International Journal of Cybersecurity Intelligence & Cybercrime

Volume 3 | Issue 1 Article 2

2-28-2020

# Illegal Gambling and Its Operation via the Darknet and Bitcoin: An Application of Routine Activity Theory



## Recommended Citation

Choi, S., Choi, K. Sungu-Eryilmaz, Y., & Park H. (2020). Illegal gambling and its operation via the Darknet and Bitcoin: An application of routine activity theory. International Journal of Cybersecurity Intelligence and Cybercrime, 3(1), 3-23.

Choi. S., Choi. K., Sungu-Eryilmaz, Y & Park. H.(2020). *International Journal of Cybersecurity Intelligence and Cybercrime, 3* (1), 3-23.

# Illegal Gambling and Its Operation via the Darknet and Bitcoin: An Application of Routine Activity Theory

Sinyong Choi, University of Nevada, Las Vegas, Nevada, Nevada, U.S.A

Kyung-Shick Choi, Bridgewater State University, Massachusetts, U.S.A & Boston University, Massachusetts, U.S.A

Yesim Sungu-Eryilmaz, Boston University, Massachusetts, U.S.A

Hee-Kyung Park*, Seoul National University, Seoul, South Korea

*Keywords; bitcoin, Darknet, cybercrime, online gambling, Tor.*

**Abstract:**

The Darknet and Bitcoins have been widely utilized by those who wish to anonymously perform illegal activities in cyberspace. Restricted in many countries, gambling websites utilize Bitcoin payments that allow users to freely engage in illegal gambling activities with the absence of a formal capable guardian. Despite the urgency and limited knowledge available to law enforcement regarding this issue, few empirical studies have focused on illegal gambling websites. The current study attempts to examine the characteristics and operations of online gambling websites on both the Darknet and Surface Web, which allow Bitcoin payments. The findings suggest that both websites on the Surface Web and Darknet have similar and distinctive features that attract and encourage online users to engage in extensive illegal gambling activities and potentially other illegal activities as well. The study concludes with policy recommendations to remedy the issue of online gambling.

## Introduction

Over the past five years, the online gambling industry has been growing at a substantial rate due to the advancement of technology, including the rapid spread of smartphone devices and wireless Internet devices, which allows for more accessibility to the Internet. This allows for the online gambling industry to be highly accessible while providing gamblers the privacy and convenience they want.

According to Grand View Research (2019), the global online gambling market was valued at approximately 48.52 billion USD in 2018 and is estimated to reach 102.97 billion USD by 2025. With the rapid growth of the online gambling market, numerous countries have legalized online gambling because it generates jobs and capital.

*Corresponding author

Hee-Kyung Park, DDS, MSc, PhD. Department of Oral Medicine and Oral Diagnosis, School of Dentistry & Dental Research Instutite Seoul National University, #101, Daehak-ro, Jongro-Gu, Seoul, Korea, 03080

Email: dentopark@snu.ac.kr

However, many developed nations have not benefited from the enlarged online gambling market due to the strict regulation of online gambling. For example, China strictly prohibits all forms of online gambling, and online gambling is treated differently throughout the U.S. Although forty-eight states have legalized at least some form of gambling, online gambling is still illegal in most states (Homeyer, 2011). A few states, including Nevada, New Jersey, and Delaware currently offer some type of regulated online gambling game such as casino and poker (Murray, 2017). Online gambling operators who are licensed by their jurisdiction must locate their servers within the territory of the jurisdiction, and online gamblers who wish to play on those licensed gambling websites should also be physically located within state borders (Trimble, 2012). In addition, the U.S. created the Unlawful Internet Gambling Enforcement Act (UIGEA) in 2006 to prevent online gambling companies from lawfully utilizing financial transactions and payment systems, which has restricted online gambling by limiting the transaction of national currencies to organizations hosting gambling websites (Homeyer, 2011; Wang, & Antonopoulos, 2016). Under this condition, Bitcoin online gaming websites have emerged as expanding illegal online activities.

Cryptocurrency can be used to pay for things electronically, making it like a conventional euro or dollar that can now be used in various online markets. What makes cryptocurrency different is its decentralized characteristics; the cryptocurrency network is not fettered by any sole authority (Choi, 2015). Bitcoin is one of the most popular cryptocurrencies, which was first introduced in an article titled *Bitcoin: A Peer-to-Peer Electronic Cash System* by an author who did not use his real name but used the pseudonym of Satoshi Nakamoto. Bitcoin was designed to initiate a peer-to-peer electronic transaction directly without the need for any financial institution, which enables the process to be anonymous and transparent (Nakamoto, 2008).

Due to cryptocurrency transactions being unregulated, Bitcoin has been widely used in an attempt to circumvent restrictive regulations in numerous countries and aids in online gambling. Since Bitcoin has its own payment processor, there is no waiting time for bank transactions, exceedingly low transaction fees, and no currency exchanges (Pathe, 2014). In addition, Bitcoin casinos tend not to require age verification, address checks, or other personal information but minimal user information such as an email address. Furthermore, purely digital and encrypted transactions disable financial tracking and conceal the identity of gamblers, as well as gambling operators. Although online gambling is forbidden in many countries, the rapid growth and use of Bitcoin makes law enforcement investigations much more complicated due to the jurisdictional issues and variance in regulations at the international level (Pathe, 2014; Seth, 2014).

The anonymity of Bitcoin transactions easily allows criminals to engage in unlawful activities without being tracked in cyberspace. Bitcoin has been used for illicit business transactions carried out in the cyber realm, where everyone can remain anonymous via Darknet (Choi, 2014; Rudesill, Caverlee, & Sui, 2015). Prior to explaining the Darknet, the conception of the Surface Web and Deep Web must be discussed. Some people may believe that almost all information on the Internet can be identified by a Google search. Yet, there is a whole separate online realm out of the reach of any standard search engine. Surface web, also known as the Indexed web, Visible web, Indexable web, or Clearnet, is the part of the World Wide Web that can be discovered by conventional search engines such as Google, Bing, or Yahoo through standard Web browsers such as Firefox, Chrome, or Safari. However, other parts of the Web which have not been indexed and cannot be searched by conventional search engines are called 'Deep web', also called the Invisible web or Hidden web (Bergman, 2001). While it is almost impossible to estimate the size of the Deep Web, earlier research suggested that the size of the Deep Web is nearly 4000 to 5000 times larger than the Surface Web (Finklea, 2017).

Darknet is defined as a small part of the Deep web, which is unapproachable via standard web browsers. Most of the content stored on the Darknet can be discovered on the Tor (The Onion Router) network, which is an anonymous network that can be accessed via downloading the browser (Clearing Up Confusion, 2014). As Tor network allows users to browse and host a site anonymously, this is well known as the bases of criminal operators who conduct illegal activities such as drug dealings, hacking, hiring of hitmen, child pornography, identity theft, money laundering, terrorist activities, etc. (Rudesill, Caverlee, & Sui, 2015). Silk Road, a major online market used for the sale of illicit goods and services in Bitcoin, was the embodiment of illegal activity that occurs on the Darknet (Schumer Pushes to Shut Down, 2011). The Dark web has become a shelter that harbors illegal activity both in the cyber and physical realms.

Considering the rapid expansion of Bitcoin gambling sites and the nature of the Darknet, the anonymous network can significantly facilitate illegal gambling operations. While there are many studies addressing online gambling addiction issues, few studies address the issues of Bitcoin gambling sites and the Darknet.

Numerous studies have also shown that online gambling raises public concerns, including illegal operations, fraud, money laundering, or problem gambling (Banks, 2012; Fiedler, 2013; Griffiths, 2010; Trimble, 2012). It is known that most of the online gambling markets are captured by illegal operators, and play a vital role even in regulated markets (Fiedler, 2013; Trimble, 2012). Although the regulator legally obliged online gambling operators to locate their servers within their particular jurisdiction, it still faces problems with those operators who do not have a license (Trimble, 2012).

