DECENTRALIZATION: THE DEATHBED OF CYBER FORENSICS, WITH TOR AS A CASE STUDY

Aritra Chatterjee, B.A. LL.B., National Law University, Odisha

ABSTRACT

This paper explores how decentralization technologies, have impacted the field of cyber forensics, focusing on Tor as a case study. With the rise of digital technology, cybercrimes have become more sophisticated, making forensic tools crucial for investigating and prosecuting offenses. However, decentralized networks disrupt traditional methods of cyber forensics like evidence collection, authentication. Tor, a decentralized anonymity tool, enables users to hide their identities and access the dark web, creating significant obstacles for forensic experts. The paper examines these challenges, from the rise of decentralization to its effects on law enforcement, and concludes by discussing the balance between protecting privacy and combating cybercrime.

Introduction

With the mark of the digital age, we are witnessing not only ground-breaking development in every technological field but also an unprecedented rise in the sophistication and frequency of cybercrimes. Without computers or other digital devices, today entire business empires and government would almost cease to continue. This coupled with the proliferation of cheap, effective and easy to use technology has led to more and more people using and depending on them for their personal and professional life. However, this same has also resulted in a gigantic leap in the quantity and refinement of cybercrimes.[1] With the evolution of these cybercrimes, cyber forensics has come out to be an indispensable tool for investigating, analyzing, and prosecuting offenses involving digital evidence. Cyber forensics relies on the ability to analyze, trace and retrieve digital footprints. However, the rise of decentralization technologies such as blockchain networks, peer-to-peer systems, and anonymity tools like Tor have fundamentally disrupted traditional forensic methods, making them extremely unviable.[2] [3]

Decentralization

The concept of decentralization can be found in various fields and disciplines, ranging from Political Science to the Internet. Usually, an umbrella term for referring to network architectures spanning from decentralized to distributed, decentralization is defined as “the transfer of control of an activity or organization to several local offices or authorities rather than one single one.”[4] Decentralization can be explained better using Baran’s Topology[5], which distinguishes between centralized, decentralized and distributed networks.

[1] Renu, 'Impact of Cyber Crime: Issues and Challenges' (2019) 3 *International Journal of Trend in Scientific Research and Development* 1569-1572 <https://doi.org/10.31142/ijtsrd23456> accessed 7 December 2024.

[2] Ashley Brinson, Abigail Robinson and Marcus Rogers, ‘A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics’ (2006) 3 Digital Investigation 37.

[3] ‘What Is the Tor Browser?’ (*WhatIs*) <https://www.techtarget.com/whatis/definition/TOR-third-generation-onion-routing> accessed 11 December 2024.

[4] Oxford Learner’s Dictionaries, 'Decentralization' <https://www.oxfordlearnersdictionaries.com/definition/english/decentralization?q=decentralization> accessed 7 December 2024.

[5] P Baran, ‘On Distributed Communications Networks’ (1964) 12 IEEE Transactions on Communications Systems 1.

