Duboka mreža i mračni internet

Radočaj, Ema

Undergraduate thesis / Završni rad

2020

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, University of Zagreb, Faculty of Humanities and Social Sciences / Sveučilište u Zagrebu, Filozofski fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:131:048569

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-07-16**

Sveučilište u Zagrebu
Filozofski fakultet
University of Zagreb
Faculty of Humanities
and Social Sciences

Repository / Repozitorij:

ODRAZ - open repository of the University of Zagreb
Faculty of Humanities and Social Sciences

zir.nsk.hr

dabar
DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

SVEUČILIŠTE U ZAGREBU
FILOZOFSKI FAKULTET
ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI
Ak. god. 2019./2020.

Ema Radočaj

Duboka mreža i mračni internet

Završni rad

Mentor: dr. sc. Tomislav Ivanjko

Zagreb, rujan 2020.

Izjava o akademskoj čestitosti

Izjavljujem i svojim potpisom potvrđujem da je ovaj rad rezultat mog vlastitog rada koji se temelji na istraživanjima te objavljenoj i citiranoj literaturi. Izjavljujem da nijedan dio rada nije napisan na nedozvoljen način, odnosno da je prepisan iz necitiranog rada, te da nijedan dio rada ne krši bilo čija autorska prava. Također izjavljujem da nijedan dio rada nije korišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

_____

(potpis)

Sadržaj

Sadržaj ii
1. Uvod 1
2. Povijest Interneta i World Wide Weba 2
3. Duboka mreža 3
3.1. Indeksiranje sadržaja 3
3.2. Vrste nevidljivosti World Wide Weba 4
3.2.1. Sadržaj koji nije moguće indeksirati 7
3.2.2. Namjerno sakrivanje sadržaja 7
3.3. Veličina duboke mreže 8
3.4. Mračna mreža 9
4. Mračni internet 10
4.1. Tor 11
4.1.1. Princip rada Tora 12
4.1.2. Tor skrivene usluge 13
4.2. Freenet 14
4.3. Invisible Internet Project (I2P) 15
5. Kibernetički kriminal 17
5.1. Kibernetički kriminal na mračnom internetu 17
5.2. Crna tržišta 18
5.2.1. Svileni put 18
5.2.2. AlphaBay 19
5.3. Kriptovalute 20
5.3.1. Bitcoin 20
5.3.2. Monero 21
5.3.3. ZCash 22

6. Zaključak 24
7. Literatura 26
Sažetak 31
Summary 32

1. Uvod

Razvitkom interneta postignuta je globalna povezanost i mogućnost dolaska do potrebnih informacija bez kojih bi današnju svakodnevicu bilo izuzetno teško zamisliti. U svega nekoliko sekundi pretragom putem internetske tražilice saznaju se upute o načinu dolaska do željene lokacije, moguće je naručiti komad odjevnog predmeta s dostavom na kućnu adresu ili pak naučiti novu vještinu uz pomoć video lekcija. Međutim, uz općepoznatu činjenicu da bez interneta život vrlo vjerojatno ne bi bio ono što je danas po pitanju komunikacije i razmjene informacija, privatnost je postala veoma upitna. Radi povećanja razine privatnosti i osiguravanja anonimnosti razvijene su i tehnologije koje to omogućuju, ali su one, nažalost, privukle i korisnike koji tu tehnologiju koriste u ilegalne svrhe od kojih su najpoznatije Tor i *The Invisible Internet Project*.

U ovom će radu biti ukratko opisan razvitak samog Interneta i *World Wide Weba* nakon čega slijedi razrada dijela svjetske mreže čiji sadržaj nije dostupan putem uobičajenih mrežnih pretraživača i tražilica kojima se većina korisnika interneta svakodnevno služi. Sukladno tome razrađene su duboka i mračna mreža koje obuhvaćaju sav neindeksirani sadržaj gdje su naglašene vrste sadržaja koje nije moguće indeksirati te načini na koji je neki sadržaj moguće sakriti od mrežnih paukova koje tražilice koriste za oblikovanje indeksa mrežnih mjesta i stranica. Sljedeće se poglavlje fokusira na mračni internet koji korisnicima pruža anonimnost njihovog identiteta prilikom korištenja interneta te mrežna mjesta kojima je moguće pristupiti isključivo korištenjem posebnih softvera razvijenih za pristup *darknetu*. Naposljetku su istaknute kriminalne aktivnosti za koje pojedinci iskorištavaju anonimizirajuće tehnologije, s naglaskom na razvitak i način poslovanja crnih tržišta.

2. Povijest Interneta i World Wide Weba

Podloga za razvitak interneta bila je mreža ARPANET, projekt američkog ministarstva obrane (*U.S. Advanced Research Projects Agency - ARPA*), čiji su koncepti prvotno objavljeni 1967. godine. Ideja je realizirana 1969. godine kada je na Sveučilištu u Kaliforniji (UCLA) uspostavljen prvi čvor (engl. *node*) ARPANET mreže. Tadašnja zamisao je bila stvaranje mreže sveučilišnih računala putem koje bi znanstvenici i ustanove spojene na tu mrežu mogle komunicirati i razmjenjivati računalne resurse.[1] Za daljnji razvitak ARPANET-a prema današnjem internetu zaslužna je Agencija za napredne istraživačke projekte (*Defense Advanced Research Projects Agency* - DARPA) koja je pokrenula novi projekt s ciljem stvaranja više mreža koje će međusobno biti povezane. Provođenjem dodatnih istraživanja dvojice znanstvenika DARPA-e koji se smatraju „očevima interneta“, Vintona Cerfa i Roberta Kahna, usvojio se pojam „*internet*“ i ujedno je 1973. razvijen TCP (*Transmission Control Protocol*) protokol. Nadalje su provođena istraživanja povezivanjem sveučilišnih mreža što je 1. siječnja 1983. godine rezultiralo usvajanjem TCP/IP grupe protokola kao standardnog protokola ARPANET-a, a danas ga koriste sva umrežena računala.[2]

Nakon ARPANET-a i razvitka Interneta dalje je slijedio nastanak svjetske mreže - *World Wide Web*a. Za razvitak *World Wide Web*-a zaslužan je znanstvenik Tim Berners-Lee koji je na CERN-u (Europsko vijeće za nuklearna istraživanja) 1989. iznio prvi prijedlog svjetske mreže.[3] Godine 1990., Berners-Lee razvio je tri ključne tehnologije koje su temelj *Weba*: HTML (*HyperText Markup Language*), URL (*Uniform Resource Locator*) i HTTP (*Hyper Text Transfer Protocol*) protokol.[4] HTML je služio kao jezik za označavanje, URL se odnosio na jedinstvenu adresu nekog sadržaja, a HTTP protokol služio je za dohvaćanje i prikaz mrežnog sadržaja. Nedugo zatim pojavila se prva mrežna stranica[5] s kojom je započelo širenje *World Wide Weba*.

---

[1] Rouse, M., 2017. *What Is ARPANET? - Definition From Whatis.Com*.SearchNetworking. Dostupno na: https://searchnetworking.techtarget.com/definition/ARPANET (5.7.2020.)
[2] Scos.training. *History Of TCP/IP* | Scos Training. Dostupno na: https://www.scos.training/history-of-tcp-ip/ (5.7.2020.)
[3]Home.cern. *Where The Web Was Born* | CERN. Dostupno na: https://home.cern/science/computing/where-web-was-born (5.7.2020.)
[4]World Wide Web Foundation. *History Of The Web*. Dostupno na: https://webfoundation.org/about/vision/history-of-the-web/ (5.7.2020.)
[5] Info.cern.ch. *Http://Info.Cern.Ch*. Dostupno na: http://info.cern.ch/ (5.7.2020.)

3. Duboka mreža

Duboka mreža (engl. *Deep Web*), također poznata i pod nazivima nevidljiva mreža (engl. *Invisible Web*) i skrivena mreža (engl. *Hidden Web*), obuhvaća sav sadržaj na internetu koji nije pretraživ korištenjem konvencionalnih mrežnih tražilica (engl. *search engine*) kao što su to Google, Bing, Ask.com, AltaVista i tako dalje. Sadržaj duboke mreže nije indeksiran, a on uključuje mrežne stranice, intranete, mreže i mrežne zajednice koje su namjerno ili nehotice sakrivene te su nevidljive ili nedostupne mrežnim paukovima za indeksiranje.[67]

Prema riječima Michaela K. Bergmana, "pretraživanje interneta može se usporediti s povlačenjem mreže preko površine oceana. Bez obzira na to što će velika količina informacija biti pronađena, još uvijek postoji mnoštvo informacija koje se nalaze dublje i zbog toga ne bivaju dohvaćene. Razlog je jednostavan: većina informacija na *World Wide Webu* nalazi se na dinamičko-generiranim stranicama koje konvencionalne tražilice nikada neće pronaći."[8]

3.1. Indeksiranje sadržaja

Mrežne tražilice koriste indeksiranje kako bi prilikom upita korisnika u što kraćem mogućem roku dale odgovarajući i zadovoljavajući rezultat na upit. Indeksiranje je proces organizacije informacija te analize mrežnih stranica kao i izdvajanje pojmova radi lakšeg razlikovanja mrežnih stranica. S obzirom na to da se mrežne stranice, a pritom i njihov sadržaj, neprekidno mijenjaju, tražilice moraju konstantno provoditi proces indeksiranja.[9]

Tražilice za pomoć kod indeksiranja koriste tzv. paukove (engl. *spiders*), još poznati i pod nazivima mrežni pauk (engl. *web crawler*) ili mrežni robot. Mrežni pauk je program

[6] Techopedia.com. 2019. *What Is The Deep Web? - Definition From Techopedia*. Dostupno na: https://www.techopedia.com/definition/15653/deep-web (21.6.2020.)
[7] Dictionary.cambridge.org. n.d. *DEEP WEB | Meaning In The Cambridge English Dictionary*. [online] Dostupno na: https://dictionary.cambridge.org/dictionary/english/deep-web (21.6.2020.)
[8] Bergman, M., K., 2001. White Paper: The Deep Web: Surfacing Hidden Value. *The Journal of Electronic Publishing*, 7(1). Dostupno na: https://doi.org/10.3998/3336451.0007.104 (21.6.2020.)
[9] Comer, D., 2019. *The Internet Book: Everything You Need to Know about Computer Networking and How the Internet Works*. 5th ed. Boca Raton: CRC Press.

