

DARKWEB

**A Guide to Dealing with the
Dark Spot on the Deep Web**

NICK MATTHEW

DARK WEB

A Guide to Dealing with the Dark Spot on the
Deep Web

NICK MATTHEW

Contents

[Management summary](#)

[List of terms and explanation](#)

[TERM EXPLANATION](#)

[introduction](#)

[initial position](#)

[issue, controversy](#)

[Objectives of the work and expected Results](#)

[content part](#)

[Explanation of terms and their mutual demarcation](#)

[The deep web](#)

[The dark web](#)

[Original idea of the deep web and the Tor technology](#)

[Explanation of the gate technology](#)

[Top-level domain .onion](#)

[Search engines in the deep web and dark web](#)

[Systematic consideration](#)

[Useful areas of application and their justifications](#)

[Guide for the general Internet user in dealing with the Darknet and the Tor technology behind it](#)

[Two personas to describe the general_____Internet user](#)

[Step-by-step instructions:](#)

[How can I come in what Should I put attention on?"](#)

[Step 1: create awareness of anonymity](#)

[Step 2: Download and install VPN](#)

[Step 3: Download and install Tor Browser](#)

[Step 4: Find and Visit Onion Websites](#)

[Step 5: Do not resize the Tor Browser window](#)

[Step 6: Disable JavaScript in Tor Browser](#)

[Step 7: Disconnect or cover the webcam](#)

[Step 8: Disconnect or cover the microphone](#)

[Step 9: Do not use personal information](#)

[Step 10: Buy goods and pay on the dark web](#)

[Conclusion / Recommendations](#)

[Dangers, legal aspects,](#)

[recommendations anden_____general internet user](#)

[Conclusion, final word](#)

[Appendix A:](#)

[An order in Dark web do as part of a self-experiment](#)

Management summary

There is a lot of media coverage of the dark web. In the meantime, the general public seems to be aware that, among other things, illegal business is taking place on the Darknet. However, very few people know that the underlying original idea of more anonymity when using the Internet was not illegal and that the dark web is only a small part of the so-called "deep web".

The Deep Web contains the data on the Internet that can no longer be found using normal web search engines. This is the case, for example, as soon as a website requires a login, which means that 90 to 99 percent of the data on the Internet is now used for Count Deep Web.

The dark web is a part of the deep web that not only cannot be found via web search engines, but also deliberately wants to be invisible. In order to be able to access the areas of the dark web, special software is required, such as the Tor Browser. The data traffic runs encrypted and via countless, randomly selected computers. This makes it difficult to monitor and trace information about communications.

State censorship, such as that which prevails in authoritarian countries with non-existent freedom of opinion and information, can be circumvented in this way. Thanks to such anonymous, untraceable communication channels, politically persecuted people can exchange information with each other, organize themselves and, if necessary, create counter-movements to dictatorships or repression. There are those who believe that the dark web contributes to the functioning of a modern democracy. The Darknet can be understood as a mirror of society. In the supposedly anonymous and protected environment, what is already slumbering deep inside a person is offered and disclosed. Accordingly, so-called "hidden services", i.e. services which should remain hidden from the public. Drugs are at the top of the list and are therefore the goods traded the most on the Darknet.

The general Internet user will find various tips and tricks in step-by-step instructions that show how to get into the dark web and how to be as safe and anonymous as possible.

The Darknet is not a legal vacuum and has become the focus of investigative

and prosecuting authorities. The latest reports show, for example, that investigations are being carried out on the Darknet and that they are always successful.

In discussions about the dangers of the dark web, one can consider whether it would make sense to simply ban the dark web altogether. However, a ban does not change the people who move on it and their attitude. It just shifts the action to a different location. Everyone has to decide for themselves whether the Darknet should be banned. Open questions provide food for thought and at the same time form the conclusion of the present certificate work.

List of terms and explanation

EXPLANATION

coin	Digital currency and name of the decentralized accounting system that can be used worldwide
blacklisting	Black list, blocked list of people or things that should be disadvantaged in any way compared to those not listed
rowsers	Computer program for displaying websites on the World Wide Web
DarkNet	Synonym for «surface web». Whenever possible, the term "surface web" is used in this certificate work.
DarkWeb	Synonym for «surface web». Whenever possible, the term "surface web" is used in this certificate work.
clients	End device that requests services from a server
crawler	Synonymous with «Spider», computer program that automatically searches the World Wide Web and analyzes websites.
DeepWeb	Part of the internet that cannot be found by normal web search engines. This is especially true for websites that are protected with a password or are on an encrypted network (darkwebnews.com, n.d.-b).

k web Part of the deep web that is deliberately hidden and whose IP addresses are anonymized. Special software (browser Tor, I2P, Freenet) is required for access (darkwebnews.com, n.d.-b).

kNet Alternative spelling of «Darknet». Whenever possible, the spelling “Darknet” is used in this certificate work.

kWeb Synonym for «dark web». Whenever possible, the term “Darknet” is used in this certificate work.

row Escrow means trust or deposit. Some marketplaces on the dark web offer this service. The amount paid by the buyer is blocked for the seller until the buyer has confirmed that he has received the goods in perfect condition.

fake Fraud, Fraud, Fake

ker Person attempting to gain access to computer systems. Can be positive or criminal in nature.

idress Address in computer networks which – like the internet – is based on the internet protocol (IP).

Internet Global network of computer networks

link Short for hyperlink, a cross-reference that allows you to jump to another electronic document or to another location within a document

Files Contains the automatically maintained log of all or specific actions of processes on a computer system.

on	Special-use top-level domain for using hidden services in the anonymization service The Onion Routing (Tor)
er	Computer that provides computer functionality such as utilities, data, or other resources for other computers or programs ("clients") to access, usually over a network.
ler	Synonym for «crawler», computer program that automatically searches the World Wide Web and analyzes websites.
faceWeb	Part of the Internet that lies on the surface, is publicly accessible and/or accessible via web search engines.
il	The Onion Routing, network for anonymizing connection data
TE	Alternative spelling of «Tor». Whenever possible, the spelling “Tor” is used in this certificate work, as this corresponds to the official spelling of “The Tor Project” (The Tor Project, 2018b).
N	Virtual Private Network, virtual private (self-contained) network that enables a point-to-point connection for secure data transmission
browser	Computer program for displaying websites on the World Wide Web

www world wide web

introduction

il position

The Darknet: «What is it?», «How do I get in there?» and «Are there really only illegal goods there?». The general internet user will ask himself these or similar questions when he hears the word «Darknet». It seems that the general public has little to no knowledge of the dark web. However, the name suggests that it will be something dark, forbidden, illegal. Only those who deal more intensively with the topic know that the original idea – namely more anonymity when using the Internet – was not illegal and that the dark web is only a small part of the so-called “deep web”.

, controversy

In most German-language popular media, the terms Darknet and Deep Web are used synonymously. In reality, however, the dark web and deep web are by no means identical.

Because the Darknet is only a small part of the Deep Web and it has a bad reputation: the Darknet is supposed to be a marketplace for scoundrels, bandits, dealers, murderers, rapists and other people involved in illegal activities. This comes up again and again in everyday conversations. However, the fact that the original idea and the associated anonymization technique called "Onion Routing" or "The Onion Routing" or "Tor" for short was a thoroughly legal and benign one seems to elude the knowledge of the general public.

Need to be part of their own lives or fear that of their informants
Politically oppressed or dissidents, Oppositionists from dictatorship-led countries, journalists, whistleblowers

Must reckon with criminal
consequences and violence
Dealers, murderers, pedophiles, buyers
and consumers of illegal goods and
services

It is relatively easy for the general Internet user to acquire sufficient (semi-)knowledge by means of Internet research in order to access the Deep Web. Once in

Deep Web, the step into the dark web is a small one - and the dangers and legal aspects of dealing with the dark web are likely to be little or not known.

Various reports on the success of searches on the dark web have raised voices after a ban on the dark web. But there are also other opinions that find that the dark web as a whole helps to evade control and censorship. Accordingly, a ban on the underlying technologies would be an attack on modern democracy («INTERVIEW ON ADVANTAGES OF DARKNET», 2017).

Objectives of the work and expected Results

The certificate work deals with the original idea of the Tor anonymization technology and shows the distinction between the two terms "Deep Web" and "Darknet" and their classification on the Internet. The various purposes (legal and criminal) should be explained. It is important for the author to be able to show that the basic idea is fundamentally of positive origin.

The result is a guideline for dealing with the Darknet, which shows the

general Internet user the advantages of the Tor technology and how to use it for legal purposes. In a step-by-step guide, the general internet user learns what is needed to enter the Deep Web and Darknet. He gets a rough overview of how it works and how to navigate and also learns which dangers and legal aspects need to be taken into account. In a self-experiment, an order is placed via the Darknet. The knowledge gained from this will also be included in the guideline.

content part

anation of terms and their mutual demarcation

What is behind the terms "Deep Web" and "Darknet" and how they differ from each other is explained below:

The deep web

The Internet as a whole consists of myriad networks (Shuler, 2002). The publicly accessible part of the internet is the internet as we know it. Synonyms for this are "Free Web", "Freenet", "Visible Net", "Surface Web", "Clear Web" and "Clear Net". It can be seen from the name that this is public data on the Internet that can be found using web search engines.

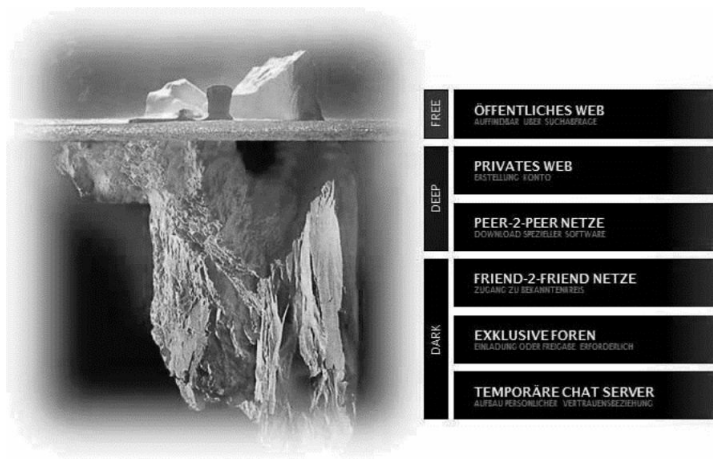
As soon as data on the Internet can no longer be found using normal web search engines, this is referred to as the Deep Web or Invisible Net. This is the case, for example, as soon as a website requires a login, is operated via an unusual port, or is only known to a small group (Ruef, 2016).

