

# The Dark Web & Insurance

*Anthony Mormino, SVP Legal, May 2019  
Casualty Actuarial Society  
2019 Spring Meeting in New Orleans*

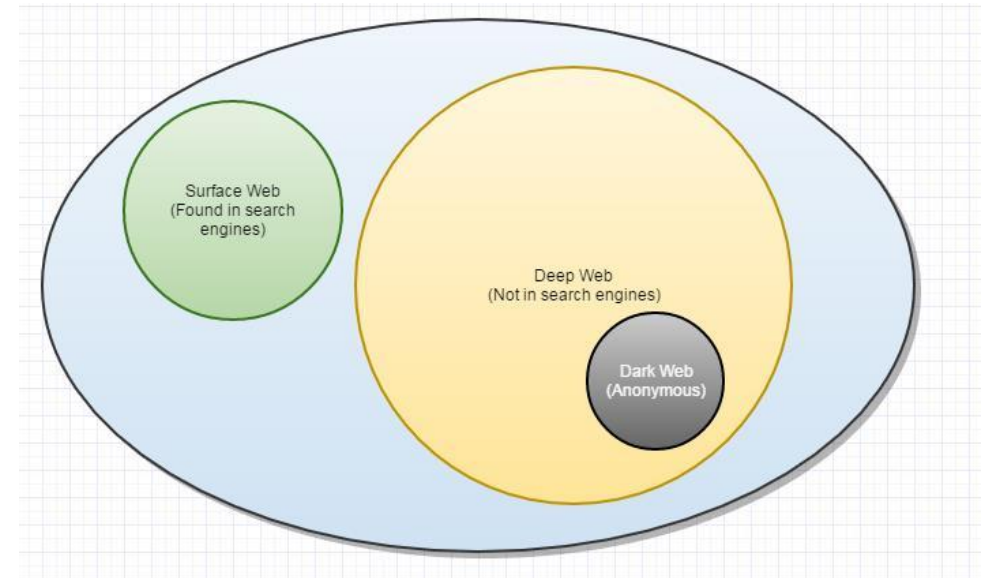
## Dark Web & Insurance - Abstract



- In the past five years, the **Dark Web** is a feature of almost any discussion about the Internet, cyber-attacks, and hackers whose criminal activities **cause insured losses**.
- Insurance companies to **have a grasp** on how the Dark Web may play a known or unknown role in cyber-attacks that result **in insured losses**.
- Yet understanding Dark Web can be a challenging proposition due to the very **"black box" nature of the Dark Web and the relative secrecy and strict security** with which it operates.
- *The purpose of this presentation is to demystify the Dark Web for insurance industry participants, and help them get a better sense how the Dark Web operates, and its relevance to insurance.*

## Table of Contents / Agenda

1. Why should insurance companies care about the Dark Web?
2. What is the Dark Web?
3. How does the Dark Web work?
4. Bitcoin and Altcoins
5. Common uses for the Dark Web
6. Dark Web topics that affect insurance
7. Conclusion – The Future of the Dark Web



# Why should insurance companies care about the Dark Web?



## Why care?

- Small part of the internet, yet **vehicle of largest insured data hacks**
- Dark Web has **grow exponentially** in short time, increasing **insured risk**
- Increased insurance **opportunities**
- Insurers and their **own data** a big risk, starts on Dark Web
- Can put a company out of business or **severely harm it**
  - Sony Pictures shut down over its parody of N. Korean leader
    - The movie called “The Interview”
  - Non-Petya Virus
- **Wild West of the Internet**



# What is the Dark Web?

## What is it?

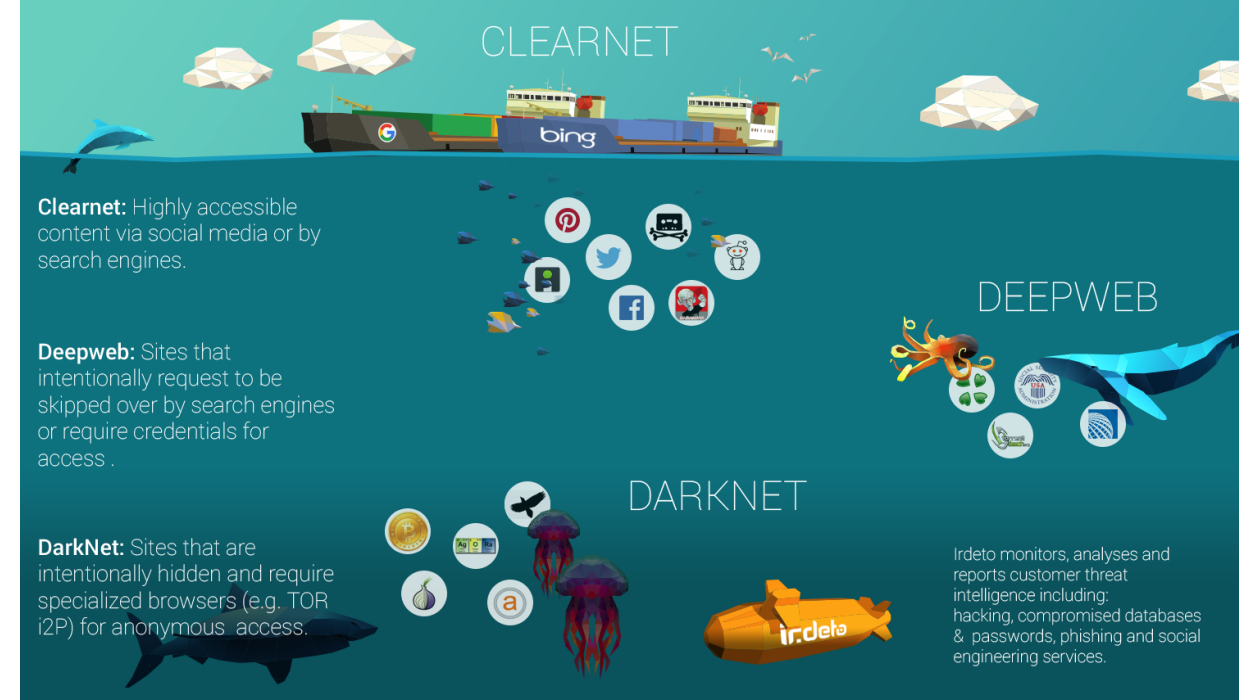
- The internet = Clearnet + Deepweb + Darkweb



