging and buyer statistics). However, this information does not seem to give rise to specific rights, nor are there similar obligations as for the sellers. For instance, there is no specific reference to the revocation of buyer privileges if the escrow system is not respected. From this perspective, the Buyer's Guide seems to be a collection of voluntary disclosures made by the Silk Road; yet it is not clear from the wiki whether the platform also considered the relationship with the buyer to have a contractual nature.

One aspect that is much more detailed in the Buyer's Guide rather than the Seller's Guide is the reference to the escrow. In addition to the information on the release of the payment, this part elaborates on what happens if the seller and the buyer do not agree on whether the shipment has been made. The guide specifies that should the package never arrive or arrive not in the expected condition, there might be a right—most likely given by the sellers themselves—to ask for a full or partial refund. To be eligible, buyers would have to click a "resolve" button, and that would give them access to the "resolution center," where the two parties would initially try to solve the dispute bilaterally, and "'in the rare event that an agreement can't be reached, a Silk Road admin would be right there to mediate and investigate if necessary." This demonstrates the existence of a platform-led dispute resolution body adjudicating potential issues arising out of problematic deals (Ortolani, 2016).

This section analyzed and classified the various types of legal rules that can be extracted from the contractual relationship between the Silk Road as a platform and its users, to exemplify the rights and obligations undertaken within this transaction framework. In what follows, these rules are further put into context from the perspective of identity management.

IDENTITY MANAGEMENT ON THE SILK ROAD AS A START-UP STATE

A lot has been written about the pseudonymous identity of Silk Road users (Huang, 2015; Kozinski, 2015; DiPiero, 2017; Holm, 2017). As a place where users themselves considered they broke the laws of their own states either because they would not recognize their legitimacy or simply want to shop for other legal standards, the Silk Road would make use of digital aliases as a way to hedge users from the risks incurred by engaging in commerce on the platform. However, what is less explored is the fact that in becoming users on the Silk Road, individuals would have to create accounts which were under the direct control of the Silk Road administrator. The management of these accounts would thus become an administrative task of implementing the platform's main rules and principles, albeit in a seemingly arbitrary way. As the administrator, Ulbricht had the possibility to demote sellers, to ban users from the forum, or most importantly to "kill users" (see Supplementary Annex 5). It remains unclear how exactly Ulbricht has made use of this discretion. However, what can be determined is the fact that the Silk Road operated in an organic way, namely, by dealing with issues as they came along. For instance, when Ulbricht writes the forum post regarding the creation of a Silk Road wiki, he does not mandate it to specific users but rather asks for their opinion and collaboration. When forum participants indicate they believe a wiki would not necessarily solve the questions most users would repetitively turn to the forum to (e.g., how the reputation system worked; how escrow worked; and what intermediation fee was charged by the Silk Road), Ulbricht shared

[17] https://antilop.cc/sr/vendors/

with the community his doubts in moving further with the idea: "hmmm . . . figured someone would want to do this. I guess I'll figure out how to set it up. reply to this thread if you want to be a contributor to the wiki[18]." This interaction is illustrative of the many *ad hoc* ideas and decisions that needed to be made in the course of the platform's life. Unlike a traditional legal system, systematically coupled with procedures which allow for the implementation of rights and obligations, the Silk Road was a victim of the consideration that libertarianism does not require rules. In addition, none of the admins, including Ulbricht himself, had any experience or training in governance. In such a context, the Silk Road legal concepts come across as the creations of a start-up state, with little to no systematization in rule-making, as well as with questionable consistency.

This raises two main points that are pertinent for the digital identity discussion, stemming from the same consideration, namely, that not acknowledging the importance of procedural rules affects the delivery of justice in cyberspace: first, as a private, hidden platform acting as an administrative institution keeping records of its users, the Silk Road can be an (extreme) illustration of the pitfalls of the private governance of identity; second, the Silk Road generated its own legal standards and also created the infrastructure necessary for the enforcement of these standards, which can be a relevant illustration for the code-is-law narrative coined decades ago by Lessig (2000).