Depending on which source you believe, between 90 and 99 percent of the data on the Internet cannot be found via web search engines and is therefore not indexed (20 minutes, 2017; darkwebnews.com, o.J.-a, o.J.-b). In order to call up these websites, the user must know the exact domain or IP address. A search query on a web search engine will not return results containing non-indexed deep web sites.

According to the above definition, the deep web includes all websites protected by user logins, all internal websites and internal data within protected networks of companies, organizations and also private individuals. The majority of the data existing in the deep web therefore has no illegal background.

If you compare the Internet to an iceberg floating in the sea, the invisible part lying under the water surface is the deep web. To get to this part of the iceberg, you have to dive carefully.

Figure 2: Illustration of the Free Web, Deep Web and Dark Web using the metaphor of an iceberg



Note: (Ruef, 2016).

The dark web

The Darknet is part of the Deep Web and is the sum of those networks that not only cannot be found via web search engines, but also deliberately want to be invisible. So-called "hidden services", i.e. services that are intended to remain hidden from the public, are offered here.

The term "Dark Web" used in Figure 2 is equivalent to the term "Darknet". In this certificate work, whenever possible, the term "Dark Web" used.

As with the Free Web and Deep Web, there are corresponding websites on the Darknet. As of January 2018, there were 6,608 dark websites (Hyperion Gray, 2018) on the dark web – quite a number

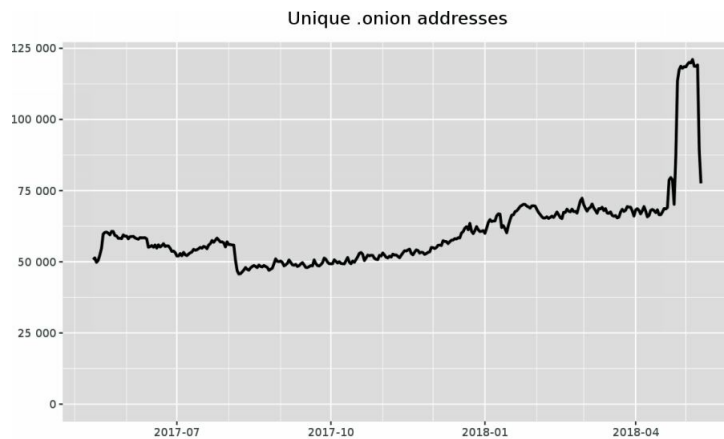
manageable number compared to the 1,876,077,522 (=1,876 billion) active websites (as of May 12, 2018) on the entire Internet (Internet Live Stats, 2018; Netcraft, 2018). The "Dark Web Map" provides an overview of the various dark websites - a kind of digital map with screenshots of all dark websites (Hyperion Gray, 2018).

In addition to dark websites, there are also chat and file-sharing services on the Darknet that are operated as hidden services. Place the 6,608 screenshots

in the Hyperion Gray map

So it only represents an excerpt of the actual Darknet. However, because there is no complete, publicly accessible and searchable directory of the currently more than 75,000 hidden services (according to Figure 3), this excerpt is a useful approximation (spiegel.de, 2018).

Figure 3: Number of unique .onion addresses and development from May 2017 to May 2018



The Tor Project - <https://metrics.torproject.org/> Note: (The Tor Project, 2018a).

In the special friend-2-friend networks (F2F), data is only exchanged decentrally among friends. So you first build up a circle of acquaintances and friends before you can exchange data there (Ruef, 2016).

The private forums are exclusive, invite-only clubs. As long as you don't know anyone who vouches for you, access becomes impossible (Ruef, 2016).

And finally, there are the temporary chat servers. These are set up at short notice and for very specific transactions, only to be switched off again afterwards. Communication is fully encrypted and no logs are created (Ruef, 2016).

In order to be able to access the areas of the dark web, special software is

required, such as the Tor Browser (Reilly, 2017). Applied to the iceberg metaphor shown in Figure 2, this means that the dark web represents the bottom of the iceberg. Special diving equipment is required to dive there.

It turns out that the deeper you go in the Darknet, the greater the effort. Convenience and ease of use are sacrificed in favor of greater security and anonymity. These areas are therefore not attractive for normal activities, but all the more so for actors involved in illegal activities (Ruef, 2016).

Original idea of the deep web and the Tor technology

When accessing the Darknet, the data traffic is encrypted and runs via countless, randomly selected computers. This makes it difficult to monitor and trace information about communications. Especially when communicating with sensitive information as content, no monitoring and traceability is desired. Bypassing state censorship, such as that which prevails in authoritarian countries with non-existent freedom of opinion and information, can also be a motivation for using encrypted, anonymous communication options. For example, during the Arab Spring in Egypt, an increase in communication via Tor technology was observed (Zahorsky, 2011). Arab Spring activists were able to access the usually blocked social media channels via the Tor network and spread their information about the revolution. Whistleblowers (the most well-known of whom is probably the former CIA employee Edward Snowden) also use the deep web to bring explosive information to the public. But politically persecuted people also use the possibilities of anonymous communication channels. Anonymization helps journalists protect their sources. Anonymous, untraceable communication thus plays an important role in avoiding negative consequences from government censorship, reprisals and persecution. Whistleblowers (the most well-known of whom is probably the former CIA employee Edward Snowden) also use the deep web to bring explosive information to the public. But politically persecuted people also use the possibilities of anonymous communication channels. Anonymization helps journalists protect their sources. Anonymous, untraceable communication thus plays an important

role in avoiding negative consequences from government censorship, reprisals and persecution.

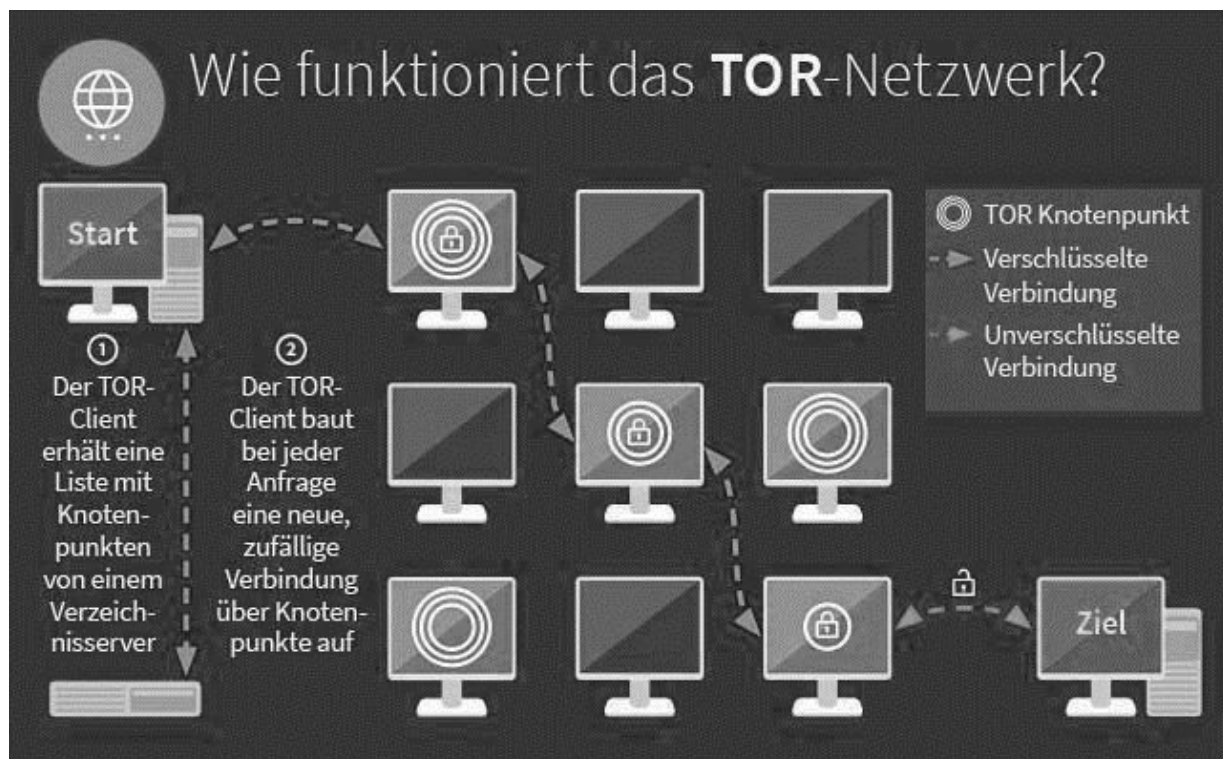
Marc Ruef, co-owner of the company scip AG, which specializes in information security, and lecturer at the HWZ Zurich, answers in an interview with 20 Minuten as follows: "The idea of the Darknet is to be able to exchange information anonymously and uncontrolled." And he adds: «...even in countries with extensive state control and strict censorship, the Darknet plays an important role. A technologically uninhibited exchange of data is an important part of a modern democracy.» (20 minutes, 2017).

Explanation of the gate technology

The anonymization and encryption technology used in the Darknet can be described as a kind of digital invisibility cloak. Tor is dominant. Tor originally stood for "The Onion Routing". The basic idea of the structure is similar to that of an onion: the core of the onion is hidden under several skins. The same applies to Tor: the core, consisting of the identity and activity of the respective Internet user, is hidden under several layers of anonymization (Mey et al., 2017).

The anonymization technique is called onion routing. The web content is routed via constantly changing, random routes - via so-called "nodes". This connection is encrypted and the only unsecured step is the last one: that from the gate Exit node to destination (Bärlocher, 2017). This keeps the true identity of whoever requested the data anonymous to the web server on the other side.

