HAW HAMBURG

**BACHELORARBEIT**

# Eine interdisziplinäre Analyse forensischer Methoden zur Rückverfolgung von Blockchain-Transaktionen

vorgelegt am 15. September 2025

Cem Aslan

Erstprüfer: Prof. Dr. Nils Martini
Zweitprüfer: Prof. Dr. Robert Mores

**HOCHSCHULE FÜR ANGEWANDTE WISSENSCHAFTEN HAMBURG**
Department Medientechnik
Finkenau 35
20081 Hamburg

## Zusammenfassung

Kryptowährungen wie Bitcoin und Ethereum haben innerhalb weniger Jahre eine bemerkenswerte Verbreitung erreicht. Im Dezember 2024 überschritt ihr Gesamtmarktwert einen Rekordwert von 3,91 Billionen US-Dollar [29]. Auch im Jahr 2025 bleiben sie trotz erheblicher Kursvolatilität ein fester Bestandteil des digitalen Finanzsystems. Diese Entwicklung bringt zugleich neue Herausforderungen für Strafverfolgungsbehörden und Regulierungsinstanzen mit sich - insbesondere bei der Nachverfolgung krimineller Geldflüsse im digitalen Raum.

Diese Arbeit untersucht die technischen, rechtlichen und ethischen Rahmenbedingungen der Rückverfolgbarkeit von Blockchain-Transaktionen. Für die Analyse wurden 50 Quellen herangezogen, darunter einschlägige wissenschaftliche Publikationen und empirische Fallstudien.

Die Ergebnisse zeigen, dass eine Kombination forensischer Methoden – darunter Clusteranalysen, graphbasierte Auswertungen und die Integration externer Informationsquellen – bei etablierten Kryptowährungen wie Bitcoin eine Identifikation verdächtiger Transaktionsmuster mit einer Erfolgsquote von bis zu 69 % ermöglicht [4]. Im Vergleich dazu weisen sogenannte Privacy Coins wie Monero oder Zcash aufgrund ihrer spezifischen Verschleierungstechniken eine deutlich geringere Identifizierungsrate von unter 20 % auf [14].

Auch rechtliche Vorgaben spielen eine zentrale Rolle. Die Datenschutz-Grundverordnung (DSGVO), die Richtlinien der Financial Action Task Force (FATF) sowie die europäische Marktregulierung für Krypto-Assets (MiCA) setzen klare Grenzen für die technische Umsetzung forensischer Analysen. Sie definieren Anforderungen an die Transparenz, Datensicherheit und die rechtskonforme Verarbeitung personenbezogener Daten.

Die Blockchain-Forensik stellt ein vielversprechendes Instrument zur Bekämpfung digitaler Kriminalität dar, doch ihre Möglichkeiten sind aufgrund der hohen Komplexität und ständigen Weiterentwicklung der Technologien begrenzt. Um sicherzustellen, dass entsprechende Analysen rechtlich abgesichert, gerecht und wirksam sind/bleiben, ist es notwendig, hierbei Technik, Recht und Ethik in der Zukunft noch enger miteinander zu verknüpfen.

## Abstract

Cryptocurrencies such as Bitcoin and Ethereum have achieved remarkable adoption within just a few years. In December 2024, their total market capitalization reached a record high of USD 3.91 trillion [29]. Despite significant price volatility, they remain a core component of the digital financial system in 2025. This development presents new challenges for law enforcement agencies and regulatory bodies—particularly in tracing illicit financial flows in digital environments.

This thesis examines the technical, legal, and ethical frameworks surrounding the traceability of blockchain transactions. The analysis is based on 50 sources, including relevant scientific publications and empirical case studies.

Findings indicate that a combination of forensic techniques - including cluster analysis, graph-based evaluations, and the integration of external data sources - can achieve identification rates of up to 69% for suspicious transaction patterns in established cryptocurrencies like Bitcoin [4]. In contrast, privacy-focused coins such as Monero and Zcash, due to their specific obfuscation mechanisms, show significantly lower identification rates of less than 20% [14].

Legal regulations also play a crucial role. The General Data Protection Regulation (GDPR), the guidelines of the Financial Action Task Force (FATF), and the European Markets in Crypto-Assets Regulation (MiCA) impose clear boundaries on the technical implementation of forensic analyses. They define requirements for transparency, data security, and the lawful processing of personal data.

Blockchain forensics represents a promising tool in combating digital crime, yet its capabilities remain limited. To ensure that analyses are legally sound, ethically justified, and practically effective, it is essential to further integrate technology, law, and ethics in future developments.

## Inhaltsverzeichnis

# Abbildungsverzeichnis



# Tabellenverzeichnis

# Abkürzungsverzeichnis

| Abkürzung | Beschreibung |
|---|---|
| ABI | Application Binary Interface |
| Abs. | Absatz |
| ACM | Association for Computing Machinery |
| AML | Anti-Money Laundering (Geldwäschebekämpfung) |
| AMLD5 | Fünfte EU-Geldwäscherichtlinie |
| AMM | Automated Market Maker |
| APIs | Application Programming Interfaces |
| BTC | Bitcoin |
| BTCParse | Tool oder Bibliothek zur Analyse von Bitcoin-Daten |
| Bzw. | Beziehungsweise |
| CASPs | Crypto-Asset Service Providers |
| CBDCs | Central Bank Digital Currencies |
| DAGs | Directed Acyclic Graphs |
| DeFi | Decentralized Finance (dezentralisierte Finanzmärkte) |
| DEXs | Decentralized Exchanges |
| DPIAs | Data Protection Impact Assessments |
| DPoS | Delegated Proof of Stake |
| DSGVO | Datenschutz-Grundverordnung |
| EOS | Enterprise Operation System / Blockchain-Projekt |
| ERC | Ethereum Request for Comments |
| ERC-20 | Ethereum Request for Comments 20 |
| ERL | Energy Recovery Linac / Environmental Research Laboratory |
| et al. | und andere |
| ETH | Ether |
| EUROPOL | Europäisches Polizeiamt |
| FATF | Financial Action Task Force |
| FBI | Federal Bureau of Investigation |
| FTX | Ehemalige Kryptobörse |
| GCNs | Graph Convolutional Networks |
| GDPR | General Data Protection Regulation |
| HTLCs | Hashed TimeLock Contracts |
| IEEE | Institute of Electrical and Electronics Engineers |
| IEEPA | International Emergency Economic Powers Act |
| IP | Internet Protocol |
| KI | Künstliche Intelligenz |
| KYC | Know Your Customer |
| KYT | Know Your Transaction |
| LIME | Local Interpretable Model-Agnostic Explanations |
| MiCA | Märkte für Kryptowerte (EU-Verordnung); engl. Markets in Crypto-Assets |
| Mio. | Million(en) |
| MLATs | Mutual Legal Assistance Treaties |
| NFTs | Non-Fungible Tokens |
| OFAC | Office of Foreign Assets Control |

| Abkürzung | Beschreibung |
|---|---|
| OSINT | Open Source Intelligence |
| PBFT | Practical Byzantine Fault Tolerance |
| PETs | Privacy-Enhancing Technologies |
| PoH | Proof of History (Konsensmechanismus bei Solana) |
| PoS | Proof of Stake |
| PoW | Proof of Work |
| pp. | Seitenangabe |
| SHA-256 | Secure Hash Algorithm 256-bit |
| SHAP | SHapley Additive exPlanations |
| SNARKs | Succinct Non-Interactive Argument of Knowledge |
| t-addrs | Transparent Addresses (Zcash) |
| THORChain | ezentraler Cross-Chain-Swap-Protokoll |
| TKG | Telekommunikationsgesetz |
| TMS | Transaction Monitoring Systems |
| TRM Labs | Unternehmen im Bereich Blockchain-Intelligenz |
| TRON | Blockchain-Plattform für dezentrale Anwendungen |
| USD | United States Dollar |
| UTXOs | Unspent Transaction Outputs |
| Vs. | Versus |
| WBTC | Wrapped Bitcoin |
| XAI | Explainable Artificial Intelligence |
| XRP | Kryptowährung von Ripple |
| zk | Zero-Knowledge |

# 1. Einleitung

## 1.1. Problemstellung und Relevanz

Die rasante Entwicklung der Blockchain-Technologie und die zunehmende Verbreitung von Kryptowährungen haben das globale Finanzsystem seit 2009 grundlegend verändert. Das explosive Marktwachstum, das im Dezember 2024 einen Höchststand von knapp 4 Billionen US-Dollar erreichte [29], verdeutlicht die ökonomische Relevanz dieser digitalen Vermögenswerte. Gleichzeitig zeigen Untersuchungen von Paquet-Cluston et al. von 2018 [22], dass allein im Zusammenhang mit Ransomware-Zahlungen von 2013 bis 2017 ein Transaktionsvolumen von mindestens 12,8 Millionen US-Dollar generiert wurde. Dies ist ein Hinweis auf die wachsende Bedeutung krimineller Aktivitäten im Krypto-Sektor. Ereignisse wie der Zusammenbruch der Handelsplattform FTX im Jahr 2022 [30] und die darauffolgende Markterholung in den Jahren 2024 und 2025 haben die regulatorischen Rahmenbedingungen in erheblichem Maße beeinflusst. Dies hat bei den zuständigen Aufsichtsbehörden, politischen Entscheidungsträgern und internationalen Organisationen zu einer verstärkten Auseinandersetzung mit der Frage geführt, wie digitale Vermögenswerte rechtlich und sicherheitsrelevant zu kontrollieren sind.

Die missbräuchliche Nutzung von Kryptowährungen rückt seit 2017 zunehmend in den Fokus von politischen Entscheidungsträgern, Strafverfolgungsbehörden und der wissenschaftlichen Forschung. Zwar bieten dezentrale Blockchain-Systeme den Nutzerinnen und Nutzern Vorteile wie Transparenz, Sicherheit und Zensurresistenz, doch eröffnen sie zugleich neue Möglichkeiten für illegale Aktivitäten wie Geldwäsche, Cyberkriminalität und Terrorismusfinanzierung. Die pseudonyme Struktur vieler Blockchains erschwert klassische Ermittlungsansätze maßgeblich, da diese auf eindeutig identifizierbare Kontodaten angewiesen sind. Daraus ergibt sich für Ermittlungsbehörden und forensische Expertinnen und Experten die Notwendigkeit, spezialisierte forensische Methoden zu entwickeln, die den Besonderheiten digitaler Transaktionssysteme gerecht werden.

Staatliche Institutionen und Ermittlungsbehörden stehen vor der Herausforderung, Blockchain-Transaktionen systematisch zu analysieren und verdächtige Aktivitäten frühzeitig zu erkennen - unter strikter Beachtung datenschutz- und verfassungsrechtlicher Grundsätze.

Die zuvor skizzierte Thematik ist nicht nur technisch relevant, sondern wirft auch tiefgreifende juristische, regulatorische und ethische Fragen auf, insbesondere im Hinblick auf die digitale Überwachung dezentraler Strukturen. Während sich die bisherige Forschung häufig auf einzelne Teilaspekte der Blockchain-Technologie wie technische Verfahren oder rechtliche Rahmenbedingungen konzentriert, verfolgt diese Arbeit einen interdisziplinären Ansatz. Das Ziel dabei ist, technologische Entwicklungen mit juristischen und ethischen Überlegungen zu

verknüpfen, um die Möglichkeiten und Grenzen der Blockchain-Forensik umfassend zu analysieren und aufzuzeigen.

## 1.2. Zielsetzung

Vor dem Hintergrund der zunehmenden Relevanz von Kryptowährungen und den damit verbundenen Herausforderungen für die Strafverfolgung und Regulierung verfolgt diese Arbeit das Ziel, forensische Methoden zur Analyse von Blockchain-Transaktionen interdisziplinär zu untersuchen. Im Fokus stehen dabei technische Verfahren, rechtliche Rahmenbedingungen und ethische Implikationen.

Ein zentraler Schwerpunkt liegt auf der detaillierten Darstellung und kritischen Bewertung etablierter Analyseverfahren wie heuristischen Ansätzen, Clustering-Algorithmen und graphbasierten Netzwerkanalysen. Zunächst werden die zuvor genannten Methoden technisch beschrieben sowie anschließend hinsichtlich ihrer Effektivität und praktischen Grenzen anhand exemplarischer Szenarien evaluiert. Besonderes Augenmerk gilt dabei der Frage, inwiefern moderne Technologien zum Schutz der Privatsphäre, etwa CoinJoin, Stealth-Adressen oder Privacy-Coins, die Rückverfolgbarkeit von Transaktionen einschränken oder verhindern können.

Darüber hinaus werden technische Herausforderungen analysiert, die sich durch neue Entwicklungen wie Cross-Chain-Mechanismen, dezentrale Finanzstrukturen und komplexe Interaktionen mit Smart Contracts ergeben. Diese Innovationen stellen etablierte forensische Verfahren wie Adress-Clustering und Transaktionsgraph-Analysen vor erhebliche methodische und technische Limitierungen, deren Tragweite vorliegend differenziert erfasst und bewertet wird.

Ergänzend untersucht die Arbeit die regulatorischen und ethischen Rahmenbedingungen, welche die Anwendung forensischer Analyseverfahren im Blockchain-Kontext bestimmen. Die entsprechende Einordnung erfolgt unter Bezugnahme auf internationale Leitlinien wie die Empfehlungen der FATF, die AMLD5 sowie die EU-Verordnung über MiCA. Datenschutzrechtliche Vorgaben, insbesondere die DSGVO, werden dabei ebenfalls berücksichtigt. Im Zentrum steht die kritische Analyse des Spannungsverhältnisses zwischen staatlicher Überwachungspflicht, dem Schutz der individuellen Privatsphäre und dem Anspruch der Zivilgesellschaft auf digitale Selbstbestimmung.

Neben der theoretischen Betrachtung umfasst die Arbeit empirisch fundierte Fallanalysen, die reale Anwendungsbeispiele forensischer Blockchain-Analysen darstellen. Anhand dokumentierter Kriminalfälle, zum Beispiel des Silk-Road-Komplexes (2013) oder des Bitfinex-Hacks (2016), wird untersucht, wie forensische Werkzeuge in der Praxis funktionieren, welche

typischen Muster sich dabei identifizieren lassen und wo jeweils die methodischen sowie technischen Grenzen liegen.

Das Ziel dieser Arbeit ist, die Blockchain-Forensik als eigenständiges Forschungsfeld mit interdisziplinärem Anspruch zu profilieren. Durch die systematische Verbindung technologischer Effektivität/Effizienz mit rechtlichen Anforderungen und ethischer Reflexion soll ein praxisrelevanter Beitrag zur Weiterentwicklung bestehender Analyseverfahren geleistet werden. Die gewonnenen Erkenntnisse sollen als Orientierungshilfe für Fachleute, Regulatoren und Ermittlungsbehörden im Umgang mit kryptobasierten Transaktionen dienen.

