



The Deep Web, the Darknet, and Bitcoin

Elisa Cooper & Akino Chikada

MarkMonitor



Agenda

- Deep Web vs Darknet
- Tor
- Underground Marketplaces
- Role of Bitcoin
- Strategies for Mitigating Abuse
- Q&A Session

Understanding the Internet Landscape

Surface Web

Searchable with standard search engines

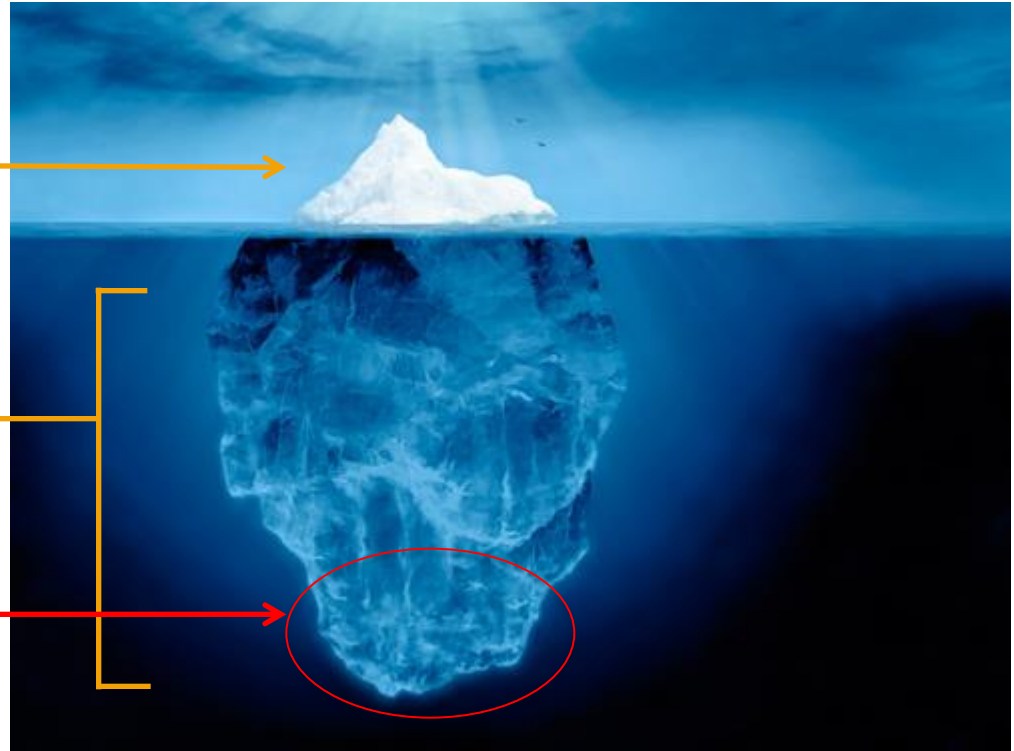
Deep Web

Un-indexed websites

Dark Web / DarkNet

Dark Web: web content that exists on the DarkNet

DarkNet: Network that can only be accessed with specific software, configurations, or authorization



The Deep Web is hundreds of times larger than the 'Surface Web'



What's in the Deep Web?

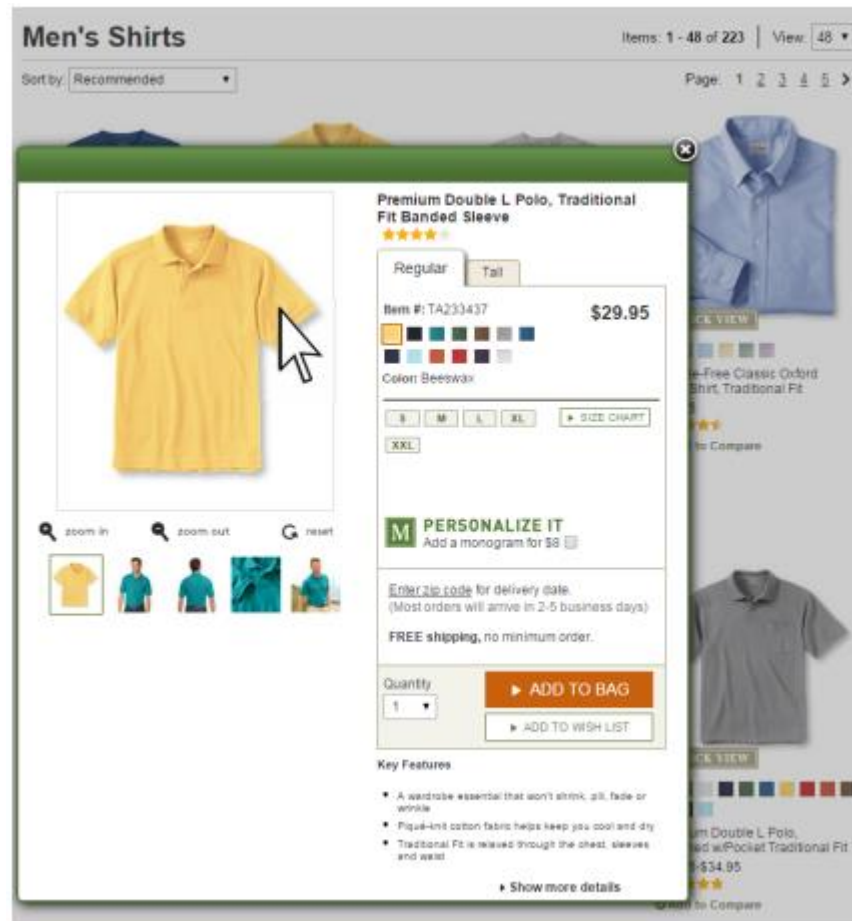
- 96% of the content exists in the deep web
 - 7500+ TB of content

- Types of content that is in the deep web:
 - Dynamic content
 - Unlinked content
 - Private Web
 - Contextual Web
 - Limited access content
 - Scripted content
 - Non-HTML/text content
 - Software
 - Web archives
 - Un-indexed websites
 - P2P networks

Deep Web Content

Not Everything in the Deep Web is Seedy

- Forms
- Login / Paywall
 - Corporate Intranet
 - Social Media Sites
- No URL





Deep Web Content of Concern

- Any un-indexed web page
 - Selling counterfeit or grey market goods
 - Collecting user credentials
 - Disseminating malware
 - Engaged in false association
 - Conducting consumer scam
- P2P sites where piracy taking place
- Marketplaces where counterfeit, grey market or unauthorized goods are sold
- Social media where impersonation is occurring

How Are Consumers Directed to the Deep Web?





