Cryptomarkets’ Phenomenon: A Conceptualization Approach

Randa Basheer

Faculty of Information Technology and Communications, Syrian Virtual University, Damascus, Syria

Correspondence should be addressed to Randa Basheer; randa_151689@svuonline.org

Received 13 January 2022; Accepted 14 March 2022; Published 27 March 2022

Abstract

In the last two decades, the Dark Web has become the perfect resort for various illicit activities. Cryptomarkets are widespread platforms in the cyberspace of the Dark Web where participants trade for illegal gaining. In this article, we present a conceptualization approach of cryptomarkets based on several recent studies on the phenomenon. We attempt to conceptualize cryptomarkets in technical and social aspects to introduce an understanding of their operating mechanisms and the robustness of their communities. We demonstrate the concept of the Satisfaction Factor that attracts individuals to cryptomarkets. Furthermore, we discuss the importance of forums to members of cryptomarkets as technical and social supportive platforms. The article also includes a comparison of cryptomarkets and conventional trading networks and discusses the efforts of law enforcement agencies and their effects in disrupting cryptomarkets. Moreover, we discuss the need for further researches.

1. Introduction

The Internet was initially a massive tool of information exchanging, though it has also become an essential platform for deliberating various goods and services of daily life. In some specific parts of it, the Internet has become a tool to trade and promote illicit and malicious products and services. The economy of such trade is booming rapidly, accompanied by a tremendous rise in the number of participants in illegal markets and a rapid increase in the types of offerings provided on these markets [1].

The concepts of the Deep Web and Dark Web appeared with the diffusion of the World Wide Web in the mid-1990s and got attention from researchers worldwide. However, this attention had a grand leap, specifically after the arrest of Ross William Ulbricht in October 2013 [2].

Many computing and networking technologies form the Deep Web, broadening its space as they expand and increase in number. On the other hand, the Dark Web, a part of the Deep Web, evolves through special anonymizing and encrypting technologies, deploying anonymous websites, and using cryptocurrencies in transactions [2].

Dark Web provides the ability to hide a user’s identity, network traffic, and the data exchanged through it. Users cannot reach the Dark Web by using standard web browsers, rather utilizing special software. Therefore, dark networks became commonly a tool for many malicious and illicit purposes such as drugs trade, hacking, child pornography, social and identity cards forgery, counterfeit items, weapons, deploying extremist content, and many others [3]. Researchers consider dark networks as the major host of different criminal activities. For example, electronic markets of the Dark Web represent proof of the Crime as a Service (CaaS), where they provide most of the items usually found in the physical black markets [4]. Dark Web consists of several anonymizing computer networks. The most famous anonymity networking software is The Onion Router (TOR) [3].

The U.S Navy released TOR in 2002 to protect communications from network surveillance and traffic analysis by anonymizing a user’s identity, location, and IP address, and the network traffic. To achieve this, TOR depends on cryptography and redirecting traffic across several random nodes on a voluntary free global network, which consists of more than 5000 relays [3].
Many individuals and organizations use TOR for legal activities, such as users of daily Internet surfing, journalists, security agencies, and many others [2]. However, this anonymity allows another group of users to commit infringements in cyberspace where illicit markets and child abuse websites prevail [5].

Websites hosted using TOR can shift from one server to another on the TOR network; these intentional shifts help in preventing tracking or identifying the website’s host or physical location [5]. Many of these hosted websites are electronic markets where trading illicit products and services take place.

Markets on the Dark Web, or cryptomarkets, changed the conventional trade of illicit merchants, especially drugs. In this paper, we attempt to conceptualize the cryptomarkets phenomenon. The following section includes five main concepts:

1. A detailed definition of a cryptomarket, including an overview of its mechanism, the importance of researching in cryptomarkets, and a brief history of the first cryptomarkets
2. The basic technical terms with which a cryptomarket works
3. The social structure of its community, methods of communication among its members, the rules and laws that govern it, and the role of feedback and rating systems
4. The Satisfaction Factor of users, which is essential for traders to succeed and for cryptomarkets to attract members
5. The importance of reputation to sellers to be able to compete and preserve customers’ loyalty

Section 3 discusses the support provided by forums to communities of the cryptomarkets in terms of the technical and social needs of the participants. Section 4 presents a comparison between cryptomarkets and conventional trading networks. Section 5 discusses the effects of law enforcement agencies on cryptomarkets’ operation and economy. Section 6 presents a discussion of the aforementioned concepts and further research fields.

2. Cryptomarkets

In this section, we discuss in detail the different facets of cryptomarkets. It includes the following aspects: an overview of cryptomarkets, the technical fundamentals, the social structure, the factors that attract users to cryptomarkets, and the importance of reputation for dealers to succeed in their business.

2.1. What Is a Cryptomarket? Researchers consider the word “cryptomarket” a slang word that originated in the forums of digital hackers [6], while others call it “Dark Net Market” [7]. Martin defines a cryptomarket as “an online forum where goods and services are exchanged between parties who use digital encryption to conceal their identities” [6].

Cryptomarkets facilitate peer-to-peer communication through anonymity techniques, in addition to using peer-to-peer cryptocurrencies (like Bitcoin) for payments. These techniques make it hard for any party, including law enforcement agencies, to monitor these markets and the activities of their users. Moreover, these platforms introduce extra social features for their communities, such as recommendation systems, ranking, feedback, and a strict escrow system controlled by the market administrators [8–10].