# What is it?

- **The Clearnet**

- Commonly known as the “Internet”.
- 10% of the "internet"
- Organized top level domains -- .com, .net, .org
- Any browser can find pages
- A.K.A. - The WWW, the "internet" we all know and love
- Common web sites, easy to access, any browser - Amazon.com, CNN.com, Casct.org, Swiss Re.com
- "Surface links" indexed daily for millions of websites - Google, Yahoo, DuckDuckGo
  - "Surface links" - Pages updated regularly
  - Newspapers, blogs, online stores, government
  - Surface links and accompanying info "archived"
  - No longer found in search engines, replaced by newer index data
  - Surface links "go away"





## What is it?



- **The Deep Web**

- 90% of the "internet"
- The place where all the surface links go
- Washington Post, US government = giant archives of older material
- Too much data for Google to index!
- *Visit specific pages to search and find*

What is it?

- The Dark Web

- < 1% of the "internet"
- Subset of the Deep Web
- Not indexed by Google etc.
- No clear visibility



# How does the Dark Web work?

## How does it work?

- Whose big idea was the Dark Web anyway?
  - DarpaNet 1970's, military
  - 1980's rise of the personal computer, data stored on unconnected computers
    - Users want to share all the "good" stuff from "data havens"
    - BBS, Usenet
    - modem connections (phone "cradles"), 1200 "baud"
  - Mid-1990's US Naval Research Laboratory creates the TOR Browser
    - Protect U.S. intelligence communications online
    - Disseminated eventually outside government
      - Dissidents

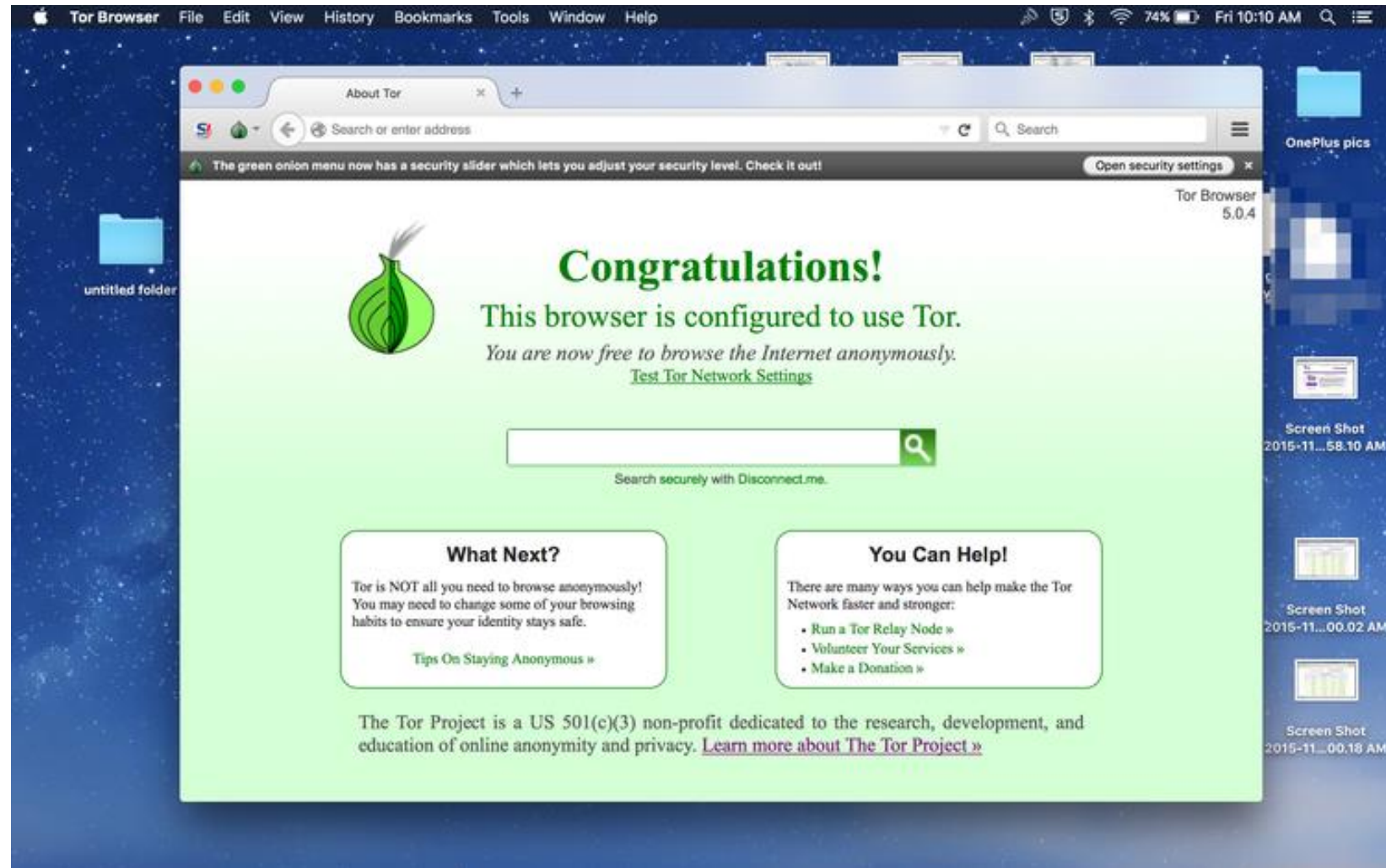
## DarpaNet + USNRL ==> File sharers + businesses become curious