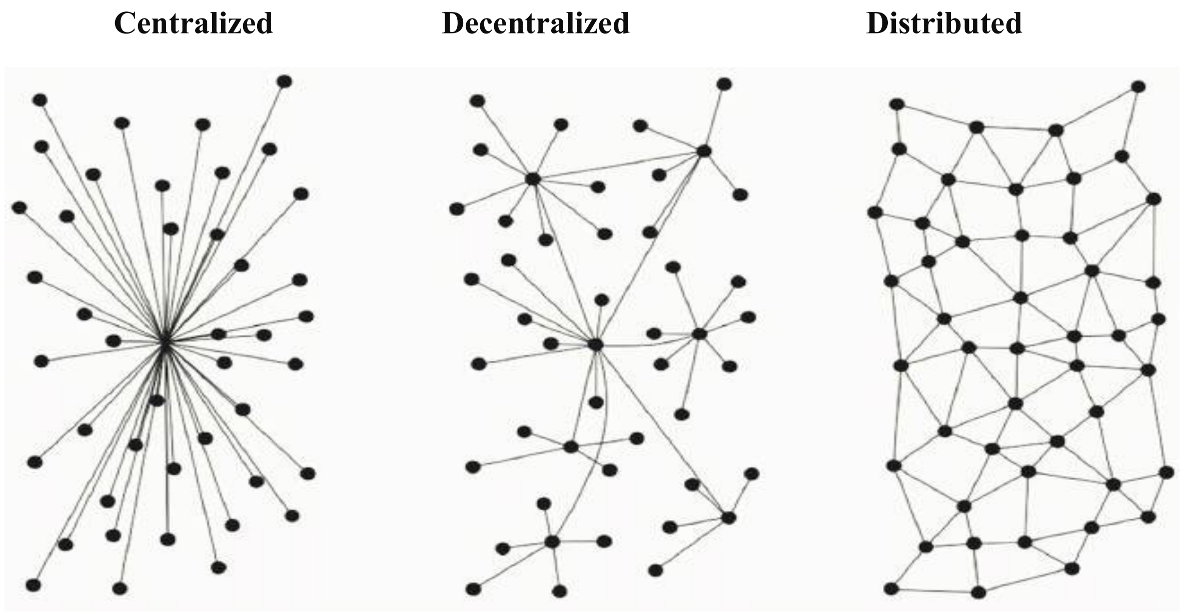


Figure 1: Various Network Topologies (Baran, 1964)

In the given schematic diagram, the **Centralized** network has one central node, that is, the sever, which is connected to all other nodes in the network, that is, the clients. This network is not much reliable as the failure or damage of the single central node disconnects all the clients and prevents them from communicating with each other.

The **Decentralized** network consists of a hierarchy of nodes, where lower nodes are connected to the nodes one level higher to them. These nodes again connect to the next higher node, thus making a network. If a few nodes fail, several parts of the network still work and are able to function.

On the other hand, we have **Distributed** networks where every node is connected to approximately the same number of nodes. Failure of few nodes does not affect the network as a whole; as the communication between the other nodes still continue, though their path might be longer.

The internet in itself is a concrete decentralized network with physical connections, but the virtual network is centralized in nature, connecting various web servers, services and platforms.[6] [7]

[6] Balázs Bodó, Jaya Klara Brekke and Jaap-Henk Hoepman, 'Decentralisation: A Multidisciplinary Perspective' (2021) 10 Internet Policy Review 1.
[7] ibid.

Characteristics of a Decentralized Network

Decentralized systems are defined by several key characteristics that distinguish them from traditional centralized systems. These characteristics include:

1. **Absence of Central Authority:** There is no single authority or node working in the center of a decentralized network. Thus, this structure enhances regulation, resilience and reduces the risk of systemic failures, due to a lack of central point of control. But this absence hinders evidence collection as there is no single repository of information.[8] [9]

2. **Anonymity and Pseudonymity:** Users have the ability to use encryptions and pseudonyms to be anonymous on the web. This takes place as all the datasets do not travel directly from the clients to the server, as in a centralized network. Instead, the datasets move through various clients.[10]

3. **Global Accessibility:** Decentralized platforms function across international borders, which poses challenges for enforcing jurisdiction-specific laws. The lack of a central authority makes it difficult to apply local regulations uniformly.[11]

4. **Distributed Control:** In decentralized systems, decision-making is distributed among multiple nodes. Each node operates independently, contributing to the overall functionality without relying on a central coordinator.[12]

5. **Fault Tolerance:** Decentralized networks are known to have very high fault tolerance because, unlike in a centralized network, even if a node or server is damaged, the rest of the nodes still function, just with the downside of taking a longer route for the

[8] 'Centralized vs. Decentralized vs. Distributed Systems' (*GeeksforGeeks*, 24 December 2018) <https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/> accessed 11 December 2024.

[9] 'On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance | Journal of Financial Regulation | Oxford Academic' <https://academic.oup.com/jfr/article/10/2/213/7606986?login=false> accessed 11 December 2024.

[10] Ahmed M Shamsan Saleh, 'Blockchain for Secure and Decentralized Artificial Intelligence in Cybersecurity: A Comprehensive Review' (2024) 5 Blockchain: Research and Applications 100193.

[11] 'What Is Decentralization? - Decentralization in Blockchain Explained - AWS' <https://aws.amazon.com/web3/decentralization-in-blockchain/> accessed 11 December 2024.