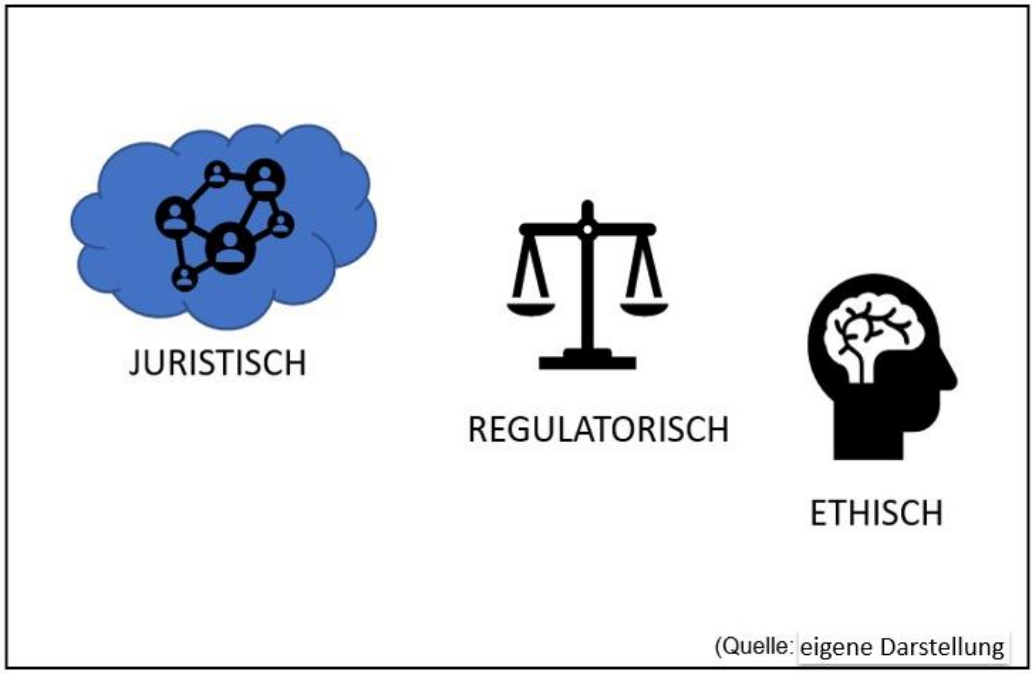


Abbildung 1: Interdisziplinäre Aspekte der Blockchain-Überwachung

Die zuvor dargestellten Zielsetzungen führen zu folgenden zentralen Forschungsfragen:

1. **Methodeneffektivität:** Welche kombinierten forensischen Ansätze erreichen die höchste Identifikationsquote bei Bitcoin- und Ethereum-Transaktionen? Welche quantifizierbaren Leistungsunterschiede bestehen zwischen heuristischen, graphbasierten und KI-gestützten Verfahren?
2. **Privacy-Technologie-Resistenz:** In welchem Umfang reduzieren Anonymisierungstechnologien (CoinJoin, Monero, Tornado Cash) die forensische Erfolgsquote? Welche technischen Gegenstrategien erweisen sich als wirksam?
3. **Regulatorische Rahmenbedingungen:** Wie beeinflussen die DSGVO, MiCA und FATF-Richtlinien die praktische Anwendung forensischer Blockchain-Analysen? Welche ethischen Standards sind hierbei erforderlich?

4. **Praxiserfolg-Determinanten:** Welche Faktoren (Reaktionszeit, KYC-Schnittstellen, internationale Kooperation) korrelieren mit erfolgreicher Rückverfolgungen bei dokumentierten Kriminalfällen?

Die vorliegende Arbeit konzentriert sich auf die forensische Analyse öffentlich zugänglicher Blockchain-Systeme, insbesondere Bitcoin und Ethereum. Private und konsortiale Blockchains wie Hyperledger Fabric oder Corda werden hierbei lediglich am Rande behandelt, da ihre geschlossene Struktur andere forensische Problemstellungen aufwirft. Der rechtliche Fokus liegt auf dem europäischen Rechtsrahmen, insbesondere der DSGVO und der MiCA-Verordnung. Steuerrechtliche Aspekte sowie spezifische Regelungen außereuropäischer Jurisdiktionen bleiben unberücksichtigt, um eine analytische Konzentration und Vertiefung zu ermöglichen.

### 1.3. Methodisches Vorgehen

Die vorliegende Untersuchung basiert auf einer systematischen Literaturrecherche einschlägiger wissenschaftlicher Publikationen, technischer Dokumentationen und aktueller Whitepapers. Als primäre Quellen dienten die wissenschaftlichen Datenbanken IEEE Xplore, ACM Digital Library, SpringerLink und Google Scholar. Ergänzend wurden Praxisquellen führender Blockchain-Forensik-Unternehmen berücksichtigt, um den aktuellen Stand angewandter Technologien einzubeziehen.

Zur Validierung der theoretischen Erkenntnisse wurde eine Fallstudienanalyse durchgeführt. Die Auswahl der Fälle erfolgte nach folgenden Kriterien:

- öffentliche Dokumentation mit verifizierbaren Quellen
- abgeschlossene Ermittlungs- oder Gerichtsverfahren
- Einsatz verschiedener forensischer Analyseverfahren
- Repräsentation unterschiedlicher Kriminalitätsformen (u. a. Ransomware, Darknet-Marktplätze, Exchange-Hacks, Geldwäsche)
- geographische Diversität der jeweiligen Jurisdiktionen

Auf dieser Grundlage erfolgen eine systematische Bewertung bestehender Methoden, die Identifikation technischer und rechtlicher Herausforderungen sowie die Diskussion möglicher Weiterentwicklungen.

Die regulatorische und ethische Einordnung basiert, wie zuvor erwähnt, auf der Analyse einschlägiger europäischer Rechtsnormen, insbesondere der DSGVO, der AMLD5 und der MiCA. Darüber hinaus werden internationale Richtlinien wie die Empfehlungen der FATF berücksichtigt. Die methodische Herangehensweise verknüpft somit die technische Analyse mit juristischer Bewertung und ethischer Reflexion.

Die Untersuchung stützt sich ausschließlich auf öffentlich zugängliche Quellen und dokumentierte Fallstudien. Vertrauliche Ermittlungstechniken staatlicher Behörden sowie proprietäre Analysealgorithmen kommerzieller Anbieter bleiben bewusst unberücksichtigt. Eine empirische Validierung durch eigene forensische Analysen erfolgt nicht, wodurch eine potenzielle Unterschätzung der tatsächlichen forensischer Kapazitäten möglich ist. Zudem kann die hohe Innovationsgeschwindigkeit im Bereich der Blockchain-Technologie und forensischer Gegenmaßnahmen dazu führen, dass einzelne Erkenntnisse rasch an Aktualität verlieren.

### 1.4. Aufbau der Arbeit

Die vorliegende Arbeit gliedert sich in sieben Kapitel, die systematisch aufeinander aufbauen und sowohl technische als auch juristische Aspekte der Blockchain-Forensik beleuchten:

- **Kapitel 2** behandelt die technologischen Grundlagen von Blockchain-Systemen. Im Fokus stehen dabei relevante Konsensmechanismen, Transaktionsmodelle und Anonymitätskonzepte, die als technische Basis für die nachfolgende forensische Analyse dienen.
- **Kapitel 3** stellt zentrale forensische Analyseansätze vor. Dazu zählen heuristische Verfahren, graphbasierte Netzwerkanalysen sowie Methoden zur Entanonymisierung pseudonymer Adressen.
- **Kapitel 4** widmet sich aktuellen Herausforderungen, die durch den Einsatz fortschrittlicher Technologien wie Privacy-Mechanismen (z. B. CoinJoin, ZK-Snarks), Cross-Chain-Protokolle und DeFi entstehen. Die forensischen Implikationen dieser Entwicklungen sowie bestehende methodische und technische Limitierungen werden dabei kritisch untersucht.
- **Kapitel 5** präsentiert sechs praxisbezogene Fallstudien, wobei jeweils typische Angriffsszenarien, Geldwäschemuster und Rückverfolgungsstrategien forensisch analysiert werden.
- **Kapitel 6** diskutiert die rechtlichen und ethischen Rahmenbedingungen der Blockchain-Forensik. Im Zentrum steht das Spannungsfeld zwischen effektiver Strafverfolgung und dem Schutz personenbezogener Daten.
- **Kapitel 7** fasst die zentralen Ergebnisse der Arbeit zusammen, reflektiert die Forschungsfragen kritisch und gewährt einen Ausblick auf zukünftige Entwicklungen sowie offenen Forschungsbedarf im Bereich der Blockchain-Forensik.

# 2. Technologische Grundlagen

## 2.1. Aufbau und Funktionsweise von Blockchains

Blockchains sind eine moderne Form verteilter Datenbanken, die Transaktionen transparent, fälschungssicher und ohne zentrale Kontrollinstanz ermöglichen [1]. Ihre Architektur basiert auf einer linearen Kette von Datenblöcken, die kryptografisch miteinander verknüpft sind [1]. Das häufig eingesetzte Unspent-Transaction-Output-Transaktionsmodell schafft dabei eine klare technische Nachvollziehbarkeit. Jeder Block enthält üblicherweise einen Zeitstempel, den Hashwert des vorherigen Blocks sowie eine Liste von Transaktionen.

Diese Verkettung sorgt für eine manipulationsresistente Datenstruktur. Jede nachträgliche Änderung würde die Hashwerte aller Folgeblöcke ungültig machen und somit sofort auffallen. Dadurch entsteht eine unveränderliche Historie, die eine forensisch überprüfbare Nachverfolgung aller Transaktionen ermöglicht.

Anstelle einer zentralen Kontrollinstanz basiert die Blockchain auf einem dezentralen Netzwerk, in dem sich die beteiligten Knoten über ein Konsensprotokoll auf die gültige Version der Datenbank einigen [1]. Diese Methode erlaubt die sichere Übertragung digitaler Werte ohne Intermediäre wie Banken, insbesondere für Kryptowährungen wie Bitcoin und Ethereum.

Eine umfassende Analyse von Conti et al. von 2018 [24] beschreibt die sicherheitsrelevanten und datenschutzbezogenen Herausforderungen im Bitcoin-Netzwerk. Dabei wird insbesondere das Spannungsverhältnis zwischen der transparenten Nachverfolgbarkeit aller Transaktionen und dem Anspruch auf die Anonymität der Nutzer hervorgehoben.

Die Verarbeitung einer Transaktion in einem Blockchain-System erfolgt typischerweise in Form der folgenden fünf Schritten:

1. **Initialisierung und Signatur:** Ein Nutzer erstellt eine Transaktion und autorisiert sie durch die digitale Signatur seines privaten Schlüssels. Diese Signatur gewährleistet Authentizität und Unverfälschtheit.
2. **Verteilung im Netzwerk**: Nach der Erstellung wird die Transaktion über das Peer-to-Peer-Netzwerk verbreitet. Dort erreicht sie alle relevanten Knoten im System.
3. **Zwischenspeicherung im Mempool:** Unbestätigte Transaktionen werden im sogenannten „Mempool“ gespeichert. Der Mempool dient als Zwischenspeicher für Transaktionen, die auf ihre Aufnahme in einen Block warten.
4. **Auswahl und Validierung:** Abhängig vom verwendeten Konsensmechanismus (z. B. Proof of Work oder Proof of Stake) wählen Miner oder Validatoren geeignete Transaktionen aus dem Mempool aus. Diese werden auf ihre Gültigkeit überprüft, etwa hinsichtlich der Signatur und des verfügbaren Guthabens.

5. **Integration in die Blockchain:** Nach erfolgreicher Validierung werden die Transaktionen in den nächsten Block aufgenommen. Dieser Block wird anschließend an die bestehende Blockchain angehängt und verteilt, wodurch die Transaktionen dauerhaft gespeichert und öffentlich nachvollziehbar sind.

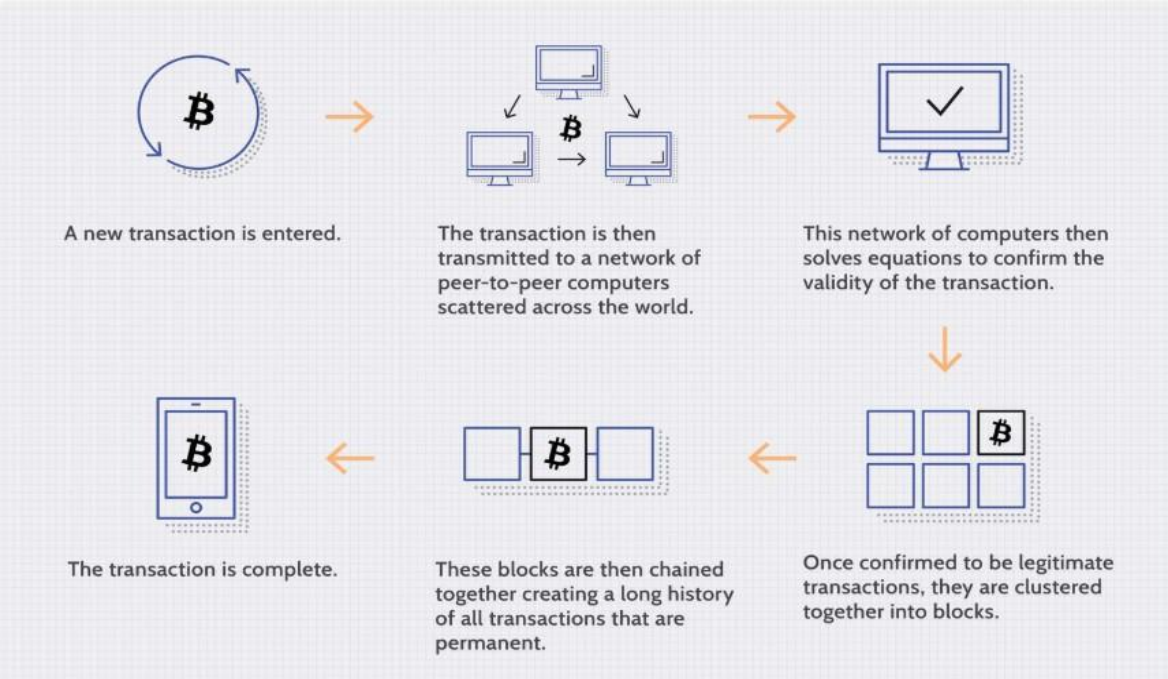


Abbildung 2: Ablauf einer Bitcoin-Transaktion im Blockchain-Netzwerk [34]

Die Sicherheit und Integrität von Blockchain-Systemen basieren auf einem modernen kryptografischen Verfahren. Im Zentrum steht die asymmetrische Kryptografie, bei der jedem Teilnehmer ein eindeutiges Schlüsselpaar zugewiesen wird:

- Der private Schlüssel dient der digitalen Signatur von Transaktionen.
- Der öffentliche Schlüssel ermöglicht deren Verifizierung durch andere Netzwerkteilnehmer.

Dieses Verfahren gewährleistet die Authentizität und Unveränderlichkeit der übermittelten Transaktionen, da nur der rechtmäßige Besitzer mit seinem privaten Schlüssel gültige Transaktionen erzeugen kann.

Ergänzend kommen Hashfunktionen wie SHA-256 zum Einsatz. Sie erzeugen aus beliebigen Eingangsdaten einen eindeutigen sogenannten Hashwert, also einen digitalen Fingerabdruck. Selbst kleinste Veränderungen in den Daten führen zu einem komplett neuen Hash, wodurch Manipulationen von den Validierungsknoten im Netzwerk unmittelbar erkannt werden.

