Do Dark Web and Cryptocurrencies Empower Cybercriminals?

Milad Taleby Ahvanooey[1(✉)], Mark Xuefang Zhu[1(✉)], Wojciech Mazurczyk[2], Max Kilger[3], and Kim-Kwang Raymond Choo[3]

[1] School of Information Management, Nanjing University (NJU), PO.Box 210023, Nanjing, People's Republic of China
M.taleby@ieee.org, xzhu@nju.edu.cn

[2] Institute of Computer Science, Faculty of Electronics and Information Technology, Warsaw University of Technology (WUT), Warsaw, Poland
wojciech.mazurczyk@pw.edu.pl

[3] Department of Information Systems and Cyber Security, University of Texas at San Antonio (UTSA), San Antonio, TX 78249-0631, USA
Max.Kilger@utsa.edu, raymond.choo@fulbrightmail.org

Abstract. The dark web is often associated with criminal activities such as the sale of exploit kits using cryptocurrencies as payment. However, the difficulty in determining the identities of dark website owners and the tracing of the associated transactions compounds the challenges of investigating dark web activities. In this study, we explore how cryptocurrencies have been involved in cybercriminal activities on the dark web and the factors that drive cryptocurrency investments. Then, we present several recommendations and guidelines for prospective investors to help identify determinant factors for assessing investment risks in the cryptocurrency marketplace. We also present several potential research opportunities in cryptocurrency.

Keywords: Cryptocurrency · Dark web · Cybercrime · Crypto market · Trustworthiness analysis

1 Introduction

The dark web has been, and continues, to be exploited by numerous malicious threat actors such as organized crime groups, terrorists, cybercriminals, and state-sponsored actors. Such marketplaces allow malicious threat actors to monetize their illicit services (e.g., exploits, hacking tools, and/or stolen information such as credit card and other sensitive information). Cryptocurrencies are one of the widely used payment methods on dark web marketplaces since they facilitate anonymous transactions [1], and the availability of hard-to-trace payment platforms compounds the challenge of law enforcement agencies in investigating malicious cyber activities on dark web.

There have been a small number of success stories, where law enforcement agencies have had reportedly taken down several illicit online marketplaces [2]. For example, according to Europol's January 2021 report [1],

P. Gladyshev et al. (Eds.): ICDF2C 2021, LNICST 441, pp. 277–293, 2022.
https://doi.org/10.1007/978-3-031-06365-7_17

> DarkMarket.onion was the largest online drug market on the dark web that has been shut down to date by law enforcement agencies. The vendors in this illicit marketplace had profited €140 million by trading all kinds of drugs as well as selling anonymous SIM cards, stolen or forged credit card details, counterfeit money, and ransomware/malware kits [3].

There are, however, hundreds to thousands of active dark markets that are still active. Not surprisingly, there are ongoing efforts in studying dark web and the associated illicit services [1]. For example, researchers have designed tools and technologies can be used by law enforcement agencies to track illicit activities on the dark web (e.g., cryptocurrency forensics [4–7]).

In this study, we study the risks associated with dark web activities, including payment systems (e.g., cryptocurrencies). We also study the factors that underpin investments in cryptocurrencies, with the aim of identifying criteria that online investors can use to inform their decision-making in cryptocurrency investments.

The rest of the article is organized as follows. The next section presents the relevant background materials. Next, the third section focuses on recently active dark markets and their services. We also present three related factors that underpin cryptocurrency investments. Then in the fourth section, we seek to determine the trustworthiness of the cryptocurrency market, by analyzing data from trustworthy resources. In the fifth section, we discuss the associated risks of the cryptocurrency market and present mitigating solutions. Finally, the last section concludes this paper.

2 Background: Dark Web and Cryptocurrencies

Darknet can be broadly defined to be a secret, encrypted, and/or covert (or anonymized) communication system. Such a hidden communication channel is generally not accessible or visible to ordinary Internet users. Dark web or The Onion Router (Tor) networks are two concepts that are associated with darknet, whose design is to ensure the anonymity of users' activities. For example, the Tor browser supports "hidden websites" utilizing an addressing strategy that depends upon randomly generated secret keys and defined by an address extension with ".onion" (e.g., http://ax555xx.onion). TOR can also be employed to provide anonymous access to existing online sites [8]. The hidden nature of the .onion websites on the Tor network can be abused to facilitate various illicit services (e.g., Silk Road marketplace), where anonymous payment systems (e.g., cryptocurrencies) are generally used in such cybercriminal activities [9,10].

Now, we will briefly summarize the various malicious cyber activities that are known to be conducted on dark web and facilitated using cryptocurrencies.

- ***Ransom and ransomware:*** Ransomware is one type of malicious software (also referred to as malware), where the attacker threatens victims by blocking access to their sensitive information unless a ransom is paid (typically using some cryptocurrency) [11,12]. Cryptocurrency has also been used as

a form of payment in physical, real-world kidnapping [13]. As depicted in Fig. 1, according to the global cyber security annual report in [14] July 2021, there have been discovered a total of 304 million ransomware cyberattacks worldwide in 2020, which was a 62% rise compared to 2019, and the second highest rate since 2016.