[12] 'Centralized vs. Decentralized vs. Distributed Systems' (n 8).

transmission of the datasets.[13]

6. **Scalability:** Decentralized networks can be easily scaled because of the ease of addition of nodes without increasing the complexity of the network.[14]

Challenges posed by Decentralization on Cyber Forensics:

With all the advantages like privacy and fault tolerance that decentralization brings, there is one major downside. Decentralization poses several significant challenges on the effectiveness and efficiency of cyber forensics. These challenges include:

1. **Evidence Collection**: Probably the biggest challenge that decentralization methods like blockchain poses to cyber forensics is evidence collection, as here evidence such as records of communication logs and transactions are dispersed across a distributed network. Even very sophisticated and advanced technology fails to retrieve these, making it extremely difficult for cyber forensics experts to track down criminals who misuse the decentralized networks like TOR to commit offences like running drug cartels, selling arms and fake passports, and propagating child pornography.[15] [16]

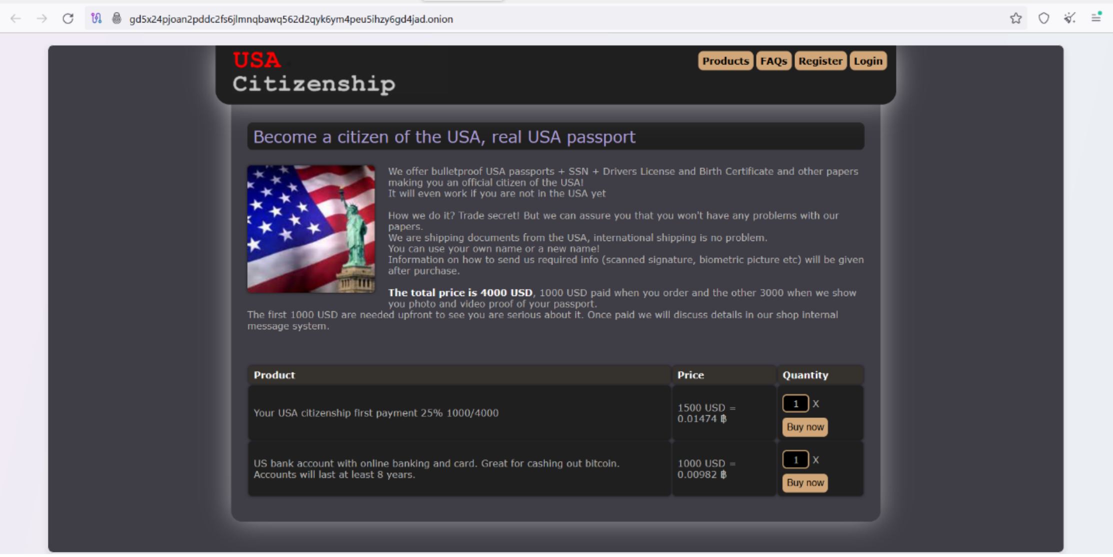
2. **Authentication and Integrity**: Even if the data is collected in form of evidence, the authenticity of the data collected from decentralized system is often violated. Proving the integrity of evidence and maintaining a secure chain of custody is significantly challenging due to the possibility of data tampering. This raises concerns about the evidentiary value of such data in legal proceedings.[17] [18]

3. **Encryption as a Double-Edged Sword**: While encryption has a vital use in today's world which is to protect individual right to privacy in terms of user data, it also poses

[13] Shamsan Saleh (n 10).
[14] 'Centralized vs. Decentralized vs. Distributed Systems' (n 8).
[15] Vinod Kumar Uppalapu and Ajay Agarwal, 'Digital Forensics Investigation Framework Based on the Blockchain, IOT, and Social Networks' (2024) 12 International Journal of Intelligent Systems and Applications in Engineering 1179.
[16] 'How Blockchain Can Improve Digital Evidence Collection and Collaboration' (*Route Fifty*, 8 March 2023) <https://www.route-fifty.com/emerging-tech/2023/03/how-blockchain-can-improve-digital-evidence-collection-and-collaboration/383756/> accessed 13 December 2024.
[17] Hany F Atlam and others, 'Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions' (2024) 13 Electronics 3568.
[18] S Adolphine Shyni and others, 'Preservation Of Digital Forensic Evidence Using Blockchain Technology' (2024) 30 Educational Administration: Theory and Practice 5556.

substantial obstacles in the cyber forensic analysis. It often poses multiple difficulties in decrypting communications or files or datasets without access to appropriate keys. This hinders the ability to gather critical evidence and use it when necessary.