So What Is the Darknet?

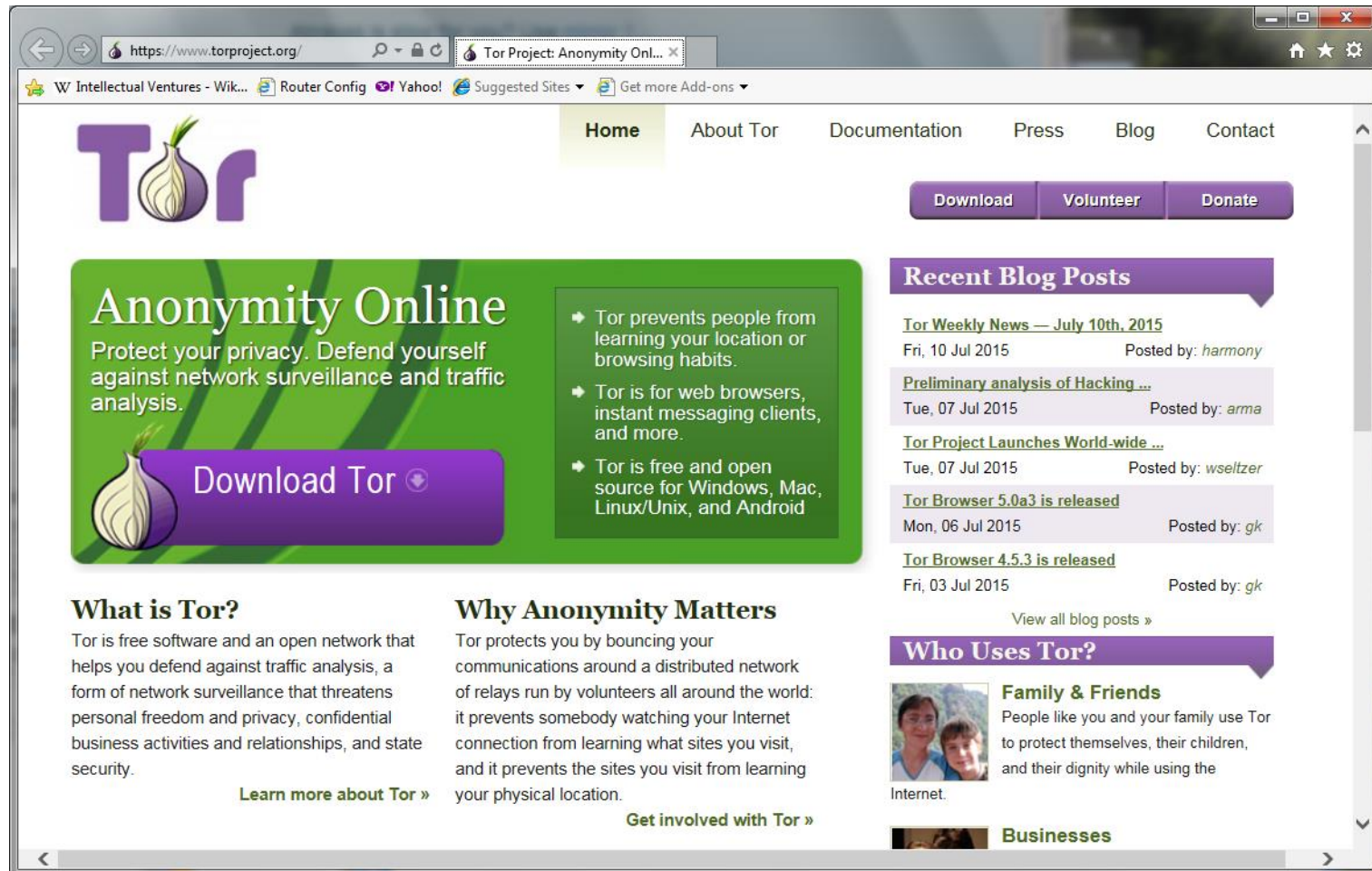
- Within the Darknet both web surfers and website publishers are entirely anonymous
- Anonymity is usually achieved using Tor
- There are a number of marketplaces (the online black market)
 - Abraxas
 - Agora Marketplace
 - Middle Earth Marketplace
 - Nucleus
 - Silk Road 1, 2 and 3