As far as the first point goes, the Silk Road example seems to have an almost prescient nature as it unfolded years before the conspicuous content moderation debates which currently weigh heavily on the shoulders of social media platforms (Klonick, 2018; Langvardt, 2018; Witt et al., 2019). The Silk Road used a contractual relationship to impose various rights and obligations to its users. Yet while a cyberlibertarian orientation allegedly formed the basis of the platform's activities, the platform administrator had a literal kill switch to deal with accounts promoting undesirable activities. Such actions would arguably be based on the violations of the platform's ToS. However, as it is currently clear also in the context of social media content moderation, the content of community guidelines and its enforcement are two separate issues that do not always overlap. The discretion Ulbricht seems to have enjoyed in taking measures against platform users is a random enforcement mechanism undermining the vision and principles expressed, for instance, in the Silk Road charter (see Supplementary Annex 1). The measures the administrator would be able to take against platform users can be considered a restriction of the user identity in the given socioeconomic context. This is comparable to the ancient practices around Roman citizenship (Koops, 2012). Roman citizenship can perhaps reflect one of the clearest examples of how access to rights and privileges can influence a person's identity within a defined social group (Kunkel, 1975): during the Republic and the Principate, only Roman citizens would live according to the so-called *ius civile* (Van den Bergh, 2011). All the rights that defined *ius civile* would only apply to citizens, and their application was overseen by a *praetor urbanus*, in front of whom citizens would have recourse to actions or defenses protecting their economic interests. Non-citizens were thus invisible from the perspective of *ius civile*[19] (Hitch, 1932). The issue of access to justice brings with it the question of exclusion on the basis of identity and the inherent ways of gaming this system through identity theft. In an online environment where a pseudonymous account is the only way of interacting with the community, banning users, or killing their accounts—and with that any reputation or community standing the user may have earned—leads to the same arbitrary exclusion from the identity management system that may have warranted the creation of multiple identities or other forms of retaliation. On the one hand, the administrator believed he was administering justice when he exercised his powers. On the other hand, whatever justice was served to the community, it did not systematically apply to all its members in the same way, because while he mimicked the creation of market-based institution to protect trade, it can be argued that Ulbricht failed—or was unwilling to—to mimic the rule of law. This is the very same problem content moderation platforms currently deal with, even when they try to design specific access to justice institutions like Facebook's new appellate court for content oversight (Constine, 2019). The lack of justice fora and principles for the delivery of justice also remains one of the main problems in current blockchain governance debates. In one of his governance statements, Ethereum core developer Vlad Zamfir states that "the blockchain should be governed on a basis of global cooperation between self-selecting members and entities from the global public" (Zamfir, 2018). Still, the institutionalization of this cooperation and the functioning of the Ethereum blockchain as a public good in terms of administering justice when harms occur remain ideals that have so far not materialized.

The second point to be made in relation to identity management systems has to do with the nature of the rules on the Silk Road. The Silk Road reputation system, together with its pseudonymous user registration, was the expression of identity certification on the dark market place. In Lessig's seminal piece proposing computer codes as a regulator of cyberspace[20], he warned that for instance privacy can be coded in the identification architecture (which is the actual practice of the Silk Road) and that cyberspace would end up being regulated by cyberspace (De Filippi and Wright, 2018). This narrative is increasingly used in contemporary cryptocommunities, like those formed around various blockchains, especially in the light of self-enforcing tools such as smart contracts, where the code is law, literally[21]. Calling the code the regulator of cyberspace, however, takes away from how law really works in society: substantive rules are made to define the body of rights and obligations benefitting or imposed on legal subjects, and procedural rules determine how substantive rules are applied in practice. While the formalism attached to procedural rules is considered to be

[18] Fn 36.

[19] They would carry with them their own laws; see R. M. Hitch, 'Our Debt to Roman Law' (1932) 13 Loy LJ 66, 71.

[20] Lessig, fn 32.

