

The background of the slide features a person wearing a dark hoodie, sitting at a desk and using a laptop. The person's face is obscured by a large, glowing blue question mark. The background is dark and filled with a pattern of binary code (0s and 1s) in a lighter blue color, creating a digital or cyber-themed atmosphere.

Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web

Presented by: Group 6

Sindhuja Banka

Yuva Sri Vemulapalli


Pranav Ganesh Soma

Naga Sekhar Reddy Kambham

Introduction

- Anonymity can not only provide a shield for the vulnerable but also a cover for malicious acting like a double-edged sword.
- There are two techniques to hide the anonymity which are:
 - Dark Web
 - Cryptocurrency
- This study aims to investigate how cybercriminals exploit cryptocurrencies for illicit activities in the Dark Web, while proposing solutions to mitigate cryptocurrency abuse and law enforcement challenges.

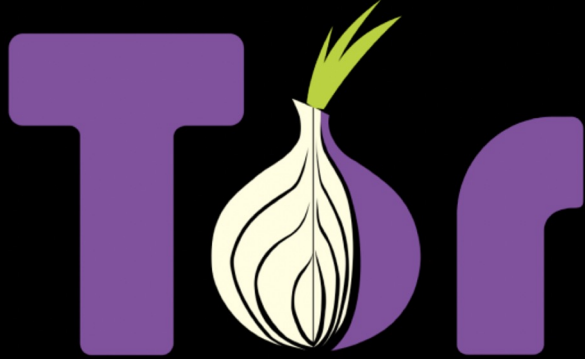




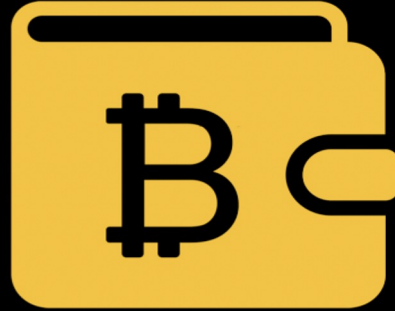
■ Problem Statement

- What are the different methods used by cybercriminals to abuse cryptocurrencies and the impact of these activities on the society?
- What are the strategies for mitigating the risks associated with cryptocurrency abuse and enhancing the effectiveness of law enforcement efforts in combating cybercrime in the Dark Web?
- What is the process of gathering cryptocurrency addresses in the Dark Web?