The aim of this study is to contribute to the criminology literature and to uncover 1) the difference between the Darknet- and Surface Web-Bitcoin gambling sites, 2) what main features encourage online users to engage in illegal gambling activities, 3) how illegal online gambling activities are potentially linked to engaging in other online criminal activities, and 4) how the owners of establishments promote and advertise their illegal websites while evading law enforcement detections. In addition, this study uses Routine Activity Theory (Cohen & Felson, 1979) in an attempt to understand illegal online gambling activities.

**Theoretical Framework: Routine Activity Theory**

Cohen and Felson (1979) argued that Routine Activity Theory could explain the incident of crime. They suggested that crimes can occur when a suitable target, the absence of the capable guardian, and a motivated offender come together at any place and time. In other words, a lack of any one of the three elements is suggested to decrease the likelihood of crime (Choi, 2008). The central premise of the theory is that crime is not an accidental act of a criminal manifestation, but a sophisticated and/or calculated occurrence (Choi, 2015). Yar (2005) used the concepts of the theory to delineate crimes in cyberspace. Cohen and Felson (1979) assumed that there will always be plenty of criminal motivations. It was also suggested that the existence of motivated offenders who have suitable targets is a given situational factor in cyberspace (Yar, 2005).

Griffiths's (2010) study briefly gives an overview of various scams that take place in and around Internet gambling sites and draws the conclusion that gambling fraud online is growing because most gamblers want to win a huge reward by betting a small amount of money. If there are people who are willing to take the risk to bet money on probability events (suitable targets), there will be people who will try to take their money (motivated offenders). A more recent study of this topic, conducted by Banks (2012), addresses the types and features of crimes that occur at the portals of Internet gambling sites. It found that numerous criminal organizations see online gambling as an opportunity to engage

in criminal activities such as fraud, theft, or extortion. In terms of money laundering, Fiedler (2013) identifies that online gambling can facilitate money laundering easily due to particular advantages such as virtuality of products and cash flows; cumbersome and complicated payment processing; the massive volume of gambling users on the market; and tax-free winnings in multiple involved jurisdictions. In sum, the suggested studies indicate that cybercriminals with various motivations exist in cyberspace.

According to routine activity theory, the suitability of targets for crime involves the offender's perceptions about the following characteristics of the target: (1) the value of the target; (2) the inertia of the target; (3) the visibility of the target; and (4) the accessibility of the target (Felson, & Boba, 2010). Regarding the *value* of the target, illegal gambling operators leave their platforms globally accessible to allow valuable consumers in other jurisdictions place a bet on their sites. The *visibility* of the target includes advertising illegal gambling sites on various online platforms where a lot of potential consumers convene (e.g., social media, online forum, and blog). As to the *accessibility* of the target, the borderless nature of the Internet and a global business environment enables illegal online gambling operators to reach their consumers globally at a minimal cost (Trimble, 2012). Regarding the *inertia* of the target, illegal gambling websites locate their assets and servers outside the territorial jurisdiction of law enforcement agencies to evade investigation. In fact, these sites make it difficult to track them by hiding their servers and identity with various schemes in cyberspace, such as proxy sites, domain proxy services, web hosting companies, or multiple relay servers placed in different jurisdictions (Choi, 2015). While there are federal laws like the Unlawful Internet Gambling Enforcement Act of 2006 that prohibit money transfers to offshore sportsbooks, a variety of deposit and payment processes can be employed to evade detection. Alternative payment options (e.g., cryptocurrencies) are also available that enable anonymous transactions and make international transactions easier (Gainsbury & Blaszczynski, 2017; Millar, 2018).

Furthermore, many studies have reported that problem gambling is more related to online gambling than offline gambling (Canale et al., 2016; Gainsbury et al., 2015; Harris, Mazmanian, & Jamieson, 2013; McCormack & Griffiths, 2013; Wood, & Williams, 2007). This tendency could be due to the particular characteristics of online gambling, such as electronic payments, constant availability, and the anonymity of play (Gainsbury et al., 2015).

A study conducted by McCormack and Griffiths (2013) explored the situational and structural characteristics of online and offline gambling. They found that online gambling has unique structural and situational features, some of which may facilitate problematic gambling behavior such as accessibility, affordability, convenience, and immersion. Brosowski and colleagues (2012) examined the behavior of gamblers who use multiple types of online gambling within one provider. It was found that online gambling sites provide multiple gambling products, which enticed online gamblers to use multiple types of games with ease and also found the link between multiple gambling engagements and problem gambling. In addition, Hing and colleagues (2014) found that advertising and promoting online gambling had an impact on increasing gambling among a subgroup of gamblers.

Regarding capable guardianship, it can fall into two main categories: formal social control and informal social control (Cohen, Kluegel, and Land, 1981). In cyberspace, law enforcement agencies should act as formal social control agent to prevent cybercrime from occurring, however many agencies still lack the ability to effectively investigate cybercrimes (Choi, 2015) and are struggling to keep pace with criminals' evolving technologies (Banks, 2012). In addition, the sophistication level and tools used by cyber-criminals make it difficult for law enforcement agencies to apprehend and prosecute offenders (Choi, 2015).

The most popular currency embraced in all Tor hidden-service transaction is Bitcoin (Moore, & Rid, 2016). Silk Road, which offered the platform to cyber vendors and buyers to carry out the cyber transaction of over 24,400 illegal goods for sale, employed Bitcoin to conduct all transactions (Christin, 2013). In fact, many illegal activities have been associated with the Darknet. Moore and Rid (2016) examined over 5000 onion domains and found that the most common usages for websites on the Tor Hidden Service are criminal and illegal activities. Criminals may be attracted to the Tor architecture as it allows anybody to browse anonymously and create an untraceable webserver hosted on the Tor network with ease (Moore & Rid, 2016). In addition, while Tor recognizes the prevalence of criminal websites on their network, it allows them to use their services by arguing that restricting Tor would not stop criminals from doing their illicit activities because they already have many options available that offer privacy other than what Tor provides (Doesn't Tor enable criminals, n.d.).

The Darknet has become a safe haven that conceals illegal activity both in virtual and physical spaces. Yet, in spite of the volume of criminal activities on the Darknet, it has received only superficial attention from researchers interested in studying Internet gambling. To the best of our knowledge, there are few datasets that explores the gambling activities on Darknet web pages.

In addition, similar to formal social control, informal social control guardians ranging from private network administrators to ordinary online citizens are not actively operative in cyberspace (Choi, 2015). In fact, according to Gainsbury and colleagues (2015), although social media platforms have been a popular venue for people to access online gambling sites through hyperlinks embedded in advertisements, there were very few regulations restricting online gambling organizations from promoting their sites on social media.

Deans and colleagues (2016) suggested that young men aged 18 to 35 are the main target market for the gambling industry, and the majority of young gamblers participate using mobile gambling apps or online platforms, amplifying the risks associated with compulsive gambling. Although Dean and colleagues' (2016) study implies the importance of informal social control agents, such as parents, teachers, or friends, in surveilling young gambler's online activities, "the ease of offender mobility and the temporal irregularity of cyber-spatial activities" (Yar, 2005, p. 423) hinder informal guardians from maintaining effective guardianship (Choi & Lee, 2017). To date, few public awareness strategies and effective social policies have been initiated to prevent compulsive online gambling.

According to Cohen and Felson (1979), an absence of any one of the three components would lead to the deterrence of crime. However, the component of capable guardianship plays a pivotal role because it is the only component that would increase the possibility of a crime occurring in a given space (Cohen & Felson, 1979). This assertion suggests that an approach to developing effective preventive measures against illegal online gambling activities should focus on the diagnosis of intervention from a capable guardianship perspective.

The current study seeks to understand the following points: (1) What factors of gambling sites on the Darknet are different from Bitcoin Gambling sites on the Surface Web; (2) what are the main factors for online gamblers to bet on online gambling sites; (3) how do Bitcoin gambling sites on both Webs employ alternative strategies to promote their site while evading law enforcement; and (4) what factors of gambling sites potentially lead to other illegal activities.

