Chain of Custody bei Incident Response Prozessen

Hausarbeit

im Masterstudiengang
Digitale Forensik

vorgelegt von

Sayed Sayedy
Matr.-Nr.: 105433

am 18. März 2024
an der Hochschule Albstadt-Sigmaringen

Dozent:	Prof. Dr. Martin Rieger
Tutor:	David Schlichtenberger, M.Sc.

Eigenständigkeitserklärung

Ich versichere, dass ich diese Studienarbeit selbstständig verfasst und keine Hilfe Dritter eingeflossen ist.

Die Stellen der Studienarbeit, die dem Wortlaut oder dem Sinn nach anderen Werken entnommen wurden, sind in jedem Fall unter Angabe der Quelle kenntlich gemacht.

Die Arbeit ist noch nicht veröffentlicht oder in anderer Form als Prüfungsleistung vorgelegt worden.

Mir ist bekannt, dass ein Täuschungsversuch prüfungsrechtliche Konsequenzen bis zur Exmatrikulation haben kann.

Mir ist bekannt, dass meine Studienarbeit einer Plagiatsprüfung unterzogen werden kann; mit einer solchen Plagiatsprüfung und einer Speicherung meiner Prüfung in einem entsprechenden System erkläre ich mich einverstanden.

Ich versichere, dass ich die von mir verfassten Studienarbeits-Lösungen innerhalb der Prüfungszeit nur der Hochschule und nicht an Dritte weitergeben werde.

18.03.2024 Sayed Sayedy

Datum, Unterschrift

Sayed Sayedy

Inhaltsverzeichnis

Abkürzungsverzeichnis

- **CoC**: Chain of Custody
- **IoT**: Internet of Things
- **SHA-256**: Secure Hash Algorithm 256-bit
- **SQL**: Structured Query Language
- **ISO/IEC**: International Organization for Standardization/International Electrotechnical Commission
- **NIST**: National Institute of Standards and Technology
- **BSI**: Bundesamt für Sicherheit in der Informationstechnik
- **ENISA**: European Union Agency for Cybersecurity
- **API**: Application Programming Interface
- **IDE**: Integrated Development Environment

1 Einleitung

Die digitale Transformation prägt zunehmend sämtliche Bereiche des gesellschaftlichen und wirtschaftlichen Lebens. Mit der wachsenden Digitalisierung steigt jedoch auch die Anzahl und Komplexität von Sicherheitsvorfällen, die eine professionelle Incident Response erfordern. In diesem Kontext gewinnt die "Chain of Custody" (CoC) – zu Deutsch die Kette der Beweissicherung – eine zentrale Bedeutung. Sie stellt sicher, dass digitale Beweismittel in einem Zustand erfasst, gesichert, analysiert und präsentiert werden, der ihre Integrität und Authentizität vor Gericht oder in Disziplinarverfahren gewährleistet (Rani, Singh Gill, & Gulia, 2024; Tsai, 2021).

1.1 Hintergrund und Bedeutung der Chain of Custody im Bereich der digitalen Forensik

Die Chain of Custody dokumentiert lückenlos den Weg, den digitale Beweismittel vom Zeitpunkt ihrer Erfassung bis zu ihrer Vorlage in einem rechtlichen oder administrativen Verfahren nehmen. Diese Dokumentation umfasst alle Interaktionen mit den Beweismitteln, einschließlich ihrer Erfassung, Lagerung, Übertragung und Analyse. Die Bedeutung der CoC ergibt sich aus der Notwendigkeit, die Integrität der Beweismittel zu bewahren und Manipulationen auszuschließen, was für die Glaubwürdigkeit und Verwertbarkeit der Beweismittel in rechtlichen Verfahren unabdingbar ist (Gallo et al., 2024).

1.2 Zielsetzung der Arbeit

Die vorliegende Arbeit hat zum Ziel, die wesentlichen Aspekte der Chain of Custody im Kontext von Incident Response Prozessen zu beleuchten. Es wird untersucht, welche technischen und organisatorischen Maßnahmen ergriffen werden müssen, um eine lückenlose und nachvollziehbare CoC zu gewährleisten. Zudem wird der potenzielle Einsatz von Blockchain-Technologie als Mittel zur Unterstützung der CoC diskutiert. Im praktischen Teil der Arbeit wird ein rudimentäres Konzept zur Implementierung der CoC mittels Python entwickelt, das die Nachverfolgung von Änderungen an digitalen Beweismitteln ermöglicht und deren Integrität sicherstellt (Rani et al., 2024; Gallo et al., 2024).

Um diese Ziele zu erreichen, stützt sich die Arbeit auf eine umfassende Literaturrecherche, die sowohl aktuelle wissenschaftliche Publikationen als auch Fachliteratur und Standards im Bereich der digitalen Forensik und der Incident Response

umfasst. Durch die Kombination aus theoretischer Erörterung und praktischer Anwendung soll ein tiefgreifendes Verständnis für die Bedeutung und Umsetzung der Chain of Custody in der digitalen Forensik vermittelt werden.

Da die Quellenangaben und Literaturhinweise essenziell für die wissenschaftliche Fundierung der Arbeit sind, werden im fertigen Dokument entsprechende Verweise auf Fachliteratur, Studien und Normen eingefügt, um die Argumentation zu stärken und den wissenschaftlichen Ansprüchen gerecht zu werden.

2 Grundlagen

Im Folgenden werden die grundlegenden Konzepte und Rahmenbedingungen der Chain of Custody (CoC) im Kontext von Incident Response Prozessen dargelegt. Dies schließt Definitionen, die Bedeutung der CoC sowie rechtliche und normative Rahmenbedingungen ein.

2.1 Definition und Konzept der Chain of Custody

Die Chain of Custody (CoC) beschreibt die dokumentierte und nachvollziehbare Kette, die den Umgang mit Beweismitteln von ihrer Erhebung bis zur Vorlage bei Gericht oder in administrativen Verfahren umfasst. Es zielt darauf ab, die Authentizität, Integrität und Unversehrtheit der Beweismittel zu gewährleisten. In der digitalen Forensik schließt dies die Erfassung, Speicherung, Übertragung und Analyse digitaler Daten ein. Die CoC dokumentiert, wer zu welchem Zeitpunkt Zugriff auf die Beweismittel hatte, und welche Veränderungen vorgenommen wurden (Casey, 2011, S. 82; Carrier, 2005, S. 47; Reith, Carr, & Gunsch, 2002).

2.2 Bedeutung der Chain of Custody in Incident Response Prozessen

Die CoC ist in Incident Response Prozessen von besonderer Bedeutung, da digitale Beweismittel oft die Grundlage für die Analyse von Sicherheitsvorfällen bilden. Eine lückenlose CoC ist notwendig, um die Glaubwürdigkeit und Verwertbarkeit der Beweismittel in rechtlichen Auseinandersetzungen zu sichern. Besonders in einer Zeit, in der digitale Daten leicht verändert oder manipuliert werden können, hilft eine ordnungsgemäß geführte CoC, Zweifel an der Zuverlässigkeit der Beweismittel auszuräumen (Gallo et al., 2024).

2.3 Rechtliche Rahmenbedingungen und Standards

Die Handhabung und Dokumentation der CoC unterliegt verschiedenen rechtlichen und normativen Rahmenbedingungen, die je nach Jurisdiktion variieren können. Zu den relevanten Rechtsnormen gehören unter anderem Strafprozessrecht, Datenschutzgesetze sowie spezifische Vorschriften zum Umgang mit elektronischen Beweismitteln. Standards wie ISO/IEC 27037:2012 bieten Richtlinien für die Identifizierung, Sammlung, Akquise und Bewahrung digitaler Beweismittel. Darüber hinaus bieten Richtlinien des National Institute of Standards and Technology (NIST) eine wichtige Ressource für

Organisationen und Ermittler im Bereich der Incident Response (ISO/IEC, 2012; NIST, 2012).

Die Einhaltung dieser rechtlichen und normativen Vorgaben ist essentiell, um die Integrität der CoC zu gewährleisten und die Verwertbarkeit der Beweismittel in rechtlichen Verfahren zu sichern. Organisationen und Ermittler müssen daher mit den relevanten Rechtsnormen und Standards vertraut sein und diese in ihren Incident Response Prozessen berücksichtigen.

3 Technische und organisatorische Maßnahmen

Um die Integrität und Authentizität digitaler Beweismittel im Rahmen der Chain of Custody (CoC) zu gewährleisten, sind spezifische technische und organisatorische Maßnahmen erforderlich. Diese Maßnahmen stellen sicher, dass digitale Daten von ihrer Erfassung bis zur Vorlage in einem rechtlichen Kontext geschützt und ihre Unversehrtheit nachweisbar ist.

3.1 Technische Maßnahmen zur Sicherung der Chain of Custody

Für die Beweissicherung spielen technische Maßnahmen wie digitale Signaturen, Verschlüsselungsverfahren und die Verwendung von Hashing-Algorithmen eine entscheidende Rolle. Insbesondere die Blockchain-Technologie bietet hier neue Perspektiven. Durch die dezentrale und manipulationssichere Dokumentation von digitalen Beweismitteln in der Blockchain kann eine zuverlässige CoC etabliert werden (Belchior, Correia, & Vasconcelos, 2019; Bonomi, Casini, & Ciccotelli, 2020).

3.1.1 Digitale Signatur und Hashing

Die digitale Signatur und das Hashing sind essenzielle Technologien zur Sicherung der CoC. Digitale Signaturen bieten eine Methode, um die Authentizität und Integrität von Daten zu verifizieren. Die Hashing-Verfahren, insbesondere die Verwendung von kryptographisch sicheren Hashfunktionen wie SHA-256, sind effektiv für die Überprüfung der Unveränderlichkeit von Daten (Lone & Mir, 2019; Reith et al., 2002).