Figure 4: Schematic representation of the connection path from client to client via the Tor network

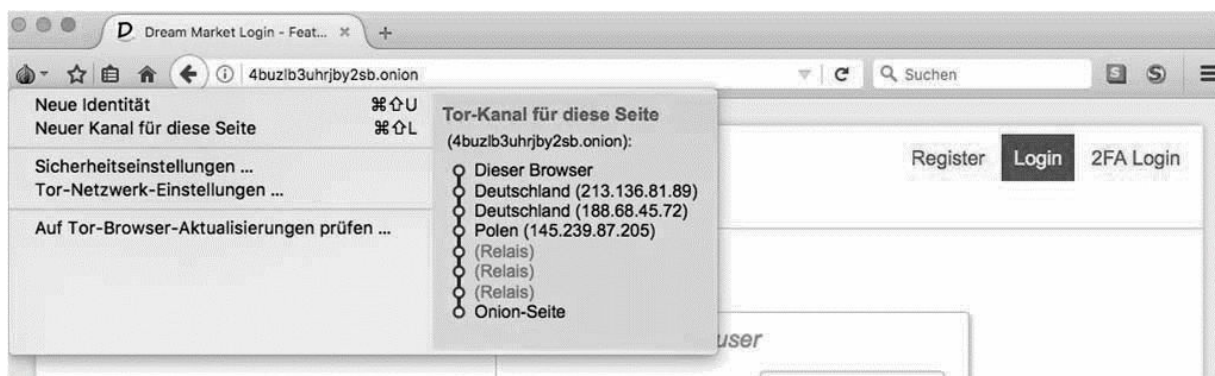


Note: (Eckermann, 2017).

The Tor nodes only know the last step, i.e. from which node the path comes, but not its beginning and its destination. No node ever knows the entire path. Each hop from node to node is provided with an encryption negotiated specifically for this connection, which makes tracing the path extremely difficult if not impossible (Bärlocher, 2017).

The connection path through the various randomly selected nodes can be viewed at any time in the Tor Browser:

Figure 5: Screenshot of the connection path in Tor Browser



Note: Own screenshot from Tor Browser.

Top-level domain .onion

The well-known top-level domains (.ch, .com, .de., .org and so on) do not exist in the Tor network. There is a single top-level domain for this: .onion.

The URLs for the various dark websites of the Hidden Services consist of a seemingly cryptic sequence of numbers and letters. The marketplace Dream Market, for example, can be reached via various URLs [removed for publication] or other onion addresses. It often happens that the onion addresses in the Darknet change frequently or so-called "mirror links" are used as alternative links. This is a precautionary measure taken by the marketplace operators to make things a little more difficult for investigators.

Search engines in the deep web and dark web

Yes, they exist: the search engines for the deep web. However, the deep web and thus also the dark web are deliberately difficult to search, which is why

search engines are often less effective than what you are used to from the public web. It is advisable to use several different search engines for each search, since not every search engine shows the same results. Possible search engines in the deep web are, for example, Torch, TorSearch. The previously known search engine called Grams – the most useful search engine on the deep web to date – has been offline since the end of 2017 (Beuth, 2017).

ematic consideration

Useful areas of application and their justifications

People living in Switzerland may wonder why anonymity on the internet is useful or even necessary. After all, apart from possible stalker attacks, there is little to fear in Switzerland. Switzerland is not considered a country at risk of terrorism. Here you can freely spread your own opinion without having to fear for your own life. And there is no danger from their own state either (Bärlocher, 2017). This free life is taken for granted by the Swiss. And this is also evident when you take a look at the Swiss entry in the Open Observatory of Network Interference (OONI) - a global network that has set itself the task of detecting censorship, surveillance and connection manipulation on the Internet and making them visible:

In Turkey, for example, the situation is somewhat different. The Turkey entry on OONI shows a long list of censored websites (Open Observatory of Network Interference (OONI), 2018b):

- porn sites
- Sites about sex education
- Gay dating sites
- File Sharing Sites
- streaming sites
- gambling portals
- Drug education sites, specifically cannabis
- Sites with politically divergent opinions, such as Hizb ut-Tahrir, an Islamist and neo-fundamentalist organization.

It is also known that Turkey completely blocks social networks, Google and various news portals depending on the situation (Frankfurter Allgemeine, 2016). This reflects the prevailing state censorship in Turkey. The regime

around Recep Tayyip Erdogan is trying to nip march protests, rallies and uprisings in the bud. Because if the opposition and those who think differently can't organize themselves and nobody knows that there is a march protest, then nobody goes there. If there is no newspaper or news portal to read that the regime is attacking innocent people, then no one gets upset about it (Bärlocher, 2017).

It is precisely here that anonymous access to the Internet and thus the circumvention of censorship can help people in crisis areas to obtain information and communicate freely. In countries with repression and political turmoil can help Tor allow dissidents and opposition figures to organize and express their opinions freely. The revolution surrounding the Arab Spring would never have happened if it hadn't been for the dark web, where people organized themselves anonymously and safely from the regime (Bärlocher, 2017).

1.1. Illegal uses

Despite the advantages shown and the fact that the Darknet and the associated anonymization is an important pillar for democracy, it is obvious that a lot of illegal things are also happening under the cloak of anonymity.

The Darknet is teeming with a wide variety of offers and retailers. The following figure shows an evaluation by Marc Ruef of the company scip AG to categorize the various goods and services traded on the Darknet. Drugs are at the top of the list and are therefore the goods traded the most on the Darknet.

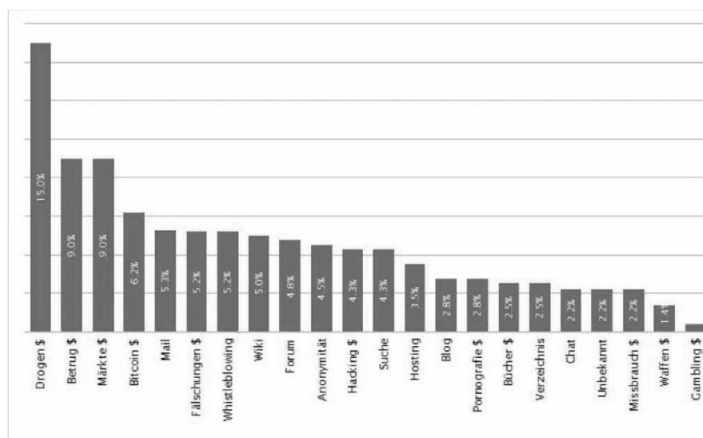


Figure 6: Categorization of

goods and services traded on the Darknet

Note: (Ruef, 2016).

The individual marketplaces work in a similar way to Amazon, for example: There are various offers (listings) with photos, descriptions, information on quality, shipping method, delivery time, etc. Escrow - the deposit of the paid purchase price until the successful delivery of the purchased item - is part of standard in many marketplaces. Vendors can be rated by buyers with stars and comments. Providers who turn out to be scammers (fraudsters) can be blocked by the operators of the marketplaces.

Guide for the general Internet user in dealing with the Darknet and the Tor technology behind it

Two personas to describe the general Internet user

This guide is deliberately aimed at general Internet users, i.e. people with average user usage, without specialist knowledge (no computer scientists, no digital risk managers or other specialist audience). It can also be referred to as "normal consumer". To better illustrate who fits the description of the general internet user and might have an interest in this guide, the following two personas have been created:

-by-step instructions:

How can I come in what Should I put attention on?"

There are countless instructions on the Internet that describe what is required for access to the dark web to succeed. A simple search with a normal web search engine such as Google or Bing is sufficient to find step-by-step instructions. It is therefore extremely easy to access the dark web. The following step-by-step instructions, which pick up on tips and tricks from various sources, will help you to be as safe and anonymous as possible. These are to be understood as advice and should therefore be followed - but they do not have to and do not claim to be correct or complete. It should also be noted that due to the speed of technical developments, one or more pieces of advice may no longer be up to date.

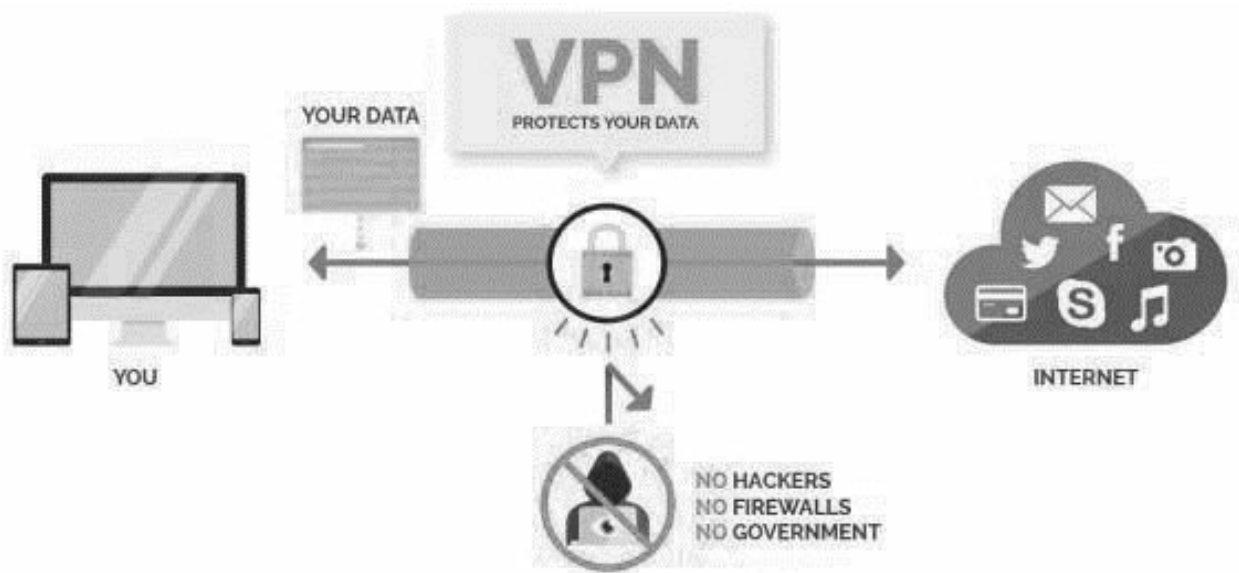
Step 1: create awareness of anonymity

The most important thing when dealing with the Darknet and with the Internet in general is that you are aware that the data traffic can be read anywhere and anytime without suitable measures.

Step 2: Download and install VPN

First of all, a VPN client (Virtual Private Network) should be installed, which is best always used when surfing, regardless of whether you surf via the Tor browser and move on the Darknet or not. A VPN client ensures that the connection to the Internet is encrypted and thus enables communication that is protected against eavesdropping and manipulation (Wikipedia.org, 2018) and this can be an advantage for all steps on the Internet.

Figure 8: Schematic representation of a VPN



When choosing a VPN client, make sure that it does not create any log files, offers fast performance, accepts cryptocurrencies such as Bitcoin, is compatible with the Tor browser and has a kill switch for DNS leaks (i.e. a kind of kill switch that immediately interrupts the Internet connection as soon as the VPN tunnel is not working as it should, until the secure VPN connection is restored (R., 2017)). If the VPN client also offers the option of using a fake IP address, for example that of another country, this further increases protection, since - in the event that the Tor Browser should be compromised - there is no trace of its effective IP address can be traced (darkwebnews.com & Tarquin, 2018). The website <https://topvpnsoftware.org>

shows, for example, the five best VPN clients including ratings and other helpful information for choosing the right VPN client (<https://topvpnsoftware.org>, 2018).