4. **Legal Gaps**: Traditional legal frameworks, such as Indian Evidence Act, 1872 did not address the complexities introduced by the decentralized systems. Even the modernized and sophisticated, newly-released, Bharatiya Sakshya Adhiniyam, 2023, struggle to address these issues. These legislative frameworks may acknowledge electronic evidence but often lack specific provisions for handling anonymous data storage and sharing across decentralized networks like blockchain. This leads to potential legal ambiguities during investigations.[19] [20]



gd5x24pjoan2pddc2fs6jlmnqbawq562d2qyk6ym4peu5ihzy6gd4jad.onion

USA
Citizenship

Become a citizen of the USA, real USA passport

We offer bulletproof USA passports + SSN + Drivers License and Birth Certificate and other papers making you an official citizen of the USA!
It will even work if you are not in the USA yet

How we do it? Trade secret! But we can assure you that you won't have any problems with our papers.
We are shipping documents from the USA, international shipping is no problem.
You can use your own name or a new name!
Information on how to send us required info (scanned signature, biometric picture etc) will be given after purchase.

The total price is 4000 USD, 1000 USD paid when you order and the other 3000 when we show you photo and video proof of your passport.
The first 1000 USD are needed upfront to see you are serious about it. Once paid we will discuss details in our shop internal message system.

Product	Price	Quantity
Your USA citizenship first payment 25% 1000/4000	1500 USD = 0.01474 ฿	1 X Buy now
US bank account with online banking and card. Great for cashing out bitcoin. Accounts will last at least 8 years.	1000 USD = 0.00982 ฿	1 X Buy now

Figure 2: Screenshot of a dark-web site which claims to sell illegal USA passports.

TOR: A Case Study

TOR, originally short for The Onion Router, is a free and open-source network that enables anonymous communication on the internet. Journalists, activists, law enforcement officers, and military personnel use Tor to communicate more safely with other parties. Other entities, such as companies, use Tor to keep business intelligence, industrial espionage, and trade secrets

[19] Uppalapu and Agarwal (n 15).
[20] 'How Blockchain Can Improve Digital Evidence Collection and Collaboration' (n 16).

safe.[21]

History of TOR:

The Onion Router also known as TOR network was initially developed in the mid-1990s by the U.S. Naval Research Laboratory. Its primary goal was to protect intelligence communications online by routing traffic through multiple servers, or nodes, to obscure the origin and destination of data. This method is called "onion routing" because it layers encryption, similar to the layers of an onion.[22]

In 2002, the first public version of Tor was launched. The project gained traction in 2004 when the U.S. Naval Research Laboratory (NRL) released its code under a free and open-source license. The Tor Project, a non-profit organization, was established in 2006 to oversee its development and expand its applications.[23] [24]. Over time, Tor evolved from a military tool into a widely used platform for privacy and anonymity.[25]

The following map, *The Anonymous Internet, 2015*, illustrates global Tor usage, highlighting daily users per 100,000 internet users and offering insights into regional adoption patterns.[26] [27]

[21] ‘What Is the Tor Browser and Is It Safe?’ (/, 16 October 2023) <https://www.kaspersky.com/resource-center/definitions/what-is-the-tor-browser> accessed 13 December 2024.
[22] ‘Onion Routing: History’ <https://www.onion-router.net/History.html> accessed 13 December 2024.
[23] ibid.
[24] ‘Onion Routing and Tor’ (*Georgetown Law Technology Review*, 29 November 2016) <https://georgetownlawtechreview.org/onion-routing-and-tor/GLTR-11-2016/> accessed 13 December 2024.
[25] ibid.
[26] DarkOwl Content Team, ‘[Interactive Timeline] Tor and Beyond: Key Developments in the History of the Darknet’ (*DarkOwl, LLC*, 6 July 2023) <https://www.darkowl.com/blog-content/interactive-timeline-tor-and-beyond-key-developments-in-the-history-of-the-darknet/> accessed 13 December 2024.
[27] ‘Tor usage worldwide: The Anonymous Internet’ (*Digitale Gesellschaft*, 21 June 2017) <https://www.digitale-gesellschaft.ch/2017/06/21/tor-usage-worldwide-the-anonymous-internet-new-infographic/> accessed 13 December 2024.