Bei den Blockchain-Technologien kommen häufig hierarchisch organisierte Hash-Datenstrukturen, sogenannte Merkle-Bäume, zum Einsatz. Dabei enthält jeder übergeordnete Knoten den Hashwert seiner untergeordneten Elemente. Dies ermöglicht eine effiziente

Verifikation einzelner Transaktionen, ohne den gesamten Blockinhalt prüfen zu müssen. Diese Struktur erlaubt es, mit minimalem Rechenaufwand nachzuweisen, dass eine bestimmte Transaktion Bestandteil eines Blocks ist, ohne alle Transaktionen erneut verarbeiten zu müssen. Diese Kombination aus kryptografischen Sicherheitsmechanismen und dezentraler Konsensfindung schafft eine robuste Infrastruktur. Ihre Eigenschaften bilden die Grundlage für viele weitere Blockchain-Anwendungen wie digitale Zahlungssysteme.

Die grundlegenden Strukturmerkmale von Blockchain-Systemen, insbesondere ihre Transparenz und die Unveränderlichkeit der gespeicherten Daten, ermöglichen prinzipiell eine vollständige Rückverfolgung sämtlicher Transaktionen. Dies bildet eine wertvolle Grundlage für forensische Analysen im digitalen Kontext.

Gleichzeitig stellen die von den Blockchain-Netzwerken eingesetzten kryptografischen Sicherheitsmechanismen, insbesondere die Verwendung von pseudonymisierten Schlüsseladressen und digitalen Signaturen, eine zentrale Herausforderung für die Ermittlungsbehörde dar: Die eindeutige Zuordnung von Transaktionen zu realen Identitäten ist häufig nur mit zusätzlichem Ermittlungsaufwand und unter Einsatz externer Datenquellen möglich.

Die zuvor dargestellten grundlegenden Architekturmerkmale einer Blockchain bilden die technische Basis für das Verständnis verschiedener Konsensmechanismen, die im folgenden Abschnitt 2.2. detailliert untersucht werden. Dabei wird deutlich, dass die Wahl des Konsensmechanismus direkte Auswirkungen auf die forensische Analysierbarkeit der Transaktionsdaten hat.

## 2.2. Konsensmechanismen und Sicherheitsmodelle

Konsensmechanismen sind zentrale Bestandteile jeder Blockchain-Architektur. Sie gewährleisten in verteilten Netzwerken ohne zentrale Instanz, dass alle Knoten über den aktuellen Zustand des Ledgers übereinstimmen. Diese Protokolle sichern nicht nur die Integrität und Konsistenz der Daten, sondern beeinflussen auch maßgeblich die Skalierbarkeit, Sicherheit und Dezentralität eines Blockchain-Systems.

Der 2009 ursprünglich von Bitcoin eingeführte Mechanismus ist der PoW [1]. Dabei konkurrieren Miner darum, ein vom Netzwerk erstelltes kryptografisches Rätsel zu lösen, indem sie einen gültigen Hashwert für einen neuen Block finden. Dieser Prozess erfordert eine erhebliche Rechenleistung und einen hohen Energieaufwand, wodurch ökonomische Eintrittsbarrieren entstehen, die aufgrund der hohen Hardware- und Stromkosten gleichzeitig zur Netzwerksicherheit beitragen. Gleichzeitig führt PoW zu Kritik hinsichtlich seiner negativen Umweltauswirkungen. Bitcoin und Litecoin verwenden dieses Verfahren weiterhin [1].

Als energieeffizientere Alternative wurde 2011 von der Bitcoin-Community hierfür der PoS entwickelt. Hier werden Teilnehmer als Validatoren ausgewählt, wobei die Auswahlwahrscheinlichkeit vom finanziellen Einsatz („Stake“) abhängt. PoS reduziert den Energieverbrauch erheblich, ohne die Sicherheit zu kompromittieren, und wurde beispielsweise von Ethereum im Rahmen des sogenannten „Merge“ im September 2022 vollständig implementiert [2]. Die grundlegende Architektur von Ethereum ist im Yellow Paper dokumentiert [3], während die PoS-Spezifikationen in separaten Ethereum Improvement Proposals festgehalten werden. PoS erlaubt zudem Delegationsmodelle, bei denen Token-Inhaber ihre Stimmrechte an andere Akteure übertragen können.

Eine wichtige Variation stellt der Delegated Proof of Stake (DPoS) dar, der in Netzwerken wie EOS oder TRON verwendet wird. Hier wählen die Teilnehmer eine begrenzte Zahl von Delegierten, die im Auftrag des Netzwerks neue Blöcke erzeugen. Dieses Modell erhöht die Effizienz und Transaktionsgeschwindigkeit, geht jedoch mit einer reduzierten Dezentralisierung einher, da in diesem Fall nur wenige Akteure die Kontrolle über die Blockproduktion besitzen.

Neuere etablierte Blockchain-Projekte wie Solana oder Avalanche haben weitere innovative Konsensmechanismen eingeführt, die auch für die forensische Analyse relevant sind [35] [36]:

- Der **Proof of History (PoH)**, wie bei Solana, erzeugt einen historischen Datensatz, der beweist, dass ein Ereignis zu einem bestimmten Zeitpunkt stattgefunden hat, was die zeitliche Nachverfolgung von Transaktionen präzisiert.
- Das **Avalanche-Protokoll** verwendet einen Metakonsens durch wiederholte Subsampling-Abstimmungen, um bezogen auf die Transaktionsfinalität eine schnelle Bestätigung zu erreichen, was die forensische Analyse von Transaktionsbestätigungen vereinfacht.

Diese Mechanismen verändern die Struktur und Muster von Transaktionen und erfordern daher angepasste forensische Methodiken, die in Kapitel 3 näher untersucht werden.

Für private oder konsortiale Blockchains, bei denen die Teilnehmer dem Netzwerk vorab bekannt und zugelassen sind, kommen häufig byzantinische Fehlertoleranzprotokolle zum Einsatz. Ein prominentes Beispiel ist das Practical-Byzantine-Fault-Tolerance-Modell, das auch bei einem böswilligen Verhalten (z. B. absichtlicher Falschvalidierung) von bis zu einem Drittel der Knoten noch einen Konsens ermöglicht. PBFT basiert auf intensiver Kommunikation zwischen den Teilnehmern und eignet sich besondere für „permissioned Blockchains“ wie Hyperledger Fabric oder Tendermint.

Die Wahl des Konsensmechanismus hat gleichzeitig erhebliche Auswirkungen auf die forensische Analyse von Blockchain-Transaktionen:

- **PoW-Systeme** ermöglichen durch ihre längere Blockzeit und klar definierte Rechenstruktur eine leichtere Nachvollziehbarkeit von Transaktionen über Zeitstempel hinweg.
- **PoS-Netzwerke** wie Ethereum (12-Sekunden-Blöcke vs. Bitcoin-10-Minuten-Blöcke) [1] generieren deutlich höhere Transaktionsfrequenzen, was die statistische Signifikanz timing-basierter Clustering-Heuristiken reduziert und komplexere Analyseverfahren erfordert.

Die Sicherheitsmodelle von Blockchain-Systemen basieren auf der Annahme, dass eine Mehrheit der Teilnehmer ehrlich agiert. Typische Angriffsvektoren umfassen die folgenden Aspekte:

- **Sybil-Attacken:** Ein Angreifer generiert zahlreiche falsche Identitäten innerhalb eines Netzwerks, um dessen Kontrolle oder Entscheidungsprozesse zu manipulieren.
- **Double Spending:** Es werden mehrere Ausgaben derselben digitalen Währung vorgenommen, was die Integrität der Transaktionen in Gefahr bringt.
- **Eclipse-Angriffe:** Ein Knoten wird vom Rest des Netzwerks isoliert und erhält ausschließlich manipulierte Informationen, um sein Verhalten zu beeinflussen.
- **Selfish Mining:** Miner halten gefundene Blöcke zurück, um sich einen strategischen Vorteil zu verschaffen und höhere Belohnungen zu erhalten.

Gegenmaßnahmen vonseiten der Blockchain-Protokolle beinhalten wirtschaftliche Bestrafung bei PoS (zum Beispiel Slashing), hohe Rechenkosten bei PoW sowie netzwerktechnische Redundanzen. Seit 2017 werden von der Forschungsgemeinschaft und verschiedenen Entwicklerteams zudem hybride Konsensansätze erforscht, die Elemente von PoW und PoS kombinieren, um ein optimales Gleichgewicht zwischen Sicherheit, Skalierbarkeit und Energieeffizienz zu erzielen.

Die Wahl des Konsensmechanismus bestimmt somit nicht nur die technischen Eigenschaften eines Blockchain-Systems, sondern beeinflusst auch maßgeblich dessen forensische Analysierbarkeit. Während PoW-Systeme durch ihre längeren Blockzeiten und deterministischen Strukturen diesbezüglich mehr Transparenz bieten, stellen PoS-Netzwerke durch ihre erhöhte Transaktionsfrequenz neue Herausforderungen für forensische Verfahren dar. Diese Unterschiede wirken sich direkt auf die im folgenden Abschnitt 2.3. behandelten Transaktionsmodelle und deren Implikationen für die Anonymität der Nutzer aus.

## 2.3. Transaktionsmodelle und Anonymitätsstufen

Verschiedene Blockchain-Systeme verwenden unterschiedliche Transaktionsmodelle, die Einfluss auf die Transparenz, Nachverfolgbarkeit und Anonymität der entsprechenden Transaktionen nehmen. Zwei der dominierenden Paradigmen sind das UTXO-Modell, wie es bei Bitcoin Anwendung findet, und das Kontomodell (Account-based Model), das unter anderem bei Ethereum eingesetzt wird. Diese Modelle unterscheiden sich nicht nur bezüglich ihrer technischen Struktur, sondern auch ihrer Eignung für forensische Analysen.

Beim UTXO-Modell wird jeder Transaktionsoutput als einzelner, nicht ausgegebener Vermögenswert gespeichert, der bei einer neuen Transaktion vollständig verwendet wird. Eine Transaktion besteht somit aus einer Menge an Inputs (verbrauchten Outputs) und neuen Outputs. Nutzer können für jede Transaktion eine neue Adresse generieren, was eine gewisse Pseudonymität ermöglicht. Da es jedoch keine Kontensalden gibt, sondern nur einzelne Vermögensfragmente, ist die Zuordnung von Zahlungsflüssen zwar komplexer als beim Account-Modell, durch Heuristiken wie die Multi-Input-Analyse nichtsdestotrotz möglich.

Das Account-Modell hingegen bildet den Zustand des Netzwerks als Kontensaldo ab, der durch Transaktionen direkt verändert wird. Jeder Account besitzt eine permanente Adresse, was die Verfolgung von Transaktionen zwar erleichtert, jedoch gleichzeitig die Privatsphäre der Nutzer reduziert. Dieses Modell ist besonders bei Smart-Contract-Plattformen wie Ethereum verbreitet, da es den Zugriff auf globale Zustände und komplexe Vertragsinteraktionen effizient unterstützt.

Beide Modelle erlauben lediglich eine pseudonyme Nutzung. Dabei sind Blockchain-Adressen nicht unmittelbar mit realen Identitäten, sondern mit Schlüsselpaaren verknüpft. Diese Pseudonymität kann jedoch durch forensische Verfahren wie Adress-Clustering, Transaktionsgraphanalyse und die Einbindung externer Datenquellen (z. B. KYC-Daten) durchbrochen werden.

Zur Erhöhung der Privatsphäre wurden von der Bitcoin-Community seit 2013 verschiedene Privacy-Enhancing Technologies (PETs) entwickelt. Ein verbreiteter Ansatz ist CoinJoin, wobei mehrere Nutzer ihre Transaktionen zu einem gemeinsamen Output bündeln, wodurch die Zuordnung einzelner Eingänge zu Ausgängen erheblich erschwert wird. Tools wie Wasabi Wallet oder JoinMarket implementieren dieses Verfahren für Bitcoin.

Eine weiterentwickelte Variante dessen stellt CoinSwap dar, wobei zwei Transaktionen gleichzeitig durchgeführt werden, ohne dass ein direkter Zusammenhang zwischen Sender und Empfänger im Transaktionsgraphen sichtbar ist. Dies wird durch den Einsatz von Hash Time-Locked Contracts (HTLCs) ermöglicht, die kryptographische Zeitschlösser implementieren, um die Sicherheit der Teilnehmer zu gewährleisten.

Stealth-Adressen ermöglichen die Generierung einmaliger Empfangsadressen, die auf der Blockchain erscheinen, jedoch nicht ohne Weiteres mit einer öffentlich bekannten Adresse verknüpft werden können. In Kombination mit dem Diffie-Hellman-Schlüsselaustausch bieten sie einen hohen Grad an Vertraulichkeit.

Darüber hinaus existieren Kryptowährungen, deren primäres Designziel vollständige Anonymität ist. Monero verwendet unter anderem Ring-Signaturen (kryptographische Verfahren, die eine Signatur aus einer Gruppe von Signaturen generieren, ohne preiszugeben, welcher Gruppenteilnehmer sie erzeugt hat), Stealth-Adressen und Confidential Transactions, um Sender, Empfänger und Betrag vollständig zu verschleiern. Zcash setzt auf Zero-Knowledge-Proofs, insbesondere zk-SNARKs, welche ermöglichen, die Gültigkeit einer Aussage zu beweisen, ohne weitere Informationen preiszugeben – um Transaktionen zu verifizieren, ohne sensible Informationen bekanntzugeben.

Aus forensischer Perspektive lassen sich hierbei drei Anonymitätsstufen unterscheiden, die sich hinsichtlich ihrer Analysierbarkeit deutlich voneinander abgrenzen (siehe Abbildung 3).

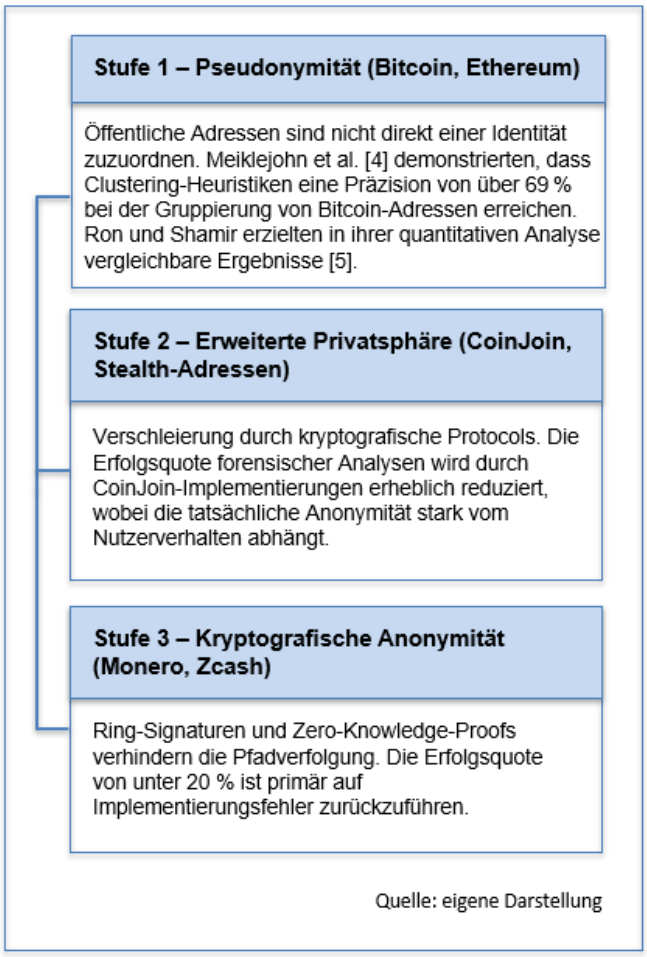


Abbildung 3: Stufen der Anonymität in Kryptowährungen

Für forensische Analysten stellen diese Abstufungen erhebliche Herausforderungen dar. Während bei pseudonymen Modellen durch Heuristiken und Open-Source-Intelligence ein hoher Grad an Rückverfolgbarkeit erreichbar ist, sind bei echten Privacy-Coins meist nur metadatenbasierte Analysen möglich, die selten gerichtsfeste Beweise liefern. Die technische Gestaltung des Transaktionsmodells beeinflusst somit maßgeblich die Auswahl und Wirksamkeit forensischer Werkzeuge.