Cryptomarkets make it possible to sell any item or promote any service worldwide. Initially, cryptomarkets focused on computer hacking, financial fraudulence, and intellectual property infringement. However, starting from 2011, a new type of market emerged, focusing mainly on the illicit drugs trade [1]. Researchers may notice that cryptomarkets are dedicated to trading drugs and related items; however, they introduce other services, such as stolen or counterfeit social cards and personal identity information, illegal weapons, and even renting hackers and killers [11]. A user can find cryptomarkets by a simple search on search engines available on TOR like the Hidden Wiki [6]. In recent years, the Dark Web witnessed massive economic growth in cryptomarkets, from products diversity to a grand increase in sales [3].

In the last two decades, many researchers implemented studies and analyses on many cryptomarkets. Here, we raise a question: what is the importance of studying and analysing cryptomarkets?

Monica and Barratt [8] suggest that there are five main reasons that make it necessary for the scientific society to research in cryptomarkets, especially drugs trade, to help scientific and security agencies to develop their methods:

1. Cryptomarkets provide the chance to analyse the supply side of drugs trade in its entirety
2. Cryptomarkets are not isolated from the broadest markets of drugs, which may include series of social and commercial supplies of a wider scope in the physical world
3. Cryptomarkets provide a new method to observe and predict evolvement directions of emerging drugs’ trade
4. Cryptomarkets introduce a demonstrating example of criminal innovation in trading and promoting drugs, and of the growth of this trade as a reaction to law enforcement agencies’ efforts
5. Cryptomarkets became a place in which drugs’ consumers can meet their needs and preferences of drugs at least partially, along with a social system that is effective and supportive

We can add to these reasons what Décary-Hétu [1] inferred about the ability to evaluate the supply and demand of drugs on cryptomarkets automatically over time, and studying drugs prices evolution and the effects of police
operations on the latter. In addition to studying the growth of the societies which expand in the hidden web where anonymous individuals gather, this aspect can provide an understanding to some sides of organized crime which is transferring from the real world to the virtual one increasingly.

Consumers can compare and buy from tens of thousands of different products from vendors located all over the world. They can also communicate directly with others and share their feedback about the offered products [12], some of which were not available in the local market or street markets [13]. Most sellers specialize in one or two products, but some senior sellers are able to utilize the supply chain effectively so that they combine the resources of many suppliers in a single business [14].

“Silk Road” market was the first practical example of cryptomarkets [14]. It started to operate in February 2011, launched by its owner Ross William Ulbricht, taking the pseudonym “Dread Pirate Roberts.” Researchers consider the business model produced by Silk Road as a “transformative criminal innovation” with a lasting impact on the method of selling and distributing illegal drugs and the nature of social relationships among its dealers. The sellers themselves also considered that Silk Road completely changed the drugs’ sale model by creating a large and relatively safe global market for drug traffickers, in addition to serving as a virtual intermediary that linked the top, middle, and retail sellers [9]. Although Silk Road was not the only market, it quickly overtook other markets with increased revenue and expanding traffic on a faster track [5].

Since the arrest of Ulbricht in 2013, dozens of alternatives to Silk Road have been deployed using hidden services on the TOR network. In a new and improved version of Silk Road, Silk Road 2.0 launched, but law enforcement agencies closed it again in November 2013 [2]. Although that period witnessed low confidence in cryptomarkets’ environment [15], the creation of many imitators followed Silk Road, and they achieved their success despite the closure of their inspiration source, and the presence of many different competitors. With this success, they evolved the rules and laws governing the markets’ business by reproducing and improving the systems followed by Silk Road [14].

2.2. Terms of Techniques. A cryptomarket uses a set of strategies to conceal the identity and IP addresses of its participants, transactions, and physical locations of its services. It uses anonymization software of highly complicated encryption technology (such as TOR, I2P, and others), in addition to cryptocurrencies, and encrypted messaging using PGP encryption key [9].

Pretty Good Privacy (PGP) is an encryption protocol that allows anyone to encrypt a message, while only the intended recipient can decrypt the data it contains using his/her private key. Keys also serve as an important identity verification tool among users, especially when the same sender sends messages using different pseudonyms, or using the same pseudonym but from different cryptomarkets [3, 16, 17]. Each seller in the market has a public PGP key that appears on his/her page, and participants use it to provide confidentiality in the negotiation and purchase stages between the seller and the buyer [4].

After the shutdown of Silk Road, cryptomarkets’ users created databases for the sellers’ encryption keys, which enabled buyers to match their preferred sellers with their public keys [17].

In its classic structure, a cryptomarket starts from a main page that contains links to pages of offered products categories and services supported by the market. The market also provides an instant messaging system that allows members to communicate directly and discussion forums to discuss market activities or place inquiries about products [11].

It is worth noting that there is another type of commercial websites in the dark networks called a “single vendor shop.” The suppliers directly create these websites, operating them in many cases in parallel with the cryptomarket. These shops sell directly to customers without any third party or broker, although this makes transactions more risky and increases the possibility of frauds, which usually discourages customers from entering the shop. Moreover, owners of these singular sites can take advantage of cryptomarkets as a starting point to inform customers about their activities on their shops. These shops mostly sell the least common products sold in cryptomarkets, especially weapons that gain great interest in private stores [11].

Cryptomarkets evolve with the development of technology and social media platforms, and researches consider that law enforcement procedures are an essential part of the cryptomarket system as well, as they unintentionally cause evolutionary pressure forcing markets’ operators to develop them and employ more up-to-date systems. Developments can include changes in hosting services, values of cryptocurrencies, and improvements in the sites’ infrastructures [14].

In terms of members’ skills, anyone with sufficient technological skills can access and trade in cryptomarkets [9]. Furthermore, cryptomarkets have become meeting points for exchanging different types of knowledge and technical consultations. They develop infrastructures with more risk management tools [14]. Forums also provide “nested support systems” for information exchange, communications, and experience sharing, in addition to “how to” instructions, and sometimes to find vendors with the best products or safest packaging styles [18].