- Late 1990's Dot Com Boom
  - WWW for formerly brick and mortar sales, legitimate
- Napster arrives, legitimacy unclear
  - Spawned series of peer-to-peer networks like Gnutella, Freenet, Kazaa, Limewire
  - Decentralized data hubs
  - Bit Torrents grow
  - Trade and distribution of copyrighted music and movie files
- Prosecutions and law suits drive Torrent traffic to the Onion Network
- The Dark Web's bad rep established!



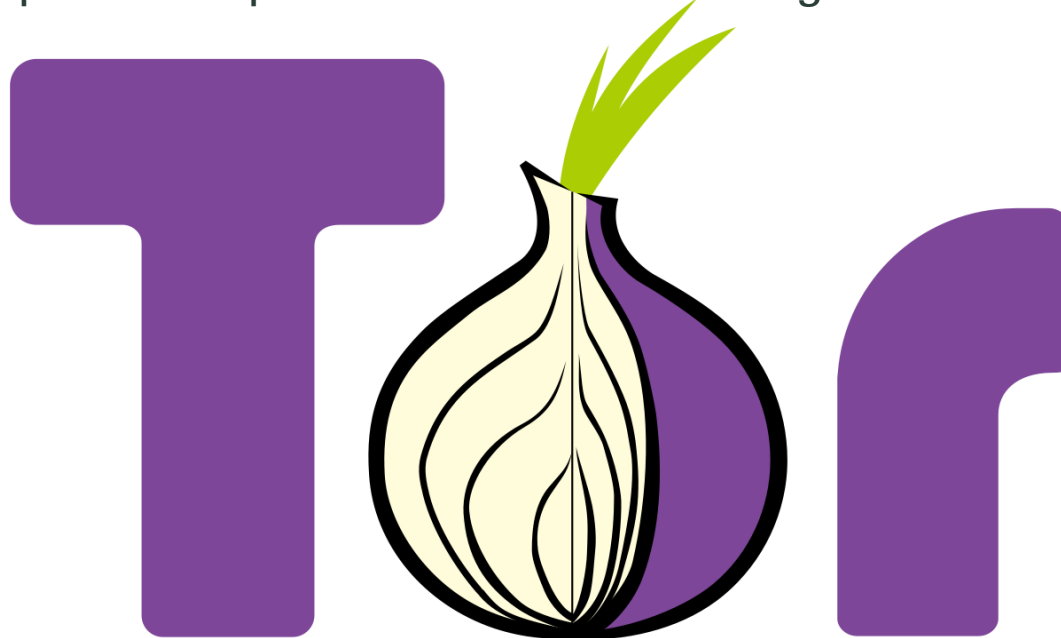
## How does it work?

- The Dark Web
  - "Dark" because few or
    - no links between pages
    - and sites
  - No indexes like Google
  - Need to know the exact address
  - Rely on "lists" compiled
    - periodically by other users
  - Most lists out of date
  - Hosted on private servers
  - One top level domain -- .onion
  - Linked by "the onion network"
  - "The Onion Router" = TOR Browser
  - TOR Browser = the main protocol for .onion domains