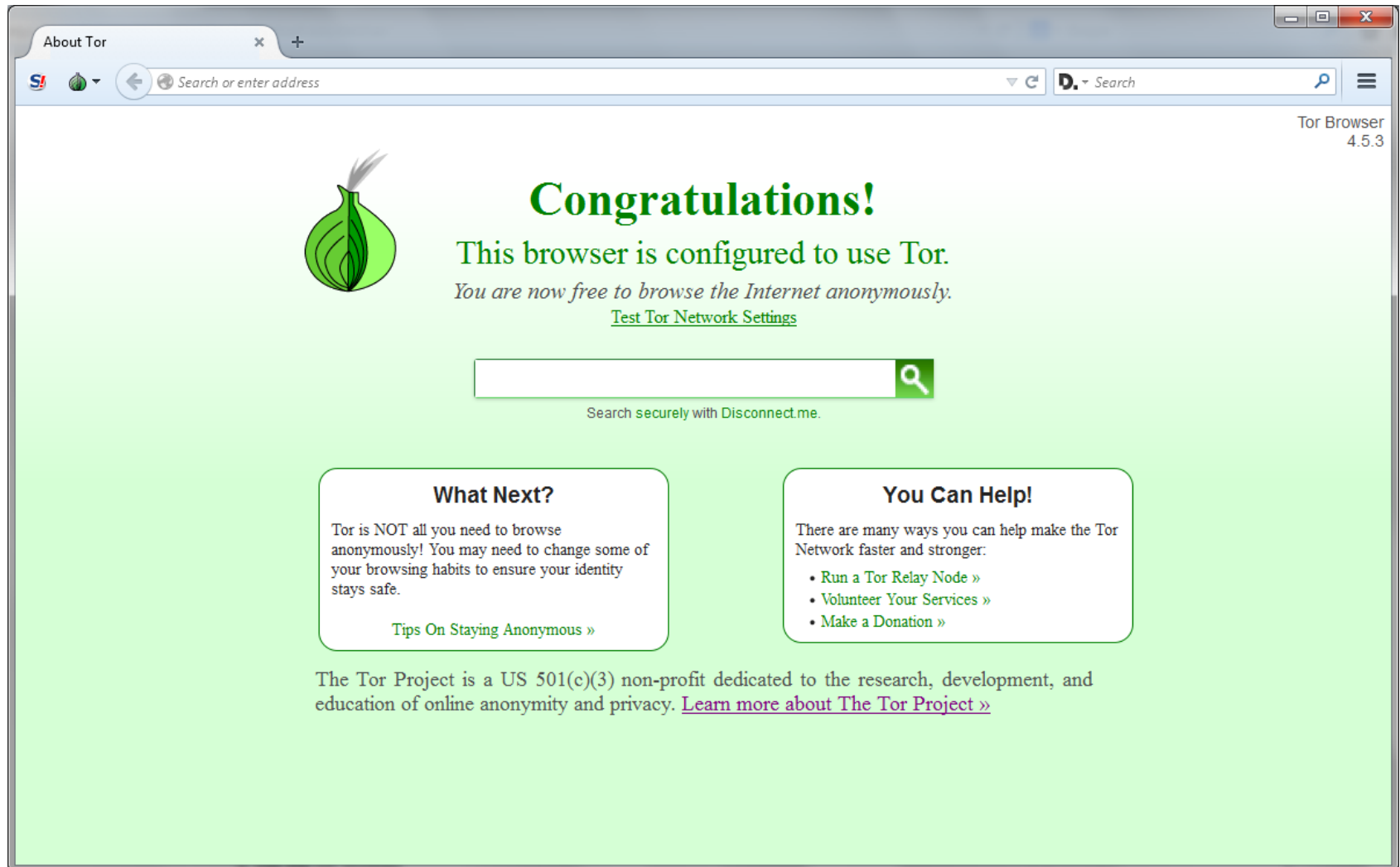
What is Tor?

- Acronym for The Onion Router
- Free software for enabling anonymous communication
- Originally developed on behalf of the U.S. intelligence community
- Today it is used by criminal enterprises, hacktivists, and law enforcement agencies
 - Users can remain anonymous
 - Activities can remain untraceable
 - Resources can remain hidden

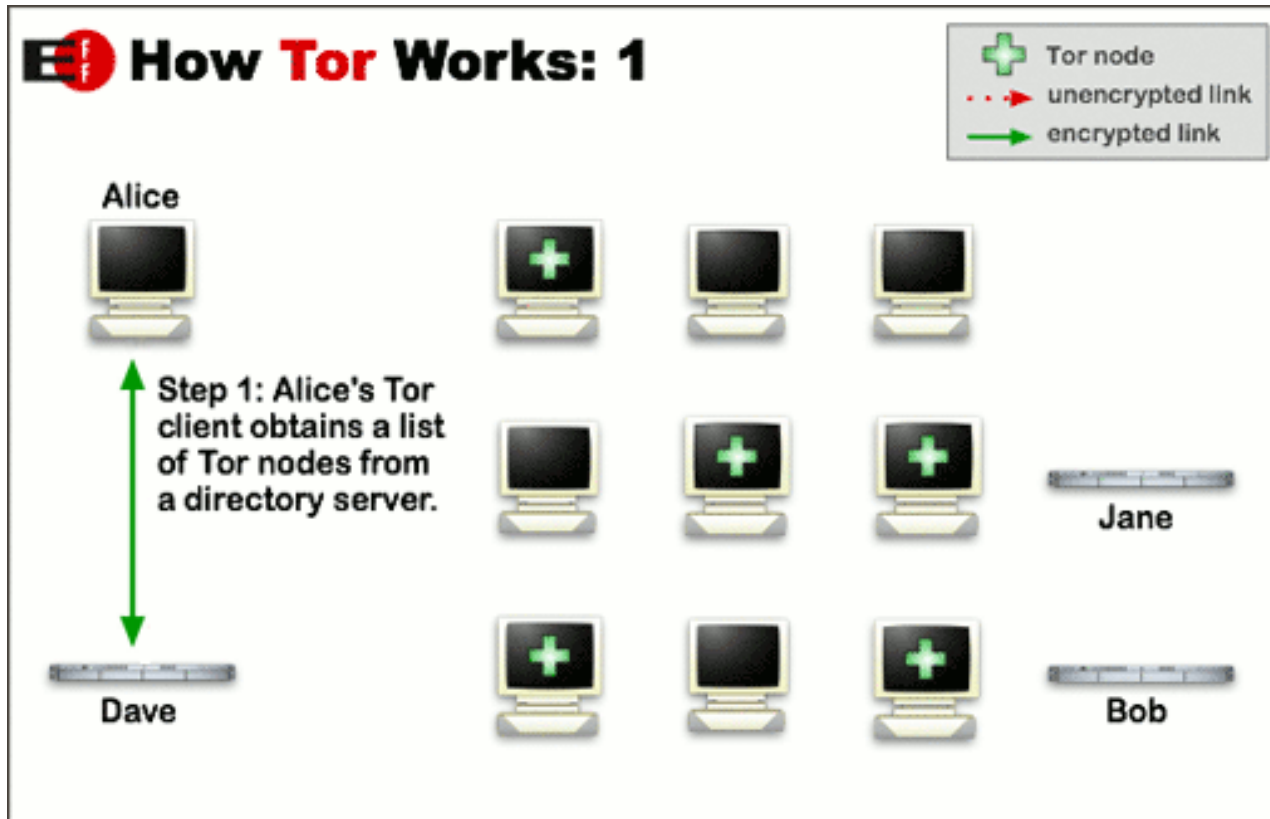
How is Tor Accessed?