[21] *Ibid.*

a trait of continental civil law[22] (La Porta et al., 2008). the same formalism can serve to enrich the code-is-law narrative by adding the perspective of the code as procedure. Rights and obligations themselves cannot be regulated through the code, while their implementation may very well be. When implementation rules are lacking, it makes the expression of rights or obligations difficult. For instance, the data protection and obligations related to payment which were embedded in the Seller's Guide have no equivalent expression in procedures that could have made the application of these obligations more transparent or systematic. It is true that "[b]y translating laws into technical rules, legal provisions are automatically enforced by the underlying technological framework[23]." However, the legal provisions automatically enforced are not the substantive standards, but inconsistent procedural rules. In comparison, consumer protection laws in Europe establish that the consumer must be protected from unfair commercial practices, and unfairness is a substantive rule that looks at the potential manipulation of the consumer through misleading or omissive practices[24]. To implement this rule in practice, additional national rules outlining specific judicial or extrajudicial procedures (e.g., injunctions or other judicial measures and access to alternative dispute resolution) needed to be drafted to guarantee the consistent application of the fairness principle. It is in vain that platforms such as the Silk Road, but similarly also Facebook and even Ethereum, draft community guidelines or governance principles, if these guidelines and principles lack a clear procedural framework which can make their application transparent and conducive to legal certainty. Absent such procedural rules (called "administrative rules" in **Figure 3** below), a control panel like the one used by Ross Ulbricht (see Supplementary Annex 5) is nothing more than the expression of randomized management, where the administrator would—when available—be tagged in forum posts bringing issues to his attention (e.g., users being disrespectful on the forum), and if he decided to take any action, this action would be mostly left at his discretion, should it fall under a category of rules which were not preset in the ToS.

[22] See for instance the debate on legal origins, Rafael La Porta, Florencio Lopez-de-Silanes, and Andrei Shleifer, 'The Economic Consequences of Legal Origins' (2008) (46)2 Journal of Economic Literature 285.

[23] De Filippi and Wright, fn 52 at 194.

[24] Directive 2005/29/EC concerning unfair business-to-consumer commercial practices [2005] OJ L149/22.

			Rule category		
	Legal rule	Consequence	Constitutional	Contractual	Administrative
Charter	Self-ownership Accountability Equality Pacta sunt servanda	-	✓		
Seller Contract	Data protection (client anonymity)	If saving or asking for personal data, then vendor account removed	✓	✓	
Seller's Guide	Information duties & mandatory disclosures (shipping, Seller's Guide, describing items accurately)	If not abiding by these rules, then vendor account removed		✓	
	Performance in good faith	If description not 'truthful', then vendor account removed		✓	
	Payment in Escrow	If payment outside Escrow or new vendors finalizing early, then vendor account removed	✓	✓	
	Restricted items (e.g. weapons, CP)	-	✓	✓	
	Prohibition of defects of consent (fraud, threat)	-		✓	
Buyer's Guide	Tampering with reputation systems Buyer statistics (reputation)	If posting fake reviews, then vendor account removed	✓	✓	✓
	Resolution center for Escrow	-	✓	✓	✓

FIGURE 3 | Overview of the most prominent legal rules in terms of service.

Blockchain governance does not raise the discretion issue to the same extent, given that accountability is supposedly left up to the consensus protocol deployed by specific blockchain networks. Yet perhaps the most important point to be made in this respect is that even in a decentralized, self-enforcing system, procedural rules are vital in determining the path of decision making. In a way, a consensus protocol is a procedure in itself. Still, the scaling of blockchain ecosystems from performing a function of currency exchange to delivering a broader category of transactions (e.g., self-sovereign identity systems) ultimately depends on how such ecosystems will deal with harms that may arise within their scope and how such harms ought to be remedied. That entails setting clear expectations regarding the balance of rights and obligations between the participants to these transactions, but also their standing in relation to the network itself.

CONCLUSION

This article looked at the Silk Road dark market as a cryptocommunity that deployed a unique identity management system. This identity was based on the roles users could perform on the platform and what their rights and obligations actually entailed. To do so, attention was paid to the essential contractual framework documents such as the Seller's and Buyer's Guides, but also the Silk Road Charter, which were all sources of rules created within the Silk Road community by its administrator, Ross Ulbricht.