## Methodology

Since only a few studies have focused on empirical reviews of Bitcoin and the Darknet regarding online gambling, this study scrutinizes different types of gambling sites and compares each site ac-

cording to the different features of gambling sites on the Darknet versus the Surface Web. Data were collected from May to August 2017, and coding and analysis were conducted in September 2017. Utilizing IBM SPSS software, we conducted multiple regression analyses to delineate the pattern of online gambling operations as well as to determine the main factors that encourage online gamblers to place a bet on the gambling sites.

**Sample and Procedure**

One of the biggest challenges to conducting an empirical analysis of Internet sites is determining the true size of the population from which to obtain a representative sample. The Internet is in constant flux; its size, dimensions, and composition are changing constantly as websites appear, disappear, move, and change. Although search engines such as Google index the contents of a part of the Internet, no comprehensive directory of websites exists. Therefore, it is difficult to establish the true size of the population of websites. Without the true population, it is impossible to use representative sampling techniques in social science research. Thus, research using websites as the unit of analysis often rely on a less accurate purposive sampling technique (Schafer, 2002).

For this study, a purposive sample of 69 Bitcoin gambling sites on the Surface Web was compiled from GamblingBitcoin.com (https://gamblingbitcoin.com). It provides "reviews and comparisons of Bitcoin poker sites, Bitcoin blackjack, roulette and other games. . . to guide you to the right sites." (Welcome to GamblingBitcoin.com, n.d., para. 5). Of the 69 sites, 26 were no longer operational or unavailable, and 13 sites did not provide service to customers whose IP location was within the US jurisdiction. Given our research is conducted in the US, we were unable to browse certain sites so we excluded them. Thirty sites were chosen as the sample of Bitcoin gambling sites on the Surface Web.

Tor browser, the most well-known Darknet browser, was chosen as the platform to collect gambling sites from the Darknet. A purposive sample of 216 sites containing only Tor hidden services (HS) was listed on The Undernet Directory (https://underdj5ziov3ic7.onion.link/). This website is "a link list designed for the Tor network. . . " listing .onion sites ("About this site", n.d., para. 1). Of the 216 HS addresses, only 54 were active, and the others were down or not working. After repetitive sites were excluded, 24 sites, in the end, were narrowed down for the sample of gambling sites on the Darknet.

While retrieving samples, we found that some sites were operating on both the Darknet and Surface Web. Expecting interesting findings from this group, we searched each name of Darknet gambling sites on Google to find the sites having domain names on both Webs for further investigation. As a result, 18 gambling websites were revealed having sites on both Webs. Of those, one site overlapped with a sample from the Surface Web. Consequently, the final sample consisted of 53 sites, including 29 sites from only the Surface Web, 18 from both the Surface and Dark Web and six from only the Dark Web. Considering the amorphous character of the Internet, this purposive sample, although limited in the sense of generalizability, provides perhaps the best representation of the phenomenon in question. It is important to recognize that although it depends on the jurisdiction, we judged the legality of online gambling by US standards. Therefore, our sample of gambling sites is considered illegal since cryptocurrency gambling is not allowed in the US.

Each site was examined to identify the information and variables that reveal its characteristics, such as the type of games, registration, promotion, payment, etc. In addition, a Myip.ms (https://myip.ms) was selected to access WHOIS records, which contain hosting information, websites, and IP databases beyond domain names. Yet, none of the information for Darknet sites was found on WHOIS records. The scope and depth of information offered by websites varied widely; some provided a limited

amount of information, whereas others were fairly large. Accordingly, this analytic approach might underestimate the prevalence of some elements within this sample of gambling websites.

As a result, based on the information provided by the gambling website and its WHOIS data, a codebook was created, and coding of the sample was handled independently according to the codebook. Of the observed variables, only statistically significant variables were addressed in this study. The visitors per day were measured at the ratio level, and the other variables were dichotomized as 0 = No and 1 = Yes.

Table 1 shows the overall sample characteristics and their target suitability measurements in the current study. According to WHOIS records, the average number of visitors per day for gambling sites was 2,355.64 (SD=3,788.71). Specifically, daily visitors only on the Surface Web ranged from 200 to 14,100 (N=29, M=3,621.90, SD=4,370.35) and those on both the Surface and Dark Web ranged from 200 to 2,280 (N=18, M=315.56, SD=490.261), revealing that online gamblers are at a higher likelihood of using Bitcoin gambling sites on only the Surface Web rather than those on both the Surface [SW] and Dark Web [DW].

The IP owners stated in the WHOIS database were classified as either the Web hosting company or CDN provider. The Web hosting company provides space on a server owned or leased for use by

**Table 1.** ***Descriptive Statistics***

| | SW and/or DW (*N*=53) | | SW (*N*=29) | SW and DW (N=18) | DW (N=6) |
|---|---|---|---|---|---|
| Measures | Mean (SD) | *N* (%) | *N* (%) | *N* (%) | *N* (%) |
| *Dependent Variable* | | | | | |
| **Visitors per Day** | 2,355.64 (3,788.71) | | | | |
| *Independent Variable* | | | | | |
| **IP Owner** | | | | | |
| Web Hosting | | 23 (43.4) | 6 (20.7) | 17 (94.4) | |
| CDN | | 24 (45.3) | 23 (79.3) | 1 ( 5.6) | |
| Unknown | | 6 (11.3) | | | 6 (100 ) |
| **WHOIS Privacy Service** | | | | | |
| No | | 7 (13.2) | 7 (23.3) | | |
| Yes | | 36 (67.9) | 18 (60 ) | 18(100 ) | |
| Unknown | | 10 (18.9) | 4 (16.7) | | 6 (100 ) |
| **Target Suitability(TS)_1** | | | | | |
| Dice | | 9 (17.0) | 8 (27.6) | 1 ( 5.6) | |
| **TS_2** | | | | | |
| Requiring registration | | 39 (73.6) | 21 (72.4) | 17 (94.4) | 1 (16.7) |
| **TS_3** | | | | | |
| IFNOT_Username | | 6 (11.3) | 5 (17.2) | 1 ( 5.6) | |
| IFNOT_GoogleAuthenticator | | 6 (11.3) | 5 (17.2) | 1 ( 5.6) | |
| IFNOT_PrivateURL | | 5 ( 9.4) | 3 (10.3) | 1 ( 5.6) | 1 (16.7) |
| IFNOT_BitcoinAddress | | 4 ( 7.5) | 3 (10.3) | 1 ( 5.6) | |

Continued on next page

customers hosting their website (What is Web Hosting?, n.d.). A content delivery network (CDN) is a system of geographically distributed servers that allow for the fast delivery of website content to end-users. While a CDN does not host a website, it helps improve website performance and protect

**Table 1 – Continued from previous page**

| | SW and/or DW (*N*=53) | | SW (*N*=29) | SW and DW (N=18) | DW (N=6) |
|---|---|---|---|---|---|
| Measures | Mean (SD) | *N* (%) | *N* (%) | *N* (%) | |
| **TS_4** | | | | | |
| IFYES_Email | | 37 (69.8) | 19 (65.6) | 17 (94.4) | 1 (16.7) |
| IFYES_Password | | 38 (71.7) | 20 (69.0) | 17 (94.4) | 1 (16.7) |
| IFYES_DateofBirth | | 11 (20.8) | 11 (37.9) | | |
| IFYES_Address | | 9 (17.0) | 9 (31.0) | | |
| IFYES_Proof_deposit | | 11 (20.8) | 11 (37.9) | | |
| **TS_5** | | | | | |
| Deposit_Bitcoin | | 53 (100 ) | 29 (100 ) | 18 (100 ) | 6(100) |
| Deposit_Ethereum | | 4 ( 7.5) | 4 (13.8) | | |
| Deposit_Litecoin | | 23 (43.4) | 5 (17.2) | 17 (94.4) | 1 (16.7) |
| Deposit_OtherCryptocurrency | | 2 ( 3.8) | 2 ( 6.9) | | |
| **TS_6** | | | | | |
| Withdrawal_Bitcoin | | 53 (100 ) | 29 (100 ) | 18 (100 ) | 6(100) |
| Withdrawal_Ethereum | | 2 ( 3.8) | 2 ( 6.9) | | |
| Withdrawal_ Litecoin | | 20 (37.7) | 2 ( 6.9) | 17 (94.4) | 1 (16.7) |
| **TS_7** | | | | | |
| Promotion_Blog | | 8 (15.1) | 8 (27.6) | | |
| Promotion_Googleplus | | 6 (11.3) | 6 (20.7) | | |
| Promotion_Reddit | | 6 (11.3) | 6 (20.7) | | |
| Promotion_Facebook | | 16 (30.2) | 16 (55.2) | | |
| Promotion_BitcoinForum | | 7 (13.2) | 7 (24.1) | | |
| Promotion_Faucet | | 5 ( 9.4) | 5 (17.2) | | |
| Promotion_OtherEvents | | 12 (22.6) | 12 (41.4) | | |
| **TS_8** | | | | | |
| Chinese | | 25 (47.2) | 6 (20.7) | 18(100) | 1 (16.7) |
| Danish | | 19 (35.8) | 1 ( 3.4) | 17 (94.4) | 1 (16.7) |
| **TS_9** | | | | | |
| Feat_UserChat | | 5 ( 9.4) | 5 (17.2) | | |
| Feat_LiveBetting | | 8 (15.1) | 8 (27.6) | | |
| Feat_LicenseVerification | | 14 (26.4) | 14 (48.3) | | |

