DOI: https://doi.org/10.52756/ijerr.2023.v32.017 *Int. J. Exp. Res. Rev.*, Vol. 32: 195-205(2023)

Original Article | *Peer Reviewed* | *Open Access*

International Journal of Experimental Research and Review (IJERR)

ISSN: 2455-4855 (Online)
www.iaph.in
ISSN 2455-4855

Anonymity in decentralized apps: Study of implications for cybercrime investigations

Arjun Chetry* and Uzzal Sharma

Department of Computer Science and Engineering, Assam Don Bosco University, Guwahati, India

E-mail/Orcid Id:

AC, chetry.arjun@gmail.com, https:// orcid.org/0000-0003-0405-4471; *US,* druzzalsharma@gmail.com, https://orcid.org/0000-0002-5264-1016

Article History:

Received: 17th Jun., 2023
Accepted: 16th Aug., 2023
Published: 30th Aug., 2023

Keywords:
Anonymous communication, decentralized application, DApps, OSINT, cybercrime investigation, digital evidence, digital forensics.

Abstract: In the digital age, cybercrime facilitated by anonymous communication apps raises significant concerns. Criminals exploit the anonymity provided by these apps, creating challenges for law enforcement and cybersecurity professionals when investigating and combating cybercrime. The complexity of decentralized applications (DApps) without centralized servers further complicates evidence certification. Although anonymity features to protect privacy, they impede the establishment of connections between digital accounts and real-world identities. In centralized server environments, data access for investigations is relatively straightforward. However, this study reveals that DApps present challenges due to decentralized control, anonymity, encrypted communication, and jurisdictional issues. DApps designed for anonymous communication allow users to interact without revealing their identities, making it challenging to trace criminals. While cybercrime investigations in centralized environments involve systematic evidence collection, correlation, analyzing communication patterns, collaboration with agencies, tracking IP addresses, legal authorization, and forensic analysis of digital devices, DApps-based investigations require vital intelligence gathering through open-source techniques (OSINT). This includes retrieving digital footprints, analyzing social media profiles, and tracing ownership information. Moreover, investigators may exploit human vulnerabilities, engage in deceptive communication, or use social engineering techniques to gather information while carefully considering the balance between user privacy and investigative requirements. In this study, we explore the many facets of anonymity in DApps and what challenges they impose for the investigation of cybercrime. The anonymity of users and their transactions in the context of new blockchain and decentralized technology presents difficulties for law enforcement. In the end, our research helps shed light on the complex relationship between anonymity in decentralized systems and the need for fairness online.

Introduction

In today's digital age, the alarming prevalence of cybercrime through anonymous communication apps raises serious concerns for every internet user. Criminals exploit the anonymity offered by these apps and networks and engage in various illicit activities, evading identification and location tracking. While anonymity features protect privacy, facilitate free expression, and enable whistleblowing or reporting sensitive information without fear of retribution, they also impose significant challenges in investigating and combating cybercrime for law enforcement agencies and cybersecurity professionals (Raj, 2019). The encryption and anonymity provided by such platforms make it challenging to trace the origin of attacks and identify the perpetrators (Wu et al., 2021). Extracting evidence from these devices becomes crucial in identifying and prosecuting cybercriminals involved in hacking, cyber espionage, identity theft, online fraud, and other illicit activities. However, even after extracting digital evidence from devices used in anonymous communication during such criminal activities, establishing a connection between a digital account or online identity and a real person in the physical world remains a common challenge. This

***Corresponding Author:** chetry.arjun@gmail.com

challenge is further amplified in the context of decentralized applications (DApps) involved in cybercrime cases, as there is no centralized server to certify the evidence or support investigating agencies (Alabdulwahhab, 2018; Cai et al., 2018). Moreover, if DApps allow users to interact using pseudonyms or without revealing their real identities, their anonymity poses additional difficulties for investigators in establishing links between specific individuals and their actions on the DApps.

Cybercrime investigation procedure in centralized server environment

Cybercrime investigation procedures necessitate a systematic and methodical approach to acquiring evidence, analyzing data, and identifying perpetrators engaging in criminal activities through digital means. The specific steps involved in these procedures can vary, contingent upon the nature and complexity of the cybercrime under investigation, but they generally adhere to a core set of critical principles (Chougule et al., 2022; Hunton, 2011; Jeffries and Apeh, 2020).Gathering Digital Evidence: Immediately at the complainant's end, it is essential to collect digital evidence entails analyzing logs, extracting data, examining communication records, and preserving files with utmost forensic integrity to ensure its admissibility in legal proceedings(Granja and Rafael, 2017; Reedy, 2020).

Investigators analyze the gathered digital evidence like identifying patterns, timestamps, and event sequences that can provide insights into the attacker's actions to establish connections and correlations between different pieces of data and make it acceptable in a court of law (Yeboah-Ofori and Brown, 2020). Investigators trace digital footprints left by cyber criminals through communication patterns, analyzing channels like e-mails, instant messages, and social media interactions to uncover potential leads and link attackers to that cybercrime (Schwerha, 2004). Cybercrime investigations often necessitate collaboration with diverse entities, including law enforcement agencies, cybersecurity firms, and international partners, as cybercriminals frequently operate across borders (Chang, 2017; Redford, 2011). This collaborative approach involves sharing information, exchanging intelligence, and coordinating joint efforts to track and apprehend suspects effectively (Wang et al., 2021). Investigators may approach an intermediary to assist the investigation by providing information or logs related to the attacker's account or activities (Sorbán, 2019). IP addresses serve as valuable clues that can guide investigators to the origin of cybercrime. By tracing these addresses and collaborating with ISPs, investigators endeavor to unveil the physical location or user associated with malicious activities, though challenges may arise if the attacker conceals their real IP or employs a botnet, proxy servers, VPN, etc. (Jordan, 2020; Kesari et al., 2017; Shah and Chudasama, 2021). Investigators may use open-source intelligence techniques or tools to trace the perpetrators. Various tools and Linux distro are publicly available for investigators and digital forensics experts in this regard. Investigators use forensic techniques to extract, analyze, and interpret data from various sources. This involves examining file systems, network logs, memory dumps, and metadata to reconstruct the events leading to the cybercrime (Caviglione et al., 2017; Patil et al., 2022). Therefore, in the case of centralized environment, LEAs may approach the intermediary servers to provide the information about the perpetrator.