Figure 9: Screenshot of the <https://topvpnsoftware.org> website



Rank	VPN Provider	Price	Features	Compatibility	Countries	Score	More Info
1	IPVANISH VPN	\$5.20 <i>Exclusive 34% discount only via our link!</i>	<ul style="list-style-type: none"> ✓ No Logs ✓ Protects From Tor Vulnerabilities ✓ Hides Tor From ISP ✓ Best Anonymity ✓ T3 Awards Winner 		60	98%	VISIT SITE READ REVIEW
2	NordVPN	\$11.95	<ul style="list-style-type: none"> ✓ Great Speed ✓ Good For Torrents ✓ 24 Hour Chat Support ✓ Bitcoin Accepted 		57	91%	VISIT SITE READ REVIEW
3	STRONG VPN	\$10.00	<ul style="list-style-type: none"> ✓ Fast Speed ✓ Great Support ✓ Easy To Use ✓ Good Privacy 		22	85%	VISIT SITE READ REVIEW
4	PrivateVPN	\$10.95	<ul style="list-style-type: none"> ✓ Good Speed ✓ User Friendly ✓ Good Security ✓ Accepts Bitcoin 		43	74%	VISIT SITE READ REVIEW
5	overplay	\$9.95	<ul style="list-style-type: none"> ✓ Great Speed ✓ Smart DNS Included ✓ Simple To Use ✓ Has "JetSwitch" 		48	66%	VISIT SITE READ REVIEW

Note: (<https://topvpnsoftware.org>, 2018).

Step 3: Download and install Tor Browser

As explained above, special software is required for access to the dark web. Popular web browsers like Internet Explorer, Google Chrome, Mozilla Firefox, Apple Safari, etc. are unable to connect to the dark web websites. An appropriate browser is required: either the more widespread Tor browser, which is the focus of this certificate work, or the lesser-known browsers I2P

and Freenet (Reilly, 2017).

It is recommended to stop all services connecting to the Internet before downloading and only start the VPN client downloaded and installed in step 2 and connect to another country. If the connection is established via VPN, the Tor Browser can be accessed via the official website <https://www.torproject.org> can be downloaded with the common web browser that has been normally used until now. Tor Browser should definitely have the official website <https://www.torproject.org> downloaded because download files from other websites could be compromised.

Installing Tor Browser is no different than installing other popular programs and is simple. From this point on, all the programs required for anonymous access to the Deep Web and Darknet are installed and the Onion websites can be visited immediately.

Step 4: Find and Visit Onion Websites

For the general Internet user, it may seem unusual and strange at first that the usual WWW addresses do not work or do not exist for surfing the deep web and dark web and cannot be found via the common web search engines such as Google or Bing. The various websites in the Deep Web and Darknet are controlled via so-called "onion addresses". In order to find onion addresses, the search engines for the deep web and dark web mentioned in Section 2.5 can be used. Or you can visit one of the numerous public websites on the Internet that are accessible without a Tor browser and list onion addresses for various websites in the deep web and dark web. Such a list with 4'715 links of different categories can be found for example at Darkwebnews.com.

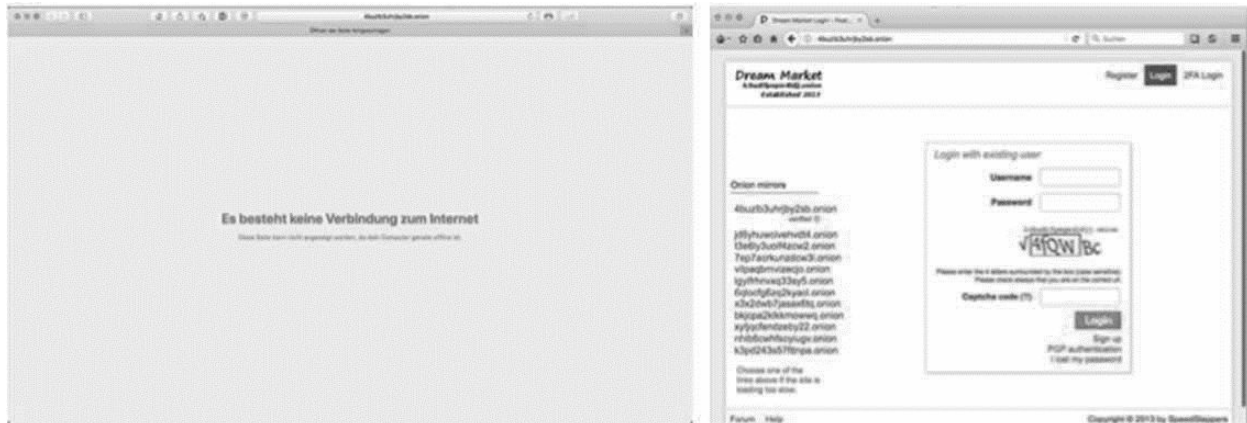
Figure 10: Screenshot of the website <https://darkwebnews.com/deep-web-links>

Name	URL	Description	Goods/Services	Need Registration	Need Invite	Status	Category	Screenshot
#1 Dream Market	http://4buzlb3uhrjby2sb.onion	Dream Market is Marketplace for Drugs, Digital Goods and Other Services.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	
#2 Silk Road 3	http://silkroad7m2puhj.onion/	Silk Road 3 is the DarkNet's most resilient Marketplace. Products are sorted in categories. They sell Cannabis, Stimulants, Ecstasy, Opioids, Benzos, Dissociatives, Psychedelic, Prescription, and Other products.	Drugs, Weapons	Yes	No	Online	Marketplace Drugs	
#3 Valhalla	http://valhallaxmn3fydu.onion/	Valhalla is marketplace for Drugs sorted in categories. There are a lot of Cannabis, Stimulants, Empathogens, Psychedelics, Opiates, Pharmacy, Dissociatives and Depressants.	Drugs	Yes	No	Online	Marketplace Drugs	
#4 Point / Tochka Free Market	http://tochka3evlj3sxdv.onion	Tochka is dark market shipping to all countries. Drugs and other categories are sorted in categories.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	
#5 WallStreet Market	http://wallstylzjhkvrmj.onion	WallStreet Market is one of the newest markets on the darknet and it particularly specializes in digital goods.	Drugs, Digital Goods	Yes	No	Online	Marketplace Drugs	
\$\$\$	http://2jv5rmgnmze5l6l4.onion/	Only old users have access to join this website for cash	-	Yes	Yes	Online	Uncategorized	
\$\$\$	http://2jv5r7k66ralyk3g.onion/	Only old users have access to join this website for cash	-	Yes	Yes	Online	Uncategorized	
\$\$\$	http://2jv5rmgnmze5l6l4.onion	\$\$\$ is Invite only website, only old users have access to join or Invite you.	-	Yes	Yes	Online	Uncategorized	

Note: (darkwebnews.com, n.d.-a).

For example, if you click on the first link (#1 Dream Market, <http://4buzlb3uhrjby2sb.onion>) in the list opens the website of Dream Market, a marketplace for drugs, digital goods and other services. As shown earlier, the website only opens if the link is opened via the Tor Browser. If the link is opened via a common web browser, no website can be displayed, as can be seen in Figure 11 below.

Figure 11: Screenshot of two browser windows comparison (left Safari, right Tor)



Note: Own representation. Important: There are also normal websites on the free web, via which the onion addresses can be controlled and the pages can be displayed in the standard web browser. This may sound simple - after all, there is no need to install the Tor browser - and therefore seems tempting. However, this is not advisable in any respect, as this makes your own IP address visible, anonymity is not guaranteed and you are vulnerable and traceable as a result.

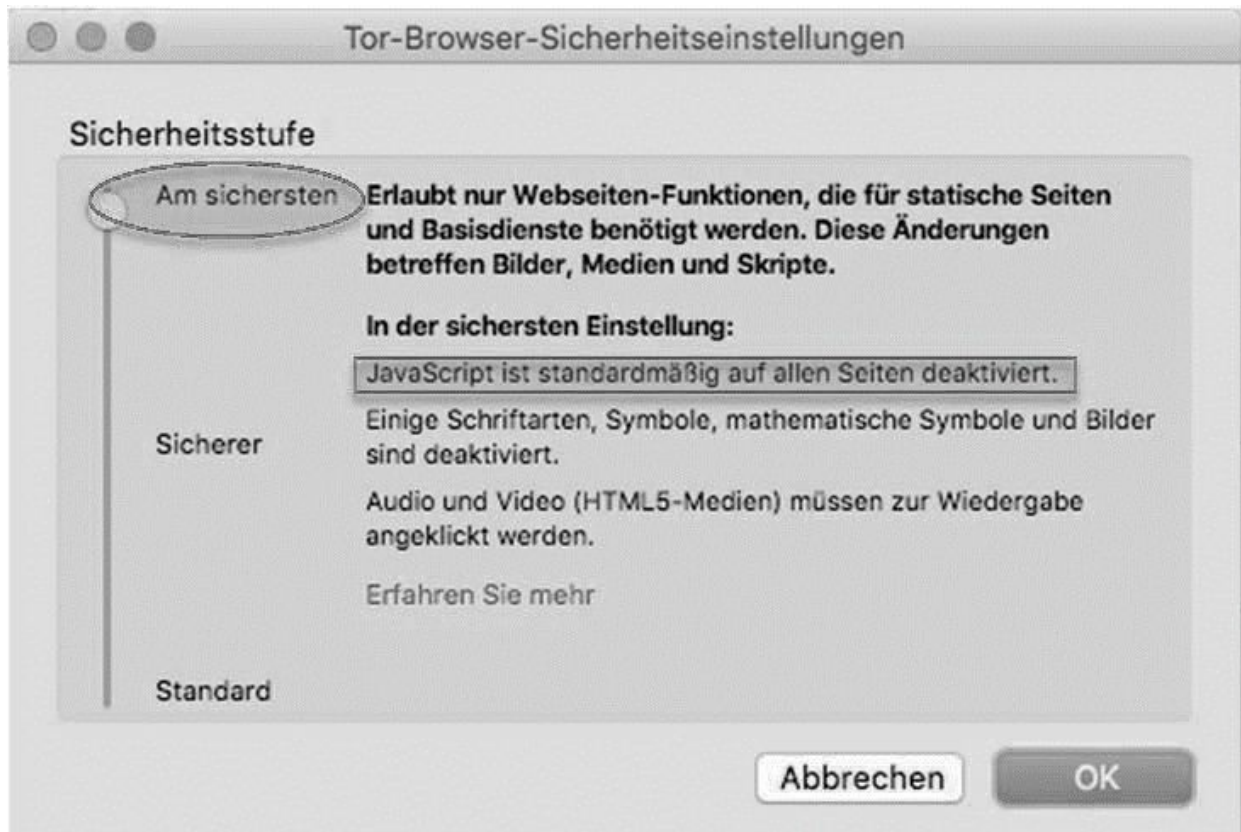
Step 5: Do not resize the Tor Browser window

It may sound strange to the general internet user, but the size that the Tor Browser window opens should not be changed. The reason is that even the smallest changes in the window size mean an individual setting on the individual computer. This individual setting can be discovered and traced by law enforcement agencies. If the window size is not changed, you move with the same default settings as the majority of other Tor Browser users, so you don't stand out from the crowd and cannot be traced back.