Aufbauend auf diesen technologischen Grundlagen und Anonymitätsstufen werden im folgenden Kapitel die konkreten forensischen Methoden untersucht, mit denen Ermittler bei Blockchains Transaktionsmuster analysieren und verdächtige Aktivitäten identifizieren können. Dabei wird deutlich, wie die in Kapitel 2.3. erläuterten Transaktionsmodelle und Anonymitätsstufen die forensischen Ansätze prägen.

Die zuvor dargestellten Anonymitätsstufen und Transaktionsmodelle bilden das technologische Fundament, auf dem forensische Analysen diesbezüglich aufbauen. Wie Meiklejohn et al. (2013) [4] gezeigt haben, ermöglicht gerade das Verständnis dieser strukturellen Eigenschaften die Entwicklung effektiver Analysemethoden. Das folgende Kapitel 3. widmet sich daher den forensischen Verfahren, die trotz der pseudonymen Natur von Blockchain-Systemen entwickelt wurden.

Diese Methoden bilden die Grundlagen moderner Blockchain-Analyse. Allerdings stoßen etablierte Verfahren zunehmend an Grenzen, da neue Blockchain-Technologien wie Monero oder Zcash gezielt darauf ausgerichtet sind, die Rückverfolgbarkeit zu erschweren oder zu verhindern. Diese technischen Herausforderungen werden im folgenden Kapitel detailliert analysiert.

# 3. Methoden der Blockchain-Forensik

## 3.1. Heuristische Verfahren und Adress-Clustering

Die in Kapitel 2 erläuterten technologischen Grundlagen verschiedener Blockchain-Systeme bilden die Basis für ein vertieftes Verständnis forensischer Analysemethoden. Dieses Kapitel systematisiert die aktuell verfügbaren Werkzeuge der Blockchain-Forensik, von den etablierten heuristischen Ansätzen über graphbasierte Netzwerkanalysen bis zu modernen Entanonymisierungstechniken. Dabei wird deutlich, wie die spezifischen Eigenschaften unterschiedlicher Blockchain-Architekturen, etwa UTXO-Modelle oder Account-basierte Systeme, die Auswahl und Effektivität forensischer Verfahren maßgeblich beeinflussen.

Eine der zentralen Herausforderungen der Blockchain-Forensik besteht in der Identifikation von Entitäten hinter pseudonymen Adressen. Da öffentliche Blockchains wie Bitcoin und Ethereum keine direkten Identitätsdaten speichern, greifen forensische Analysten auf sogenannte heuristische Verfahren zurück, um logische Zusammenhänge zwischen Adressen

herzustellen. Das entsprechende Adress-Clustering ermöglicht die Zuordnung multipler Adressen zu einer gemeinsamen Kontrolleinheit.

Die Multi-Input-Heuristik basiert auf der Annahme, dass alle Eingangsadressen einer Transaktion von derselben Person kontrolliert werden. Diese Annahme ist gültig, da zur Signierung alle zugehörigen privaten Schlüssel erforderlich sind. Dadurch entsteht eine logische Verbindung zwischen den verwendeten Adressen. Werden mehrere UTXOs in einer Transaktion vereint, können deren Quelladressen somit einem gemeinsamen Cluster zugeordnet werden. Meiklejohn et al. [4] wendeten diese Technik erstmals 2013 systematisch im Rahmen einer groß angelegten Bitcoin-Analyse an. Sie findet heute bei kommerziellen Analyseplattformen wie Chainalysis Reactor und Elliptic Investigator breite Anwendung (siehe Kapitel 3.4.).

Eine ergänzende Methode stellt die Change-Address-Heuristik dar. Sie basiert auf dem Verhalten vieler Wallets, nach Durchführung einer Transaktion automatisch eine neue Adresse zu generieren, auf die das Wechselgeld übertragen wird. Die Identifikation solcher Wechselgeldadressen erfolgt anhand typischer Merkmale wie Einmalverwendung und spezifischer Transaktionsstrukturen. Allerdings implementieren moderne Wallets zunehmend Verschleierungsstrategien, wodurch die Zuverlässigkeit dieser Heuristik erheblich sinkt.

Ein weiteres Instrument ist die Einzahlungsheuristik, bei der Adressen identifiziert werden, die in typischen Mustern auf Plattformen wie Börsen oder Marktplätzen verwendet werden. Wenn beispielweise zahlreiche kleinere Beträge von verschiedenen Adressen an eine zentrale Adresse gesendet werden, kann dies auf eine Sammeladresse einer Börse hindeuten. In Verbindung mit öffentlich bekannten Adressen dieser Plattformen (z. B. durch KYC-Leaks oder selbst deklarierte Wallets) lassen sich dadurch größere Entitäten kartieren.

Diese Heuristiken ermöglichen die Bildung sogenannter Adress-Cluster, welche die Grundlage für weiterführende Analysen wie Graphanalysen, Risikobewertungen und die Verfolgung von Transaktionen bilden. Empirische Studien von Meiklejohn et al. [4], Ron und Shamir [5] sowie Harrigan und Fretter [6] demonstrieren die Effektivität heuristischer Clustering-Verfahren bei Bitcoin, wobei die Genauigkeit je nach verwendeter Methodik und verfügbaren Datenquellen variiert. Die in Kapitel 2.3 dargestellten Heuristiken erreichen dabei hohe Präzisionsraten. Diese Erfolgsquoten beziehen sich auf die korrekte Zuordnung von Adressen zu Entitäten in kontrollierten Testumgebungen und können in der forensischen Praxis, je nach verfügbaren Zusatzinformationen und Nutzerverhalten, deutlich variieren. Deren Effektivität hängt dabei stark vom Adressverhalten der Nutzer und der von diesen jeweils genutzten Privacy-Technologie ab.

Trotz ihrer Effektivität sind heuristische Verfahren nicht unumstritten. Sie beruhen auf Annahmen, die nicht in allen Kontexten gültig sind, insbesondere dann, wenn Nutzer bewusst

Strategien zur Adressentkopplung einsetzten. Zudem können fehlerhafte Heuristiken zu False Positives führen, wodurch unabhängige Adressen fälschlich einem Cluster zugewiesen werden. Aus diesem Grund werden diese Methoden zunehmend mit zusätzlichen Datenquellen kombiniert, etwa aus OSINT, Netzwerkverkehrsanalysen oder KYC-Datenbanken.

In der forensischen Praxis bilden heuristische Clustering-Verfahren die Grundlage vieler Analyseplattformen. Kommerzielle Tools wie Chainalysis Reactor und Elliptic Investigator sowie Open-Source-Plattformen wie BlockSci [9] nutzen kombinierte Heuristiken, um Adressbeziehungen sichtbar zu machen und Entitäten wie Darknet-Märkte, Mixing-Dienste oder Ransomware-Gruppen zu identifizieren. Die Kombination aus heuristischer Logik und verifizierten Datenquellen ermöglicht eine zunehmend präzise Kartografierung der Krypto-Ökonomie.

Die praktische Anwendung dieser heuristischen Clustering-Verfahren wird in Kapitel 5.1. am Beispiel des Silk-Road-Falls deutlich, wo die Multi-Input-Heuristik maßgeblich zur Identifikation des Betreibers beitrug. Kapitel 5.2. zeigt, wie Adress-Clustering zur Aufdeckung komplexer Geldwäsche-Netzwerke eingesetzt wurde.

### 3.2. Graphbasierte Netzwerkanalyse

Neben den zuvor erläuterten heuristischen Verfahren zählt die graphbasierte Netzwerkanalyse zu den leistungsfähigsten Methoden der forensischen Untersuchung von Blockchain-Transaktionen. Diese Technik nutzt die inhärente Struktur von Blockchains als gerichteten Graphen, um die Beziehungen zwischen Adressen, Transaktionen und Entitäten sowohl visuell als auch rechnerisch zu modellieren und auszuwerten.

Je nach Perspektive unterscheidet man typischerweise zwischen folgenden zwei Modelltypen:

- **Adressgraph:** Knoten repräsentieren einzelne Wallet-Adressen, Kanten die Transaktionen zwischen ihnen.
- **Transaktionsgraph:** Jede Transaktion wird als Knoten dargestellt und durch die Ausgabe- bzw. Eingabeadressen werden verschiedene Transaktionen und die daran beteiligten Adressen miteinander verbunden.

Beide Modelle ermöglichen die Analyse des digitalen Geldflusses über die Zeit und die Identifikation typischer Muster.

Ein zentrales Element ist dabei die Pfadverfolgung, bei der von einer Ausgangsadresse – etwa einer bekannten Wallet aus einem Ermittlungsverfahren – ausgehend die Abflüsse über mehrere Transaktionsschritte hinweg verfolgt werden. Dadurch lassen sich Zieladressen, Empfängercluster oder potenzielle Verschleierungstechniken wie Mixer oder

Börsenübergänge sichtbar machen. Die in Kapitel 3.4. beschriebenen kommerziellen Tools nutzen die automatisierte Pfadverfolgung mit eingebetteten Heuristiken zur Echtzeitüberwachung.

Zur Identifikation vernetzter Adressgruppen kommen Community-Detection-Verfahren zum Einsatz. Algorithmen wie Louvain und Infomap analysieren Informationsflüsse im Graphen und erkennen Cluster mit überdurchschnittlicher interner Transaktionsaktivität. Solche Gruppen können auf eine gemeinsame Kontrolle, Dienstleistungsnutzung oder kriminelle Zusammenarbeit hindeuten.

Ein weiteres Anwendungsfeld ist die Zentralitätsanalyse, mit der statistisch ermittelt wird, welche Knoten im Netzwerk besonders einflussreich oder verbindend sind. Typische Metriken dabei sind die folgenden:

- **Degree-Centrality:** Zahl direkter Verbindungen,
- **Betweenness-Centrality:** Funktion als Transaktionsbrücke,
- **Eigenvector-Centrality:** Einfluss durch Verbindungen zu wichtigen Knoten.

Diese Analysen helfen dabei, sogenannte Key-Players zu identifizieren, zum Beispiel Adressen von Mixing-Diensten, Ransomware-Akteuren oder zentralen Wallets großer Börsen.

Die Visualisierung der Netzwerkstrukturen dient hierbei nicht nur der Interpretation, sondern stellt vielmehr ein eigenständiges Analyseinstrument dar. Dynamische Darstellungen, insbesondere in Verbindung mit zeitlicher Skalierung, ermöglichen die Erkennung ungewöhnlicher Aktivitätsmuster wie koordinierter Geldbewegungen oder Chain-Hopping zwischen verschiedenen Kryptowährungen. Die Open-Source-Plattform BlockSci [9] bietet ein leistungsfähiges Framework zur Blockchain-Analyse, das speziell für die Verarbeitung großer Datenmengen und die Implementierung komplexer graphbasierter Methoden entwickelt wurde.

Dabei ist die graphbasierte Analyse nicht frei von Einschränkungen. Sie kann durch Privacy-Techniken wie CoinJoin, Atomic Swaps oder Cross-Chain-Transfers erheblich an Aussagekraft verlieren. Zudem steigt der Rechenaufwand bei großen Netzwerken exponentiell mit der Zahl der Knoten und Verbindungen. Effiziente Algorithmen und spezialisierte Datenstrukturen wie Adjacency-Maps (Nachbarschaftsmatrizen) oder Merkle-DAGs sind für die skalierbare Anwendung dieser Methoden daher essenziell.

In der Praxis ergänzt die graphbasierte Netzwerkanalyse heuristische Verfahren, indem sie abstrakte Beziehungen sichtbar macht, die über direkte Transaktionsverknüpfungen hinausgehen. In Verbindung mit Clustering, OSINT und Risikoklassifikation bildet sie einen integralen Bestandteil moderner Blockchain-Forensik.

## 3.3. Techniken zur Entanonymisierung

Die Entanonymisierung verfolgt das zentrale Ziel forensischer Untersuchungen im Bereich der Blockchain-Analyse, d. h. die Verbindung zwischen pseudonymen Blockchain-Adressen und realweltlichen Identitäten herzustellen. Da die meisten Blockchain-Systeme keine personenbezogenen Daten speichern, erfolgt die Entanonymisierung durch eine Kombination technischer Analyseverfahren mit externen Datenquellen.

Ein verbreiteter Ansatz ist hierbei die Transaktionsgraphanalyse, bei der aus Transaktionshistorien und Adress-Clustern abgeleitet wird, welche Adressen möglicherweise derselben Kontrolleinheit zuzuordnen sind. Besonders aussagekräftig sind Interaktionen mit bekannten Entitäten wie Kryptowährungsbörsen, Zahlungsdiensten oder illegalen Marktplätzen. Adressen, die regelmäßig mit KYC-verpflichteten Plattformen kommunizieren, können als Ausgangspunkt für die Identifikation genutzt werden.

Ergänzend kommen Netzwerkverkehrsanalysen zum Einsatz. Dabei wird untersucht, wie Transaktionen im Peer-to-Peer-Netzwerk (z. B. Bitcoin) weitergeleitet werden. Biryukov et al. [7] zeigten, dass durch passives Monitoring und Timing-Analysen eine Zuordnung von Transaktionen zu IP-Adressen möglich ist. Bei ihren Experimenten konnten bis zu 60 % der Transaktionen erfolgreich zu Ursprungs-IPs zurückverfolgt werden [7], wobei die Erfolgsquote stark von der Netzwerktopologie und den eingesetzten Gegenmaßnahmen abhängt. Diese Methode erfordert jedoch ein umfangreiches Monitoring und präzise Timing-Analysen.

Eine weitere wirkungsvolle Methode ist die Nutzung von OSINT. Hierbei werden öffentlich zugängliche Informationen wie Social-Media-Beiträge, Forendiskussionen, Pastebin-Leaks oder Darknet-Datenbanken analysiert, um Verbindungen zwischen Nutzernamen, Wallet-Adressen und Transaktionen herzustellen. So konnten in der Praxis Betrugswallets durch die Auswertung öffentlich zugänglicher Kommunikationskanäle identifiziert werden.

