International Journal of Trend in Scientific Research and Development (IJTSRD)
Special Issue on Recent Advances in Computer Applications and Information Technology
Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Digital Forensics: Computer Crime Investigation

Tushar Ramdham, Shivam Meshram

G H Raisoni University, Amravati, Maharashtra, India

Abstract

As a crucial topic within the realm of cybersecurity, digital forensics is essential to the investigation and prevention of crimes using computers. As digital technologies, internet usage, cloud computing, and smart devices continue to rise exponentially, cybercrimes like ransomware attacks, identity theft, financial fraud, hacking, data breaches, and cyberterrorism have become much more commonplace globally. The necessity for methodical digital investigation procedures has never been greater, as criminals increasingly rely on digital platforms to carry out and hide their operations. A systematic framework for locating, preserving, gathering, analysing, and presenting digital evidence in a way that is acceptable in court is offered by digital forensics[1]. This study examines the basic ideas of digital forensics, concentrating on computer crime investigation and methods for recovering erased data. The retrieval of erased or concealed data is among the most crucial components of digital forensic inquiry. In contrast to popular assumption, deleted files are not instantaneously removed from storage devices; rather, the operating system just identifies the storage space as usable again and eliminates file references. Using specific forensic methods, such data can be recovered until it is overwritten. Forensic disc imaging, file carving, metadata reconstruction, hash verification, and timeline analysis are some of the data recovery techniques covered in this study. The study also looks at the organised digital forensic investigation procedure, which uses cryptographic hashing algorithms like MD5 and SHA-256 to guarantee integrity and authenticity[2] The study also examines popular forensic tools including EnCase, FTK, Autopsy, Wireshark, and Volatility that help investigators retrieve, examine, and interpret digital evidence from memory systems, networks, and computers. Additionally, the study draws attention to contemporary difficulties in digital forensic investigations, such as disputes over jurisdiction, cloud-based systems, and encryption. The results highlight the importance of digital forensics in preventing cybercrimes and bolstering cybersecurity regimes. The incorporation of automation, artificial intelligence, and advanced analytics into forensic investigations will further improve accuracy, efficiency, and dependability as technology develops. The significance of contemporary digital forensic procedures in preserving cyber resilience, legal compliance, and digital trust in the linked world of today is highlighted by this study, which advances our understanding of them.[3].

KEYWORDS: *Forensic imaging, file carving, hash algorithms, network forensics, memory forensics, cyber security, evidence preservation, incident response, forensic tools, digital forensics, computer crime investigation, cybercrime, deleted data recovery, digital evidence, and data integrity.*

1. Introduction

Digital technologies' quick development has changed how people, companies, and governments function. Cloud platforms, smartphones, computers, and internet-based communication systems have all become indispensable parts of modern life. But this digital revolution has also resulted in a sharp rise in computer-related offences and cybercrimes. Criminals use technology flaws to carry out ransomware attacks, identity theft, data theft, financial fraud, hacking, and cyberstalking. For crimes involving digital systems, conventional investigative techniques are therefore insufficient. Digital forensics has emerged as a specialised area of forensic science as a result of this. The process of locating, protecting, gathering, evaluating, and presenting digital evidence in a way that complies with the law is known as digital forensics. It guarantees that electronic evidence is treated with care so that its integrity is preserved and it can be used in court. Digital evidence is much more easily changed, erased, or distorted than physical evidence. Thus, in order to guarantee authenticity and dependability, investigators need to adhere to established protocols.[4] Over the past 20 years, the area of digital forensics has seen substantial change. At first, research mostly concentrated on stand-alone computer systems. The scope has now broadened to encompass cloud settings, Internet of Things (IoT) devices, mobile devices, and extensive network infrastructures. Expertise in a variety of fields, such as operating systems, file systems, cryptography, networking, and virus analysis, is necessary for contemporary cybercrime investigations.