- **Digitale Signaturen** basieren auf asymmetrischer Kryptografie, bei der ein öffentlicher und ein privater Schlüssel zum Einsatz kommen. Der Ersteller eines Dokuments oder einer Datei generiert mit seinem privaten Schlüssel eine digitale Signatur, die an die Datei angehängt wird. Empfänger können mit dem öffentlichen Schlüssel des Erstellers die Signatur überprüfen und somit die Authentizität und die Unversehrtheit der Datei verifizieren. Digitale Signaturen sind rechtlich bindend und können in Gerichtsverfahren als Beweismittel dienen.
- **Hashing** ist ein Verfahren, bei dem aus beliebig großen Datenmengen ein eindeutiger, fester Zeichenwert (Hashwert) erzeugt wird. Ändert sich auch nur ein Bit der ursprünglichen Daten, resultiert dies in einem völlig anderen Hashwert. Hashfunktionen werden genutzt, um die Integrität von Daten zu überprüfen. So können Unterschiede zwischen dem ursprünglichen und einem späteren Zustand

der Daten leicht identifiziert werden. Hashwerte digitaler Beweismittel werden oft dokumentiert, um später deren Unveränderlichkeit beweisen zu können.

3.1.2 Verschlüsselung

Verschlüsselung schützt sensible Daten vor unbefugtem Zugriff. Sie wird durch die Verwendung von symmetrischen oder asymmetrischen Schlüsseln erreicht, die Daten in eine nicht lesbare Form umwandeln. Im Kontext der CoC sichert sie die Vertraulichkeit der Daten während der Übertragung und Lagerung (Palmbach, 2015). Die Kombination aus digitaler Signatur, Hashing und Verschlüsselung bildet einen robusten Mechanismus zum Schutz der CoC in digitalen Forensikprozessen (Beutelspacher 2015, S. 20-35; Gallo et al., 2024).

- **Symmetrische Verschlüsselung** verwendet denselben Schlüssel für die Ver- und Entschlüsselung. Sie ist effizient und eignet sich besonders für die Verschlüsselung großer Datenmengen. Allerdings muss der Schlüssel sicher übermittelt und aufbewahrt werden.
- **Asymmetrische Verschlüsselung** nutzt ein Schlüsselpaar, bestehend aus einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel darf bekannt gegeben werden und dient der Verschlüsselung. Der private Schlüssel bleibt geheim und wird zur Entschlüsselung verwendet. Diese Methode eignet sich besonders für den sicheren Austausch von Daten über unsichere Kanäle.

Die Kombination aus digitaler Signatur, Hashing und Verschlüsselung bietet einen robusten Schutzmechanismus für die CoC in digitalen Forensikprozessen. Sie ermöglicht es, die Authentizität, Integrität und Vertraulichkeit digitaler Beweismittel effektiv zu sichern.

3.2 Organisatorische Maßnahmen

Neben technischen sind auch organisatorische Maßnahmen essenziell für die Aufrechterhaltung der CoC. Dazu gehören die Prozessdokumentation und die Schulung der Mitarbeiter. Die Prozessdokumentation sorgt für die lückenlose Aufzeichnung aller Vorgänge im Umgang mit Beweismitteln, während Schulungen sicherstellen, dass alle Beteiligten die Bedeutung der CoC verstehen und entsprechend handeln (ISO/IEC 27037:2012; NIST 2012).

Die Einhaltung von Standards und Best Practices ist entscheidend für die Wirksamkeit von Incident Response und IT-Forensik. Zu diesen Standards gehören nicht nur ISO/IEC

27037:2012 und NIST SP 800-86, sondern auch Richtlinien und Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der European Union Agency for Cybersecurity (ENISA). Diese Institutionen bieten umfassende Leitfäden und Best Practices für die digitale Forensik und Incident Response, die die Anforderungen an die Chain of Custody (CoC) und die allgemeine Reaktion auf Sicherheitsvorfälle unterstützen. Die kontinuierliche Überprüfung und Anpassung der Prozesse, im Hinblick auf aktuelle Bedrohungen und neue technologische Entwicklungen, sind weitere wichtige Aspekte, die von diesen Standards und Empfehlungen abgedeckt werden.

3.2.1 Prozessdokumentation

Die Prozessdokumentation spielt eine entscheidende Rolle in der Sicherung der Chain of Custody (CoC). Sie dient der nachvollziehbaren Aufzeichnung aller Vorgänge im Umgang mit Beweismitteln, was essenziell für die Beweisführung in juristischen Prozessen ist. Dabei ist es wichtig, eine Präzision zu wahren, die sicherstellt, dass jede Aktion mit den Beweismitteln, von ihrer Entdeckung am Tatort bis zur Präsentation im Gerichtssaal, festgehalten wird. In diesem Kontext können Blockchain-Technologien einen bedeutenden Mehrwert bieten. Die Unveränderlichkeit der Blockchain ermöglicht eine manipulationssichere Aufzeichnung, die nicht nur die Integrität der Beweise sichert, sondern auch die Effizienz der forensischen Prozesse verbessert. Zum Beispiel erleichtern Smart Contracts automatisierte Abläufe, welche die Protokollierung standardisieren und potenzielle menschliche Fehler minimieren können (Belchior et al., 2019).

Darüber hinaus können blockchain-basierte Systeme zur Dokumentation der CoC, wie B-CoC, den forensischen Prozess durch die Bereitstellung einer transparenten und nachvollziehbaren Aufzeichnung unterstützen, die alle Interaktionen mit dem Beweismittel lückenlos dokumentiert (Bonomi et al., 2020). Dies umfasst:

- **Erfassung**: Dokumentation des Zeitpunkts, Orts und der Art und Weise der Erfassung digitaler Beweismittel.
- **Übertragung**: Protokollierung aller Übertragungen von Beweismitteln zwischen Personen oder Standorten, inklusive der beteiligten Personen und der verwendeten Transportmittel.
- **Lagerung**: Aufzeichnung der Lagerorte und der Lagerbedingungen.
- **Zugriff**: Dokumentation aller Zugriffe auf die Beweismittel, einschließlich der Identität der zugreifenden Personen und des Zwecks des Zugriffs.
- **Analyse**: Detaillierte Aufzeichnung aller Analyseaktivitäten und -ergebnisse.

Für die Prozessdokumentation werden oft spezialisierte Softwarelösungen eingesetzt, die die Erfassung und Verwaltung der Dokumentation unterstützen und die Integrität der Daten sicherstellen. Die ISO/IEC 27037:2012 und andere Standards, wie BSI-Richtlinien und ENISA-Empfehlungen, geben Richtlinien vor, wie eine solche Dokumentation strukturiert sein sollte, um den Anforderungen an die CoC gerecht zu werden.

3.2.2 Schulung und Bewusstseinsbildung

Die Schulung und Sensibilisierung aller Beteiligten ist ebenso von fundamentaler Bedeutung für die CoC. Eine adäquate Schulung in der Anwendung von Blockchain-Systemen und in den Prinzipien der digitalen Forensik kann dazu beitragen, dass Beweismittel korrekt gehandhabt und aufgezeichnet werden. Das Verständnis für die zugrunde liegenden Prozesse der Blockchain, wie sie in grundlegenden Arbeiten wie denen von Nakamoto (2008) und Dierksmeier und Seele (2020) beschrieben werden, ist hierbei von besonderer Wichtigkeit. Solche Schulungsprogramme sollten auf den neuesten Standards und Praktiken basieren und von renommierten Institutionen angeboten werden, um sicherzustellen, dass sie die sich ständig ändernden Anforderungen der digitalen Forensik und der IT-Sicherheit abdecken.

Darüber hinaus sollten Schulungsprogramme nicht nur technische Kenntnisse vermitteln, sondern auch ein Bewusstsein für ethische Aspekte schaffen, die bei der Handhabung von digitalen Beweisen auftreten können. Dierksmeier und Seele (2020) betonen die moralischen Dimensionen der Blockchain-Technologie und wie sie Geschäftsethik beeinflussen kann. Dies ist insbesondere relevant, da Entscheidungen in der CoC nicht nur technische, sondern auch rechtliche und moralische Konsequenzen haben können.

Die Implementierung effektiver Schulungs- und Bewusstseinsprogramme erfordert eine kontinuierliche Überprüfung und Anpassung der Lehrpläne, um mit den sich entwickelnden Technologien wie Blockchain und den Best Practices in der digitalen Forensik Schritt zu halten. Institutionen wie das National Institute of Standards and Technology (NIST) bieten hierfür ein solides Fundament durch Publikationen und Leitfäden, die als Basis für Bildungsmaßnahmen dienen können (NIST, 2012).

Die Kombination aus fortlaufender Bildung und praktischen Übungen, wie von Bonomi, Casini und Ciccotelli (2020) in der Entwicklung eines blockchainbasierten CoC-Prototyps demonstriert, kann entscheidend dazu beitragen, das Personal auf die Herausforderungen im Umgang mit Beweismitteln in der digitalen Welt vorzubereiten. Dies umfasst auch die Vertrautheit mit forensischen Werkzeugen und Verfahren, die im Einklang mit rechtlichen Standards die Integrität von Beweismitteln garantieren können.