Step 6: Disable JavaScript in Tor Browser

It is well known that JavaScript is not very secure (Tung, 2016). Therefore, it is recommended to disable the insecure JavaScript in the Tor Browser in the security settings.

Figure 12: Screenshot of security settings in Tor Browser



Note: Own representation.

Step 7: Disconnect or cover the webcam

Hackers and governments have the technical means to gain access to third-party computers and to activate webcams unnoticed. We therefore recommend either disconnecting the webcam from the computer or - if it is permanently installed in the computer - covering it in a suitable way, for example with black, opaque adhesive tape, a webcam cover (Link:<https://soomz.io/de/>) or other tools.

Figure 13: Webcam covers



Note: (soomz.io, n.d.).

Step 8: Disconnect or cover the microphone

The same applies to the microphone as to the webcam: the microphone can also be activated externally by third parties without being noticed. Accordingly, the microphone should be separated from the computer or - if it is permanently installed in the computer - covered in a suitable way, for example with black, thick adhesive tape.

Step 9: Do not use personal information

If you are too careless in dealing with your personal data, the best VPN client and the latest version of the Tor browser are of no use. Therefore, personal data such as your real name, home address, telephone numbers, photos, the usual e-mail address and the standard password (which, in the worst case, is used for countless services) should under no circumstances be used on the Darknet. It is recommended to use fresh data each time, never used on the dark web. For the e-mail address, we recommend using anonymous e-mail services which, depending on the provider, have Open PGP data encryption, do not create log files, provide spam protection or have other services to protect privacy and anonymity. Such providers can be found on the site <https://darkwebnews.com/anonymous-email> (darkwebnews.com, n.d.-c).

Step 10: Buy goods and pay on the dark web

If you intend to buy goods on the Darknet, there are also important tips for safe payment that should be observed. Cryptocurrencies are used to pay in the Darknet, and the best-known and most widespread is called Bitcoin. How Bitcoins can be acquired is deliberately not dealt with in this certificate work, but reference is made to the relevant documents on the subject.

An important golden rule for staying under the radar of the police and not losing money by closing one's cryptocurrency exchange account is the following: It is recommended never to transfer cryptocurrencies directly from one's exchange account to a marketplace or anywhere else on the dark web (applies also for the reverse direction). Because a direct transfer can be used to track exactly where the cryptocurrency came from or where it went. This can lead to your own exchange account being closed, the credit being lost and further measures (blacklisting, criminal prosecution, etc.) being taken. To avoid this, cryptocurrencies should always be transferred from your own exchange account to a so-called "wallet" and from there to the Darknet.

Conclusion / Recommendations

dangers, legal aspects, recommendations and general internet user

Dangers lurk in the dark web. People of all kinds, often with a criminal motive, cavort here, which is why the Darknet has become the focus of investigative and law enforcement authorities. And the authorities have already succeeded in identifying Darknet users despite encryption and anonymization technologies (Richard, 2017). Because the Tor Browser also has vulnerabilities that could be exploited by hackers, criminals, authorities and others after they became known (Richard, 2018b).

You have to be aware of these dangers when dealing with the Darknet.

The Darknet is not a legal vacuum. There is no such thing as a legal vacuum. Many of the crimes committed using the dark web can be addressed by existing laws. Drugs are grown, sold, shipped, imported and consumed. No new laws are needed for this. This also applies to crimes in the field of cybercrime (e.g.

B. Sale of stolen data). Corresponding laws are in place to punish them (20 minutes, 2017). The following messages show that this is happening:

«FBI Employed CMU To Unmask Dark Web Suspects»(Richard, 2017)

«FBI Hacked Tor and Took Down A Child Sexual Exploitation Site»(Richard, 2018a)

"Switzerland is investigating against dealers on the dark web"(20 minutes, 2018)

However, it is important to remember that if the police are able to use technological means to track down child molesters on the dark web, then authoritarian regimes, for example, can also use the same method to

prosecute freedom fighters (Bärlocher, 2017)

Conclusion, final word

In discussions about the dangers of the dark web, one can consider whether it would make sense to simply ban the dark web altogether. To block access and to criminalize any attempt to somehow gain access. However, it must not be forgotten that a modern democracy is based on the fact that differing opinions and worldviews in terms of morals and ethics can meet on one level without having to feel persecuted (Bärlocher, 2017). The Darknet can be understood as a mirror of society. In the supposedly anonymous and protected environment, what is already slumbering deep inside a person is offered and disclosed. Whether these are criminal intentions or pedophilic desires. Banning the Darknet doesn't change that person or their attitude.

Everyone has to decide for themselves whether the Darknet should be banned. The following questions provide food for thought:

"How much freedom do we want to give up for security, which is then often just an illusion?" (Bärlocher, 2017).

"Is 14 arrested pedophiles worth that hundreds of thousands of freedom fighters live in fear of persecution?" (Bärlocher, 2017).

"Who do we protect and how? And while we're protecting some, who are we putting at risk?" (Bärlocher, 2017).

Appendix A:

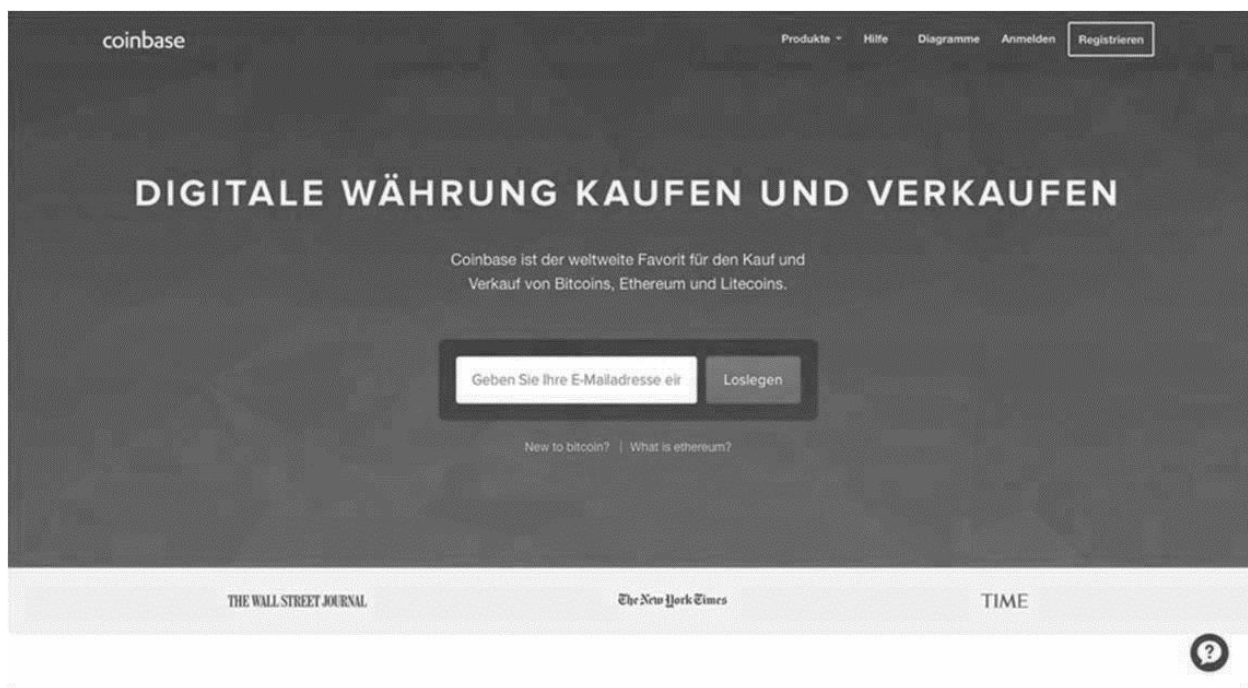
An order in Dark web do as part of a self-experiment

The reader of the present certificate work may ask themselves whether the goods and services offered in the various marketplaces are really genuine and are delivered/executed when ordered. The author has decided to place an order on the Darknet as part of a self-experiment and to incorporate his findings into this certificate work. Since the self-experiment after consultation with the course management has no influence on the assessment of the present certificate work, the resulting findings can be found in the appendix. The following screenshots were created by the author himself and some contain personal data. For self-protection and also in the knowledge that this self-experiment crosses the border to illegality,

«censored» covered.

Coinbase is a marketplace to buy and sell cryptocurrencies like Bitcoin, Bitcoin Cash, Ethereum and Litecoin. It also offers the service of a wallet to keep the purchased cryptocurrencies safe and to make and receive payments.