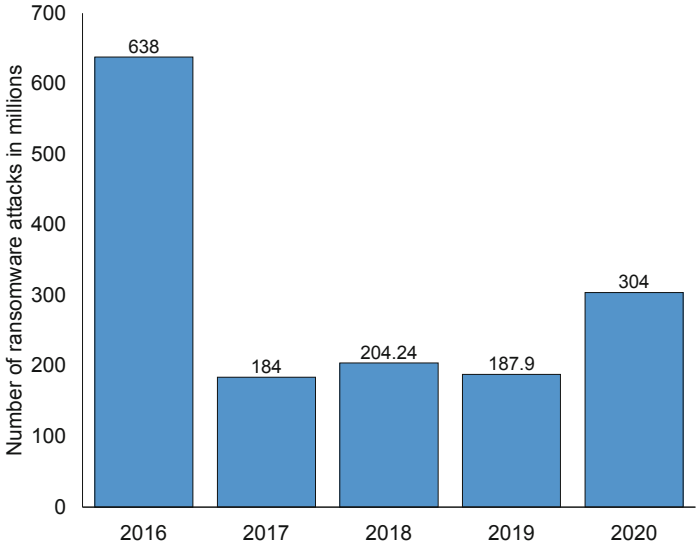

Fig. 1. Number of ransomware attacks per year 2016–2020

Moreover, according to the latest crypto-ransomware family analysis reported by the Kaspersky Lab in [15] April 2021, the number of specific users that confronted ransomware on their devices was "1,091,454" a decrease compared to "1,537,465" in 2019. Among these numbers, to date of the Kaspersky's report, WannaCry holds 21.85% of the share (see Fig. 2), which is the highest infection rate in the history, with damage in overall at least $4 billion across 150 countries.

- ***Money laundering:*** Money laundering is the process of hiding the origins of illicit proceeds (e.g., proceeds of crime), usually via a complex sequence of transactions (including those involving cryptocurrency).
- ***Firearms trafficking:*** It has been known that the dark web has been abused to facilitate the trading of illegal firearms or weapons, and cryptocurrencies are used as payments [16]. For example, according to a study conducted on the international firearms trade by RAND Europe in 2017 [17], the dark web services have reportedly increased the accessibility of weapons for the same prices compared to the black market on the street.

– ***Child pornography/abuse/exploitation):*** It has been known that cryptocurrencies have been used to pay for commercial child pornography, abuse, exploitation materials and/or services (e.g., over a webcam) [18].

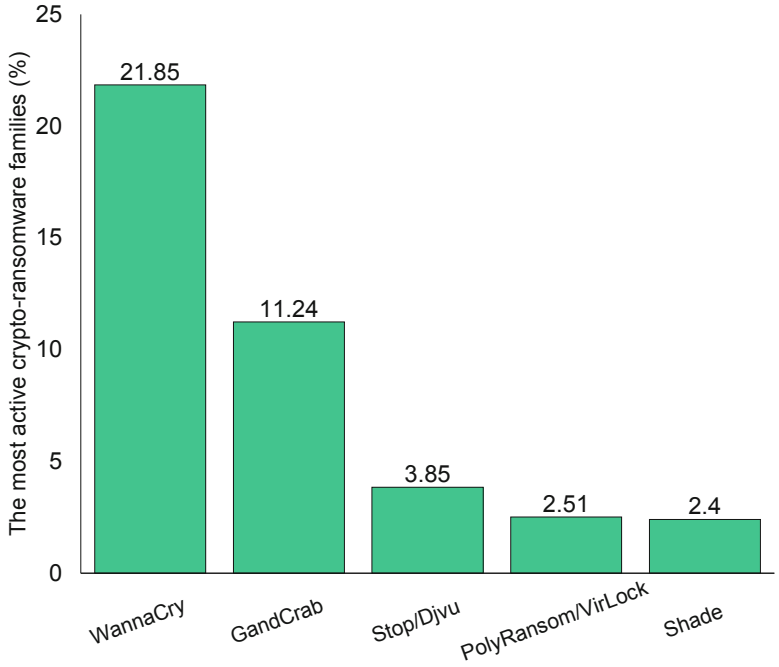

Fig. 2. Five most active crypto-ransomware families in 2020 discovered by Kaspersky [15].

– ***Contract Killers:*** There exist many dark websites that allow one to hire a hitman to murder another person [9]. For example, a White-hat hacker named "bRpsd" reportedly helped the FBI to arrest several hitmen in May 2016 by hacking into the "Besa Mafia" site on the dark web, and leaking contract information such as user accounts, client messages and other information. This hidden website provided a link between hitmen and clients, and the price of a murder service reportedly ranged between 5,000$ and 200,000$. In addition, it was reported that one could also employ a contractor to mug (instead of murdering the victim by paying 500$ or to set a target car on fire for 1,000$ [19].
– ***Human trafficking:*** This is an online black marketplace where criminals utilize hidden websites to sell human trafficking services, for example in organ trade or sex trafficking [20]. According to the U.S. State Department [21], there were 118,932 victims of human trafficking in 2019. However, only 11,841 traffickers were prosecuted with only 9,568 successful convictions. It has been

also observed that most of the traffickers utilize tools such as encryption and constantly switch between profiles and sites on the darknet to avoid being tracked by law enforcement agencies.

- ***Drug trafficking:*** Like the other criminal activities, the dark web provides an anonymous marketplace for drug dealers (suppliers) and addicts (consumers) to sell or purchase drugs using cryptocurrencies such as Ethereum, Bitcoin, Monero, and Ripple [16,20]. According to Europol's January 2021 report [1], "DarkMarket.onion" was the largest online drug black market that has been shut down by law enforcement agencies in a collaborative operation involving the United Kingdom (the National Crime Agency), the U.S. (DEA, FBI, and IRS), Germany, Denmark, Moldova, Australia, and Ukraine. In addition, it was revealed that "DarkMarket" had +500,000 users, 24,000 dealers, and 320,000 transactions. Among these transactions, more than 4,650 Bitcoins and 12,800 Monero tokens were paid.
- ***Hacking community services:*** There exist a number of hacking forums or communities throughout the dark web that provide underground marketplaces for trading different tools or services, as well as stolen/leaked information – see also Table 1 [22,23].