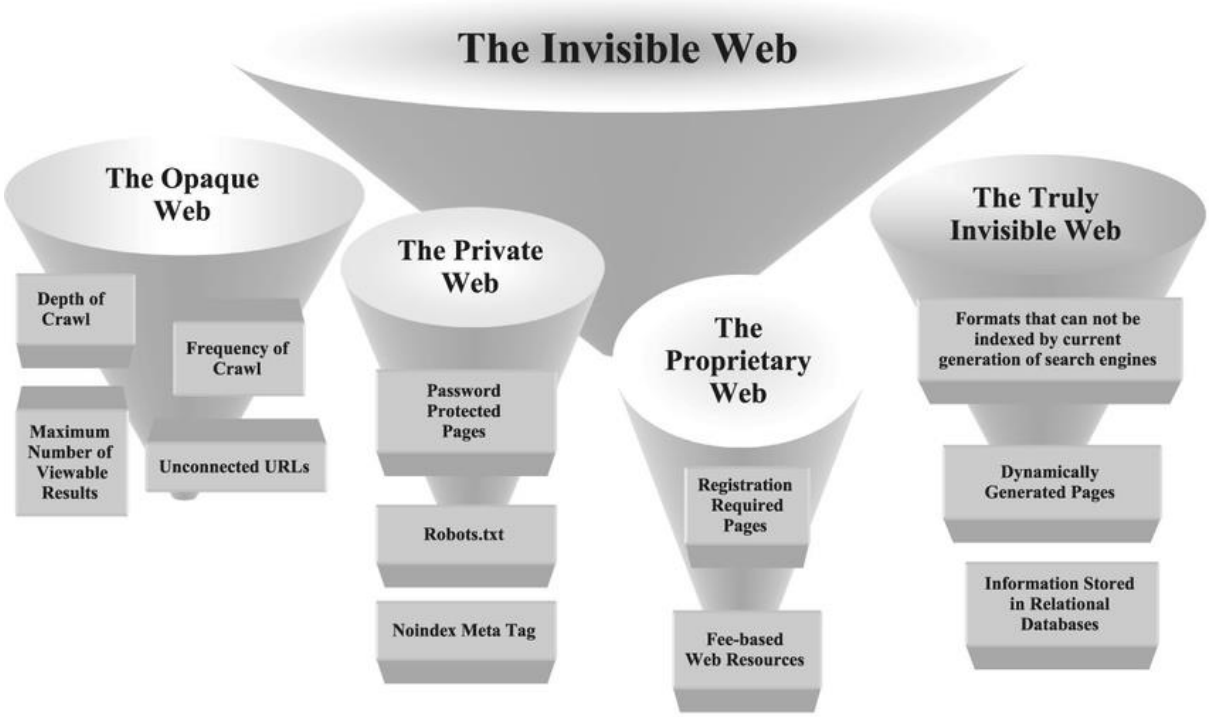
koji pristupa mrežnim stranicama i preuzima njihov sadržaj, odnosno proučava ga i indeksira stranice kako bi izdvojio ključne riječi te onda prelazi na drugu stranicu putem hiperveza na trenutnoj stranici. Pronađeni i indeksirani sadržaj se pohranjuje kako bi tražilica, prilikom sljedećeg upita korisnika, dala relevantne rezultate.[10] Na taj način dolazi do indeksiranja sadržaja svake mrežne stranice na koju paukovi naiđu.

3.2. Vrste nevidljivosti World Wide Weba

Postoje četiri vrste nevidljivosti na *World Wide Web*-u:

- Neprozirni *Web* (engl. *The Opaque Web*)
- Privatni *Web* (engl. *The Private Web*)
- *Web* u vlasništvu (engl. *The Proprietary Web*)
- Stvarno nevidljivi *Web* (engl. *The Truly Invisible Web*). [11]

[10] Sherman, C., Price, G., 2001. *The Invisible Web: Uncovering Information Sources Search Engines Can't See*. Medford, N. J.: CyberAge Books.
[11] Ibid., str. 70.



Slika 1. Prikaz vrsti nevidljivosti World Wide Weba. Preuzeto iz: Ford, N., Mansourian, Y. 2006. The invisible web: An empirical study of „cognitive invisibility“. Journal of Documentation. 62(5). str. 584 – 596

Neprozirni *Web* čini sadržaj koji mrežne tražilice mogu indeksirati, ali isto ne bude učinjeno. Faktori koji utječu na to zašto neki sadržaj nije indeksiran su dubina dohvaćanja mrežnih stranica do koje će mrežni paukovi ići, učestalost dohvaćanja sadržaja na mrežnim stranicama, maksimalan broj vidljivih rezultata i nepovezani URL-ovi. Naime, trošak indeksiranja sadržaja bit će veći s obzirom na to do koje je dubine određeno da tražilica vrši indeksiranje, stoga često dolazi do slučajeva gdje podstranice neke mrežne stranice neće biti prikazane u rezultatima pretraživanja što uzrokuje izostavljanje potencijalno vrijednih i relevantnih podataka. Nadalje, *Web* se svakodnevno mijenja u smislu da se konstantno pojavljuju nove stranice, ali i jednako tako uklanjanju. Zbog kontinuiranih promjena na *Webu*, paukovi će se periodično vraćati i na one stranice koje su već prethodno posjetili zbog mogućih promjena koje su se na njima dogodile ili ako su uklonjene. Uz to, nove stranice koje se pojavljuju podložne su izostavljanju prilikom indeksiranja jer mali broj već postojećih stranica

upućuje na novokreirane pa će one ostati u “nevidljivom” dijelu *Weba*. Uz učestalost dohvaćanja sadržaja stranica, na vidljivost ili nevidljivost sadržaja utječe i maksimalan broj rezultata koji mrežna tražilica može prikazati. Obično je to između 200 i 1000 rezultata, a sadržaj koji nije prikazan u tim rezultatima zbog ograničenja, ostaje nevidljiv. Naposljetku, neprozirni *Web* sačinjavaju i nepovezane stranice u slučaju kada novi sadržaj nije indeksiran putem “Dodaj URL” forme na mrežnim tražilicama ili kada ne postoje poveznice koje bi na tu stranicu upućivale.

Mrežne stranice koje su namjerno isključene iz rezultata tražilica čine privatni *Web*. To su stranice koje zahtijevaju prijavu korisničkim imenom i lozinkom, koriste *robots.txt* datoteku koja paukovima onemogućuje pristup stranici ili u *meta* oznaci sadrže “*noindex*” oznaku zbog čega paukovima neće biti vidljiv sadržaj stranice već samo “glava” stranice.

Web u vlasništvu čine stranice koje zahtijevaju registraciju (besplatnu ili uz pretplatu) i prihvaćanje uvjeta korištenja kako bi njihov sadržaj bio vidljiv i dostupan pojedincu. Iako je većina sadržaja stranica *Weba* u vlasništvu besplatna, mrežni paukovi nemaju sposobnost ispunjavanja formi za registraciju pa takav sadržaj neće biti indeksiran.

Stvarno nevidljivi *Web* obuhvaća onaj sadržaj stranica koji tražilice ne mogu indeksirati jer je sačinjen od PDF ili *Postscript* datoteka, *Flash* ili *Shockwave* animacija, izvršnih programa ili komprimiranih datoteka. Zbog manjka tekstualnog (HTML) sadržaja, tražilice nisu u mogućnosti takve stranice ispravno kategorizirati sukladno sadržaju koji se na njima nalazi. Iako neke takve stranice sadrže njen opis u HTML spremniku (engl. *HTML container*), tražilice bi u takvom slučaju prije indeksirale opis metapodataka nego sam sadržaj datoteke. Također, podaci koji su pohranjeni u relacijskim bazama podataka se također smatraju istinski nevidljivim sadržajem jer mrežni paukovi ne razumiju strukturu baze podataka i ne znaju način na koji se njima upit postavlja kako bi se povratno dobio traženi podatak. Uz tražilicama nečitljiv sadržaj, poteškoće kod indeksiranja stvaraju i dinamički generirane stranice koje tražilice, najčešće, odbijaju indeksirati. Naime, pošto takve stranice koriste skripte i generiraju svoj sadržaj pri postavljanju upita, može se dogoditi da iste budu

napravljene kao zamke za paukove u smislu da masovno korištenje skripti na stranici pauka može “zarobiti” među tisućama stranica, a sve s namjerom kako bi se mrežna tražilica opteretila nepotrebnim sadržajem.