4 Einsatz von Blockchain-Technologie

Die Blockchain-Technologie, ursprünglich entwickelt als das technische Rückgrat von Bitcoin, hat weitreichende Anwendungsmöglichkeiten, die weit über Kryptowährungen hinausgehen. Ihre Eigenschaften wie Transparenz, Manipulationssicherheit und Dezentralisierung bieten innovative Lösungsansätze für zahlreiche Herausforderungen in verschiedenen Branchen, einschließlich der digitalen Forensik und der Sicherstellung der Chain of Custody (CoC). Die Integration von Blockchain-Technologie in den Incident Response Prozess und die Chain of Custody kann die Dokumentation und Sicherung digitaler Beweismittel revolutionieren. Die inhärente Transparenz und Unveränderlichkeit der Blockchain bietet neue Möglichkeiten für die Beweissicherung und das Management von forensischen Daten (Pilkington, 2016).

4.1 Grundlagen der Blockchain-Technologie

Die Blockchain-Technologie wird zunehmend in unterschiedlichen Bereichen eingesetzt und gewinnt auch in der digitalen Forensik an Bedeutung. Eine ausführliche Einführung in die grundlegenden Prinzipien und Anwendungen bietet die Bundesnetzagentur (2021). Melanie Swan (2021) hebt hervor, wie die Blockchain in der digitalen Forensik zur sicheren und unveränderlichen Aufzeichnung der Chain of Custody genutzt werden kann, indem jeder Block in der Blockchain eine verifizierbare Liste von Transaktionen enthält, die durch kryptografische Verfahren gesichert sind (Pilkington, 2016; Crosby et al., 2016; Fraunhofer FIT, 2021).

Blockchain ist eine verteilte Datenbank, die eine fortlaufende Liste von Transaktionsdatensätzen führt, die als Blöcke bezeichnet werden. Jeder Block enthält einen kryptographischen Hash des vorherigen Blocks, einen Zeitstempel und Transaktionsdaten. Die Daten in einem Block können nicht rückwirkend geändert werden, ohne alle nachfolgenden Blöcke zu ändern, was eine hohe Sicherheit gegenüber Datenmanipulation bietet (Nakamoto, 2008).

4.2 Anwendungsfälle der Blockchain in der Chain of Custody

Die Blockchain-Technologie kann in der digitalen Forensik eingesetzt werden, um eine sichere und unveränderliche Dokumentation der CoC zu erstellen. Dies umfasst die Dokumentation von Beweismittel-Transaktionen und die Integritätssicherung von Beweismitteln durch die Erstellung und Speicherung von Hashwerten in der Blockchain. Zudem kann die Blockchain für Zugriffskontrolle und Authentifizierung genutzt werden,

um die Authentizität von Nutzern zu überprüfen, die auf Beweismittel zugreifen möchten (Christidis & Devetsikiotis, 2016). Blockchain-Anwendungen in der CoC umfassen das Management von Beweismitteltransaktionen, wo jede Übertragung, Lagerung oder Analyse als Blockchain-Transaktion aufgezeichnet wird. Dies erhöht die Nachvollziehbarkeit und Authentizität der Beweismittel im gesamten forensischen Prozess (Christidis & Devetsikiotis, 2016; Belchior et al., 2019).

- **Dokumentation von Beweismittel-Transaktionen**: Jede Übertragung, jede Analyse oder sonstige Interaktion mit einem digitalen Beweisstück kann als Transaktion in der Blockchain gespeichert werden. Dies schließt Informationen über Zeitpunkt, beteiligte Personen und Art der Interaktion ein.
- **Integritätssicherung von Beweismitteln**: Durch die Erstellung von Hashwerten digitaler Beweismittel und deren Speicherung in der Blockchain kann deren Unveränderlichkeit gewährleistet werden. Änderungen am Beweismittel führen zu einem anderen Hashwert, wodurch Manipulationen sofort erkennbar sind.
- **Zugriffskontrolle und Authentifizierung**: Blockchain-Technologie kann genutzt werden, um Zugriffsrechte zu verwalten und die Authentizität von Nutzern zu überprüfen, die auf Beweismittel zugreifen möchten.

4.3 Vorteile und Herausforderungen

Die Vorteile der Blockchain-Technologie in der digitalen Forensik umfassen Transparenz und Nachvollziehbarkeit der Beweismittel-Interaktionen sowie Manipulationssicherheit durch kryptografische Verkettung der Blöcke. Zudem reduziert die Technologie Vertrauensprobleme, da sie ohne eine zentrale Autorität auskommt. Herausforderungen beinhalten Skalierbarkeit, Komplexität der Implementierung und rechtliche sowie regulatorische Fragen, die durch die neuartige Technologie aufgeworfen werden (Crosby et al., 2016). Die Nutzung der Blockchain-Technologie im CoC-Management bietet mehrere Vorteile:

- **Transparenz:** Alle Transaktionen sind für berechtigte Parteien sichtbar und können nicht geändert werden, was die Nachvollziehbarkeit erhöht (Swan, 2021).
- **Sicherheit:** Die Verwendung von Kryptographie stellt sicher, dass Beweismittel während des gesamten forensischen Prozesses nicht manipuliert werden können (Yan et al., 2020).
- **Effizienz:** Blockchain kann den Zeit- und Arbeitsaufwand für die Verwaltung der CoC reduzieren, indem manuelle Aufgaben automatisiert werden (Lone & Mir, 2019).

Zu den Herausforderungen gehören:

- **Skalierbarkeit:** Die steigende Anzahl von Transaktionen kann die Blockchain verlangsamen (WeKing et al., 2020).
- **Komplexität:** Die Integration in bestehende Systeme kann komplex und kostspielig sein.
- **Rechtliche und regulatorische Fragen:** Es gibt Unsicherheiten bezüglich der rechtlichen Anerkennung von blockchainbasierten Beweisen (Bonomi et al., 2020).

Die Einführung der Blockchain in die CoC stellt einen vielversprechenden Ansatz dar, um die Authentizität und Integrität digitaler Beweismittel zu sichern. Trotz der Herausforderungen bietet die Technologie das Potenzial, die Praxis der digitalen Forensik signifikant zu verbessern und die Verlässlichkeit der CoC in digitalen Ermittlungen zu erhöhen. Fortschritte in der Blockchain-Technologie und deren Anpassung an die spezifischen Anforderungen der digitalen Forensik könnten diese Herausforderungen in Zukunft weiter minimieren.

Die Auswirkungen der Blockchain-Technologie auf Geschäftsmodelle und ihre Anwendung in der forensischen Wissenschaft werden weiterhin erforscht und entwickelt, um diese Herausforderungen zu überwinden (Aouidef et al., 2021).

5 Praktischer Teil: Implementierung eines Prototyps

Der praktische Teil dieser Arbeit widmet sich der Entwicklung eines Prototyps zur Demonstration der Chain of Custody (CoC) mittels Blockchain-Technologie. Dieser Prototyp soll eine rudimentäre Implementierung der CoC in einem Python-basierten Programm darstellen, wobei Änderungen an digitalen Beweismitteln durch die Generierung von Hashwerten verfolgt und in einer Blockchain gespeichert werden.

5.1 Konzeption des Prototyps

5.1 Konzeption des Prototyps:

Im Rahmen dieser Arbeit habe ich ein Prototyp entwickelt, der die Prinzipien der Blockchain-Technologie nutzt, um eine robuste Chain of Custody (CoC) zu demonstrieren. Der Fokus lieg dabei auf der Erstellung und dem Management von Hashwerten für digitale Beweismittel. Wesentlich ist dabei, dass der Prototyp eine breitere Palette von Dateiformaten automatisch erkennt und verarbeitet, was über die typische Konzeption hinausgeht. Die Gestaltung umfasst verbesserte Fehlerbehandlung und eine detailliertere Protokollierung, die sowohl die Authentizität als auch die Integrität digitaler Beweismittel im gesamten forensischen Prozess gewährleistet. Der Prototyp soll die Generierung und Verwaltung von Hashwerten für digitale Beweismittel ermöglichen und die Unversehrtheit der Daten mittels Blockchain garantieren. Dies dient der Dokumentation ihres Ursprungszustands und ermöglicht die Nachverfolgung von Änderungen. Die Integrität der Beweismittel wird durch eine sichere und nachvollziehbare Dokumentation sichergestellt. Der Prototyp soll u.A. folgende Kernfunktionalitäten umfassen:

- **Erfassung digitaler Beweismittel**: Automatische Erzeugung von Hashwerten für digitale Dateien (Beweismittel) bei ihrer Erfassung, um deren Ursprungszustand zu dokumentieren.
- **Änderungsverfolgung**: Erzeugung neuer Hashwerte nach jeder Änderung an einer Datei, um eine fortlaufende Überwachung und Dokumentation der Integrität zu ermöglichen.
- **Protokollierung**: Jede Aktion und jeder erzeugte Hashwert wird zusammen mit Zeitstempeln und ggf. Benutzeridentifikationen in einer Protokolldatei oder einer Datenbank gespeichert.
- **Integritätsprüfung**: Möglichkeit zur Überprüfung der Integrität der Beweismittel anhand der gespeicherten Hashwerte und Protokolleinträge.

5.2 Entwicklungsumgebung und Werkzeuge

In Bezug auf die Entwicklungsumgebung und Werkzeuge wurden zusätzliche Bibliotheken und Tools eingeführt, um den erweiterten Anforderungen des Prototyps gerecht zu werden. Neben der Nutzung von Python 3 und der hashlib-Bibliothek für die Hashwertgenerierung, wurden Automatisierungstechniken integriert, um die Vielfalt der Dateitypen zu unterstützen. Diese Verbesserungen erhöhen die Funktionalität des Prototyps signifikant und erweitern dessen Anwendungsbereich über traditionelle digitale Beweismittel hinaus.