The Operations Security (OPSEC) is the most common term regarding the logistic services provided to clients, and it expresses all procedures used to protect commercial transactions from the interception of law enforcements [19]. Members need to show good OPSEC and digital experience in order to ensure avoiding law enforcement operations and reducing the chances of being involved in a fraud [20].

Stealth is one of the most important logistic services, as it directly faces the risk of legal authorities’ inspections. Displaying stealth techniques used by the seller influences the buyer’s decision as to whether or not it is good to buy from this seller. It also forms a part of the seller’s rating that buyers leave on the market rating system and feedbacks on the seller’s page or forum threads [19].

Along with cryptomarkets, many drug dealers fulfil their deals by means of other tools that support the digital environment of those deals, even by the open Internet, phone, email, social media platforms, or by using applications and websites such as Grindr and Gumtree [14].
Encrypted messaging services form a part of the social media on the market, providing some security features that can protect customers from police disclosure or prosecution [3]. Some vendors consider encrypted messaging applications as a part of customer service bundle that they offer to potential buyers. Some other vendors consider it as an alternative channel they can use in “direct dealing” in cases of increased pressure from law enforcement, or when their favourite cryptomarket does not operate, where it can provide a temporary means to conduct deals until the establishment of the next new market [20].

Figure 1 summarizes the technical essentials a cryptomarket depends on to work successfully.

2.3. Social Structure. Cryptmarkets have a composition similar to markets on the Surface Web (e.g., Amazon and eBay). The cryptomarket community generally consists of four levels [12]:

(i) Administrators: they are responsible for operating and controlling the market. Their basic tasks include determining policies under which the market will operate, licensing and suspending members’ accounts, supervising transactions unlisted in the market, creating new products categories, and defining accepted and prohibited products’ types, in addition to creating and imposing new security procedures as needed.

(ii) Moderators: the moderator assists in site maintenance, in addition to providing customer support services. Their primary tasks include organizing forum discussions, identifying fraudulent activities, and responding to requests for assistance and complaints from vendors and consumers.

(iii) Vendors: they use the market to sell illegal goods. Any merchant can create a “vendor page” following simple steps starting from registering in the market, after which they can create and manage their “store” and start making deals with consumers.

(iv) Consumers: they purchase goods through the market, and they represent the majority of registered users. They can access vendors’ pages, purchase products, and provide feedback about the vendor and the product upon receipt, as well as writing posts on discussion forums.

It is worth noting that there are many buyers and sellers maintain accounts across several cryptomarkets at the same time. This allows them to expand the circle of communication and trade with a larger group of users, as it also ensures the trade continues on the network in case one of the markets faced an unexpected shutdown. In the latter case, a state of “migration” may occur from one cryptomarket to another. Therefore, this expanded membership is a means of facilitating the migration process for both sellers and buyers [12].

On the other hand, sellers work to ensure the consistency of the seller’s identity, as it is the key to acceptance and trustworthiness. Therefore, famous sellers establish themselves across different cryptomarkets, and in some cases with the help of the market operators who preregister the pseudonyms of the known sellers when creating a new site. Operators also allow sellers to transfer their comments to the new market, and automatically, the good sellers will have an entourage of former customers on the new market [18], although using the same pseudonyms on several markets may expose them to law enforcements in case the latter possess leaked information about vendors’ identities [17]. There are applied fees for each registered vendor account, though some vendors work on several markets to appear more clearly in the Dark Web markets. Moreover, they seek to increase their profits and market share in the presence of competition expected in this type of trade. On the other hand, accounts multiplicity may be due to the volatile nature of this type of markets [16].

In each cryptomarket, a set of rules govern the market and users must abide by them. For example, Martin [12] mentioned the basic rules of Pandora market, including identifying prohibited items, such as child porn, and services that cause harm to people, such as hitmen, and the need to use the PGP Public Key to encrypt messages between suppliers and buyers. Such procedural rules and guidelines provide sufficient knowledge to users about acceptable and unacceptable behaviours in the market and create a regulated trading environment for both sellers and consumers. Administrators and moderators also impose these rules, and they penalize violators with penalties such as suspending or closing the accounts of offending users.

Although buyers pay for products in advance, the system does not release the payments to sellers unless the buyer confirms the receipt of the product. The reputation of a seller is also very important in the market community, where each seller is associated with a satisfaction rating, feedback, and notes written by previous buyers, which all inform future buyers of the seller’s reputation before making the purchase. The feedbacks include detailed comments about products quality, accuracy of delivery time, and other related ecommerce metrics. On the other hand, a description of the buyer’s reputation is available for the seller to check before approving the sale [2, 6, 9].

The rating system assists buyers by directing them across the market to find highly rated sellers and products [14]. This system is what makes cryptomarkets unique, as it provides a dual reputation mechanism that instills confidence in both sellers and buyers, protects the anonymity of identities, and facilitates frequent transactions [11]. The best way for a seller to gain the trust of potential customers is to get high rankings in the cryptomarket standardized rating system. The rating system often consists of a five-star scale and enables buyers to write short reviews [19].

There are several factors that buyers consider for a seller to gain their trust. Sellers must be polite and responsive when buyers contact with them via encrypted messages or forums, provide reliable information about their products and trade terms, and ship their goods quickly. Without these factors, sellers may run the risk of losing orders [19]. Sellers pay an instrument when registering in the market, and a commission on every sale to the market officials. The officials in turn provide escrow services to protect both.
the seller and the buyer, in addition to intervening to resolve disputes if necessary [21]. Most cryptomarkets offer the escrow service where the system keeps the money until the buyer finalizes the transaction. However, market operators may exploit this central guarantee model in an action known as “exit scam,” where they close the entire market and flee with the funds deposited in the system. This evolution has prompted some cryptomarkets to offer multisignature guarantee to finalize the deal before the funds are released [8]. In other cases, buyers may defraud as well, such as claiming that they have not received the goods, or that they complain about the received quality or quantity, with a request for compensation [22].