A screenshot of the Tor Project website as it appeared in mid-2015. The browser window shows the URL https://www.torproject.org/. The website has a purple and green color scheme. At the top, there's a navigation bar with links: Home, About Tor, Documentation, Press, Blog, and Contact. Below this is a secondary navigation bar with buttons for Download, Volunteer, and Donate. The main content area is divided into several sections. On the left, there's a large green box with the text 'Anonymity Online' and a sub-headline 'Protect your privacy. Defend yourself against network surveillance and traffic analysis.' Below this is a purple button that says 'Download Tor' with a small onion icon. To the right of this box is a list of three bullet points: 'Tor prevents people from learning your location or browsing habits.', 'Tor is for web browsers, instant messaging clients, and more.', and 'Tor is free and open source for Windows, Mac, Linux/Unix, and Android'. Below the green box, there are two columns of text. The left column is titled 'What is Tor?' and describes Tor as free software and an open network that helps defend against traffic analysis. Below this text is a link 'Learn more about Tor »'. The right column is titled 'Why Anonymity Matters' and explains how Tor protects users by bouncing communications around a distributed network of relays. Below this text is a link 'Get involved with Tor »'. On the right side of the page, there's a section titled 'Recent Blog Posts' which lists several recent posts with their dates and authors. Below this is a link 'View all blog posts »'. At the bottom right, there's a section titled 'Who Uses Tor?' which includes two sub-sections: 'Family & Friends' with a photo of a family and text about protecting themselves and their children, and 'Businesses' with a photo of people in a meeting.

The Tor Browser

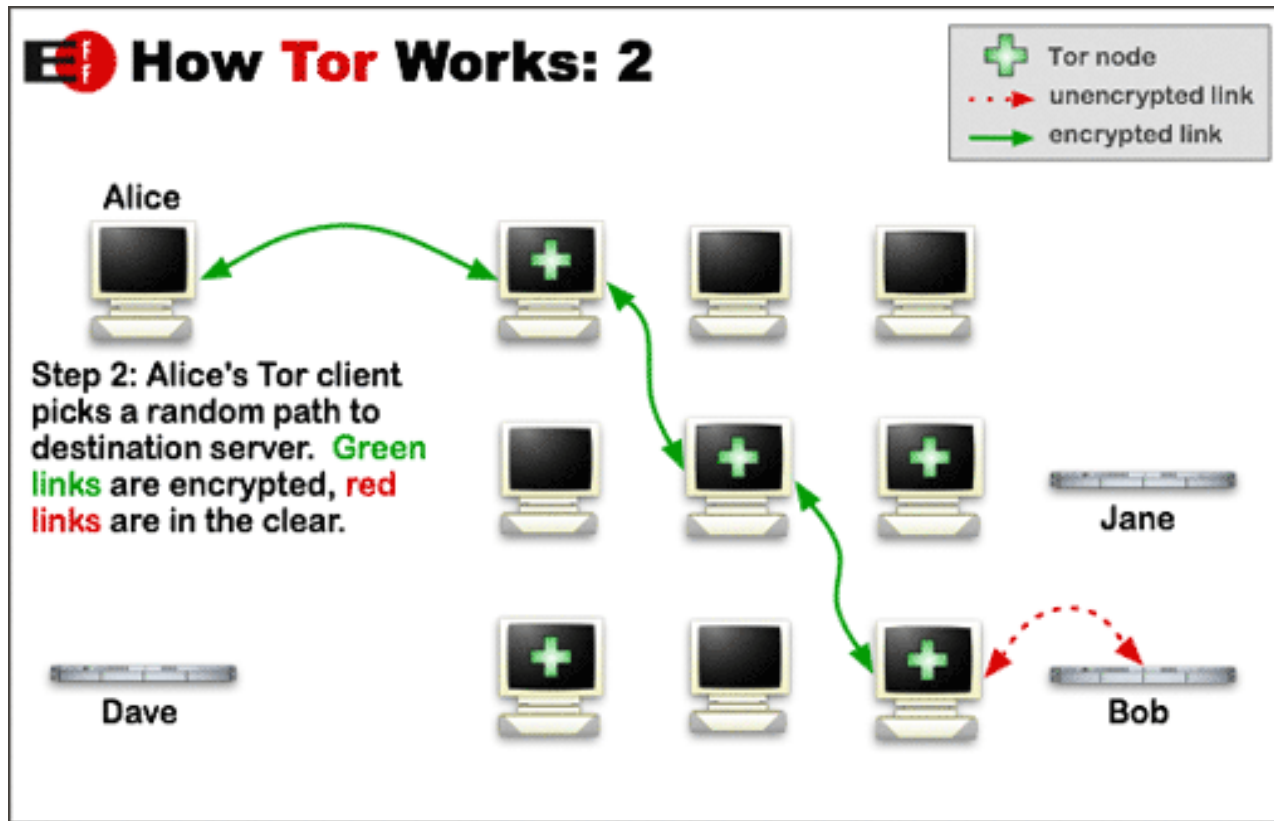


How Does Tor Work?