Zur Speicherung der Hashwerte und Transaktionen wird eine Blockchain simuliert, für die ein einfaches, persistentes Datenmodell verwendet wird, wie es auch in einfachen Blockchain-Implementierungen wie der von Nakamoto (2008) beschrieben ist. Grundlegendes Kryptologieverständnis, wie in Beutelspacher (2015) erörtert, ist für die sichere Anwendung solcher Bibliotheken essenziell, während SQLite als Datenbanksystem für die Protokollierung dient (Beutelspacher 2015).

- **Programmiersprache**: Python wird aufgrund seiner breiten Akzeptanz in der wissenschaftlichen Gemeinschaft, seiner umfangreichen Standardbibliothek und der Verfügbarkeit von Drittanbieterbibliotheken für Kryptografie und Datenbankinteraktionen gewählt.
- **Kryptografie-Bibliotheken**: Für die Hashing- und eventuelle Verschlüsselungsfunktionalitäten wird die hashlib-Bibliothek verwendet, die standardmäßig in Python enthalten ist. Sie unterstützt verschiedene Hashing-Algorithmen wie SHA-256, der für die Zwecke dieses Prototyps als ausreichend sicher gilt.
- **Datenbanksystem**: SQLite wird als Datenbanksystem für die Protokollierung verwendet. Es bietet eine leichte, dateibasierte Lösung, die keine separate Serverinstallation erfordert und direkt von Python aus über die sqlite3-Bibliothek angesprochen werden kann.
- **Entwicklungsumgebung (IDE)**: Für die Entwicklung des Prototyps kann eine integrierte Entwicklungsumgebung wie PyCharm oder Visual Studio Code verwendet werden. Beide bieten umfangreiche Unterstützung für Python-Entwicklung, einschließlich Codevervollständigung, Debugging und Versionskontrolle.

Die Entwicklung beginnt mit der Einrichtung der Entwicklungsumgebung, gefolgt von der Implementierung der Kernfunktionalitäten des Prototyps. In jeder Entwicklungsphase

wird eine iterative Vorgehensweise angewendet, die es ermöglicht, den Prototyp kontinuierlich zu testen und zu verbessern.

5.3 Implementierung

Die Implementierungsphase beinhaltete nun die Entwicklung von Funktionen, die eine Vielzahl von Dateitypen verarbeiten und ihre Änderungshistorie in einer sichereren, manipulationssicheren Datenbank protokollieren. Neue Mechanismen zur Fehlerbehandlung wurden eingeführt, um die Stabilität und Zuverlässigkeit des Prototyps zu verbessern. Diese Erweiterungen tragen zur einer lückenlosen und vertrauenswürdigen Chain of Custody bei und verstärken die Sicherheit und Nachvollziehbarkeit innerhalb des forensischen Prozesses.

Gemäß den Richtlinien der ISO/IEC 27037:2012 werden die Protokolleinträge in einer manipulationssicheren Datenbank gespeichert, wofür sich eine SQLite-Datenbank als geeignet erweist. Diese Schritte tragen dazu bei, die Authentizität und Unversehrtheit digitaler Beweismittel durch den gesamten forensischen Prozess zu gewährleisten. Die Umsetzung solcher Maßnahmen reflektiert zudem die Empfehlungen der ENISA und des BSI für die sichere Handhabung digitaler Beweise und die Aufrechterhaltung einer effektiven CoC.

5.3.1 Generierung von Hashwerten

Für jedes digitale Beweismittel wird ein eindeutiger Hashwert generiert, der bei jeder Änderung des Beweismittels aktualisiert wird. Die Hashwerte werden nach einem Verfahren ähnlich dem von Yan et al. (2020) generiert. Die Generierung von Hashwerten für digitale Beweismittel ist ein fundamentaler Schritt, um deren Integrität zu sichern. Der Prozess umfasst folgende Schritte:

- **Auswahl des Hash-Algorithmus**: SHA-256 wird aufgrund seiner Sicherheit und der breiten Akzeptanz in der Kryptografie-Gemeinschaft gewählt. SHA-256 ist resistent gegen Kollisionen, was bedeutet, dass es praktisch unmöglich ist, zwei unterschiedliche Eingaben zu finden, die denselben Hashwert erzeugen.
- **Berechnung des Hashwerts**: Für jedes digitale Beweismittel wird der Hashwert durch die Anwendung des SHA-256-Algorithmus auf den Inhalt der Datei berechnet. Dies geschieht durch die Nutzung der **hashlib**-Bibliothek in Python:

```
import hashlib
```

```
def generate_hash(file_path):
    with open(file_path, 'rb') as f:
        file_content = f.read()
        hash = hashlib.sha256(file_content).hexdigest()
        return hash
```

- **Speicherung des Hashwerts**: Der erzeugte Hashwert wird zusammen mit den Metadaten des Beweismittels (z.B. Dateiname, Erstellungszeitpunkt) gespeichert, um eine spätere Überprüfung zu ermöglichen.

5.3.2 Protokollierung der Änderungshistorie

Jede Interaktion mit den Beweismitteln wird protokolliert und in der Blockchain gespeichert. Die Protokollierung folgt einem Ansatz, der in Studien wie denen von Lone und Mir (2019) diskutiert wird, und beinhaltet Zeitstempel, Nutzeridentifikation und den jeweiligen Hashwert:

1. **Erstellung eines Protokolleintrags**: Für jede Aktion wird ein Protokolleintrag erstellt, der den Zeitpunkt der Aktion, die Art der Änderung, den Nutzer, der die Änderung vorgenommen hat, und den neuen Hashwert des Beweismittels enthält.

2. **Speicherung des Protokolleintrags**: Die Protokolleinträge werden in einer SQLite-Datenbank gespeichert, um eine dauerhafte und manipulationssichere Aufzeichnung zu gewährleisten:[1]

```
import sqlite3

def log_change(action, user, file_path, new_hash):
    conn = sqlite3.connect('cochain.db')
    cursor = conn.cursor()
    cursor.execute('''CREATE TABLE IF NOT EXISTS changes
                      (timestamp DATETIME DEFAULT CURRENT_TIMESTAMP,
action TEXT,
                       user TEXT, file_path TEXT, hash TEXT)''')
    cursor.execute('''INSERT INTO changes (action, user, file_path, hash)
                      VALUES (?, ?, ?, ?)''', (action, user, file_path,
new_hash))
```

[1] Diese Implementierung zeigt den Einsatz von Technologien zur Sicherung der Chain of Custody in der digitalen Forensik. Die Codesnippets unterstützen den Prototypenbau und veranschaulichen relevante Programmierkonzepte. In der Praxis wäre eine Literaturuntermauerung üblich, um die Methodenwahl und technologische Relevanz zu bekräftigen.

```
    conn.commit()
    conn.close()
```

5.3.3 Prüfung der Protokollierungskette

Es wird eine Funktion implementiert, um die Integrität der gespeicherten Daten zu überprüfen. Diese Prüfung soll sicherstellen, dass die Datenkette intakt ist und seit der Erfassung des Hashwerts keine Änderungen ohne entsprechende Protokollierung stattgefunden haben. Die Überprüfung der Protokollierungskette ermöglicht es, die Integrität und Unveränderlichkeit der Beweismittel zu validieren:

1. **Überprüfung des Hashwerts**: Für jedes Beweismittel wird der aktuelle Hashwert berechnet und mit dem gespeicherten Hashwert verglichen. Unterschiede weisen auf eine mögliche Manipulation hin.

2. **Analyse der Protokolleinträge**: Die Protokolleinträge werden analysiert, um festzustellen, ob alle Änderungen an den Beweismitteln ordnungsgemäß dokumentiert wurden. Unstimmigkeiten oder fehlende Einträge können auf Probleme in der CoC hinweisen.

5.4 Test und Validierung

Der Prototyp wird einer Reihe von Tests unterzogen, um seine Funktionalität zu überprüfen. Die Teststrategie orientiert sich an der von Bonomi et al. (2020) vorgestellten Methode zur Validierung von Blockchain-Anwendungen in der digitalen Forensik. Die Testphase dient der Überprüfung der Funktionalität des Prototyps, einschließlich der korrekten Generierung von Hashwerten und der lückenlosen Protokollierung von Änderungen. Nicht-funktionale Tests bewerten Leistung, Sicherheit und Benutzerfreundlichkeit (Bundesnetzagentur, 2021).

5.4.1 Teststrategie

Basierend auf den Empfehlungen von Bonomi et al. (2020), wird eine umfassende Teststrategie entwickelt, die sowohl automatisierte als auch manuelle Tests einschließt. Die Tests konzentrieren sich auf die Überprüfung der Integrität der Blockchain-Daten, die Effizienz der Hashwert-Generierung und die Sicherheit der Protokollierungskette:

- **Funktionstests**: Überprüfung der korrekten Funktion aller Komponenten des Prototyps. Dies umfasst die Generierung von Hashwerten, die Protokollierung von Änderungen und die Verifizierung der Datenintegrität.
- **Sicherheitstests**: Bewertung der Widerstandsfähigkeit des Prototyps gegenüber Manipulationsversuchen und anderen Sicherheitsbedrohungen. Dies beinhaltet Tests auf Schwachstellen in der Implementierung der Blockchain sowie in der Handhabung der digitalen Beweismittel.
- **Leistungstests**: Messung der Antwortzeiten und Ressourcennutzung unter verschiedenen Betriebsbedingungen, um die Skalierbarkeit und Effizienz des Prototyps zu bewerten.

5.4.2 Testdurchführung

Die Testdurchführung orientiert sich an den Best Practices für Softwaretests in der digitalen Forensik. Es werden verschiedene Szenarien simuliert, die typische Anwendungsfälle in der Forensik abdecken, um ein realistisches Bild der Leistungsfähigkeit des Prototyps zu erhalten. Die Ergebnisse werden dokumentiert und analysiert, um potenzielle Verbesserungen zu identifizieren.