2.4. Satisfaction Factor. Users’ satisfaction plays an important role in the growth and success of cryptomarkets. We call it the “Satisfaction Factor.”

Satisfaction Factor includes several important partials, such as the effectiveness of methods followed to avoid monitoring and the ability to interact with others without revealing identities or expose themselves to violence that may occur in other environments. The more experienced the member becomes, the more he/she feels a sense of security. When users experience anonymity, they are able to engage in forums without being afraid to reveal sensitive information that may lead to social stigma or self-incrimination. Some users who have firm self-confidence and high technical skills can offer their digital skills for rent to the local merchants or those with less experience or with less computer skills [18]. Cryptomarket users consider they have the opportunity to enjoy several things, like using their digital skills and developing them, and the feel that they can preserve personal dignity where they conduct their businesses with anonymous personages. In addition to the ability to control the purchase and selection of drugs in the so-called “rational consumer” mind-set, which selects the product according to its variety, value, and quality in a manner that reduces potential harm, a process that is difficult to achieve in transactions outside the Internet reliably [13].

The Satisfaction Factor also includes the emotional attraction that cryptomarkets represent to both sellers and consumers, as the secret and hidden nature of cryptomarkets attracts them [14], especially those with liberal ideals and believes in creating a space to experience personal freedom, as cryptomarkets produced the openness to them to discuss illegal behaviours that users outside the cryptomarkets’ borders cannot perform. Although that the continued closures by legal authorities threatens the confidence of the participants in the possibility of permanent freedom, their desire to rebuild this possibility in other dark places on the web increases [10].

Good stealth experience when shipping by mail is an important measure of the seller’s quality, as the method of packaging and shipping out of sight of legal authorities and postal inspection is an important and desirable quality in the seller. Packaging methods include using regular containers such as a DVD case or any similar harmless item, as well as providing a return address with a legal appearance. The seller keeps the product in the box after good air discharge, using moisture barrier bags, tightly closing and cleaning of any external marks on the sealed cover. Finally, members use untraceable payment systems for postage fees [18].

Some market members also show their enjoyment by demonstrating their technical skills especially to challenge law enforcement agencies. These “crime temptations” play a role in the Satisfaction Factor when achieving successful transactions. This type of satisfaction often turns into a “libertarian” and “anti-interventionist” attitude towards the state operations in drugs ban, and some cryptomarkets’ officials announced this position clearly in the sites’ documents [13].

We can explain customers’ turnout to buy drugs from cryptomarkets by the ability to confirm the quality of drugs in terms of the substance. Cryptomarkets provide a set of services including information, tips, and drug testing services to verify the quality of the products that the user tends to buy with the lowest risk ratio of impurity [7].

At the initial emergence of cryptomarkets, there was a high level of technical skills necessary to work in a cryptomarket,
which effectively limited the access of those who do not have those skills. As a result, small technological elite emerged that cares about common interests in an environment in which advanced computer technologies have become a unique supportive culture of a virtual digital community. However, with the increase of technology development, its spread, and the ability to learn it by various groups, and the access to cryptocurrencies, has become more easy to use, cryptomarkets are no longer the preserve of this elite, and the flow of market participants from amateurs, beginners, middle-class experts, and professionals has increased [10].

The anonymity provided by the encrypted connection led to some elevation in the level of professionalism in business management on cryptomarkets. This professionalism depends on several factors including exchanging information, sellers’ keenness to provide high-quality products and services, courteous professional communication, competitive pricing, and conflict avoidance. In addition, members seek to make their forum posts highly visible and attractive to viewers. Many sellers also keep an “update” section on their profiles to ensure frequent visits from buyers, such as posting the latest news about their business and dealing requirements [22].

Figure 2 summarizes the basic elements that contribute in building the Satisfaction Factor.

2.5. The Pursuit of Reputation. The good reputation of a seller promotes cooperation, ensures customers’ loyalty, and increases the seller’s revenue [19]. Good reputation along with the username, good customer service, and highly valued feedback are important bases for successful distribution networks [16], and in cryptomarkets, reputation is visible for anyone to see [22]. Therefore, participants consider the reputation system in cryptomarkets as one of the main aspects in establishing and maintaining trust among users [17].

Vendors strive to establish their usernames as a brand. They use their profiles to clarify the rules regarding how to order merchandise, shipping time, refunds and delivery information, changes in exhibits, problems with the site or shipping, new shipping rules, or banned countries. These updates are a way to maintain their reputation and to protect themselves from negative reactions and to prevent obtaining low ratings [22].

Norbutas [17] discussed the role of reputation in the trade mechanism in cryptomarkets. The study demonstrates the work of the reputation system where it publishes buyers’ comments that reflect the sellers’ trustworthiness and the quality of their products. These comments are of a significant importance to the customers as they include information about previous actions of the sellers, which attract new buyers to the reputable seller and warn them about the fraudulent one. On the other hand, frequent transactions between the same buyers and sellers play an important role in maintaining trust over time; thus, sellers strive to maintain stable identities across markets. The study also found that reputation is transferable, as famous sellers with steady identities and good reputations enjoy additional features offered to them from the market as a special support. In case of a market shutdown or departure, market officials offer those sellers the option to maintain their identities and transfer them along with their reputation records to the new market, which helps them to keep their old customers and gain more confidence.