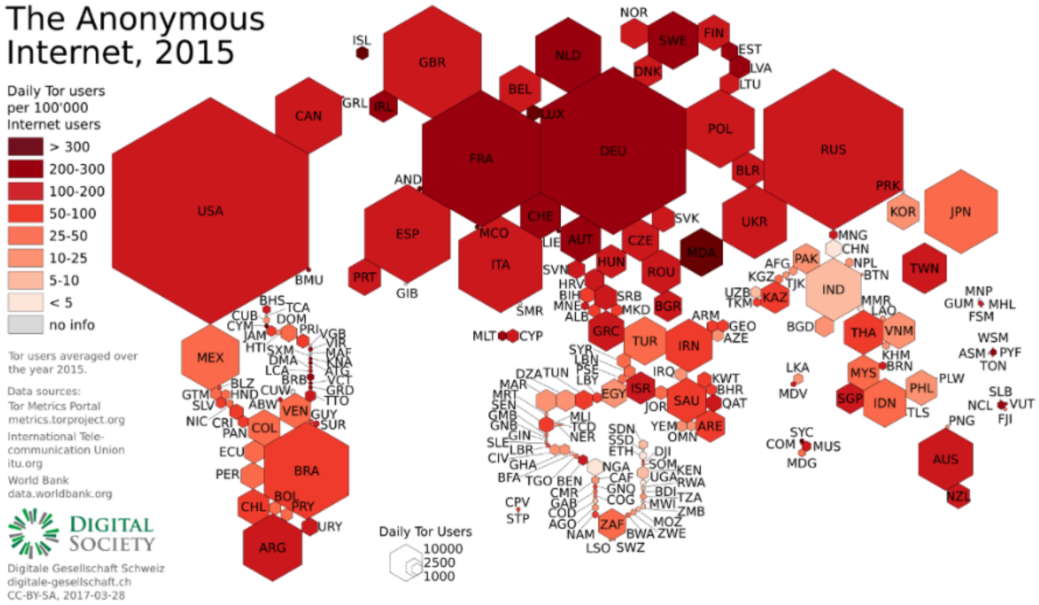


Figure 3: "The Anonymous Internet, 2015" map

Working of the Onion-Routing

Onion routing ensures anonymous communication by encrypting and routing data through multiple servers, called nodes. The process starts when a user sends data via the Tor network. It selects a random path of at least three nodes: an entry node, a middle node, and an exit node. Each node knows only its immediate predecessor and successor but not the entire path, preserving anonymity. The data is encrypted in multiple layers, like an onion. At the user's end, the data is wrapped in several layers of encryption, each corresponding to a node in the route. As the data passes through each node, one encryption layer is peeled off, revealing the next destination. The exit node removes the final layer and forwards the plaintext data to its destination.[28] [29]

This design ensures no single node knows both the sender and receiver, protecting user privacy and making it difficult to trace the communication back to its origin.[30] [31]

[28] 'Working of Tor Browser' (*GeeksforGeeks*, 13:00:22+00:00) <https://www.geeksforgeeks.org/working-of-tor-browser/> accessed 13 December 2024.

[29] 'What Is Tor? | How Does It Work? | Everything About Tor Network' <https://techofide.com/blogs/what-is-tor-how-does-it-work-everything-about-tor-network/> accessed 13 December 2024.

[30] ibid.

[31] Abid Khan Jadoon and others, 'Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web' (2019) 299 Forensic Science International 59.