Eine der verlässlichsten Entanonymisierungsmethoden ergibt sich aus der Verknüpfung mit KYC- und AML-Daten, die durch regulierte Börsen und Zahlungsdienstleister erhoben werden. Ermittlungsbehörden können auf gerichtliche Anordnung Zugriff auf diese Daten erhalten, wenn ein Zusammenhang zu einer verdächtigen Adresse besteht. In der Praxis ist dies besonders dann relevant, wenn gestohlene oder gewaschene Kryptowährungen auf Handelsplattformen transferiert werden, die gesetzlich zur Identitätsverifizierung verpflichtet sind.

Zudem werden zunehmend komplexe Cross-Layer-Ansätze verwendet, bei denen Blockchain-Daten mit Webdaten verknüpft werden. Eine Studie von Goldfeder et al. [8] zeigte, dass durch die Korrelation von Transaktionsdaten mit Webtracking-Informationen (Cookies, JavaScript-Logik, Referrer-Informationen) Nutzer entanonymisiert werden konnten, die in Online-Shops

Kryptowährungen verwendeten. Durch Cross-Site-Correlation und session-based Linking konnten einzelne Transaktionen spezifischen Geräten und Nutzerprofilen zugeordnet werden.

Die Effektivität der Entanonymisierung hängt stark vom verwendeten Blockchain-Typ sowie den eingesetzten Privacy-Technologien ab. Während Bitcoin und Ethereum trotz Pseudonymität aufgrund der öffentlichen Verfügbarkeit der Transaktionshistorie eine gewisse Nachverfolgbarkeit ermöglichen, stellen sogenannte Privacy-Coins wie Monero oder Zcash deutlich größere Herausforderungen dar. Ohne externe Leaks oder schwerwiegende Implementationsfehler ist eine eindeutige Zuordnung hier kaum möglich. In solchen Fällen bleibt oft nur eine metadatenbasierte Risikoeinschätzung oder Verhaltensanalyse.

Die in Kapitel 2.3. erläuterten Ring-Signaturen bei Monero [13] verschleiern gezielt die Herkunft von Transaktionen. Eine Zuordnung der Eingangsadresse zu der tatsächlich ausgegebenen Adresse ist kryptografisch dann nicht möglich, da in Bezug darauf alle Gruppenmitglieder statistisch gleich wahrscheinlich erscheinen. Kumar et al. [14] zeigten jedoch, dass bis April 2017 etwa 62 % der Transaktionen dennoch rückverfolgbar waren, vor allem durch Schwächen bei der Auswahl der Ring-Mitglieder. Für forensische Analysten stellt dies eine erhebliche Herausforderung dar, da die klassische Pfadverfolgung dabei weitgehend scheitert. In solchen Fällen bleiben vorrangig sekundäre Ansätze wie die Auswertung von Implementierungsfehlern oder externen Metadatenlecks.

Die forensischen Implikationen dieser Technologien sind grundlegend: Während bei Bitcoin die Multi-Input-Heuristik eine Zuordnung von 60 bis 70 % der Adressen ermöglicht, reduzieren Ring-Signaturen diese Quote erheblich (siehe Kapitel 2.3.). Diese Diskrepanz verdeutlicht die technologische Asymmetrie zwischen Analyse und Verschleierung.

Die in Kapitel 2.3. beschriebenen Zero-Knowledge-Proofs (zk-SNARKs) bei Zcash [15] ermöglichen eine Blockchain mit hoher Integrität bei minimaler Transparenz. Forensisch bleibt hier meist nur die Analyse der transparenten Adresstypen („t-addrs“) sowie der Wechselwirkungen zwischen transparenten und abgeschirmten Transaktionen.

HTLCs, wie sie bei Atomic Swaps eingesetzt werden, bilden die Grundlage für kettenübergreifende Transaktionen. Ihre kryptografische Struktur verhindert die Manipulation durch eine der beiden Parteien. Für die Forensik bedeutet dies, dass der Informationsfluss nicht mehr einer einzigen Blockchain entnommen werden kann, sondern über mehrere Ledgers hinweg rekonstruiert werden muss. Dies erfordert eine neue Klasse von Analysewerkzeugen.

Im forensischen Alltag zeigt sich, dass eine Kombination verschiedener Techniken die höchsten Erfolgsquoten erzielt. Während die alleinige Nutzung von Heuristiken fehleranfällig sein kann, führt deren Verknüpfung mit KYC-Daten, OSINT-Quellen und

Netzwerkbeobachtungen zu belastbaren Ergebnissen. Insbesondere bei Ransomware-Ermittlungen, Darknet-Operationen oder Börsenhacks hat sich diese Methodenkombination als zielführend erwiesen.

### 3.4. Tools und Plattformen der Forensik

Die zunehmende Komplexität von Blockchain-Netzwerken sowie die Vielfalt forensischer Fragen haben aufseiten der Strafverfolgungsbehörden seit 2014 zur Entwicklung spezialisierter Softwarelösungen geführt, die große Mengen an Transaktionsdaten analysieren, visualisieren und interpretieren können. Diese Analysewerkzeuge sind heute sowohl für Strafverfolgungsbehörden als auch Unternehmen mit Compliance-Aufgaben unverzichtbar.

Zu den führenden kommerziellen Plattformen zählen laut McShane (2023) [47] Chainalysis, Elliptic und CipherTrace, wobei Letzteres seit 2021 ein Teil von Mastercard ist. Diese drei Systeme bieten umfangreiche Funktionen zur Transaktionsverfolgung, Adressklassifikation, Risikoanalyse und Entitätszuordnung. Die Grundlage dieser bildet ein umfassendes Clustering bekannter Wallets, kombiniert mit KYC-gestützten Datenquellen, maschinellem Lernen und graphbasierten Analysen.

Chainalysis Reactor, das Flaggschiffprodukt von Chainalysis, ermöglicht die visuelle Darstellung und Analyse komplexer Transaktionsverläufe. Nutzer können Transaktionen rückverfolgen, Wallets bewerten und automatisierte Reports generieren. Die Software ist eng mit Chainalysis KYT verknüpft, das eine Echtzeitüberwachung sowie Risikoeinstufung ein- und ausgehender Transaktionen für Börsen und Banken erlaubt. Eine bedeutende Weiterentwicklung ist das Cross-Chain Investigations Framework von Chainalysis, das die Verfolgung von Vermögenswerten über Bitcoin-Ethereum-Bridges mit erhöhter Genauigkeit ermöglicht [48].

Elliptic bietet mit seiner Plattform „Elliptic Investigator“ vergleichbare Funktionen und fokussiert sich auf die Einhaltung regulatorischer Standards. Zusätzlich stellt Elliptic eine API-gestützte Infrastruktur zur Verfügung, die sich in Compliance-Prozesse integrieren lässt, mit besonderem Fokus auf FATF-Vorgaben, Anti-Geldwäsche-Maßnahmen und Terrorismusfinanzierung [49].

CipherTrace verfolgt einen breiteren Ansatz, der neben der Blockchain-Analyse Marktüberwachung, Darknet-Intelligence und Forensik für Datenschutzwährungen wie Monero umfasst. Die Plattform liefert Risikoscores, Herkunftsanalyse und Verhaltensklassifikation in Echtzeit.

Neben kommerziellen Lösungen existieren Open-Source- und akademische Tools, die insbesondere in der Forschung und bei unabhängigen Analysen zum Einsatz kommen. Ein

Beispiel ist BlockSci [9], ein leistungsfähiges Framework zur Analyse von Bitcoin-Daten, das speziell auf große Datenmengen und flexible Analysen ausgerichtet ist. Es erlaubt die Kombination heuristischer Clusteringverfahren mit benutzerdefinierter Python-Logik.

Weitere akademische Ansätze wie BitIodine [10] demonstrierten bereits 2014 die Machbarkeit automatisierter Adressklassifikation und Entitätserkennung in Bitcoin-Netzwerken.

Das EU-geförderte Projekt GraphSense bietet seit 2016 eine modulare Plattform für Blockchain-Forensik, die neben klassischen Funktionen die Erstellung eigener Metriken, Risikoanalysen und Datenexporte ermöglicht. Aufgrund seines modularen Aufbaus eignet sich GraphSense besonders für Forschung und Lehre [50].

Neben etablierten kommerziellen und akademischen Plattformen existiert seit 2018 ein wachsendes Ökosystem an Open-Source-Werkzeugen für forensische Analysen, die insbesondere für kleinere Unternehmen, Forschungseinrichtungen und unabhängige Ermittler relevant sind. Tools wie BTCParse ermöglichen die Extraktion und Analyse von Bitcoin-Transaktionen ohne kommerzielle Lizenzen. Orbit bietet eine modulare, Python-basierte Plattform für erweiterte Graphanalysen mit integrierter Visualisierung. CryptoHound kombiniert KI-gestützte Analysen mit benutzerfreundlichen Dashboards für Ermittlungsarbeiten. Diese Open-Source-Alternativen bieten zwar nicht den gleichen Funktionsumfang und dieselbe Datenabdeckung wie kommerzielle Lösungen, erlauben jedoch eine kostengünstige Einstiegsmöglichkeit und fördern die Transparenz der eingesetzten Verfahren.

Zusätzlich werden seit 2019 zunehmend Machine-Learning-gestützte Systeme entwickelt, die Muster im Transaktionsverhalten automatisch erkennen und klassifizieren. Weber et al. [20] zeigten, dass Graph Convolutional Networks zur Erkennung von Geldwäschemustern eingesetzt werden können. Ähnliche Ansätze wurden für die Identifikation von Ponzi-Schemata und Mixing-Vorgängen adaptiert. Diese Verfahren sind jedoch stark von der Qualität der jeweiligen Trainingsdaten abhängig und für adversarial manipulation anfällig, etwa durch ein bewusst verändertes Verhalten der Zielgruppen.

Die Entwicklung risikobasierter Analysesysteme begann bereits 2014, als Möser et al. [23] erstmals ein formales Modell zur Risikobewertung von Bitcoin-Transaktionen vorschlugen, das die Gefahr zukünftiger Blacklistings quantifizierte und so den Grundstein für moderne Risk-Scoring-Systeme legte.

In der Praxis zeigt sich, dass keine einzelne Plattform eine vollständige Lösung für den forensischen Analysebedarf im Bereich der Kryptowährungen bietet. Vielmehr hängt die Effektivität forensischer Werkzeuge von der Kombination aus Adressdatenbanken, graphischer Modellierung, Risikobewertung und externer Datenintegration ab. Auch der

Kontext, zum Beispiel der Einsatz bei Ermittlungsbehörden versus Compliance-Abteilungen, beeinflusst die Auswahl der Tools erheblich.

Die Verfügbarkeit leistungsstarker Werkzeuge hat die Erfolgsquote forensischer Analysen deutlich erhöht. Gleichzeitig wirft ihre Nutzung datenschutz- und ethikbezogene Fragen auf, insbesondere wenn private Adressen falsch klassifiziert oder Transaktionen voreilig mit illegalem Verhalten assoziiert werden. Diese Thematik wird im Rahmen der rechtlichen und ethischen Betrachtungen in Kapitel 6 vertieft behandelt.

Die Integration forensischer Tools in regulatorische Compliance-Workflows markiert einen wichtigen Entwicklungsschritt. Durch standardisierte APIs und Risikobewertungssysteme können Krypto-Dienstleister heute automatisiert Transaktionen auf verdächtige Muster prüfen und bei Auffälligkeiten manuelle Überprüfungen einleiten. Diese Entwicklung markiert einen Paradigmenwechsel von reaktiver Forensik nach Straftaten hin zu präventiver Analyse und Risikominimierung. Die damit verbundenen datenschutzrechtlichen Implikationen werden in Kapitel 6 diskutiert.

Die Leistungsfähigkeit der vorliegend vorgestellten forensischen Werkzeuge demonstriert eindrucksvoll das Potenzial moderner Blockchain-Analyse. Gleichzeitig offenbart sich dabei eine technologische Asymmetrie: Während forensische Methoden stetig verfeinert werden, entwickeln sich Privacy-Technologien in einem noch höheren Tempo weiter. Diese evolutionäre Dynamik zwischen Analyse und Verschleierung prägt die im folgenden Kapitel diskutierten technischen Herausforderungen von Grund auf.

Zugleich unterliegen kommerzielle Forensik-Plattformen methodischen und epistemischen Limitationen, die kritisch reflektiert werden müssen. Die Bewertungskriterien und Algorithmen bezogen auf die Risikoeinstufung von Wallet-Adressen sind nicht standardisiert, was zu Reliabilitätsproblemen führt. Die Bewertungskriterien verschiedener Anbieter können zu unterschiedlichen Klassifikationsergebnissen führen. Studien zeigen Abweichungen von bis zu 34 % zwischen verschiedenen Anbietern bei identischen Wallet-Clustern [33]. Zudem bestehen in Bezug auf die institutionelle Rollenverteilung potenzielle Interessenkonflikte, da diese Unternehmen sowohl Behörden als auch regulierte Finanzdienstleister bedienen, was zu einer aus Sicht der datenschutzrechtlichen Aufsicht unerwünschten Vermischung von Strafverfolgungsinteressen und kommerziellen Compliance-Anforderungen führen kann.

Besonders problematisch ist die mangelnde Falsifizierbarkeit von Risikoklassifikationen: Wird eine Wallet als „hochriskant“ eingestuft, existieren oft keine standardisierten Verfahren zur Überprüfung oder Anfechtung dieser Bewertung. Open-Source-Alternativen wie BlockSci und GraphSense bieten methodische Transparenz und ermöglichen die Entwicklung standardisierter Analyseverfahren. Eine zukünftige Herausforderung besteht somit in der

Entwicklung forensischer Standards, die sowohl Effektivität als auch Transparenz, Nachvollziehbarkeit und Falsifizierbarkeit gewährleisten.

Die methodische Intransparenz kommerzieller Forensik-Tools manifestiert sich in Form der folgenden drei Dimensionen:

- **Algorithmische Opazität:** Die Bewertungskriterien bleiben proprietär, was die Nachvollziehbarkeit der Risikoeinstufungen verhindert.
- **Inkonsistente Klassifikationen:** Unterschiedliche Anbieter liefern in Bezug auf die gleichen Adress- bzw. Wallet-Cluster teils stark divergierende Ergebnisse.
- **Eingeschränkte Falsifizierbarkeit:** Die Anfechtung von Risikoeinstufungen ist und bleibt ohne standardisierte Verfahren problematisch.

Dies wirft grundlegende Fragen zur Falsifizierbarkeit und Reliabilität auf, insbesondere im strafrechtlichen Kontext. Studien zeigen erhebliche Unterschiede bei den Klassifikationsergebnissen verschiedener Anbieter wie Chainalysis oder Elliptic. Ein weiteres Problem besteht in der Doppelfunktion vieler Anbieter als Dienstleister für sowohl für Strafverfolgungsbehörden als auch Finanzunternehmen, was bei der Risikobewertung potenzielle Interessenkonflikte birgt.

