A qualitative mapping of Darkweb marketplaces

Dimitrios Georgoulias
Cyber Security Group
Aalborg University
Copenhagen, Denmark
dge@es.aau.dk

Jens Myrup Pedersen
Cyber Security Group
Aalborg University
Copenhagen, Denmark
jens@es.aau.dk

Morten Falch
Cyber Security Group
Aalborg University
Copenhagen, Denmark
falch@es.aau.dk

Emmanouil Vasilomanolakis
Cyber Security Group
Aalborg University
Copenhagen, Denmark
emv@es.aau.dk

2021 APWG Symposium on Electronic Crime Research (eCrime) | 978-1-6654-8029-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/eCrime54498.2021.9738766

***Abstract*—Darkweb marketplaces have evolved greatly since the rise of the Silk Road in 2011, the first platform of its kind, and have become a highly profitable underground trading ecosystem, which provides anonymity for both buyers and sellers. Law enforcement along with researchers, have been successful in taking down marketplaces over the years. However, the combination of mechanisms implemented by these platforms (e.g. payment mechanisms, cryptocurrencies, trust systems), along with the success of the Tor network's anonymity properties, have made marketplaces much more enticing to users, while providing ease of access and use, as well as resilience against hostile actions. Through qualitative methods, this paper presents a mapping of darkweb marketplaces. We systematically investigate the operation of 41 marketplaces, along with 35 vendor shops, and gather information about the mechanisms and features implemented. Additionally, to acquire real world information, we explore the marketplaces' integrated forums, as well as 3 popular independent ones, focusing on discussions between vendors, buyers and marketplace owners, on topics related to illegal trading. We believe that gaining an up-to-date and deep understanding of the framework that marketplaces are built upon, is the first step towards discovering weak spots in the cyber security product and service market, with the disruption of its operation being the ultimate goal.**

***Index Terms*—darkweb, marketplaces, illegal trading, cryptocurrency, cybercrime**

I. Introduction

The year 2010 marks the appearance of underground marketplaces in the Darkweb. It all started with the *The Farmer's Market*, which moved its operation from the clearweb to the Tor network. However, *Silk Road* is considered as the first successful darkweb marketplace of its type, due to its much greater impact [1]. This type of marketplace could effectively provide anonymity to its clients. This was achieved through utilizing the Tor network, and specifically its hidden service function. Potential buyers would use the hidden service's onion address to access the marketplace, remaining anonymous while doing so. They would then be met with a variety of vendors offering products and services, from which they could choose according to their personal preference. Furthermore, the implementation of Bitcoin (BTC) transactions, certainly added to the anonymity of all involved parties, namely the buyers, sellers, and marketplace owners.

This adoption of an online marketplace, has served as a blueprint for all the marketplaces that succeeded Silk Road in the last decade. Implementations have only become more robust and resilient against takedown and infiltration attempts from LEAs. Furthermore, the variety of products and services available for purchase, has increased considerably, along with their availability and the cryptocurrencies that can be used to acquire them. Darkweb marketplaces are part of an ecosystem that operates similarly to legitimate enterprises, with the most important addition being anonymity. They present mechanisms, such as vendor reputation systems, escrow, communication encryption (e.g. PGP), review systems, integrated forum sections with discussions, and customer support functions, all of which aim to build a chain of trust between the buyers, sellers and the marketplace owners. Furthermore, this trust is achieved without either of the parties involved, revealing their identities to one another. The darkweb is considered somewhat of a mystery by most users, which creates hesitation, mistrust and even fear, disheartening users from ever using it. Consequently, minimizing the risk of clients getting scammed by vendors, in combination with anonymous transactions and communications, as well as the sense of a community through forum discussions (both integrated and independent), create an environment where clients can feel safe and more encouraged to carry out purchases.

The products and services available on the darkweb marketplaces present great variety. Some popular examples are drugs, guns, bank card and account credentials, social network platform accounts (e.g. hacked Facebook and Twitter accounts), counterfeits (e.g. fake driving licenses), hacking services, exploit kits, botnet services (e.g. DDoS attacks, botnet rentals and sales) and malware. However, since the COVID-19 epidemic outbreak, the marketplace scene has adapted. Many vendors have been trying to capitalize on people's fear of infection, and the global need for protection against the virus. This has lead to marketplace product listings also including testing kits, vaccines, forged test results, as well as fake vaccination certificates [2].

Darkweb marketplaces have been getting more and more successful over the years. The revenue generated reached approximately $1.7 billion in 2020, 75% ($1.3 billion) [3] of which was reportedly generated by the Russian marketplace Hydra, making it by far the most profitable marketplace. Furthermore, for the year 2020, ranking countries according to

both the value sent to these marketplaces (purchases) and the value earned by them (revenue), presents Russia dominating the top of the list in both aspects, with the United States and Ukraine occupying the second and third place respectively [3].

In this paper, we investigate the current state of marketplaces in the darkweb. We focus on 41 marketplaces and their forums, but we also navigated through 35 vendor shops, as well as 3 independent darkweb forums, in order to gain a deeper understanding of the entire darkweb ecosystem. Our contribution lies in mapping the darkweb marketplace infrastructure, by documenting the mechanisms and features implemented by marketplaces in the darkweb, as well as the practices applied by vendors, buyers and marketplace owners. We argue that gaining detailed insights on the infrastructure's different characteristics and properties, is a stepping stone towards vulnerability discovery, exploitation, and consequently, the disruption of darkweb operations related to cyber attack products and services, such as botnets, malware and exploit trading.

II. Methodology

The information gathered for the purposes of this paper, originate from 3 main sources; 41 marketplaces, including their integrated forums, 35 vendor shops, and 3 popular darkweb forums. Regarding the choice of platforms, the marketplaces we include are all that were operational at the time of this paper (August 2021), and the forums were chosen based on popularity. Vendor shops, being shops of individual sellers, present very limited variety of features and properties, and do not provide as much insight as marketplaces, since they are considerably smaller. However, navigating through them provided additional data on various basic mechanisms that are shared in common with the bigger marketplaces, but since their number is quite high, for the purpose of this paper we deemed exploring 35 of them to be sufficient. The information we document originates from a combination of Frequently Asked Questions (FAQ) sections, as well as guides and discussions between marketplace users, both vendors and buyers, found on the forums. Visiting each marketplace and vendor shop individually, and attempting to test out each platform's features and infrastructure, was necessary towards gaining as much insight as possible on the darkweb market.

In more detail, the way this process was executed, was firstly visiting the marketplace, and documenting the CAPTCHA mechanisms. We then proceed to make a user account, since in the majority of the platforms it is a requirement (apart from some special cases), to gain access to the product listings. In many cases there would be another CAPTCHA required to finalize the registration, which was also documented. The next step included navigating though the FAQ section and forum sections of the site, where we would typically acquire information on the features and properties of each marketplace. We would then focus on browsing through several product listings, vendor profiles, and user reviews, gaining insight on elements such as currency, payment methods, and reputation systems. Furthermore, we would also test the features discovered, along with some basic mechanisms such as deposits and withdrawals, as well as go through the purchase process up until the point of payment. However, we did not carry out any purchases due to ethical and legal considerations. The way we tracked down the onion addresses for all of the platforms we visited, was through *introduction points*, sites (often both on the clearweb and darkweb) serving as directories for hidden services. Apart from the procedure described, previous academic research on some of the elements mentioned in this paper, also provided guidance, contributing to our efforts (see Section IV).

A. Ethical issues

At this point we need to address the ethical standpoint of this paper. All of the platforms we investigated are part of the public digital space and free to access. Since we interacted with each platform's functions as plain users, we did not cause any disruption to the services, and did not in any way negatively affect the experience of other users. Furthermore, we did not acquire or analyze any type of user sensitive data. We only utilized publicly available sources, such as forum discussions and reviews, without disclosing information that could potentially breach the privacy of any individuals or risk exposing their identity.

It has been argued by previous research that these platforms can be viewed as a safer alternative to conventional real-world drug trading, due to its digital nature [4]–[9]. Hence, it should be clearly stated that the goal of this work is not to bring down marketplaces. This research instead aims to be used as a stepping stone towards disrupting specific cyber attack services, with Distributed Denial of Service (DDoS) service providers as a prime example [10]. Lastly, we do not provide a full list of the targeted marketplaces, but we do however mention some of them by name throughout this article, in order to showcase various operational features and example mechanisms that they implement. The rationalization behind this is that we want to avoid directing traffic to as many platforms as possible, but without hindering the scientific contribution of this paper.

III. Marketplace Elements

In the effort of mapping darkweb marketplaces, we categorize the properties of these platforms into *Access & Authentication, Products & Purchases, Shipping & Delivery, Vendor Reputation, Support, Disputes & Community, and Marketplace Revenue*.

A. Access & Authentication

1) Access: The majority of darkweb selling points, as well as all of the 41 marketplaces we investigate in this paper, are free to access and can be located through both clearweb and darkweb websites or using darkweb search engines such as *Torch*. However, there are a number of platforms that are only available through a registration fee, or through invites, which are made available to trusted users. These users can

vouch for newer members, that will then avoid paying for the access, which can get quite expensive (e.g. the *KickAss* forum fee is $450). Despite the restricted access mechanism, invites for some of these platforms can often be found for sale on marketplaces, sometimes for a fraction of the price. Additionally, it is not uncommon practice for paid-access shops and forums to offer some kind of discount to attract new members, which they will advertise in popular forums such as *Dread*.