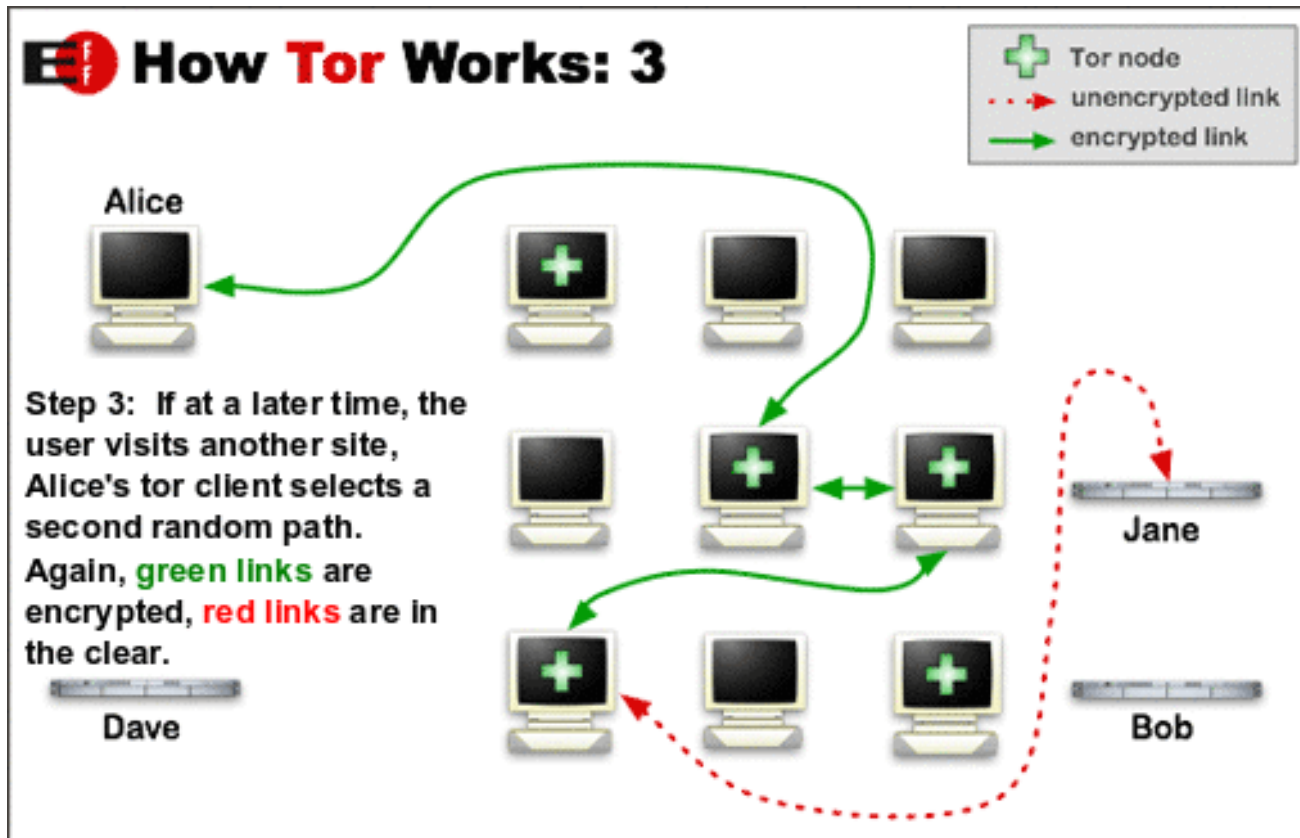
torproject.org

How Does Tor Work?



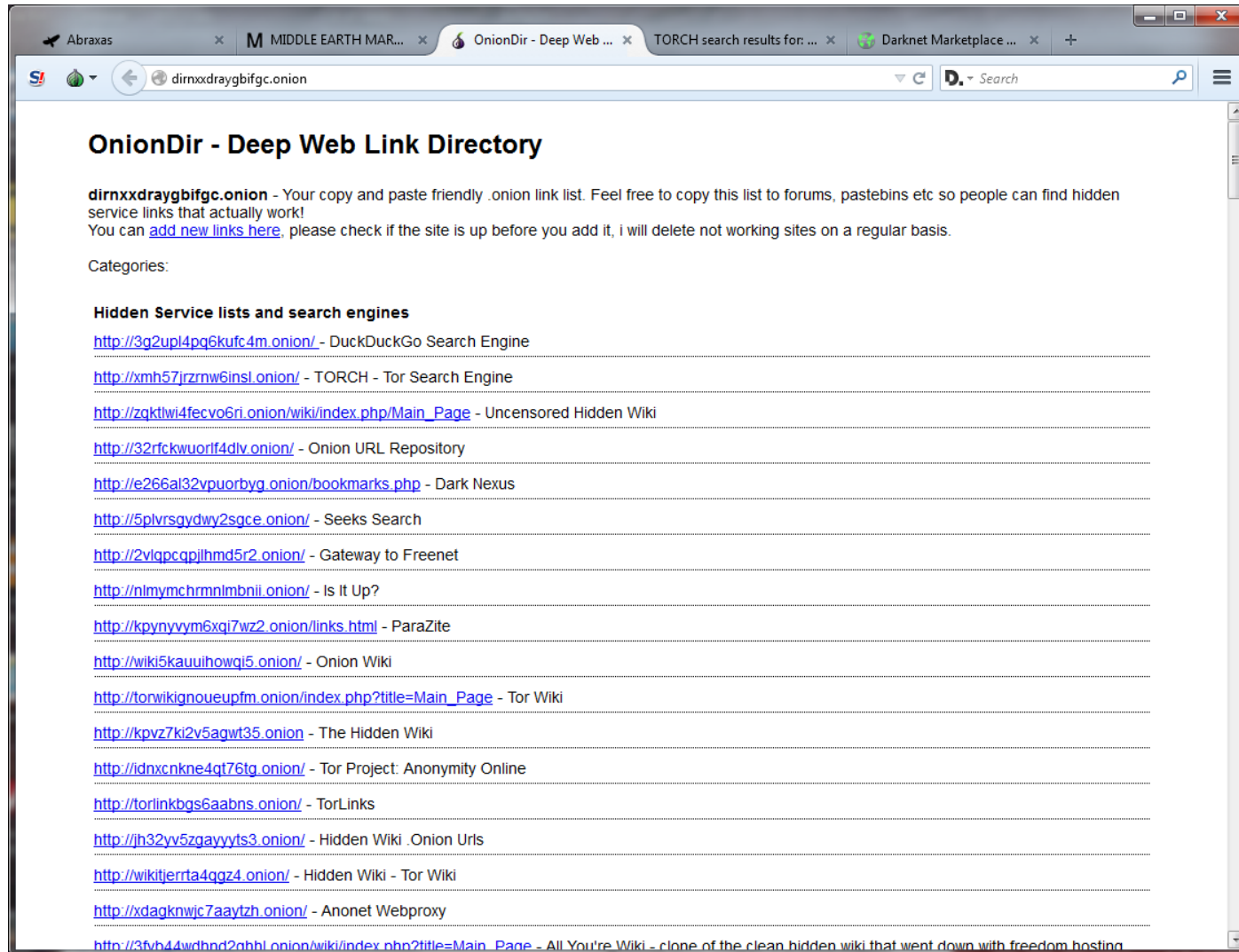
torproject.org

How Does Tor Work?