These rules were further contextualized by addressing the setup of the identity management system used by Ross Ulbricht, critically analyzed from two perspectives stemming out of the lack of procedural rules to systematically enforce the private regulatory framework: arbitrariness as the main pitfall arising out of the private governance of identity systems and the code-as-procedure view complementing existing narratives surrounding the regulatory nature of the code deployed in cyberspace.

Overall, virtual worlds such as the Silk Road—especially given their use of the Bitcoin blockchain—are a source of untapped potential in exploring further questions relating to how more contemporary blockchain ecosystems can be profiled in terms of community and transactional dynamics.

Whether for social media platforms or for contemporary cryptocommunities, general procedures are vital in establishing consistent operations. Even where specific rules have not yet been developed, procedural clarifications can play a crucial role in dealing with the policy discretion that may be inherent to legal orders coexisting with the state. So far, the legitimacy of these orders has been analyzed primarily through the perspective of substantive rights and obligations and how they may conflict with state law. However, it is equally necessary to explore the notion of procedural law when dealing with the governance of cyberspace, as it may be a much needed ground for convergence between the many legal orders which have emerged between the physical and virtual realities.

DATA AVAILABILITY STATEMENT

Publicly available datasets were analyzed in this study. This data can be found here: https://antilop.cc/sr/.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

REFERENCES

AlQahtani, A. A., and El-Alfy, E. M. (2015). Anonymous connections based on onion routing: a review and a visualization tool. *Proc. Comput. Sci.* 52, 121–128. doi: 10.1016/j.procs.2015.05.040

Augot, D., Chabanne, H., Chenevier, T., George, W., and Lambert, L. (2017). "A user-centric system for verified identities on the bitcoin blockchain," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM 2017, CBT 2017. Lecture Notes in Computer Science*, eds J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí (Cham: Springer).

Bar-Gill, O., and Porat, A. (2017). Disclosure rules in contract law, harvard law school John M. *Paper presented at the Olin Center Discussion Paper No. 907* (Chicago, IL: University of Chicago).

Bartlett, J. (2015). *The Dark Net*. Brooklyn, NY: Melville House.

Biometric Technology Today (2017). Accenture and Microsoft add blockchain tech to biometrics ID platform. *Biometric Technol. Today* 7:12. doi: 10.1016/s0969-4765(17)30141-8

Biswas, K., and Muthukkumarasamy, V. (2016). "Securing smart cities using blockchain technology," in *Proceedings of the IEEE 18th International Conference on High Performance Computing and Communications, IEEE 14th International Conference on Smart City, IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Piscataway, NJ.

Can, U., and Alatas, B. (2019). A new direction in social network analysis: online social network analysis problems and applications. *Phys. A Stat. Mech. Appl.* 535:122372. doi: 10.1016/j.physa.2019.122372

Casino, F., Dasaklis, T. K., and Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics Inform.* 36, 55–81. doi: 10.1016/j.tele.2018.11.006

Christin, N. (2012). "Traveling the silk road: a measurement analysis of a large anonymous online marketplace," in *Proceedings of the 22nd International Conference on World Wide Web* (Pittsburgh, PA: CyLab), 213–224.

Cleaver, G. M. (2011). *The Idea of Self-Ownership*. Victoria: ORCA.

Cohen, G. A. (1995). *Self-Ownership, Freedom & Equality*. Cambridge, MA: Cambridge University Press.

Constine, J. (2019). *Facebooks New Policy Supreme Court Could Override Zuckerberg*. San Francisco, CA: Techcrunch.

De Filippi, P., and Wright, A. (2018). *Blockchain and the Law*. Cambridge, MA: Harvard University Press.

DiPiero, C. (2017). Deciphering cryptocurrency: shining a light on the deep Dark Web. *Univ. Ill. Law Rev.* 2017:1267.

Dizgovin, F. R. (2016). Foundations of specific performance in investor-state dispute settlements: is it possible and desirable. *Flor. J. Int. Law* 28, 1–62.

Dunphy, P. (2018). "A first look at identity management schemes on the blockchain," in *Proceedings of the IEEE Security and Privacy Magazine special issue on Blockchain Security and Privacy*, Piscataway, NJ.

Eisenberg, M. A. (2003). Disclosure in Contract Law. *Calif. Law Rev.* 91, 1645–1691.