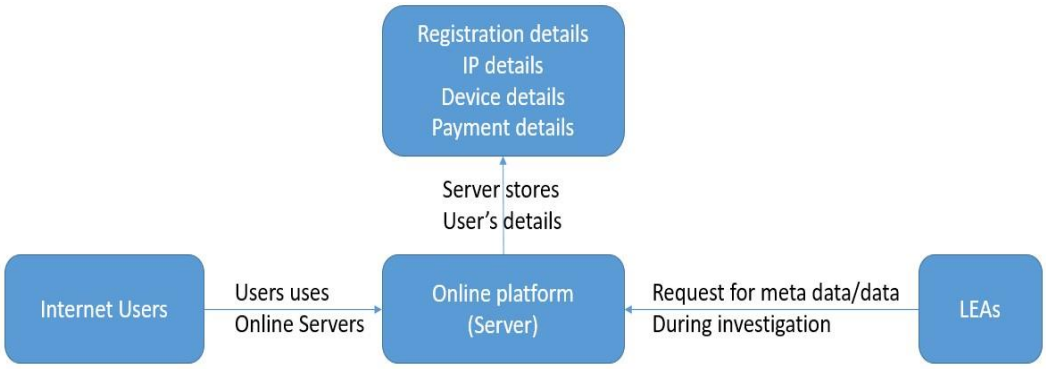

Figure 1. Centralized server-based data request

Investigation challenges involving centralized server-based cases

Several challenges arise in cybercrime investigations involving centralized servers, including jurisdictional issues due to varying laws across countries. Accessing data or cooperation from server operators in different jurisdictions can be difficult. Moreover, the vast amount of user data stored on these servers raises concerns about data privacy and protection, requiring investigators to comply with relevant laws. Even with user registration,

DOI: https://doi.org/10.52756/ijerr.2023.v32.017

cybercriminals can use fake credentials or anonymous accounts, leading to difficulties in identifying them. Tracing anonymous accounts and linking them to specific individuals requires meticulous investigation, collaboration with service providers, and data analysis. Data encryption on centralized servers can also hinder investigations, as decryption is time-consuming and only sometimes feasible. Preserving evidence becomes critical as cybercriminals may swiftly delete incriminating data upon detecting ongoing investigations. Law enforcement agencies (LEAs) must act swiftly to preserve data and issue legal requests before permanently deleting relevant information.

Furthermore, the lack of specialized technical expertise in digital forensics, data analysis, and network security presents significant challenges for LEAs in effectively tackling online cybercrime cases. Using anonymizing operating systems like Whonix and Tails, which employ the Tor network to route internet traffic through multiple relays, further complicates investigations (Goohs Jr, 2021; Ranakoti et al., 2017). These systems enhance user privacy by utilizing pseudonyms, obfuscating IP addresses, and employing encrypted communication channels with added layers of complexity and data fragmentation across multiple virtual machines (VMs) and nodes. However, there may still be novel ways to find this hidden information, so the investigators should explore the possibilities (Nurmi & Niemelä, 2017). As a result, data retrieval and correlation become more challenging for investigators, ultimately protecting users' online activities but posing significant obstacles for cybercrime investigators.

Addressing these challenges necessitates a comprehensive approach involving continuous collaboration between law enforcement agencies (LEAs), international cooperation agreements, technological investments, legal reforms, and robust investigator training programs. Equipping investigators with the necessary skills to navigate the complexities of cybercrime investigations within centralized servers is essential. Striking a delicate balance between safeguarding user privacy and effectively combating cybercrimes is crucial for ensuring public safety in the digital era. The rapidly evolving nature of centralized servers and associated technologies introduces new features, encryption methods, and security measures that may impede investigations. To stay effective, LEAs must stay updated on technological advancements, invest in ongoing training, and collaborate with experts to adapt to these dynamic landscapes.

Centralized & Decentralized applications

DApps for communication signify a paradigm shift from reliance on Trusted Third Parties (TTP) to decentralized, trust-based applications utilizing blockchain technology, fundamentally shaping our digital interactions (Pop et al., 2020; Yue et al., 2021). In contrast to conventional communication apps that depend on centralized servers and intermediaries, DApps employ blockchain or peer-to-peer networks, enabling direct communication between users and guaranteeing heightened privacy, security, and resistance to censorship. These DApps exhibit enhanced resilience and autonomy by eliminating single points of failure, empowering users to regain control over their data and communications (Petcu et al., 2023). Moreover, DApps possess the capacity to transcend geographical barriers, functioning without intermediaries, making them a compelling option for future global, decentralized communication networks. However, it is essential to acknowledge that while blockchain-empowered decentralized apps can bring numerous positive impacts, their utmost privacy features might also create a safe environment for illicit users engaging in illegal activities.