2) Protection Mechanism - CAPTCHAs: The majority of the 41 marketplaces we visited for the purposes of this article implemented DDoS and crawling protection (see Appendix C). Most platforms would firstly place the user in a queue, lasting a few seconds, and then prompt a CAPTCHA which would either be a standalone mechanism, or part of the registration/login page. In the former scenario, after solving the first CAPTCHA, there would usually be a second one embedded in the registration/login page. The CAPTCHAs implemented are typically text-based, image-based, e.g. image puzzle solving or image matching under a specific context, in a question and answer format, e.g. mathematical equations, and lastly in an analog clock format (see Figures 1 4 and Appendix D[1]). In this case the user is met with an analog clock face showing a random hour/minute combination. They then have to beat a one minute timer, which starts counting down immediately after the web page loads, in which time they have to choose the two correct numbers corresponding to the hours and minutes of the time shown, in a 12 hour format, from two drop down menus located below the clock itself. The *Vice City* marketplace also uses a CAPTCHA where the user is given a set of 9 symbols, some of which are colored in, along with a 3x3 table with empty circles. To solve the CAPTCHA, the user must then choose the circles that share the same position on the table, as the colored symbols on the given image. The *ASAP* marketplace, uses a set of moving text characters, the user must distinguish and input. Furthermore, the *Yakuza Market* CAPTCHA implementation is the solution of a basic mathematical equation, while the *Nemesis* marketplace utilizes an image based puzzle, where a photo is split into 24 blocks, with 5 of them not matching. The user needs to simply choose the misplaced image blocks. The *Monopoly* marketplace CAPTCHA, out of a set of rings, requires the user to click on the broken ring, while the *Kingdom Market*, deploys an image-based numerical puzzle, where the user needs to click on 9 boxes containing numbers, in the correct ascending order. *The Majestic Garden* market/forum, prompts the user with a text based CAPTCHA, along with 3 simple questions/puzzles. *CannaHome* after a simple text based CAPTCHA, deploys a secondary mechanism, where some characters of a small text are marked with red arrows. The user needs to pick out these characters, input them in the bracket below and they can then proceed to the homepage. Lastly, it should be noted that all of the CAPTCHAs with a timer would be standalone mechanisms, and in most of these cases there would be a second CAPTCHA at the login page.

3) Marketplace Verification: An optional, but crucial step in regard to the user's security, is the verification of the marketplace's identity (see Appendix C). In the darkweb, it is quite common for fake mirror addresses to make their appearance, in an effort to phish users, by imitating the original marketplace. This often occurs in the case of a marketplace's seizure by Law Enforcement Agencies (LEAs). In this case, cybercriminals take advantage of the seizure, and rush to set up a new hidden service, which poses as the original marketplace, where users get phished and scammed. For this reason marketplace owners implement the Pretty Good Privacy (PGP) protocol for authentication. They create a key pair, public and private, and they use the private key to create signed messages, that the users can then verify using the public key. The user can find the public key of the marketplace, on the platform itself (often behind another CAPTCHA), as well as on popular darkweb forums and *introduction points*[2], which also adds to its validity. One of the two main practical uses of this mechanism, is to authenticate the list of onion addresses that the marketplace can be accessed through, also referred to as mirrors. The marketplace owners create a message which contains all of the mirror addresses, and then sign this message with their private key, proving the legitimacy of the hidden service. This way the user can be certain that they are visiting the original marketplace, by locating the onion address they are using to connect in the signed list of mirror addresses. The second application of the PGP protocol, is to verify the identity of the marketplace owners. This message is often referred to as a *Canary*, it traditionally contains the date and timestamp of its issuing, and it is renewed frequently. In some cases, this message was found to also contain news headlines from popular websites or darkweb forums, proving the message was created recently (e.g. White House Market). Through this system, the users are reassured that the individuals behind the marketplace's operation are still the original owners. In some cases the two aforementioned messages, are combined into a single one, which is yet again updated with a set frequency. It should be noted that the marketplaces will hold onto the same private key, since it essentially is the proof of the marketplace ownership, and serves as the foundation of the entire authentication mechanism. An additional verification method implemented by many marketplaces, is including the onion address of the hidden service, in the background image of the CAPTCHA. This helps the user ascertain that they are not visiting a fake, identical to the original, platform. Lastly, another factor that can contribute towards determining a marketplace's validity, is forum posts of esteemed members, publicly announcing their support towards a platform, as well as discussions providing positive or negative feedback.

4) Registration: After going through the queue, and solving the standalone CAPTCHA (if one is utilized), users are able to

[1]We discovered several different CAPTCHAs, but they were a similar implementation to the ones illustrated in Figure 1.

[2]Introduction points are sites, both in the clearweb and in the darkweb, that contain onion addresses of several platforms, often along with their PGP keys. Examples include *Recon* and *Dark.Fail*.

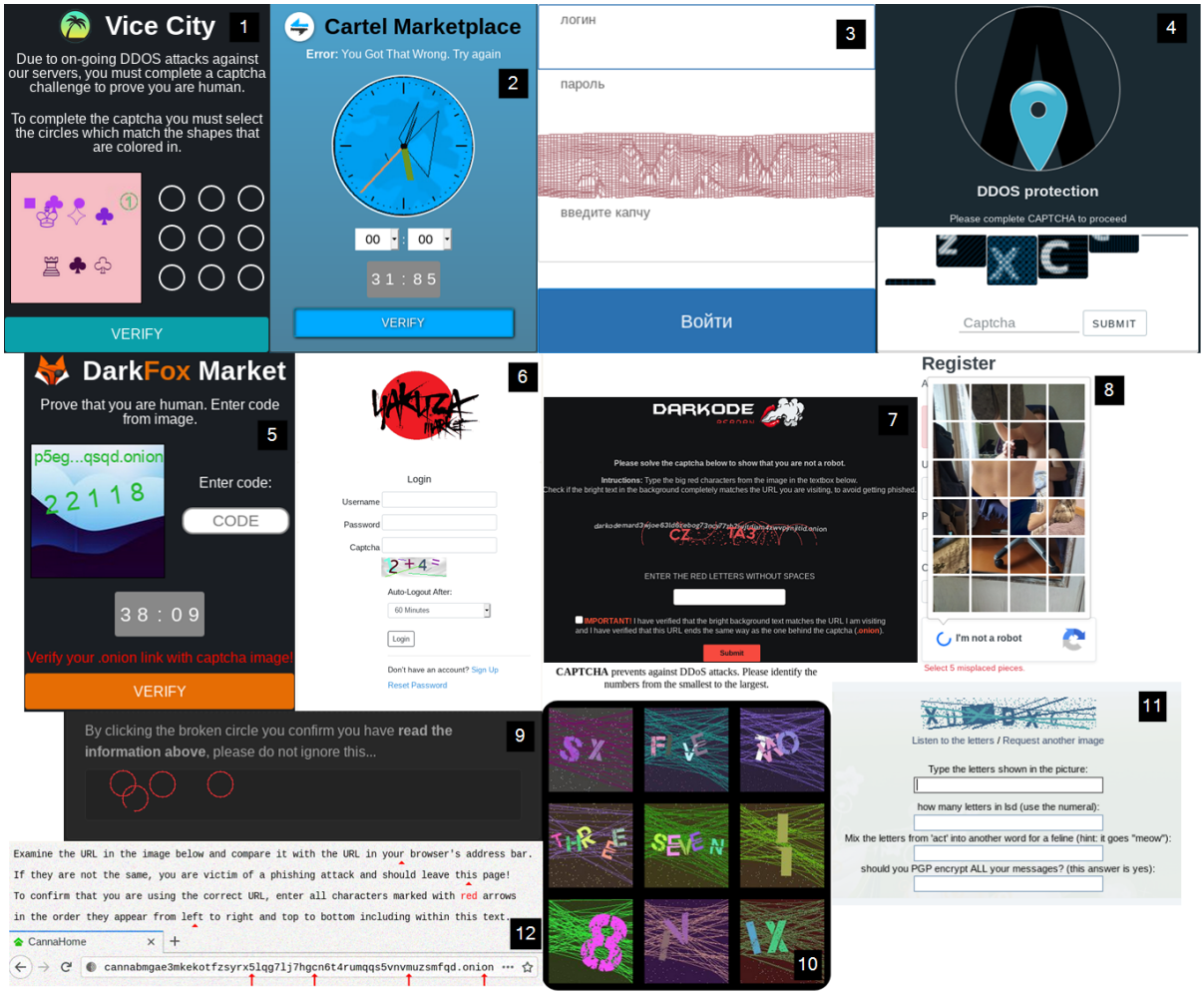

Fig. 1. CAPTCHAs from popular darkweb marketplaces: *1. Vice City, 2. Cartel Marketplace, 3. Hydra, 4. ASAP, 5. DarkFox Market, 6. Yakuza Market, 7. Dark0de Reborn Market, 8. Nemesis Marketplace, 9. Monopoly Marketplace, 10. Kingdom Market, 11. The Majestic Garden, 12. CannaHome*

either log in, in the case of an existing account, or register for a new one. In the case of registration, the process is simple. The information the user has to input in the form, are their username and password, and in most cases a 6-digit pin, which serves authentication purposes. Some marketplaces may also have mandatory Two-Factor Authentication (2FA), which in most cases translates into the user entering their PGP key (see Section III-A5). On one particular platform, the user PGP public key was even used instead of a password, for login purposes. In the majority of the marketplaces we investigated, the last step included a mnemonic given to the user, which was either a simple sentence composed of random everyday words, or a string of random characters. Since none of these platforms required an e-mail address in the registration process (apart from some minor exceptions), this mnemonic is to be used in the case the user ever needs to recover their forgotten login credentials. To finalize the registration, the user has to verify their mnemonic, in most cases solve a CAPTCHA, and then they can access the marketplace through the login page. At this point it should be mentioned that in most of the marketplaces, the user cannot reach the product listings unless they register and login with their account (see Appendix C). However, there was one specific platform that allowed for purchases without the need of registering an account, with the PGP key of the buyer acting as the sole identification method.