websites from malicious cyberattacks by hiding the origin server IP (Beal, n.d.). It was revealed that 79.3% (n=23) of sites on the SW employed CDN providers and 94.4% (n=17) of sites on both the SW and DW used Web hosting providers. The WHOIS privacy service, also known as the domain proxy service that protects the personal information of gambling sites from WHOIS searches, was coded dichotomously.

Figure 1 shows the distribution of the 43 addresses that were identified, composed of those provided not only by real registrants (n=7) but also by companies providing WHOIS privacy service that was used more than half of the study sites (67.9%, n=36), consisting of 60% (n=18) of sites on the SW and 100% (n=18) of sites on both the SW and DW. All seven online sites that did not use the domain proxy service were located in Curacao (n=5), Ireland (n=1), and Costa Rica (n=1), which permit licensed Bitcoin gambling websites to operate. Although those operating in Curacao and Ireland accept local players, Bitcoin casinos licensed in Costa Rica are only allowed for foreign players.

The type of game was measured by the Dice (17.0%, n=9) variable. To play this game, users simply place their bet on one of the two chances, click the dice, and wait for the result. It is notable that 8

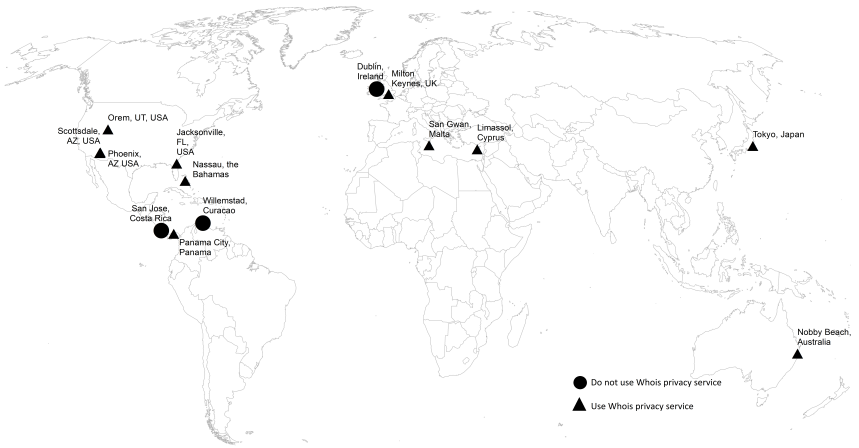


***Figure 1.*** **Distribution of the 43 addresses**

out of 9 sites offering the dice game were on the SW. While the dice was the most common, most sites offered several types of games. The number of types ranged from 1 to 12 different types.

In terms of the registration required, 72.4 % (n=21) of sites on the SW, 94.4% (n=17) of sites on both the SW and DW and 16.7% (n=1) of sites on the DW required registration for gambling. The sites that did not require registration (n=14) asked for information on extra security. The information asked by those sites were measured according to the following variables: username (11.3%, n=6); Google authenticator (11.3%, n=6); private URL (9.4%, n=5); and user's Bitcoin address (7.5%, n=4). Google authenticator is a mobile application that generates two-step verification codes, which have to be typed whenever a user wants to log into their account. Google authenticator is used to enhance user account security in addition to password. When logging in, users have to enter unique codes created by Google authenticator on the user's phone. Used codes will not be used again. For more information on Google authenticator refer to https://www.google.com/landing/2step/\#tab=how-it-protects. The private URL that is automatically given by these sites can be used as accounts, and users can return to their account by typing the given URL. In addition, the information asked by the sites (n=39) requiring registration were coded dichotomously as follows: email (69.8%, n=37); password (71.7%, n=38); date of birth (20.8%, n=11); address (17.0%, n=9); and the proof of deposit (20.8%, n=11). A screenshot or photo of bank statements to prove that deposits were made.

To measure deposit methods, Bitcoin (100%, n=53), Ethereum (7.5%, n=4), Litecoin (43.4%, n=23), and other cryptocurrencies (3.8%, n=2) were coded. Ethereum, also called as Ether, is a cryptocurrency generated by a decentralized platform developed by the Ethereum Foundation. For more information on Ethereum refer to https://www.ethereum.org. Litecoin is an open source peer-to-peer cryptocurrency developed by Charlie Lee. For more information on Litecoin refer to https://litecoin.com. For the purposes of an efficient analysis, the other cryptocurrencies variable was created by grouping 27 different currencies that were found on the specific sites. The sites using Litecoin as a deposit method were on the SW and/or DW, all sites using Ethereum or other cryptocurrencies were on the SW. Likewise, the withdrawal method was measured by the Bitcoin (100%, n=53), Ethereum (3.8%, n=2), and Litecoin (37.7%, n=20) variables. Most of the sites (94.4%, n=17) on the SW and DW employed Litecoin as a deposit and withdrawal method. Bitcoin was not used for analysis because all observed sites used it.

The measures of the promotion consisted of 7 variables; Blog (15.1%, n=8), Google plus (11.3%, n=6), Reddit (11.3%, n=6), Facebook (30.2%, n=16), and Bitcoin forum (13.2%, n=7) were used as platforms for promotion. In addition, Faucet (9.4%, n=5), a bonus system giving free credits for a free bet on a regular basis regardless of betting, and other events (22.6%, n=12) including free bet and Jackpot, were observed for promotion options. All sites containing the promotion variables were on the SW.

In terms of language, Chinese (47.2%, n=25) and Danish (35.8%, n=19) were coded. While all sites supported English and several sites had more than one language option, most of the sites on the SW and DW had Chinese (100%, n=18) and Danish (94.4%, n=17) as a language option. The feature was measured according to the following variables: User chat (9.4%, n=5), Live betting (15.1%, n=8), and License verification (26.4%, n=14), showing legitimacy for operation. License verification is a certificate of gambling license conferred by authorities of the country in which a gambling website based. All sites having feature variables were on the SW.

### *Results*

The study sample consisted of 53 sites on one or both the Surface Web (SW) and Dark Web (DW) and was examined using 11 categories. Figure 2 is a bar chart of sites' daily visitors. The number of visitors per day for gambling sites only on the SW ranged from 200 to 14,100 (N=29, M=3,621.90, SD=4,370.35) while those on both the SW and DW ranged from 200 to 2,280 (N=18, M=315.56, SD=490.261), revealing that online gamblers have a higher likelihood of using Bitcoin gambling sites only on the SW rather than those on both the SW and DW.