The retrieval of erased or concealed data is among the most important components of digital forensic inquiry. A common tactic used by cybercriminals to delete evidence is to erase files or format storage devices. The real data is still present on the storage medium even after a file is deleted. Rather, the system indicates that the file location is open for new data. Specialised forensic procedures may typically recover data until it is erased. This feature serves as the cornerstone for recovering erased data in digital investigations. A methodical procedure is used in digital forensic investigations to guarantee the validity of the evidence. Potential evidence is identified, preserved via forensic imaging, examined with specialised equipment, recovered data is analysed, and a comprehensive report is prepared as part of the standard investigative procedure.[5] Commonly used hash algorithms like MD5 and SHA-256 are used to confirm that the evidence hasn't been tampered with during analysis. These cryptographic methods ensure the authenticity of data by creating distinct digital fingerprints of it. New difficulties for investigators have emerged in recent years due to the growing usage of cloud storage platforms and encryption technology. Criminals hide their actions using anti-forensic methods, anonymisation tools, and encrypted drives. Additionally, because of jurisdictional and data ownership concerns, cloud computing platforms make

investigations more difficult. With the incorporation of automation, artificial intelligence, and advanced analytics to enhance investigative effectiveness, digital forensics is still developing in spite of these obstacles. Beyond criminal investigations, digital forensics is critical to incident response and enterprise security. Businesses utilise forensic analysis to investigate data breaches, find internal dangers, and stay in compliance with regulations. Governments use digital forensic methods to combat cyberterrorism and protect national security systems. As cyber threats continue to grow more complex, the need of digital forensic science in maintaining cyber resilience is increasing. [6] This research paper aims to explore the fundamental concepts of digital forensics with an emphasis on computer crime investigation and techniques for data recovery. Also discussed are frequently used forensic tools, methods, challenges, and future developments in the discipline. Understanding these elements is crucial for developing cybersecurity frameworks and ensuring justice in the digital age.

Modern civilisation has undergone tremendous change as a result of the massive adoption of digital gadgets and the quick development of information technology. But along with the advancement of technology, there has been a sharp rise in cybercrime, including ransomware attacks, identity theft, financial fraud, hacking, data breaches, and digital espionage. There is a greater need than ever for trustworthy digital forensic investigation techniques since people, businesses, and governments depend more and more on digital systems for financial transactions, communication, and storage. A subfield of forensic science called "digital forensics" is dedicated to identifying, obtaining, preserving, analysing, presenting, and examining digital evidence. Digital forensics, as opposed to traditional forensic techniques, works with intangible data that is kept on electronic devices including servers, cellphones, computers, cloud platforms, and network infrastructures. Keeping digital evidence reliable and authentic is one of the biggest problems in digital investigations. Modification, deletion, encryption, and remote destruction of digital data are all simple processes. Therefore, in order to avoid contaminating or changing evidence, investigators must adhere to established protocols and use instruments that have been approved by science. Methods like cryptographic hash verification and forensic photography are crucial for guaranteeing that the evidence gathered stays consistent over the course of the inquiry. Furthermore, network forensics, mobile device forensics, cloud forensics, and Internet of Things (IoT) investigations are now included in the scope of digital forensics due to the growing complexity of cybercrime. Investigations become increasingly difficult due to the fact that modern cyberattacks sometimes involve encrypted storage systems, multiple devices, and cross-border contact. The structured digital forensic investigation procedure, which includes evidence gathering, forensic imaging, hash verification, recovered deleted data, and forensic analysis, is the main topic of this research article. In addition to examining current issues and research gaps in the sector, the study seeks to emphasise the significance of standardised procedures in computer cybercrime investigations. Digital forensics, as opposed to traditional forensic techniques, works with intangible data that is kept on electronic devices including servers, cellphones, computers, cloud platforms, and network infrastructures. Keeping digital evidence reliable and authentic is one of the biggest problems in digital investigations. Modification, deletion, encryption, and remote destruction of digital data are all simple processes.

Fig.1 - Digital Forensic Investigation Process Diagram

2. Literature Review

Due to the increased sophistication and prevalence of cybercrimes over the past 20 years, digital forensics has undergone tremendous change. The primary focus of early digital forensics research was on computer hard disc investigations and fundamental file recovery methods. But as technology advances so quickly, the scope of forensic inquiry has broadened to encompass network systems, mobile devices, cloud computing environments, and Internet of Things (IoT) devices. To guarantee the admissibility of digital evidence in court cases and standardise the digital investigation process, researchers have created a number of models, frameworks, and procedures. The creation of models for the structured investigation process was one of the core contributions to digital forensic research. According to studies, digital evidence needs to be treated with caution to avoid contamination or manipulation. Research organisations and forensic specialists have developed standard models that emphasise phases including identification, preservation, collecting, examination, analysis, and reporting. These methodical techniques guarantee investigations are reliable, consistent, and compliant with the law.[7] Extensive research has also been conducted on methods for recovering deleted data. Research shows that the operating system usually does not erase the data when a file is deleted; instead, it just removes the file reference from the file allocation table. This enables the use of specialised methods like file carving and metadata reconstruction by forensic specialists to recover deleted files. NTFS, FAT, and EXT are just a few of the file systems that researchers have studied to learn about the differences in deletion and data recovery methods