5) User Authentication: After establishing their account, the user can login using with their credentials, and in most cases, by additionally solving a CAPTCHA. However, users also have the option of setting up 2FA (see Appendix C), which is achieved through PGP or by using a Time-based One-Time Password (TOTP) [11]. In the case of PGP, the user must initially register their public key in their account. Every time they try to log in, after entering their password, the marketplace will use that public key to sent an encrypted message to the user, which contains an additional passphrase. The user must then decrypt the message, derive the passphrase and enter it to complete the log in process. If TOTP is chosen as the authentication method, the user is provided with a QR code, as well as a text code, both intended to be used for generation of one-time codes. This can be accomplished using

authentication applications, such as Google Authenticator or KeePassXC.

B. Products & Purchases

1) Product Listings: The products available in the darkweb marketplaces have been well documented over the years [12]–[14], with more recent work even accounting for the changes that came as a result of the COVID-19 pandemic [15]. For this reason, we decided to mainly focus on the framework that surrounds the listing process of these products, as well as the code of conduct that dictates how they are carried out.

Depending on the platform in question, the rules regarding product listings can slightly vary. Marketplaces will have rules in place forbidding certain products from being listed on the platform. These products are usually child pornography, terrorism related products, weapons, human/animal abuse material, murder for hire services, and most recently, so-called COVID-19 "cures". These individual types of products and services, can still be found in dedicated vendor shops, with some being more difficult to track down than others, due to their varying level of legality and how closed the corresponding community is (e.g. firearm versus child pornography vendor shops).

In addition to the rules regarding the products and services, vendors must follow certain requirements, in order to create listings on the platform. In some marketplaces these requirements are obligatory, but in others, vendors are given more freedom. Vendors are primarily asked to provide information on the type of their product, exact quantity and price, production origin, an image of the product, the shipping available destinations and origin, as well as shipping methods and their pricing. This applies to physical product listings, since digital product listings (e.g. stolen bank credential information), do not need to include any information related to shipping. Some marketplaces may be very specific regarding this information. For example, *Cartel Marketplace* explicitly asks for an image showing a large quantity of the product, along with a piece of paper stating the names of the vendor and the marketplace.

There is also precedent of marketplaces having listings of various products, but without implementing the typical "add to cart" mechanism, that is used on legitimate platforms on the clearweb. An example is the *Cave Tor* marketplace, which apart from the product information, they will only include the vendors' contact information, that potential buyers can use to set up the purchase privately with the vendor. Some marketplaces, such as *The Majestic Garden*[3], will not even display product listings, but will adopt a forum architecture, where clients can find vendors for the products they need in specific sections and threads of the forum.

A big contributor to a vendor's success on a marketplace is also the level of exposure that their listed products are able to get. Clients visiting a marketplace, will find that some products are being showcased, taking priority over others. This is done through a number of factors, such as feedback related to the product or vendor, popularity, listing interaction from the clients, as well as the buyer's browsing history on the site. For example, in the case of the *Cartel Marketplace*, the implementation of this mechanism is called *Cartel PageRank*, it is awarded to the product, and the higher it is, the more traction a product will get. The *White House Market* also has a similar mechanism in place, which moves the top 20 sellers, based on the amount of sales in the last 45 days by Monero (XMR) value, higher up the product list. Lastly, vendors can choose to pay for the promotion of their products (see Section III-F4) by issuing a fee to the marketplace, instead of letting the algorithm do it for them, by factoring in the aforementioned variables. With the *White House Market* again as an example, vendors can bid for eight spots, rotating every single week, where their products can be featured.

2) Currency: The most popular and most widely used cryptocurrencies to conduct payments in darkweb marketplaces, are BTC and XMR. The differences between the operation of the two protocols, have great impact on the level of anonymity that they are able to offer to their users.

a) Bitcoin (BTC): The main issue with the usage of BTC has been privacy. Transactions made with BTC can be monitored, due to the fact that they are publicly announced on the blockchain. By using a block explorer, one can easily find information about payments made to certain wallet public addresses, along with their origin, the exact amount transferred, transaction history and balance. This leads to Bitcoin having a *fungibility* issue [16], meaning that two BTC coins can never be regarded as equal, since every BTC can be traced back to its point of creation in a defining way. Furthermore, acquiring BTC from a cryptocurrency *exchange*, will require providing some kind of identification, also known as *Know Your Customer (KYC)* information. The combination of these two facts, can potentially lead to the deanonymization of users, in the event of a marketplace seizure. In such a scenario, gaining access to the marketplace's wallet, could lead to LEAs following the trail back to the public address (or addresses in the case more than one are being used) of a buyer, which can then be linked to the user's real identity, through the information available to the exchange service. In an effort to make BTC more anonymous, *mixers*, or also known as *tumblers* [17], [18], came into play, which aim at erasing the trail the transactions leave behind, for a small fee. One simple example scenario, would be making a payment to the mixer service, which would "mix" the funds with those of other users, and then transfer the amount to the desired destination wallet address. With the mixer acting as the middle man, the trail that could lead back to the original user, is harder to follow. This mechanism can also be used to launder BTC, where a user could send the funds to the mixer, and then have the mixer transfer the funds back to them, after the "mixing" process is complete. However, similarly to how exchanges operate, mixer services will often keep information about their users, which can be used to trace back to the user a transaction originates from. Additionally, this way of operation is very

[3]This specific marketplace is not included in the list of 41 platforms we investigated, since it was not free to access. We did however document its CAPTCHA mechanism (see Figure 1) and found information regarding its operation through forums discussions.

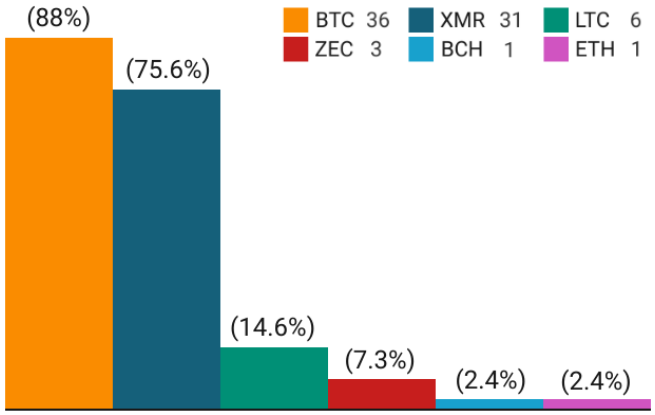

Fig. 2. Cryptocurrency adoption on the 41 darkweb marketplaces. The legend depicts the total number of marketplaces out of the 41, that allow for transactions with each cryptocurrency.

prone to phishing attacks and scams, which translates into fake service providers, that will keep the funds for themselves after the user has transferred them.

b) Monero (XMR): Despite Bitcoin's popularity over the years, the most recommended and safest practice to carry out payments on the darkweb, is through the usage of Monero. XMR obfuscates the origin, destination, and amount of the transactions, which makes tracking them back to users extremely challenging for LEAs [19], [20]. XMR also has the *fungibility* property [16], contrary to BTC (see Section III-B2a), making coins interchangeable. Marketplace users are encouraged to swap out any BTC they own for XMR and then move forward with their purchases. Even in the event that a user would like to make a transaction specifically using BTC, the recommended course of action, deducted from guides and discussions on the darkweb, is to initially convert BTC into XMR, then convert again to BTC using a second independent wallet, and only then go through with the transaction. Both of these practices are effective, due to the fact that the trail is lost the moment the BTC amount is converted into XMR. Despite the additional security that XMR offers, marketplaces seem to be making an effort to make transactions even more safe for users, with *AlphaBay* as an example, which uses XMR mixers as an extra layer of security.

Bitcoin and Monero might be the most frequently used cryptocurrencies at the moment (July 2021), but there are certainly others being used as well, namely Litecoin (LTC), Zcash (ZEC), Bitcoin Cash (BCH) and Ethereum (ETH). In Figure 2 we present the percentage of cryptocurrency usage throughout the 41 marketplaces we investigated.

Lastly, in the particular case of *Hydra*, there are a few additional methods of payment. The Russian marketplace also accepts payments through the *QIWI Wallet*, which allows for anonymous transactions, and through SIM card top-ups [21].

3) Wallets: Payments on the marketplaces, can be done either through off-site wallets, or through each platform's on-site wallet (if it utilizes one). Regarding off-site wallets, darkweb guides and forums threads advise users against using *custodial/hot wallets* to store their cryptocurrency. In this scenario, the user shares custody of their private key with a third party, and since the user does not have exclusive control over their private key, the same can be stated about their funds (*"Not your keys, not your coins."* [22]). Conversely, *non-custodial/local wallet* usage is encouraged, such as hardware wallets, where the private keys are saved locally and are never shared with anyone [23]. In the case of a purchase, the user deposits the amount to a cryptocurrency address, unique for every purchase.

With on-site wallets, users can deposit funds in various cryptocurrencies, depending on the platform, and credit them on their accounts. This is done through a cryptocurrency address, generated by the marketplace, which is unique for every user, and usually available for a certain period of time (e.g. 7 days). Users can then use these funds, or account *balance*, to carry out their purchases, instead of using their own wallets. The users can still maintain their own wallet as mentioned above, from which they perform the balance top-ups. Each user has the option to withdraw their balance at any point, but the process differs per marketplace (see Sections III-F3 and III-B6). Purchasing via an on-site wallet, translates into the funds being redacted from the account balance. Some platforms, e.g. *Dark0de*, have an on-site wallet, but also allow for payments through the users' wallets.