Freund, A. (2017). "Automated, decentralized trust: a path to financial inclusion," in *Handbook of Blockchain, Digital Finance, and Inclusion*, eds D. Lee Kuo Chuen, and R. Deng (Cambridge, MA: Academic Press).

Gebhardt, J. H. (1947). Pacta sunt servanda. *Modern Law Rev.* 10, 159–170.

Goanta, C., and Hopman, M. (2020). Cryptocommunities as legal orders
Greenberg, A. (2012). *This Machine Kills Secrets: How Wikileakers, Cypherpunks, and Hacktivists Aim to Free the Worlds Information*. Boston, MA: Dutton.
Hitch, R. M. (1932). Our debt to roman law. *Loyola Law J.* 13, 66–92.
Holm, E. (2017). The darknet: a new passageway to identity theft. *Int. J. Inform. Sec. Cyber.* 6, 41–50. doi: 10.19107/ijisc.2017.01.04
Hou, H. (2017). "The application of blockchain technology in E-government in China," in *Proceedings of the 26th International Conference on Computer Communications and Networks* (Vancouver, BC: IEEE).
Huang, A. (2015). Reaching within silk road: the need for a new subpoena power that targets illegal bitcoin transactions. *Boston Coll. Law Rev.* 56:10.
Ibba, S., Pinna, A., Seu, M., and Pani, F. E. (2017). "CitySense: blockchain-oriented smart cities," in *Proceedings of the ACM International Conference Proceeding Series*, New York, NY.
Jaffe, C., Mata, C., and Kamvar, S. (2017). "Motivating urban cycling through a blockchain-based financial incentives system," in *Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing and 2017 ACM International Symposium on Wearable Computers*, New York, NY.
Jeremy, A. (2000). Pacta sunt servanda the influence of canon law upon the development of contractual obligations. *Law Just.Christ. Law Rev.* 144, 4–17.
Klonick, K. (2018). The new governors: the people, rules, and processes governing online speech. *Harvard Law Rev.* 131:1598.
Koops, E. (2012). Second-Rate citizens: junian latins and the constitutio antoniniana. *Maastricht J. Eur. Comp. Law* 19, 223–239. doi: 10.1177/1023263x1201900202
Kozinski, A. (2015). The two faces of anonymity. *Capital Univ. Law Rev.* 43, 1–17.
Kunkel, W. (1975). *An Introduction to Roman Legal and Constitutional History*. Oxford: Clarendon Press.
La Porta, R., Lopez-de-Silanes, F., and Shleifer, A. (2008). The economic consequences of legal origins. *J. Econ. Literature* 46, 285–332. doi: 10.1257/jel.46.2.285
Langvardt, K. (2018). Regulating online content moderation. *Georget. Law J.* 106:3024739.
Lemieux, V. L. (2016). Trusting records: is blockchain technology the answer? *Rec. Manag. J.* 26, 110–139. doi: 10.1108/rmj-12-2015-0042
Lessig, L. (2000). *Code Is Law: On Liberty in Cyberspace*. Cambridge, MA: Harvard Magazine.
Locke, J. (1821). *Two Treaties of Government*. London: Whitmore and Fenn.
Marsal-Llacuna, M.-L. (2018). Future living framework: is blockchain the next enabling network? *Technol. Forecast. Soc. Chang.* 128, 226–234. doi: 10.1016/j.techfore.2017.12.005
May, T. (1992). *The Crypto Libertarian Manifesto*. Available online at: https://www.activism.net/cypherpunk/crypto-anarchy.html (accessed March 25, 2020).
Mazzacano, P. J. (2011). Force majeure, impossibility, frustration & the like: excuses for non-performance: the historical origins and development of an autonomous commercial norm in the CISG. *Nordic J. Commerc. Law* 11, 1–54.
McMillan, R. (2014). *Hacker Dreams Up Crypto Passport Using the Tech Behind Bitcoin*. San Francisco, CA: WIRED.
Mears, J. (2018). The rise and rise of ID as a service. *Biometric Technol. Today* 2018, 5–8. doi: 10.1016/s0969-4765(18)30023-7