between platforms. Data integrity verification and forensic imaging are another significant field of literature. The significance of constructing a bit-by-bit forensic image of storage media prior to examination is emphasised by researchers. This guarantees that the original evidence won't be altered. The literature extensively discusses hashing algorithms like MD5 and SHA-256 as crucial instruments for preserving the chain of custody and confirming the authenticity of data. The development of network forensics is another result of the rise in internet usage. In order to identify virus communication, illegal access, and cyberattacks, research in this field focuses on recording and examining network traffic. Firewall records, packet captures, and network logs are all essential pieces of evidence in cybercrime investigations. According to research, intrusion detection systems and real-time monitoring are crucial for assisting with forensic investigations.[8] Because smartphones are used by so many people, mobile forensics has become a significant topic of study. Messages, applications, call records, and geolocation data can all be extracted from mobile devices using methods that researchers outline. Issues like encryption, cloud synchronisation, and device lockout systems make investigations more difficult and need for sophisticated forensic techniques. A fast expanding topic that has been extensively covered in recent research is cloud forensics. In cloud contexts, distributed storage, multi-tenancy, and jurisdictional concerns make traditional forensic techniques difficult to use. Cloud service providers can be included in collaborative frameworks proposed by researchers to support efficient investigations while preserving user privacy and legal compliance. The literature emphasises ethical and legal issues in addition to technological ones in digital forensic investigations. Academics stress the significance of upholding national cyber laws, guaranteeing the integrity of the evidence, and preserving the chain of custody. Digital evidence that is handled improperly could be excluded from use in court. As a result, legal compliance is regarded as being just as significant as technological proficiency. Artificial intelligence and machine learning integration in digital forensics are the main topics of recent research developments. AI expedites investigation times and increases efficiency in automated evidence processing, anomaly identification, and malware categorisation. In the future, researchers predict that AI-driven forensic tools will be crucial in managing complex cybercrime cases.[9]

Important Results from Earlier Research and Identification of Research Gaps:

Prior studies in the field of digital forensics have repeatedly shown how important it is to adhere to a documented, standardised, and legally compliant investigative process to guarantee that digital evidence is still acceptable in court. Researchers and forensic experts concur that the reliability of digital evidence may be called into question during judicial proceedings in the absence of a systematic methodology that addresses identification, acquisition, preservation, examination, analysis, and reporting. In addition to guaranteeing uniformity in investigations, standardisation safeguards the validity and integrity of the data gathered. One important result from earlier research is that because of the way file systems behave by nature, erased data can frequently be recovered. Usually, the operating system does not permanently erase the underlying data when a user deletes a file; instead, it just removes the reference to the file.[10] Additionally, studies have shown how important forensic imaging is for maintaining original digital evidence. Analysing the original storage media directly runs the risk of changing metadata, timestamps, or system structures. In order to do all of the examinations, investigators make a forensic image of the storage device bit by bit. This guarantees that the original evidence is unaltered and ready for use in court if necessary. The application of cryptographic hash algorithms, such as MD5 and SHA variations, is closely associated with this procedure. Investigators can confirm that the forensic image is a precise replica of the original source by using hash functions, which create distinct digital fingerprints of data. The integrity of the evidence is preserved throughout the course of the inquiry when matching hash values verify that no manipulation or change has taken place. Furthermore, prior research highlights the increasing significance of network forensics in detecting cyber breaches and tracking down malevolent activity. Investigators must examine network logs, packet captures, and traffic patterns in order to identify malware spread, data exfiltration, and unauthorised access due to the growing frequency of cyberattacks. In order to prosecute hackers, network forensic techniques are essential for reconstructing attack timelines and assigning actions to particular sources.