In the context of wallets, one mechanism that stands out among the marketplaces, is *AlphaBay*'s *AlphaGuard*. In the case that the marketplace is seized by law enforcement, this mechanism will broadcast a set of onion and Invisible Internet Project (I2P) addresses through various channels on the web that the users can visit and retrieve their funds (these channels are not however specified). This is done through a key that each user is given by the marketplace at the point of registration called the *wallet recovery key*, and along with their username and password, it can be used to empty the on-site wallet by moving the funds to a new deposit address chosen by the user. The description of this mechanism is in line with the information provided by the marketplace owner themselves. We were not able to test it, since it would require an attack against the marketplace to take place, but we were however provided with a wallet recovery key after the registration process.

4) Escrow: Escrow is the primary mechanism through which darkweb marketplace sales are carried out. When a client purchases a product, both in the cases of an on-site and an off-site wallet, the paid amount is transferred to a cryptocurrency wallet owned by the marketplace. The wallet public address used to deposit the funds, is unique for every purchase. The amount will remain there up until the client verifies that they have received the product they purchased. Only then will the amount be released from the wallet and transferred to the wallet of the vendor. This system aims to avoid incidents of fraudulent behavior from the side of the vendors. In the case of its absence, the marketplace would not be serving as an intermediary, meaning that the vendor would be directly paid by the customer. In this scenario, it would be

very easy for the vendor to lie about dispatching the ordered items, or even simply cutting all ties with the client altogether, while having received the paid amount.

5) Auto-Finalize: From the vendor's side, in order to offer some type of assurance that the funds will eventually reach them, even if the client does not notify the marketplace about the delivery of the order, marketplaces implement the *Auto-Finalize* mechanism. This mechanism dictates that after a set time interval (e.g. 14 days, or even 45 days), if the client has not verified the delivery of the ordered product, the order will be finalized automatically, releasing the funds from escrow to the corresponding vendor. Failing to finalize the order, in some marketplaces, will lead to the client account receiving negative rating, incentivizing users to finalize as soon as possible.

6) Multisignature Escrow (Multisig): One issue that still remains, despite the implementation of the escrow mechanism, is *Exit Scams*. In an escrow purchase scenario, since the paid funds are initially transferred from the client to the marketplace wallet, the whole amount is under the control of the marketplace. Since the rise of darkweb marketplaces, there have been many incidents, where the marketplace would shut down, going offline without prior notice to the vendors and clients. All the funds gathered from every single purchase carried out, would remain with the marketplace owners, with vendors left unpaid, and some of the clients paying for a product that will be never dispatched (some orders might have already been on the way to the clients). Some examples of exit scams are those of the *Wall Street Market*, *Icarus Market*, *Elite Market* and *Empire Market*, with the last one, shutting down and stealing $30 million worth of bitcoin in the process [24].

To eliminate the danger of exit scams, many marketplaces support BTC multisignature escrow payments, or *multisig* (see Appendix C). In a multisig scenario, the main idea is that out of the three entities involved in a purchase, namely the buyer, the vendor, and the marketplace itself, there is always authorization from two of them needed, to finalize a transaction. This effectively means that in order for the transaction to be completed, the corresponding private keys will be needed, to provide the two necessary signatures. Typically, one signature will come from the client, after they have received the product, and one from the vendor themselves. In the case that the client does not finalize the order after receiving the item, the marketplace and vendor can provide the two signatures. Most importantly, in the event of a marketplace exit scam, the funds are not trapped inside the marketplace wallet, which is the case with the standard escrow paying scheme. The funds can be released through common understanding between the vendor and client, agreeing to both sign off on the transaction, and let the purchase process reach finalization without further issues. The same practice applies when paying for marketplace commission fees (see Section III-F1).

7) Direct Payments: Direct payments were not implemented on either of the marketplaces we explored, contrary to vendor shops, for which this was the only available payment option. One exception to this rule, was the *Televend* marketplace. Televend uses the *Telegram* application, as a platform to carry out sales. Users can join a channel, and purchase their product of choice, directly from the vendors. The hidden service site is only utilized to present information such as reviews, feedback, vendor profiles, listings, and to provide vendor registration and verification, making the Telegram channels the actual marketplace. The purchase process is automated through the deployment of Telegram bots, and without utilizing any type of escrow mechanism.

8) Finalize Early (FE): Many marketplaces, have a mechanism in place, which allows for the transfer of the paid funds to the vendor, immediately after the payment has come through from the buyer, before the ordered items are even dispatched. This mechanism is called *Finalize Early (FE)*. Early finalization aims to provide ease from the vendor's side, who does not have to wait for the order to arrive to the client to receive the payment. Additionally, in case a client fails to finalize the order, the vendor does not have to sit through the whole duration of the escrow wait time, which can sometimes be more than a month. Marketplaces will only provide the finalize early badge/capability to highly trusted vendors, replacing standard escrow. For example, *World Market*, which is a very popular marketplace, will only assign the label to vendors that have reached the "level 5", which requires 250 sales, $25 000 in sale volume, and 90% positive feedback from past clients. Some marketplaces will also take into consideration sales, reviews and feedback from other marketplaces that the vendor has been making sales on, as well as whether they already have achieved the FE verification on other platforms.

The question that naturally arises from the implementation of the FE functionality, is why should a client want to buy from such a vendor, since due to the absence of escrow, they essentially have no fall-back in the case their order never arrives. There is no assurance that the product will even be dispatched in the first place. The answer comes from the requirements that a vendor needs to fulfill to achieve the FE status. Having this status is on itself a guarantee that the vendor is well established, verified, offering high quality products, and held in very high esteem in the darkweb marketplace ecosystem. The probability of scams from these vendors are extremely low, since no vendor would risk damaging their reputation, that they worked so hard to build. Additionally, in many occasions, in order to motivate the buyers and make buying from FE vendors more appealing, marketplaces will offer some kind of discount. An example is the *Cartel Market*, which applies a 5% discount to orders from such vendors. This serves vendors, marketplaces, and buyers alike. Vendors, make more sales, which directly means more profit. Marketplaces are hosting these sales, which translates into more commission fees from each sale (see Section III-F1). Lastly, buyers get a better price for the product of choice, which will be of higher quality, because of the prestige that accompanies the FE status.

9) Refunds: In the case of a transaction running into issues and a refund is necessary, the buyer will provide a cryptocurrency address, where the funds will be deposited, or in the case of an on-site wallet, the amount will be credited to their account balance.

C. Shipping & Delivery

The details surrounding the dispatch of a physical product, and its delivery to the buyer, are a determining factor in how cost efficient and discrete a purchase from the darkweb can be. Vendors will list the shipping methods available and the client is free to choose whichever they prefer, but there are many details that can make the difference between a successful delivery and prosecution by the law. It should also be mentioned, that regardless of which of the following methods the client chooses to use, any private information given to the vendors, such as names and addresses, are always encrypted through the PGP protocol.

1) Origin & Destination Countries: The first determining factor regarding the risk taken when purchasing from a darkweb marketplace, is the country of origin, that the product will be shipped from, as well as the country it will be delivered to. Ordering from foreign countries, carries far greater risk than doing it domestically. The main reason behind this, is the fact that the product will go through customs twice, once leaving the country of origin and once entering the destination country, increasing the probability of the order getting intercepted. Many users are tempted to place an order from outside their countries, due to the fact that in the majority of cases one can find the same product at a lower price from non-domestic vendors. Furthermore, according to past experiences from marketplace buyers found on forums and guides, packages arriving from certain countries are labeled as more probable to contain illegal items, with some examples being the Netherlands and Colombia, in connection to drug trafficking. Ordering from these countries will certainly carry greater risk for a buyer, since the package carries more suspicion than usual. Similarly, some countries have more strict custom checks, with Sweden and Norway as examples, making packages ordered internationally, while being a citizen of these countries, more prone to getting intercepted at customs.

2) Real Name & Address: Throughout forums and marketplaces, discussions and guides point to the same practice, when it comes to placing an order. The users are always encouraged to use their real private information, namely their names and addresses. The main reason behind this course of action, is that not doing so, is considered much more suspicious behavior. Handling an order from a darkweb marketplace, the same way one would treat an order from a legitimate online shop, is much less likely to draw any attention. It is considered that even if something goes wrong with a delivery and a package is intercepted by LEAs, as long as it cannot be proven that the order and payment were carried out by the buyer, then the buyer is safe from prosecution. This applies even in the case that the buyer signs for the delivery, making Operational Security (OPSEC) of the utmost importance in both scenarios.

3) Post Office (PO) Boxes: Another available option for buyers, is using a Post Office (PO) box. Creating a PO box requires a real name and address, tying the user's identity to its existence. Using a fake ID is strongly advised against, since it is much more likely to create suspicion. By registering a PO box the buyer loses plausible deniability, since the box is registered under their name, and unlike their address which is public, it is private. Hence, the majority of forum user posts, pointed towards avoiding the usage of PO boxes (see Appendix A), and many vendors will not list PO boxes as a delivery option, considering this method to be an OPSEC risk.

There were two more interesting practices mentioned on the forums. One was using fake IDs to open PO boxes in "mom-and-pop" shops (small family business shops), which the users should close after receiving their order. They would then repeat the same process on another shop, with a new box. The second method was UPS store boxes. In this case the buyer registers for PO box, but under the pretense that it is to be used for an online business, sidestepping the requirement to provide their real name. Instead, they provide a fake business name, which cannot be tied directly to the user.

4) Drops: Apart from having the package delivered to their house, a user can also choose to use a *drop*. Drops are in essence locations that cannot be related to the buyer, but can still be used to receive mail. Guides on the darkweb explain how to choose the optimal location, as well as how to make it look as less suspicious as possible. An example given, is choosing an uninhabited house, at which the user should go from time to time, without making themselves memorable, but creating the belief to the rest of the neighborhood that there is someone associated with the premises. A guide even mentioned performing some kind of maintenance on the grounds, such as mowing the lawn. Nonetheless, the main suggestion was that the user should send mail to that address using an alias, as a means of "priming" the address. This would help towards not drawing any unwanted attention when the marketplace order finally arrived in the mail. However, drops are generally discouraged, since as previously mentioned, using the real address and name is the safest option.