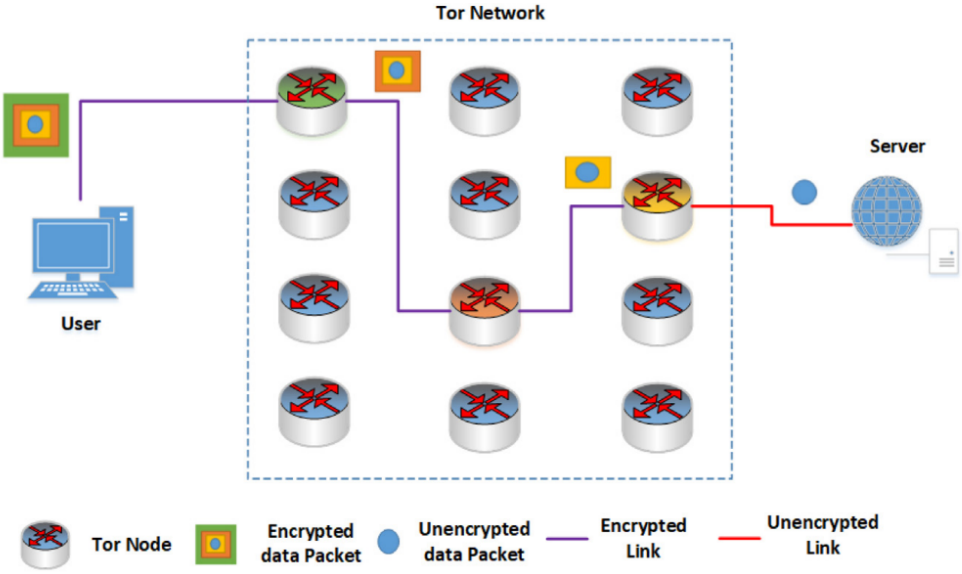


Figure 4: Working of the Onion Routing

How TOR Hinders Cyber Forensics

The Onion Router (TOR) poses significant challenges to cyber forensics investigations. One of the primary ways Tor hinders cyber forensics is by masking the identity and location of users. The use of multiple relays and encryption makes it extremely difficult to trace the origin of traffic, as the final destination only sees the Tor exit node rather than the actual sender. This anonymity can obscure the identity of criminals or attackers, making it harder for forensic experts to identify and apprehend suspects.[32]

Additionally, Tor allows users to access the dark web, where illicit activities, such as drug trafficking, illegal pornography, and hacking services, are often conducted. Even when traces of criminal activity are found, the information available may be insufficient to tie suspects to a crime.[33]

In cyber forensic investigations, the challenge of tracing and deciphering encrypted communications over Tor requires sophisticated technical expertise and resources. This complexity not only increases the time and cost of investigations but also limits the

[32] Malak Alfosail and Peter Norris, 'Tor Forensics: Proposed Workflow for Client Memory Artefacts' (2021) 106 Computers & Security 102311.
[33] Jadoon and others (n 31).

effectiveness of traditional forensic techniques.[34] [35]

Tor's impact on cyber forensics can be seen in the case of Silk Road, the notorious dark web marketplace. Silk Road allowed users to engage in illegal activities, such as drug trafficking and money laundering, while maintaining anonymity through Tor. The use of Tor made it difficult for authorities to trace the identities and locations of the individuals involved. Despite this, investigators eventually managed to track down the site's creator, Ross Ulbricht, through a combination of digital footprints, undercover operations, and traditional forensic methods.[36] This case illustrates how Tor can complicate investigations, requiring significant resources and expertise to bypass its encryption and uncover illicit activities hidden on the dark web.[37] [38]

Conclusion

Decentralization, indeed proves to be a double-edged sword. While it is deemed to be crucial for individual privacy, in today's privacy focused world, the downside it brings can no way be looked down upon. Decentralized networks risk the propagation of illegal activities ranging from selling ammunitions, drugs, illegal passports, to hiring hitmen and even child pornography. It is definitely to be pondered upon whether one's personal right to privacy supersedes the need to prevent these gruesome cybercrimes.

Due to the layers of nodes and the lack of centralization, it becomes extremely difficult for cyber forensics expert to track down people and cartels on the decentralized networks. Thus, indeed decentralization is the deathbed of cyber forensics.

[34] ibid.

[35] Alfosail and Norris (n 32).

[36] 'Ross William Ulbricht's Laptop' (*Federal Bureau of Investigation*) <https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop> accessed 14 December 2024.

[37] 'Inside Darknet: The Takedown of Silk Road | Centre for Crime and Justice Studies' <https://www.crimeandjustice.org.uk/publications/cjm/article/inside-darknet-takedown-silk-road> accessed 14 December 2024.

[38] 'Southern District of New York | U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud | United States Department of Justice' (7 November 2022) <https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction> accessed 14 December 2024.

Bibliography

1. Alfosail M and Norris P, ‘Tor Forensics: Proposed Workflow for Client Memory Artefacts’ (2021) 106 Computers & Security 102311

2. Atlam HF and others, ‘Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions’ (2024) 13 Electronics 3568

3. Baran P, ‘On Distributed Communications Networks’ (1964) 12 IEEE Transactions on Communications Systems 1

4. Bodó B, Brekke JK and Hoepman J-H, ‘Decentralisation: A Multidisciplinary Perspective’ (2021) 10 Internet Policy Review 1

5. Brinson A, Robinson A and Rogers M, ‘A Cyber Forensics Ontology: Creating a New Approach to Studying Cyber Forensics’ (2006) 3 Digital Investigation 37

6. ‘Centralized vs. Decentralized vs. Distributed Systems’ (*GeeksforGeeks*, 24 December 2018) <https://www.geeksforgeeks.org/comparison-centralized-decentralized-and-distributed-systems/> accessed 11 December 2024