Offene, wissenschaftlich validierte Alternativen wie BlockSci oder GraphSense bieten einen methodischen Gegenpol - durch eine transparente Replikation von Analysen und standardisierte Verfahren. Dabei bleiben sie jedoch hinsichtlich der Datenabdeckung und Nutzerfreundlichkeit hinter den kommerziellen Lösungen zurück. Die Zukunft forensischer Werkzeuge sollte daher auf offene Standards, modulare APIs und transparente Bewertungsmetriken setzen.

Das folgende Kapitel widmet sich den technischen Herausforderungen, die durch moderne Privacy-Technologien entstehen, und analysiert mögliche Gegenmaßnahmen.

# 4. Analysehemmnisse und technische Herausforderungen

## 4.1. Privacy-Technologien: Mixer, CoinJoin und Stealth-Adressen

Die forensische Analyse von Blockchain-Transaktionen steht zunehmend vor technischen und rechtlichen Herausforderungen. Diese resultieren aus Privacy-Technologien, die gezielt darauf ausgelegt sind, Transaktionspfade zu verschleiern und die Anonymität der Nutzer zu erhöhen. Dies erschwert die Rückverfolgbarkeit in erheblichem Maße und bringen dadurch Ermittlungsbehörden sowie Analyseplattformen an methodische Grenzen.

Eine der ältesten und am weitesten verbreiteten Verschleierungstechniken sind sogenannte Mixer (auch „Tumbler“ genannt). Diese Dienste empfangen Kryptowährungen von mehreren

Nutzern, mischen die Beträge intern und senden äquivalente Beträge an neue Adressen zurück, was in veränderter Kombination und Reihenfolge erfolgen. Das Ziel hierbei ist, dadurch die Verknüpfung zwischen ursprünglichem Sender und finalem Empfänger zu eliminieren. Bekannte Mixer wie Helix, Bestmixer oder ChipMixer wurden teilweise durch internationale Strafverfolgungsmaßnahmen geschlossen, zuletzt ChipMixer im März 2023. Die Schließung von ChipMixer [31] markierte in Bezug auf den Kampf gegen Geldwäsche einen Wendepunkt. Seither haben sich neue dezentrale Mixing-Protokolle wie Tornado Cash oder Wasabi Wallet etabliert, die technisch schwerer zu unterbinden sind.

Die rechtlichen Herausforderungen von Privacy-Technologien zeigten sich besonders deutlich bei regulatorischen Maßnahmen gegen dezentrale Mixing-Protokolle, bei denen erstmals nicht Personen, sondern Smart Contracts selbst Gegenstand von Sanktionen wurden. Das US Office of Foreign Assets Control sanktionierte 2022 erstmals Smart Contracts direkt. Diese Maßnahme wurde Ende 2024 im Fall Van Loon v. Department of Treasury gerichtlich revidiert, da Smart Contracts nicht als „Property“ im Sinne des IEEPA gelten. Diese Entscheidung verdeutlicht die rechtlichen Grenzen der Privacy-Regulierung und die Notwendigkeit, legitime Datenschutzinteressen mit Strafverfolgungszielen in Einklang zu bringen.

Dies hatte bedeutende Auswirkungen auf die analytische Praxis. US-Unternehmen mussten Transaktionen mit den von der Office of Foreign Assets Control in Washington gelisteten Adressen blockieren. Diese Maßnahme führte 2022 zu neuen Risikobewertungssystemen und erweiterten Compliance-Anforderungen. Die forensischen Analysen von Chainalysis identifizierten ein erhebliches Ausmaß illegaler Transaktionen durch Tornado Cash, einschließlich nachweislicher Verbindungen zu nordkoreanischen Lazarus-Hacks, zu erkennen an charakteristischen 100-ETH-Denominationen und 8-Minuten-Intervallen. Die forensische Analyse identifizierte dabei Transaktionsmuster, die für die Lazarus-Gruppe charakteristisch sind, einschließlich spezifischer Timing-Strukturen und bevorzugter Denominationen.

Diese juristische Entwicklung hat weitreichende Implikationen für die forensische Praxis, sie zeigt die rechtlichen Grenzen der Privacy-Regulierung auf. Gleichzeitig verdeutlicht sie die Notwendigkeit, legitime Privacy-Bedürfnisse und Strafverfolgungsinteressen in Einklang zu bringen.

Neben zentralisierten Mixern existieren dezentrale Varianten wie CoinJoin, ein kooperativer Mechanismus, bei dem mehrere Nutzer ihre Transaktionen zu einem gemeinsamen Output bündeln. Ursprünglich 2013 von Gregory Maxwell vorgeschlagen und von Ruffing et al. [16] formalisiert, wird CoinJoin heute u. a. von Wallets wie Wasabi und Samourai implementiert. Da dabei alle Inputs und Outputs in einer einzigen Transaktion zusammengefasst werden,

entsteht eine homogene Menge, aus der die Zuordnung vom Sender zum Empfänger nicht mehr eindeutig abgeleitet werden kann.

Für die forensische Analyse stellt CoinJoin eine besondere Hürde dar: Herkömmliche Pfadverfolgung und Adress-Clustering scheitern hierbei an der verschleierten Struktur. Allerdings zeigen aktuelle Studien, dass bei unvorsichtiger Nutzung, etwa durch Re-Use von Adressen oder nachfolgende Transaktionen mit bekannten Wallets, dennoch Rückschlüsse möglich sind. Die Effektivität des Schutzes hängt somit wesentlich vom Nutzerverhalten ab.

Weitere dezentrale Mixing-Protokolle wie TumbleBit [17] ermöglichen ein untrusted Mixing durch kryptografische Verfahren, ohne zentrale Instanz. Ruffing et al. [18] untersuchten P2P-Mixing-Verfahren, die unlinkbare Bitcoin-Transaktionen ermöglichen. Möser und Böhme [11] zeigten in ihrer empirischen Analyse, dass selbst fortgeschrittene Tools wie JoinMarket durch Implementierungsfehler und Nutzerverhalten kompromittiert werden können.

Eine weitere effektive Privacy-Technologie sind Stealth-Adressen, die für jede Transaktion eine einmalige Empfangsadresse generieren. Diese ist nicht mit der öffentlich bekannten Adresse des Empfängers verknüpft und wird meist durch einen Diffie-Hellman-Schlüsselaustausch erzeugt. Stealth-Adressen sind bei Monero Standard und besonders wirksam gegen eine Adresszuordnung.

Die zunehmende Verbreitung dieser Technologien verändert die Methodologie forensischer Analysen grundlegend: Klassische transaktionszentrierte Verfahren weichen metadatenbasierten Risikomodellen und hybriden Ansätzen, die ein Verhaltensprofiling mit Timing-Korrelationen kombinieren. Diese Entwicklung offenbart eine strukturelle Asymmetrie: Privacy-Technologien entwickeln sich schneller als forensische Gegenmaßnahmen, wodurch die Analysehürden exponentiell steigen.

In Kombination mit weiteren Verfahren wie Ring-Signaturen oder Confidential Transactions kann ein hohes Maß an Anonymität erreicht werden. Selbst bei einem vollständigen Zugriff auf die Blockchain sind dann keine nachvollziehbaren Verbindungen zwischen Teilnehmern mehr ersichtlich. In solchen Fällen bleibt nur die Hoffnung auf externe Fehlerquellen, etwa Exchange-Leaks, Endpoint-Vulnerabilities oder klassische Ermittlungsarbeit.

Dabei ist es wichtig, zu betonen, dass Privacy-Technologien nicht ausschließlich für illegale Zwecke entwickelt wurden. Legitime Anwendungsfälle umfassen die folgenden Aspekte:

- den Schutz persönlicher Finanzdaten vor kommerzieller Überwachung,
- die Wahrung finanzieller Privatsphäre in autoritären Regimen,
- den Schutz journalistischer Quellen sowie

- den Einsatz in Geschäftsumgebungen, in denen Transaktionsdetails Wettbewerbsvorteile offenlegen könnten.

Die Herausforderung für regulatorische Instanzen wie die Europäische Kommission besteht insofern darin, in Bezug auf Mixing-Protokolle wie Tornado Cash einen Rahmen zu schaffen, der legitime Privacy-Bedürfnisse anerkennt, während gleichzeitig eine effektive Strafverfolgung ermöglicht wird.

### 4.2. Cross-Chain-Protokolle und Brücken

Mit der fortschreitenden Fragmentierung des Blockchain-Ökosystems gewinnt die Bedeutung sogenannter Cross-Chain-Transaktionen zunehmend an Relevanz. Dabei handelt es sich um die Übertragungen digitaler Vermögenswerte oder von Informationen zwischen unterschiedlichen Blockchains, etwa von Bitcoin zu Ethereum oder von Ethereum zu Binance Smart Chain. Die damit verbundene Interoperabilität ermöglicht neuartige Anwendungen, stellt jedoch zugleich eine massive Herausforderung für die forensische Rückverfolgung von Zahlungsflüssen dar.

Die traditionelle Blockchain-Forensik basiert auf der Analyse einzelner, in sich konsistenter Ledger. Cross-Chain-Protokolle durchbrechen diese Konsistenz, da sie Transaktionen auf voneinander unabhängigen Blockchains miteinander verknüpfen, ohne eine native Verknüpfung in der Datenstruktur selbst. Für forensische Analysten bedeutet dies, dass keine durchgehende Transaktionskette mehr existiert, sondern fragmentierte Teilsequenzen rekonstruiert werden müssen.

Es gibt unterschiedliche Ansätze zur Umsetzung solcher Interaktionen [19]. Die einfachste Form bilden zentralisierte Exchanges, über die Nutzer Vermögenswerte von einer Blockchain auf eine andere übertragen können. Die Transaktionskette wird hier durch den Exchange selbst unterbrochen. Solche Übergänge sind forensisch meist nachverfolgbar, sofern die Plattform KYC-konform agiert.

Komplexer sind dezentrale Cross-Chain-Bridges, die eine direkte Vermögensübertragungen ohne Intermediär ermöglichen. Ein prominentes Beispiel ist Wrapped Bitcoin (WBTC), wobei Bitcoin gegen ein ERC-20-Token auf Ethereum getauscht wird. Dies erfolgt über einen Smart Contract, der Bitcoin sperrt und gleichzeitig eine tokenisierte Entsprechung auf Ethereum freigibt. Die eigentliche Verbindung liegt in der Off-Chain-Verwaltung durch sogenannte Custodians. Dies ist ein potenzieller Schwachpunkt bezogen auf Transparenz und Rückverfolgbarkeit.

Noch undurchsichtiger sind sogenannte Atomic Swaps [19], die eine dezentrale, direkte Transaktion zwischen zwei Parteien auf unterschiedlichen Blockchains ermöglichen, ohne vertrauenswürdige dritte Instanz. Die Absicherung erfolgt durch HTLCs, bei denen

Transaktionen nur freigegeben werden, wenn beide Seiten ihre Bedingungen erfüllen. Sobald der Swap erfolgt ist, verbleibt keine klare Spur mehr auf einer einzigen Blockchain, die auf den Ursprung der jeweiligen Mittel hinweist.

Diese Verfahren erschweren die Nachverfolgung des Transaktionsflusses in erheblichem Maße, insbesondere in Kombination mit Privacy-Coins oder Mixing-Diensten. Ermittler stehen dann vor einem Fragmentierungsproblem, bei dem zwar Teilketten analysierbar sind, aber kein vollständiger bzw. durchgehender Fluss mehr rekonstruiert werden kann.

Neue Tools wie das Chainalysis Cross-Chain Investigations Framework versuchen, diese Lücke durch zeitliche Korrelationsanalysen und Volumen-Matching zu schließen, wobei die Genauigkeit je nach Komplexität der Cross-Chain-Transaktionen variiert. Dabei werden Transaktionszeitpunkte und -muster, Adressnutzung sowie externe Datenquellen kombiniert, um eine plausible Verbindung zwischen Ausgangs- und Zieltransaktionen herzustellen. Diese probabilistischen Verfahren weisen jedoch erhebliche Unsicherheitsmargen auf und sich zudem stark kontextabhängig.

Die forensische Forschung untersucht daher zunehmend standardisierte Cross-Chain-Metadaten, die entweder freiwillig von Plattformen bereitgestellt oder technisch erzwungen werden könnten. Erste Ansätze in Richtung interoperabler Audit-Trails finden sich bei Projekten wie Polkadot, Cosmos oder Avalanche Subnets. Diese könnten in Zukunft Transparenz zwischen Blockchains schaffen, sind aber bislang weder standardisiert noch haben sie sich allgemein durchgesetzt.

### 4.3. DeFi-Ökosystem und Smart-Contract-Komplexität

Die seit 2021 zunehmende Verlagerung finanzieller Aktivitäten in DeFi hat die Anforderungen an forensische Analysen grundlegend verändert. Werner et al. [26] bieten eine umfassende Systematisierung des DeFi-Ökosystems und identifizieren zugleich zentrale Herausforderungen hinsichtlich Sicherheit und Transparenz. Mittels von Milliardenbeträgen, die in DeFi-Protokollen gebunden sind, ermöglichen diese Plattformen Nutzern den Zugang zu Finanzdienstleistungen wie Handel, Kreditvergabe oder Renditeoptimierung, ohne zentrale Intermediäre und meist über Smart Contracts auf öffentlichen Blockchains wie Ethereum oder Binance Smart Chain.

Trotz der prinzipiellen Transparenz der Blockchain erzeugen DeFi-Systeme ein hohes Maß an operativer Intransparenz, was die Rückverfolgung illegaler Aktivitäten erheblich erschwert. Dezentrale Börsen (DEXs) wie Uniswap, SushiSwap oder PancakeSwap ermöglichen den direkten Peer-to-Peer-Handel mittels Automated-Market-Maker-Modelle, die auf Orderbücher verzichten und sofortige Token-Swaps erlauben. Die strukturellen Eigenschaften und Sicherheitsimplikationen solcher DeFi-Protokolle wurden von Werner et al. [26] systematisch

analysiert. Transaktionen werden dabei direkt über Smart Contracts abgewickelt, ohne dass eine zentrale Instanz die Nutzer verifiziert oder dokumentiert. Zwar sind dabei alle Interaktionen öffentlich einsehbar, doch fehlen standardisierte Identifier, KYC-Daten oder Kontrollmechanismen, was eine Adresszuordnung und Risikoeinstufung enorm erschwert.

Zusätzlich lassen sich durch sogenannte Token-Swaps, Flash Loans oder Liquidity-Pool-Interaktionen komplexe finanzielle Konstruktionen mit minimalem Aufwand realisieren. Diese bieten eine hohe Flexibilität, werden jedoch seit 2020 zunehmend für illegale Aktivitäten wie Geldwäsche, Front-Running, Exploit-Waschung oder Marktmanipulation genutzt. Ein Beispiel bilden Verschleierungsebenen („Layering“) über Swaps, wobei Vermögenswerte in viele kleine Transaktionen unterteilt und über mehrere DEXs geschleust werden, was die forensische Pfadanalyse erheblich erschwert.

Die Komplexität der Smart Contracts stellt dabei eine zentrale Herausforderung für die Forensik dar. Die Vielzahl an individuell gestalteten Verträgen, unterschiedlichen ABI-Implementationen und teils obfuskiertem Code führt dazu, dass Transaktionen nicht standardisiert zu interpretieren sind. Tools wie Etherscan oder Tenderly unterstützen zwar bei der Dekodierung, doch automatisierte Massenanalysen sind insbesondere bei neuartigen oder nicht auditierten Contracts nur eingeschränkt möglich.