5) Dead Drops: Some vendors will also provide *dead drops* [25], [26] as a means of delivery, which was initially documented on the *Hydra* marketplace in 2014. In this scenario, the purchased item is left at a random location, that only the buyer and the vendor are aware of. No names or addresses are exchanged, maintaining anonymity for both parties, and sidestepping the dangers associated with normal post. These locations can be anything from remote spots, like a specific tree in a random street, to very public places, such as public transport stations. The item drops are handled by individuals known as *droppers*, who get paid on commission depending on the type and amount of the product they deliver [26].

The execution of a dead drop can be summarized into a few simple steps: finding the perfect location, placing the item, taking a picture on which the exact spot where the item was placed is marked, and lastly, including the GPS coordinates along with a map screenshot of the exact location. After the drop is made, the dropper will upload all the information on the marketplace, so that the buyer can use them to retrieve the package [26], [27].

6) Packaging: Another determining factor on whether a delivery will be successful or not, is packaging. Packaging can easily be the cause of a delivery drawing unwanted attention,

and getting intercepted by LEAs. For this reason, discussions on forums, along with previous research on the subject [28], point to certain practices, that are utilized to avoid detection, through eliminating smell and DNA traces, that could be left on the package. These practices are air-vacuuming the item at least once, use of heat-sealed bags/Moisture Barrier Bags (MBBs) and Mylar paper, printed labels, use of decoys for external packaging, in which the item can be hidden, and cleaning the packaging with alcohol. Furthermore, data points towards the use of specific gear while packaging the items, such as cotton and latex/rubber gloves, used in combination with one another, long sleeve shirts, hairnets, ski masks, even full body protective suits, such as hazmat suits. One more practice suggested, is using a different room to externally package the item, than the room in which the product is held, which in the case of drugs, could potentially contaminate the packaging, making it prone to detection. Information on the darkweb suggests making a compact list, of all of the above methods that a vendor could use to package an item before delivery. This way, the vendor would be less likely to make a mistake, making the whole process of shipping safer.

In the case of firearms, vendors have been documented to ship the weapons disassembled, in different packs and through different postal services, including an assembly guide [29]. Additionally, in order to conceal the products, most vendors will use unorthodox methods of packaging:

[Purchased products are concealed] ..."In Computer devices; In cans never opened; In air freshener or coca cans; In books; In stoles of pairs of shoes; It may come in bottles; In all kind of Computer devices; In Electrical goods; And in all kind of products." - [30]

One can also find 3D printing plans for firearms and their parts, listed as digital products [29] (see Section III-C9).

7) Return Address: Not including a return address on the package, or using fake addresses or names, can cause suspicion and draw unwanted attention to the package. For this reason, it is often recommended that vendors use either a real address and name belonging to random individuals, or a business, preferably small. In the first scenario, vendors are even encouraged to use the information of people living in neighborhoods with a bad reputation. The justification for this is that in the case of a returned package, it is supposedly less likely that the package will be reported to the police. Vendors also have the option of using the return addresses belonging to businesses or shopping centers, but in combination with a fake minor identifier, such as office or floor number.

8) Tracking: Users are also advised against tracking their order, unless it is provided freely by the post service, since in this scenario LEAs cannot prove that the order is actually related to the user. In both cases however, buyers are strongly discouraged to use this feature, since it can leave traces.

9) Digital Products, Autoshops & Automated Vending Carts (AVCs): In the case of digital products bought on the marketplaces, the process becomes much simpler. The methods of shipping include sending a message to the buyer, by using the built in platform messaging system encrypted with PGP, attaching a file containing the product, or providing a download link. Digital items can also be sent via e-mail, and in the case of debit card, or PayPal account balance, they can also be delivered directly as a transfer to a bank account, PayPal account, or cryptocurrency deposit. Users can also use cryptocurrency to acquire transfers through Western Union.

Some marketplaces will also implement *Autoshops*, which aims to make digital purchases faster, by eliminating the escrow mechanism. The funds are directly transferred at the moment of purchase, following the *finalize early* mechanism (see Section III-B8), thus making the purchase process instantaneous. After the payment is complete, the buyer receives the digital product through the same channels mentioned above.

Lastly, it should be mentioned that there is a special type of platform offering digital products, known as AVCs [31], which function entirely automatically, and one could in essence describe them as standalone autoshops.

D. Vendor Reputation

A vital element regulating the entire darkweb marketplace ecosystem, is trust. Vendors' reputation, has a great impact on their financial success, since it is the primary contributing factor towards building the trust of potential buyers. The darkweb can often seem a scary place, with users feeling hesitant to go forward with purchases, or even visit certain platforms. Being scammed by darkweb marketplace vendors is quite common, when their reputation is not taken into account by buyers. By creating a safe environment, users are encouraged to trust the vendors and carry out purchases. Since trust appears to have such a great influence on every individual associated with these platforms, marketplaces have implemented certain mechanisms that aim to build that trust, and make sure it does not get compromised at any point in the future.

1) Reviews & Feedback: Similarly to legitimate online platforms, reviews and client feedback also play a leading role in shaping the reputation of a vendor. Users who have purchased from a vendor, are given the option to post a review based on their experience. This review can be on the vendor themselves, or the specific product. Furthermore, buyers are given a specific time window after the purchase (e.g. 14 days), in which they can submit their evaluation. After this time window elapses, the evaluation cannot be changed.

Due to the importance of reviews in shaping the reputation of vendors, some marketplaces have systems in place, which aim to eliminate fake review instances on their platforms, such as the *Fake Review Detector* of the *ASAP* marketplace. Lastly, evaluations can also be found on darkweb forums, contributing to shaping the opinion around a vendor through reviews and discussions between past buyers (see Section III-E).

2) Reputation Classes & Cross-Platform Reputation: Classes are one of the main mechanisms used on marketplaces to inspire trust to users. The implementation of these mechanisms, varies per marketplace but the notion remains the same: the higher the verification level of the vendor or product, the

more confidence it instills to potential buyers. Furthermore, vendors can be often individually evaluated on individual elements such as overall quality of their products, shipping, responsiveness, communication and labeled as a source of "value for money" products, all of which establish the level of trust, efficiency and ease, that comes when associating with that vendor.

The most common applications of this system, is vendor *levels/ranks* (e.g. from 1 to 3, 1 to 6, or 1 to 10), which is derived from the number of sales carried out on the marketplace. A *star* system is very similar to the "1-5" system used in clearweb online shops, which is most commonly calculated from the user reviews of the vendor, based on their experience. It can also be applied to products, based on their individual client reviews. *Statuses* are used by the *Televend* market, which provides a very detailed overview of the requirements necessary for each status to be appointed, namely vendor time of operation, positive reviews, and sales. They start with the new vendor status, then verified, established, trusted, elite, veteran, and lastly legendary status. Some other mechanisms used are *tiers* (e.g. bronze, gold, diamond), color based ranking, positive feedback percentages, and the *Finalize Early* status (see Section III-B8). One more metric that can be used, is the ratio between disputes won and disputes lost (see Section III-E3), as well as the amount of total disputes filed against them by buyers, which will be included on their profile along with their class. Having a poor ratio, or a large number of disputes, impairs the vendor's chance at reaching high reputation and finally receiving the FE badge. It also rises suspicion from the side of potential clients, regarding the vendor's practices. Furthermore, there are cases that vendors are ranked separately on different aspects of their business (see Section III-D1), and in combination with the received client feedback and dispute resolution statistics, they are assigned an average ranking, which can be in any of the forms mentioned above. Reviews can also serve as a graphical representation of clients' feedback on a specific product, with the *Cartel Marketplace* as an example, which uses a bar filled with green, yellow, and red blocks, underneath the product, to illustrate the positive, average, and negative reviews, respectively.

Some marketplaces allow for the activity of the vendor in other marketplaces to be included in the calculation of their ranking, after the vendor proves their identity. Vendors can maintain the same username across platforms, if they provide the proof required (e.g. PGP key), which aims to help them preserve the reputation that has already been built around that username, their clientele, as well as make them more attractive to new buyers. This translates into vendor information that can serve as criteria to assign them a ranking, being available across different platforms. This led to another ranking mechanism, the marketplace verification levels. These levels are assigned according to how many marketplaces can vouch for the specific vendor. For example, if a vendor is already high ranked in three marketplaces, a new fourth marketplace can assign them the verification level "3" when they join the platform, and they will be awarded the "verified" badge, if their status reaches a high verification level. The contribution of vendor information taken from marketplaces that were seized by LEAs at some point in time, in most cases, was found to persist and still be counted towards the vendors' verification levels after the marketplaces' takedown. It should be mentioned that the exact formula that is used to assign trust levels to vendors, namely which specific vendor characteristic's and performance statistics are taken into account, as well as their individual impact, are often left undisclosed by marketplaces for security reasons (e.g. *AlphaBay Marketplace*).

Lastly, it should also be mentioned that gaining a high verification level on a marketplace, also affects the position of a vendor's listing in the search results, in the corresponding product category. This raises the probability of users purchasing the product, which drives the vendor's sales up, contributing towards their verification level going even higher, and placing their listings high on that product category yet again, creating a cycle.

3) Harm Reduction: With the *White House Market* and the *Dark0de Reborn Market* as the first to implement it, the *Harm Reduction* initiative aims to mitigate the dangers that can occur from drug impurity. According to this mechanism, vendors can include a testing kit in their listings, which then the buyer can use to test the product they received and evaluate its quality. They can then submit the test results on the marketplace through a dedicated form, along with a review of the tested product signed with their PGP key, and a photo showing the product, the results, the vendor name and the date. They can also post this information on the *Dread* forums sections */d/HarmReduction* and */d/Reviews*, as well as on the sections dedicated to each marketplace, namely */d/WhiteHouseMarket* and */d/Dark0deReborn*. Posting a test result, will earn the reviewer a *Quality Tester Badge*, and doing so regularly, will lead to earning perks, such as gift cards that can be used for purchases on the marketplace.