3. Forums: Technical Discussions and Beyond

Forums on the Dark Web represent discussion spaces that work in support to businesses on cryptomarkets. Through forums, users share information and express their points of view about products’ usage (especially drugs), availability, and prices. Therefore, it is one of the most common services on the Dark Web [3].

Cryptomarkets’ operators often provide discussion forums with the market, and there are external forums as well that are not related to a particular cryptomarket but contain a commercial section for the same purpose. These forums cover most topics related to goods and services traded in the market, though the majority of posts are drug-related threads created by the vendors themselves to promote their products and interact with their customers, focusing often on logistics [19]. On the other hand, forums allow buyers to discuss various aspects related to their drug purchase, quality, and comparisons between sellers, aiming to help each other in selection, usage, and other things [13].

Bancroft [13] found that cryptomarket users became more confident in questioning vendor’s claims about the quality of the latter’s merchandise, compared to users buying from physical markets outside the Internet, prompting sellers to provide evidences that justify their claims. This indicates a shift in the strength of the cryptomarket user. This transformation includes a kind of users’ union in terms of supporting each other with knowledge.

However, another side of the forums proves the existence of real societies that lie beyond those seemingly objective discussions, and they are represented by strong collectivism standards of unity, support, and mutual interactions that sometimes show a high energy of sympathy. Ladegaard [23] discussed this aspect of the forums. In addition to issues related to security, practical and technical matters, and drug purchase and usage, forums involve social issues as well, or topics for “leisure time,” which may be considered a means of social mingling and chatting with acquaintance. Some discussions express solidarity, in which some members ask to borrow from others, when he/she lacks a few dollars or cents to complete a deal, and he/she finds some other members who are willing to help. This microlending process and then paying it back also helps to increase trust between members in a growing environment of collegueship.

This may express their desire for a community of their own, as Ladegaard [23] explained when studying the supportive community of Silk Road. Members showed their eagerness to support Silk Road, especially when the FBI seized it. They expressed those feelings through their chats that requested “archiving the forums to preserve the knowledge they contain,” showing how important “mirroring” the forums is, “regroup” or “unite” and create a new “home”. Society members were emotionally involved with the sudden events taking place in those markets, expressing them in a sad and emotional tone by using words that stimulate feelings such as “home” as an expression of the market,
“brothers and sisters” as an expression of its members, and the group as a whole with the word “family”. At another stage, and after the forums’ backup was retrieved by volunteers who had sufficient electronic skills, Silk Road members expressed their joy about the forums return, along with the discussions they contained, with the word “memories,” “joy,” and feelings that “overwhelmed” them and a “true community feeling.”

Cryptomarkets show more than just business deals and technical skills. Beyond these markets, there are societies that believe this type of trade is a “noble” and “commendable practices.” Therefore, some researchers see cryptomarkets as a practice of resistance and the liberalism represented in that trade deals promote social harmony and obtaining of individual rights, as long as they do not violate the rights of others. On the other hand, some sellers have also expressed that their actions on cryptomarkets are to help farmers and chemistry students in various countries, and calling it “activating fair trade,” and they see themselves as moral representatives promoting what they consider a peaceful and human way of life [24].

4. Cryptomarkets versus Conventional Drug Markets

Unlike conventional networks, cryptomarkets do not need the involvement of any intermediate nodes (carriers, brokers, wholesalers, and street retailers). Dealers can easily trade and send drugs directly to consumers locally and globally [6]. Cryptomarkets shorten the distance between the buyer and the producer by dispensing the intermediate nodes, and it encourages this transformation due to the profitability of transactions with a smaller number of mediators [21].

Moreover, this fundamental difference may explain the spread of cryptomarkets for drugs’ trade as a less harmful alternative [6], and traffickers as well consider it relatively free of the violence that is usually associated with the traditional drug market [9].

This transformation also includes the technical fact of cryptomarkets, where they operate over large-scale computer networks, and because of the speed, flexibility, and mutual nature of electronic communications, researchers
consider this a major shift in the drugs’ trade compared to similar operations across traditional markets [12]. Users as well consider their infrastructure “low risk, high traffic, high mark-up, secure, and anonymous” [9].

Furthermore, visibility level may be a primary reason that buyers prefer cryptomarkets. Due to the clarity of criminal activities on street-level drug markets, they face both law enforcement operations and the potential violence of competing groups. While in cryptomarkets, visibility is no longer a major security threat due to anonymity, encrypted messaging systems, discussion forums, vendor profiles, and comment systems where sellers and buyers can communicate directly [22], in addition to the massive availability of different types and quantities of drugs accompanied with reduced risks related to the products quality [19].

Vendors consider this environment less risky for themselves as well, where physical strength is not important in the online world. On the contrary, the characteristics of a successful vendor rely on good customer service, good reputation, and ingenious marketing skills [16, 22].

However, cryptomarkets’ business represents a fraction of the global drug trade as Aldridge and Décair-Hétu [25] suggest. Although it allows direct linkage among different parties and cuts some of the mid-level of the market, fraud, and law enforcement activities form important factors that may impede the growth of cryptomarkets, in addition to the technical factors related to the nature of these markets, where accessing them requires a degree of technological knowledge. Moreover, even in case technical skills were available for users, some may not easily trust the security provided by these services, especially with the pressure caused by the media that cover the arrests associated with cryptomarkets. Another limitation is the fact that sellers send products using mail systems that face the risk of surveillance and seizure by security agencies, which can happen within borders or across countries. Therefore, some may withhold from purchasing from cryptomarkets because they do not want to receive products through the mail, and they prefer their current supply of drugs from the retailers they know and trust.

5. Cryptomarkets in the Face of Law Enforcement

What we have discussed so far does not mean that cryptomarkets are impervious to risks and sudden events that may affect them slightly or significantly.