Metjahic, L. (2018). Deconstructing the DAO: the need for legal recognition and the application of securities laws to decentralized organizations. *Cardozo Law Rev.* 39, 1533–1550.
Michaels, L., and Homer, M. (2017). "Regulation and supervision in a digital and inclusive World," in *Handbook of Blockchain, Digital Finance, and Inclusion*, eds D. Lee Kuo Chuen, and R. Deng (Cambridge, MA: Academic Press).
Motoyama, M., McCoy, D., Levchenko, K., Savage, S., and Voelker, G. (2011). "An analysis of underground forums," in *Proceedings of ACM Internet Measurement Conference*, Berlin.
Mudambi, S., and Schuff, D. (2010). What makes a helfpul online review? A study of customer reviews on Amazon.com. *MIS Q.* 34, 185–200.
Nozick, R. (1977). *Anarchy, State & Utopia*. New York, NY: Basic Books.
Ortolani, P. (2016). Self-enforcing online dispute resolution: lessons from Bitcoin. *Oxf. J. Legal Stud.* 36, 595–629. doi: 10.1093/ojls/gqv036
Reijers, W., OBrolcháin, F., and Haynes, P. (2016). Governance in blockchain technologies & social contract theories. *Ledger* 1, 134–151.
Resnick, P., and Zeckhauser, R. (2002). Trust among strangers in internet transactions: empirical analysis of eBays reputation system. *Adv. Appl. Microecon.* 11, 127–157. doi: 10.1016/s0278-0984(02)11030-3
Rivera, R., Robledo, J. G., Larios, V. M., and Avalos, J. M. (2017). "How digital identity on blockchain can contribute in a smart city environment," in *Proceedings of the International Smart Cities Conference* (Wuxi: IEEE).
Rothbard, M. (1978). *For a New Liberty: The Libertarian Manifesto*. New York, NY: Collier Books.
Sharma, P. K., Moon, S. Y., and Park, J. H. (2017). Block-VN: a distributed blockchain based vehicular network architecture in smart city. *J. Inform. Process. Syst.* 13, 184–195.
Sullivan, C., and Burger, E. (2017). E-residency and blockchain. *Comput. Law Sec. Rev.* 33, 470–481. doi: 10.1016/j.clsr.2017.03.016
Van den Bergh, R. (2011). *Communication and Publicity of the Law in Rome*. New York, NY: SUBB Jurisprudentia.
Van Parijs, P. (1995). *Real Freedom For All*. Oxford: Oxford University Press.
Vlavianos, G. (1993). Specific performance in the civil law: mediating between inconsistent principles inherited from a roman-canonical tradition via the french astreinte and the québec injunction. *Rev. Gen. Droit* 24, 469–619.
Walch, A. (2017). The path of the blockchain lexicon (and the Law). *Rev. Bank. Finance Law* 36, 713–767.
Wehberg, H. (1959). Pacta sunt servanda. *Am. J. Int. Law* 53, 775–786.
Witt, A., Suzor, N., and Huggins, A. (2019). The rule of law on instagram: an evaluation of the moderation of images depicting womens bodies. *Univ. N. S. Wales Law J.* 42, 557–596.
Yang, C., Chen, X., and Xiang, Y. (2018). Blockchain-based publicly verifiable data deletion scheme for cloud storage. *J. Netw. Comput. Appl.* 103, 185–193. doi: 10.1016/j.jnca.2017.11.011
Zamfir, V. (2018). *My Intentions for Blockchain Governance Medium*. Available online at: https://medium.com/@Vlad_Zamfir/my-intentions-for-blockchain-governance-801d19d378e5 (accessed March 25, 2020).
Zhang, N., Zhong, S., and Tian, L. (2017). Using blockchain to protect personal privacy in the scenario of Online taxi-hailing. *Int. J. Comput. Commun. Control* 12:886. doi: 10.15837/ijccc.2017.6.2886
Zyskind, G., Nathan, O., and Pentland, A. (2015). "Decentralizing privacy: using blockchain to protect personal data," in *Proceedings of the IEEE Security and Privacy Workshops* (Singapore: SPW), 180–184.

Conflict of Interest: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.