From the side of the sellers, vendors who receive 1 positive test result for their product, will earn the *Product Tested* badge on the product page. Receiving 3 positive test results, will lead to the vendor being awarded the *Quality Vendor* badge, which is shown on the vendor profile, while earning positive test results systematically will give the opportunity to the vendor to apply for a reduced commission fee from the marketplace. Lastly, harm reduction listings will gain priority over normal ones in the *Featured* listing feed of the marketplace.

The harm reduction mechanism, apart from more safety for the buyers, also leads to more profit, for both the vendors and the marketplaces. Vendors offering high quality products on these marketplaces will lead to more and more people trusting them and their products. This trust will then lead to customers being more encouraged to choose these vendors over others, leading to more purchases on the marketplaces that host them. Consequently, the marketplaces' profits will also increase, since more purchases carried out through the platform translates into more commission fees.

E. Support, Disputes & Community

Mechanisms that are meant to handle any arising issues, regarding purchases from the marketplaces, have great impact on how successful, profitable and popular a marketplace will eventually become. Knowing that there will be assistance from the platform when needed, creates the feeling of safety to the buyers, making them more inclined to use it, constantly growing the marketplace's client base.

1) Support Staff: The majority of marketplaces, make sure to have dedicated support staff in place, that will assist users deal with any challenges they might face. This is quite often stated clearly on each platform, or even advertised, since it plays such a important role in its smooth operation. Users are able to create support tickets, explaining the challenge they are facing, which will be addressed by the support staff. In some cases there will be an automated support bot, which will initially try to resolve the situation, and if that fails, the user will be redirected to a staff member. Furthermore, the staff is usually composed of individuals speaking different languages, and are available in a variety of time zones, in an effort to accommodate for the different geolocations that the clients might be located in, and provide 24/7 assistance.

2) FAQ Sections: Since darkweb marketplaces implement so many mechanisms and are composed of so many different elements which regulate their operation, they deploy FAQ sections which aim to assist users use the platform, as well as inform them of the rules they need to follow. Depending on the marketplace, FAQs can provide information regarding the rules regulating purchases, selling, payments, and any other basic piece of information needed from buyers and vendors to use the platform, including guides on some of the implemented mechanisms, such as PGP and 2FA.

3) Disputes: In the case of a buyer not being satisfied with the way their purchase was handled by a vendor, they can create a dispute. In a situation like this, the buyer will create a ticket explaining what has gone wrong with their order from a vendor, and the support staff of the marketplace will try to handle it [4]. A dispute will usually be created due to issues related to shipping, such as longer delivery times than expected/no delivery, in combination with the vendor being unresponsive. It can also be related to the state of the delivered product, such as receiving a different product than advertised, a damaged product, or a lesser amount of the product than paid for, and it can only be created for a specific time period, which in most cases is a few days before the auto-finalize is executed. In general, most marketplaces propose users should initially try to solve all issues they might run into, by contacting the vendor directly. If that fails (e.g. unresponsive vendor), they are then encouraged to submit a ticket, creating the dispute, and getting the support staff involved to resolve the situation. This process does not apply to purchases from FE vendors, since the order is considered completed the moment the payment is completed, meaning that the buyer forfeits the right to dispute. Marketplaces strive towards their users not creating disputes lightly, so they explicitly warn them that if they end up losing a dispute, they will receive negative feedback/rating from the marketplace administrators.

As mentioned in section III-D2, dispute resolutions can greatly impact the reputation of a vendor. The lost/won ratio of a vendor's disputes, as well as the number of total disputes filed against them, are all taken into consideration by marketplaces in the process of rank appointment, making the dispute mechanism very effective in the marketplace's effort to keep vendors' operation in check.

4) Forums: Forums' importance in the darkweb is vital. They are a place of discussion on various topics, with one of them being marketplaces. Potential buyers can easily browse through these discussions between former buyers that evaluate, promote, criticize vendors, and report scammers, helping newcomers to assess the risks when choosing to buy from a vendor. In addition, they include guides on some of the more technical aspects of using the darkweb, such as PGP encryption, cryptocurrency payments and 2FA. Forums are also used by vendors to advertise their services, by clients looking for a specific product/service, as well as by marketplaces promoting their platform, and making various public announcements. Specifically, marketplaces can choose to have an individual integrated forum, or use *Dread*, with a section dedicated to their platform. An example is *DarkFox Market*, which uses a dedicated section of *Dread*, called */d/DarkFoxMarket*, for posts related to the marketplace.

5) Communication: Communication between vendors and buyers, is to be carried out through the platform itself, for which marketplaces will mostly utilize the PGP protocol. Vendors are specifically forbidden from listing any other means of contact in their product listings or profiles, such as *Jabber/Extensible Messaging and Presence Protocol (XMPP)* or *Wickr*, in combination with the marketplace's policy of not conducting sales off-marketplace. There are cases that the marketplace itself will provide an alternative communication mechanism, which is very often a *Jabber/XMPP* server in combination with *OMEMO Multi-End Message and Object Encryption (OMEMO)*, *PGP* or *Off-The-Record (OTR)* encryption, dedicated to fulfilling the platform's needs.

Despite the fact that the properties of vendor shops are a subset of the ones found on marketplaces, the means of communication used differed between the two types of platforms. In more detail, vendor shop owners, apart from on-site contact forms, were found to also include messaging applications such as *Telegram* and *Wickr*, or preferred communication via encrypted email services such as *Mail2Tor* or *ProtonMail*.

F. Marketplace Revenue

In this section we document four main sources of income for marketplaces: *purchase commissions, the vendor status, withdrawals*, and *listing promotions*. In addition to these sources, some marketplaces will also deploy certain mechanisms which aim to keep the users engaged and motivated to keep using

[4]The *AlphaBay* marketplace, has successfully managed to automate the dispute solving procedure, by creating the *Automatic Dispute Resolver (ADR)*.

the platform, while in some cases also receiving commissions from their usage by clients (see Appendix B).

1) Purchase Commissions: The role that marketplaces play in the darkweb trading ecosystem, is serving as a platform where vendors can list their products, and buyers can easily browse through and carry out purchases. The owners of these platforms do not actually sell any products, so their profits and economic incentives to run a marketplace are not sales. A basic source of income is commissions. Marketplaces will require a fee from vendors (in some cases from buyers as well), which is a percentage of the total amount paid for the purchase. In most cases, commissions range from 3% to 6%, but with some caveat. Varying per platform, commissions are either a standard fixed amount, or fluctuate depending on the price paid, the amount of product purchased, whether the purchase was carried out using the escrow or multisignature escrow mechanism (*DarkFox charges a 5% fee for normal escrow and 4% for multisignature escrow*), as well as depending on the rank of the vendor (e.g. lower vendor rank, translates into a higher commission paid to the marketplace).

2) Vendor Status: Another source of income for darkweb marketplaces, is granting the vendor status. Individuals interested in becoming vendors, have the option to upgrade their accounts by paying a fee, the vendor bond. This fee varies per marketplace, and it mainly lies between $100 and $500, but can exceed that depending on the level of prestige and reputation of each marketplace, even reaching the $1500 margin in the case of the *World Market*. Depending on the marketplace, the vendor bond can also be refundable. In addition, some platforms also require proof of product in order to provide the status, or even that the total value of the available products, amount to or surpass a specific price margin (e.g. *Hydra* marketplace will only grant the status if the cost of all goods is over $400). However, some marketplaces do not require a fee to provide the status, as long as the individual in question can provide proof of past experience as a vendor on other platforms. Lastly, *Hydra* does not follow the vendor bond scheme, and instead of a fixed fee, it requires a monthly subscription or "rent" from the vendors. The price for this rent begins at $400 per month, but can drop down to $125, if the vendor chooses to opt for a 12-month prepayment.

3) Withdrawals: Some marketplaces also require withdrawal fees, which are applied every time a user wants to make a withdrawal from their on-site wallet balance (see Section III-B3). This fee can be a fixed amount, like in the case of *World Market*, which applies a flat 0.0003 BTC rate ($\approx$ $14 in August 2021), or a percentage of the amount withdrawn, with the *Dark0de Reborn* marketplace as an example, which applies a fixed 2.5% rate. In some cases it can also be a combination, where a flat rate would apply up until a specific amount, and then a percentage rate is applied from that point onward. An example is the *Liberty* marketplace, which applies a flat $1 rate for purchases up to $100, and then a percentage rate of 1%, for every transaction over that $100 margin. Some marketplaces will also have a limit set, regarding the minimum amount that users can withdraw, and the minimum they can deposit. An example is the *DarkFox Market* which has a 0.00005 BTC ($\approx$ $2.3 in August 2021) minimum limit for deposits, and a 0.0005 BTC ($\approx$ $23 in August 2021) minimum limit for withdrawals.

4) Listing Promotion: An additional source of income for these platforms, is the fee paid by vendors to promote their products, as discussed in section III-B1. Most marketplaces will assign a specific number of listing spots, which will be positioned higher than any other listing, on the homepage of the marketplace. These listings are usually called *Featured Listings*, and are more likely to get higher traction by clients, since these products are the first that a visiting user will see. Vendors can bid for these slots, and if they win the auction, they are then able to use the listing slot for a certain time period. In the case of the *AlphaBay* marketplace, this time period is two weeks, and the slots available every week are eight. The auction for the next listing slots also lasts two weeks, until the expiration of the previously auctioned slots. In the case of *White House Market*, the winning bid for a featured listing slot has been known to range from $2000, up to $3000 per month.