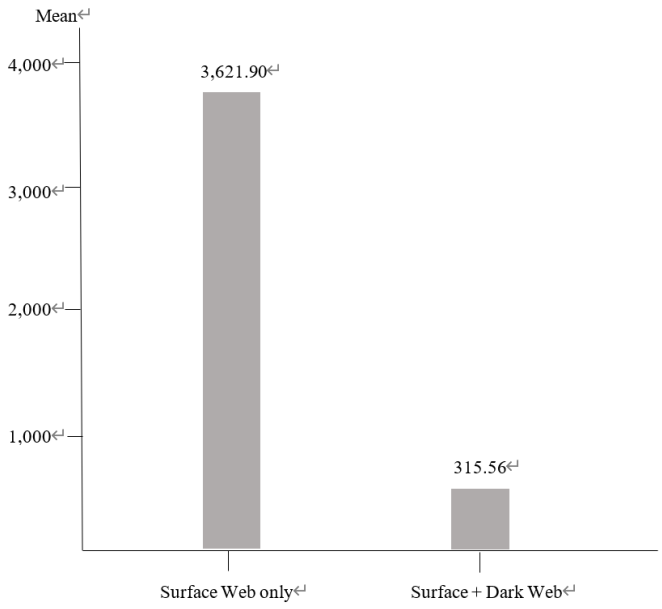


***Figure 2*. Bar chart of the average visitors per day**

In Table 2, multiple regression analysis displays the list of target suitability measures that predicted daily visitors of Bitcoin gambling websites. All variables had a significant effect on visitors per day ($p<.05$). Unstandardized coefficients (B), standard errors (SE) standardized coefficients ($\beta$), p-values, $R^2$, and adjusted $R^2$ are displayed in Table 2.

**Table 2.** ***Multiple Regression Analysis for Factors Predicting Visitors per Day.***

| Predictors | B | SE | β | p |
|---|---|---|---|---|
| **Target Suitability(TS)_1** | | | | |
| Dice | 3,916.43 | 1,294.47 | .41 | .00*** |
| $R^2$ | | .17 | | |
| Adjusted $R^2$ | | .15 | | |
| **TS_2** | | | | |
| Requiring registration | -2,727.96 | 1,360.56 | -.29 | .05* |
| $R^2$ | | .08 | | |
| Adjusted $R^2$ | | .06 | | |
| **TS_3** | | | | |
| IFNOT_Username | 8,845.82 | 2,738.22 | .79 | .01** |
| IFNOT_GoogleAuthenticator | 4,870.31 | 2,320.32 | .43 | .04* |
| IFNOT_PrivateURL | -7,116.91 | 2,455.51 | -.53 | .01** |
| IFNOT_BitcoinAddress | -7,664.46 | 3,652.39 | -.57 | .04* |
| $R^2$ | | .27 | | |
| Adjusted $R^2$ | | .20 | | |
| **TS_4** | | | | |
| IFYES_Email | -11,495.30 | 2,994.79 | -1.30 | .00*** |
| IFYES_Password | 7,312.90 | 3,073.94 | .80 | .02* |
| IFYES_DateofBirth | 7,155.30 | 2,161.88 | .81 | .00*** |
| IFYES_Address | -9,019.46 | 2,678.22 | -.95 | .00*** |
| IFYES_Proof_deposit | 4,140.14 | 1,560.20 | .47 | .01** |
| $R^2$ | | .47 | | |
| Adjusted $R^2$ | | .40 | | |
| **TS_5** | | | | |
| Deposit_Ethereum | 7,360.00 | 2,472.92 | .55 | .01** |
| Deposit_Litecoin | -3,446.36 | 1,025.59 | -.46 | .00*** |
| Deposit_OtherCryptocurrency | -7,142.00 | 3,317.77 | -.39 | .04* |
| $R^2$ | | .28 | | |
| Adjusted $R^2$ | | .23 | | |
| **TS_6** | | | | |
| Withdrawal_Ethereum | 7,360.00 | 2,526.38 | .40 | .01** |
| Withdrawal_Litecoin | -3,092.68 | 1,039.12 | -.41 | .01** |
| $R^2$ | | .24 | | |
| Adjusted $R^2$ | | .20 | | |
| **TS_7** | | | | |
| Promotion_Blog | 3,829.61 | 1,191.47 | .38 | .00** |
| Promotion_Googleplus | -3,279.17 | 1,213.62 | -.30 | .01** |
| Promotion_Reddit | -2,933.31 | 1,324.76 | -.26 | .03* |
| Promotion_Facebook | 2,453.18 | 963.08 | .31 | .02* |
| Promotion_BitcoinForum | -4,039.08 | 1,319.08 | -.38 | .00*** |
| Promotion_Faucet | 5,397.73 | 1,332.82 | .44 | .00*** |
| Promotion_OtherEvents | 2,756.80 | 1,099.76 | .32 | .02** |
| $R^2$ | | .66 | | |
| Adjusted $R^2$ | | .58 | | |

Continued on next page

**Table 2 – Continued from previous page**

| Predictors | B | SE | β | p |
|---|---|---|---|---|
| **TS_8** | | | | |
| Chinese | 2,997.37 | 1,381.66 | .40 | .04* |
| Danish | -5,410.26 | 1,440.81 | -.70 | .00*** |
| $R^2$ | | .43 | | |
| Adjusted $R^2$ | | .39 | | |
| **TS_9** | | | | |
| Feat_UserChat | 8,261.63 | 1,250.81 | .68 | .00*** |
| Feat_LiveBetting | 2,448.26 | 1,020.59 | .25 | .02* |
| Feat_LicenseVerification | 2,676.63 | 860.40 | .33 | .00*** |
| $R^2$ | | .57 | | |
| Adjusted $R^2$ | | .54 | | |

*p<.05, **p<.01, ***p<.001

The findings indicated that Dice game is positively correlated with the number of daily visitors (p<.001), suggesting individuals are less likely to play games on gambling sites that require registration (p=.05). The results suggest that gambling websites that did not require registration and had Username (p=.01) and Google authenticator (p=.04) options for extra security had a relatively high number of daily visitors, whereas those that had the Private URL (p=.01) and Bitcoin Address (p=.04) options for extra security had a relatively small number of daily visitors. Similarly, gambling websites that required Password (p=.02), Date of Birth (p<.001), and Proof of deposit (p=.01) to play the game had a relatively high number of daily visitors, whereas those that required Email (p<.001) and Address (p<.001) had a relatively small number of visitors per day.

It was also found that Ethereum was positively correlated with the number of daily visitors in regards to both Deposit (p=.01) and Withdrawal methods (p=.01), whereas Litecoin was negatively correlated with the number of daily visitors in regards to both Deposit (p<.001) and Withdrawal methods (p=.01). Regarding the Language, Chinese (p=.04) was positively related to the number of daily visitors, whereas Danish (p<.001) was negatively associated with the number of daily visitors.

Table 2 showed that Blog (p<.001), Facebook (p=.02), Faucet (p<.001), and Other events (p=.02) used for promotion had a positive relationship with the number of daily visitors, whereas Google plus (p=.01), Reddit (p=.03), and Bitcoin forum (p<.001) used for promotion were negatively related to the number of daily visitors. In terms of the Feature, User chat (p<.001), Live betting (p=.02), and License verification (p<.001) had a positive correlation with the number of daily visitors.

### *Discussion*

Reviewing the website contents of gambling on both Surface and/or Dark Web allows for several key observations to be made about how these sites manage to operate while evading law enforcement detection, the role of the Internet in their operations, and what other illegal activities are possibly engendered by illegal online gambling activities. The findings of this study indicate that Bitcoin gambling sites on the Surface Web are more popular among online gamblers than sites on both the Dark and Surface Web. Although the number of visitors to the Dark Web sites cannot be observed, it would be fair to argue that Darknet gambling sites are not yet prosperous compared to those on the Surface Web. In fact, Surface Web Bitcoin gambling sites have more promotion options, games, and diverse features when compared to Darknet gambling sites. This may be due to the fact that Dark Web technology is not yet familiar to general Internet users (Clemmitt, 2016). Another possible explanation is that gambling websites employing Bitcoin share similar characteristics with those on the Darknet,

implying that online gamblers may not need to play on Darknet gambling sites for anonymity because they can still play and place bets on the Surface Web.