Centralized servers offer easier data accessibility for investigating agencies as data is stored in one location, allowing cooperation with the server owner for information. They retain data for extended periods, aiding retrospective investigations, and have clear accountability. Legal compliance is more straightforward, but they are vulnerable to single points of failure. In contrast, decentralized servers complicate data access with distributed storage, prioritize user privacy and anonymity, and may lack a central authority for legal requests. Data retention can be shorter, and while distributed security is more robust, tracing malicious activities becomes challenging for investigators. The development of DApps has led to the emergence of various innovative contract platforms like Binance Smart Chain, EOSIO, TRON, Fantom, Polygon, Solana, Avalanche, etc. However, there is no straightforward way to compare the entire DApps ecosystem of each platform (Zheng et al., 2023).

Decentralized applications (DApps) for Communication – LEAs perspective

Decentralized communication applications present unique challenges and considerations in the context of investigation and law enforcement activities as they offer enhanced security and anonymity for every user. Striking a balance between user privacy and the need for effective law enforcement is a complex challenge in the evolving

DOI: https://doi.org/10.52756/ijerr.2023.v32.017

digital landscape. LEAs must adapt their investigative strategies, collaborate with experts, and explore novel methods to investigate DApps-related criminal activities in a rapidly evolving digital landscape. DApps can implement secure messaging and communication protocols, ensuring that conversations between protected users from eavesdropping and tampering, along with many other technical features possible in DApps (Abdulaziz et al., 2018; Shen et al., 2021).

With so many anonymity features available, it is pertinent to mention that illicit users will be attracted to Daps for committing online crimes. In DApps, just like in any other online environment, cyber frauds can manifest in various forms, and some of these are as mentioned below.

Role of DApps in anonymous communication

One of the most significant roles of DApps is enabling anonymous communication, allowing users to interact

Table 1. DApps features and investigation challenges

Particulars	LEAs – challenges in investigation
Decentralized Control	The lack of a single entity or central server may hinder ongoing investigative methods that rely on centralized servers to retrieve evidence. Moreover, in case of a requirement to remove unwanted content or block unwanted apps.
Anonymity and Pseudonymity	Features offering pseudonyms may motivate illicit users to migrate, as this anonymity can facilitate criminal behavior and hinder attribution.
Encrypted Communication	While this protects user privacy, it can also hinder LEAs from intercepting and accessing communications related to criminal activities.
Tracing Transactions	DApps often involve cryptocurrencies or blockchain technology, making financial transactions more challenging to trace. This can hinder efforts to follow the money trail and identify financial patterns related to illegal activities.
Jurisdictional Challenges	DApps work on global platforms, and illicit users may hide their identity behind fake details or IP Addresses.
Time-Sensitive	DApps may have a time limit in storing the metadata, offering an advantage to illicit users.
Cryptographic protocols	Public-key cryptography, cryptographic hashing, and symmetric encryption ensure secure and confidential data transmission.
Zero-knowledge proofs (ZKPs)	Zero-knowledge proofs are cryptographic techniques that allow one party (the prover) to prove the truth of a statement to another party (the verifier) without revealing any additional information. ZKPs can demonstrate knowledge of specific data without disclosing the data itself, enhancing privacy in DApps.
Ring signatures	Ring signatures enable a user to sign a message on behalf of a group of users, making it difficult to determine which specific user in the group performed the signing. This feature enhances the anonymity of transactions within DApps.
Identity solutions	DApps can leverage decentralized identity solutions, such as self-sovereign identity (SSI) or decentralized identifiers (DIDs), to create and manage user identities in a privacy-preserving manner.

Table 2. DApps based frauds

Frauds Types	Description
Scams and Ponzi Schemes	Malicious actors create fraudulent DApps promising high returns or rewards, deceiving users into investing funds.
Phishing Attacks	Hackers may try to steal sensitive information by creating fake DApps interfaces or websites resembling legitimate ones.
Smart Contract Vulnerabilities	Smart contract code's vulnerabilities can be exploited to manipulate transactions, drain funds, or disrupt DApps.
Pump and Dump Schemes	Fraudsters spread misleading information to artificially inflate a token's value within a DApps and then profit by "dumping" their holdings, causing significant losses for other users.
Fake Exchanges	Fraudulent DApps may pose as cryptocurrency exchanges, enticing users to deposit their funds only to have them stolen or lost.

DOI: https://doi.org/10.52756/ijerr.2023.v32.017

Table 3. DApps-based apps – category-wise

Category	DApps for Anonymity
Messaging	Briar, qTox, Ricochet, Status, Session, Keybase, etc.
Disposable Messages	Session, Status, Element, Briar, Secure Scuttlebutt, DUST, Stealthy, etc.
Anonymous Email Services	Send Safely, Mail fence, Proton Mail, Cwtch, etc.
Anonymous Voice Calls	Ring Confidentiality, Snomed, Tox, Session, Riot.im, Orchid, etc.
Forums	Mastodon, Peertube, Zero Talk, Namecoin, etc.
File sharing	Onion Share, IPFS, Swarm, Tahoe-LAFS, I2P Torrents, Filecoin, Sia, Storj, Bluzelle, Golem, etc.
Social networks	Steemit, Minds, Peepeth, Sapien, Indorse, Sphere, LBRY, etc.
Marketplaces	Open Bazaar, BitShares, etc.
Virtual Private Network (VPN)	KelVPN, Orchid, Mysterium Network, Sentinel, Privatix, Tachyon VPN, Substratum, etc.

and exchange information without revealing their real-world identities. As individuals and organizations become increasingly aware of the value of online privacy and secure communication, the popularity of DApps with anonymous communication will likely continue growing, especially in an era of extensive data collection and surveillance. These decentralized solutions offer an essential counterbalance to centralized data silos and surveillance, empowering users to reclaim control over their digital interactions while preserving their fundamental rights to privacy and freedom of expression. Such DApps empower whistleblowers and journalists to share information securely and confidentially, protecting their identities and ensuring the dissemination of important news without fear of retaliation. Data, once recorded, cannot alter it, ensuring the integrity and trustworthiness of the application.