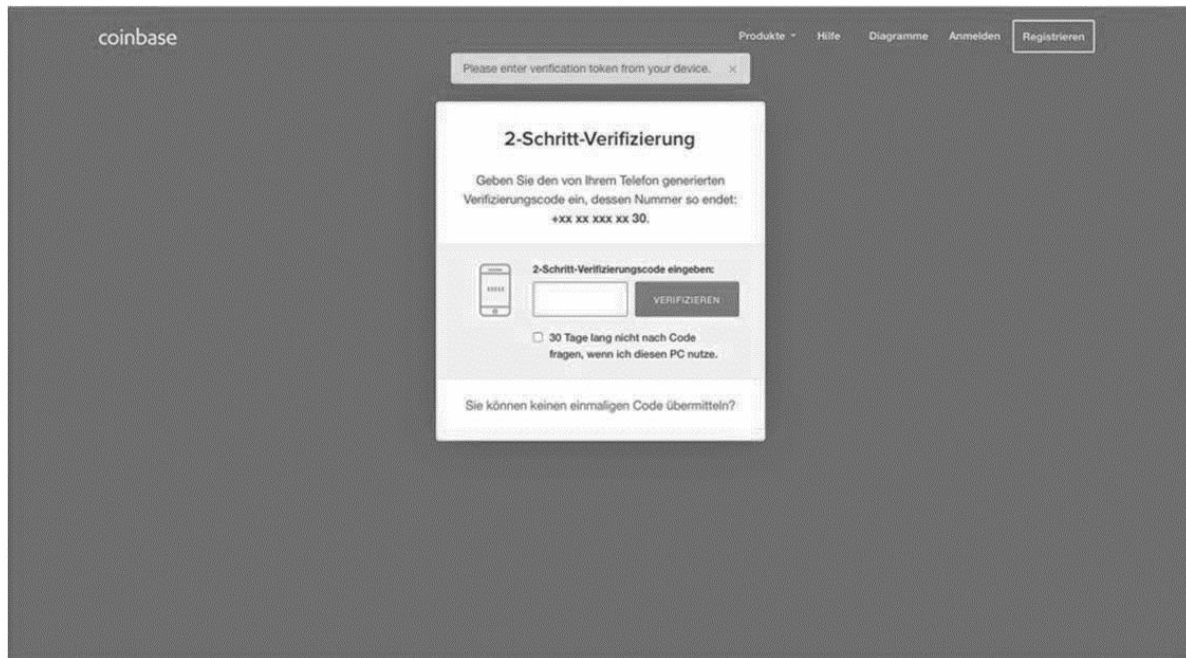
Figure 14: Coinbase login page



Note: (Coinbase, 2018).

The login to Coinbase works with an e-mail address and password as well as a 2-step verification with a one-time code sent via SMS.

Figure 15: 2-step verification at Coinbase



Note: (Coinbase, 2018).

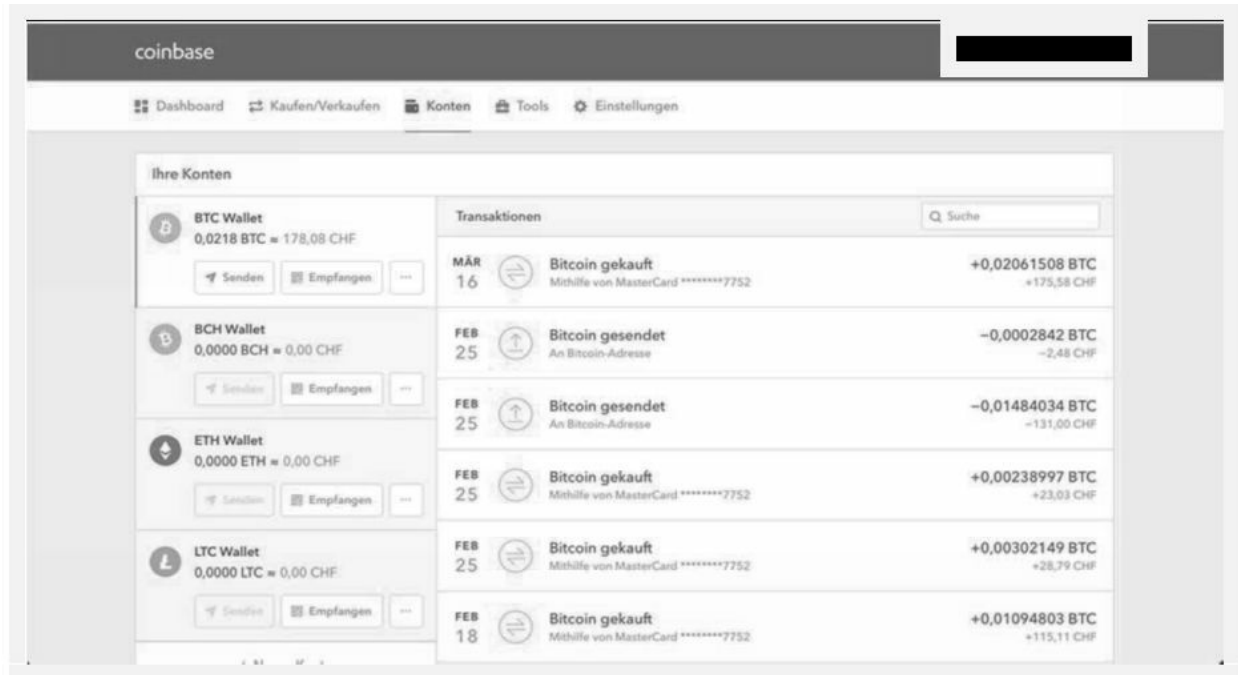
As a further security measure, Coinbase requires that each new device be authorized. For this purpose, an e-mail with a link is sent to the user. The new device is authorized by clicking on this link.

Figure 16: Authorize new device

Note: (Coinbase, 2018).

After logging in to Coinbase, the wallet with the transaction history is visible. It shows the current balance and past transactions (bought bitcoins, sold bitcoins, sent bitcoins, received bitcoins).

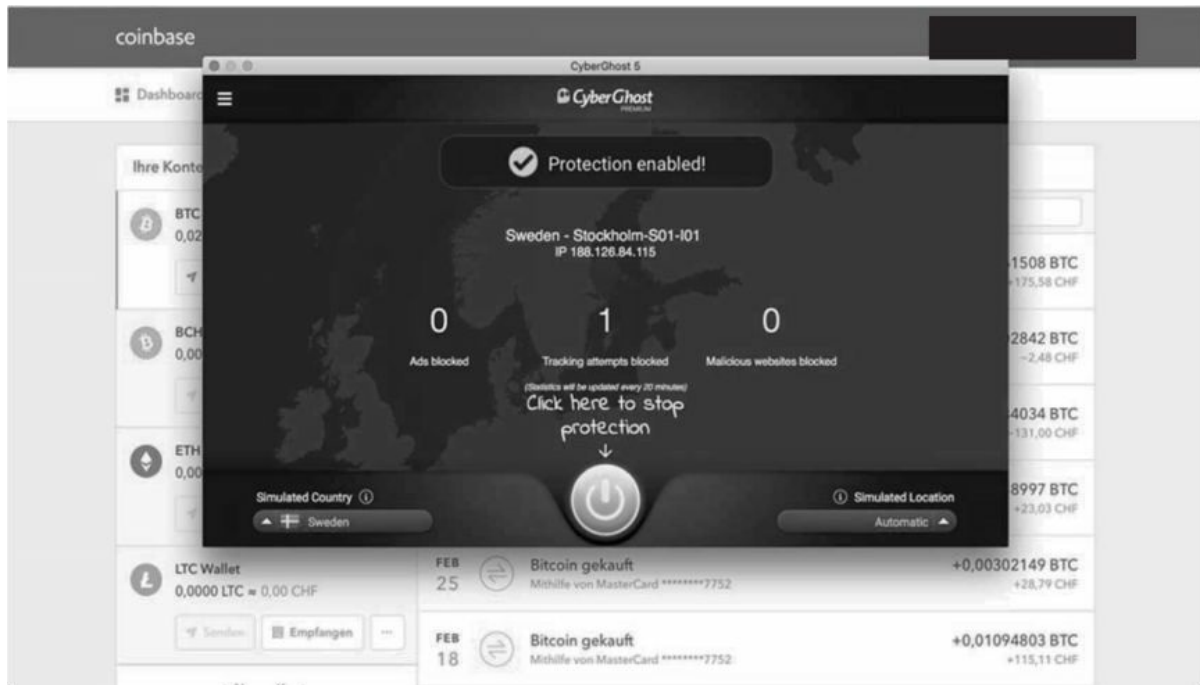
Figure 17: Bitcoin wallet with transaction history



Note: (Coinbase, 2018).

After the Bitcoin wallet has sufficient credit, the step into the Darknet can now be made. To do this, the VPN client must first be opened and activated.

Figure 18: VPN client CyberGhost activated



Note: (CyberGhost, 2018).

Since the VPN connection is established, the Tor Browser can now be started.

During the Tor Browser startup process, it will check for updates. In this case, updates are available and the Tor Browser needs to be updated.

Figure 21: Tor Browser update process

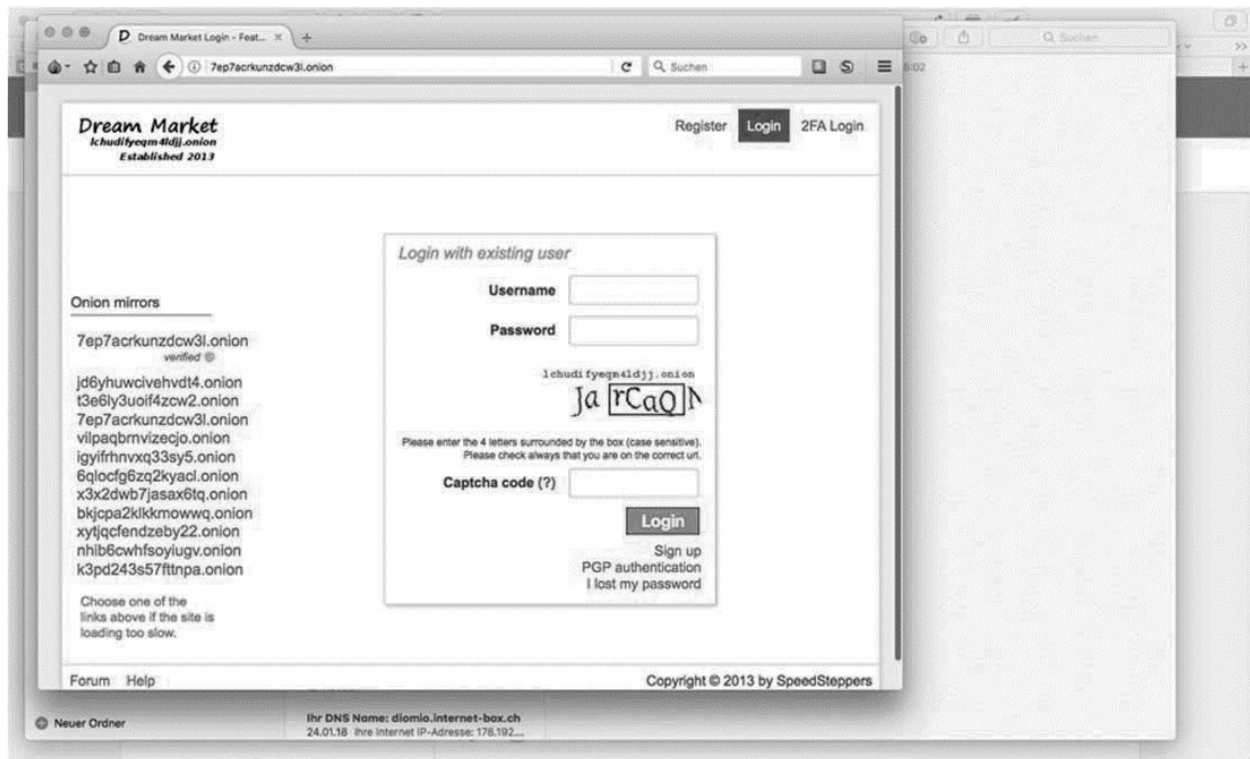


Note: (The Tor Project, n.d.).