Martin [6] indicates that they suffer from a weak point, which is their dependence on cryptocurrencies that security agencies can track. While the system encrypts commercial transactions of cryptocurrencies, transfers that involve the conversion of real currencies into cryptocurrencies or vice versa leave a trace in official records, which means that the security authorities can monitor who buys and sells cryptocurrencies, but the nature of purchases after this transfer remains hidden.

In addition, the metadata included in a document can reveal its author; for example, the data included in an image may provide the camera type, date and time, and often the geographical location, unless the user erases this data or does not record it in the first place [18].

On the other hand, Broséu et al. [16] suggest that investigating in illegal trade on the Dark Web can be done by creating a single collaborative intelligence model that combines digital data (e.g., data obtained through various studies on cryptomarkets) and physical data related to the products themselves (e.g., the substances) producing one integrated interpretation. The physical data may include the physical and chemical characterization of mailed products, which may deepen the knowledge about cryptomarkets in terms of the country of origin, product quality, and distribution strategies of the networks.

The FBI and other law enforcement agencies have closed a few cryptomarkets, while some others have experienced significant fraud by a market official, or had external hacking attacks [22]. Many law enforcement groups have adopted the practices and techniques followed by the criminals themselves with other investigation techniques to combat illegal activities on the Dark Web. In 2011, the FBI used a robust application called Metasploit in “Operation Torpedo” to penetrate the dense layers of anonymity presented by TOR and carried out the operation against three websites of child pornography [2].

In October 2013, the FBI seized Silk Road, the first encrypted market that attracted international attention, after several months of intense surveillance. This operation marks the first major disruption of a cryptomarket. In November 2014, there was “Operation Onymous,” the second operation with an international cooperation of law enforcement, including the FBI, the Department of Homeland Security, and the Europol, and it led to the seizure of many cryptomarkets and arrests all over the world, including Silk Road 2.0, Cloud-Nine, and Hydra [1, 26]. After this operation, Agora and Evolution became the largest markets, but in May 2015, Evolution officials closed the market and fled with an "exit scam," while Agora voluntarily closed in September 2015 and refunded its users [27].

Décair-Hétu and Giommoni [1] discussed the actual impact of police and law enforcement operations on Dark Web sites. There are limited evidences to support the effectiveness of police campaigns to reduce the supply and/or demand of illicit drugs, as studies show that their impact is negligible or very little on the number of drug users or suppliers, or drug prices. In addition, markets’ participants adapt to this effect through the strategies of displacement from one market to another. Tactical displacement is the most common form of adaptation. Police interventions may lead to a shift from the “open” to “closed” drug markets with dealers who may adopt technical solutions, such as mobile phones and messaging applications to contact suppliers and customers. Location displacement is another common form of adaptation to police operations. For example, Silk Road (SR1) members quickly moved to other cryptomarkets (Agora-Cloud-Nine-Evolution-Hydra-Sheep-Silk Road 2.0 (SR2)-Black Market Reloaded (BMR)). Operation Onymous greatly affected sales in cryptomarkets’ system. Although it did not target Agora and Evolution, it affected the supply and consumption of drugs on them, as in the
weeks after the operation, the total number of merchants and the number of new merchants who registered each week decreased. A few dealers in the nontargeted markets stopped selling as well, and on the consumption side, the number of sales decreased, although drug prices remained the same.

Despite police operations, cryptomarkets remain a vital system of drug trafficking, as each “shock” ends with the launch of many new cryptomarkets [17].

6. Future Directions for Further Research

Studying Dark Web sites is of great importance to many parties. Law enforcement agencies have substantial motivations for tackling the drug trade on the dark network by disrupting cryptomarkets. Such procedures aim for reducing users’ confidence in cryptomarkets and the anonymity of their actions, in addition to identifying markets’ members and gaining evidential data to prosecute perpetrators [7]. Furthermore, drugs policymakers, criminologists, and social scientists have a growing interest in limiting the harm of the trade and restraining liberal political motives on drug cryptomarkets [28].

Researchers call for continuous analyses of cryptomarkets to discover justifications for the criminal phenomena, identify possible organizations or alliances, and then target them and detect criminals. Law enforcement agencies exploit all potential gaps, whether technical, such as developing sophisticated mathematical methods that benefit from software flaws, or human errors in users’ practices, such as failures in OPSEC that can facilitate deanonymization [4, 29].

Vendors with multiple accounts may hide important actors in the drug trade behind those accounts, as vendors located on several cryptomarkets usually manage numerous listings [16]. On the other hand, PGP encryption enables the creation of unique identities and allows users to select specific individuals to interact with [17]. Therefore, analysing PGP keys associated with usernames may disclose the relationships among vendors’ profiles within the same market or on different ones more than what the usernames alone can show, considering that the PGP key works as a user-authentication tool [16].

In this context, researchers suggest several methodologies that help different organizations to investigate cryptomarkets and limit their activity. Some studies show that a small portion of merchants possess the largest shares of listings and sales. In other words, main actors have the advantage of having a well-organized structure according to the number of listings they manage, the number of markets in which they are active, and the types of drugs they offer for sale. Therefore, targeting such individuals can profoundly affect the course of commercial operations on the market and destabilize its economy. Moreover, employing attacks on the reputation systems, which are the vital engines of successful trades on cryptomarkets, can disrupt the overall trust in the cryptomarkets’ community [1, 16].

Broad strategies with extensive global participation should be taken to prevent and detect malicious sites. Security organizations worldwide can direct the knowledge gained from analysing Dark Web data to effectively put these strategies in the physical world while ensuring that the investigation and enforcement resources are deployed efficiently [2, 16]. Moreover, researchers suggest that a wider scope of responsibility should be established to include different public and private sectors in society in a kind of pro-active cooperation that reduces the efforts through sharing knowledge and frameworks [29].