Types of DApps for anonymous communication

Some of the DApps are for anonymous communication or sharing of data with features like end-to-end encryption, pseudonymous usernames, etc. Some route all traffic through the Tor network, making it difficult for anyone to track who is communicating with whom.

Investigation challenges in DApps in comparison to Centralized Server

The investigation may differ in every case depending on the case and the process of committing such crimes. In addition, the person involved in any crime may influence the types of evidence possible for retrieval in that case.

However, let us broadly compare the existing centralized based server and decentralized based environment for the investigation procedure. Investigation challenges in Decentralized Applications (DApps) may differ significantly from those in centralized server-based systems.

As DApps are working on multiple servers, it may be challenging to track down all data or transactions involved in a particular case and to bring the same in a court-acceptable form. In the case of the intermediate central server, LEAS can get user registration information, IP address involved, etc. However, in the absence of centralized server in DApps, it is difficult for LEAs to identify the illicit user involved in any crime. In addition, most of these DApps are based on blockchain technology, which is immutable, so it may not be possible to remove or edit data or files as per complains received during the investigation. Even after identifying a particular account involved in illicit activities, it may be tedious to identify the evidence to link that particular account with the real-world user.

Investigation changes for cybercrime involving DApps platforms.

With the increasing adoption of DApps, tackling these cyber threats becomes crucial to safeguarding decentralised ecosystems' long-term viability and safety. The inherent design of DApps, aimed at enhancing user privacy and security, creates complexities that traditional investigative approaches may need help to address effectively. In order to combat cybercrime in decentralized applications, a comprehensive strategy and close cooperation between law enforcement agencies and technology providers are essential(Dyson et al., 2019; Rahmadika et al., 2021). While some DApps store data on the blockchain, others may rely on off-chain storage or peer-to-peer networks, making data collection and preservation complex. When dealing with cases related to decentralized applications, a meticulous and well-organized investigative approach is necessary to gather crucial evidence and apprehend the culprits.

DOI: https://doi.org/10.52756/ijerr.2023.v32.017

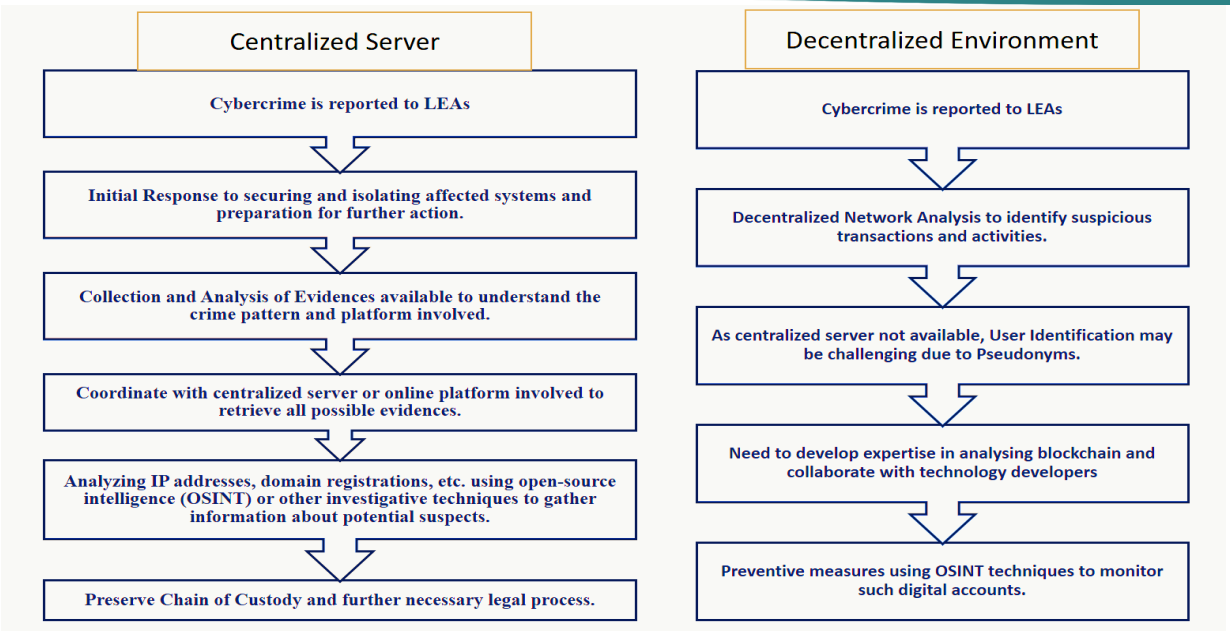

Figure 2. Comparison of centralized and decentralized investigation

While DApps provide anonymity at the content level, metadata that reveals communication patterns, transaction frequency, or timing can be crucial in investigations. However, obtaining such metadata is often challenging in anonymous DApps environments. Therefore, investigating DApps-based frauds is challenging compared to centralized server cases, where officers can easily approach well-established communication channels of online platforms involved in a crime to obtain perpetrator details. Some areas to target or follow while investigating cases involving DApps may be as below.