According to studies, the complexity of contemporary smartphones, encryption systems, and application-based data storage structures necessitate the use of specialised extraction and analysis techniques in mobile device forensics. Not with standing these developments, the literature points out a number of important research gaps that still need to be filled. The lack of internationally recognised forensic standards is one of the main causes for concern.[11] Over the past 20 years, the area of digital forensics has seen tremendous change, with scholars putting out a number of models and frameworks to standardise investigative techniques. By emphasising steps like identification, preservation, collecting, examination, analysis, and reporting, early forensic models highlighted the value of methodical evidence processing. These fundamental models offered an organised method that enhanced digital investigations' dependability and consistency. The significance of forensic imaging as a fundamental element of digital evidence preservation has been emphasised by numerous studies. According to researchers, forensic photography is an essential component of contemporary investigations since direct inspection of the original storage medium may result in inadvertent data alteration. An precise replica of the original storage device, including both active and deleted files, is produced thanks to bit-by-bit imaging techniques. Cryptographic hash functions, which are used to confirm the integrity of data, are another important area of study. MD5 and SHA are two examples of hash algorithms that produce distinct digital fingerprints of data. The hash value that is produced is completely changed if even a single bit of data is changed. Hash verification is now a commonly used technique to ensure that forensic photos don't change from their original sources. Hash verification, according to academics, increases the legitimacy of digital evidence in court. Mechanisms for recovering erased data have also been the subject of much research.

3. Research Methodology

The research's technique is founded on a systematic framework for digital forensic investigations, which is intended to guarantee safe evidence management, the recovery of erased data, and legal admissibility in situations involving computer criminality. The investigation procedure integrates forensic photography, hash verification, and analytical reconstruction techniques in a controlled and methodical manner because digital evidence is extremely sensitive and easily manipulated.

Three fundamental elements are emphasised by the methodology: digital proof traceability, authenticity, and integrity. All phases of the inquiry are recorded to preserve the chain of custody and avoid data contamination. A forensic image is made and validated prior to analysis, rather than the original storage media being examined directly. This guarantees that over the course of the investigation, the original evidence will not be altered. Investigation Workflow for Systems: The adopted methodology's general process is organised as follows: Identification of evidence, preservation of evidence, forensic acquisition, forensic imaging, hash verification, examination, and recovery of deleted data, event reconstruction and analysis, reporting, and secure archiving While preserving data integrity, this workflow guarantees a linear progression from gathering evidence to final reporting. Identification and Preservation of Evidence:[12] Finding possible sources of digital evidence, such as PCs, servers, network logs, USB drives, and external storage devices, is the first step in the inquiry. Particular focus is placed on volatile memory (RAM), which may hold important data like encryption keys and active programs. Evidence is kept through controlled procedures after it has been identified. To stop remote tampering, devices are separated from networks. The purpose of hardware write blockers is to stop unintentional data alteration. To guarantee accountability, appropriate documentation and chain of possession records are kept. Important preservation strategies include of: The initial handling of a suspect device is a crucial step in digital forensic investigations that has a direct bearing on the admissibility and integrity of the evidence. To stop remote access, manipulation, or data alteration, the suspect device must first be isolated. Since network-connected devices may receive remote wiping instructions, automated updates, or external directives, it is crucial to isolate them right away by cutting network cables, turning off Wi-Fi, or putting mobile devices in Faraday bags in order to protect both volatile and non-volatile data. Write-blocking techniques are used after isolation to guarantee that no data is altered while being examined. Read-only access to storage medium is made possible by write-blocking hardware or software. This stops metadata, timestamps, and file system structures from being inadvertently changed by the operating system or forensic tools[14]

Imaging and Forensic Acquisition:

Data capture is carried out following preservation. Static acquisition (after shutdown) or live acquisition (if the system is operating) can be used for this. Static acquisition is usually recommended in order to prevent evidence from being altered. After that, a forensic image is produced. An precise bit-by-bit replica of the storage device, complete with active and deleted data, slack space, and unallocated space, is called a forensic image. The original device is kept unaltered while the forensic image serves as the working copy for examination. Process for Hash Verification : Hash verification is an essential part of the process. Following forensic imaging, a digital fingerprint of the original storage device and the forensic image is produced using cryptographic hash techniques like MD5 or SHA-256.It verifies that if the two hash values are the same: The forensic picture is a perfect replica. There was no data modification during imaging. The integrity of the evidence is preserved. It is appropriate for use in court. A slight change in the data will yield an entirely different hash value. Hash verification, thus, offers mathematical evidence of validity and enhances the investigation's legitimacy. The forensic report contains the hash values, which are saved for later confirmation. Review and Recovery of Deleted Information: The forensic photograph is examined and analysed by investigators after integrity has been verified. Finding pertinent artefacts and retrieving erased or buried data are the main goals of this phase. Although the file system no longer contains the file's reference after a file is destroyed, the data itself stays in unallocated space until it is replace. Deleted files can frequently be retrieved using file carving and metadata reconstruction techniques. Among the steps in the examination procedure are: Conducting keyword research, Analysis of log files, Analysis of a browser's history, The detection of malware artefacts In order to ascertain how the cybercrime [16]A structured framework for digital forensic inquiry is used in this study to guarantee the reliability, integrity, and admissibility of the evidence. Each of the methodology's several successive stages is in line with accepted forensic standards. The identification and isolation of questionable digital devices is the first step in the examination. To avoid remote manipulation or data loss, devices are unplugged from networks. Faraday shielding techniques can be used to prevent wireless signals in mobile devices.