- **Generierung von Hashwerten:** Tests zur Überprüfung der Konsistenz und Einzigartigkeit der erzeugten Hashwerte für verschiedene Arten von digitalen Beweismitteln.
- **Protokollierung und Nachverfolgung von Änderungen:** Überprüfung der Genauigkeit und Vollständigkeit der Änderungsprotokolle in der Blockchain.
- **Integritätsprüfung:** Validierung der Mechanismen zur Überprüfung der Unversehrtheit der gespeicherten Daten.

5.4.3 Validierung der Ergebnisse

Nach Abschluss der Tests werden die Ergebnisse mit den ursprünglichen Anforderungen abgeglichen, um die Erfüllung der gestellten Ziele zu validieren. Zusätzlich werden die Ergebnisse genutzt, um die allgemeine Zuverlässigkeit und Anwendbarkeit des Prototyps in realen forensischen Szenarien zu bewerten. Die Validierung umfasst auch eine rechtliche Bewertung, um die Konformität mit den relevanten Standards und Gesetzen sicherzustellen.

- **Bewertung der technischen Lösung:** Vergleich der Testergebnisse mit den technischen Spezifikationen und Anforderungen.

- **Rechtliche Überprüfung:** Abgleich der Implementierung mit den rechtlichen Rahmenbedingungen der digitalen Forensik und der Beweissicherung.

5.4.4 Dokumentation und Berichterstattung

Die Dokumentation und Berichterstattung ist ein wesentlicher Bestandteil der Test- und Validierungsphase des Prototyps. Sie bietet nicht nur einen detaillierten Überblick über den gesamten Testprozess und dessen Ergebnisse, sondern gewährleistet auch die Nachvollziehbarkeit und Rechenschaftspflicht in Bezug auf die Entwicklung und Bewertung des Prototyps.

5.4.4.1 Dokumentation des Testprozesses

Der Testprozess sollte umfassend dokumentiert werden, einschließlich der Teststrategie, der verwendeten Testfälle, der Testumgebung und der spezifischen Testdaten. Diese Dokumentation sollte auch Informationen über die Methodik zur Fehlerbehebung und die verwendeten Werkzeuge enthalten. Bonomi et al. (2020) betonen die Wichtigkeit der transparenten Dokumentation, um die Glaubwürdigkeit und Zuverlässigkeit von forensischen Werkzeugen und Methoden zu gewährleisten.

5.4.4.2 Berichterstattung der Testergebnisse

Die Berichterstattung sollte eine detaillierte Analyse der Testergebnisse beinhalten, einschließlich der identifizierten Probleme, Schwachstellen und potenziellen Sicherheitsrisiken. Es ist wichtig, sowohl erfolgreiche Tests als auch Fehlschläge zu dokumentieren, um ein vollständiges Bild der Prototyp-Leistung zu bieten. Die Ergebnisse sollten im Kontext der ursprünglichen Anforderungen und Ziele des Prototyps bewertet werden, um deren Erfüllung zu validieren.

5.4.4.3 Bewertung und Empfehlungen

Auf Basis der Testergebnisse sollte der Bericht eine Bewertung des Prototyps hinsichtlich seiner Eignung für den Einsatz in realen forensischen Szenarien enthalten. Dies umfasst eine Diskussion über die Stärken und Schwächen des Prototyps sowie Empfehlungen für weitere Verbesserungen oder Forschungsarbeiten. Die Diskussion kann sich auf vergleichbare Studien und Veröffentlichungen stützen, um die Ergebnisse in einen breiteren wissenschaftlichen und praktischen Kontext zu stellen.

5.4.4.4 Rechtliche Konformität und Standards

Die Dokumentation sollte ebenfalls die Konformität des Prototyps mit relevanten rechtlichen Standards und Best Practices überprüfen. Dies beinhaltet eine Bewertung der

Übereinstimmung mit Normen wie ISO/IEC 27037:2012 und den Richtlinien des NIST, die in der digitalen Forensik und im Incident Response als Richtlinien dienen.

6 Diskussion

Die Diskussion dieses Forschungsprojekts bietet die Gelegenheit, die Ergebnisse der Implementierung des Prototyps und die Anwendung von Blockchain-Technologie in der Chain of Custody (CoC) im Kontext der digitalen Forensik zu reflektieren. Es werden sowohl die technologischen als auch die rechtlichen Herausforderungen beleuchtet, die während der Entwicklung und des Tests des Prototyps identifiziert wurden. Darüber hinaus werden die Implikationen dieser Technologie für die Zukunft der Beweissicherung und des Incident Response diskutiert.

Die Entwicklung des Prototyps hat gezeigt, dass technologische Lösungen, insbesondere die Automatisierung von Hashwerten und deren Protokollierung, eine signifikante Verbesserung der Integritätssicherung ermöglichen können. Die Anwendung der Blockchain-Technologie verspricht eine weitere Revolutionierung der CoC durch ihre Eigenschaften der Unveränderlichkeit und Transparenz (Christidis & Devetsikiotis, 2016).

6.1 Bewertung der technischen Lösung

Die Implementierung des Prototyps hat gezeigt, dass die Blockchain-Technologie das Potenzial hat, die CoC in digitalen Forensikprozessen zu revolutionieren. Die Unveränderlichkeit und Transparenz der Blockchain bieten einzigartige Vorteile für die Authentifizierung und Nachverfolgung digitaler Beweismittel. Dies steht im Einklang mit den Erkenntnissen von Pilkington (2016), der die transformative Wirkung der Blockchain auf verschiedene Sektoren hervorhebt.

Allerdings wurden auch technische Herausforderungen deutlich, insbesondere im Hinblick auf die Skalierbarkeit und die Integration mit bestehenden forensischen Tools und Systemen. Diese Herausforderungen sind konsistent mit den Beobachtungen von Yan et al. (2020), die betonen, dass die Effizienz der Blockchain bei wachsender Datenmenge eine kritische Betrachtung erfordert.

Die Verwendung von Python, speziell der **hashlib** und **sqlite3** Bibliotheken, hat sich als effektiv erwiesen, um eine einfache, doch robuste Lösung zu implementieren.
Stärken:

- **Einfachheit und Effizienz**: Die Implementierung zeigt, dass mit verhältnismäßig einfachen Mitteln eine signifikante Verbesserung der Nachverfolgbarkeit und Sicherheit in der CoC erreicht werden kann.

- **Erweiterbarkeit**: Der modulare Aufbau des Prototyps ermöglicht eine leichte Anpassung und Erweiterung, um zusätzliche Anforderungen oder Funktionen zu integrieren.

Schwächen:

- **Skalierbarkeit**: Bei der Verarbeitung sehr großer Datenmengen oder in sehr dynamischen Umgebungen könnten Leistungsprobleme auftreten. Die Leistungsfähigkeit der SQLite-Datenbank und die Effizienz der Hash-Berechnung bei großen Dateien sind potenzielle Begrenzungen.
- **Sicherheit**: Obwohl der Prototyp grundlegende Sicherheitsmechanismen integriert, sind weitere Maßnahmen erforderlich, um ihn gegen fortgeschrittene Bedrohungen zu schützen.

6.2 Anwendbarkeit und Grenzen der Blockchain-Technologie

Die Anwendbarkeit der Blockchain in der CoC ist vielversprechend, aber es gibt Grenzen und Bedenken. Einerseits bietet die Technologie eine verbesserte Sicherheit und Nachvollziehbarkeit von Beweismitteln, wie auch Lone und Mir (2019) in ihrer Forschung darlegen. Andererseits werfen rechtliche und regulatorische Fragen, einschließlich der Anerkennung von blockchain-basierten Beweisen in Gerichtsverfahren, neue Herausforderungen auf. Diese Bedenken spiegeln sich in der Arbeit von Bonomi et al. (2020) wider, die die Notwendigkeit betonen, rechtliche Rahmenbedingungen weiterzuentwickeln, um mit den technologischen Fortschritten Schritt zu halten.

Die Untersuchung der Blockchain-Technologie hat deren Potenzial aufgezeigt, die CoC durch eine dezentrale, manipulationssichere Dokumentation zu stärken. Ihre Anwendung in der digitalen Forensik könnte die Authentizität und Integrität von Beweismitteln in bisher unerreichter Weise sichern.

Anwendbarkeit:

- **Transparente und unveränderliche Protokollierung**: Die Blockchain bietet eine ideale Plattform für die Protokollierung von Beweismitteltransaktionen, die nicht nachträglich verändert werden können.
- **Automatisierte Vertragsabwicklung**: Smart Contracts könnten automatisierte Prozesse ermöglichen, die die Effizienz und Zuverlässigkeit der CoC weiter erhöhen.

Grenzen:

- **Komplexität und Kosten**: Die Implementierung einer Blockchain-Lösung kann komplex sein und erfordert eine sorgfältige Planung und Ressourcen. Insbesondere öffentliche Blockchains können aufgrund von Transaktionsgebühren kostspielig in der Nutzung sein.
- **Datenschutzbedenken**: Die unveränderliche Speicherung von Informationen in der Blockchain kann im Konflikt mit Datenschutzanforderungen stehen, insbesondere wenn es um sensible oder persönliche Daten geht.
- **Technologische Reife**: Trotz des großen Potenzials befindet sich die Anwendung der Blockchain-Technologie außerhalb des Finanzsektors noch in einem frühen Stadium. Es besteht Unsicherheit bezüglich der langfristigen Viabilität und Akzeptanz.