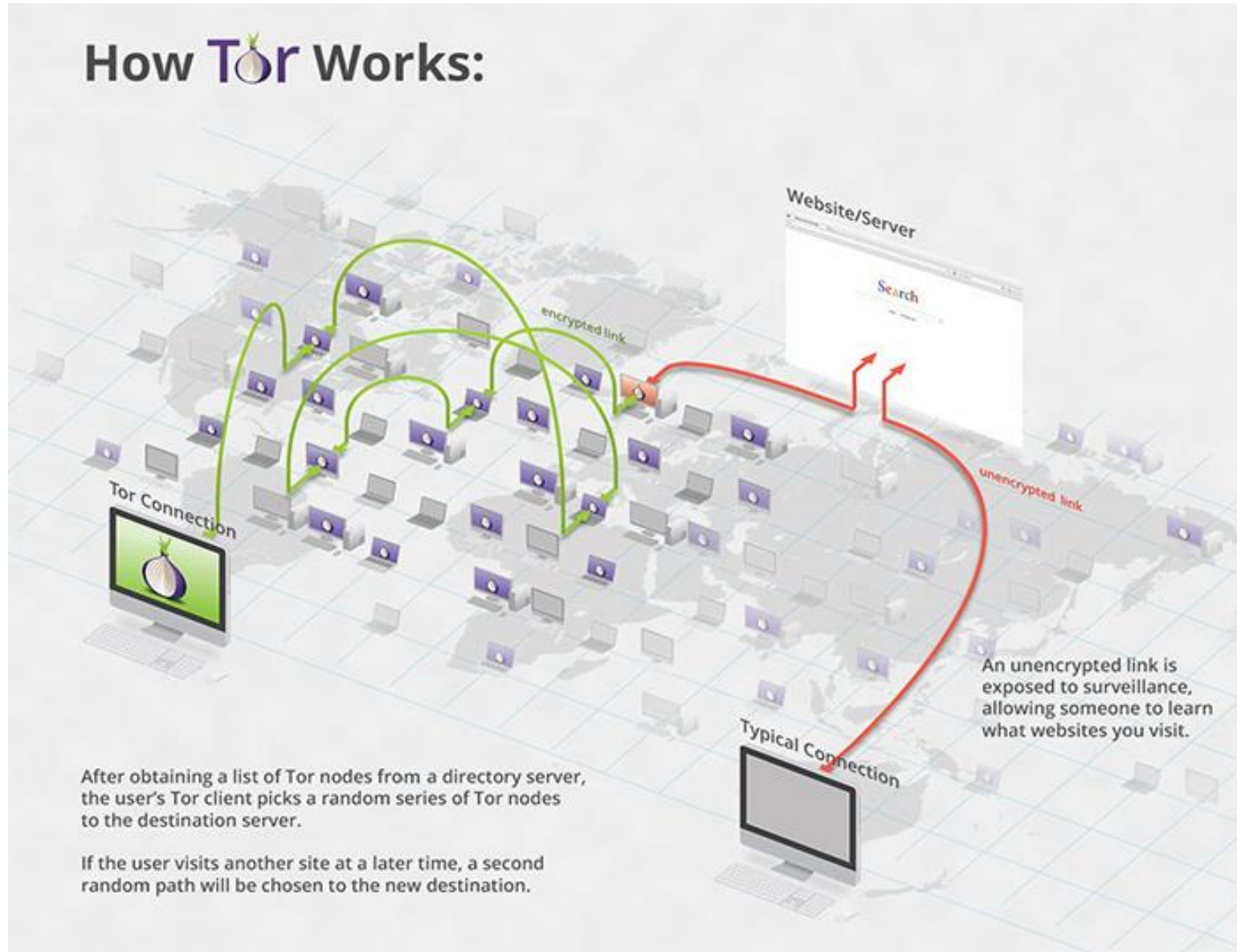


## Technically speaking, how does it work?

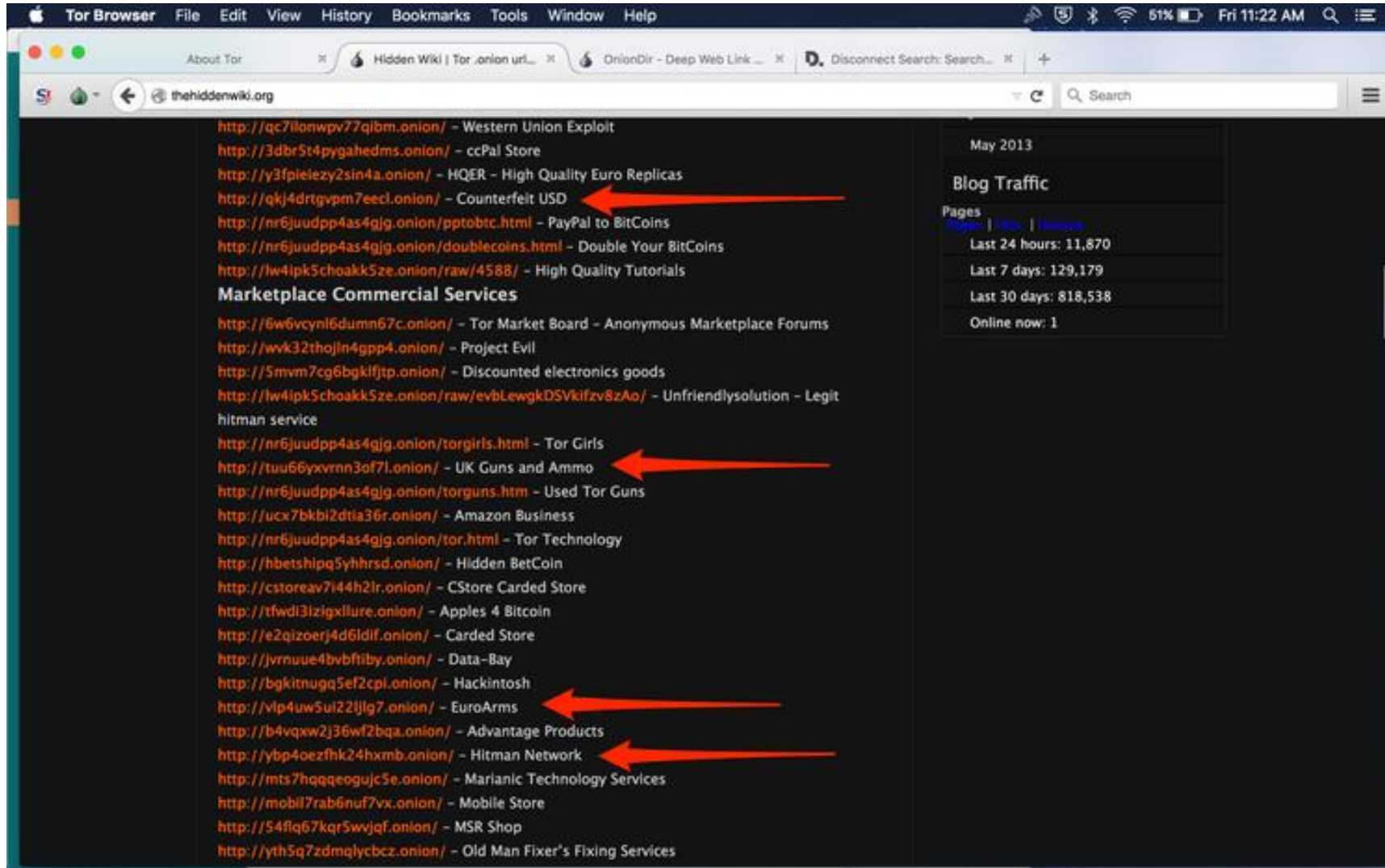
- Technically Speaking
- Key to TOR = "onion routing" = Encrypt web traffic in succeeding "layers" (of the "onion")
  - Initial data sender uses TOR Browser to encrypt and send data to second TOR
  - Randomly chooses computers to send the traffic = "hops" or "bounces"
  - Each computer encrypts the data before passing the data on to the next one
- None of the "hops" or computers can match data origin or destination = anonymity of the sender
  - Data encrypted