In order to guarantee the dependability, integrity, and admissibility of digital evidence in cybercrime investigations, this study uses a methodical and structured framework for digital forensic analysis. To reduce contamination, data manipulation, and procedural errors during the investigative process, the technique is based on accepted forensic concepts, standardised rules, and scientifically proven methods. With an emphasis on theoretical analysis and the real-world implementation of digital forensic techniques, the study employs a qualitative and procedural research methodology. Identification, preservation, acquisition, verification, examination, analysis, and reporting are among the fundamental forensic steps that are integrated into the framework. To preserve the integrity of the evidence and guarantee legal compliance, each step is carried out in a sequential manner. Appropriate planning and scope determination precede the investigation. At this point, investigators establish legal authorisation, such as warrants or organisational approval, discover possible sources of digital evidence, and ascertain the nature of the suspected cybercrime. A precise specification of the investigation's goals guarantees procedural concentration and helps avoid needless data handling. Additionally, choosing the right forensic tools, confirming the dependability of the program, and guaranteeing laboratory preparedness are all part of preparation. To ensure that forensic software generates reliable and consistent results, tool validation is crucial. This phase enhances the investigation's scientific legitimacy. Potential sources of evidence are found after the investigation's scope has been established. Computers, hard drives, mobile devices, USB storage media, cloud accounts, network logs, and Internet of Things devices are a few examples of these. One of the most important theoretical concepts in digital forensics is preservation.