- Gather information about DApps involved in the crime
- Document all evidence about suspicious transactions, activities, etc.
- OSINT for IP Addresses and Geolocation information of that account
- Assistance from DApps developers, cybersecurity / forensics experts for further necessary procedures.

Gathering intelligence using OSINT techniques

Gathering intelligence through OSINT techniques for DApps involves leveraging publicly available information from various online sources to gain insights into users, transactions, and related entities within the DApps ecosystem. This approach aims to acquire valuable data without requiring specialized access or hacking. OSINT can track users' digital footprint across multiple platforms, providing insights into their interests, affiliations, and potential connections(Hwang et al., 2022). DApps users often maintain online identities on various social media platforms. By monitoring these profiles, investigators can extract valuable information, such as real names, locations, and other personal details associated with the digital account.

Additionally, users might engage in discussions or seek support on public forums and community platforms, offering potential hints about their identity. Investigators can cross-reference usernames or email addresses across different online services to identify the individuals behind specific digital accounts. If users have uploaded profile pictures or other images on their DApps accounts, conducting a reverse image search can lead to discovering other instances of the same image online, potentially linking to social media accounts or other sources related to the individual. Moreover, OSINT can be used to trace ownership information by examining publicly available domain registration details of the DApps or related websites, potentially revealing the actual identity of the account holder (Azad, 2022).

Regarding payment-related information, transactions are often publicly available on the blockchain, particularly in cryptocurrencies. Although blockchain transactions are pseudonymous, OSINT can be applied to explore interactions between addresses, uncovering transaction patterns or connections with known entities that may provide clues about the user's identity. The anonymous nature of DApps can make it difficult for investigators to verify users' identities, potentially leading to false positives or negatives in their investigations. Social engineering and targeted operations require careful planning and coordination to avoid compromising the investigation's integrity or violating the rights of innocent users. Depending on the importance of the case and the involvement of DApps with anonymous communication, investigators may attempt to exploit human vulnerabilities to gather information about suspects or criminal activities. In this regard, social engineering

DOI: https://doi.org/10.52756/ijerr.2023.v32.017

Exchange	Description
CoinDCX	CoinDCX reserve the right to freeze an account for fraud prevention while identity checks are completed or if compelled to by law enforcement. In order to comply with Indian regulations, CoinDCX requires some personal information to verify your account.
Coinswitch Kuber	CoinSwitch Kuber has frozen accounts in the past due to unclear government regulations earlier in 2022. CoinSwitch Kuber complies with regulations that make KYC mandatory in India.
ZebPay	ZebPay was launched in 2014 and relaunched in India in 2020. ZebPay reserves the right to freeze accounts if compelled to by law or governments, but it is unlikely.
Paxful	In Paxful all personal accounts have 2FA and OTP. Paxful is a global exchange, they have to comply with various regulators. Reserves the right to freeze accounts
Binance India	Binance security protocols include 2FA, secure offline cold storage for most assets, and real-time monitoring. They require a photo ID and personal information to verify your account.
Unocoin	Unocoin features like 2FA, and a paper wallet. Unocoin is compliant with Indian regulations, so would require some personal information.