Anonymity Services



Dark Web



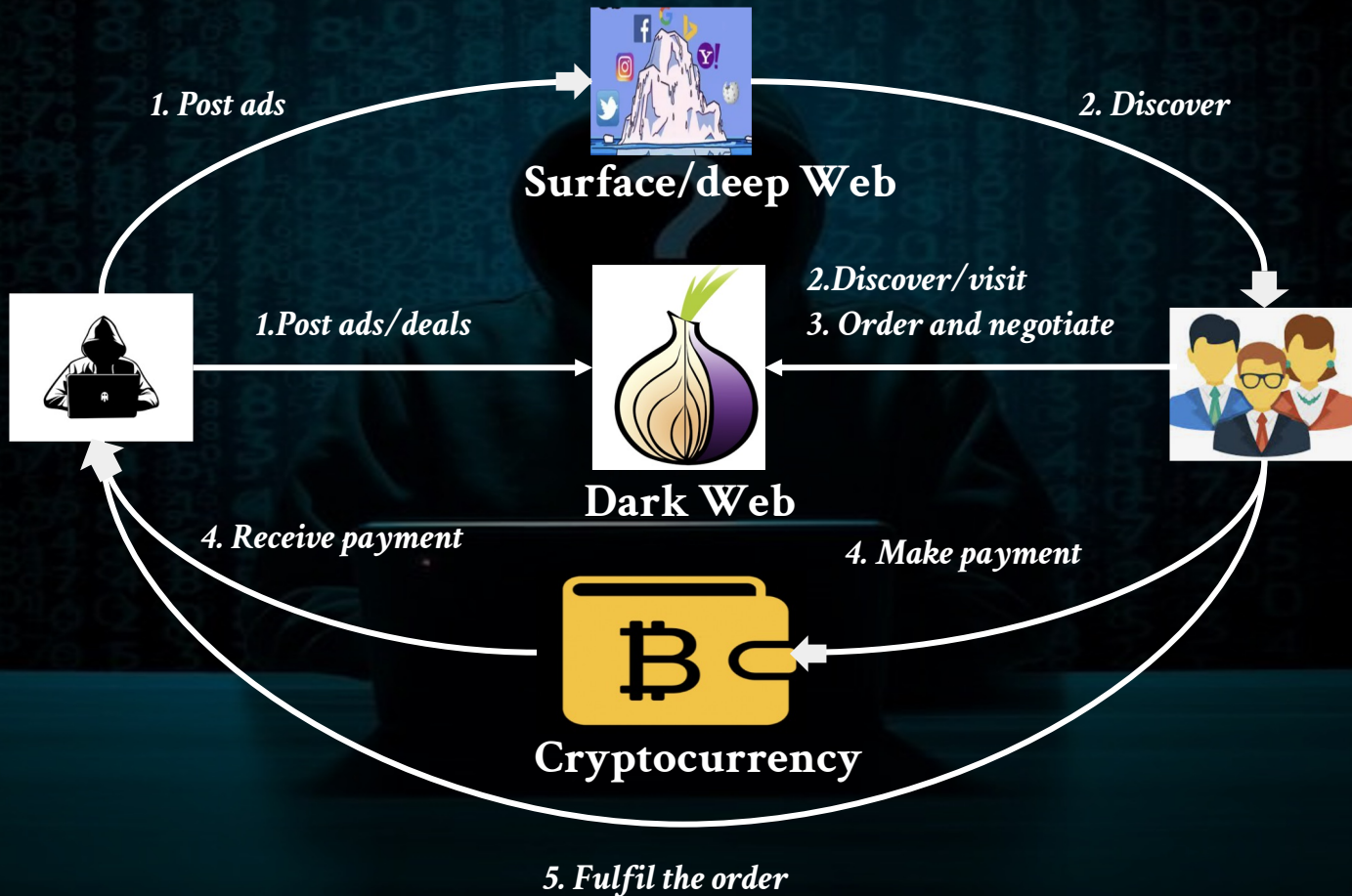
Cryptocurrency

Background

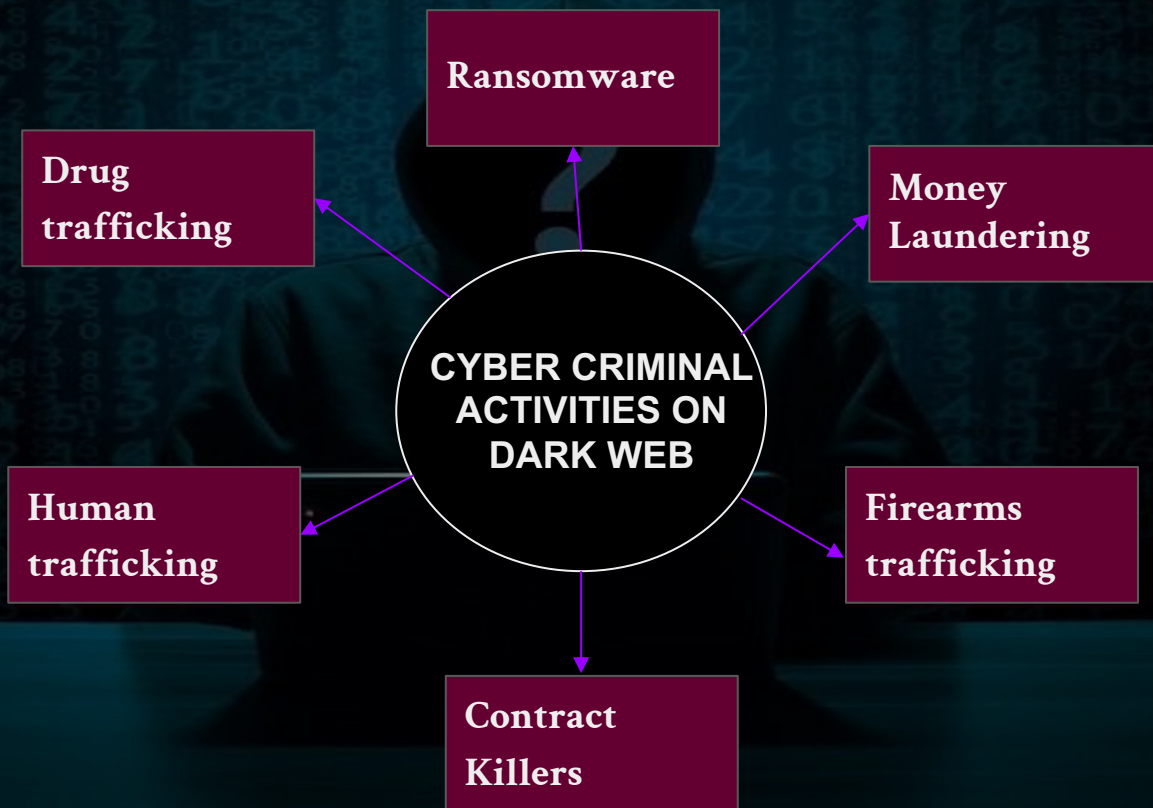
- Bitcoin is a decentralized digital cryptocurrency that relies on cryptography algorithms and a peer-to-peer network to manage a fully distributed ledger without a central authority.
- Unlike the traditional banking system, the absence of a central authority means that financial activities will remain pseudonymous.
- Bitcoin users generate multiple public addresses with corresponding verifiers of the ownership (i.e., private keys)