The results of the study show that the borderless nature of the Internet is attractive for gambling operators. Gambling sites are able to access their targets globally while locating their properties and servers wherever they want. Another feature that makes transnational operations safe is anonymous operations. The findings reveal that Darknet sites are operated anonymously with Darknet technology, whereas sites on the Surface Web are operated while protected from revealing confidential information of their server and assets by employing a WHOIS privacy service and CDN, which impede effective investigation for tracking down gambling rings by law enforcement. In addition, it is notable that those personal information protection techniques, which were developed as a means of protecting websites from cyberattacks, have been exploited by illegal gambling operators to hide their identity (Banks, 2012). In addition, the results showing the locations of the registrant, which did not use the WHOIS privacy service were in areas where Bitcoin gambling, is legal implies that even people in places where online gambling is banned can run gambling sites anonymously if confidential information protection means are used.

From the user aspects, it was found that some features enable anonymous gambling activities. Using encrypted currencies as deposit and withdrawal methods makes it extremely difficult to trace transactions. In addition, the findings show that Bitcoin gambling sites that require registration or ask for private information such as a private Bitcoin address, email, and address tend to have few daily visitors. This may lead to the conclusion that online gambling prefer anonymous gambling activities. Therefore, anonymity is one of the key features that preserve illegal gambling sites from the investigation of law enforcement agencies.

The findings also indicate that Bitcoin gambling sites provide venues for criminal opportunities for offenders in cyberspace. As suggested in Fiedler's (2013) study, Bitcoin gambling sites are apt for money laundering. Various deposit and withdrawal options that allow for more money laundering opportunities might be attractive for offenders. Likewise, sophisticated payment processes, such as paying in other currencies different from the one in which the user deposited, makes it extremely difficult to trace.

The results of this study indicate that the anonymous nature of gambling sites are possibly associated with youth gambling involvement. Gambling sites that do not require registration enable younger populations who are prohibited from gambling due to age limits play without restrictions. Therefore, the increased availability of online gambling may lead to increases in the prevalence of youth gambling and to the development of gambling problems among young people.

Also, anonymity can be exploited for fraud if operators victimize their customers by refusing to payout gambling winnings and block the victim's access to sites by depriving them of membership or shutting down the sites (Banks, 2012; Griffiths, 2010).

In addition, the findings of the study support the claims that online gambling is susceptible to problem gambling (Canale et al., 2016; Gainsbury et al., 2015; Harris, Mazmanian, & Jamieson, 2013; McCormack & Griffiths, 2013; Wood, & Williams, 2007). Equipped with the instant payment and no transaction fee, the Dice game, which was positively linked to the number of daily visitors, seems to provoke gambling addiction because of the nature of the game: it is extremely simple (one-click betting), short (less than 3 seconds for one game), convenient (automatic betting), and limitless. Moreover, numerous promotion options, including the Faucet, bonus, free bet, and events, keep users occupied in

games, and the real-time nature of sites, including user chat and live betting makes, it increasingly addictive. Therefore, a Bitcoin gambling user easily becomes a victim of gambling addiction.

The finding that gambling sites that have license verification tend to have higher numbers of daily visitors seems to be in line with the outcomes suggested by Shelat and Egger (2002), who surveyed 31 online gamblers to identify how they choose which online gambling sites to trust. They concluded that online gamblers judge the credibility of an online gambling site based on information about who the operator is, its legality, and the fairness of the game. This may be because license verification showing legitimacy for operation gives a false sense of legitimacy to some users when in reality legality is determined based on the territorial jurisdiction of the user's IP (Trimble, 2012). In addition, the license possibly indicates to users that the games on the site are fair and reliable.

In terms of security, the findings pertaining to the required information for registration reveal the user's concern about the security behind the anonymous and private gameplay. It can be concluded that users prefer to log in to their account by entering a username/password or Google authenticator keys rather than private URL. In addition, in the case of Bitcoin gambling sites employing conventional transaction methods, the proof of deposit may make online gamblers feel secure after making a deposit.

Given the price volatility of cryptocurrency, the findings in regard to Ethereum and Litecoin may indicate that gamblers expect to win rewards not only from betting but also from price volatility. This is because although the price was almost similar on January 1, 2015 (Ethereum= $1, Litecoin = 2$), the price of Ethereum reached approximately 751 dollars, whereas the price of Litecoin reached approximately 225 dollars on the same date in 2018 (Cryptocurrency statistics, n.d.). Thus, it can be argued that the different change rate in the price of cryptocurrencies may affect the popularity of gambling sites utilizing cryptocurrencies.

In terms of the languages employed by gambling sites, it can be concluded that gambling users from China, where online gambling is heavily restricted, use Bitcoin gambling sites as an alternative platform for online gambling. However, the negative correlation between those using Danish and the number of daily visitors may be explained by Denmark's online gambling legislation. Gambling users from Denmark, where online casinos are legal, may not need to gamble on gambling sites using cryptocurrencies ("Denmark Gambling 2018," 2017).

The findings reinforce the importance of capable guardianship to prevent and detect illegal online gambling operations. Aside from their own blogs, online gambling rings promote their sites through social networking sites. Although advertising on platforms such as Google Plus, Reddit, and Bitcoin forum seems less effective for promotions, Facebook, which is the largest social networking site (Most famous social, 2017), is mainly used for larger Bitcoin gambling sites for advertisement. The findings can be beneficial for developing effective prevention measures to deter illegal online gambling when combined with target-hardening activities.

### *Policy Implication*

Based on the findings, it can be suggested that anonymous gambling may cause several widespread problems such as illegal operations, adolescent gambling, fraud, or money laundering. In terms of formal social control, while the structures of the Darknet and Bitcoin are highly complex, various techniques have been introduced in an effort to investigate the Darknet (Bradley & Stringhini, 2019; Fidalgo et al., 2019; White, Kakkar, & Chou, 2019) as well as tracing Bitcoin transactions (Al Jawaheri et al., 2020). Since these cyber investigative techniques are sophisticated, time-sensitive, and require a high level of proficiency in using various investigative toolkits and of understanding

in cybersecurity, law enforcement agencies should continue their efforts to constantly develop skilled agents and enhance their ability in cyber investigations. In addition, successful cyber investigations by which the individuals behind the server are uncovered does not necessarily mean the end of the case since they could conduct only the divided function as a part of the criminal enterprise. In addition, the server is often located in countries outside of the US (White, Kakkar, & Chou, 2019). These challenges indicate that investigators should be familiar with both traditional, international, and cyber elements of the investigation.

In terms of informal social control, given that online gambling rings promote their sites on social media platforms and vulnerable young people using smartphones spend most of their time on social networking apps, it would be important for Internet-based companies to effectively regulate people from using their sites for illegal or unauthorized purposes. In fact, social media providers should take measures to regulate inappropriate content on their sites. For example, Facebook announced recently that additional people would be employed to enhance the capability of monitoring content regarding harm and harassment that are posted to the social networking site (Tsukayama, 2017). Although regulated posts are limited to violent content, this indicates that major social networking sites actually initiate monitoring inappropriate content. To effectively regulate illegal online gambling in the private sector, the range of restricted content needs to be extended to other unlawful posts, including illegal gambling advertisements, and rapid reporting and response systems for taking down illicit contents should be built based on the simple reporting procedures.

The ICANN, managing the WHOIS database, may be able to play a vital role in effectively tracking illegal gambling websites by providing registration data. In the absence of a WHOIS policy, there has been controversy over the extent of publicly displaying registration data of domain owners, ranging from the creation and expiration dates for registration to contact information of domain owners (Masnick, 2015). Considering the interests of domain owner's privacy, cybersecurity, and law enforcement, the ideal rules regarding data privacy and protection may need to display at least partial information that does not reveal confidential information in the WHOIS database and only give access to non-public information to third party requestors providing legitimate orders from judicial tribunals for accessing the data, while the ICANN stores all registration data including registrant, administrative, and technical contact information. Without due process, end-users would only be able to contact the registrant of domain owners, either through anonymized contact information or other technical and legal means. Also, this regulation should apply to all registrations on a global basis ("Data Protection and Privacy Update," n.d.).