3.2.1. Sadržaj koji nije moguće indeksirati

Mrežne tražilice su optimizirane za pretragu i indeksiranje stranica s tekstualnim sadržajem, odnosno sadržajem pisanim *HyperText Markup Language* (HTML) kodom. Takve su stranice povoljne i jednostavne za uvrštavanje u indeks tražilice jer se iz njih lako iščitava sadržaj i tematika što tražilicama olakšava klasifikaciju. One stranice koje mrežni paukovi neće biti u mogućnosti dohvatiti, a tražilice indeksirati, smatraju se sadržajem duboke mreže i on se naposljetku svodi na:

- nepovezane stranice
- mrežne stranice koje se uvelike sastoje od slikovnih, zvučnih ili video datoteka
- stranice koje se primarno sastoje od PDF datoteka, Postscript datoteka, Flash animacija, Shockwave animacija, izvršnih programa (.exe) ili komprimiranih datoteka (.zip, .tar, .rar)
- sadržaj stranica pohranjen u relacijskim bazama podataka
- stranice čiji se sadržaj generira u stvarnom vremenu
- dinamički generirani sadržaj.

3.2.2. Namjerno sakrivanje sadržaja

HTML kod sastoji se od dva glavna dijela: glave (engl. *head*) i tijela (engl. *body*) koji se označavaju oznakama <head></head> i <body></body>. U *head* dijelu zapisani su naslov HTML dokumenta i informacije koje opisuju sadržaj, metapodaci. Na temelju metapodataka tražilica vrši klasifikaciju. *Body* dio dokumenta je ujedno i njegova “jezgra” gdje se nalazi sadržaj mrežne stranice.

Tražilice prilikom indeksiranja koriste metapodatke koji se nalaze unutar meta oznaka u HTML kodu i sadržaj same stranice kako bi sadržaj ispravno kategorizirale. Iz

metapodataka se iščitavaju ključne riječi i opis sadržaja stranice. Ako se neku stranicu namjerno želi isključiti iz prikaza rezultata pretrage, isto je moguće napraviti korištenjem protokola za isključenje robota prilikom pokušaja dohvaćanja stranica (engl. *The Robots Exclusion Protocol*), dodavanjem metaoznake "*noindex*" ili zaštitom stranice lozinkom.[12]

Protokol za isključenje robota podrazumijeva kreiranje datoteke na poslužitelju pod nazivom *robots.txt* kojom se od mrežnih paukova i drugih mrežnih robota zahtijeva da ne pristupaju određenim stranicama, podstranicama, datotekama ili direktorijima te da ih ne pregledavaju i indeksiraju.

Za sprječavanje pristupa mrežnih robota ujedno se koristi i metaoznaka "*noindex*" koja se upisuje u *head* dio HTML dokumenta, no ona, za razliku od *robots.txt* datoteke, može zaustaviti jedino indeksiranje neke specifične stranice na mrežnom mjestu. Uz *noindex* oznaku može se navesti i *nofollow* oznaka kako roboti ne bi pratili poveznice prisutne na stranici i indeksirali ih.[13]

Optimalan način za zabranu indeksiranja neke stranice je postavljanje lozinke na istu. Tako se pristup omogućava samo određenim pojedincima kojima su dani pristupni podaci.

3.3. Veličina duboke mreže

Brzina kojom se internet svakodnevno mijenja i raste uvelike utječe na utvrđivanje veličine duboke mreže. Istraživanje iz 2017. godine[14] ukazuje na činjenicu da je zbog navedenog skoro pa nemoguće dobiti točan podatak o veličini duboke mreže, no po procjenama se smatra da je ona četiri do pet tisuća puta veća od površinske mreže (engl. *Surface Web*). Površinsku mrežu čini indeksirani sadržaj, dostupan

[12] Sherman, C., Price, G., 2001. *The Invisible Web: Uncovering Information Sources Search Engines Can't See*. Medford, N. J.: Cyber Age Books.
[13] Castro, E., 2007. *Getting People to Visit: Keeping Visitors Away*. HTML, XHTML and CSS, Sixth Edition: Visual QuickStart Guide. Berkeley: Peachpit Press.
[14] Finklea, K., 2017. *Dark Web*. Dostupno na: https://fas.org/sgp/crs/misc/R44101.pdf (12.7.2020.)

pretraživanjem i korištenjem konvencionalnih mrežnih tražilica i pretraživača (*Google Chrome*, *Mozilla Firefox*, *Microsoft Edge* i drugi). Radi lakše usporedbe, danas na površinskoj mreži postoji preko 1,7 milijardi mrežnih stranica, a broj kontinuirano raste. Primjerice, u 2017. godini broj stranica porastao je za 59,17% u odnosu na 2016. godinu.[15]

3.4. Mračna mreža

Mračna mreža (engl. *Dark Web*) je dio duboke mreže i čini ga sadržaj koji je namjerno sakriven i pristup mu je moguć isključivo uz korištenje određenih alata i programa. Jednako kao i kada je u pitanju duboka mreža, sadržaj mračne mreže nije dostupan korištenjem klasičnih mrežnih tražilica. U slučaju mračne mreže, sadržaj se nalazi na mračnom internetu ili drugom obliku privatnih mreža koje se zasnivaju na *peer-to-peer* povezanosti. Neke od takvih mreža putem kojih je moguće pristupiti mračnom internetu su Tor mreža, *Freenet* i *Invisible Internet Project* (I2P).[16] Struktura mračne mreže pruža izuzetnu anonimnost korisnika i osigurava privatnost njegovog identiteta pa shodno tome ona služi kao idealna podloga za kriminalne i terorističke aktivnosti, s kojim se i sam pojam mračne mreže nerijetko primarno povezuje.[17]

[15] Internet Live Stats. *Total Number Of Websites*. Dostupno na: https://www.internetlivestats.com/total-number-of-websites/ (12.7.2020.)
[16] Ciancaglini, V., Balduzzi, M., McArdle, R., Rösler. 2015. *Below the Surface: Exploring the Deep Web*. Dostupno na: https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf (10.6.2020.)
[17] Ozkaya, E., Islam, R., 2019. *Inside the Dark Web*. Boca Raton: CRC Press.

4. Mračni internet

Mračni internet (engl. *darknet*) je privatna računalna mreža koja radi na internetu, a pristup imaju isključivo pojedinci kojima je to dozvoljeno ili imaju odgovarajući softver i alate.[18] Smatra se da je pojam "*darknet*" po prvi put definiran i spomenut u studenom 2002. godine u istraživanju četvero Microsoftovih inženjera sigurnosti. U tom je istraživanju mračni internet općenito definiran kao "skup mreža i tehnologija koje se koriste za dijeljenje digitalnog sadržaja" i navodi se da nije zasebna mreža nego dio aplikacijskog sloja, prekrivajuća mreža (engl. *overlay network*), koji se nalazi na već postojećim mrežama - internetu.[19] Fred von Lohmann također je vršio istraživanja vezana uz mračni internet te je, uključujući i pitanje privatnosti, mračni internet definirao kao "skup mreža i drugih tehnologija koje ljudima omogućuju da ilegalno dijele digitalni sadržaj koji je zaštićen autorskim pravima s malo ili bez ikakvog straha da će biti uhvaćeni".[20]

Mračni internet pojedincima koji ga koriste jamči anonimnost što je rezultiralo masovnom stvaranju mrežnih mjesta i zajednica gdje se na raspolaganje stavljaju razne ilegalne usluge. Taj dio interneta posjećuju i aktivno koriste kriminalci, teroristi, hakeri, ubojice, dileri i naposljetku, njihovi klijenti. Glavni razlog korištenja crnih tržišta je upravo anonimnost koja je prisutna kod identiteta kupca, prodavača i načina plaćanja. Uz razvoj i popularizaciju crnih tržišta, svoj je vrhunac dostigla i kriptovaluta Bitcoin s kojom je moguće plaćanje bez saznanja o identitetu kupca. *Darknet* je 2011. godine otkrivanjem jednog od najpoznatijih crnih tržišta koji se na njemu nalazi, Svilenog puta (engl. *Silk Road*), dobio veliku medijsku pozornost. Ujedno je i utvrđeno kako se osim ilegalnog dijeljenja sadržaja zaštićenog autorskim pravima, *darknet* i mračna mreža (engl. *Dark Web*) koriste i za razne druge kriminalne radnje kao što su prodaja narkotika, naručivanje ubojstava, prodaja ukradenih osobnih podataka, dijeljenje dječje pornografije i slično.

[18] Dictionary.cambridge.org. 2020. *DARKNET | Meaning In The Cambridge English Dictionary*. Dostupno na: https://dictionary.cambridge.org/dictionary/english/darknet (10.6.2020.)
[19] Biddle, P., England, P., Peinado, M., Willman, B. 2002. The Darknet and the Future of Content Protection. U: J. Feigenbaum (ur.), *Digital Rights Management*. Washington: Springer. str. 155-176.
[20] Wood, J. A., 2010. The Darknet: A Digital Copyright Revolution. *Richmond Journal of Law and Technology*, 16 (4). Dostupno na: https://scholarship.richmond.edu/jolt/vol16/iss4/4/ (10.6.2020.)

Neki od najpoznatijih *darkneta* su Tor (*The Onion Router*), I2P (*The Invisible Internet Project*) i Freenet. Navedene su kreirane upravo zbog želje i potrebe za anonimnim načinom komuniciranja i pretraživanja na internetu bez uplitanja nekih trećih strana kao što su, primjerice, pružatelji internetskih usluga.[21] Sukladno, IP adresa korisnika i stranice koje je posjećivao u *darknetu* neće biti vidljivi.