6.3 Zukünftige Entwicklungen und Forschungsbedarf

Die zukünftigen Entwicklungen in der digitalen Forensik und der CoC werden voraussichtlich stark von der Weiterentwicklung der Blockchain-Technologie beeinflusst werden. Es besteht ein erheblicher Forschungsbedarf, um die technischen, rechtlichen und ethischen Fragen, die mit der Anwendung dieser Technologie verbunden sind, vollständig zu adressieren. Die Forschung sollte sich insbesondere auf die Optimierung der Blockchain für forensische Zwecke, die Entwicklung von Standards für die Verwendung blockchain-basierter Beweise und die Untersuchung der Auswirkungen auf die Privatsphäre konzentrieren.

Die Untersuchung der Chain of Custody (CoC) in digitalen Forensikprozessen und der Einsatz von Blockchain-Technologie sowie die Entwicklung eines Prototyps werfen Licht auf zukünftige Entwicklungen und den damit verbundenen Forschungsbedarf. Um die Effektivität, Sicherheit und Praktikabilität dieser Ansätze zu verbessern, sind weitere Untersuchungen und Innovationen erforderlich.

Die Diskussion zeigt, dass die Blockchain-Technologie das Potenzial hat, die Praxis der digitalen Forensik und der CoC grundlegend zu verändern. Während der Prototyp wichtige Einblicke in die Machbarkeit und die Vorteile dieser Technologie bietet, unterstreichen die identifizierten Herausforderungen die Notwendigkeit weiterer Forschung und Entwicklung. Es ist entscheidend, dass zukünftige Arbeiten die technologischen Möglichkeiten mit den rechtlichen und ethischen Anforderungen in Einklang bringen, um die Integrität und Effektivität der digitalen Forensik zu gewährleisten.

6.4 Erweiterung der technischen Lösung

Die Evaluation des Prototyps und die Anwendung der Blockchain-Technologie in der Chain of Custody (CoC) haben zahlreiche Möglichkeiten für die Erweiterung der technischen Lösung aufgezeigt. Diese Erweiterungen zielen darauf ab, die Leistungsfähigkeit, Sicherheit und Anwendbarkeit der CoC in digitalen Forensikprozessen zu verbessern.

6.4.1 Integration fortgeschrittener kryptografischer Techniken

Die aktuelle Implementierung des Prototyps kann durch die Integration fortgeschrittener kryptografischer Techniken, wie Zero-Knowledge-Proofs und homomorphe Verschlüsselung, verbessert werden. Diese Technologien ermöglichen es, die Authentizität und Integrität von Beweismitteln zu überprüfen, ohne sensible Informationen preiszugeben (Yan et al., 2020). Dies adressiert Datenschutzbedenken und erhöht die Sicherheit und Privatsphäre in der Beweisführung.

6.4.2 Verbesserung der Skalierbarkeit

Die Skalierbarkeit des Prototyps kann durch die Anwendung von Sharding-Techniken oder dem Einsatz von Nebenketten (Sidechains) verbessert werden. Diese Ansätze ermöglichen es, die Belastung der Hauptblockchain zu reduzieren, indem Transaktionen und Datenverarbeitungsaufgaben auf mehrere Ketten verteilt werden. Dies kann die Verarbeitungsgeschwindigkeit erhöhen und die Effizienz des Systems verbessern (WeKing et al., 2020).

6.4.3 Entwicklung benutzerfreundlicher Schnittstellen

Die Erweiterung der technischen Lösung umfasst auch die Entwicklung von intuitiven und benutzerfreundlichen Schnittstellen für die Interaktion mit dem CoC-System. Dies kann die Akzeptanz und Anwendbarkeit der Technologie in der Praxis erhöhen, indem es Ermittlern und forensischen Analysten erleichtert wird, Beweismittel zu verwalten und die CoC zu überwachen.

6.4.4 Implementierung von Smart Contracts

Die Anwendung von Smart Contracts in der CoC kann die Automatisierung von Prozessen wie der Verifizierung, dem Transfer und der Speicherung von Beweismitteln ermöglichen. Smart Contracts können vordefinierte Bedingungen und Regeln durchsetzen, was die Effizienz steigert und das Risiko menschlicher Fehler reduziert (Belchior et al., 2019).

6.4.5 Erforschung der Interoperabilität

Die Fähigkeit des CoC-Systems, mit verschiedenen Blockchain-Plattformen und bestehenden forensischen Tools zu interagieren, ist für die breite Anwendung entscheidend. Die Erforschung der Interoperabilität zwischen verschiedenen Blockchain-Netzwerken und der Integration mit traditionellen forensischen Datenbanken ist daher ein wichtiger Schritt in der Weiterentwicklung der technischen Lösung.

6.4.6 Fazit

Die vorgeschlagenen Erweiterungen der technischen Lösung spiegeln das Potenzial der Blockchain-Technologie wider, die Praxis der digitalen Forensik und der CoC nachhaltig zu verändern. Durch die Berücksichtigung von Datenschutz, Skalierbarkeit und Benutzerfreundlichkeit sowie die Integration mit bestehenden forensischen Prozessen kann die Blockchain-Technologie eine robuste, sichere und effiziente Lösung für die Herausforderungen der Beweissicherung bieten.

6.5 Blockchain-Technologie in der digitalen Forensik

6.5 Blockchain-Technologie in der digitalen Forensik

Die Einführung der Blockchain-Technologie in die digitale Forensik markiert einen Wendepunkt in der Art und Weise, wie Beweismittel gesammelt, verwaltet und präsentiert werden. Durch ihre Fähigkeit, Unveränderlichkeit, Transparenz und Nachverfolgbarkeit zu garantieren, bietet die Blockchain das Potenzial, die Authentizität und Integrität digitaler Beweismittel signifikant zu verbessern.

6.5.1 Potenziale und Anwendungen

Die Anwendung der Blockchain in der digitalen Forensik erstreckt sich über verschiedene Bereiche, einschließlich der Chain of Custody (CoC), der Beweissicherung und der Identitätsverifizierung. Wie von Pilkington (2016) und Yan et al. (2020) diskutiert, ermöglicht die Blockchain eine lückenlose Aufzeichnung der Beweishistorie, wodurch jeder Schritt im Umgang mit dem Beweismittel nachvollziehbar wird. Darüber hinaus kann die Blockchain-Technologie zur Entwicklung von sicheren digitalen Identitäten beitragen, was besonders relevant ist, um die Herkunft digitaler Beweismittel zu verifizieren.

6.5.2 Herausforderungen

Trotz der offensichtlichen Vorteile sind mit der Implementierung der Blockchain-Technologie in die digitale Forensik auch Herausforderungen verbunden. Dazu gehören

Fragen der Skalierbarkeit, der Kompatibilität mit bestehenden forensischen Werkzeugen und der rechtlichen Anerkennung von blockchain-gesicherten Beweismitteln. WeKing et al. (2020) und Belchior et al. (2019) weisen auf die Notwendigkeit hin, bestehende rechtliche Rahmenbedingungen anzupassen, um die neuen Technologien vollständig integrieren zu können.

6.5.3 Zukünftiger Forschungsbedarf

Die fortlaufende Evolution der Blockchain-Technologie und ihre Anwendung in der digitalen Forensik erfordern kontinuierliche Forschung. Zukünftige Studien sollten sich auf die Entwicklung von Standards für die Verwendung von Blockchain in der Forensik, die Untersuchung der Interoperabilität zwischen Blockchain-Plattformen und traditionellen forensischen Werkzeugen sowie die Bewertung der Auswirkungen auf die Privatsphäre konzentrieren. Besonders relevant sind hier die Arbeiten von Bonomi et al. (2020), die eine blockchainbasierte CoC für das Management digitaler Beweise vorstellen, und von Aouidef et al. (2021), die die Potenziale und Herausforderungen von Blockchain in der Online-Streitbeilegung analysieren.

6.6 Forschungsbedarf

Die Untersuchung der Blockchain-Technologie in der digitalen Forensik hat wichtige Erkenntnisse und Perspektiven für die zukünftige Forschung aufgedeckt. Um die Potenziale der Blockchain voll auszuschöpfen und ihre Integration in forensische Prozesse zu optimieren, sind weitere Forschungsarbeiten in mehreren Schlüsselbereichen erforderlich.

6.6.1 Entwicklung von Interoperabilitätsstandards

Die Fähigkeit unterschiedlicher Blockchain-Systeme, nahtlos miteinander zu interagieren, ist für die effektive Anwendung in der digitalen Forensik von entscheidender Bedeutung. Zukünftige Forschungsarbeiten sollten sich auf die Entwicklung von Standards konzentrieren, die die Interoperabilität zwischen verschiedenen Blockchain-Plattformen und den traditionellen forensischen Tools sicherstellen. Solche Standards würden die Übernahme der Blockchain-Technologie in bestehende forensische Prozesse erleichtern und ihre Effektivität bei der Beweisführung verbessern.

6.6.2 Rechtliche Rahmenbedingungen und Anerkennung

Die rechtliche Anerkennung von durch Blockchain gesicherten Beweismitteln stellt eine erhebliche Herausforderung dar. Es bedarf weiterer Forschungsarbeiten, um die rechtlichen Rahmenbedingungen zu definieren, die die Verwendung von Blockchain in

der Beweissicherung und im Gerichtsverfahren regeln. Diese Forschung sollte sich auf die Entwicklung von Richtlinien konzentrieren, die die Integrität und Authentizität von blockchain-gesicherten Beweisen gewährleisten und ihre Anerkennung in rechtlichen Verfahren erleichtern.