Figure 22: Tor Browser has been updated

After the Tor Browser has been updated, the marketplace Dream Market can now be visited. This can be reached via the onion addresses [links removed for publication] or other alternative mirror links.

Figure 23: Dream Market login page



Note: («Dream Market», 2018).

The login works at Dream Market using a username, password and a Captcha code. After a successful login, the current balance, the number of unread messages, news as well as a menu structure and a search window that enable you to search the marketplace are visible.

Figure 24: Dream Market start page after successful login



Note: («Dream Market», 2018).

The marketplace offers each user their own bitcoin wallet. This bitcoin wallet can be controlled via its own bitcoin address. This bitcoin address is required to transfer bitcoins from your wallet (e.g. at Coinbase) to the one at Dream Market. For security reasons, this Bitcoin address changes regularly; but at the latest after each successful transfer. Accordingly, the latest Bitcoin address must be retrieved before each new transfer.

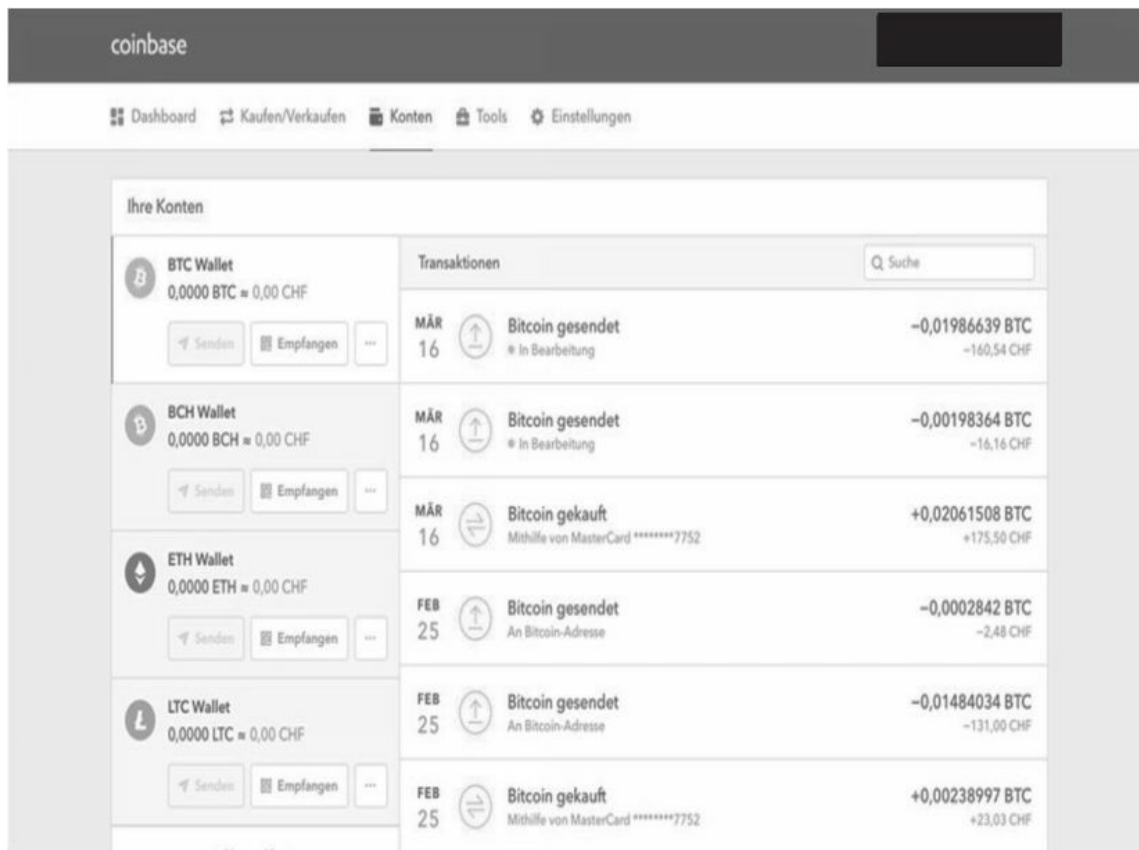
Figure 25: Bitcoin address for Dream Market account



Note: («Dream Market», 2018).

The Bitcoin address is simply copied from the Tor browser window and pasted into the Coinbase transfer.

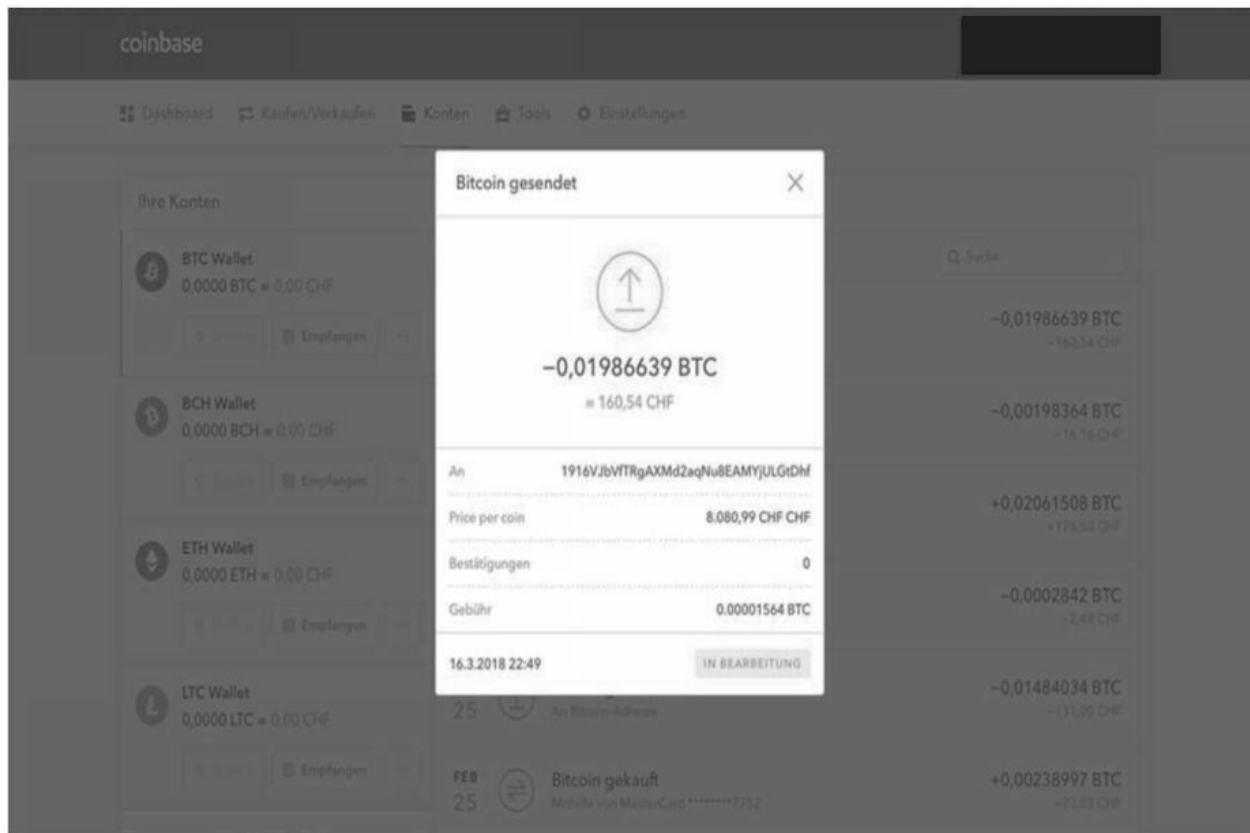
Figure 26: Bitcoins sent from Coinbase to Dream Market address



Note: (Coinbase, 2018).

The bitcoin transfer takes a moment, depending on the volume of payments on the global bitcoin market. The status of the Bitcoin transfer can be called up at Coinbase at any time.

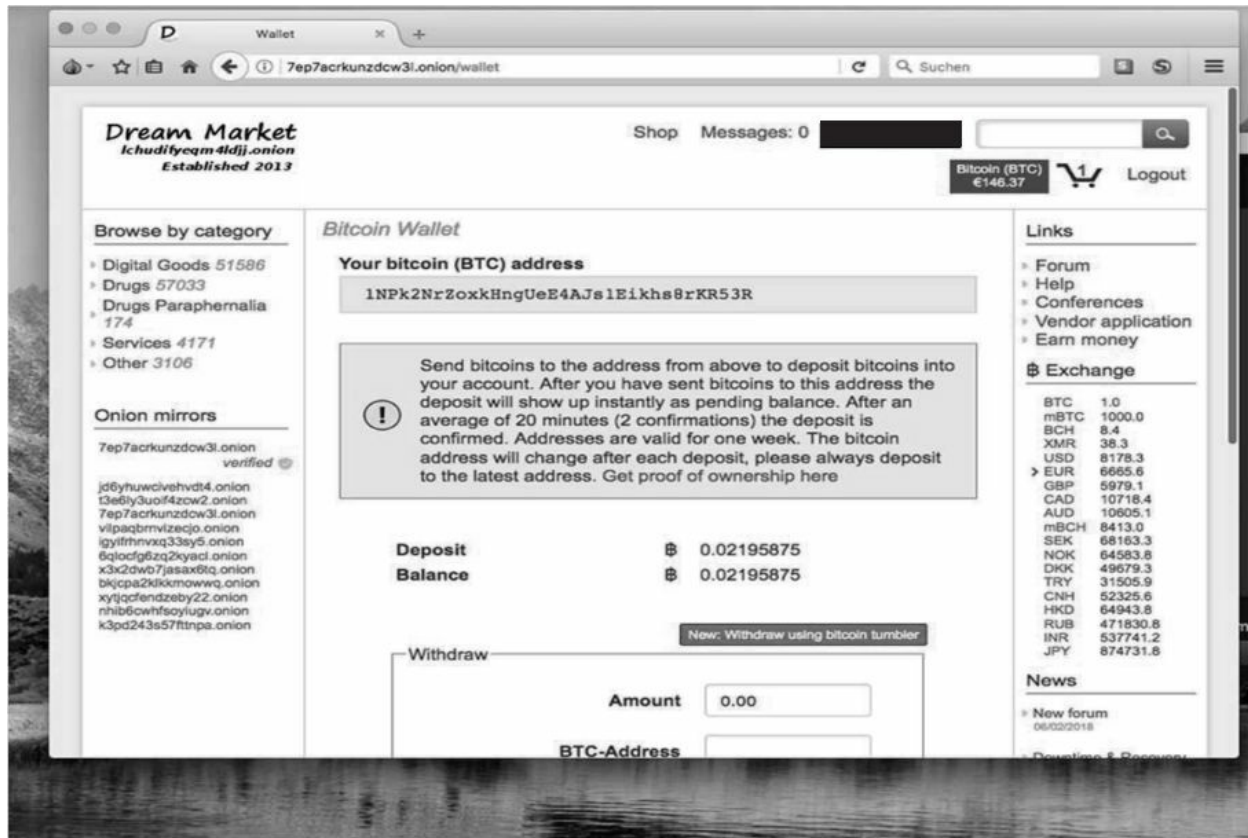
Figure 27: Bitcoin transfer pending at Coinbase