# TOR – “The Onion Router,” based on Firefox, free



# DW Links

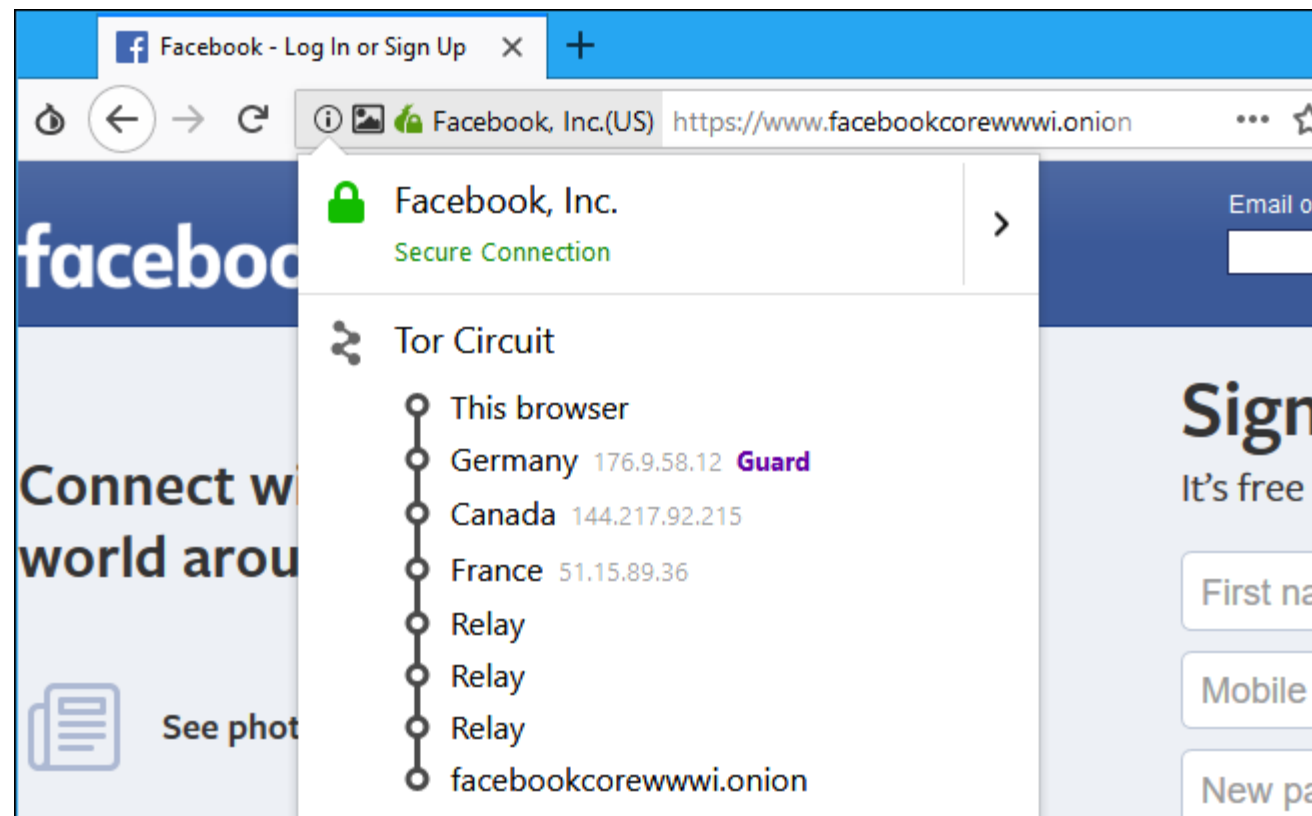


# Common uses for the Dark Web



## Good uses for DW anonymity

- Dark Web Anonymity = Good
  - Pro-privacy or anti-establishment groups
  - Citizens of totalitarian societies can communicate with the outside world
  - Access uncensored news stories around the world
  - Connect to sites blocked by their local ISPs or governments
  - Human rights groups and journalists sharing information that could otherwise be tracked
  - Political dissidents publish views without discovery
  - Socially, politically, personally sensitive communications, chat rooms, web forums



# More good uses for DW anonymity

- Facilitated the Arab Spring uprising in 2010, avoided govt detection and arrest
- Whistleblowers, uncover corruption or wrongdoing
  - Fear for freedom or lives
  - Download info into service like "Dead Man Zero," "dead-man switches"
  - Release information if don't log in to service periodically
- Spawned cryptocurrencies like Bitcoin and other block chain currencies



## Bad uses for DW anonymity

- Dark Web Anonymity = Bad
  - Silk Road - The most well-known online marketplace and drug bazaar on the dark web
  - Illegal drugs, mostly
  - Pharmaceuticals
  - Illegal adult material
  - Credit cards
  - Identity theft, SSNs, medical info
  - Copyrighted materials.
  - Hacking software
  - Hackers for hire (steal competitors' secrets, attack or disable competitors or rivals)
  - Anything else you can imagine that you might not say out loud!