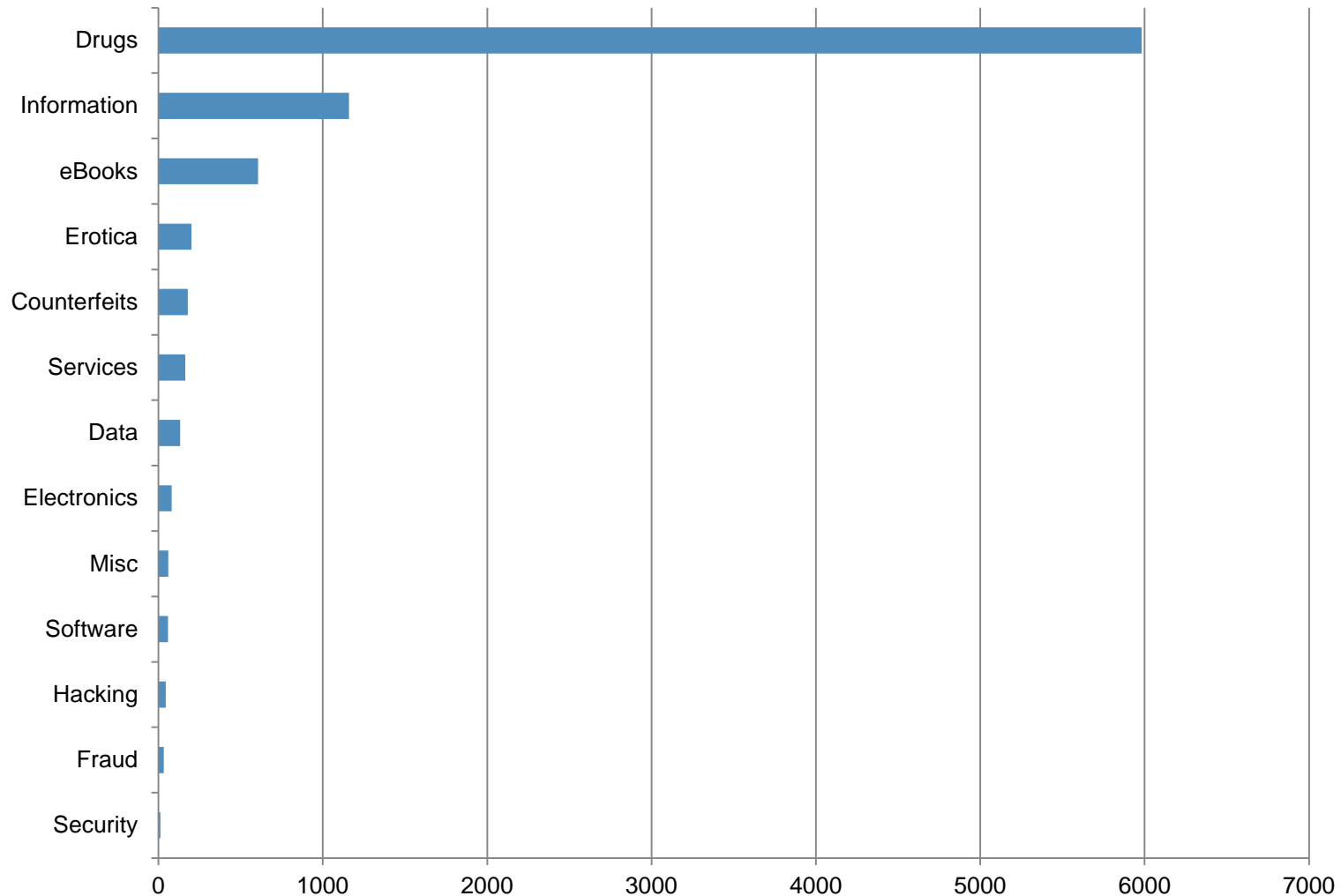


torproject.org

Accessing Underground Marketplaces



What's Sold on a Typical Tor Marketplace?



Source: Abraxas marketplace



Underground Marketplaces on Tor

- Typically require registration
- Some require invitation to join
 - Link on another site – not difficult to obtain
- Some marketplaces are sophisticated
 - Seller ratings
 - Seller profiles
 - Order history
 - Online discussions groups

Typical Tor Marketplace

Abraxas

abraxasdegupusel.onion

Abraxas is slow for you? Use mirror 1.

Listings Profile Messages Orders Forums Support

JenniferJones72 Logout
Wallet Escrow
BTC 0.00000000 0.00000000
DASH 0.00000000 0.00000000

Listings

Search Go

Digital Goods 2807
Drugs 5472
Drugs Paraphernalia 307
Services 163
Other 335

BTC Exchange
\$ 295.83
€ 265.11
£ 397.34
¥ 190.62
₹ 374.71

DASH Exchange
\$ 0.01285300
€ 3.80
£ 3.41
¥ 5.11
₹ 2.45
₹ 4.82

25g Super Lemon Haze FE
0.75441692 B(🇩🇪)

How To Hack Into A Comput...
0.02000000 B(🇩🇪)

How To Achieve Maximum Ar...
0.02140000 B(🇩🇪)

28x Oxycontin 80mg
2.90450515 B(🇩🇪)

2 GRAM MDMA DUTCH HIGH GRA...
0.26404592 B(🇩🇪)

100g Brown Colour MDMA cristal fr...
4.19689084 B(🇩🇪)

Acrylic Snuff Bullet - NEW!
0.06422673 B(🇩🇪)

50gr Mazar-Sharif Hash A+ Coffee
0.81099819 B(🇩🇪)

Secret Betting Club and Making LOT: A Guide To Field-Manufactured Exp...
0.00338035 B(🇩🇪)

14.0 Grams Straight off the Key Coc...
2.53526554 B(🇩🇪)

14g Dutch MDMA Best Quality
0.79194916 B(🇩🇪)

Drugs4you

Rivotril®
Clonazepam
2 mg
9 comprimidos birranurados

Revised Black Book
A Guide to Field-Manufactured Explosives

AcirLa
April 16, 2015

MASERATI

PATENTE DI GUIDA REPUBBLICA ITALIANA
1. RABIERA
2. ROBERTO
22/06/76 CATANIA
09/10/2010 U.C.G.
10/11/2015 U7481554P
S. GREGORIO DI CATANIA (CT)
VIA BELLINI 38

Typical Tor Marketplace - Pirated Software

The screenshot displays a web browser window with a Tor marketplace interface. The address bar shows a .onion URL. A navigation bar at the top includes links for Listings, Profile, Messages, Orders, Forums, and Support. A user profile for 'JenniferJones72' is visible in the top right, along with wallet and escrow information for BTC and DASH. The main content area features a sidebar with category filters (Digital Goods, Data, Drugs, E-Books, Erotica, Fraud, etc.) and a list of software products. Each listing includes a thumbnail, title, description, price, shipping information, and vendor details.

Software :: Digital Goods :: ...

abraxasdegupusel.onion/c/AO6BIMZQwV?q=&sort=users.trades&deliver_to=1

Abraxas is slow for you? Use mirror 1 .