3 Cryptocurrency: A New Stage for Economic Globalization

Over the last decade, the globalization of online markets, and the use of cryptocurrencies as untraceable payment systems have increased their international popularity and changed the face of the digital economy and black market trade by developers who are involved in controlling various types of criminal cartels [20]. As a result, the popularity of cryptocoins and their international availability have led to the very dynamic increase in value, that rise in pressure on them from global regulatory bodies and governments.

However, law enforcement agencies and regulatory organizations have sometimes taken quite severe and differing countermeasures to limit or ban trading with cryptocurrencies in various economic unions and countries such as the EU, China, the USA, and more. But these efforts have technically failed as the number of cryptocurrency trades and their market values have exponentially increased and have had a revolutionary global impact over the last two years [24]. These regulatory agencies are expected to ponder whether their actions and multinational policies have made any impact or demonstrate benefits to the world digital markets. These agencies and governmental bodies are attempting to carefully balance the problems of digital economy control and the perceived downsides of crypto market such as money laundering as a strategy to support terrorism or cybercrimes [25].

Below, we discuss three key, important economic characteristics or determinant factors and none of them can be wholly satisfied by the untraceable cryptocurrencies such as Bitcoin, Ethereum, or Monero. These characteristics

Table 1. Examples of dark web-based forums/markets and their associated services [22, 23]

Name	Examples of services provided	Membership information
Nulled	This is a dark market to trade through sale or purchase hacked or leaked information by cybercriminals. To transact payment operations, this site utilizes cryptocoins such as Litecoin, Bitcoin, and Ethereum	Created: 2015 Members: +3,900,000 Language: English Current status: active
Dread	This is a Tor-based Reddit-style forum where members can post, share, and comment among different groups. While the main aim of Dread is to provide a censorship free forum, it also affords several other services such as pentesting or ethical hacking and selling stolen information	Created: 2018 Members: +15,000 Language: English Current status: active
CrackingKing	This is a tutorial platform that provides tools and educational materials for learning hacking strategies. Also, members can find leaked or stolen information as well as get access to their linked available markets	Created: 2002 Members: +394,000 Language: English Current status: active
CryptBB	This is a private hacking community in which a rigorous application policy is deployed for accepting members who can pass an interview. Also, they recently added a new hidden market on their website named "newbies" for trading drugs using cryptocoins such as Bitcoin and Monero	Created: 2017 Members: +356,000 Language: English Current status: active
FreeHacks	This is a Russian community platform that gathers cybercriminals and hackers to solidify and expand their information in the field	Created: 2011 Members: +200,000 Language: Russian Current status: active
RaidForums	This is an online marketplace for trading cyber attack tools and hacked databases to commit credential stuffing attacks	Created: 2015 Members: +445,000 Language: English Current status: active
XSS.is	This is a Russian forum that provides knowledge on illicit topics related to hacking, malware applications, and financial fraud. Some of such services and tools which are anonymous could only be unlocked by paying for a premium account	Created: 2018 Members: +200,000 Language: Russian Current status: active

can impact the investors' decision-making when they are choosing a target cryptoasset to invest in by highlighting the potential risks.

If we consider cryptocoins as a new type of alternative investment asset, we can define the following three economic factors that can impact the decision-making of

investors: *legitimacy of investment source*, *price explosiveness*, and *correlation of price changes with other assets* such as miners, trading rules and others. Most significantly, the diversifying and hedging capability of these cyptocurrencies cannot be underestimated [12].

In the following points, we briefly explain the determinant factors on the decision-making of investors considering the risk as a multidimensional phenomenon [26]. Technically, we believe that the risk of investments in cryptocurrencies involves key influential factors that can be measured as a function of probabilities and consequences. In other words, we need to discover the factual evidence from the digital currency systems which can be characterized by the following factors.

- ***Legitimacy of investment source:*** This factor involves identifying the trustworthiness of a cryptocurrency system by analyzing the existence of a support agency or a branch that provides online or offline services for investors. In some cases, an investor needs to receive some systematic support where there is a problem with the online wallet-login or transactions such as the case where an online wallet is locked out. It is essential to provide these types of support services to address the possible risks and protect the rights of investors in such systems. For example in Bitcoin, if an investor forgets their wallet password, he or she has no way to reset it or access the owned Bitcoins. In other words, the investor loses all the funds due to forgetting the wallet password [27]. To measure this factor, we assign a binary value (0 or 1) according to the existence of support services for each cryptocurrency.
- ***Price explosiveness or explosivity:*** This factor represents an asset's exponential price increase which involves evaluating the existence of bubbles in cryptocurrency prices by considering its price in several periods. That is, an asset bubble refers to an extreme price acceleration that could not be expressed by the typical primary economic variables [28,29]. The Generalised Supremum Augmented Dickey-Fuller (GSADF) test is used to identify the explosiveness periods which can be expressed as follows:

$$\Delta_t = \mu + \beta \Delta_{t-1} \sum_{i=1}^{p} \delta_{r_w} \beta \Delta_{t-i} + \epsilon_t. \tag{1}$$