Figure 3. Cryptocurrency Exchanges – terms & conditions

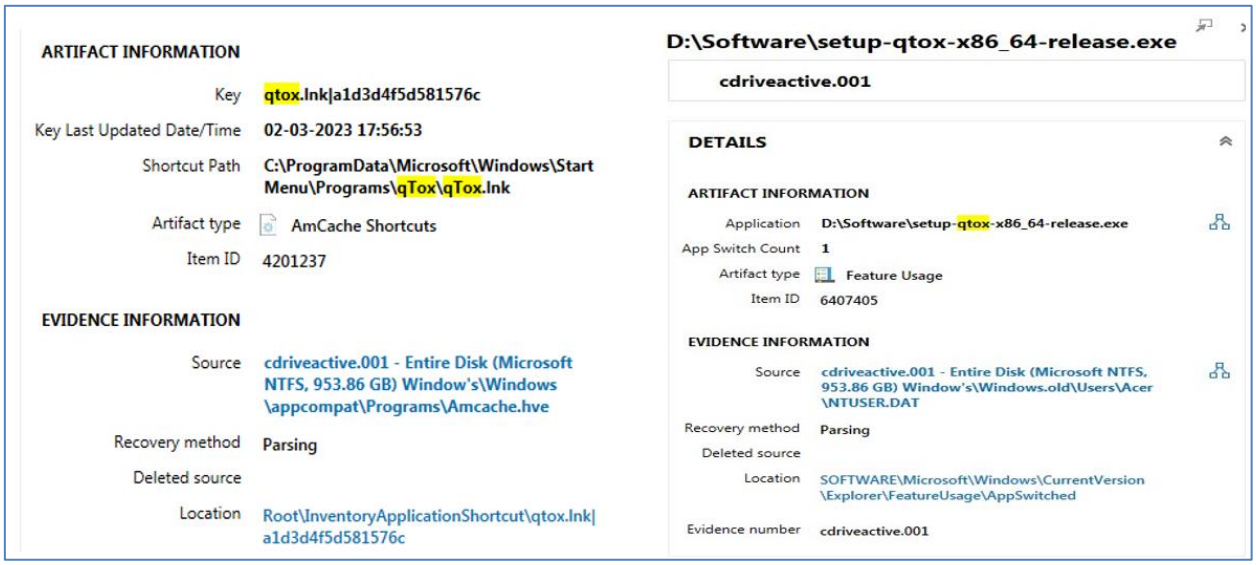

Figure 4. Example of host based digital evidences in qtox

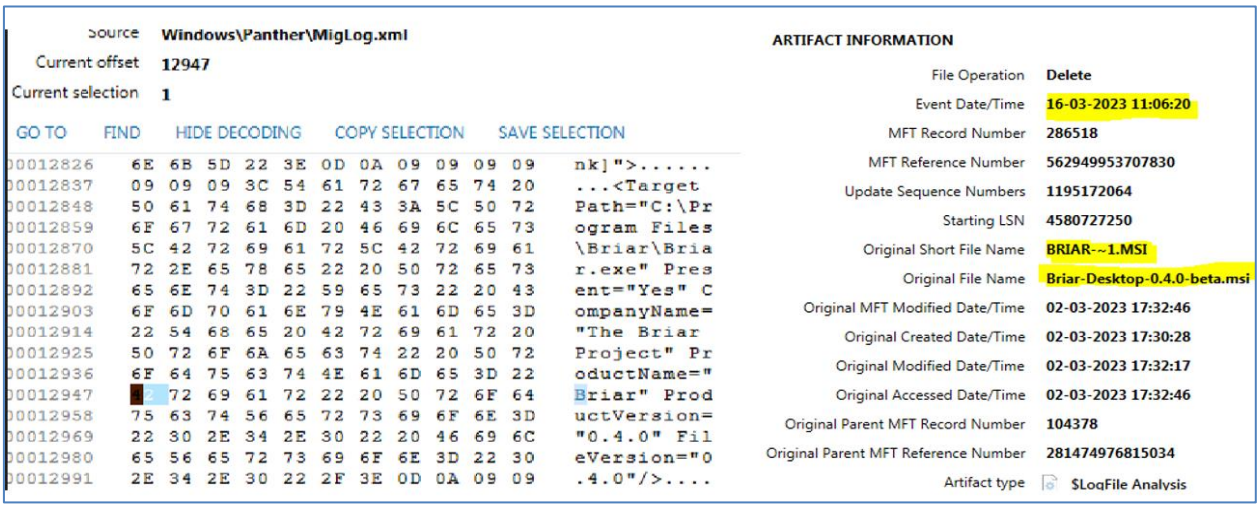

Figure 5. Example of host based digital evidences in briar

DOI: https://doi.org/10.52756/ijerr.2023.v32.017

techniques may assist the investigator in manipulating individuals to reveal sensitive information or perform actions that could compromise their security and finally retrieve valuable information.

Further, Investigators may use deceptive communication to extract information or entice criminals into revealing their identities or intentions. Furthermore, law enforcement officers or agents may pose as ordinary users and get involved within DApps to gain access to private groups or criminal networks. Agents may join private DApps groups or messaging channels to monitor communications, gather evidence, and identify key figures involved in criminal activities. Agents may engage in targeted communications to provoke criminal actors into revealing their intentions or committing illegal actions, leading to their eventual arrest. By employing these OSINT techniques, investigators can gain valuable intelligence about DApps, their users, and their activities, facilitating better understanding and potential investigative efforts within the decentralized ecosystem.

Digital Devices involved and retrievable digital evidence

In cybercrime investigations involving DApps, digital evidence is crucial in identifying and prosecuting perpetrators. The nature of the DApps and available features determine the types of digital evidence that investigators can analyze. If the DApps operate on a blockchain, all transactions are recorded transparently and immutably. Analyzing blockchain transactions associated with the crime can help investigators understand the flow of funds and identify the involved parties. Collecting and presenting such transactions as evidence can be vital in building a case. These transactions are linked to digital wallet addresses, and investigating the ownership and usage of these addresses can provide insights into the identities and activities of the individuals connected to the cybercrime (Di Stefano, 2022). Furthermore, reaching out to cryptocurrency exchanges might yield additional information, as these platforms may collect specific user data during registration as per their terms and conditions (Brasse & Hyun, 2023).

In case multiple applications are installed on a single device, while DApps themselves may not store IP addresses, other associated services or platforms used alongside DApps may log IP addresses. These logs can be valuable in identifying the users' geographic location involved in the cybercrime. Some DApps use decentralised data storage services (Zheng et al., 2023). Examining these services can uncover essential evidence related to the case.

Digital devices and related evidence

In rare instances, if there is a specific suspect, examining their digital devices for various activities such as browsing history, files, or communications may reveal further evidence to confirm suspicions (Santamaria et al., 2023). Therefore, investigators can gather the necessary evidence to bring cybercriminals to justice by carefully analyzing blockchain transactions, IP logs, decentralized storage services, and digital devices. We use to and briar applications for the analysis of digital evidence and found that various types of host-based digital evidence are available in the digital device, even after deletion of such apps, if the investigator can retrieve the device during investigation for retrieval of digital pieces of evidence (Abbing et al., 2023; Ermoshina et al., 2016).

Technological countermeasures:

The delicate balance between privacy and security must be kept in mind while adopting these countermeasures to avoid invasive user surveillance and protect user privacy rights. Furthermore, new difficulties and solutions will arise in anonymity and criminality detection in decentralized apps as technology advances.