6.6.3 Verbesserung der Skalierbarkeit und Effizienz

Die Skalierbarkeit von Blockchain-Systemen ist eine wesentliche Herausforderung, die ihre Anwendbarkeit in der digitalen Forensik beeinträchtigt. Zukünftige Forschungsinitiativen sollten sich darauf konzentrieren, innovative Lösungen zur Verbesserung der Skalierbarkeit und Effizienz von Blockchain-Systemen zu entwickeln. Dies könnte die Erforschung neuer Konsensmechanismen, die Optimierung von Blockchain-Protokollen und die Anwendung von Techniken wie Sharding und Sidechains umfassen.

6.6.4 Datenschutz und ethische Überlegungen

Der Schutz personenbezogener Daten und die Berücksichtigung ethischer Prinzipien sind entscheidend für die Anwendung der Blockchain-Technologie in der digitalen Forensik. Zukünftige Forschungsarbeiten sollten sich mit der Entwicklung von Mechanismen befassen, die den Datenschutz gewährleisten und gleichzeitig die Integrität und Transparenz der Beweiskette aufrechterhalten. Dies umfasst die Untersuchung von Ansätzen wie der Anonymisierung von Daten, der Verwendung von Privacy Coins und der Implementierung von Zero-Knowledge-Proofs.

6.6.5 Praktische Implementierung und Testung

Schließlich ist es notwendig, die praktische Implementierung und Testung von blockchain-basierten Lösungen in der digitalen Forensik weiter voranzutreiben. Experimentelle Prototypen und Pilotprojekte können wertvolle Einblicke in die Machbarkeit, Leistung und Anwendbarkeit von Blockchain-Systemen in realen forensischen Szenarien liefern. Diese praktischen Erfahrungen sind entscheidend, um die Technologie weiterzuentwickeln und ihre Effektivität in der Beweissicherung zu validieren.

7 Fazit und Ausblick

Die eingehende Untersuchung des Einsatzes der Blockchain-Technologie in der digitalen Forensik, speziell im Kontext der Chain of Custody (CoC), hat deren transformative Kraft deutlich gemacht. Die Bereitstellung einer unveränderlichen, transparenten und sicheren Methode zur Verfolgung digitaler Beweise positioniert die Blockchain als eine zukunftsweisende Lösung für bestehende Herausforderungen innerhalb der digitalen Forensik.

7.1 Fazit

Die Forschung und Entwicklung des Prototyps innerhalb dieser Arbeit unterstreichen die praktische Anwendbarkeit der Blockchain-Technologie zur Stärkung der CoC in forensischen Verfahren. Durch die Sicherstellung der Integrität und Authentizität digitaler Beweise kann die Blockchain das Vertrauen in forensische Untersuchungen festigen und somit einen bedeutenden Beitrag zur Gerechtigkeitswahrung leisten. Dennoch hat die Diskussion auch gezeigt, dass die Implementierung dieser Technologie mit verschiedenen Herausforderungen verknüpft ist, besonders hinsichtlich rechtlicher Rahmenbedingungen, der Skalierbarkeit und des Datenschutzes.

Diese Arbeit beleuchtet die kritische Rolle der CoC innerhalb der digitalen Forensik und bietet durch die Einbeziehung von Kryptologieprinzipien, wie sie von Beutelspacher (2015) dargelegt wurden, einen fundierten Einblick in Möglichkeiten zur Verbesserung der Sicherheitspraktiken. Die Implementierung technischer Maßnahmen, wie Hashing und Protokollierung, liefert einen soliden Ansatz zur Gewährleistung der Beweisintegrität. Parallel dazu hebt die Anwendung der Blockchain-Technologie das revolutionäre Potenzial hervor, die CoC durch eine dezentralisierte, transparente und manipulationssichere Dokumentation zu stärken.

7.2 Ausblick

Die Zukunft der Blockchain-Technologie in der digitalen Forensik ist vielversprechend, erfordert jedoch weiterführende Forschung und Entwicklung, um ihre volle Effektivität zu entfalten. Die Etablierung von Interoperabilitätsstandards, die Anpassung rechtlicher Rahmenbedingungen und die fortlaufende Verbesserung der Technologie sind entscheidend, um ihre praktische Anwendung zu erleichtern. Die Exploration von Datenschutzmechanismen spielt ebenfalls eine wesentliche Rolle, um ein Gleichgewicht

zwischen der Sicherung von Beweisen und dem Schutz persönlicher Daten zu gewährleisten.

Die vorliegende Arbeit legt einen umfassenden Überblick über die aktuelle Situation der CoC in digitalen Forensikprozessen vor und setzt einen Meilenstein für zukünftige Entwicklungen in diesem Bereich. Die Sicherung der CoC bleibt ein zentrales Anliegen der digitalen Forensik, um die Glaubwürdigkeit und Verwertbarkeit digitaler Beweismittel in juristischen Verfahren zu gewährleisten. Die kontinuierliche Anpassung an neue technologische Entwicklungen und die Integration interdisziplinärer Forschungsansätze sind maßgeblich, um diesen Herausforderungen effektiv zu begegnen.

Zusammenfassend bietet diese Arbeit einen detaillierten Einblick in die Bedeutung und die Umsetzung der CoC in der digitalen Forensik, betont die Relevanz der Blockchain-Technologie als innovatives Instrument zur Beweissicherung und legt den Grundstein für weiterführende Forschungsarbeiten in diesem dynamischen und entscheidenden Feld der digitalen Forensik.

8. Anhang

In diesem Abschnitt werden zusätzliche Informationen, Daten und Materialien aufgeführt, die im Verlauf der Arbeit erwähnt oder verwendet wurden. Dies kann die Reproduzierbarkeit der Forschungsergebnisse verbessern und dem Leser einen tieferen Einblick in die durchgeführten Analysen geben.

A Code des Prototyps

Der folgende Code stellt den Kern des Prototyps dar, der für die Demonstration der Chain of Custody (CoC) im Rahmen dieser Arbeit entwickelt wurde. Der Prototyp illustriert, wie Hashwerte zur Sicherung der Integrität digitaler Beweismittel generiert, Änderungen protokolliert und die Unversehrtheit der Daten überprüft werden kann.

Voraussetzungen

- Python 3.x
- SQLite3 (in Python standardmäßig enthalten)

Code-Struktur

Der Code umfasst drei Hauptfunktionen:

1. **generate_hash**: Generiert den SHA-256 Hashwert einer Datei.
2. **log_change**: Protokolliert Änderungen an Dateien in einer SQLite-Datenbank.
3. **verify_integrity**: Überprüft die Integrität einer Datei anhand des gespeicherten Hashwerts.

Quellcode des Prototyps:

```
import hashlib
import sqlite3
from datetime import datetime
import os
import getpass  # For user authentication
import tkinter as tk
from tkinter import filedialog
from tkinter import messagebox

# Initialize GUI for file selection and user feedback
root = tk.Tk()
root.withdraw()  # Hide the main window

# User Authentication
```

```
def user_authentication():
    username = input("Enter username: ")
    password = getpass.getpass("Enter password: ")
    # Implement database check or other authentication mechanism here
    # Placeholder logic
    if username == "sayed" and password == "forensikguy":
        messagebox.showinfo("Authentication", "Authentication
Successful!")
        return True
    else:
        messagebox.showerror("Authentication", "Authentication Failed!")
        return False

# Initialize database with error handling
def init_db():
    try:
        conn = sqlite3.connect('cochain.db')
        cursor = conn.cursor()
        cursor.execute('''
            CREATE TABLE IF NOT EXISTS file_changes (
                id INTEGER PRIMARY KEY,
                file_path TEXT NOT NULL,
                action TEXT NOT NULL,
                hash TEXT NOT NULL,
                user TEXT NOT NULL,
                timestamp DATETIME DEFAULT CURRENT_TIMESTAMP
            )
        ''')
        conn.commit()
    except sqlite3.Error as e:
        messagebox.showerror("Database Error", f"An error occurred: {e}")
    finally:
        conn.close()

# Generate SHA-256 hash value for a given file path
def generate_hash(file_path):
    try:
        hasher = hashlib.sha256()
        with open(file_path, 'rb') as file:
            buf = file.read()
            hasher.update(buf)
        return hasher.hexdigest()
    except Exception as e:
        messagebox.showerror("Hashing Error", f"An error occurred while
generating hash for {file_path}: {e}")
        return None
```

```
# Log changes to both database and a text file
def log_changes(file_paths, action, user):
    for file_path in file_paths:
        hash_value = generate_hash(file_path)
        if hash_value:
            try:
                # Log to database
                conn = sqlite3.connect('cochain.db')
                cursor = conn.cursor()
                cursor.execute('''
                    INSERT INTO file_changes (file_path, action, hash,
user)
                    VALUES (?, ?, ?, ?)
                ''', (file_path, action, hash_value, user))
                conn.commit()
                # Log to text file
                with open('change_log.txt', 'a') as log_file:
                    log_file.write(f"{datetime.now()}: {action} performed
on {file_path} by {user}, Hash: {hash_value}\n")
            except sqlite3.Error as e:
                messagebox.showerror("Logging Error", f"An error occurred
while logging changes: {e}")
            finally:
                conn.close()

# Verify the integrity of files
def verify_integrity(file_path):
    try:
        current_hash = generate_hash(file_path)
        conn = sqlite3.connect('cochain.db')
        cursor = conn.cursor()
        cursor.execute('''
            SELECT hash FROM file_changes
            WHERE file_path = ?
            ORDER BY timestamp DESC
            LIMIT 1
        ''', (file_path,))
        row = cursor.fetchone()
        if row and row[0] == current_hash:
            messagebox.showinfo("Integrity Check", "The integrity of the
file is intact.")
        else:
            messagebox.showwarning("Integrity Check", "Warning: The
integrity of the file might be compromised.")
    except sqlite3.Error as e:
```

```
        messagebox.showerror("Integrity Verification Error", f"An error
occurred during integrity verification: {e}")
    finally:
        conn.close()

# Main function to orchestrate the CoC process
if __name__ == '__main__':
    if user_authentication():
        init_db()
        file_paths = filedialog.askopenfilenames(title="Select files to
monitor")  # File selection dialog
        user = 'forensic_user'  # Replace with actual user from
authentication
        log_changes(file_paths, 'Creation', user)
        for file_path in file_paths:
            verify_integrity(file_path)
```

Hinweise zur Ausführung

- Vor der ersten Ausführung des Codes muss die Datei, deren Integrität überwacht werden soll, im selben Verzeichnis wie das Skript vorhanden sein.
- Der Code protokolliert jede Änderung an der Datei und speichert den aktuellen Hashwert zusammen mit einem Zeitstempel in der Datenbank.
- Die Funktion **verify_integrity** überprüft die Integrität der Datei, indem sie den aktuellen Hashwert, mit dem zuletzt in der Datenbank gespeicherten vergleicht.