  where Δ_t is the price of cryptocoin in time t, and μ, β, δ are parameters predicted utilizing Ordinary least squares (OLS) regression, as well as, p is the number of lags set according to BIC, $r_w = r_2 - r_1$ is a rolling interval window that begins and ends respectively with a fraction r_1 and a fraction r_2 [28]. The $H_0 : \beta = 1$ represents the null hypothesis against $H_1 : \beta > 1$ which indicates explosive bubbles.
- ***Correlation of price changes with other external factors:*** This factor involves measuring effective dependencies such as volume of trades, nature of untraceable trades, and crypto-mining, which can impact the price changes in the crypto market. Since such dependencies involve unique strategies which each cryptocoin utilizes to provide trading services or to attract

investors/traders, the process of measuring the price impact is a very complicated task. Herein, let us assume that the price impact is a behaviorally-based measure which is partially justified according to the Kyle model [30], and relies on two linear economic variables: *traded volume* and *permanent in time* [31]. In the Kyle model, an insider investor and noise investors request orders that are convinced by a Market Maker (MM) in each time step Δt. Therefore, the price adjustment rules Δp of the MM can be considered as a linear impact in the whole signed volume, as follows:

$$\Delta p = \lambda \epsilon v. \tag{2}$$

where λ is an impact measure and is thoroughly proportional to the liquidity of the crypto market. In other words, the price adjustment is somewhat permanent, which is, the price change among time $t = 0$ and $t = T = N\Delta t$.

$$p_T = p_0 + \sum_{n=1}^{N-1} \Delta p_n = p_0 + \lambda \sum_{n=1}^{N-1} \epsilon_n \upsilon_n. \tag{3}$$

In this equation, it is assumed that the impact $\lambda \epsilon_n \upsilon_n$ of trades within the nth time interval continues unabated up to some specified time. According to price manipulation by the [32], the adjustment of linear price in the Kyle model is the only condition that does not permit price manipulation; hence, the *provided impact is constant (permanent)*. This impact stays permanent as the sign of the trades should not be serially correlated if the price is to track an unpredictable (random) path. We refer the interested reader to [31] for checking details of the mathematical proof for the above-mentioned equation. In the Kyle model, the schedule of trading by an insider is exactly such that the ϵ_n is not correlated [30]. However, the real data from markets (e.g., cryptocurrency) shows the sign of correlations of the traded volume during various timescales [31]. According to the theory of modern portfolio introduced by Markowitz [33], the risks of exposure to a specific asset can be decreased by maintaining a varied portfolio of assets; the more independent or less correlated assets, the lower systematic risk, and as a result, the superiority of the diversified portfolio. From a practical perspective, a conventional way to vary the portfolio is through international diversification by maintaining global stocks [34]. Considering the above provable factors, the risks of investments in cryptocurrencies can be assessed more efficiently.

4 Cryptocurrency Trustworthiness Analysis

In this section, we conduct an empirical analysis of the top five most reputed cryptocurrencies (cryptoassets) by considering the determinant factors on the decision-making of investors that we have summarized in Sect. 3.

4.1 Legitimacy Analysis of Cryptoasset Source

To analyze this determinant factor, we have investigated the trustworthiness of each cryptoasset considering the available information related to their transparency and physical location of their company or organization by checking

their official websites and law enforcement agency reports such as through the US Attorney's office and the U.S. Securities and Exchange Commission. Table 2 lists the detailed results of our investigation. During our study, we considered five conventional cryptoassets that are currently receiving a very large volume of trades from investors so far. Among such assets, three of them, including Bitcoin, Ethereum, and Ripple provide untraceable transactions by keeping the identity of users anonymous. They do not offer any tracking or monitoring services for law enforcement agencies in case of emergencies to find criminals who have used such payment systems for covering their crimes [35,36].

On the other hand, two cryptoassets including Tether and Ripple give some transparent services to law enforcement agencies when they present official warrants and prove their legal claim to the information. However, according to the NY Attorney General's report, Tether and Bitfinex deceived investors and the crypto market by exaggerating reserves, concealing roughly $850 million in losses around the world, and NY Attorney General Letitia James subsequently banned all trading activity using such cryptoassets in the state of New York [37,38].

4.2 Price Explosiveness Analysis

To identify price explosivity as a determinant factor, we investigated the price explosiveness of selected cryptoassets (see Table 3), considering economic measures such as the volume of trade, bubbles in the price of assets, and the volatility of price changes during a month period from April 19th, 2021 to May 19th, 2021. To collect real-world data from trustworthy resources, we obtained the volume of trade and price changes by following the same sources as the other references [28,43].

However, the existing price explosiveness analysis measures consider the volume of trade and the real price for calculating the bubbles of financial assets using the Eq. 1, but we believe that the source of an asset is authentic; thus, we can rely upon such measures. Otherwise, because the three evaluated cryptoassets (e.g., BTC, ETH, and XMR) do not offer any regulatory support and financial standards, the use of such measures is technically useless. To prove this assumption, as depicted in Table 3, it can be observed that the price of the evaluated cryptoassets has been changing roughly, i.e., a BTC's price decreased by $17,893 and ETH's price gained $614 during a month.