Recommendation for LEAs and DApps develops or DApps experts

Balancing investigative needs with user privacy and digital rights is a delicate ethical challenge. Investigators must navigate the fine line between upholding the law and respecting individual privacy in the context of DApps. However, in case of illicit activities by any users, it is equally essential for the investigator to trace the perpetrator and give justice to the victim. In addition, addressing challenges due to Anonymous communication in the fast-paced nature of decentralized systems requires technical expertise, collaboration among international agencies, and an updated legal framework. Secondly, jurisdictions often have distinct data privacy laws and regulations, and the enforcement of these laws can conflict when dealing with cross-border data flow on DApps. The legal treatment of DApps and cryptocurrencies can differ significantly from one jurisdiction to another. Some countries have embraced blockchain technology and cryptocurrencies, while others have imposed strict regulations or outright bans. In cases involving cross-border criminal activities or fraud on DApps, investigating authorities must seek extraterritorial jurisdiction to pursue suspects or enforce legal actions outside their jurisdiction. Additionally, as an investigator in the technical domain, every investigator should have

DOI: https://doi.org/10.52756/ijerr.2023.v32.017

adequate knowledge of the usage of technical facilities, tools and techniques, including various professional Linux distro, etc., which may help them proceed and collect information about such DApps and illicit activities in that DApps. Advancements in digital forensics and cooperation between international law enforcement agencies are vital for investigating crimes effectively in this decentralized and borderless landscape.

Conclusion

In conclusion, decentralized anonymous communication systems present both challenges and legitimate uses. It is clear that while they may be exploited for criminal purposes, they also play a crucial role in protecting privacy, enabling free expression, and facilitating secure communication. Addressing cybercrime in DApps requires a multifaceted approach that balances preserving privacy rights with the necessity for effective law enforcement. Even though DApps offer advantages to illicit users engaging in illegal activities, it has been demonstrated that investigators can retrieve valuable information through targeted investigation techniques. For future work, we should focus on conducting more detailed digital forensics analyses of digital devices involved in DApps activities and examining network packets or artifacts. By continuing to explore and adapt investigative methodologies, law enforcement agencies can better respond to the challenges posed by decentralized anonymous communication systems while upholding the principles of justice, privacy, and security.

Conflict of Interest:

The authors have attested to the complete absence of any acknowledged conflict of interest in the present scholarly manuscript.

References

Abbing, R. R., Diehm, C., & Warreth, S. (2023). Decentralised social media. *Internet Policy Review*, *12*(1). https://doi.org/10.14763/2023.1.1681

Abdulaziz, M., Çulha, D., & Yazici, A. (2018). A decentralized application for secure messaging in a trustless environment. *2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT)*, 1–5. https://doi.org/10.1109/IBIGDELFT.2018.8625362

Alabdulwahhab, F. A. (2018). Web 3.0: the decentralized web blockchain networks and protocol innovation. *2018 1st International Conference on Computer Applications & Information Security (ICCAIS)*, 1–4. https://doi.org/10.1109/CAIS.2018.8441990

Azad, I. (2022). An introduction to cryptocurrency investigations. In *Privacy, Security And Forensics in The Internet of Things (IoT)* (pp. 97–129). Springer. https://doi.org/10.1007/978-3-030-91218-5_5

Brasse, A., & Hyun, S. (2023). Cryptocurrency Exchanges and the Future of Cryptoassets. In *The Emerald Handbook on Cryptoassets: Investment Opportunities and Challenges* (pp. 341–353). Emerald Publishing Limited. https://doi.org/10.1108/978-1-80455-320-620221022

Cai, W., Wang, Z., Ernst, J. B., Hong, Z., Feng, C., & Leung, V. C. M. (2018). Decentralized applications: The blockchain-empowered software system. *IEEE Access*, *6*, 53019–53033. https://doi.org/10.1109/ACCESS.2018.2870644

Caviglione, L., Wendzel, S., & Mazurczyk, W. (2017). The future of digital forensics: Challenges and the road ahead. *IEEE Security & Privacy*, *15*(6), 12–17. https://doi.org/10.1109/MSP.2017.4251117

Chang, L. Y. C. (2017). Cybercrime and cyber security in ASEAN. *Comparative Criminology in Asia*, 135–148. https://doi.org/10.1007/978-3-319-54942-2_10

Chougule, H., Dhadiwal, S., Lokhande, M., Naikade, R., & Patil, R. (2022). Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption and Blockchain. *Procedia Computer Science*, *215*, 71–77. https://doi.org/10.1016/j.procs.2022.12.008

Di Stefano, F. (2022). *Money laundering in the decentralized era: how blockchain technology enables illicit activities*.

Dyson, S., Buchanan, W. J., & Bell, L. (2019). The challenges of investigating cryptocurrencies and blockchain related crime. *ArXiv Preprint ArXiv:1907.12221*.

Ermoshina, K., Musiani, F., & Halpin, H. (2016). End-to-end encrypted messaging protocols: An overview. *Internet Science: Third International Conference, INSCI 2016, Florence, Italy, September 12-14, 2016, Proceedings 3*, 244–254. https://doi.org/10.1007/978-3-319-45982-0_22

Goohs Jr, J. A. (2021). Reasonable Expectation of Privacy in an IP Address: The Tor Browser and

Other Anonymization Measures. *Colum. Undergraduate L. Rev.*, *18*, 127.