4.1. Tor

The Onion Routing (skraćeno Tor) je razvijen u svrhu postizanja anonimnosti prilikom korištenja interneta i pritom pomaže sprečavanju analize mrežnog prometa (engl. *traffic analysis*). Prvi koncepti *onion* mreže potječu iz 1995. godine kada su David Goldschlag, Mike Reed i Paul Syverson došli na ideju za razvijanje mreže putem koje neka treća strana koja nadgleda mrežu ne bi imala uvid u korisnikovu aktivnost. Tor je zamišljen i naposljetku realiziran zbog potrebe za većom razinom sigurnosti i privatnosti kao i zbog prava na pristup i objavu necenzuriranog online sadržaja što bi se postiglo enkripcijom i usmjeravanjem internetskog prometa preko više poslužitelja.[22]

Zbog izrazite razine anonimnosti koju pruža, pojedinci i organizacije Tor koriste za pristup mrežnim mjestima koja su blokirana od strane davatelja internetskih usluga u nekim državama, privatno dijeljenje podataka i komunikaciju preko interneta, izbjegavanje praćenja aktivnosti na internetu te krađe osobnih podataka. Primjerice, novinarima olakšava komunikaciju sa "zviždačima" (engl. *whistleblower*), pojedincima koji otkrivaju tajne i ilegalne aktivnosti organizacija.[23] Tor je također i dio sustava *SecureDrop*, sustava otvorenog izvornog koda u koji zviždači učitavaju dokumente i anonimno komuniciraju s medijskim kućama tako im služeći kao anonimni izvor informacija.[24]

[21] Wood, J. A., 2010. The Darknet: A Digital Copyright Revolution. *Richmond Journal of Law and Technology*, 16 (4). Dostupno na: https://scholarship.richmond.edu/jolt/vol16/iss4/4/ (10.6.2020.)
[22] Torproject.org. *The Tor Project | Privacy & Freedom Online*. Dostupno na: https://www.torproject.org/about/history/ (21.06.2020.)
[23] 2019.torproject.org. *Tor Project: Overview*. Dostupno na: https://2019.www.torproject.org/about/overview.html.en (23.6.2020.)
[24] Blog.torproject.org. 2016. *Tor At The Heart: Securedrop | Tor Blog*. Dostupno na: https://blog.torproject.org/tor-heart-securedrop (5.8.2020.)

Tor se sastoji od dva dijela: Tor preglednika i Tor mreže.[25] Tor preglednik i njegovo korisničko sučelje bazirani su na pregledniku *Mozilla Firefox*. Putem njega je jednako moguć pristup svim mrežnim stranicama kao i na površinskom *Webu*, ali i posebnim stranicama s *.onion* završetkom koje se nalaze samo unutar Tor mreže. Korištenjem Tor preglednika zajamčena je anonimnost prilikom korištenja jer se promet usmjerava preko Tor mreže, a ne direktno prema mrežnim stranicama kao što je to slučaj kod uobičajenih mrežnih preglednika.

4.1.1. Princip rada Tora

Tor mreža je decentralizirana računalna mreža koju čini skup volonterskih poslužitelja preko kojih promet putuje. Korištenjem Tora zajamčena je sigurnost od praćenja internetske aktivnosti. Korištenjem alata za nadzor mreže i analizu prometa otkriva se IP adresa pošiljatelja kao i IP adresa odredišta, odnosno posjećene stranice. Korištenjem dodatnih alata, IP adresa se dodatno može povezati i s fizičkom lokacijom korisnika interneta.[26]

Uobičajeno usmjeravanje internetskog prometa funkcionira tako da promet putuje do destinacije najkraćim mogućim putem. Usmjernik (engl. *router*) će informacije potrebne za prijenos prometa iščitati iz zaglavlja podatkovnog paketa. Iz tih je informacija usmjerniku vidljiv izvor podataka, gdje se taj izvor nalazi te odredište prometa. Takav se promet lako otkriva pomoću alata za nadzor i analizu mrežnog prometa jer oni otkrivaju IP adresu pošiljatelja i IP adresu odredišta, odnosno posjećene stranice. S druge strane, Tor koristi tzv. usmjeravanje luka (engl. *The Onion Routing*) gdje se internetski promet prosljeđuje preko mnogo čvorova mreže. Tor mrežu čini oko 6500[27] poslužitelja koja se nazivaju „čvorovi“ (engl. *nodes*). Ti poslužitelji su takozvani “volonteri”, odnosno računala korisnika, i njih na raspolaganje

[25] Eff.org. *What is a Tor Relay? | Tor Challenge.* Dostupno na: https://www.eff.org/torchallenge/what-is-tor.html (23.6.2020.)
[26] 2019.torproject.org. *Tor Project: Overview*. Dostupno na: https://2019.www.torproject.org/about/overview.html.en (23.6.2020.)
[27] Metrics.torproject.org. *Servers – Tor Metrics*. Dostupno na: https://metrics.torproject.org/networksize.html (23.6.2020.)

može staviti i održavati bilo koji pojedinac ili organizacija u svijetu. Usmjeravanje luka koristi enkripciju na aplikacijskom sloju i ona se slojevito primjenjuje na podatkovni paket koji se šalje kroz Tor mrežu. Tako enkriptirani podaci kod slanja prolaze kroz više čvorova u mreži, umjesto da direktno pristignu do njegovog odredišta što znači da u slučaju presretača na mreži, isti neće biti u mogućnosti saznati informaciju o početnoj IP adresi podatkovnog paketa koji je poslan, već će vidjeti samo IP adresu čvora gdje se paket trenutno nalazi.[28]

Vrste čvorova koje postoje na Tor mreži su: čuvar i srednji čvor (engl. *guard and middle relay*), izlazni čvor (engl. *exit relay*) i most (engl. *bridge*). Svi čvorovi Tor mreže pohranjeni su u poslužiteljskom direktoriju (engl. *server directory*) iz kojeg se prilikom slanja paketa nasumično biraju određeni čvorovi preko kojih će on putovati. Nijedan čvor nema uvid u kompletnu putanju paketa već mu je samo vidljivo od kojeg je čvora primio paket i gdje je isti potrebno dalje usmjeriti. Tor stavlja sloj enkripcije na sadržaj paketa i IP adresu čvora. Slojevi enkripcije postepeno se uklanjaju pomoću provjere sigurnosnih ključeva kod svakog prijelaza paketa preko čvora. Ovim načinom usmjeravanja paketa će odredištu biti vidljiva jedino IP adresa posljednjeg čvora u putanji paketa, odnosno izlaznog čvora. S obzirom na to da su sve IP adrese čvorova Tor mreže javno dostupne, neki pružatelji usluge interneta iste odluče blokirati. U takvim se slučajevima mogu koristiti tzv. mostovi koji za razliku od preostalih vrsti čvorova nisu navedeni u Torovom poslužiteljskom direktoriju. [29]

4.1.2. Tor skrivene usluge

Tor skrivene usluge (engl. *Tor hidden services*) ili usluge luka (engl. *onion services*) su mrežna mjesta i stranice koje nisu dostupne korištenjem uobičajenih mrežnih pretraživača već isključivo putem Tor mreže. URL-ovi takvih stranica imaju poseban domenski nastavak .onion umjesto, primjerice .com, .net, .org i tako dalje. Nazivi adresa u Tor mreži sastoje se od 16 ili 56 znakova i mogu sadržavati brojeve dekadskog brojevnog sustava između i uključujući 2 i 7 te mala slova abecede. Adrese

[28] Ozkaya, E., Islam, R., 2019. *Inside the Dark Web*. Boca Raton: CRC Press.
[29] Community.torproject.org. *Tor Project | Types Of Relays On The Tor Network*. Dostupno na: https://community.torproject.org/relay/types-of-relays/ (10.7.2020.)

sa 16 znakova pripadaju u drugu verziju adresa, a one sa 56 znakova u treću verziju.[30] Primjerice, adresa stranice Tor projekta, www.torproject.org, ima svoju .onion adresu expyuzz4wqqyqhjn.onion. Danas u Tor mreži postoji približno 200 tisuća jedinstvenih .onion adresa druge verzije.[31]

4.2. Freenet

Ian Clarke je 2000. godine[32] u svrhu anonimnog dijeljenja i dohvaćanja datoteka razvio decentraliziranu *peer-to-peer* mrežu pod nazivom *Freenet*. Isto kao i Tor mreža, čini ju mnoštvo čvorova koja mogu biti računala tzv. prijatelja ili stranaca. Komunikacija između čvorova je kriptirana i usmjerena preko ostalih čvorova u mreži radi težeg otkrivanja identiteta pojedinca koji pristupa sadržaju, ali i samog sadržaja. Spajanje na *Freenet* moguće je na dva načina: omogućavanjem nesigurnog načina rada kod kojeg se spajanje vrši na čvorove stranaca ili spajanjem na čvorove ljudi koje pojedinac poznaje – prijatelja. Za spajanje na čvorove prijatelja, obje strane moraju razmijeniti i unijeti tzv. reference čvorova (engl. *node references*) kako bi spajanje bilo uspješno. Korištenjem nesigurnog načina rada čvor pojedinca bit će vidljiv svakom drugom čvoru u *Freenet* mreži, dok će isključenjem te opcije vidljivost čvora imati isključivo čvorovi prijatelja i jedino će oni moći vidjeti vrstu prometa koja čvorom prolazi.[33]