If we calculate all trade activities over the aforementioned period, the number of financial losses that BTC holders face will be over $100 Million which has been caused by the price manipulation in the meantime. Technically, the blockchain-based cryptoassets (e.g., BTC, ETH, and XMR) can perform a hard fork function [44] to invalidate transactions, since there is no regulatory support for such assets, they can even manipulate the wallet of clients [35–40]. Therefore, the lack of regulatory support and standards opens a lot of concerns regarding their legitimacy and transparency. It has been reported that approximately $400 million of investments in Initial Coin Offerings (ICOs) utilizing Ethereum platform have been stolen by attackers in 2017 [45,46].

Table 2. Legitimacy analysis of conventional cryptoassets' source considering the existence of physical company and their regulatory support.

Name	Description on cryptoasset source/company	Legitimacy analysis
Bitcoin (BTC) [35]	BTC is an open-source P2P Electronic Cash System invented by an unknown individual or a group of anonymous individuals who go by the name of Satoshi Nakamoto. There is no available/known company that physically is affiliated with this system	Release date: January 2009 Transactions: untraceable Current status: active Legitimacy: (×)
Ethereum (ETH) [56]	ETH or Ether is an open-source cryptocurrency platform introduced by a programmer named Vitalik Buterin. In theory, he claimed that Ether enables Distributed Applications (DApps) and Smart Contracts to be designed and executed without any interference, downtime, control, or fraud from a third party. In 2016, an attacker employed a security backdoor/flaw in the DAO project and stole $50 millions of Ether. Later, the ETH community voted to hard fork the blockchain to invalidate the stolen $50 M of Ether	Release date: July 2015 Transactions: untraceable Current status: active Legitimacy: (×)
Ripple (XRP) [39,40]	XRP is a real-time digital-currency-exchange open-source platform designed by Ripple Labs Inc., which is a US-based technology company. The U.S. Securities and Exchange Commission regulated the Ripple Labs Inc. and incorporated it in the state of Delaware by issuing a license number "SEC-CIK #0001685012" in October 2016	Release date: December 2012 Transactions: transparent Current status: active Legitimacy: (✓)
Monero (XMR) [36]	XMR is a privacy-focused cryptoasset which works based on an open-source mining protocol called RandomX. There is no available known company that is physically affiliated with this cryptoasset. However, there is untrustworthy research which suggests the founder of Bitcoin is also the designer of Monero	Release date: April 2014 Transactions: untraceable Current status: active Legitimacy: (×)
Tether (USDT) [37,41]	USDT is a token-backed cryptoasset issued by Tether Ltd. The USDT was originally named "realcoin" and its website states that it is incorporated in Hong Kong with offices in the USA and Switzerland but without giving details. Basically, Tether aims at maintaining the digital currency valuations stable, i.e., a "stablecoin" which was initially supposed to always be worth $1.00. However, according to the New York Attorney General, "Tether's claims that its virtual currency was fully backed by U.S. dollars at all times was a lie" [38]	Release date: July 2014 Transactions: transparent Current status: active Legitimacy: (✓)

Table 3. Price explosiveness analysis of selected cryptoassets considering a month of volatility [42].

Cryptoasset	Price: April 19th, 2021 at 12:00:00 AM	Price: May 19th, 2021 at 11:00:00 PM	Growth (↑)/Loss (↓) rate	
			1 month (%)	1 month (%)
Bitcoin BTC	$55,384	$37,491	↑ +0.00%	↓ −32.3%
Ethereum ETH	$2,158	$2,772	↑ +28.4%	↓ −0.00%
Ripple XRP	$1.330	$1.215	↑ +0.00%	↓ −9.05%
Monero XMR	$318.98	$240	↑ +0.00%	↓ −32.9%
Tether USDT	$0.9998	$1.002	↑ +0.003%	↓ −0.00%

4.3 Correlation of Price Changes with Other External Factors

Technically, there are external influential factors such as the open-source structure of the platform (e.g., BTC, ETH, XRP, XMR), crypto-miners (e.g., BTC, XMR) and so their correlation with price changes is questionable. Below, we describe the correlation of the aforementioned external factors on price changes in detail.

- ***Open-source-based cryptoassets:*** In general, open-source software is a type of program in which source code is openly published under a license so that the main designer - whether it is a company, a person, or a copyright holder - will allow other end-users the rights to study, change, use and share it for any purposes. Since most cryptoassets have been developed based on open-source protocols such as BTC, ETH, XRP, and XMR, they are susceptible to reverse engineering attacks. In other words, attackers can easily find the source code of cryptoassets systems and study their security flaws to implement the *hard fork* or crack wallet passwords [10]. Due to the emergence of open-source crypto-projects, greedy strategists are developing similar ideas and try to attract more investments for these platforms every day. This feature is the main reason for the appearance of +700 cryptoassets and their often rapidly changing valuations. On the other hand, the anonymity of such cryptoassets keeps their owners identities invisible and protects them from being caught by law enforcement agencies in the case where any kind of fraud or abuse happens [47].
- ***Crypto-miners*** are machines (e.g., Bitwats [BT, DBT, CBT]) or software (e.g., Kryptex, BitMine, ECOs) which help clients to mine cryptocurrency to make a small amount of crypto-coin per hour without spending any money for it. In other words, miners make profits by completing "blocks" of verified transactions that are newly added to the blockchain. In practice, the designers of cryptocurrencies utilize such miners to cover the traceability of transactions. There exist two mechanisms for mining: *i)* solo-mining (or mining alone), *ii)* joining a pool. Utilizing a mining pool instead of solo-mining mechanisms has several privileges: it raises the possibility of receiving payments for mining and decreases the necessity of a specific mining machine.