Listings Profile Messages Orders Forums Support

JenniferJones72 Logout
Wallet Escrow
BTC 0.00000000 0.00000000
DASH 0.00000000 0.00000000

Software / Digital Goods / Listings

Search Go

☐ No FE first ☐ I can buy ☐ Active vendor Sort: Vendor #deals Show domestic first ☐ Unknown Go

Name	Price	Shipping	Vendor
 Discover how to open, identify, target, and close, hot 'n ready leads with a snea...	0.01689818	From:Unknown To:worldwide	etimbuk 5/5 , 200~500
 Long Tail Pro Platinum 2.4.26 SEO (Best keyword research software) Long Tail Pro is a powerful keyword research software. Long Tail Pro allows the user to generate hun...	0.01689818	From:Unknown To:worldwide	etimbuk 5/5 , 200~500
 CCleaner Pro + Business CCleaner removes cookies, temporary files and various other unused data that clogs up your operating...	0.01689818	From:Unknown To:worldwide	etimbuk 5/5 , 200~500
 Facebook Software (5 softwares in 1) Get 5 i... softwares in 1 bundle. Ill give you the following : software for an unbeli...	0.05069453	From:Unknown	etimbuk 5/5 , 200~500
 Ranking Software (6 softwares in 1) Get... softwares in 1 bundle. Ill give you the following software for an unbelieva...	0.06759271	From:Unknown	etimbuk 5/5 , 200~500

BTC Exchange
\$ 295.89
€ 265.16
£ 397.42
¥ 190.66
₹ 374.79

DASH Exchange

Typical Tor Marketplace - Luxury Goods

The screenshot shows a web browser window displaying the Abraxas marketplace. The address bar shows the URL `abraxasdegupusel.onion/c/MQNLVpw5lv?q=wallet`. A message at the top says "Abraxas is slow for you? Use mirror 1 .". The navigation bar includes links for Listings, Profile, Messages, Orders, Forums, and Support. A user profile for JenniferJones72 is visible in the top right, showing a Wallet balance of 0.00000000 BTC and 0.00000000 DASH. The main content area displays a list of wallet replicas for sale. On the left, there is a sidebar with a search bar containing "wallet" and a "Go" button. Below the search bar, there are category links: Other (335), Counterfeits (178), Electronics (80), Jewellery (8), Lab Supplies (1), Miscellaneous (18), Weapons (33), Digital Goods (2807), Drugs (5473), Drugs Paraphernalia (307), Services (163), and Other (335). At the bottom left, there are exchange rates for BTC and DASH. The main listing area has filters for "No FE first", "I can buy", "Active vendor", and a "Sort: Default" dropdown. The listings are sorted by price, with the first item being a "wallet Replica-1124" for 0.28741501 BTC. The second item is a "Wallet Replica" for 0.33137260 BTC. The third item is a "Zipper Wallet M60017 Replica" for 0.32122854 BTC. The fourth item is a "Wallet N60825 Replica" for 0.28741501 BTC. The fifth item is a "Wallet N60824 Replica" for 0.29755907 BTC. Each listing includes a small image of the wallet, a title, a description, a price, a shipping location (Hong Kong), and a vendor name (Bigdeal100).

Other :: Abraxas

abraxasdegupusel.onion/c/MQNLVpw5lv?q=wallet

Abraxas is slow for you? Use mirror 1 .

Listings Profile Messages Orders Forums Support

JenniferJones72 Logout

Wallet Escrow

BTC 0.00000000 0.00000000

DASH 0.00000000 0.00000000

Other / Listings

wallet Go

Other (335)

Counterfeits (178)

Electronics (80)

Jewellery (8)

Lab Supplies (1)

Miscellaneous (18)

Weapons (33)

Digital Goods (2807)

Drugs (5473)

Drugs Paraphernalia (307)

Services (163)

Other (335)

BTC Exchange

\$ 295.74

€ 265.03

£ 397.22

¥ 190.56

\$ 374.6

DASH Exchange

0.01278903

\$ 3.78

€ 3.39

£ 5.08

¥ 2.44

\$ 4.79

No FE first I can buy Active vendor Sort: Default Show domestic first Unknown Go

Name Price Shipping Vendor

wallet Replica-1124 0.28741501 From: Hong Kong FE Only Bigdeal100, 0

For whom(M/F): male Description: This wallet is 1:1 exactly replica, top Grade Quality Guarant...

Wallet Replica 0.33137260 From: Hong Kong FE Only Bigdeal100, 0

Wallet Replica Description This Prada Wallet Replica is even better than 1:1 replica...

Zipper Wallet M60017 Replica 0.32122854 From: Hong Kong FE Only Bigdeal100, 0

Description Zipper Wallet M60017 is 1:1 replica, comes with serial number, authenticity car...

Wallet N60825 Replica 0.28741501 From: Hong Kong Bigdeal100, 0

Wallet N60825 Replica Description Wallet N60825 is 1:1 replica, comes with serial num...

Wallet N60824 Replica 0.29755907 From: Hong Kong FE Only Bigdeal100, 0

Wallet N60824 Replica Description Wallet N60825 is 1:1 replica, comes with serial num...

Typical Tor Marketplace - Pharmaceuticals

The screenshot shows the Abraxas Tor marketplace interface. The browser address bar displays `abraxasdegupusel.onion/?q=xanax`. A banner at the top reads "Abraxas is slow for you? Use mirror 1 .". The navigation menu includes "Listings", "Profile", "Messages", "Orders", "Forums", and "Support". The user "JenniferJones72" is logged in, with a "Logout" button and a "Wallet" link. The wallet balance shows 0.00000000 BTC and 0.00000000 DASH. The "Listings" section on the left shows categories: Digital Goods (2807), Drugs (5473), Drugs Paraphernalia (307), Services (163), and Other (335). Below this is a "BTC Exchange" table and a "DASH Exchange" table. The main listing area shows a table of products for sale, including "100 Bars x 2 MG", "FIVE HUNDRED (500) of our elite 2mg replica bars", "Alprazolam-XR (Alprazolam) 50x2mg", "1mg (clonazepam) x 8 -> TOMORROW", and "40x 1mg Upjohn football UK". Each listing includes a product image, name, price, shipping information, and vendor details.