In addition, given that anonymous online gambling enables adolescents to place a bet online without restriction, it is required for guardians that are overseeing them, such as parents, to play important roles as gatekeepers. A treatment center that specializes in video game and Internet addiction, Techaddiction, advises parents of adolescent gamblers to set rules for healthy web browsing. For example, the center teaches how to install software blocking online gambling sites as well as other malicious websites and to place computers in open areas where parents can surveil the online activities of their children ("Teenage Gambling Online," n.d.).

Furthermore, given that the Internet is an uncontrolled and uncensored entity, it is hard to control all activities that children may indulge in. As a result, it is suggested that parents pay particular attention in keeping abreast with the online activities of their children, such as checking their web history to see what sites they are visiting, enough to ensure that they are not engaging in online gambling (Choi, Cho, and Lee, 2019; Choi et al., 2019).

With regard to target-hardening activity, public awareness programs can play an important role in minimizing negative outcomes of online gambling activities (Choi, 2015). Based on the existing gambling awareness program, Problem Gambling Awareness Month which is operated by the National Council on Problem Gambling (March Is Problem Gambling, n.d.), it can be modified into the program that focuses on problem gambling provoked by illegal online gambling activities. The program should highlight that the nature of online gambling, such as 24/7 availability, make it possibly more addictive and difficult to recover than offline gambling. To prevent citizens from being involved in illegal online gambling activities, it should also emphasize law and regulations pertaining to online gambling to facilitate the acquisition of solid ethical standards for online gambling users. In addition, given that anonymous gambling has made it accessible to minors who typically would be identified as under age at a physical betting establishment, the awareness program should be extended to the schools or school campaigns against illegal online gambling should be implemented.

### *Conclusion*

The anonymous nature of cryptocurrencies and Darknet technology allows the online gambling industry to evade regulations imposed by the authority and investigation of law enforcement agencies. Not only is the operation illegal, but it can also lead to other online illegal activities such as fraud, money laundering, adolescent gambling, or problem gambling. To further understand the nature of anonymous gambling, this study examined: (1) how online gambling sites operate; (2) what factors are attractive for online users to participate in illegal gambling activities; (3) how illegal online gambling activities potentially lead to other online criminal activities; and (4) how online gambling operators preserve operations while evading from the investigation of law enforcement agencies.

By collecting information from 53 sites on the Surface Web and Dark Web, the analysis was conducted to compare the characteristics of each site and uncover what factors contribute to gambling activities at the portals of Bitcoin gambling sites on both the Dark and Surface Web. The results suggest that Bitcoin gambling sites on the Surface Web are more popular among online gamblers and are more active than Darknet gambling sites. In addition, the findings indicate that not only are Darknet sites operated anonymously, but sites on Surface Web reach customers globally while protecting them from exposing their identity. The analysis revealed several factors of popular gambling websites. Also, it was found that users of Bitcoin gambling sites were susceptible to gambling addiction and other online illegal activities such as money laundering, fraud, and underage gambling.

Based on the findings of this study, possible suggestions have been made for effective formal social control, such as the constant development of capable investigators in digital forensics. In terms of informal social control, it was suggested that Internet-based companies, such as Facebook should regulate inappropriate content and people from using their site for illegal purposes. In addition, data privacy and protection regulations balancing concerns of privacy information protection, IT security, and law enforcement should be developed and activated for efficient tracking on unlawful websites. The role of parents as gatekeepers was addressed to prevent their children from online gambling. Regarding target-hardening activity, a public awareness program was suggested to prevent gambling users from negative outcomes of illegal online gambling activities.

Due to the amorphous nature of the Internet, the sample may not represent the true population, which could present bias issues. These data was derived from only 53 cases, which may not be sufficient for accurate analysis. Inclusion of Bitcoin and Darknet gambling sites could improve the quality of this research if it were presented in the form of content analysis. In addition, further research should be conducted to compare Bitcoin gambling laws that are classified according to game type and region.

Together with the need for an evaluation study of crime prevention measures, the limitations provide opportunities for future research involving follow-up using a sufficient number of cases or comparing legal online gambling sites with illegal counterparts. Such work would enable us to determine illegal online gambling trends and patterns and to anticipate future directions of its operations and activities further.

**Declaration of Interest Statement**

The authors declare that they have no conflicts of interest.

**References**

About this site. (n.d.). Retrieved from https://underdj5ziov3ic7.onion.link/help

About WHOIS. (n.d.). Retrieved from https://whois.icann.org/en/about-whois

Al Jawaheri, H., Al Sabah, M., Boshmaf, Y., & Erbad, A. (2020). Deanonymizing tor hidden service users through bitcoin transactions analysis. *Computers & Security, 89*, 101684.

Banks, J. (2012). Online gambling and crime: a sure bet? *The ETHICOMP Journal.* Retrieved from http://shura.shu.ac.uk/6903/

Beal, V. (n.d.). CDN – Content Delivery Network. *Webopedia.* Retrieved from https://www.webopedia.com/TERM/C/CDN.html

Bergman, M. K. (2001). Whitepaper: the deep web: surfacing hidden value. *Journal of Electronic Publishing, 7*(1).

Bhattacharjee, S. (2016). A statistical analysis of bitcoin transactions during 2012 to 2013 in terms of premier currencies: Dollar, euro and rubles. *Vidwat: The Indian Journal of Management, 9*(1), 8-16.

Bradley, C., & Stringhini, G. (2019). A qualitative evaluation of two different law enforcement approaches on dark net markets. In IEEE (Eds.), *2019 IEEE European Symposium on Security and Privacy Workshops* (EuroS&PW) (pp. 453-463), NY: IEEE.

Brito, J., & Castillo, A. (2013). *Bitcoin: A primer for policymakers.* Retrieved from https://www.mercatus.org/system/files/GMU_Bitcoin_042516_WEBv2_0.pdf

Brosowski, T., Meyer, G., & Hayer, T. (2012). Analyses of multiple types of online gambling within one provider: an extended evaluation framework of actual online gambling behaviour. *International Gambling Studies, 12*(3), 405-419.

Canale, N., Griffiths, M. D., Vieno, A., Siciliano, V., & Molinaro, S. (2016). Impact of Internet gambling on problem gambling among adolescents in Italy: Findings from a large-scale nationally representative survey. *Computers in Human Behavior, 57*, 99-106.

Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*(1), 308.

Choi, K-S., Earl, K.J., Park, A., & Della Giustina, J. (2014). Use of synthetic cathinones: legal issues and availability of darknet. *VFAC Review, 7*, 19-32.

Choi, K. S. (2015). *Cybercriminology and digital investigation*. El Paso, Texas: LFB Scholarly Publishing.

Choi, K. S., Cho, S., & Lee, J. R. (2019). Impacts of online risky behaviors and cybersecurity management on cyberbullying and traditional bullying victimization among Korean youth: Application of cyber-routine activities theory with latent class analysis. *Computers in Human Behavior, 100*, 1-10.

Choi, K. S., Earl, K., Lee, J. R., & Cho, S. (2019). Diagnosis of cyber and non-physical bullying victimization: A lifestyles and routine activities theory approach to constructing effective preventative measures. *Computers in Human Behavior, 92*, 11-19.

Choi, K. S., & Lee, J. R. (2017). Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory. *Computers in Human Behavior, 73*, 394-402

Christin, N. (2013). Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In *Proceedings of the 22nd international conference on World Wide Web* (pp. 213-224). ACM.

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice, 19*, 91-150.

Clearing up confusion – deep web vs. dark web. (2014, March 27). Retrieved from https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/

Clemmitt, M. (2016). The dark web. *CQ Researcher, 26*, 49-72. Retrieved from http://library.cqpress.com/

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American sociological review, 4*(4), 588-608.

Cohen, L. E., Kluegel, J. R., & Land, K. C. (1981). Social inequality and predatory criminal victimization: An exposition and test of a formal theory. *American Sociological Review, 46*(5), 505-524.

Cryptocurrency statistics. (n.d.). Retrieved from https://bitinfocharts.com/

Data Protection and Privacy Update: Seeking Community Feedback on Proposed Compliance Models. (n.d.). Retrieved from https://www.icann.org/news/blog/data-protection-and-privacy-update-seeking-community-feedback-on-proposed-compliance-models

Deans, E. G., Thomas, S. L., Daube, M., & Derevensky, J. (2016). "I can sit on the beach and punt through my mobile phone": The influence of physical and online environments on the gambling risk behaviours of young men. *Social Science & Medicine, 166*, 110-119.