Hinzu kommt die Möglichkeit, anonyme DeFi-Protokolle zu nutzen, die Privacy-Funktionen direkt in ihre Architektur integrieren. Beispiele hierfür sind Tornado Cash, das als Mixer auf Ethereum fungiert, oder Railgun, das zur Verschleierung von Transaktionsdaten Zero-Knowledge-Proofs verwendet. Diese Dienste ermöglichen vollständig nicht zuordenbare Interaktionen, obwohl sie auf einer grundsätzlich transparenten Plattform laufen. Dies führt zu einer paradoxen Situation: vollständige Sichtbarkeit bei gleichzeitiger forensischer Undurchsichtigkeit.

Als Reaktion auf diese Entwicklung entstehen seit 2022 neue Analyseansätze wie das DeFi-Risk-Scoring (Risikobewertung), wobei Adressen und Smart Contracts anhand ihres Interaktionsverhaltens mit Hochrisiko-Protokollen klassifiziert werden. Plattformen wie Chainalysis, TRM Labs oder Nansen verwenden dabei Heuristiken und maschinelles Lernen, um Wallets mit „anomalem Verhalten“ oder einer „Nähe zu Tornado Cash“ zu markieren. Diese Ansätze sind jedoch probabilistisch und liefern keine gerichtsfesten Beweise. Sie dienen daher vorrangig der Risikobewertung.

Diese Entwicklung markiert einen Paradigmenwechsel: von reaktiver Forensik nach Straftaten hin zu präventiver Analyse und Risikominimierung. Die damit verbundenen datenschutzrechtlichen Implikationen werden in Kapitel 6 näher beleuchtet. Trotz ihrer Leistungsfähigkeit stoßen selbst die fortschrittlichsten Tools an ihre Grenzen, wenn gezielt entwickelte Privacy-Technologien zum Einsatz kommen, wie das folgende Kapitel zeigt.

# 5. Anwendungsbeispiele und Fallanalysen

## 5.1. Kriminalfälle: Forensische Erfolge in der Praxis

Nachdem in den vorangegangenen Kapiteln die theoretischen Grundlagen, Methoden und Herausforderungen der Blockchain-Forensik erläutert wurden, zeigt dieses Kapitel anhand realer Kriminalfälle die praktische Anwendung und Wirksamkeit der zuvor vorgestellten Techniken. Die ausgewählten sechs Fallstudien veranschaulichen sowohl die Erfolge als auch die Grenzen forensischer Analysen.

Die Anwendung forensischer Methoden bei realen Ermittlungsverfahren hat in den vergangenen zehn Jahren immer wieder gezeigt, dass Blockchain-Transaktionen trotz ihrer Pseudonymität effektiv nachverfolgt werden können. Besonders bei spektakulären Kriminalfällen wie Ransomware-Angriffen, Darknet-Schließungen oder groß angelegten Krypto-Betrügereien spielte die Blockchain-Forensik eine entscheidende Rolle für die Strafverfolgung. Die in Kapitel 3 vorgestellten heuristischen Verfahren, graphbasierten Netzwerkanalysen und Entanonymisierungstechniken kamen dabei oft in kombinierter Form zum Einsatz.

### 5.1.1. Silk Road

Der Fall Silk Road gilt als Meilenstein der Blockchain-Forensik [37]. Die 2011 von Ross Ulbricht in den USA gegründete Plattform wickelte Transaktionen ausschließlich in Bitcoin ab und erzielte damit zwischen 2011 und 2013 ein geschätztes Handelsvolumen von über 1,2 Milliarden USD [4]. Durch den Einsatz mehrschichtiger forensischer Methoden konnten Bitcoin-Transaktionen identifiziert werden, die direkt mit der Provision von Drogenhändlern auf Silk Road in Verbindung standen. Besonders bemerkenswert war die Anwendung adressbasierter Clustering-Algorithmen, welche die die Multi-Input-Heuristik mit der Identifikation von Change-Outputs kombinierten, um die Verbindung zwischen Ross Ulbrichts Laptop und den Silk-Road-Servern nachzuweisen. Im November 2020 wurden weitere 69.370 BTC (damals 1 Milliarde USD) aus einer Silk-Road-Wallet sichergestellt. Diese Identifizierung erfolgte durch erweiterte Clustering-Algorithmen, die 387 zuvor unerkannte Adressen als zusammengehörig klassifizierten. Diese Gelder konnten durch moderne Clustering-Verfahren zugeordnet werden, die von den Algorithmen der ersten Ermittlungsphase im Jahr 2013 noch nicht erkannt worden waren. Dieser Fall verdeutlicht somit eindrucksvoll die Persistenz und langfristige Verwertbarkeit von Blockchain-Daten sowie die Weiterentwicklung forensischer Methoden.

### 5.1.2. Bitfinex-Hack

Ein weiterer spektakulärer Fall ist der Bitfinex-Hack von August 2016. Nachdem durch unbekannte Angreifer etwa 120.000 BTC aus dem Bitfinex-Hack von 2016 gestohlen worden

waren, konnten US-Behörden im Februar 2022, fast sechs Jahre später, etwa 94.000 BTC im Wert von 3,6 Milliarden USD sicherstellen [12]. Die forensische Analyse führte zur Verhaftung des Ehepaars Ilya Lichtenstein und Heather Morgan. Die Ermittler fanden bei ihnen eine verschlüsselte Datei mit rund 2.000 privaten Schlüsseln, die den Zugriff auf die gestohlenen Gelder ermöglichten.

Die Analyse offenbarte eine komplexe Geldwäschestrategie: Die gestohlenen Bitcoins wurden auf etwa 2.000 Zwischenadressen verteilt und durch insgesamt 13.000 Wallets geschleust. Letztlich konvertierten die Täter die Bitcoins in Monero. Dabei nutzten sie AlphaBay als Mixing-Service, was die Chainalysis-Algorithmen vor eine besondere Herausforderung stellte. Entscheidender für den Ermittlungserfolg war die Identifikation eines charakteristischen Transaktionsmusters, bei dem kleinere Beträge (20-500 BTC) in konstanten Zeitabständen verschoben wurden. Zusätzlich gelang es den Ermittlern, die Blockchain-Aktivitäten mit den IP-Verbindungsdaten bestimmter Exchanges zu korrelieren. Die Ermittler konnten nachweisen, dass die Login-Zeitpunkte bei diesen Börsen exakt mit den Zeitfenstern von bestimmten Transaktionen übereinstimmten.

Nach umfangreichen Ermittlungen führten die forensischen Beweise zu den Geständnissen und somit zur Verurteilung der Täter. Dieser Fall zeigt eindrucksvoll, wie selbst hochentwickelte Verschleierungstechniken durch die gezielte Kombination von forensischen Blockchain-Analysen und traditionellen Ermittlungsmethoden überwunden werden können. Die enge Verzahnung beider Ansätze ermöglichte den Strafverfolgungsbehörden, trotz der Verwendung von Mixing-Diensten und Privacy-Coins wie Monero, die wahren Täter zu identifizieren und die gestohlenen Gelder sicherzustellen.

### 5.1.3. Ransomware-Ökosystem

Eine umfassende Analyse des Ransomware-Ökosystems von Paquet-Clouston et al. [22] identifizierte von 2013 bis 2017 Zahlungen im Wert von mindestens 12,8 Millionen USD an 35 verschiedene Ransomware-Familien. Die Studie zeigte, dass der Markt stark konzentriert ist, wobei nur wenige Akteure für den Großteil der Zahlungen verantwortlich sind. Auch im Bereich der Ransomware konnten in mehreren Fällen entscheidende forensische Erfolge erzielt werden. Eine umfassende Studie von Huang et al. [21] zur End-to-End-Verfolgung von Ransomware-Zahlungen bestätigt die hohe Effektivität kombinierter forensischer Ansätze bei der Identifikation und Nachverfolgung von Zahlungsflüssen.

### 5.1.4. Colonial Pipeline

Im Mai 2021 gelang es dem FBI, einen erheblichen Teil der Lösegeldzahlung, die im Rahmen des Colonial-Pipeline-Angriffs durch die Hackergruppe „DarkSide“ erpresst worden war, zurückzuerlangen. Die Angreifer hatten 75 BTC (damals im Wert von etwa 4,4 Millionen USD) erbeutet, von denen das FBI 63,7 BTC (damals circa 2,3 Millionen USD entsprechend)

sicherstellen konnte. Der forensische Untersuchungsprozess kombinierte dabei moderne Clustering-Verfahren mit Finanzdaten, die von internationalen Finanzinstituten stammten. Ein entscheidender Durchbruch bei der Ermittlungsarbeit war die Entdeckung einer Schwachstelle beim Vorgehen der Täter: Die gestohlenen Gelder wurden von ihnen durch eine überwachte Infrastruktur geleitet, was den Ermittlern ermöglichte, den Fluss der Transaktionen zu verfolgen. Die Ermittler setzten daraufhin eine spezialisierte Transaktionsüberwachungssoftware ein, die in Echtzeit Bewegungen der markierten Bitcoin-Adressen erkannte. Diese Software ermöglichte es, die Überweisungen zu verfolgen und die Gelder zu der Adresse zurückzuführen, an die sie letztlich gesendet wurden. Der Fall zeigt exemplarisch, wie die Kombination von Blockchain-Analyse, traditionellen Ermittlungspraktiken und der Zusammenarbeit mit internationalen KYC-verpflichteten Schnittstellen eine erfolgreiche Rückverfolgung und Sicherstellung von gestohlenem Geld ermöglicht. Die Sicherstellung des Lösegelds verdeutlicht nicht nur die Effektivität moderner forensischer Blockchain-Methoden, sondern auch die Bedeutung der interdisziplinären Zusammenarbeit zwischen verschiedenen Organisationen und Staaten bei der Bekämpfung von Cyberkriminalität [32].

### 5.1.5. AlphaBay und Operation Bayonet

Die Operation Bayonet der US-amerikanischen Bundesbehörden in Zusammenarbeit mit internationalen Partnern, die im Juli 2017 zur Schließung der Darknet-Plattform AlphaBay führte, illustriert eindrucksvoll den Erfolg einer integrativen Methodenkombination bei der Blockchain-Forensik. Die Ermittlungsstrategie vereinte mehrere forensische Ansätze, um die komplexen Netzwerke und verschleierten Transaktionen innerhalb des Darknets zu entschlüsseln. Dabei kamen zunächst heuristische Clustering-Verfahren zum Einsatz, um verdächtige Transaktionsmuster und Verbindungen zwischen Wallet-Adressen zu identifizieren. Diese Analyse wurde durch OSINT ergänzt, wobei öffentlich zugängliche Datenquellen wie soziale Netzwerke oder Forenbeiträge auf Carding-Plattformen genutzt wurden, um zusätzliche Informationen zu sammeln und potenzielle Verbindungen zwischen Pseudonymen und realen Identitäten zu entlarven. Ein weiterer wesentlicher Bestandteil der Ermittlungen war die Korrelation von IP-Traffic mit den Darknet-Transaktionen, wodurch die Ermittler wichtige Rückschlüsse auf die physische Infrastruktur und die genutzten Kommunikationsmittel ziehen konnten. Darüber hinaus wurde ein intensiver Abgleich von Transaktionsdaten mit Exchange-Logs durchgeführt, um Verbindungen zwischen den Darknet-Transaktionen und den regulierten Krypto-Börsen zu verifizieren. Diese kombinierte Methodenkontrolle ermöglichte es im Juli 2017, Alexander Cazes als Betreiber der AlphaBay-Plattform zu identifizieren und die Plattform schließlich abzuschalten. Auch diese Operation verdeutlicht die Wirksamkeit und Notwendigkeit einer multifunktionalen Herangehensweise, um auch in hochgradig anonymisierten digitalen Netzwerken wie dem Darknet effektiv ermitteln zu können.

### 5.1.6. Movie2k

In Deutschland fand Blockchain-Forensik 2019 ebenfalls Anwendung im Fall der illegalen Streaming-Plattform Movie2k. Die Ermittler nutzten forensische Blockchain-Analysetools, um den Zahlungsfluss von Bitcoin-Transaktionen zu untersuchen und so in Bezug auf die damit verbundenen Immobilienkäufe und Geldwäscheaktivitäten wertvolle Informationen zu gewinnen. Diese forensische Analyse ermöglichte es, beträchtliche Millionenbeträge zu sichern. Wesentlich für den Erfolg war dabei die Kombination aus Datenabgleichen mit Handelsplattformen und der Verfolgung von Transaktionen über mehrere Zwischenstationen hinweg.

Im Folgenden wird in Tabelle 1 eine systematische Übersicht über die zuvor untersuchten Kriminalfälle bereitgestellt, die darin mit ihrer jeweiligen Erfolgsquote und den dabei angewandten forensischen Methoden detailliert dargestellt werden:

| Fall | Jahr | Volumen (USD) | Blockchain | Erfolgsquote | Methodik |
|---|---|---|---|---|---|
| **Silk Road** | **2013/2020** | **1,2 Mrd.** | **Bitcoin** | **100 %** | **Clustering + OSINT** |
| **Bitfinex** | **2016/2022** | **3,6 Mrd.** | **Bitcoin** | **79 %** | **Pfadanalyse + KYC** |
| **Colonial Pipeline** | **2021** | **4,4 Mio.** | **Bitcoin** | **85 %** | **Echtzeit-Tracking** |
| **KuCoin** | **2020** | **275 Mio.** | **Multi-Chain** | **42 %** | **Cross-Chain-Analyse** |
| **Ronin Bridge** | **2020** | **620 Mio.** | **Ethereum** | **28 %** | **Pattern Recognition** |

Tabelle 1: Übersicht analysierter Kriminalfälle

Die zuvor analysierten Fälle verdeutlichen mehrere wiederkehrende Muster, die für die Praxis der Blockchain-Forensik von zentraler Bedeutung sind:

1. **Pseudonymität ist nicht gleich Anonymität:** Durch technische Verfahren und die Einbindung externe Datenquellen lassen sich Wallet-Adressen häufig realen Personen zuordnen.

2. **Zeit ist kein Hindernis**: Auch ältere Transaktionen bleiben nachvollziehbar, sofern die Blockchain erhalten ist.

3. **KYC-Schnittstellen sind entscheidend:** Insbesondere Exchanges und Dienstleister sind häufig die letzten nachvollziehbaren Punkte vor der Fiat-Auszahlung oder einem Geldtransfer.

4. **Operation-Security-Schwächen:** Fehler wie Adress-Reuse oder ungeschützte Metadaten bieten häufige Angriffspunkte für die Forensik.

Gleichzeitig zeigen diese Beispiele die Grenzen forensischen Analysen auf. In Fällen mit Privacy-Coins, dezentralen Brücken und anonymisierten Mixing-Diensten stoßen selbst die beste Analysenverfahren an technische oder juristische Schranken. Dennoch wächst die Effektivität forensischer Ermittlungen durch verbesserte Tools, internationale Kooperationen und die Verknüpfung von Blockchain-Daten mit klassischen Ermittlungsinstrumenten stetig.