LISTING OPTIONS

- Contact Seller
- Favorite Listing
- Favorite Seller
- Alert when restock
- Report Listing

BROWSE CATEGORIES

- Fraud 10542
- Drugs & Chemicals 36773
- Guides & Tutorials 4708



lacoste shirts - fake

These are copies but good quality. comes in s, m, l, xl and many colors, let me know when you order

Sold by MrAsia - 0 sold since Mar 30, 2015 Vendor Level 1 Trust Level 4

	Features	Origin country	Features
Product class	Physical package	Thailand	Worldwide
Quantity left	Unlimited	Ships to	Escrow
Ends in	Never	Payment	

free tracked air 7-14 days - 14 days - USD +0.00 / item

Purchase price: USD 35.00

Qty: 1 Buy Now



Shop by Category

- Apparel 341
  - Clothing 175
  - Handbags 20
  - Sunglasses 56
  - Watches 69
- Art 3
- Biotic materials 2
- Books 911
- Collectibles 14
- Computer equipment 74
- Custom Orders 90
- Digital goods 651
- Drug paraphernalia 330
- Drugs 11,191
- Electronics 102
- Erotica 626
- Fireworks 15
- Food 9
- Forgeries 158
- Hardware 27
- Herbs & Supplements 11
- Home & Garden 11
- Jewelry 90
- Lab Supplies 51

messages 0 orders 0 account B0.00

Search

a few words from  
ad Pirate Roberts

Hi, lopoling  
logout



sort by: bestselling

Domestic only

update



Hublot - Classic Fusion Automatic Watch [Rep

seller: ReplicaAAA(100)  
ships from: China

B1.31  
add to cart



Rolex GMT Master II -Red and Black Replica

seller: AsianVixen(100)  
ships from: China

B1.85  
add to cart



Burberry Warm Down jacket Replica

seller: FoxyGirl(100)  
ships from: China

B1.08  
add to cart

# Bad uses, let's go shopping on the DW!

- For example
  - Medical records - \$1 to \$60
    - = Names, DOB, SSN, medical info
    - = Create fake identities (17M in 2017)
    - = Open credit cards, obtain loans
    - = Bill fraudulent medical procedures to insurers
  - Bank account info - \$200-\$500
  - Credit card info - \$4-\$8 (volume discounts)
  - eBay + PayPal accounts - \$10-\$300 (+/- activity)
  - PII like Name, address, date of birth, email, and phone number, salary,
    - vehicle registration plate, SSN - \$1-\$4
  - Copy of electric bill or passport - \$40
  - Credit report - \$25



Number	Type	Name	Country	City	Phone	Mail	DOB	Price	Select
372845	AMEX	Charles S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
528713	MasterCard	Christopher S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
845450	DISCOVER	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
371527	AMEX	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
846880	DISCOVER	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
651920	DISCOVER	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
845857	DISCOVER	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
371198	AMEX	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
534248	MasterCard	Eric S.	US	...	Y	Y	Y	40\$	<input type="checkbox"/>
371726	AMEX	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
537161	MasterCard	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
447639	VISA	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
371730	AMEX	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
528730	MasterCard	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>
853659	DISCOVER	Eric S.	US	...	Y	N	Y	40\$	<input type="checkbox"/>



# Bitcoin and Altcoins

## What is Bitcoin?

- Combination of
- Everything you don't know about finance
- with
- Everything you don't know about technology



## Altcoins

- Different names, same thing
  - cryptocurrencies,
  - altcoins,
  - virtual currencies,
  - electronic coins,
  - digital coins,
  - digital tokens,
  - blockchain tokens