Denmark Gambling 2018. (2017, Jun 12). Retrieved from https://iclg.com/practice-areas/gambling-laws-and-regulations/denmark

Doesn't Tor enable criminals to do bad things?. (n.d.). Retrieved from https://www.torproject.org/docs/faq-abuse.html.en\#WhatAboutCriminals

Domain Name Registration Process. (2017, July). Retrieved from https://whois.icann.org/en/domain-name-registration-process

Felson, M., & Boba, R. L. (2010). *Crime and everyday life*. Thousand Oaks, CA: Sage

Fidalgo, E., Alegre, E., Fernández-Robles, L., & González-Castro, V. (2019). Classifying suspicious content in tor darknet through Semantic Attention Keypoint Filtering. *Digital Investigation, 30*, 12-22.

Fiedler, I. (2014). Online gambling as a game changer for money laundering? In Ötsch, W., Grözinger, G., Beyer, K., Bräutigam, L. (Eds.), *The political economy of offshore jurisdictions* (pp. 79–95). Marburg, Germany: Metropolis.

Finklea, K. (2017, March 10). Dark Web. *Congressional Research Service*, Retrieved from https://fas.org/sgp/crs/misc/R44101.pdf

Gainsbury, S. M., Russell, A., Wood, R., Hing, N., & Blaszczynski, A. (2015). How risky is Internet gambling? A comparison of subgroups of Internet gamblers based on problem gambling status. *New Media & Society, 17*(6), 861–879.

Gil, P. (2017, July 12). *What is an 'IP address'? is it the same as 'domain name'?*. Retrieved from Lifewire website: https://www.lifewire.com/what-is-an-ip-address-24833148.

Griffiths M. (2010). Crime and gambling, a brief overview of gambling fraud on the Internet. *Internet Journal of Criminology*. Retrieved from http://irep.ntu.ac.uk/id/eprint/23349/

Grand View Research (2019, August). *Online gambling market size, share & trends analysis report by type (sports betting, casinos, poker, bingo), by device (desktop, mobile), by region, and segment forecasts, 2019 – 2025.* Retrieved from Grand View Research website: https://www.grandviewresearch.com/industry-analysis/online-gambling-market?utm_source=prnewswire.com\&utm_medium=referral\&utm_campaign=PRN_Aug27_onlinegambling_ICT_RD1\&utm_content=Content

Harris, N. M., Mazmanian, D., & Jamieson, J. (2013). Trust in Internet gambling and its association with problem gambling in university students. *Journal of Gambling Issues, 28*, 1-17.

Hing, N., Cherney, L., Blaszczynski, A., Gainsbury, S. M., & Lubman, D. I. (2014). Do advertising and promotions for online gambling increase gambling consumption? An exploratory study. *International Gambling Studies, 14*(3), 394-409.

Homeyer, K. D. (2011). Can a state seize an Internet gambling website's domain name? an analysis of the Kentucky case. *UNLV Gaming Law Journal, 2,* 107-131

How to choose the right web hosting. (2017, September 11). Retrieved from https://www.webhostingsecretrevealed.net/choose-the-right-web-hosting/

March Is Problem Gambling Awareness Month, (n.d.), Retrievedfromhttps://www.ncpgambling.org/programs-resources/programs/pgam/

Masnick, M. (2015, Jun 24). ICANN's War On Whois Privacy. *techdirt*. Retrieved from https://www.techdirt.com/articles/20150623/17321931439/icanns-war-whois-privacy.shtml

McCormack, A., & Griffiths, M. D. (2013). A scoping study of the structural and situational characteristics of internet gambling. *International Journal of Cyber Behavior, Psychology and Learning (IJCBPL), 3*(1), 29-49.

Mercer, E. (n.d.). How to register a domain name anonymously. *Chron*. Retrieved from http://smallbusiness.chron.com/register-domain-name-anonymously-45330.html

Mitchell, B. (2017, May 05). *What is a server in computer networking?*. Retrieved from Lifewire website: urlhttps://www.lifewire.com/servers-in-computer-networking-817380

Moore, D., & Rid, T. (2016). Cryptopolitik and the darknet. *Survival, 58*(1), 7-38.

Most famous social network sites worldwide as of September 2017, ranked by number of active users (in millions). (2017, September). Retrieved from https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/

Murphy, V. E., Murphy, M. M., & Seitzinger, M. V. (2013). Bitcoin: questions, answers, and analysis of legal issues. Congressional Research Service. Retrieved from https://fas.org/sgp/crs/misc/R43339.pdf

Murray. B. (2017, October 13). *Governor Christie announces online gaming growth agreement with Nevada and Delaware.* Retrieved from State of New Jersey Office of The Governor website: http://nj.gov/governor/news/news/552017/approved/20171013b.html

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

Pathe, S. (2014, March 2). Gamblers wager billions on unregulated Bitcoin betting sites. *Pbs Newshour.* Retrieved from http://www.pbs.org/newshour/updates/bitcoin-gambling-sites-fly-regulatory-radar/

Rudesill, D. S., Caverlee, J., & Sui, D. (2015). *The deep web and the darknet: A look inside the internet's massive black box.* NW Washington, DC: Wilson center. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676615\#\#

Sablik, T. (2013, December 16). Digital currency: New private currencies like bitcoin offer potential - and puzzles. *Econ Focus: Third Quarter 2013, 17*(3), 18 - 27.

Schafer, J. A. (2002). Spinning the web of hate: Web-based hate propagation by extremist organizations. *Journal of Criminal Justice and Popular Culture, 9*(2), 69-88.

Schumer Pushes to Shut Down Online Drug Marketplace. (2011, June 5). *NBC New York*. Retrieved from http://www.nbcnewyork.com/news/local/123187958.html

Seth, S. (2014, October 24). How bitcoin casino works. Retrieved from Investopedia website: http://www.investopedia.com/articles/investing/102214/how-bitcoin-casinos-work.asp

Shelat, B., & Egger, F. N. (2002, April). What makes people trust online gambling sites?. In *CHI'02 Extended Abstracts on Human Factors in Computing Systems* (pp. 852-853). ACM.

Teenage Gambling Online - Risks, Self-Test, & Advice. (n.d.). Retrieved from http://www.techaddiction.ca/teenage-gambling-online.html

Trimble, M. (2012). Proposal for an international convention on online gambling. In A. Cabot & N. Pindell (Ed.), *Regulating Internet Gaming*. Las Vegas, NV: UNLV Gaming Press. Retrieved from https://ssrn.com/abstract=2089935

Tsukayama, H. (2017, May 3). Facebook adds 3,000 employees to screen for violence as it nears 2 billion users. *The Washington Post*. Retrieved from https://www.washingtonpost.com/news/the-switch/wp/2017/05/03/facebook-is-adding-3000-workers-to-look-for-violence-on-facebook-live/?utm_term=.3232af2a6cab

Wang, P., & Antonopoulos, G. A. (2016). Organized crime and illegal gambling: How do illegal gambling enterprises respond to the challenges posed by their illegality in China? *Australian & New Zealand Journal of Criminology, 49*(2), 258-280.

Welcome to GamblingBitcoin.com!. (n.d.). Retrieved from https://gamblingbitcoin.com/home/

What is Web Hosting?. (n.d.). Retrieved from https://www.website.com/beginnerguide/webhosting/6/1/what-is-web-hosting?.ws

White, R., Kakkar, P. V., & Chou, V. (2019). Prosecuting darknet marketplaces: challenges and approaches. *Department of Justice Journal of Federal Law and Practice, 67*(1) , 65-80.

Wood, R. T., & Williams, R. J. (2007). Problem gambling on the Internet: Implications for Internet gambling policy in North America. *New Media & Society, 9*(3), 520-542.

Yar, M. (2005). The novelty of 'cybercrime' an assessment in light of routine activity theory. *European Journal of Criminology, 2*(4), 407-427.