Svaki korisnik *Freeneta* djeluje i kao klijent i kao poslužitelj. Pojedinac daje na raspolaganje drugim korisnicima dio svog mrežnog skladišnog prostora i ujedno koristi prostor drugih korisnika u svrhu dijeljenja i dohvaćanja datoteka.[34] Putem *Freeneta* nije moguće pristupati istim stranicama kao što je to moguće putem, primjerice, Tor-

[30] Gayard, L., 2018. *Darknet: Geopolitics and Uses*. London: ISTE Ltd, Hoboken: John Wiley & Sons, Inc.
[31] Metrics.torproject.org. 2020. *Onion Services – Tor Metrics*. Dostupno na: https://metrics.torproject.org/hidserv-dir-onions-seen.html?start=2020-05-21&end=2020-08-17 (17.8.2020.)
[32] Wood, J. A., 2010. The Darknet: A Digital Copyright Revolution. *Richmond Journal of Law and Technology*, 16 (4). Dostupno na: https://scholarship.richmond.edu/jolt/vol16/iss4/4/ (10.6.2020.)
[33] Freenetproject.org. *Documentation*. Dostupno na: https://freenetproject.org/pages/documentation.html#understand (7.7.2020.)
[34] Taylor, I., 2005. Freenet. *From P2P To Web Services And Grids*. London: Springer.

a, već ima svoje mrežne stranice („*freesites*“), forume, čavrljanja, elektroničku poštu, mikroblogove i slično.[35]

4.3. Invisible Internet Project (I2P)

The Invisible Internet Project, poznatiji pod akronimom I2P, je pokrivna mreža (engl. *overlay network*) na internetu koja osigurava anonimnu, *peer-to-peer* komunikaciju i sigurno dijeljenje poruka putem interneta, a sama mreža radi na aplikacijskom i transportnom sloju protokola. [36] Prvotno je 2003. godine najavljena i potom razvijena decentralizirana mreža naziva *anonCommFramework* koja je pružala anonimnu komunikaciju. Nakon implementacije usmjernika, kasnije tijekom godine, ona postaje I2P. Decentraliziranost I2P mreže osigurava sakrivenost identiteta korisnika s obzirom na to da računalo svakog sudionika u mreži služi kao jedan od čvorova preko kojih mrežni promet prelazi. U slučaju nadziranja mreže, početna i odredišna IP adresa prometa neće biti poznata. I2P ujedno koristi i *end-to-end* enkripciju i tzv. usmjeravanje češnjaka (engl. *garlic routing*).[37]

Garlic routing je 2000. godine razvio Michael J. Freedman[38] po uzoru na usmjeravanje luka (engl. *onion routing*) te je ono implementirano u I2P. Poruka koja je poslana preko I2P mreže naziva se “češnjak” i sastoji se od nekoliko enkriptiranih poruka koje su grupirane i svaka takva poruka naziva se češanj češnjaka (engl. *clove*). Uz navedeno se dodatno koristi i slojevita enkripcija, kao što je to slučaj i kod usmjeravanja luka.[39] Za pristup I2P mreži potrebno je da svaki korisnik ima postavljen I2P usmjernik na računalu koji za anonimiziranje i prijenos poruka koristi dvije vrste tunela: dolazni (engl. *inbound tunnel*) i odlazni (engl. *outbound tunnel*). Poruka se prosljeđuje kroz tunele, preko niza članova s I2P usmjernikom. Svaki korisnik I2P mreže bira broj

[35] Freenetproject.org. *Freenet Project*. Dostupno na: https://freenetproject.org/pages/help.html (7.7.2020.)
[36] Dcssproject.net. 2015. *Invisible Internet Project (I2P) – Digital Citizenship And Surveillance Society*. Dostupno na: https://dcssproject.net/i2p/index.html (12.7.2020.)
[37] Mann, B., 2020. *What Is I2P & How Does It Compare Vs. Tor Browser In 2020?*. Blokt - Privacy, Tech, Bitcoin, Blockchain & Cryptocurrency. Dostupno na: https://blokt.com/guides/what-is-i2p-vs-tor-browser#Who_develops_/_manages_I2P (2.8.2020)
[38] Geti2p.net. 2014. *Garlic Routing - I2P*. Dostupno na: https://geti2p.net/en/docs/how/garlic-routing (2.8.2020)
[39] Norris, J., 2020. *The Privacy Pros And Cons Of The I2P Network*. Vpnmentor.com. Dostupno na: https://www.vpnmentor.com/blog/pros-cons-i2p-network/ (2.8.2020)

članova od kojih će se tunel sastojati. Kod slanja poruke koristi se odlazni, a kod zaprimanja dolazni tunel što znači da komunikacija između dva korisnika nikada neće prolaziti istim putem. Za razmjenu jedne poruke, slanje i zaprimanje odgovora, poruka će proći kroz ukupno četiri tunela.[40][41]

Uz anonimnu komunikaciju, I2P također pruža i jednako takvo udomljavanje mrežnih stranica što u usporedbi sa stranicama na *World Wide Webu* nije slučaj jer se usluga udomljavanja plaća njenim pružateljima (engl. *hosting provider*). Stranice udomljene na I2P-u nazivaju se *eepsites* i domenski nastavak im je .i2p. Jednako kao i kod stranica s .onion nastavkom koje su dostupne jedino putem Tor pretraživača, pristup *eepsite*ima moguć je isključivo iz I2P mreže korištenjem pretraživača koji je postavljen na način da koristi I2P usmjernik.[42]

[40] Geti2p.net. *Intro - I2P*. Dostupno na: https://geti2p.net/en/about/intro (2.8.2020)
[41] Geti2p.net. 2014. *Garlic Routing - I2P*. Dostupno na: https://geti2p.net/en/docs/how/garlic-routing (2.8.2020)
[42] Gehl, R. W., 2018. *Weaving The Dark Web*. Cambridge, Massachusetts: The MIT Press.

5. Kibernetički kriminal

Kibernetički kriminal (engl. *cybercrime*) podrazumijeva korištenje računala kao sredstvo u izvođenju ilegalnih radnji kao što su to počinjenje kaznenoga djela, krađa identiteta, trgovanje dječjom pornografijom i intelektualnim vlasništvom ili kršenje privatnosti.[43] Ova vrsta kriminala postojana je i na površinskoj te dubokoj mreži, no popularizacijom mračnog interneta kriminalci se sve više okreću *darknetima*, najčešće Toru, kao mjestu gdje se smatraju nedodirljivima.

5.1. Kibernetički kriminal na mračnom internetu

U mračnoj mreži nalazi se povelik broj crnih tržišta jer ona predstavljaju jednostavnu i sigurnu razmjenu željenih, ilegalnih dobara. Pojam sigurnosti se u ovom slučaju odnosi na nemogućnost saznanja identiteta kupca i prodavača što uzrokuje priljev velike količine korisnika i daljnjeg širenja mračne mreže. Uz crna tržišta postoje i razne stranice putem kojih određeni pojedinci nude svoje usluge zainteresiranima, a za kupnju usluga i proizvoda prilikom plaćanja se koriste kriptovalute kao dodatan korak prema osiguravanju tajnosti identiteta.

Najzastupljenija ilegalna aktivnost je prodaja opojnih sredstava i oružja. Stranice crnih tržišta uz objavljene artikle za prodaju također imaju i sustav recenzija gdje kupci mogu ostavljati svoje osvrte na uslugu i kupljeni proizvod što potencijalne kupce još više potiče na kupnju preko mračnog interneta uz samu činjenicu da je ovakav način kupnje manje rizičan od uobičajenog sastajanja s prodavačem uživo. Mračni internet se istodobno koristi i za komunikaciju među teroristima za planiranje i dogovaranje oko terorističkih aktivnosti, dok je hakerima ono idealna platforma za ponudu usluga poput DDoS (*Distributed Denial of Service*) napada, izrade virusa, krađe osobnih podataka, hakiranje korisničkih računa i slično.

Nadalje, još neki drugi oblici kibernetičkog kriminala u mračnoj mreži obuhvaćaju narudžbu ubojstva, prodaju zloćudnih softvera, prodaju i izradu lažnih osobnih

[43] Dennis, M. A. *Cybercrime | Definition, Statistics, & Examples*. Encyclopedia Britannica. Dostupno na: https://www.britannica.com/topic/cybercrime (30.6.2020.)

dokumenata i vozačkih dozvola, distribuciju dječje pornografije, ilegalnu razmjenu egzotičnih životinja i slično.[44]

5.2. Crna tržišta

Anonimnost Tor mreže omogućila je nekontrolirani razvoj crnih tržišta koja su ujedno i najveći izvor nepoćudnog sadržaja i ilegalnih radnji. Crna tržišta neprestano privlače nove mušterije i prodavače zbog svoje uređenosti. Prema istraživanju Europskog centra za praćenje droga i ovisnosti o drogama (*European Monitoring Centre for Drugs and Drug Addiction* - EMCDDA)[45] utvrđeno je da sama regulacija takvih mrežnih tržišta kupcima i prodavačima daje dodatan osjećaj sigurnosti kada su u pitanju sigurnost kupnje, kvaliteta usluge ili proizvoda i način plaćanja.