Dark Web Ecosystem



Background



Motivation and Challenges

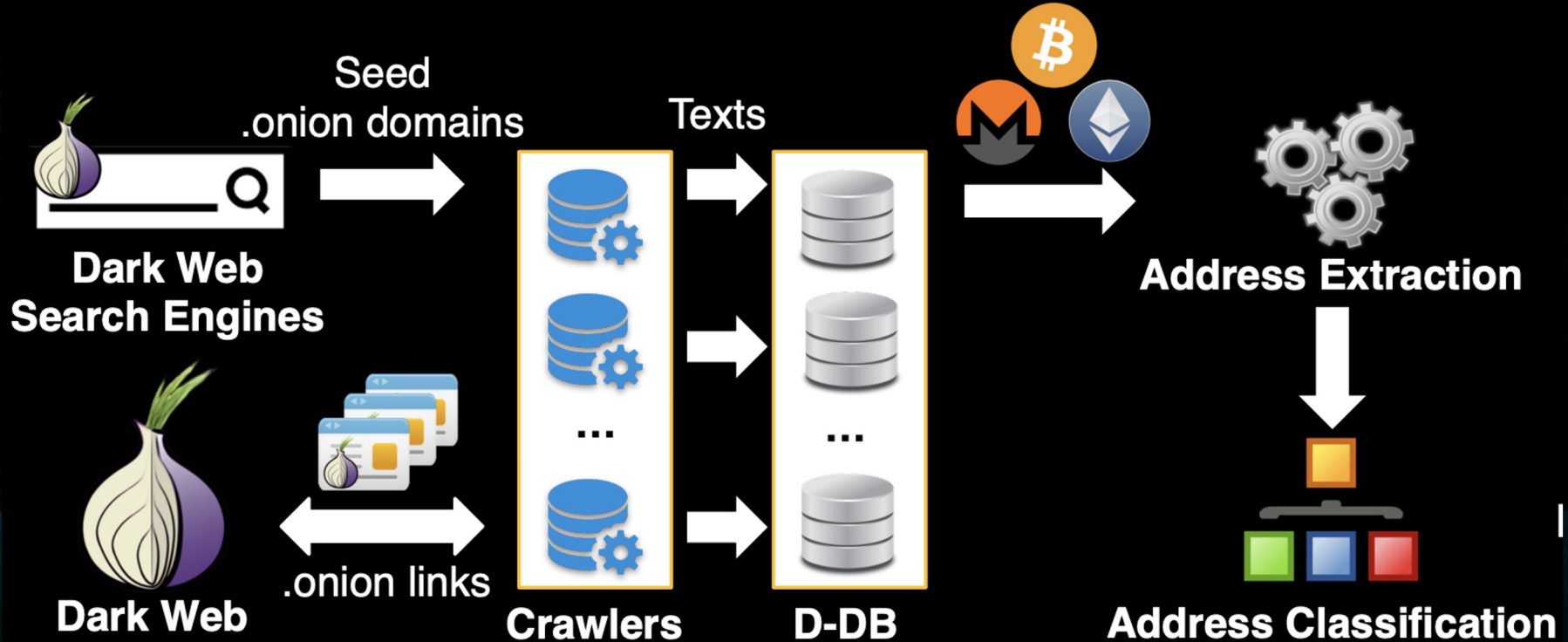
Motivation:

The limited coverage and outdated data of the Dark Web in previous studies motivated us to conduct an in-depth investigative study to understand how perpetrators abuse cryptocurrencies in the Dark Web

Challenges:

- I. Collecting large-scale data on the dark web is not possible due to the inherent nature of the dark web
- II. Cryptocurrency is designed for users who want pseudonymity, hence it is difficult to find the owner of an account
- III. Even after collecting data, further analysis needs to be done to understand the data that is collected

Data Collection: MFScope





Crawling the Dark Web

- First 10k onion addresses were obtained by Tor based search engines like Ahmia and Fresh Onions
- From the collected addresses, web crawling is done to traverse text contents on dark websites to get more links
- Total of 27M Onion websites are obtained using this technique

Address Extraction

- From the 27M Onion sites that were obtained earlier, Bitcoin, Ethereum and Monero addresses were extracted.
- Addresses were filtered out by using regex, to filter invalid addresses and addresses without any transactions.

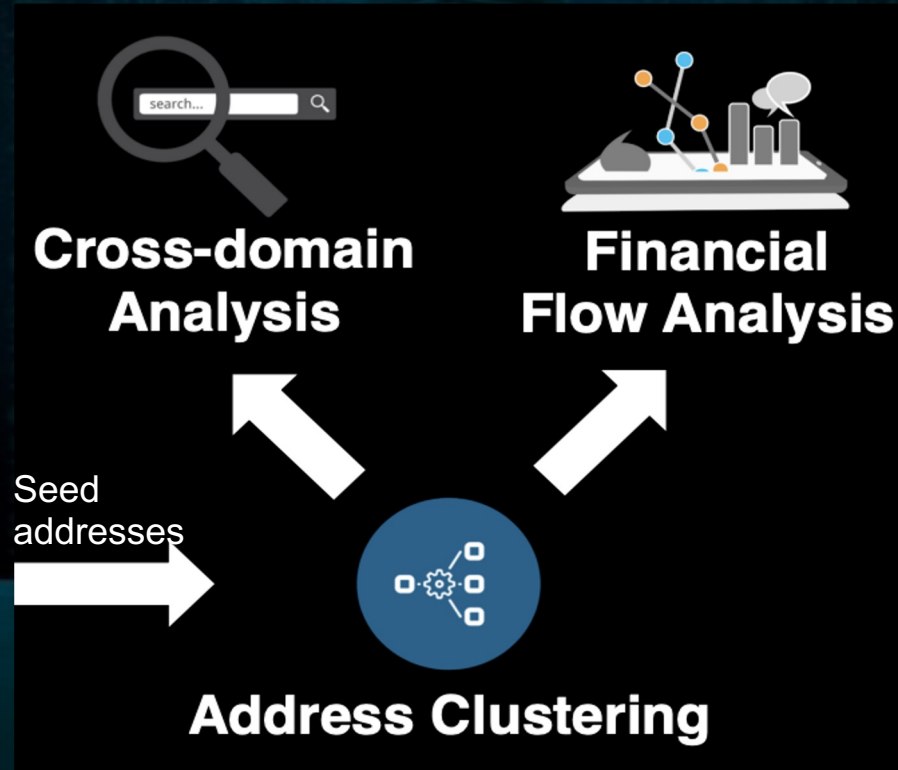
	BTC	ETH	XMR	Total
<i># domains</i>	2,886	180	121	3,187
<i># webpages</i>	1,579,047	4,743	4,410	1,588,200
<i># extracted addresses</i>	34,265,032	12,138	49,852	34,327,022
<i># distinct addresses</i>	9,906,129	649	38,440	9,945,218
<i># preprocessed addresses</i>	5,440	50	61	5,551