Fig.2 - Hash Verification Process in Digital Forensic Imaging

4. Result

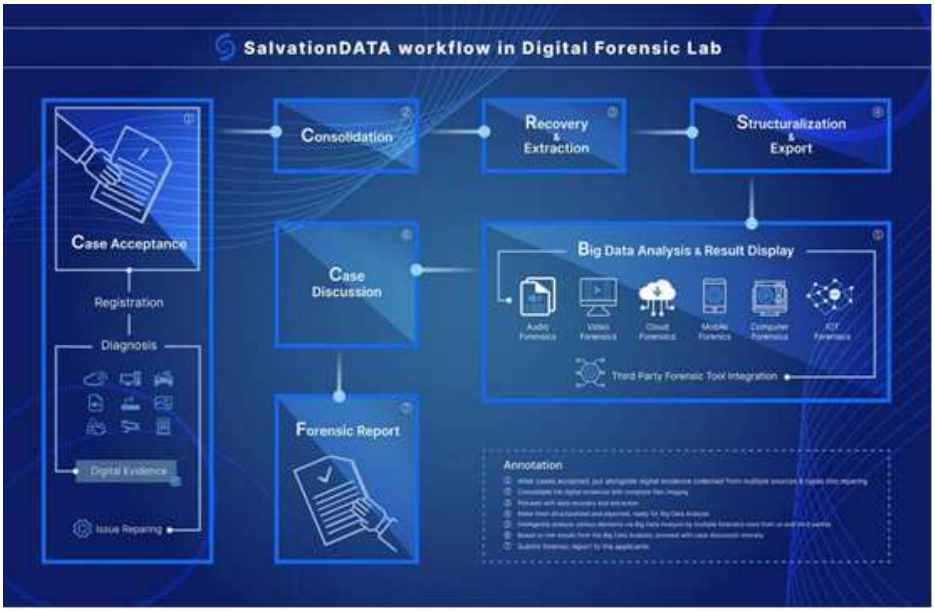

Fig.3 - Digital Forensic Investigation Result Workflow

5. Conclusion

Due to its ability to facilitate the methodical identification, preservation, analysis, and presentation of digital evidence, digital forensics is essential to contemporary computer crime investigations. Due to the exponential rise in cybercrime, conventional methods of inquiry are no longer adequate to manage intricate digital settings. According to this study, forensic imaging, hash verification, and recovered data are essential elements of a trustworthy investigation process.[17] Digital evidence's validity and integrity are preserved throughout the course of the inquiry thanks to the hash verification technique. Digital traces are still available even after deliberate deletion attempts, as evidenced by the ability to retrieve erased data from unallocated storage space. The possibility of a successful prosecution is increased and the investigation process is considerably strengthened by these capabilities Digital forensics has become a cornerstone of modern cybercrime investigations due to its structured and scientifically grounded approach to handling digital evidence. In an era where cybercrime is growing at an exponential rate—ranging from data breaches and identity theft to ransomware attacks and financial fraud—traditional investigative techniques alone are no longer sufficient to address the complexity of digital environments. The rapid advancement of technology, widespread internet usage, and the increasing reliance on digital devices have created vast volumes of data that require specialized tools, methodologies, and expertise to examine effectively.[18]

This study highlights the critical role of key forensic procedures such as forensic imaging, hash verification, and data recovery in establishing a reliable and defensible investigative process. Forensic imaging ensures that an exact bit-by-bit copy of the original storage media is created, thereby preserving the integrity of the original evidence. This process allows investigators to conduct analysis on a duplicate while maintaining the untouched state of the original device, which is essential for legal admissibility. Hash verification further strengthens the credibility of digital evidence by ensuring data integrity throughout the investigative lifecycle. By generating unique hash values before and after analysis, investigators can demonstrate that the evidence has not been altered, either intentionally or accidentally. This cryptographic validation technique reinforces the chain of custody and enhances the trustworthiness of the findings presented in court.[19] Moreover, the ability to recover deleted or hidden data from unallocated storage space demonstrates the resilience of digital traces. Even when perpetrators attempt to erase incriminating information, remnants of data often remain accessible through specialized forensic tools and techniques. This capability significantly increases the likelihood of uncovering critical evidence that may otherwise appear lost, thereby strengthening the investigative process and supporting successful prosecution. In conclusion, digital forensics not only enhances the accuracy and efficiency of cybercrime investigations but also ensures that digital evidence meets legal standards of authenticity and reliability. As cyber threats continue to evolve, the importance of adopting advanced forensic methodologies, continuous technological innovation, and professional training cannot be overstated. The integration of robust forensic practices ultimately contributes to the delivery of justice, the deterrence of cybercriminal activities, and the protection of digital ecosystems worldwide.[20]

Reference

[1] W. Stallings, *"Cryptography and Network Security: Principles and Practice, 2017."* Pearson, 2017.

[2] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *"Bitcoin and Cryptocurrency Technologies, 2016."* Princeton University Press, 2016.

[3] W. Diffie and M. Hellman, *"New Directions in Cryptography, 1976."* IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[4] W. Diffie and M. Hellman, *"New Directions in Cryptography, 1976."* IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[5] W. Stallings, *"Cryptography and Network Security: Principles and Practice, 2017."* Pearson, 2017.

[6] S. Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System, 2008."* 2008.

[7] G. Wood, *"Ethereum: A Secure Decentralised Generalised Transaction Ledger, 2014."* Ethereum Project Yellow Paper, 2014.

[8] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *"Bitcoin and Cryptocurrency Technologies, 2016."* Princeton University Press, 2016.

[9] S. Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System, 2008."* 2008.

[10] D. Johnson, A. Menezes, and S. Vanstone, *"The Elliptic Curve Digital Signature Algorithm (ECDSA), 2001."* International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[11] W. Diffie and M. Hellman, *"New Directions in Cryptography, 1976."* IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[12] R. Rivest, A. Shamir, and L. Adleman, *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, 1978."* Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[13] D. Johnson, A. Menezes, and S. Vanstone, *"The Elliptic Curve Digital Signature Algorithm (ECDSA), 2001."* International Journal of Information Security, vol. 1, no. 1, pp. 36–63, 2001.

[14] S. Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System, 2008."* 2008.

[15] A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder, *"Bitcoin and Cryptocurrency Technologies, 2016."* Princeton University Press, 2016.