Premda je glavna svrha mračnog interneta pružanje anonimnosti tijekom korištenja istog, potrebno je poduzeti i neke dodatne korake kako bi crna tržišta uistinu nastavila osiguravati anonimnost identiteta te kvalitetu usluge. Kako bi kupci mogli razaznati proizvode i usluge koje su kvalitetne i vrijedne nabave, integriran je sustav za ostavljanje recenzija i povratnih informacija kao što je to, primjerice, ugrađeno i kod mrežnih tržišta *eBay*, *Amazon*, *Etsy* i drugih. Ostavljanje povratnih informacija nedvojbeno dosta pomaže kod filtriranja lažnih i prevarantskih prodavača čija usluga nije dostatna za daljnju distribuciju. Isto tako je potrebno osigurati najpouzdaniji način izvođenja transakcija stoga se na crnim tržištima koriste kriptovalute, s obzirom na to da se radi o digitalnom okruženju stoga plaćanje gotovinom nije optimalno.

5.2.1. Svileni put

Svileni put (engl. *Silk Road*) jedno je od najpoznatijih i modernijih digitalnih crnih tržišta u dubokoj mreži koje se razvilo u veljači 2011. godine zbog potrebe za anonimnim

[44] Ozkaya, E., Islam, R., 2019. *Inside the Dark Web.* Boca Raton: CRC Press.
[45] Gayle, D., 2016. *Online Market 'Is Turning Drug Dealers From Goons To Geeks'*. The Guardian. Dostupno na: https://www.theguardian.com/world/2016/feb/11/online-market-turning-drug-dealers-goons-geeks-darknet (11.7.2020.)

načinom prodaje narkotika.[46] Uz opojna sredstva, Svileni put bio je poznat i po udomljavanju usluga pranja novca. Tržište Svileni put je dilerima i klijentima bilo mjesto za dogovor oko kupnje koje je pružalo potpunu anonimnost identiteta jer se za transakcije koristila kriptovaluta Bitcoin zbog svoje praktičnosti i anonimnosti prilikom transakcija.

Osnivač Svilenog puta je Ross Wiliam Ulbricht, poznat i pod nadimkom Dread Pirate Roberts, tržište je pokrenuo upravo s idejom da ono bude platforma za prodaju i nabavu opojnih i drugih zabranjenih sredstava bez saznanja vlade. Svileni put je u veoma kratkom periodu, privuklo mnoštvo zainteresiranih za korištenje koji su također htjeli sudjelovati u prodaji svojih narkotika te je popularnost Svilenog puta rapidno rasla. Kraj tržišta postignut je Ulbrichtovim uhićenjem 2013. godine[47], no time je također uzrokovan daljnji razvitak tržišta kao što su *Silk Road 2.0* te mnogih drugih.

5.2.2. AlphaBay

Nakon završetka rada crnog tržišta Svileni put, pojavilo se novo tržište pod nazivom *AlphaBay* koje je pokrenuo Alexandre Cazes i njime je upravljao od prosinca 2014. godine do srpnja 2017. godine kada je uhićen.[48] Tržište *AlphaBay* se isto kao i njegov prethodnik nalazilo u mračnoj mreži i pristup mu je bio moguć isključivo korištenjem Tora. U trenutku kada je tržište ukinuto, na njemu se nalazilo preko 250 000 oglasa vezanih uz prodaju narkotika i otrovnih kemikalija te više od 100 000 oglasa za prodaju ukradenih i lažnih identifikacijskih dokumenata te drugih osobnih podataka, krivotvorene robe, zlonamjernih softvera, hakerskih alata, vatrenog oružja i pružanje neovlaštenih usluga. Zbog navedenog se *AlphaBay* smatralo najvećim crnim tržištem,

[46] Christin, N., 2012. *Traveling the Silk Road: a Measuremenet analysis of a large anonymous online marketplace*. Dostupno na: https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf (10.6.2020.)
[47] Bertrand, N., 2015. *The FBI Staged A Lovers' Fight To Catch The Kingpin Of The Web's Biggest Illegal Drug Marketplace*. Business Insider. Dostupno na: https://www.businessinsider.com/ross-ulbricht-will-be-sentenced-soon--heres-how-he-was-arrested-2015-5 (10.6.2020.)
[48] United States District Court Eastern District of California, 2017. *Cazes Forfeiture Complaint And Exhibits*. Washington, DC. Dostupno na: https://www.justice.gov/opa/press-release/file/982821/download (11.6.2020.)

dok je Svileni put na svom kraju 2013. godine sadržavalo otprilike 14 000 oglasa za ilegalnu robu i usluge.[49]

5.3. Kriptovalute

Kriptovaluta je digitalni ili virtualni novac koji je kreiran kao sredstvo digitalne razmjene. Ključna karakteristika kriptovaluta je ta što ih ne izdaje niti jedno središnje tijelo stoga vlada nije u mogućnosti njima manipulirati. Pojam „kripto" u nazivu ukazuje na metode enkripcije koje se koriste za postizanje velike razine sigurnosti kod transakcija.[50] Kriptovalute se pohranjuju u digitalnom novčaniku, a on se uglavnom nalazi na mrežnim stranicama servisa koji tu uslugu pružaju ili je moguće preuzeti aplikaciju na mobilni uređaj.

Za izvršenje transakcija u mračnoj mreži najviše se koriste kriptovalute *Bitcoin*, *Monero* i *ZCash*.[51] Trenutni ukupni broj postojećih valuta iznosi 5 726, a njihov udio na tržištu prelazi 270,5 milijardi dolara.[52]

5.3.1. Bitcoin

Kriptovaluta *Bitcoin* (skraćeno BTC) je prva decentralizirana *peer-to-peer* mreža za vršenje transakcija prvi put predstavljena 2009. godine, a jedan Bitcoin danas doseže vrijednost od oko 12 tisuća dolara.[53] Identitet programera koji ju je kreirao nije poznat, već se vodi pod imenom Satoshi Nakamoto.

---

[49] Sulleyman, A., 2017. *Alphabay: What is the Dark Web marketplace linked to several deaths?*. The Independent. Dostupno na: https://www.independent.co.uk/life-style/gadgets-and-tech/news/alphabay-down-reddit-what-is-it-dark-web-website-illegal-drugs-marketplace-us-justice-department-a7851681.html (10.7.2020.)

[50] Frankenfield, J., 2020. *Cryptocurrency. Investopedia*. Dostupno na: https://www.investopedia.com/terms/c/cryptocurrency.asp (13.7.2020.)

[51] CoinNewsLive. 2019. Meet The Top 3 Cryptocurrencies Used On The Dark Web - Coinnewslive. Dostupno na: https://coinnewslive.com/meet-the-top-3-cryptocurrencies-used-on-the-dark-web/ (13.07.2020.)

[52] CoinMarketCap. 2020. Cryptocurrency Prices, Charts And Market Capitalizations | Coinmarketcap. Dostupno na: https://coinmarketcap.com/ (13.7.2020.)

[53] CoinDesk. 2020. *Bitcoin Price Index — Coindesk 20*. Dostupno na: https://www.coindesk.com/price/bitcoin (15.8.2020.)

Za korištenje je potrebno preuzeti Bitcoin novčanik (engl. *Bitcoin wallet*) na računalo ili mobilnu aplikaciju koji će generirati Bitcoin adresu putem koje je moguće vršiti i primati uplate. Bitcoin adrese ne zahtijevaju unos osobnih podataka ili bankovni račun, a zapis svake transakcije koja se izvrši pomoću Bitcoina pohranjuje se u tzv. blok lanaca (engl. *block chain*) čime se rješava pitanje verifikacije i validnosti uplata.[54]

Kako niti jednu kriptovalutu, pa tako i Bitcoin, ne izdaju banke ili središnja tijela, ono se može pridobiti na dva načina: računalnim rudarenjem i kupnjom s nacionalnim novčanim valutama. Za rudarenje je potrebno posjedovati snažnu računalnu opremu, posebice grafičke kartice i napajanje, a prilikom rudarenja računala rješavaju kompleksne matematičke algoritme.[55]

5.3.2. Monero

Monero (skraćeno XMR) je decentralizirana *peer-to-peer* kriptovaluta otvorenog koda razvijena 2014. godine.[56] Razvila se iz kriptovalute Bytecoin nakon što su otkriveni njeni nedostaci, među kojima je presudan bio taj da je prilikom samog predstavljanja kriptovalute ustanovljeno kako 80% "novčića" koji će ikada moći biti prikupljeni rudarenjem zapravo već postoje. Nadalje je nastala kriptovaluta Bitmonero, a nakon skraćivanja naziva danas je poznata kao Monero.[57]

Bytecoin je koristio CryptoNote protokol koji je između ostalog primijenjen i na Monero, a protokol obuhvaća prstenaste potpise, tajne adrese i prilagodljiva ograničenja.[58] Prstenasti potpis (engl. *ring signatures*), je vrsta digitalnog potpisa koji se koristi prilikom autorizacije transakcija. Potpis čini skup od nekoliko pojedinaca pa samim

[54] Bitcoin.org. *FAQ - Bitcoin*. Dostupno na: https://bitcoin.org/en/faq (30.6.2020.)
[55] Reiff, N., 2020. *What Are The Advantages Of Paying With Bitcoin?*. Investopedia. Dostupno na: https://www.investopedia.com/ask/answers/100314/what-are-advantages-paying-bitcoin.asp (5.8.2020.)
[56] Frankenfield, J., 2019. Monero Definition. Investopedia. Dostupno na: https://www.investopedia.com/terms/m/monero.asp (24.8. 2020.)
[57] BitDegree.org Online Learning Platforms. 2020. *Complete Monero Guide: Everything About The Famous Monero Coin*. Dostupno na: https://www.bitdegree.org/tutorials/monero/#strongthe-history-of-monerostrong (24.8.2020.)
[58] Mycryptopedia. 2018. *Cryptonight & Cryptonote Explained – Mycryptopedia*. Dostupno na: https://www.mycryptopedia.com/cryptonight-cryptonote-explained/ (24.8.2020.)

time prilikom autorizacije transakcije neće biti moguće razaznati točnog člana čijim je potpisom ona odobrena.[59] Tajna adresa služi za slanje uplate te istu stvara pošiljatelj uplate za svaku transakciju koju izvrši. Za kreiranje tajne adrese koriste se tzv. ključ za trošenje (engl. *spend key*) i ključ za gledanje (engl. *view key*). Ključ za trošenje služi za slanje uplata, a s ključem za gledanje prikazuju se pristigle uplate. Ako pojedinac odluči podijeliti stanje svog računa s nekim drugim, isto je u mogućnosti napraviti dijeljenjem svojega ključa za gledanje.[60] Nadalje, prilagodljiva ograničenja odnose se, primjerice, na veličinu blokova i razinu težine rudarenja. Blokovi se stvaraju rudarenjem i sadrže transakcije te *coinbase* transakcije. *Coinbase* transakcije dodaju nove Monero novčiće u mrežu.