Address Classification

- Each of these 5440 Bitcoin addresses were manually checked by 10 Security researchers
- Addresses classified as Illicit, Possible Illicit and Legitimate.
- 85 Illicit addresses are our point of interest and will be referred as seed addresses

Category	Count	Ratio
Legitimate addresses	884	16.25%
Possible illicit addresses	4,471	83.75%
Illicit addresses	85	
Total	5,440	100.00%

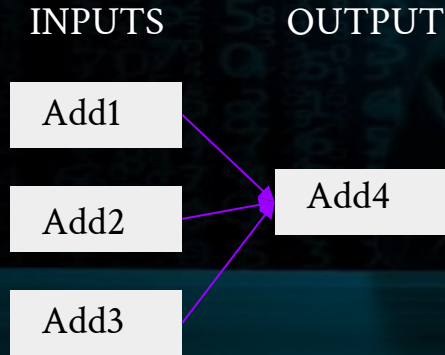
Data Analysis: MFScope



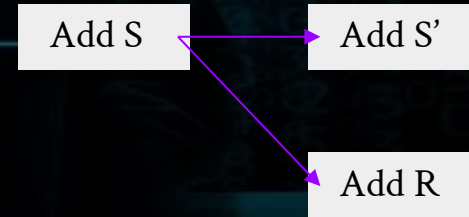
Clustering Illicit addresses

Ownership of multiple bitcoin addresses can be analyzed based on:

Multi Input Transactions



Change Addresses



Cross Domain Analysis

- *Cross-domain Analysis* module in MFScope conducts a Google search by using the illicit addresses from the Address Clustering module as keywords and publishes search results to a database
- Blockchain information sites that publish blockchain data are excluded since they are out of concern here

Category	Seed	MI	MI+CA	Total
Tor proxy	38	38	45	121
Community	35	59	20	114
Sales	17	27	9	53
Media	10	17	5	32
Archive	4	12	6	22
Miscellaneous	1	3	4	8
Unavailable	8	17	6	31
Total	113	173	95	381

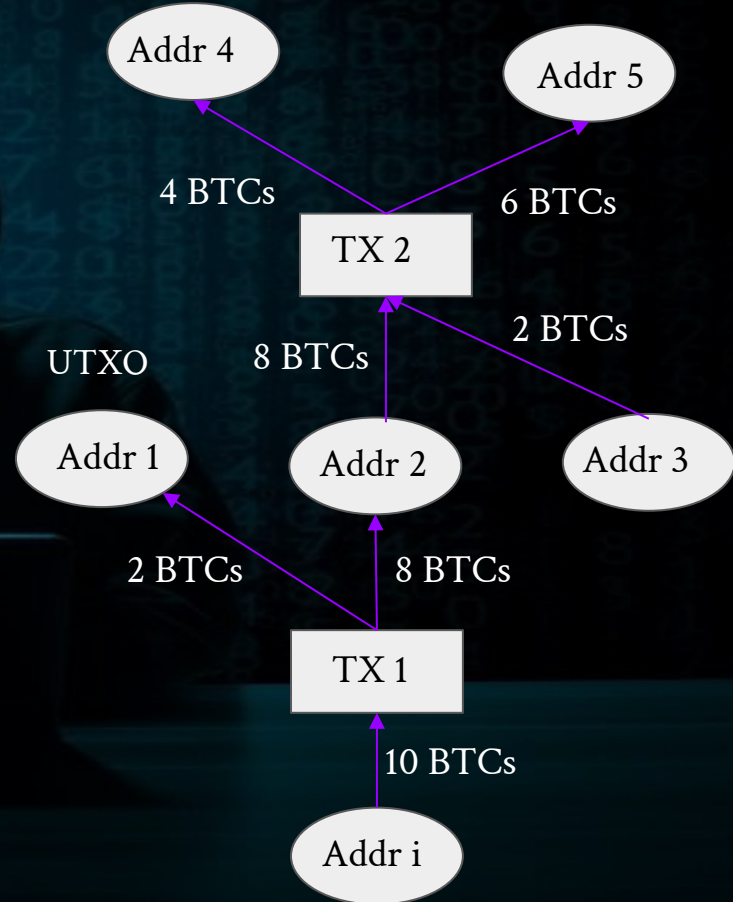
Financial Flow Analysis

- Taint Based bitcoin flow analysis is conducted
- Certain Stop conditions are specified