7. ‘Decentralization Noun - Definition, Pictures, Pronunciation and Usage Notes | Oxford Advanced Learner’s Dictionary at OxfordLearnersDictionaries.Com’ <https://www.oxfordlearnersdictionaries.com/definition/english/decentralization?q=decentralization> accessed 7 December 2024

8. ‘How Blockchain Can Improve Digital Evidence Collection and Collaboration’ (*Route Fifty*, 8 March 2023) <https://www.route-fifty.com/emerging-tech/2023/03/how-blockchain-can-improve-digital-evidence-collection-and-collaboration/383756/> accessed 13 December 2024

9. ‘Inside Darknet: The Takedown of Silk Road | Centre for Crime and Justice Studies’ <https://www.crimeandjustice.org.uk/publications/cjm/article/inside-darknet-takedown-silk-road> accessed 14 December 2024

10. Jadoon AK and others, 'Forensic Analysis of Tor Browser: A Case Study for Privacy and Anonymity on the Web' (2019) 299 Forensic Science International 59

11. 'On DeFi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance | Journal of Financial Regulation | Oxford Academic' <https://academic.oup.com/jfr/article/10/2/213/7606986?login=false> accessed 11 December 2024

12. 'Onion Routing and Tor' (*Georgetown Law Technology Review*, 29 November 2016) <https://georgetownlawtechreview.org/onion-routing-and-tor/GLTR-11-2016/> accessed 13 December 2024

13. 'Onion Routing: History' <https://www.onion-router.net/History.html> accessed 13 December 2024

14. 'Ross William Ulbricht's Laptop' (*Federal Bureau of Investigation*) <https://www.fbi.gov/history/artifacts/ross-william-ulbrichts-laptop> accessed 14 December 2024

15. Shamsan Saleh AM, 'Blockchain for Secure and Decentralized Artificial Intelligence in Cybersecurity: A Comprehensive Review' (2024) 5 Blockchain: Research and Applications 100193

16. Shyni SA and others, 'Preservation Of Digital Forensic Evidence Using Blockchain Technology' (2024) 30 Educational Administration: Theory and Practice 5556

17. 'Southern District of New York | U.S. Attorney Announces Historic $3.36 Billion Cryptocurrency Seizure And Conviction In Connection With Silk Road Dark Web Fraud | United States Department of Justice' (7 November 2022) <https://www.justice.gov/usao-sdny/pr/us-attorney-announces-historic-336-billion-cryptocurrency-seizure-and-conviction> accessed 14 December 2024

18. Team DC, '[Interactive Timeline] Tor and Beyond: Key Developments in the History of the Darknet' (*DarkOwl, LLC*, 6 July 2023) <https://www.darkowl.com/blog-content/interactive-timeline-tor-and-beyond-key-developments-in-the-history-of-the-darknet/> accessed 13 December 2024

19. ‘Tor usage worldwide: The Anonymous Internet’ (*Digitale Gesellschaft*, 21 June 2017) <https://www.digitale-gesellschaft.ch/2017/06/21/tor-usage-worldwide-the-anonymous-internet-new-infographic/> accessed 13 December 2024

20. Uppalapu VK and Agarwal A, ‘Digital Forensics Investigation Framework Based on the Blockchain, IOT, and Social Networks’ (2024) 12 International Journal of Intelligent Systems and Applications in Engineering 1179

21. ‘What Is Decentralization? - Decentralization in Blockchain Explained - AWS’ <https://aws.amazon.com/web3/decentralization-in-blockchain/> accessed 11 December 2024

22. ‘What Is the Tor Browser?’ (*WhatIs*) <https://www.techtarget.com/whatis/definition/TOR-third-generation-onion-routing> accessed 11 December 2024

23. ‘What Is the Tor Browser and Is It Safe?’ (/, 16 October 2023) <https://www.kaspersky.com/resource-center/definitions/what-is-the-tor-browser> accessed 13 December 2024

24. ‘What Is Tor? | How Does It Work? | Everything About Tor Network’ <https://techofide.com/blogs/what-is-tor-how-does-it-work-everything-about-tor-network/> accessed 13 December 2024

25. ‘Working of Tor Browser’ (*GeeksforGeeks*, 13:00:22+00:00) <https://www.geeksforgeeks.org/working-of-tor-browser/> accessed 13 December 2024