Granja, F. M., & Rafael, G. D. R. (2017). The preservation of digital evidence and its admissibility in the court. *International Journal of Electronic Security and Digital Forensics*, *9*(1), 1–18. https://doi.org/10.1504/IJESDF.2017.081749

Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law & Security Review*, *27*(1), 61–67. https://doi.org/10.1016/j.clsr.2010.11.001

Hwang, Y.-W., Lee, I.-Y., Kim, H., Lee, H., Kim, D., & others. (2022). Current status and security trend of osint. *Wireless Communications and Mobile Computing*, *2022*. https://doi.org/10.1155/2022/1290129

Jeffries, S., & Apeh, E. (2020). Standard operating procedures for cybercrime investigations: a systematic literature review. *Emerging Cyber Threats and Cognitive Vulnerabilities*, 145–162. https://doi.org/10.1016/B978-0-12-816203-3.00007-1

Jordan, A. (2020). *Cybercrime prevention principles for internet service providers*.

Kesari, A., Hoofnagle, C., & McCoy, D. (2017). Deterring cybercrime: Focus on intermediaries. *Berkeley Tech. LJ*, *32*, 1093.

Nurmi, J., & Niemelä, M. S. (2017). Tor de-anonymisation techniques. *Network and System Security: 11th International Conference, NSS 2017, Helsinki, Finland, August 21-23, 2017, Proceedings 11*, 657–671. https://doi.org/10.1007/978-3-319-64701-2_52

Patil, A., Banerjee, S., Jadhav, D., & Borkar, G. (2022). Roadmap of digital forensics investigation process with discovery of tools. *Cyber Security and Digital Forensics*, 241–269. https://doi.org/10.1002/9781119795667.ch11

Petcu, A., Pahontu, B., Frunzete, M., & Stoichescu, D. A. (2023). A Secure and Decentralized Authentication Mechanism Based on Web 3.0 and Ethereum Blockchain Technology. *Applied Sciences*, *13*(4), 2231. https://doi.org/10.3390/app13042231

Pop, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2020). Blockchain based decentralized applications: Technology review and development guidelines. *ArXiv Preprint ArXiv:2003.07131*.

Rahmadika, S., Firdaus, M., Lee, Y.H., & Rhee, K.H. (2021). An Investigation of Pseudonymization Techniques in Decentralized Transactions. *J. Internet Serv. Inf. Secur.*, *11*(4), 1–18.

Raj, K. (2019). *Foundations of blockchain: the pathway to cryptocurrencies and decentralized blockchain applications*. Packt Publishing Ltd.

Ranakoti, P., Yadav, S., Apurva, A., Tomer, S., & Roy, N. R. (2017). Deep web \& online anonymity. *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, 215–219. https://doi.org/10.1109/IC3TSN.2017.8284479

Redford, M. (2011). US and EU Legislation on Cybercrime. *2011 European Intelligence and Security Informatics Conference*, 34–37. https://doi.org/10.1109/EISIC.2011.38

Reedy, P. (2020). Interpol review of digital evidence 2016-2019. *Forensic Science International: Synergy*, *2*, 489–520. https://doi.org/10.1016/j.fsisyn.2020.01.015

Santamaria, P., Tobarra, L., Pastor-Vargas, R., & Robles-Gómez, A. (2023). Smart Contracts for Managing the Chain-of-Custody of Digital Evidence: A Practical Case of Study. *Smart Cities*, *6*(2), 709–727. https://doi.org/10.3390/smartcities6020034

Schwerha, J. J. (2004). Cybercrime: legal standards governing the collection of digital evidence. *Information Systems Frontiers*, *6*, 133–151. https://doi.org/10.1023/B:ISFI.0000025782.13582.87

Shah, A., & Chudasama, D. (2021). Investigating Various Approaches and Ways to Detect Cybercrime. *Journal of Network Security*, *9*(2), 12–20.

Shen, M., Zhang, J., Zhu, L., Xu, K., & Du, X. (2021). Accurate decentralized application identification via encrypted traffic analysis using graph neural networks. *IEEE Transactions on Information Forensics and Security*, *16*, 2367–2380. https://doi.org/10.1109/TIFS.2021.3050608

Sorbán, K. (2019). The role of Internet intermediaries in combatting cybercrime: Organisation and liabilities. *Central and Eastern European EDem and EGov Days*, 19–31. https://doi.org/10.24989/ocg.v335.1

Wang, S.Y. K., Hsieh, M.L., Chang, C. K.M., Jiang, P.S., & Dallier, D. J. (2021). Collaboration between law enforcement agencies in combating

cybercrime: Implications of a Taiwanese case study about ATM hacking. *International Journal of Offender Therapy and Comparative Criminology*, *65*(4), 390–408. https://doi.org/10.1177/0306624X20952391

Wu, K., Ma, Y., Huang, G., & Liu, X. (2021). A first look at blockchain-based decentralized applications. *Software: Practice and Experience*, *51*(10), 2033–2050. https://doi.org/10.1002/spe.2751

Yeboah-Ofori, A., & Brown, A. D. (2020). Digital forensics investigation jurisprudence: issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences*, *6*(1), 1–8. https://doi.org/10.24966/FLIS-733X/100045

Yue, K., Zhang, Y., Chen, Y., Li, Y., Zhao, L., Rong, C., & Chen, L. (2021). A survey of decentralizing applications via blockchain: The 5G and beyond perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2191–2217. https://doi.org/10.1109/COMST.2021.3115797

Zheng, P., Jiang, Z., Wu, J., & Zheng, Z. (2023). Blockchain-based Decentralized Application: A Survey. *IEEE Open Journal of the Computer Society*. https://doi.org/10.1109/OJCS.2023.3251854

How to cite this Article:

Arjun Chetry and Uzzal Sharma (2023). Anonymity in decentralized apps: Study of implications for cybercrime investigations. *International Journal of Experimental Research and Review*, *32*, 195-205.

DOI : https://doi.org/10.52756/ ijerr.2023.v32.017