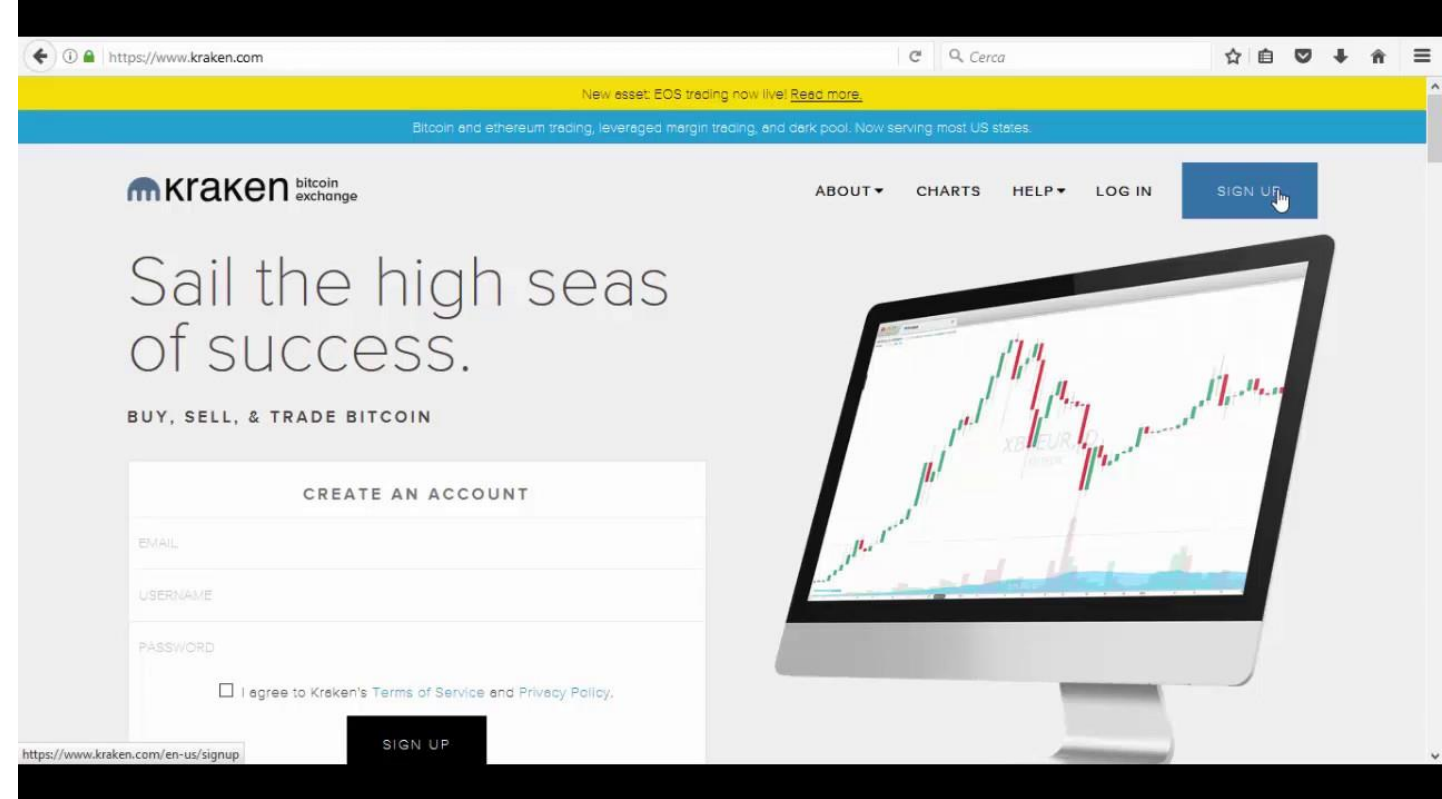
- The aggregated cryptocurrency market capitalization?
  - 2017 to 2018 – USD\$18 billion to USD\$135 billion
  - 650% increase.

# Altcurrency

- What is it?
  - #1 = Bitcoin "currency" created in 2009
  - Medium of exchange
  - Cryptography for creation and management instead of central authority, e.g., no US Treasury printing USD
  - Transactions are made with no middle men – meaning, no banks
  - Anonymity, conceal source + buyer & conceal receipt + seller
    - Less so today, law enforcement
- How do you get it?
  - Altcoin clearing houses, access the block chain or accounting system for that currency
  - Buy altcoin using USD, deposit it to your digital “wallet,” clearing house records your ownership in blockchain
- Who created it?
  - Unknown person or group using the alias **Satoshi Nakamoto**
  - Integrated ideas cypherpunk community
  - A cypherpunk is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change.
  - Originally for free speech only, no good/bad purposes

# Altcurrency

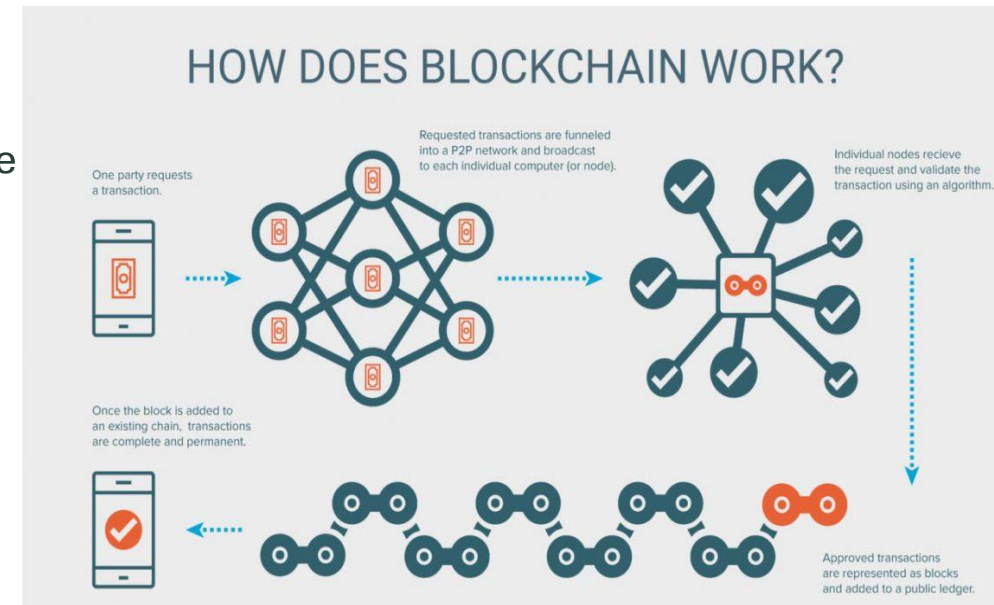
- What can you buy?
  - Legit
    - Bitcoin to book hotels on Expedia,
    - Shop for furniture on Overstock
    - Xbox games
    - Tesla
    - Argentina – currency controls, no credit cards, BTC for Uber
    - Bank settlements
  - Illegit
    - Anything bought or sold anonymously
    - Drugs, guns, etc
    - Bribes untraceable





