Name	Price	Shipping	Vendor
100 Bars x 2 MG (alprazolam) is used to treat anxiety disorders, panic disorders, and anxiety caused by depres...	0.55818126	From: Unknown To: Worldwide	Meds2Buy 5/5, 20~50
500 Bars 2mg Replicas (500 bars) FIVE HUNDRED (500) of our elite 2mg replica bars that are now the buzz of the USA2USA Domestic...	2.28346880	From: United States To: United States Only	FE Only FreeTrade 5/5, 100~200
Alprazolam-XR (Alprazolam) 50x2mg Alprazolam-XR brand, Extended release High-quality product made by Alprazolam is on...	0.45669376	From: EU To: Worldwide	Klaymen, 0
1mg (clonazepam) x 8 -> TOMORROW This vendor only sells meds that are produced for dispensing in US pharmacies as those manufacturers...	0.38903543	From: United States To: USA	FE Only CapHayata, 0
40x 1mg Upjohn football UK belongs to a class of drugs called benzodiazepines, which are central nervous system depressan...	0.45977221	From: United Kingdom To: Worldwide	FE Only Yaoming-UK 5/5, 70~100

Typical Tor Marketplace - Counterfeits

The screenshot shows a web browser window with the address bar displaying `abraxasdegupusel.onion/c/k77coQgrqU`. The page header includes navigation links: Listings, Profile, Messages, Orders, Forums, Support. A user profile for JenniferJones72 is visible in the top right corner, showing a Wallet and Escrow section with balances for BTC (0.00000000) and DASH (0.00000000). A message "Abraxas is slow for you? Use mirror 1 ." is displayed. The main content area is titled "Counterfeits / Other / Listings". It features a search bar, filters (No FE first, I can buy, Active vendor), sort options (Default), and a "Show domestic first" checkbox. The listings are displayed in a grid format, showing various counterfeit items with their respective prices and IDs. The items include:

- 50 euro counterfeits x 6 notes - 30 (0.13240213 B)
- wallet Replica-1124 (0.28815523 B)
- Wallet Replica (0.33222603 B)
- Yeezy II Shoes Replica gray (0.52545953 B)
- Yeezy II Shoes Replica black (0.52545953 B)
- Yeezy II Shoes Replica black (0.52545953 B)
- Air Yeezy II Red October Vers (0.52545953 B)
- Zipper Wallet M60017 Replica (0.32205584 B)
- Wallet N60825 Replica (0.28815523 B)
- Wallet N60824 Replica (0.29832541 B)
- key bag 0100 (0.23730430 B)
- Classical monogram Travel Bag (0.79666445 B)

On the left side, there are sections for "BTC Exchange" and "DASH Exchange" with various currency conversion rates. The BTC Exchange section shows rates for USD, EUR, GBP, and JPY. The DASH Exchange section shows rates for USD, EUR, GBP, and JPY.

Typical Tor Marketplace – Account Info

mobile St... OnionDir... TORCH searc... http...ion/ Bitcoin - ... Fraud ... Stop The Sca... D. Disconne... M MIDDLE E... Items by ...

abraxasdegupusel.onion/c/654m5BuyBK?q=bank+account

Abraxas is slow for you? Use mirror 1 .






Listings Profile Messages Orders Forums Support

JenniferJones72 Logout
Wallet Escrow
BTC 0.00000000 0.00000000
DASH 0.00000000 0.00000000

Fraud Related / Digital Goods / Listings

bank account Go

☐ No FE first ☐ I can buy ☐ Active vendor Sort: Default Show domestic first ☐ Unknown Go

Name	Price	Shipping	Vendor
 Full Account & Routing numbers	0.03338915 B	From:Unknown	safetybets 0
 Bonus Cashout Tutorials	0.01669457 B	From:Unknown	safetybets 0
 NOTE - With this source, you can cashout your funds to the following. (1) Bank Account (2)...	0.06677830 B	From:Unknown	etimbuk 5/5 200-500
 NOTE - With this source, you can cashout your funds to the following. (1) Bank Account (2)...	0.06677830 B	From:Unknown	etimbuk 5/5 200-500
 It's often considered the definitive guide for eCommerce fraud. TOPICS INCLUDE (but not limited...	0.20000000 B	From:Unknown	fake 5/5 200-500
<p>MarkMonitor® PART OF THOMSON REUTERS</p>			



So What Role Does Bitcoin Play?

- Sites utilize Bitcoin to conduct transactions
- Other types of cryptocurrency are sometimes accepted
 - Dash (formerly known as Darkcoin)

How Does Bitcoin Work?

- Anonymous payment system
 - Utilizes peer-to-peer technology to operate with no central authority
 - Relies upon “Miners” rewarded with Bitcoin to conduct network transactions
 - Transactions are conducted electronically using URIs which can be imbedded in QR codes for use with mobile devices
- Bitcoin can be bought and sold through online exchanges
 - Currently 13 million Bitcoin in circulation
 - Current value of a Bitcoin is ~\$295 US
 - By 2140, there will be no more than 21 million Bitcoin



Features of Bitcoin

- Decentralized
 - The Bitcoin network is not controlled by any one central authority - every machine that mines Bitcoin and processes transactions makes up a part of the network, and the machines work together
- Anonymous
 - Bitcoin addresses are not linked to names, addresses, or other personally identifying information
- Fast
 - Money can be sent anywhere and arrives within minutes, as soon as the Bitcoin network processes the payment
- Non-Reversible
 - When Bitcoins are sent, there's no getting them back, unless the recipient returns them to you – they are gone forever

Identifying Abuse in Deep Web





Mitigating Abuse in Deep Web

- Enforcement options
 - C&Ds to website operators
 - Take-down requests to ISPs
 - Notices to marketplaces, social media sites, mobile app stores



Identifying Abuse in the Darknet

- Understand your level of risk
 - FIs must be monitoring for account information
 - Those with counterfeiting issues should determine if these marketplaces provide means of mass distribution
 - All others should:
 - Determine whether you need regular monitoring OR
 - Periodic monitoring for changes to the threat landscape
- Track abuse over time
 - Evolving area of the Internet



Mitigating Abuse in the Darknet

- Due to anonymity, online enforcement difficult
 - May be information if seller profiles are available
 - E-mail addresses may be used to uncover additional information
 - May consider test-buys to understand what is being sold
 - Truly counterfeit, grey market, stolen
- For stolen account or credential information
 - Work with internal fraud teams to determine next steps



Thank You!

- For information on MarkMonitor solutions, services and complimentary educational events
 - Contact us via email:
field.marketing@markmonitor.com
 - Visit our website at:
www.markmonitor.com
 - Contact us via phone:
US: 1 (800) 745 9229
Europe: +44 (0) 203 206 2220