It is worth noting, and as we mentioned previously in this article, that cryptomarkets work side by side with encrypted messaging apps. Therefore, exploiting such technologies can immensely reveal information about the drug trade parties and prove the possibility of conducting striking wide-scale breakdowns on the online drug trade. This possibility is highlighted by a most recent operation that took place worldwide. In June 2021, OTF Greenlight/Trojan Shield took place through a collaboration of multiple worldwide security organizations from over 20 countries using an encrypted device service developed by the FBI in coordination with the Australian Federal Police. The operation involved massive arrests (over 800) and seizures of tons of illegal substances and items and over 48 million dollars in various global currencies and cryptocurrencies [30].

In the latest studies, researchers have discovered changes in the behaviour of cryptomarkets in response to global health or social changes, the most important of which is the pandemic. This suggests that researchers expand the scope of research in cryptomarkets to respond to public health threats resulting from citizens being exposed to a massive amount of disseminated misinformation that leads to a new economy in the Dark Web concerned with prescription drugs. Findings from these studies motivate policymakers and public agencies to use these insights for better evaluating and developing legislation related to medical and health substances to combat the drug economy in the Dark Web [31].

In the future, it is anticipated that cryptomarkets will tend to rely on advanced integrated social platforms that are mainly privacy-oriented. These platforms are multifunctional decentralized spaces with robust privacy, security, and ease of use features. The functions will include trading and communication, P2P connections, secure payments and transfers, cryptocurrency management, and encrypted chat, creating a new attraction for members to the marketplaces. This development calls for paying attention to studying the technologies on which these platforms will be based and finding solutions to monitor them and disrupt or reduce their impact [29].

On a different aspect, researchers proposed that instead of eradicating the Dark Web, policymakers should methodically target criminals and malicious activity patterns while striving to develop the Dark Web for purposeful objectives and positively shape it [2, 16].

In the same context, opinions have risen recently that encourage different government and private institutions to follow several directions concerning the Dark Web and its misuse. These directions include [32] the following:

1. Exploiting the advantages of the Dark Web and its technologies rather than standing against them
(2) Giving perpetrators on the Dark Web the chance to make mistakes in concealing their identities and the secrecy of their trades, which can lead them to expose their identities and thus incriminate themselves

(3) Collaborating with encryption and anonymization software developers, such as TOR, to find solutions to regulate or stop the hidden services since they are the prime host of illegal activity and content on the Dark Web

(4) Activating the ethical code in cyberspace in conjunction with rational monitoring procedures to focus on the positive usage of the Dark Web while indicating the hidden risks in it, producing a balance that facilitates and creates a more safe and free Internet

7. Conclusions

Cryptomarkets are widespread Dark Web platforms for illegal gaining through trading various illicit products and services, especially drugs. The technical complexity of websites on the Dark Web makes them unique in operational mechanisms and hard to track by legal authorities. Moreover, behind this technological appearance lies a society of cryptomarket members that are supportive to each other and to the community they belong to, where they express, sometimes sentimentally, their beliefs towards that community, and call for a stand to preserve it. Global law enforcement agencies worked together in action against cryptomarkets. However, studies show that these actions had a slight effect on the overall business of cryptomarket users, as the latter often find a way to regather and continue their business on available replacements or create new ones. In this paper, we introduce a conceptualization approach of cryptomarkets. We discuss the definition of cryptomarkets, their technical bases, their social structure, and the supporting role of forums. We define the Satisfaction Factor, which comprises numerous social and technical elements that play a significant role in attracting users to cryptomarkets. Furthermore, we presented a comparison of cryptomarkets and conventional markets and discussed the effects of law enforcement operations on the sustainability of cryptomarkets and their business. We indicate several directions for further research in cryptomarkets in particular and the Dark Web in general. Our conceptualization approach can provide a head start for new researchers to better understand the phenomenon of cryptomarkets and find new research opportunities in the domain.

Data Availability

Data sharing not applicable to this article, as no datasets were generated or analysed. This article describes a theoretical research.

Conflicts of Interest

The author declares that they have no competing interests.

References

[1] D. Décary-Hétu and L. Giommoni, “Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of operation onymous,” Crime, Law and Social Change, vol. 67, no. 1, pp. 55–75, 2017.

[2] D. S. Rudesill, J. Caverlee, and D. Sui, The Deep Web and the Darknet: A Look Inside the Internet’s Massive Black Box, Woodrow Wilson International Center for Scholars, 2015.

[3] A. Grimani, A. Gavine, and W. Moncur, “An evidence synthesis of strategies, enablers and barriers for keeping secrets online regarding the procurement and supply of illicit drugs,” International Journal of Drug Policy, vol. 75, p. 102621, 2020.

[4] G. Me and L. Pesticcio, “Tor Black Markets: Economics, Characterization and Investigation Technique,” in In Cyber Criminology. Advanced Sciences and Technologies for Security Applications, H. Jahankhani, Ed., pp. 119–140, Springer Cham, 2018.

[5] E. Jardine, “The dark web dilemma: tor, anonymity and online Policing,” vol. 21, p. 30, 2015.

[6] J. Martin, “Lost on the Silk Road: online drug distribution and the ‘cryptomarket,’” Criminology & Criminal Justice, vol. 14, no. 3, pp. 351–367, 2014.

[7] J. Mounteney, A. Oteo, and P. Griffiths, “The Internet and drug markets: shining a light on these complex and dynamic systems,” in The Internet and Drug Markets., European Monitoring Centre for Drugs and Drug Addiction, Luxembourg, 2016.