However, the use of a mining pool is not always beneficial since it depends on several variable characteristics such as the computational power needed for mining complexity as well as the current hash rate of the pool. The high number of clients in pools are to be expected to mine a block rapidly, but the amount of mined reward is lower than solo-mining. Recently, due to the profitability, convenience, and pseudonymity of cryptoassets, they are becoming ideal targets for cybercriminals such as ransomware operators. Moreover, the increasing popularity of crypto-coins and the development of malware can result in the infection of their infrastructures or devices by turning them into a covert form of mining machines [47,48].

According to the Micro Trend report in 2017, 4,894 Bitcoin miners were discovered, which generated more than 460,259 Bitcoins by undercover mining activities. Moreover, the report mentioned that over 20% of such miners were related to a network or web-based cyberattack [47]. Similarly, according to the latest Avira Protection Labs report on 25 January 2021 [48], they registered a 53% increase in cryptomining malware-based cyberattacks in Q4-2020 compared to Q3-2020. They believe that while several Bitcoin holders are struggling to access their wallets [27], the price of one Bitcoin was valued about +$36,000. Later, its price reached +$63,000 on 15 April 2021, which is the highest growth rate in this cryptocurrency's history [42]. Unsurprisingly, the Avira team speculated that there exists a connection between the number of crypto-mining malware activities and Bitcoin's fast price rise.

5 Discussion and Future Suggestions

Currently, the dark web and cryptoassets are one of the main sources of anonymous activities and the Tor browser is freely available for downloading on the Internet. Consequently, due to such hidden services, the public is becoming intensively concerned about how they can protect their information and investment funds in the digital world. However, law enforcement agencies such as the FBI, Europol, and Interpol have expended a significant level of effort to reduce the risks on both global economic systems as well as reduce the humanitarian costs these systems generate. However, there are still a number of opportunities in the dark market and cryptoasset ecosystems (see Table 1, and Table 2) which could allow cybercriminals to take advantage of such services and further violate human rights without being apprehended by law enforcement agencies. Below, we discuss various open challenges and suggest possible countermeasures to reduce the risks of the dark web and cryptoassets.

– ***Regulatory limitations and Internet governance:*** Governments or regulatory organizations must introduce strategies for regulating user activities on the dark web. As we mentioned in Sect. 2, the number of dark markets is increasing dramatically as well as an increase in the various types of crimes taking place through such hidden web services without being adequately monitored. Therefore, they must be suppressed by newly developed cyber forensics tools so that the privacy of innocent users is protected and both traditional as

well as cybercriminals are caught as quickly as possible. For example, the FBI utilizes a Computer and Internet Protocol Address Verifier (CIPAV) tool for identifying the location of users who have disguised their identity by employing Tor network services or proxy servers [20]. The abilities and resources of law enforcement agencies such as China's Ministry of Public Security (MPS), the FBI, Europol, and Interpol among others can be merged and coordinated efficiently to deploy their defensive policies or cyber-forensics tools for monitoring such services [1,49]. Moreover, it is important that many governments around the world must cooperate with the aforementioned law enforcement agencies to mitigate the risks of dark web services.

– ***Cryptocrimes and ransomware attacks:*** The crypto market has faced an unbelievable growth in terms of the total volume of trade in 2020 due to the increasing thousands of investors who are turning to crypto-coins every day as a method through which to store market place assets of value during the COVID-19 crisis. Nevertheless, the rise of money through digital exchanges provides a potential target or opportunity for both traditional as well as cybercriminals looking to execute scams, frauds, and asset theft. Statistics have shown that fraud was one of the leading cybercrimes in 2020, followed by theft and ransomware attacks [50,51]. According to statistical data reported by CipherTrace's annual Crypto Anti-Money Laundering and Crime Report in 2021 [50], $1.9 Billion was stolen by the crypto criminals in 2020, which had decreased compared to $4.5 Billion in 2019. Similarly, such crimes reached a value of $1.7 Billion through the facilities of the crypto market in 2018, and this amount increased approximately 165% in 2019 [51]. Note that such statistical data implies that there exists an urgent necessity for "heavy-handed" tools to be utilized by law enforcement agencies for suppressing such crypto crimes by blocking dark web-based hacking forums and websites (see Table 1). In general, most of the hacking service providers do not communicate via common messaging applications about selling their ransomware or malware products. They employ encrypted messaging platforms such as Telegram to have covert conversations with their clients that are beyond the reach of law enforcement agencies. Technically, often these new generations of malware have no generic patterns or abnormal activities since they are customized according to the requirements of the buyer and thus gain the advantage of being difficult to detect. Moreover, hacking service providers present various means to compose convincing content for phishing cyberattacks utilizing legitimate documentation and authentic invoices [3,20]. To defeat these kinds of phishing attacks, we strongly recommend law enforcement agencies establish special task forces for tracking and blocking various methods of payment through legitimate and pseudo-legitimate payment systems which are being used by phishing attacks for money laundering through the crypto market. While law enforcement agencies have taken a number of mitigation actions to reduce such cyberattacks, the aforementioned statistics provide sufficient evidence that they have failed to significantly reduce or eliminate these threats so far.