Note: (Coinbase, 2018).

Once the transfer is complete, the bitcoins have been credited to the wallet on Dream Market. This can be seen from the new higher Bitcoin balance.

Figure 28: Bitcoins received and credited to Dream Market account

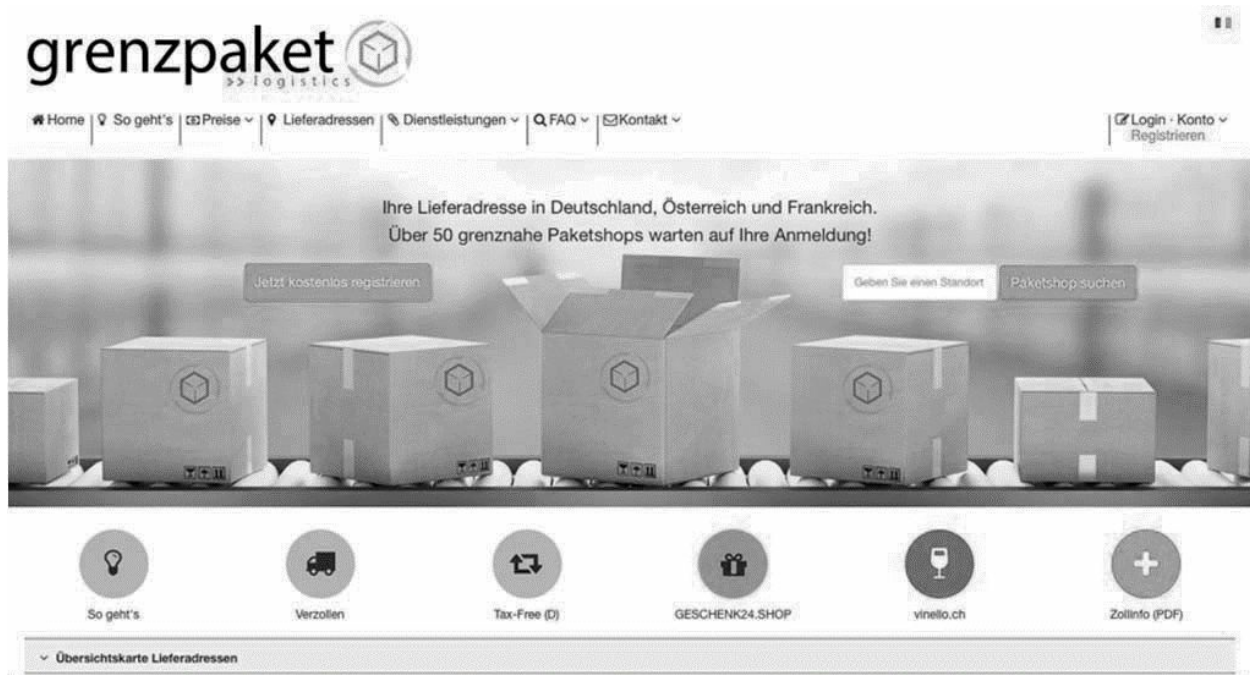


Note: («Dream Market», 2018).

Now all the requirements are met to shop at Dream Market. At this point it is not necessary to present the wide range of goods and services offered on Dream Market.

Instead, an important tip follows: In order for an order to arrive, a correct postal address is required. However, providing your name and home address is not recommended in any way. In order to be able to order goods on the Darknet without personal information, border parcel services are a good option. There are various providers and one of them is Grenzpaket GmbH, for example, which has the URL www.Grenzpaket.ch can be reached.

Figure 29: Website www.Grenzpaket.ch

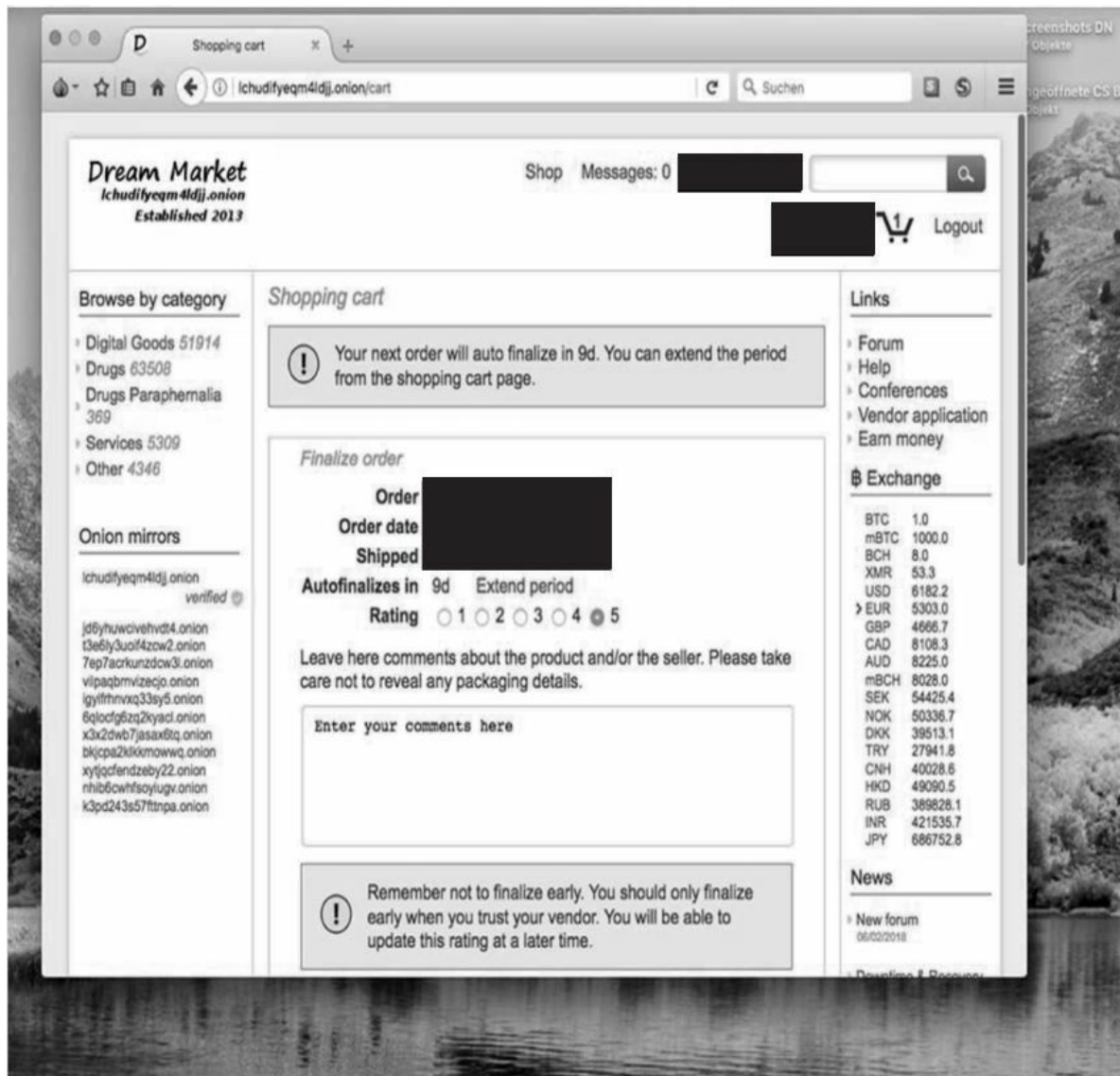


Note: («Border Package», 2018).

A Grenzpaket customer receives a sort of post box with an ID number. This ID number and the address of the mailbox must be specified when ordering on the Darknet. As soon as a shipment has arrived at Grenzpaket, the customer receives a notification either by SMS and/or e-mail.

The order on the Darknet has been placed and the status can be seen in the Dream Market user account.

Figure 30: Order placed and shipped



Note: («Dream Market», 2018).

At this point, the number of days in which the automatic finalization of the escrow will take place is also displayed. This means that the system automatically sets the order to Completed, thereby releasing the amount paid to the seller - without any action on the part of the buyer. However, before the number of days has expired, the buyer has the option of extending the period for automatic finalization. This is if the ordered goods have not yet arrived. Also at this point, the buyer has the option of a so-called

to open a dispute. In this arbitration process, buyers and sellers can explain their situation and the marketplace will find a solution that is fair for both

parties.

The rating, which the buyer can give based on points (5 = best grade, 1 = worst grade), is included in an overall rating of the seller. In addition, the buyer has the option of entering a comment text for his rating.

About a week and a half after the order was placed, the ordered goods actually arrived. This self-experiment shows that it is actually possible to order illegal goods and services on the Darknet and that these can also be delivered.

In conclusion, however, it can be assumed that some of the goods and services offered on the Darknet are not genuine, are not delivered, are used by fraudsters to swindle money or are fictitious and used by investigators as a trap.