1. Unspent UTXO output
2. End with Known Cryptocurrency
3. Number of Transactions

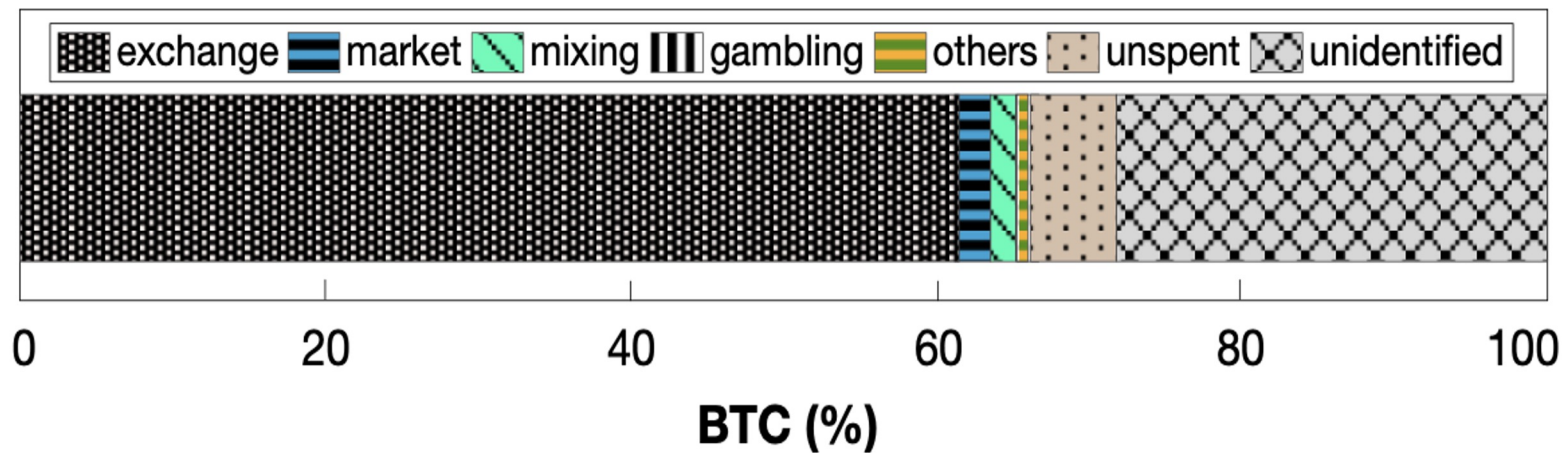
Service

Belongs to a blockchain
service



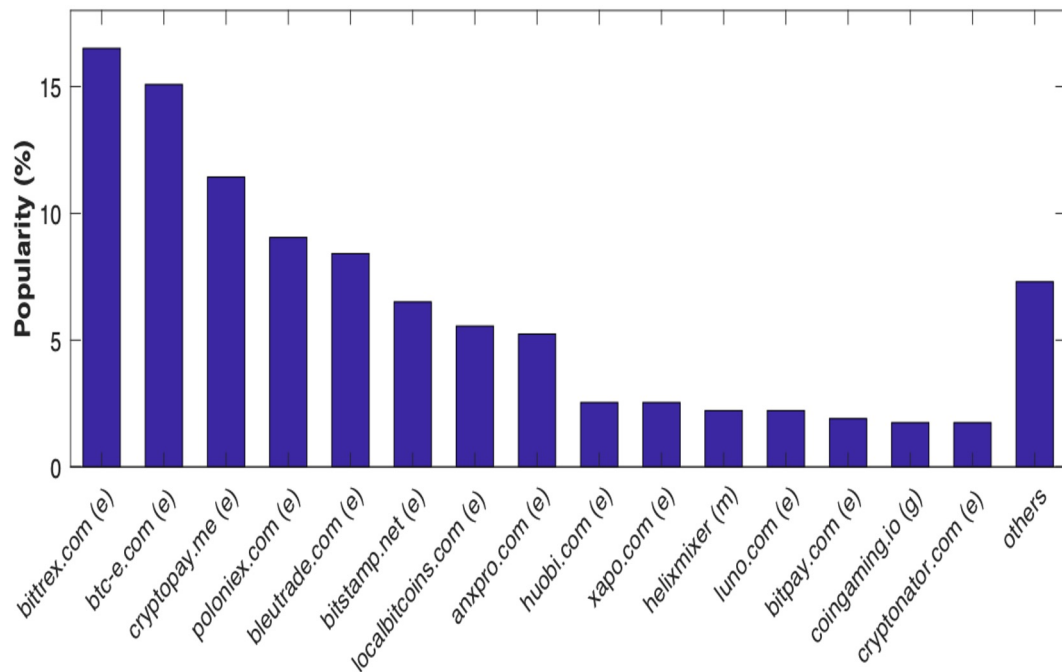
Tracing Cryptocurrency

Most of the illicit money (~61%) went into the exchanges, with the rest into market, coin mixing, gambling, coin mixing, gambling.



Tracing Cryptocurrency (cont..)

- Most of the cryptocurrency services that were used were not following KYC regulations
- Rest of the websites were either coin mixing websites or gambling websites



100

-
- The diagram illustrates the flow of money and information in a cybercrime ecosystem. It shows the interaction between Customers, Perpetrators, and various underground services.
- Legend:**
- Money flow
 - Information flow
- Key Elements:**
- Customers:** Represented by a group of blue icons. They interact with Site A (Arms trafficking) and Site B (Hacking as a service).
 - Perpetrator:** Represented by a black icon with a Bitcoin symbol. They manage a Bitcoin wallet (Cluster ID: 1Nkm*) and interact with Site C (Image for sale), Site D (User profile on an underground forum), and Site E (A hacking blog).
 - Bitcoin network:** A cloud icon representing the network. Transactions flow from the Perpetrator's wallet to the network and then to exchange services.
 - Exchange services:** Bittrex, BTC-e, Bitstamp, and LocalBitcoins.com. These services facilitate the conversion of Bitcoin into fiat currency.
 - Underground Services:**
 - Site A: Arms trafficking** (Tor network)
 - Site B: Hacking as a service** (Tor network)
 - Site C: Image for sale** (Tor network)