# Altcurrency

- Technically speaking
  - **Cryptocurrency** = chain of digital signatures stored on a decentralized public ledger = blockchain
  - Private key unique to an owner, show ownership, digital wallet holds your key (for an in-depth explanation, refer to the original **Bitcoin whitepaper** by Satoshi Nakamoto)
  - Cryptocurrencies are **transferred from one owner to another** by adding a transaction to the blockchain
  - **Validators** – Keep blockchains secure from hacking by validating transactions (miners)
  - Incentive to validate = get new coins and/or "sender fees"
  - "**Consensus mechanisms**" to validating transactions
    - Proof-of-Work (PoW) – Mining, create new coins, get new coins = fee
      - Validate transactions by running algorithm
      - to solve a cryptographic puzzle
    - Proof-of-Stake (PoS) – Validate only, earn a fee
      - Validate transactions by staking or depositing cryptocurrency



#	COIN	PRICE	24H	MKT CAP	LIQUIDITY	DEVELOPER	COMMUNITY	TOTAL	LAST 7 DAYS
1	 <b>Bitcoin</b> BTC	\$7,527.85	-0.5%	\$129,135,486,078	\$6,425,404,358	98%	88%	91%	
2	 <b>Ethereum</b> ETH	\$409.93	-2.9%	\$41,368,150,093	\$2,425,329,957	95%	71%	85%	
3	 <b>EOS</b> EOS	\$7.00	-4.2%	\$6,326,721,806	\$794,471,897	93%	63%	78%	
4	 <b>XRP</b> XRP	\$0.432936	-3.3%	\$17,013,819,407	\$235,293,513	82%	68%	74%	
5	 <b>Litecoin</b> LTC	\$75.74	-2.6%	\$4,360,424,392	\$275,053,191	74%	65%	73%	
6	 <b>Tron</b> TRX	\$0.03115607	-6.9%	\$2,044,470,884	\$147,158,980	86%	59%	72%	
7	 <b>Monero</b> XMR	\$123.54	-1.8%	\$2,011,143,069	\$25,998,286	90%	62%	71%	
8	 <b>Cardano</b> ADA	\$0.131946	-6.9%	\$4,105,152,410	\$73,895,535	87%	56%	71%	
9	 <b>Dash</b> DASH	\$208.55	-5.7%	\$1,714,238,449	\$206,196,165	81%	55%	70%	
10	 <b>Stellar</b> XLM	\$0.265020	-5.6%	\$4,964,181,760	\$56,029,353	79%	60%	69%	
11	 <b>Zcash</b> ZEC	\$188.49	-6.4%	\$845,889,136	\$147,334,956	88%	49%	69%	
12	 <b>Ethereum Classic</b>	\$15.04	-6.4%	\$1,554,800,523	\$210,753,850	79%	51%	68%	

# Dark Web topics that affect insurance

# Dark Web & Insurance

- Cyber Insurance - Increased awareness of dark web increased interest in buying cyber insurance
- Dark web monitoring services
  - If your name is out there someone may be preparing you to be hacked
- Increased interest by hackers in hacking larger insurers and their troves of customer data
- Health data of customers particularly valuable
  - Identity theft
  - Buy highly valuable prescription drugs and re-sell them
- The opioid epidemic - Buy OxyContin on the internet, re-sell, OD, increased insured losses (Chinese factories sell ingredients by the ton)
- Detect the next big cyber-attack, stop it before it happens
- Learn how the Black Hats work, fight fire with fire
- Buy back data bases from hackers before they sell it
  - Way cheaper than paying the resulting losses

# Conclusion – The Future of the Dark Web



## The future

- Democratization of the Dark Web
  - Technology makes it easier to use
  - More people surf the Dark Web, exponential growth
- Citizens seek out increased privacy
  - Back lash to Facebook and Google collecting and selling your data
  - Move their activities to the Dark Web
  - Better security = a "darker" Dark Web
  - Daily Stormer, for example
- Decentralization of marketplaces
  - Peer to peer selling with cryptocurrencies
  - Harder to shut down

New Technologies

# The future = Mainly the privacy of the average citizen

- Blockchain assignment of addresses
  - No need for IP addresses
  - Less government control and management of top level domains
- Net neutrality less of an issue
  - Increased use of private TOR servers, peer to peer not ISPs
  - Zeronet
- Cryptocurrencies become far more commonplace
  - Already exploding in flavors
  - Fraud in ICOs abounds today
- Private and untraceable delivery services grow
- Living on-line anonymously comes into vogue
- Dark Web "justice system" created
  - Self-regulated like Yelp for the Clearnet
  - Do you know your Uber Rating?



The image shows a screenshot of the Tor Project website. At the top, the word "Tor" is written in a large, purple, stylized font, with a small onion icon integrated into the letter 'o'. To the right of the logo is a navigation menu with links: "Home" (highlighted in a light green box), "About Tor", "Documentation", "Press", and "Blog". Below the navigation is a large green banner with the text "Anonymity Online" in white. Underneath this, it says "Protect your privacy. Defend yourself against network surveillance and traffic analysis." There is a purple button with the text "Download Tor" and a small download icon. To the right of the button 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". A small onion icon is also visible in the bottom left corner of the banner.

# Questions?



# Legal notice

©2019 Swiss Re. All rights reserved. You are not permitted to create any modifications or derivative works of this presentation or to use it for commercial or other public purposes without the prior written permission of Swiss Re.

The information and opinions contained in the presentation are provided as at the date of the presentation and are subject to change without notice. Although the information used was taken from reliable sources, Swiss Re does not accept any responsibility for the accuracy or comprehensiveness of the details given. All liability for the accuracy and completeness thereof or for any damage or loss resulting from the use of the information contained in this presentation is expressly excluded. Under no circumstances shall Swiss Re or its Group companies be liable for any financial or consequential loss relating to this presentation.