Monero je postao izrazito popularan nakon zatvaranja crnog tržišta Svileni put zbog sumnje u sigurnost Bitcoina te je shodno tome postao njegova najčešće birana alternativa zbog izrazite razine privatnosti koju pruža svojim načinom verifikacije i slanja transakcija pošto je istima nemoguće ući u trag.

5.3.3. ZCash

ZCash (skraćeno ZEC) je kriptovaluta predstavljena 2016. godine, a prvotno je nastala 2013. godine pod nazivom *Zerocoin*. U odnosu na BitCoin i Monero za koje nisu poznati identiteti njihovih tvoraca, ZCash je kreirala istoimena tvrtka, a njen razvoj nastavlja tvrtka Electric Coin Company. Osnivač i direktor tvrtke ECC je Zooko Wilcox te su ujedno i javno dostupna imena ostalih članova tima koji prvenstveno djeluju u područjima računarstva i kriptografije. [61][62]

Uslijed potrebe za anonimnim načinom provođenja transakcija na mračnoj mreži, ZCash je uz Bitcoin i Monero najčešće korištena kriptovaluta. Tajnost identiteta

[59] Monero – secure, private, untraceable. *Moneropedia: Ring Signature*. Dostupno na: https://web.getmonero.org/resources/moneropedia/ringsignatures.html (24.8.2020.)
[60] Monero – secure, private, untraceable. *Moneropedia: Stealth Address*. Dostupno na: https://web.getmonero.org/resources/moneropedia/stealthaddress.html (24.8.2020.)
[61] Wheal, C., 2018. *A History Of Zcash (ZEC)*. OpenLedger DEX. Dostupno na: https://dex.openledger.io/a-history-of-zcash-zec/ (25.8.2020.)
[62] Electric Coin Company. *About - Electric Coin Company*. Dostupno na: https://electriccoin.co/about/ (25.8.2020.)

korisnika postiže tehnologijom *Zero-knowledge Succinct Non-Interactive Argument of Knowledge* (skraćeno zk-SNARKs) kojom je moguće dokazati posjedovanje neke informacije bez otkrivanja iste i bez uspostavljanja komunikacije između strane koja informaciju dokazuje i one koja ju treba verificirati.[63] Sve izvršene transakcije bit će zabilježene u bloku lanaca (engl. *block chain*) koji je javno dostupan, ali je transakciju moguće izvršiti na dva načina: transparentni ili privatni. Kod transparentne transakcije koristi se transparentna adresa, odnosno *t-address.* U tom će slučaju u bloku lanaca adrese pošiljatelja i primatelja te vrijednost same transakcije biti vidljivi. S druge strane, kod korištenja zaštićenih adresa, *z-address*, sve informacije o transakciji ostaju nepoznate. [64]

[63] Zcash. *What Are Zk-Snarks?*. Dostupno na: https://z.cash/technology/zksnarks/ (25.8.2020.)
[64] Zcash. *How It Works*. Dostupno na: https://z.cash/technology/ (25.8.2020.)

6. Zaključak

Ideja pojedinca o razvijanju mreže koja se sastoji od nekoliko međusobno povezanih računala pokrenula je lavinu novih vizija, teorija i istraživanja koja su naposljetku vodila prema njenom unaprjeđenju i rapidnom razvijanju globalne mreže. Jednostavne statičke mrežne stranice pisane čistim HTML kodom bile su začeće *World Wide Weba* kakav danas postoji, a ljudska znatiželja i ispitivanje granica uvjetovale su umrežavanju cijelog svijeta i razvijanju raznih usluga i servisa. Internet je postao primarni izvor informacija, mjesto za relaksaciju te jedno od glavnih komunikacijskih sredstava. Brzina kojom se svjetska mreža širila vodila je prema razvitku pomagala za lakše pronalaženje željenih podataka, mrežnih tražilica. U samim počecima sadržaj *Weba* nije bio opširan stoga je uspješno bio spremljen i lako pretraživ indeksom tražilica. Međutim, onaj sadržaj stranica koji paukovi mrežnih tražilica nisu dohvatili smatrao bi se dijelom duboke mreže koja zbog tehničkih ograničenja tražilica potencijalno nikada neće biti vidljiva na površinskoj mreži. Daljnjim razvitkom mrežnih servisa napravljene su *online* sobe za čavrljanje, društvene mreže, usluge internet bankarstva, portali za kupnju proizvoda te mnogi drugi servisi koji su zahtijevali unos nekih osobnih i privatnih podataka pojedinca. Iako su osjetljivi podaci enkriptirani, ubrzo je ustanovljeno da vlada i neki pružatelji internetske usluge provode nadzor mreže što je također mogla i vršiti neka treća strana korištenjem odgovarajućih alata. Posljedično se javila potreba za anonimnim pretraživanjem interneta, a navedeno su pružali *darkneti* od kojih je najistaknutija Tor mreža. Tor mrežni promet usmjeruje na način da se u slučaju nadzora mreže neće moći zaključiti izvor i odredište podataka. Sukladno, korisnicima je zajamčena tajnost njihovog identiteta i bezbrižno pretraživanje te komunikacija na internetu. Međutim, postoji i određena skupina ljudi koja je navedene pogodnosti odlučila iskoristiti u ilegalne svrhe. Duboka mreža i mračni internet postali su poznati u trenutku pada crnog tržišta Svileni put 2013. godine i često su bili spominjani u kontekstu ilegalnih aktivnosti. Zatvaranje Svilenog puta izazvalo je ispoljavanje novih mračnih tržišta. Na tržištima je najzastupljenija prodaja narkotika i oružja zbog velike potražnje, a nude se još i usluge narudžbe ubojstva, prodaja hakerskih alata i zloćudnih softvera, distribuira se dječja pornografija i tako dalje. Kao sredstvo plaćanja koriste se kriptovalute koje dodatno osiguravaju tajnost identiteta. Iako anonimni servisi nisu kreirani s namjerom da služe kao sredstvo

za prikrivanje dokaza i tragova kriminalaca, nažalost postoje pojedinci koji idu u ekstreme s mišlju da nikada neće biti uhvaćeni.

7. Literatura

1. 2019.torproject.org. Tor Project: Overview. Dostupno na: https://2019.www.torproject.org/about/overview.html.en
2. Bergman, M., K., 2001. White Paper: The Deep Web: Surfacing Hidden Value. The Journal of Electronic Publishing, 7(1). Dostupno na: https://doi.org/10.3998/3336451.0007.104
3. Bertrand, N., 2015. The FBI Staged A Lovers' Fight To Catch The Kingpin Of The Web's Biggest Illegal Drug Marketplace. Business Insider. Dostupno na: https://www.businessinsider.com/ross-ulbricht-will-be-sentenced-soon--heres-how-he-was-arrested-2015-5
4. Biddle, P., England, P., Peinado, M., Willman, B. 2002. The Darknet and the Future of Content Protection. U: J. Feigenbaum (ur.), Digital Rights Management. Washington: Springer. str. 155-176.
5. Bitcoin.org. FAQ - Bitcoin. Dostupno na: https://bitcoin.org/en/faq
6. BitDegree.org Online Learning Platforms. 2020. Complete Monero Guide: Everything About The Famous Monero Coin. Dostupno na: https://www.bitdegree.org/tutorials/monero/#strongthe-history-of-monerostrong
7. Blog.torproject.org. 2016. Tor At The Heart: Securedrop | Tor Blog. Dostupno na: https://blog.torproject.org/tor-heart-securedrop
8. Castro, E., 2007. Getting People to Visit: Keeping Visitors Away. HTML, XHTML and CSS, Sixth Edition: Visual QuickStart Guide. Berkeley: Peachpit Press.
9. Christin, N., 2012. Traveling the Silk Road: a Measuremenet analysis of a large anonymous online marketplace. Dostupno na: https://www.andrew.cmu.edu/user/nicolasc/publications/TR-CMU-CyLab-12-018.pdf
10. Ciancaglini, V., Balduzzi, M., McArdie, R., Rösler. 2015. *Below the Surface: Exploring the Deep Web*. Dostupno na: https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf
11. CoinDesk. 2020. Bitcoin Price Index — Coindesk 20. Dostupno na: https://www.coindesk.com/price/bitcoin