 - Site D: User profile on an underground forum** (Tor network). The profile includes posts about hacking tools and a link to a forum.
 - Site E: A hacking blog** (Tor network). The blog post mentions "my first ever blog".
 - Location info:** A globe icon representing the location of the services. Information flows from Site E to the location info.
- Transactions and Information Flow:**
- Money Flow (dashed green arrows):**
 - Customers to Site A (Arms trafficking)
 - Customers to Site B (Hacking as a service)
 - Perpetrator to Site C (Image for sale)
 - Perpetrator to Site D (User profile on an underground forum)
 - Perpetrator to Site E (A hacking blog)
 - Perpetrator to Bitcoin network
 - Bitcoin network to Exchange services
 - Information Flow (solid black arrows):**
 - Perpetrator to Site D (User profile on an underground forum)
 - Site D (User profile on an underground forum) to Site E (A hacking blog)
 - Site E (A hacking blog) to Location info

Limitations



- Difficult to analyze privacy focused cryptocurrencies like Monero as they use ring signatures.




- Difficult to find mixed/tumbled transactions on dark web because it is hard to find its origin and destination after mixing.

Future Work

- Rethink about the dark side of the anonymity services.
- Regulating limitations, internet governance and Increasing awareness of investors
- Numerous techniques exist for revealing the identities of users on the Bitcoin and Tor networks, which include Silk Road, Graph Analysis and Heuristic Approach exploring the possible dangers that come with de-anonymization

watch the little things;
a small leak will sink a great ship.
Benjamin Franklin





Thank You
Beware, Someone is always watching
you!