[8] M. J. Barratt and J. Aldridge, “Everything you always wanted to know about drug cryptomarkets * (but were afraid to ask),” International Journal of Drug Policy, vol. 35, no. 1, pp. 1–6, 2016.

[9] J. Aldridge and D. Décary-Hétu, “Not an ‘eBay for Drugs’: the cryptomarket “Silk Road” as a paradigm shifting criminal innovation,” 2014, http://ssrn.com/abstract=2436643.

[10] A. Maddox, M. J. Barratt, M. Allen, and S. Lenton, “Constructive activism in the dark web: cryptomarkets and illicit drugs in the digital `demimonde,” Information, Communication & Society, vol. 19, no. 1, pp. 111–126, 2016.

[11] A. Anselmi, “Onion Routing, Cripto-Valute e Crime Organizzato,” 2018, http://www.dirittoopenlaglobalizzazione.it/collana-quaderni-crst-centro-ricerca-sicurezza-terrorismo/.

[12] J. Martin, Conceptualising Cryptomarkets,In Drugs on the Dark Net: How Cryptomarkets Are Transforming the Global Trade in Illicit Drugs, Palgrave Pivot London, 2014.

[13] P. S. R. Angus Bancroft, “Concepts of illicit drug quality among Darknet market users: purity, embodied experience, craft and chemical knowledge,” International Journal of Drug Policy, vol. 35, pp. 42–49, 2016.

[14] A. Bancroft, The Darknet and Smarter Crime, Palgrave Macmillan, 2020.

[15] M. J. Barratt, S. Lenton, A. Maddox, and M. Allen, “What if you live on top of a bakery and you like cakes?”–Drug use and harm trajectories before, during and after the emergence of Silk Road,” International Journal of Drug Policy, vol. 35, pp. 50–57, 2016.

[16] J. Brosèus, D. Rhumorbarbe, C. Mireault, V. Ouellette, F. Crispino, and D. Décary-Hétu, “Studying illicit drug trafficking on darknet markets: structure and organisation from a Canadian perspective,” Forensic Science International, vol. 264, pp. 7–14, 2016.
[17] L. Norbutas, S. Ruiter, and R. Corten, “Reputation transferability across contexts: maintaining cooperation among anonymous cryptomarket actors when moving between markets,” International Journal of Drug Policy, vol. 76, p. 102635, 2020.

[18] A. Bancroft and P. Scott Reid, “Challenging the techno-politics of anonymity: the case of cryptomarket users,” Information, Communication & Society, vol. 20, no. 4, pp. 497–512, 2017.

[19] G. Kamphausen and B. Werse, “Digital figurations in the online trade of illicit drugs: a qualitative content analysis of darknet forums,” International Journal of Drug Policy, vol. 73, pp. 281–287, 2019.

[20] A. Childs, R. Coomber, M. Bull, and M. J. Barratt, “Evolving and diversifying selling practices on drug cryptomarkets: an exploration of off-platform direct dealing,” Journal of Drug Issues, vol. 50, no. 2, pp. 173–190, 2020.

[21] J. Demant, R. Munksgaard, D. Décary-Hétu, and J. Aldridge, “Going local on a global platform: a critical analysis of the transformative potential of cryptomarkets for organized illicit crime,” International Criminal Justice Review, vol. 28, no. 3, pp. 255–274, 2018.

[22] S. A. Bakken, K. Moeller, and S. Sandberg, “Coordination problems in cryptomarkets: changes in cooperation, competition and valuation,” European Journal of Criminology, vol. 15, no. 4, pp. 442–460, 2018.

[23] I. Ladegaard, “I pray that we will find a way to carry on this dream”: how a law enforcement crackdown united an online community,” Critical Sociology, vol. 45, no. 4-5, pp. 631–646, 2019.

[24] N. Sotirakopoulos, “Cryptomarkets as a libertarian counter-conduct of resistance,” European Journal of Social Theory, vol. 21, no. 2, pp. 189–206, 2018.

[25] J. Aldridge, D. Decary-Hétu, and Publications Office of the European Union, “Cryptomarkets and the future of illicit drug markets,” in European Monitoring Centre for Drugs and Drug Addiction: Insights 21, The University of Manchester Research, 2016.

[26] J. Van Buskirk, R. Bruno, T. Dobbins et al., “The recovery of online drug markets following law enforcement and other disruptions,” Drug and Alcohol Dependence, vol. 173, pp. 159–162, 2017.

[27] J. Demant, R. Munksgaard, and E. Houborg, “Personal use, social supply or redistribution? cryptomarket demand on Silk Road 2 and Agora,” Trends in Organized Crime, vol. 21, no. 1, pp. 42–61, 2018.

[28] M. Tzanetakis, “Informal governance on cryptomarkets for illicit drugs,” in In Governance Beyond the Law, A. Polese, A. Russo, and F. Strazzari, Eds., Palgrave Macmillan Cham, 2019.

[29] E. Kermitsis, D. Kavallieros, D. Myttas et al., “Dark Web markets,” in Security Informatics and Law Enforcement, Springer Cham, 2021.

[30] Europol, “800 Criminals Arrested in Biggest Ever Law Enforcement Operation against Encrypted Communication,” Europol Press, 2021, 2022, https://www.europol.europa.eu/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication.

[31] A. Bracci, M. Nadini, M. Aliapoulou et al., “Dark web marketplaces and COVID-19: before the vaccine,” Science, vol. 10, no. 1, p. 6, 2021.

[32] B. A. Shelby Davis, “The dark web and anonymizing technologies: legal pitfalls, ethical prospects, and policy directions from radical criminology,” Crime, Law and Social Change, vol. 76, no. 4, pp. 367–386, 2021.