– ***Increasing awareness of investors:*** During our investigation, we found that most investors do not have sufficient knowledge regarding the legitimacy of cryptocurrencies and their associated risks in large part due to a large magnitude of advertisements which highlight only the fast growth and the potential profits without sufficiently outlining the risks involved. Moreover, they are not aware that some anonymous cryptoassets are used by criminal organizations for payment services as well as investment instruments and are likely to increase the number of traditional and cybercrimes crimes committed every day. It is apparent that a small group of such cryptocurrency clients do not even care about the source of their investments and they are simply looking to profit from such assets as a "*safe heaven*" [12]. Let us ask a key question of investors who would like to invest in anonymous cryptocoins such as Bitcoin, Ethereum, Monero, etc. [1]. If they know that a financial asset supports underground criminal organizations in covering hacking services, money laundering, contract killers, drug-dealers, and other illicit and investing their money in these ecosystems? Also, there are other risks of losing their money through online facing insecure wallet policies such as no password reset strategy or legitimate support services such as offering assurances that they can shut down their system overnight or invalidate transactions using a *hard fork* such as ICOs did in 2017 [45,46]. The risks of cryptocoin loss have become the primary concern of cryptocurrency holders as well as the research community. To reduce the amount of investment in ambiguous cryptoassets with high risk, investigators must utilize provable determinant factors (see Sect. 3) and introduce risk assessment models such as AI-based fuzzy expert systems for providing efficient multiple criteria decision-making which can convince new investors to make reasonable decisions when they are investing in cryptoassets. Moreover, governments must take proper actions by facilitating an increasing awareness of people for creating a stable and reasonable balance between the trustworthiness of these systems as well as considering new proactive procedures and regulations in investment policies and restrictions regarding the use of the crypto market in the near future.
– ***Cryptocoins as a threat to humanity:*** Cryptoassets technically rely upon the integrity of the blockchain for exchanging transactions between clients' wallets. According to a recent technical report by Akamai security intelligence & threat research team on February 2021 [52], cybersecurity experts have discovered a botnet with a new defense mechanism against takedowns that employs the blockchain Ledger. In general, to disable a botnet, security experts take over the server which controls it remotely, and the botnet is disabled when there is no command to execute. However, botnet developers have come up with novel mechanisms to make such countermeasures more difficult to succeed. Since the new generations of botnets operate based on the blockchain ledger, they are globally accessible and difficult to take down. Such botnets seem to be secure against counterattacks. Technically, blockchains are a kind of "distributed ledger technology" in which a record of all transactions must be saved in all blocks since the initiation as well as each transaction requires access to or its available copy. Let us ask a question

here, what if one records a malicious code (or material) into the blockchains?, that is, "poisoning the blockchain". In this case, every Bitcoin holder receives a copy of the malicious code and the security of blockchain fails [46,53]. Nevertheless, China's MPS, the USA's FBI, Europol, and other law enforcement agencies could suppress the cryptocoins into oblivion [1]. But unfortunately, the actions of the aforementioned law enforcement agencies did not stop or significantly reduce the number of trades using untrustworthy cryptocurrencies so far [42], and new cryptoassets are increasing (e.g., +700) every day and opening uncountable dark market spaces for cybercriminals without being controlled. If proper actions against such online crypto market are not taken, criminals can run any kind of illicit operations freely and will damage the legitimate economies of nation-states and negatively affect human lives now and in the future.

6 Concluding Remarks

Thousands of newcomers are reportedly seeking to invest in cryptocurrencies every day. However, many (prospective) investors may not be aware that cryptocurrencies have been used to facilitate a broad range of malicious cyber activities (e.g., ransomware, human trafficking, trading of exploit kits and zero-day vulnerabilities). Hence, in this empirical investigation, we studied the factors that motivate cryptocurrency investment, as well as summarizing the various cybercriminal activities that are facilitated by cryptocurrencies. We hope that this study will contribute towards a better understanding of the risks associated with cryptocurrencies and cryptocurrency investments.

Acknowledgment. This work was supported in part by the National Natural Science Fund of China (NSFC) research fund for International Young Scientists (Reference No. 6211101164).

References

1. Darkmarket: World's largest illegal dark web marketplace taken down (2021). https://www.europol.europa.eu/
2. Cascavilla, G., Tamburri, D.A., Van Den Heuvel, W.-J.: Cybercrime threat intelligence: a systematic multi-vocal literature review. Comput. Secur. **105**, 102258 (2021)
3. Dargahi, T., et al.: A cyber-kill-chain based taxonomy of crypto-ransomware features. J. Comput. Virol. Hacking Tech. **15**(4), 277–305 (2019). https://doi.org/10.1007/s11416-019-00338-7
4. Fröwis, M., et al.: Safeguarding the evidential value of forensic cryptocurrency investigations. Forensic Sci. Int. Digit. Invest. **33**, 200902 (2020)
5. Vesely, V., Zadnk, M.: How to detect cryptocurrency miners? By traffic forensics! Digit. Invest. **31**, 100884 (2019)
6. Tziakouris, G.: Cryptocurrencies-a forensic challenge or opportunity for law enforcement? An interpol perspective. IEEE Secur. Priv. **16**(4), 92–94 (2018)