12. CoinMarketCap. 2020. Cryptocurrency Market Capitalizations | Coinmarketcap. Dostupno na: https://coinmarketcap.com/
13. CoinNewsLive. 2019. Meet The Top 3 Cryptocurrencies Used On The Dark Web - Coinnewslive. Dostupno na: https://coinnewslive.com/meet-the-top-3-cryptocurrencies-used-on-the-dark-web/
14. Comer, D., 2019. The Internet Book: Everything You Need to Know about Computer Networking and How the Internet Works. 5th ed. Boca Raton: CRC Press.
15. Community.torproject.org. Tor Project | Types Of Relays On The Tor Network. Dostupno na: https://community.torproject.org/relay/types-of-relays/
16. Dcssproject.net. 2015. Invisible Internet Project (I2P) – Digital Citizenship And Surveillance Society. Dostupno na: https://dcssproject.net/i2p/index.html
17. Dennis, M. A. Cybercrime | Definition, Statistics, & Examples. Encyclopedia Britannica. Dostupno na: https://www.britannica.com/topic/cybercrime
18. Dictionary.cambridge.org. 2020. DARKNET | Meaning In The Cambridge English Dictionary. Dostupno na: https://dictionary.cambridge.org/dictionary/english/darknet
19. Dictionary.cambridge.org. n.d. DEEP WEB | Meaning In The Cambridge English Dictionary. Dostupno na: https://dictionary.cambridge.org/dictionary/english/deep-web
20. Eff.org. What is a Tor Relay? | Tor Challenge Dostupno na: https://www.eff.org/torchallenge/what-is-tor.html
21. Electric Coin Company. About - Electric Coin Company. Dostupno na: https://electriccoin.co/about/
22. Finklea, K., 2017. Dark Web. Dostupno na: https://fas.org/sgp/crs/misc/R44101.pdf
23. Ford, N., Mansourian, Y. 2006. The invisible web: An empirical study of „cognitive invisibility“. Journal of Documentation. 62(5). str. 584 – 596
24. Frankenfield, J., 2019. Monero Definition. Investopedia. Dostupno na: https://www.investopedia.com/terms/m/monero.asp
25. Frankenfield, J., 2020. Cryptocurrency. Investopedia. Dostupno na: https://www.investopedia.com/terms/c/cryptocurrency.asp
26. Freenetproject.org. Documentation. Dostupno na: https://freenetproject.org/pages/documentation.html#understand

27. Freenetproject.org. Help. Dostupno na: https://freenetproject.org/pages/help.html
28. Gayard, L., 2018. Darknet: Geopolitics and Uses. London: ISTE Ltd, Hoboken: John Wiley & Sons, Inc.
29. Gayle, D., 2016. Online Market 'Is Turning Drug Dealers From Goons To Geeks'. The Guardian. Dostupno na:: https://www.theguardian.com/world/2016/feb/11/online-market-turning-drug-dealers-goons-geeks-darknet
30. Gehl, R. W. 2018. Weaving the Dark Web. Legitimacy on Freenet, Tor and I2P. Cambridge, Massachusetts: The MIT Press.
31. Geti2p.net. 2014. Garlic Routing - I2P. Dostupno na: https://geti2p.net/en/docs/how/garlic-routing
32. Geti2p.net. Intro - I2P. Dostupno na: https://geti2p.net/en/about/intro
33. Home.cern. Where The Web Was Born | CERN. Dostupno na: https://home.cern/science/computing/where-web-was-born
34. Info.cern.ch. Http://Info.Cern.Ch. Dostupno na: http://info.cern.ch/
35. internet live stats. Total Number Of Websites. Dostupno na: https://www.internetlivestats.com/total-number-of-websites/
36. Mann, B., 2020. What Is I2P & How Does It Compare Vs. Tor Browser In 2020?. Blokt - Privacy, Tech, Bitcoin, Blockchain & Cryptocurrency. Dostupno na: https://blokt.com/guides/what-is-i2p-vs-tor-browser#Who_develops_/_manages_I2P
37. Metrics.torproject.org. 2020. Onion Services – Tor Metrics. Dostupno na: https://metrics.torproject.org/hidserv-dir-onions-seen.html?start=2020-05-21&end=2020-08-17
38. Metrics.torproject.org. Servers – Tor Metrics. Dostupno na: https://metrics.torproject.org/networksize.html
39. Monero – secure, private, untraceable. Moneropedia: Ring Signature. Dostupno na: https://web.getmonero.org/resources/moneropedia/ringsignatures.html
40. Monero – secure, private, untraceable. Moneropedia: Stealth Address. Dostupno na: https://web.getmonero.org/resources/moneropedia/stealthaddress.html

41. Mycryptopedia. 2018. Cryptonight & Cryptonote Explained – Mycryptopedia. Dostupno na: https://www.mycryptopedia.com/cryptonight-cryptonote-explained/
42. Norris, J., 2020. The Privacy Pros And Cons Of The I2P Network. Vpnmentor.com. Dostupno na: https://www.vpnmentor.com/blog/pros-cons-i2p-network/
43. Ozkaya, E., Islam, R., 2019. Inside the Dark Web. Boca Raton: CRC Press.
44. Reiff, N., 2020. What Are The Advantages Of Paying With Bitcoin?. Investopedia. Dostupno na: https://www.investopedia.com/ask/answers/100314/what-are-advantages-paying-bitcoin.asp
45. Rouse, M., 2017. What Is ARPANET? - Definition From Whatis.Com.SearchNetworking. Dostupno na: https://searchnetworking.techtarget.com/definition/ARPANET
46. Scos.training. History Of TCP/IP | Scos Training. Dostupno na: https://www.scos.training/history-of-tcp-ip/
47. Sherman, C. and Price, G., 2001. The Invisible Web: Uncovering Information Sources Search Engines Can't See. Medford, N. J.: CyberAge Books.
48. Sulleyman, A., 2017. Alphabay: What is the Dark Web marketplace linked to several deaths?. The Independent. Dostupno na: https://www.independent.co.uk/life-style/gadgets-and-tech/news/alphabay-down-reddit-what-is-it-dark-web-website-illegal-drugs-marketplace-us-justice-department-a7851681.html
49. Taylor, I., 2005. Freenet. From P2P To Web Services And Grids. London: Springer.
50. Techopedia.com. 2019. What Is The Deep Web? - Definition From Techopedia. Dostupno na: https://www.techopedia.com/definition/15653/deep-web
51. Torproject.org. The Tor Project | Privacy & Freedom Online. Dostupno na: https://www.torproject.org/about/history/
52. United States District Court Eastern District of California, 2017. Cazes Forfeiture Complaint And Exhibits. Washington, DC. Dostupno na: https://www.justice.gov/opa/press-release/file/982821/download
53. Wheal, C., 2018. A History Of Zcash (ZEC). OpenLedger DEX. Dostupno na: https://dex.openledger.io/a-history-of-zcash-zec/

54. Wood, J. A. 2010. The Darknet: A Digital Copyright Revolution. Richmond Journal of Law and Technology, 16 (4). Dostupno na: https://scholarship.richmond.edu/jolt/vol16/iss4/4/
55. World Wide Web Foundation. History Of The Web. Dostupno na: https://webfoundation.org/about/vision/history-of-the-web/
56. Zcash. How It Works. Dostupno na: https://z.cash/technology/
57. Zcash. What Are Zk-Snarks?. Dostupno na: https://z.cash/technology/zksnarks/

Duboka mreža i mračni internet

Sažetak

Svjetska mreža, *World Wide Web*, dijeli se na površinsku mrežu, duboku mrežu i mračnu mrežu. Sadržaj površinske mreže dostupan je pretraživanjem putem tražilica kao što su to *Google* i *Bing* koje prikazuju indeksirani sadržaj. Duboka mreža obuhvaća onaj sadržaj koji mrežne tražilice nisu indeksirale. Ne postoji točna informacija o veličini duboke mreže, no smatra se da je ona 4 do 5 tisuća puta veća od površinskog *Weba.* Mračna mreža je dio duboke mreže, a pristup joj je moguć isključivo putem mračnog interneta korištenjem određenih alata i programa. Najpoznatiji takav servis je Tor koji jamči tajnost identiteta prilikom korištenja Tor preglednika. Zbog razine anonimnosti koju pruža, mračna mreža je leglo ilegalnih i kriminalnih radnji. Najposjećenija mjesta mračne mreže su crna tržišta koja na raspolaganje stavljaju ponajviše narkotike i oružja. Transakcije se na tržištima vrše u kriptovalutama, a najčešće korištena je kriptovaluta Bitcoin.

Ključne riječi: duboka mreža, mračni internet, mračna mreža, slojevito usmjeravanje, crna tržišta

Deep Web and Darknet

Summary

The World Wide Web is divided into the Surface Web, Deep Web and the Dark Web. The contents of the Surface web are available through the use of search engines such as Google and Bing, which show indexed content. The Deep Web shows the content which the search engines have not indexed.Information about the actual size of the Deep Web does not exist, but it is believed that its size is about 4-5 thousand times bigger than the Surface Web. The Dark Web is a part of the Deep Web, which is only accessible through the darknets with the use of special tools and applications. The most well known service is Tor which guarantees anonymity while using the Tor browser. Because of its level of anonymity, the Dark Web is full of illegal actions and crime. The most visited sites on the Dark Web are Black markets which offer a variety of narcotics and weapons. Transactions made on the Dark Web are being done with cryptocurrencies, most commonly Bitcoin.

Key words: Deep Web, darknet, Dark Web, the onion routing, black markets