A similar mechanism implemented by marketplaces to promote certain listings is *Sticky Listings*. In this case, vendors can pay a fixed fee, in order for their product to get priority over others in the search results of certain product category, for a certain time period. One example is the *White House Market* which charges $300 per week, for each sticky listing. In addition, some marketplaces will provide free sticky listings to some new vendors randomly, to help them kick start their business.

IV. Related Work

Darkweb marketplaces, have been targeted by researchers with various approaches, all aiming at gaining a deeper understanding of the darkweb trading ecosystem.

Nunes et al. [14], with the purpose of acquiring cyber threat intelligence, developed a system which would harvest information from the deepweb and darkweb. This system consisted of a crawler, a parser and a classifier, and it was used to gather data from 17 marketplaces, as well as 21 forums. They also illustrate two case studies, one on the discovery of zero-day exploits sales on the marketplaces, and one on the presence of vendors in both forums and marketplaces, using the data acquired from both types of platforms. *Nicolas Christin* [32], carried out a measurement analysis on the Silk Road marketplace, over a period of 8 months in 2011-2012, before its shutdown took place. Using daily crawls, an effort which spanned 6 months in 2012, he gained insight on the marketplace's operation, presenting data on elements of the marketplace such as products, sales, vendors, and customer feedback. Additionally, he discusses the role and importance of BTC, in the marketplace's operation. Building upon this work, *Soska* and *Christin* [13], study the growth of underground marketplaces from 2013, when the Silk Road marketplace was taken down, until 2015. They collected data from 16 marketplaces, which contributed towards understanding how the underground marketplace ecosystem operates, from the

types of products available and their evolution, to vendor presence throughout the darkweb, as well as security mechanism deployment, such as PGP.

All three of these efforts, try to unveil the darkweb marketplace infrastructure, but take a more quantitative approach compared to our work, with crawling and its resulting dataset, being the main point of focus. *Thomas S. Hyslip* [12], takes an approach more similar to ours, and illustrates the framework that surrounds the trading of digital services and products on marketplaces, while we explore the broader spectrum of products and features. *Kermitsis et al.* [33], also touch upon the characteristics and properties of darkweb markets. Conversely, our work is mainly founded on real-life applied information, such as advice and guides from popular vendors, as well as user experiences narrated on forums. We also focus more on in-depth insight on the individual properties and practices of these platforms, as well as the reputation element, which is arguably a vital factor of this framework's successful operation, creating trust between vendors, buyers and marketplaces. Lastly, there has also been research targeting specific product types, such as drugs [28], [34], [35], firearms [29], [30], [36], as well as COVID-19 vaccines and proofs of vaccination [2], [15], contributing towards investigating the different characteristics associated with each type of illegal trading.

Apart from the darkweb illegal trading framework, clearweb marketplaces and forums have also been targeted by researchers, with the same goals in mind. Despite the fact that these platforms operate in the clearweb, the methods implemented also apply to darkweb platforms due to the similarities of the two markets (e.g. trust, reputation, anonymity).

Pastrana et al. [37], developed the *CrimeBot* crawler, which was utilized to scrape underground forums, in an effort to better understand the behavior of individuals involved in cybercrime, as well as the ways that potential cyber criminals are incentivized to enter the cybercrime world. The data was harvested in a period of over 9 months, and was used to create the *CrimeBB* database. This database includes more than 48m posts, from 1m accounts of 4 forums (2018), with some posts dating back to 2005. Lastly, they present a case study on the evolution of currency exchanges, to illustrate the dataset's potential. *Hutchings* and *Holt* [38], investigate the infrastructure of the stolen data markets, through crime script analysis. Using qualitative methods, they examine the content of 1,889 communication instances between sellers and buyers, from 13 forums that operate as selling points for stolen data. *Holt* and *Lampke* [39], also work in the same direction, employing qualitative procedures to analyze 300 threads from six forums dealing in stolen data. *Holt et al.* also focuses on the element of trust, in the context of stolen data markets. The importance of the role that trust and reputation play in the illegal trading world, both in the darkweb and clearweb, is crucial, making research towards this topic of great value. Last but not least, *Vu et al.* [40] use the *CrimeBB* [37] dataset, containing 190,000 user contracts, created from June 2018 to June 2020, from one of the most popular forums *Hack Forums*, to perform an longitudinal analysis of the platform's operation. They illustrate how the forum's operation has evolved over this two-year span, from an economic, social and reputation/trust standpoint, split into the three distinct time periods, namely the period the contract was adopted (set-up era), the stable operation era, and finally the COVID-19 era.

V. Conclusion

Illegal trading on the darkweb owes its success to a combination of properties. Marketplaces deploy mechanisms that aim to provide ease of use, security, obfuscation, resilience against hostile actions, along with systems that help create an inviting and seemingly safe environment for consumers. Furthermore, these platforms have various methods of generating revenue, which in many cases are also in favor of the vendors' self interests, a fact contributing to their constant success. In this article we document these mechanisms, and investigate their role in the trading ecosystem. Systematically exploring marketplaces, vendor shops, and forums, provides insight on the factors that are contributing the most in shaping the state of the market. We argue that trust plays a vital role in that regard. The reputation that surrounds each vendor, is directly related to the number of clients that are going to decide to purchase their products. Higher reputation translates into more sales, which creates more revenue for the marketplaces hosting the vendors, through purchase commission fees. Taking the trust variable out of the equation, is bound to greatly impact the vendors' profit generation, with cyber attack related products and services as the main focal point. We believe that reputation is one of the foundations of darkweb trading, and hope that this work will inspire more research towards this topic.

References

[1] V. James King. Here's a breakdown of the $1.2 billion in silk road drug transactions. [Online]. Available: https://www.businessinsider.com/heres-a-breakdown-of-the-12-billion-silk-road-drug-transactions-2015-5?r=US&IR=T

[2] D. Georgoulias, J. M. Pedersen, M. Falch, and E. Vasilomanolakis, "Covid-19 vaccination certificates in the darkweb," 2021.

[3] Insights. Geographic distinctions in darknet market activity: U.s. and western europe have the most vendors, eastern europe and china lead in money laundering. [Online]. Available: https://blog.chainalysis.com/reports/darknet-markets-2021-geographic-breakdown

[4] J. Martin and N. Christin, "Ethics in cryptomarket research," *International Journal of Drug Policy*, vol. 35, pp. 84–91, 2016.

[5] J. Martin, *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. Springer, 2014.

[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] D. Décary-Hétu and J. Aldridge, "Sifting through the net: Monitoring of online offenders by researchers," *European Review of Organised Crime*, vol. 2, no. 2, pp. 122–141, 2015.

[8] M. J. Barratt, S. Lenton, and M. Allen, "Internet content regulation, public drug websites and the growth in hidden internet services," *Drugs: education, prevention and policy*, vol. 20, no. 3, pp. 195–202, 2013.

[9] J. Buxton and T. Bingham, "The rise and challenge of dark net drug markets," *Policy brief*, vol. 7, pp. 1–24, 2015.

[10] B. Collier, D. R. Thomas, R. Clayton, and A. Hutchings, "Booting the booters: Evaluating the effects of police interventions in the market for denial-of-service attacks," in *Proceedings of the internet measurement conference*, 2019, pp. 50–64.