7. Volety, T., et al.: Cracking bitcoin wallets: I want what you have in the wallets. Future Gener. Comput. Syst. **91**, 136–143 (2019)
8. Dalins, J., Wilson, C., Carman, M.: Criminal motivation on the dark web: a categorisation model for law enforcement. Digit. Invest. **24**, 62–71 (2018)
9. Zhou, G., et al.: A market in dream: the rapid development of anonymous cybercrime. Mob. Netw. Appl. **25**(1), 259–270 (2020). https://doi.org/10.1007/s11036-019-01440-2
10. Conti, M., et al.: A survey on security and privacy issues of bitcoin. IEEE Commun. Surv. Tutor. **20**(4), 3416–3452 (2018)
11. The State of Ransomware (2021). https://secure2.sophos.com/
12. Feng, W., Wang, Y., Zhang, Z.: Can cryptocurrencies be a safe haven: a tail risk perspective analysis. Appl. Econ. **50**(44), 4745–4762 (2018)
13. Crypto-Ransomware Attacks: The New Form of Kidnapping (2015). https://blog.trendmicro.com/crypto-ransomware-attacks-the-new-form-of-kidnapping/
14. Annual number of ransomware attacks worldwide from 2016 to 2020 (2021). https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/
15. The most active crypto-ransomware families (2021). https://securelist.com/ransomware-by-the-numbers-reassessing-the-threats-global-impact/101965/
16. ElBahrawy, A., et al.: Collective dynamics of dark web marketplaces. Sci. Rep. **10**(1), 1–8 (2020)
17. International Fire arms trade on the dark web (2021). https://www.rand.org/randeurope/research/projects/international-arms-trade-on-the-hidden-web.html
18. da Cunha, B.R., et al.: Assessing police topological efficiency in a major sting operation on the dark web. Sci. Rep. **10**(1), 1–10 (2020)
19. How a bitcoin whitehat hacker helped the FBI catch a murderer (2021). https://bitcoinmagazine.com/
20. Kaur, S., Randhawa, S.: Dark web: a web of crimes. Wireless Pers. Commun. **112**(4), 2131–2158 (2020). https://doi.org/10.1007/s11277-020-07143-2
21. Beating Human Trafficking on the Dark Web (2021). https://cobwebs.com/beating-human-trafficking-on-the-dark%20web/
22. Online Trade NULLED (2020). https://allwpworld.com/
23. The Top 5 Dark Web Forums (2021). https://webhose.io/blog/dark%20web/the-top-5-dark%20web-forums/
24. Yen, K.-C., Cheng, H.-P.: Economic policy uncertainty and cryptocurrency volatility. Finance Res. Lett. **38**, 101428 (2021)
25. Morton, D.T.: The future of cryptocurrency: an unregulated instrument in an increasingly regulated global economy. Loy. U. Chi. Int'l L. Rev. **16**, 129 (2020)
26. Olsen, R.A.: Investment risk: the experts' perspective. Financ. Anal. J. **53**(2), 62–66 (1997)
27. Lost Passwords Lock Millionaires Out of Their Bitcoin Fortune (2021). https://www.nytimes.com/2021/01/12/technology/
28. Gronwald, M.: How explosive are cryptocurrency prices? Finance Res. Lett. **38**, 101603 (2021)
29. Liu, Y., Tsyvinski, A., Wu, X.: Common risk factors in cryptocurrency. Technical report, National Bureau of Economic Research (2019)
30. Kyle, A.S.: Continuous auctions and insider trading. Econometrica J. Econometric Soc. **53**(6), 1315–1335 (1985)
31. Bouchaud, J.P.: Price Impact. Encyclopedia of Quantitative Finance (2010)
32. Huberman, G., Stanzl, W.: Price manipulation and quasi-arbitrage. Econometrica **72**(4), 1247–1275 (2004)

33. Rubinstein, M.: Markowitz's "portfolio selection": a fifty-year retrospective. J. Finance **57**(3), 1041–1045 (2002)
34. Heston, S.L., Rouwenhorst, K.G.: Does industrial structure explain the benefits of international diversification? J. Financ. Econ. **36**(1), 3–27 (1994)
35. Bitcoin Inc.: Information (2021). https://bitcoin.inc/
36. Monero Inc.: Information (2021). https://www.getmonero.org/
37. Tether Limited. Information (2021). https://tether.to/
38. Attorney General James Ends Virtual Currency Trading Platform Bitfinex's Illegal Activities in New York (Bitfinex and Tether) (2021). https://ag.ny.gov/
39. Ripple Labs Inc.: Information (2021). https://ripple.com/
40. U.S. S.E.C. or EDGAR System (2021). https://sec.report/CIK/0001685012
41. Tether LTD legal supports (2021). https://tether.to/legal/
42. The global crypto market cap, a trustworthy platform for showing the price updates of cryptoassets (2021). https://coinmarketcap.com/
43. Omane-Adjepong, M., Alagidede, I.P.: Multiresolution analysis and spillovers of major cryptocurrency markets. Res. Int. Bus. Finance **49**, 191–206 (2019)
44. Ethereum Inc.: Information (2021). https://ethereum.org/en/about/
45. U.S. Department of Justice, Attorney General's report (2020). https://www.justice.gov/archives/ag/page/file/1326061/download
46. Hackers Have Stolen $400 Million From ICOs (2017). https://fortune.com/2018/01/22/ico-2018-coin-bitcoin-hack/
47. Security 101: The Impact of Cryptocurrency-Mining Malware (2017). https://www.trendmicro.com/
48. Coinminers target vulnerable users as Bitcoin hits all-time high (2021). https://www.avira.com/en/
49. Helping police worldwide understand and investigate digital crimes, Interpol Police (2021). https://www.interpol.int/en/How-we-work/Innovation/Darknet-and-Cryptocurrencies
50. Cryptocurrency Crime and Anti-Money Laundering Report (2021). https://ciphertrace.com/
51. crypto-criminals stole $1.9B (2020). https://www.finaria.it/
52. Bitcoins, Blockchains, and Botnets (2021). https://blogs.akamai.com/
53. Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems, MIT Working Paper (2021). https://web.mit.edu/smadnick/www/wp/2019-05.pdf