B Anleitungen zur Installation und Konfiguration

Diese Anleitung führt durch die notwendigen Schritte zur Installation und Konfiguration der Umgebung, die für die Ausführung des Prototyps erforderlich ist. Der Prototyp wurde in Python entwickelt und nutzt SQLite für die Datenhaltung.

Voraussetzungen

Um den Prototyp erfolgreich auszuführen, müssen folgende Voraussetzungen erfüllt sein:

- Python 3.x ist installiert.
- Ein Texteditor oder eine integrierte Entwicklungsumgebung (IDE) für Python-Code ist verfügbar (optional, aber empfohlen).
- Grundlegende Kenntnisse im Umgang mit der Kommandozeile oder Terminal.

Schritt 1: Installation von Python

Wenn Python noch nicht installiert ist, kann es von der offiziellen Website heruntergeladen und installiert werden:

1. Besuchen Sie die offizielle Python-Website: https://www.python.org/
2. Laden Sie die neueste Python 3-Version für Ihr Betriebssystem herunter.
3. Führen Sie das Installationsprogramm aus und folgen Sie den Anweisungen. Stellen Sie sicher, dass Sie die Option wählen, um Python zum PATH hinzuzufügen.

Schritt 2: Vorbereitung der Umgebung

1. **Erstellen eines Projektverzeichnisses**: Erstellen Sie ein Verzeichnis auf Ihrem Computer, in dem Sie den Prototyp speichern möchten.

```
mkdir cochain_prototyp
cd cochain_prototyp
```

Erstellen einer virtuellen Umgebung (optional): Es wird empfohlen, eine virtuelle Umgebung zu verwenden, um die Abhängigkeiten des Projekts von anderen Python-Projekten zu isolieren.

```
python3 -m venv venv
```

1. Aktivieren Sie die virtuelle Umgebung:
    - Windows: **venv\Scripts\activate**
    - macOS/Linux: **source venv/bin/activate**

Schritt 3: Ausführen des Prototyps

1. **Kopieren des Prototyp-Codes**: Kopieren Sie den Code des Prototyps (siehe Anhang A) in eine Datei namens **cochain.py** in Ihrem Projektverzeichnis.
2. **Ausführen des Skripts**: Öffnen Sie die Kommandozeile oder das Terminal, navigieren Sie zu Ihrem Projektverzeichnis und führen Sie das Skript aus:

```
python cochain.py
```

Schritt 4: Nutzung des Prototyps

Nach dem Ausführen des Skripts wird der Prototyp gemäß den im Code definierten Funktionen agieren. Sie können den Code anpassen, um verschiedene Aktionen (z.B. Erstellung, Bearbeitung) zu simulieren und die Integritätsprüfung für die Datei durchzuführen.

Fehlerbehebung

Sollten beim Ausführen des Skripts Fehler auftreten, überprüfen Sie die folgenden Punkte:

- Stellen Sie sicher, dass Python korrekt installiert und im PATH enthalten ist.
- Überprüfen Sie, ob Sie sich in der richtigen virtuellen Umgebung befinden (falls verwendet).
- Stellen Sie sicher, dass alle Pfade korrekt im Skript angegeben sind.

Literaturverzeichnis

Aouidef, Y., Ast, F., & Deffains, B. (2021). Decentralized Justice: A Comparative Analysis of Blockchain Online Dispute Resolution Projects. *Frontiers in Blockchain, 4*. https://doi.org/10.3389/fbloc.2021.564551

Belchior, R., Correia, M., & Vasconcelos, A. (2019). JusticeChain: Using blockchain to protect justice logs. In *Lecture Notes in Computer Science* (Vol. 11877 LNCS, pp. 318–325). Springer. https://doi.org/10.1007/978-3-030-33246-4_21

Beutelspacher, A. (2015). *Kryptologie: Eine Einführung in die Wissenschaft vom Verschlüsseln, Verbergen und Verheimlichen*. Wiesbaden: Vieweg+Teubner Verlag.

Bundesnetzagentur. (2021). *Einführung in die Blockchain-Technologie*. Verfügbar unter: https://www.bundesnetzagentur.de/DE/Fachthemen/Digitalisierung/Technologien/Blockchain/Links_Dokumente/einfuehrung_bc.pdf?__blob=publicationFile&v=1

Bonomi, S., Casini, M., & Ciccotelli, C. (2020). B-CoC: A blockchain-based chain of custody for evidences management in digital forensics. In *OpenAccess Series in Informatics* (Vol. 71). Schloss Dagstuhl-Leibniz-Zentrum für Informatik. https://doi.org/10.4230/OASIcs.Tokenomics.2019.12

Dierksmeier, C., & Seele, P. (2020). Blockchain and business ethics. *Business Ethics, 29*(2), 348–359. https://doi.org/10.1111/beer.12259

Carrier, B. (2005). *File System Forensic Analysis*. Addison-Wesley Professional. https://www.oreilly.com/library/view/file-system-forensic/0321268172/

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet* (3rd ed.). Academic Press. https://booksite.elsevier.com/samplechapters/9780123742681/Front_Matter.pdf

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access, 4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation, 2*, 6–10. Verfügbar unter: https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf

ENISA. (2020). *Threat Landscape for Blockchain Technologies*. Verfügbar unter: https://www.enisa.europa.eu/publications/blockchain-security

Gallo, P., De Santis, A., & Romano, L. (2024). Ensuring the Chain of Custody of Digital Evidence with Blockchain. Elsevier. Verfügbar unter: https://www.researchgate.net/publication/377628547_The_Application_of_Blockchain_to_the_Chain_Of_Custody_of_Judicial_Evidence

ISO/IEC. (2012). ISO/IEC 27037:2012 Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. International Organization for Standardization. Verfügbar unter: https://www.iso.org/standard/44381.html

Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation, 28*, 44–55. https://doi.org/10.1016/j.diin.2019.01.002

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Decentralized Business Review*. Verfügbar unter: https://bitcoin.org/bitcoin.pdf

NIST. (2012). *NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response*. National Institute of Standards and Technology. Verfügbar unter: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf

Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*. Edward Elgar Publishing. https://doi.org/10.4337/9781784717766.00019

Fraunhofer FIT. (2021). "Blockchain - Grundlagen, Anwendungen und Potenziale". Verfügbar unter: https://www.fit.fraunhofer.de/content/dam/fit/de/documents/Blockchain_WhitePaper_Grundlagen-Anwendungen-Potentiale.pdf

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence, 1*(3). Verfügbar unter: https://utica.edu/academic/institutes/ecii/publications/articles/A0B0C286-DFA4-8D1E-2F2F6C24AC2AD7E3.pdf

Swan, M. (2021). *Blockchain: Blueprint for a New Economy*. O'Reilly Media. Verfügbar unter: https://www.oreilly.com/library/view/blockchain/9788328359215/

WeKing, J., Mandalenakis, M., Hein, A., Hermes, S., Böhm, M., & Krcmar, H. (2020). The impact of blockchain technology on business models – a taxonomy and archetypal patterns. *Electronic Markets, 30*(2), 285–305. https://doi.org/10.1007/s12525-019-00386-3

Yan, W., Shen, J., Cao, Z., & Dong, X. (2020). Blockchain Based Digital Evidence Chain of Custody in Cloud Storage. In *ACM International Conference Proceeding Series* (pp. 19–23). ACM. https://doi.org/10.1145/3390566.3391690

Tsai, H.-C., Sie, S.-H., & Huang, C.-Y. (2021). The Application of Blockchain to the Chain of Custody of Judicial Evidence. *Journal of Forensic and Legal Medicine, 76*, 102021. https://doi.org/10.1016/j.procs.2021.09.048

Rani, D., Singh Gill, N., & Gulia, P. (2024). A forensic framework to improve digital image evidence administration in IIoT - ScienceDirect. https://doi.org/10.1016/j.jii.2024.100568

T. M. Palmbach, Crime Scene Investigation and Examination: Chain of Evidence, vol. 1. Elsevier Ltd., 2015. https://doi.org/10.1016/B978-0-12-800034-2.00100-2

Gallo, H. B. P. de, Medina, O. C., Dorado, J. G., Fleming, J. A., Párraga, C., Notario, E. R., & Sanchez, E. (2024). The Application of Blockchain to the Chain Of Custody of Judicial Evidence. Verfügbar unter: https://cms.digilab.ucasal.edu.ar/uploads/The_Application_of_Blockchain_to_the_Chain_of_Custody_of_Judicial_Evidence_EN_Ver_3_f2b69b6dca.pdf