[11] N. Moretto. Two-factor authentication with totp. [Online]. Available: https://medium.com/@nicola88/two-factor-authentication-with-totp-ccc5f828b6df
[12] T. S. Hyslip, "Cybercrime-as-a-service operations," *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 815–846, 2020.
[13] K. Soska and N. Christin, "Measuring the longitudinal evolution of the online anonymous marketplace ecosystem," in *24th USENIX security symposium (USENIX security 15)*, 2015, pp. 33–48.
[14] E. Nunes, A. Diab, A. Gunn, E. Marin, V. Mishra, V. Paliath, J. Robertson, J. Shakarian, A. Thart, and P. Shakarian, "Darknet and deepnet mining for proactive cybersecurity threat intelligence," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*. IEEE, 2016, pp. 7–12.
[15] A. Bracci, M. Nadini, M. Aliapoulios, I. Gray, D. McCoy, A. Teytelboym, A. Gallo, and A. Baronchelli, "Dark web marketplaces and covid-19: The vaccines," *Available at SSRN 3783216*, 2021.
[16] Monero. (2021) Fungibility. [Online]. Available: https://www.getmonero.org/resources/moneropedia/fungibility.html
[17] M. Pechman. (2021) What are bitcoin mixers, and why do exchanges ban them? [Online]. Available: https://cointelegraph.com/news/what-are-bitcoin-mixers-and-why-do-exchanges-ban-them
[18] I. Allison. (2021) Bitcoin tumbler: The business of covering tracks in the world of cryptocurrency laundering. [Online]. Available: https://www.ibtimes.co.uk/bitcoin-tumbler-business-covering-tracks-world-cryptocurrency-laundering-1487480
[19] Monero. (2017) The merits of monero: Why monero vs bitcoin. [Online]. Available: https://www.monero.how/why-monero-vs-bitcoin
[20] Z. Albeniz. (2019) A europol officer confessed that they could not track monero (xmr) transactions. [Online]. Available: https://medium.com/@ziyahanalbeniz/a-europol-officer-confessed-that-they-could-not-track-monero-xmr-transactions-dbd568f02922
[21] F. Harris. Qiwi wallet: An e-wallet payment method! [Online]. Available: https://cryptomojo.com/qiwi-wallet/
[22] A. M. Antonopoulos. Bitcoin q&a: How do i secure my bitcoin? [Online]. Available: https://www.youtube.com/watch?v=vt-zXEsJ61U&t=0s&ab_channel=aantonop
[23] L. Sun. (2020) Blockchain explained: Custodial vs non-custodial wallets. [Online]. Available: https://medium.com/mogulproductions/blockchain-explained-custodial-vs-non-custodial-wallets-76e6128834b0
[24] J. Redman. Sources say world's largest darknet empire market exit scammed, $30 million in bitcoin stolen. [Online]. Available: https://news.bitcoin.com/sources-say-worlds-largest-darknet-empire-market-exit-scammed-30-million-in-bitcoin-stolen/
[25] J. Aldridge and R. Askew, "Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement," *International Journal of Drug Policy*, vol. 41, pp. 101–109, 2017.
[26] N. Vorobyov. (2020) A new breed of drug dealer has turned buying drugs into a treasure hunt. [Online]. Available: https://www.vice.com/en/article/g5x3zj/hydra-russia-drug-cartel-dark-web
[27] D. W. Link. (2020) How to sell drugs on darknet using dead drops. [Online]. Available: https://darkweblink.com/sell-drugs-online-dead-drops/#How-To-Format-Dead-Drop-Location
[28] D. Rhumorbarbe, L. Staehli, J. Broséus, Q. Rossy, and P. Esseiva, "Buying drugs on a darknet market: A better deal? studying the online illicit drug market through the analysis of digital, physical and chemical data," *Forensic science international*, vol. 267, pp. 173–182, 2016.
[29] R. Broadhurst, J. Foye, C. Jiang, and M. Ball, "Illicit firearms and other weapons on darknet markets," *Trends and Issues in Crime and Criminal Justice [electronic resource]*, no. 622, pp. 1–20, 2021.
[30] C. Copeland, M. Wallin, and T. J. Holt, "Assessing the practices and products of darkweb firearm vendors," *Deviant Behavior*, vol. 41, no. 8, pp. 949–968, 2020.
[31] A. Guirakhoo. (2019) Understanding the different cybercriminal platforms: Avcs, marketplaces, and forums. [Online]. Available: https://www.digitalshadows.com/blog-and-research/understanding-the-different-cybercriminal-platforms-avcs-marketplaces-and-forums/
[32] N. Christin, "Traveling the silk road: A measurement analysis of a large anonymous online marketplace," in *Proceedings of the 22nd international conference on World Wide Web*, 2013, pp. 213–224.
[33] E. Kermitsis, D. Kavallieros, D. Myttas, E. Lissaris, and G. Giataganas, "Dark web markets," in *Dark Web Investigation*. Springer, 2021, pp. 85–118.
[34] J. Martin, R. Munksgaard, R. Coomber, J. Demant, and M. J. Barratt, "Selling drugs on darkweb cryptomarkets: differentiated pathways, risks and rewards," *The British Journal of Criminology*, vol. 60, no. 3, pp. 559–578, 2020.
[35] 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.
[36] G. P. Paoli, J. Aldridge, R. Nathan, and R. Warnes, "Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web," 2017.
[37] S. Pastrana, D. R. Thomas, A. Hutchings, and R. Clayton, "Crimebb: Enabling cybercrime research on underground forums at scale," in *Proceedings of the 2018 World Wide Web Conference*, 2018, pp. 1845–1854.
[38] A. Hutchings and T. J. Holt, "A crime script analysis of the online stolen data market," *British Journal of Criminology*, vol. 55, no. 3, pp. 596–614, 2015.
[39] T. J. Holt and E. Lampke, "Exploring stolen data markets online: products and market forces," *Criminal Justice Studies*, vol. 23, no. 1, pp. 33–50, 2010.
[40] A. V. Vu, J. Hughes, I. Pete, B. Collier, Y. T. Chua, I. Shumailov, and A. Hutchings, "Turning up the dial: the evolution of a cybercrime market through set-up, stable, and covid-19 eras," in *Proceedings of the ACM Internet Measurement Conference*, 2020, pp. 551–566.

APPENDIX

A. Forum Discussion on Delivery Methods

In this appendix we present some discussions found on the *Dread* forum, regarding the usage of PO boxes.

"Your name/address is public information, anyone can order something to your house under your name. Your PO box is private as hell. Just one reason I'd prefer a mailbox." - Dread forum user

"A lot of vendors will refuse to ship to PO boxes for good reason. If your parcel is sitting at an office stinking of drugs its probably not a good thing. Not to mention a PO box is directly linked to you, where as your address as dumb as this sounds you have deniability as anyone can send anyone a parcel, there is nothing stopping me posting my neighbor a brick of coke however if i was to ship it to their private PO box and it gets found you are going to need a really good lawyer to get out of that one." - Dread forum user

B. Marketplace Specific Features

Appendix B is dedicated to illustrating features that have been implemented by marketplaces, with the purpose of keeping the users engaged and entertained, while also serving as an additional source of income for the platform owners.

a) Deadpool: This mechanism is deployed by the *Archetyp* marketplace and is in essence a betting function. Users can vote on whether each one of the currently active marketplaces, is going to exit scam, retire, or get taken down by law enforcement. The total amount of bets placed is gathered into a pot, which the users with the correct votes win.

b) Lottery: Cartel Marketplace has implemented a weekly lottery feature. Users can buy tickets for $1 each, and will be given a unique code at the moment of purchase. At the end of the week a random winning ticket is chosen, and the

entire lottery pool is credited to the winner's account balance, after a 10% fee is deducted by the marketplace. To reassure the users that the process is fair, there is an additional mechanism in place, which aims to provide transparency. A random seed is published at the start of each week, which along with the winner's information, winning ticket code and seed, are added onto a blockchain, available for download by all users.

c) Roulette: The roulette function from the *Hydra* market, as they explicitly mention on their platform, is intended to "to popularize the HYDRA platform, to attract customers, an increase in the number of orders from stores". It is implemented as a payment method, where instead of paying directly for the full price of the product, users have the option to take a gamble. They can buy chips which cost around 1% of the product's price, plus a small added percentage as commission for the marketplace. Each of these chips correspond to 1% of winning probability, so the more chips they buy, the higher the probability to win. They then place the chips on the number they wish from 1-100, and the game starts. There is only 1 winning number chosen each time, which is the integer part of a decimal number with 16 decimal digits, and if it is one of the numbers chosen by the user, they win. In this case the product is automatically bought for the user. Additionally, in the begging of the lottery, the winning number in its decimal form along with the identifying number of the current lottery, are both hashed and given to the user in order for them to authenticate the result of the lottery.

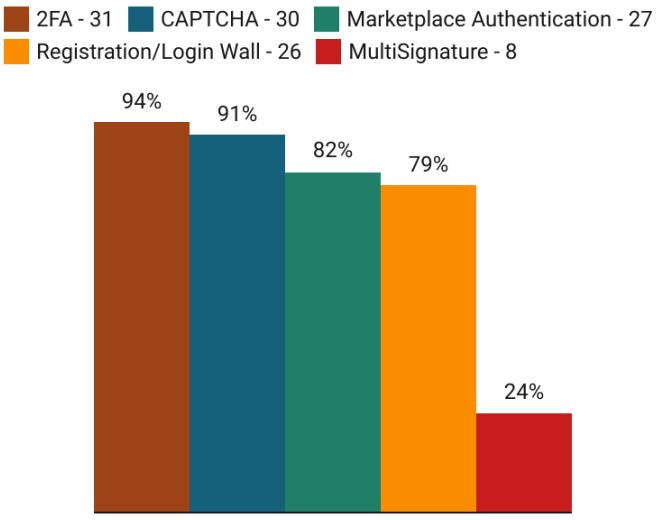

Fig. 3. Mechanism implementation on the 33 marketplaces in percentages. The legend presents the total number of marketplaces that implement each mechanism.

C. Mechanism Implementation per Marketplace

In this section we present statistics on the usage of user 2FA, CAPTCHA, and marketplace authentication mechanisms, multisignature payment scheme availability, as well as whether these platforms utilize a registration/login "wall" that the users need to bypass before reaching the listing section. It should be specified that this data presented on Figure 3 was collected in a subsequent phase of writing this paper, which in combination with the dynamic availability of darkweb marketplaces and their short life span, led to only 33 of the initial 41 being fully operational. Many of these marketplaces are still very likely to come online in the future, so we also refrain from providing their names to avoid directing traffic towards them, as discussed in section II-A.

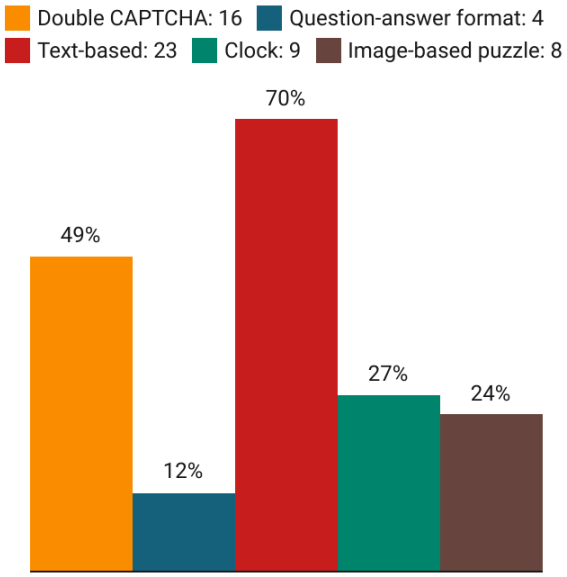

Fig. 4. CAPTCHA type usage on the 33 marketplaces in percentages. The legend presents the total number of marketplaces that implement each CAPTCHA type.

D. CAPTCHA Types

Lastly, this section is dedicated to the various CAPTCHA types that we discovered while exploring the 41 marketplaces. In common with the information provided in the previous section, the data showcased in this section are collected from 33 out of the total 41 platforms. We documented 4 different families of CAPTCHA mechanisms, namely text-based, mechanisms containing image-based puzzles, question and answer format (e.g. mathematical equation solving), and implementation of the clock CAPTCHA illustrated on Figure 1 (see Section III-A2).