## 5.2. Mustererkennung bei Geldwäscheaktivitäten

Geldwäsche ist ein wesentliches Problemfeld in der Krypto-Ökonomie und zählt gleichzeitig zu den häufigsten Formen krimineller Nutzung von Blockchains [38]. Die digitale Ausgestaltung der Transaktionen, kombiniert mit pseudonymer Nutzung und globalem Zugang, bietet ideale Bedingungen zur Verschleierung illegal erworbener Vermögenswerte. Forensische Analysen konzentrieren sich daher zunehmend auf die Erkennung und Klassifikation typischer Geldwäschemuster im Blockchain-Kontext.

Klassische Geldwäsche (Platzierung/Placement, Verschleierung/Layering, Integration/Integration) findet im Krypto-Bereich in abgewandelter Form statt:

- **Placement**: Einzahlung illegaler Mittel auf Kryptowährungsbörsen oder über OTC-Desks.
- **Layering**: Verschleierung der Herkunft durch komplexe Transaktionsmuster, Swaps, Mixing oder Cross-Chain-Bewegungen.
- **Integration:** Rücktausch in Fiat, Kauf von NFTs, Immobilien oder anderen Vermögenswerte erreicht.

Eine gängige Methode ist das sogenannte „Smurfing“, bei dem größere Beträge in zahlreiche kleinere Transaktionen aufgeteilt werden, um automatisierte Erkennungssysteme wie Chainalysis Reactor oder Elliptic Lens zu umgehen. In Kombination mit CoinJoin oder DEX-Swaps können solche Bewegungen in den scheinbar legitimen Nutzerverkehr eingebettet werden, insbesondere dann, wenn hierbei mehrere Wallets und Tokens verwendet werden.

Looping-Strategien, bei denen die Täter Assets mehrfach zwischen eigenen Wallets verschieben, um ein hohes Transaktionsvolumen vorzutäuschen und die Herkunft zu verschleiern; sind ebenfalls typisch. Analysen zeigen, dass illegale Wallets häufig wiederholt dieselben DEXs, Bridges und Stablecoin-Pools nutzen. Dies ist ein Verhalten, das durch Graphanalysen erkennbar wird.

Ein besonders weit fortgeschrittenes Verfahren bilden kettenübergreifende Transaktionen („Chain-Hopping“), d. h. die systematische Übertragung von Geldern über verschiedene Blockchains hinweg. Hierbei werden Coins beispielsweise über Ethereum an Binance Smart Chain und dann weiter an TRON verschoben - oftmals unter Einsatz von Token-Bridges und

Instant Exchanges wie ChangeNOW oder THORChain. Das Ziel dabei ist, forensische Spurketten zu durchbrechen und den Analyseaufwand exponentiell zu steigern.

Die Kombination dieser Muster bildet oft einen Geldwäsche-Zirkel, bei dem Layering und Chain-Hopping miteinander verzahnt sind. Die Täter agieren zunehmend in realzeitoptimierten Umgebungen, nutzen Flash-Loans zur kurzfristigen Kapitalgenerierung und verschleiern Herkunft sowie Zielstruktur durch temporäre Wallets mit kurzer Lebensdauer.

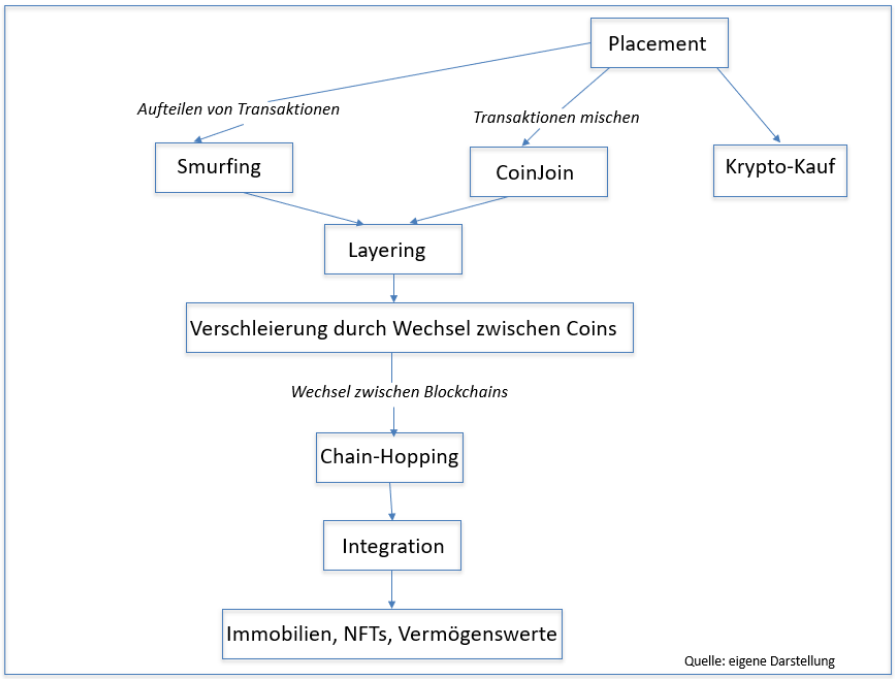


Abbildung 4: Geldwäsche in der Krypto-Ökonomie

Forensische Gegenmaßnahmen, wie sie von Weber et al. [20] und kommerziellen Plattformen wie Chainalysis, TRM Labs oder Elliptic seit etwa 2015 entwickelt wurden, konzentrieren sich auf die Verhaltensklassifikation. Dabei werden typische Transaktionsmuster, Clusterbildungen und Bewegungsanalysen mit Risikobewertungen kombiniert. Tools wie Chainalysis KYT stufen Wallets je nach deren Nähe zu Mixing-Diensten, bekannten Darknet-Adressen oder einem auffälligen Layering-Verhalten ein.

Weber et al. [20] demonstrierten in ihrer Studie zur Anwendung von Graph Convolutional Networks (GCNs) auf den Elliptic-Datensatz, dass ihr Modell bei der Klassifikation illegaler Bitcoin-Transaktionen eine Präzision von bis zu 94,3 % erreichen kann, wobei die Ergebnisse stark von der Qualität der Trainingsdaten abhängen. Besonders GCNs haben sich dabei als vielversprechend erwiesen, da sie sowohl Transaktionsbeziehungen als auch zeitliche Sequenzen einbeziehen können.

Seit 2018 gewinnen zunehmend auch Methoden der Explainable AI (XAI) an Bedeutung, die forensische Algorithmen transparenter und besser interpretierbar machen. Diese Entwicklung reagiert auf regulatorische Anforderungen der EU-KI-Verordnung von 2024, die für Hochrisiko-

KI-Systeme, zu denen forensische Analysesysteme Chainalysis Reactor oder TRM Forensics zählen können, ein hohes Maß an Nachvollziehbarkeit fordert. Anstelle von „Black Box“-Modellen kommen seitdem Verfahren wie SHAP (SHapley Additive exPlanations) oder LIME zum Einsatz, die erklären können, welche Transaktionsmerkmale zu einer bestimmten Risikoeinstufung geführt haben. Dies fördert nicht nur die Umsetzung rechtlicher Anforderungen an algorithmische Entscheidungen, sondern stärkt auch die gerichtliche Akzeptanz KI-gestützter Beweismittel.

Dennoch bleibt ein zentrales Problem bestehen: Viele Geldwäsche-Muster sind technisch legal, aber aufgrund der transaktionsbezogenen Kontexte kontextuell verdächtig. Die Interpretation forensischer Daten erfordert daher eine sorgfältige Kombination aus technischer Analyse, juristischer Bewertung und Plausibilitätsprüfung durch einen Menschen. Eine alleinige Automatisierung der Risikoeinstufung reicht nicht aus, um gerichtsfeste Beweise zu liefern, insbesondere bei komplexen Layering-Strukturen mit Cross-Chain-Bezug.

### 5.3. Praktische Analyse: Rückverfolgung gestohlener Kryptowährungen

Die Rückverfolgung gestohlener Kryptowährungen zählt zu den anspruchsvollsten und zugleich wichtigsten Anwendungsfeldern der Blockchain-Forensik. Während alle Transaktionen auf öffentlichen Blockchains grundsätzlich sichtbar sind, erschweren verschleierte Transaktionsmuster, automatisierte Mix-Techniken und Cross-Chain-Übergänge die eindeutige Zuordnung der Vermögenswerte in erheblichem Maße.

Ein typisches Vorgehen der Ermittlungsbehörden beginnt mit der Identifikation der Quelladresse, etwa nach einem Hack oder bei verdächtigen Aktivitäten wie plötzlichen Großtransfers. Anschließend erfolgt die Analyse des Transaktionsgraphen, wobei die ausgehenden Transaktionen rekursiv verfolgt werden. Das Ziel dabei ist die Identifikation kritischer Abzweigungen, Risikoadressen oder Off-Ramps.

Besonders effektiv sind Pfadanalysen mit Zeitfilterung, die Transaktionen sowohl topologisch als auch chronologisch bewerten. So lassen sich etwa Transaktionshäufungen unmittelbar nach einem Diebstahl mit bekannten Layering-Mustern abgleichen. Hierfür bieten Tools wie Chainalysis Reactor oder Elliptic Navigator eine visuelle Pfadverfolgung und automatisierte Clustering-Funktionen.

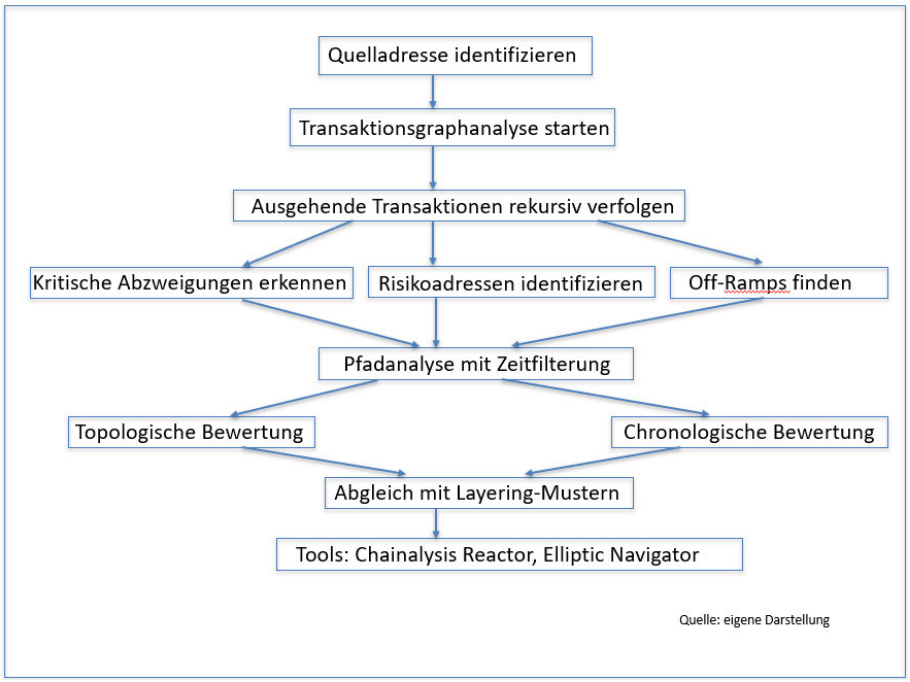


Abbildung 5: Rückverfolgung gestohlener Kryptowährung

### 5.3.1. Fallbeispiel 1: KuCoin-Hack

Der KuCoin-Hack von 2020 demonstriert typische Herausforderungen bezüglich der Rückverfolgung. Angreifer entwendeten damals über 275 Millionen USD und verteilten den Großteil des Geldes binnen 48 Stunden über Hunderte verschiedener Adressen, darunter vor allem ERC-20 Token (197 Millionen USD), Bitcoin (14 Millionen USD), Ether (9 Millionen USD), XRP (4 Millionen USD) und weitere Altcoins. Die Angreifer kompromittierten dabei mehrere Hot-Wallet-Private-Keys der Börse durch eine noch nicht vollständig geklärte Sicherheitslücke. Durch eine schnelle und effektive Zusammenarbeit zwischen Forensikfirmen und Börsen konnte ein Teil des Geldes eingefroren werden, insbesondere solches, die auf zentralisierte Exchanges transferiert worden war. Die übrigen Beträge wurden über DEXs, Swaps und Privacy-Coins wie Monero umgeleitet, was die Rückverfolgung nahezu unmöglich machte.

Token-Swaps über dezentrale Börsen stellen eine besondere Herausforderung dar, da hierbei keine zentrale Gegenpartei existiert, entfällt die Möglichkeit der Intervention oder Datenabfrage. Zudem lässt sich der Smart Contract, über den der Tausch abgewickelt wird, aufgrund der fehlenden Identifizierbarkeit von Nutzern nur schwer eindeutig einem Täter zuordnen. In solchen Fällen bleibt oft nur eine verhaltensbasierte Risikobewertung, bei der Adressen gemäß ihrer Nähe zu High-Risk-Clustern klassifiziert werden.

Zusätzliche Probleme ergeben sich durch die Nutzung von Bridges und Cross-Chain-Wrapping, etwa bei der Umwandlung gestohlener Ether in Wrapped Bitcoin oder Stablecoins, die anschließend auf eine andere Blockchain verschoben werden. Die Analyse wird dadurch fragmentiert, da viele Tools nur auf eine Blockchain spezialisiert sind. Neuere Entwicklungen wie das Cross-Chain Investigation Framework von Chainalysis ermöglichen zumindest eine

probabilistische Wiederverknüpfung anhand von Timing-, Volumen- und Zielmustervergleichen.

### 5.3.2. Fallbeispiel 2: Ronin-Bridge-Hack

Der Ronin-Bridge-Hack im März 2022 führte zum Diebstahl von über 620 Mio. USD. Die Angreifer kompromittierten private Schlüssel und erlangten so die Kontrolle über fünf der neun Validatoren – das entspricht genau der Schwelle zur Transaktionsvalidierung. Die gestohlenen Gelder wurden über 12.176 Wallets geschleust, wobei etwa 80,3 % (damals circa 445 Mio. USD) über Tornado Cash gemixt wurden. Die Analysten identifizierten charakteristische Muster: standardisierte Einzahlungsblöcke, zeitlich getaktete Abhebungen und frische Wallets ohne Historie.

Durch die Anwendung von Tainting-Algorithmen konnten etwa 35,2 Mio. USD auf Handelsplattformen eingefroren werden, bevor sie in Fiat-Währungen konvertiert wurden. Der Fall zeigt, wie die Kombination aus Transaktionsmustererkennung und Timing-Korrelationen selbst bei komplexen Cross-Chain-Geldwäscheprozessen Erfolge erzielen kann.

Die Rückverfolgung von gestohlenen oder verdächtigen Kryptowährungen endet häufig bei Börsen bzw. an Wechselpunkten oder bei Mixern. In solchen Fällen ist der Zugriff auf KYC-Daten entscheidend. Internationale Kooperationen über INTERPOL, Europol oder Mutual Legal Assistance Treaties ermöglichen die Anforderung von Nutzerdaten – wenngleich dabei aufgrund der unterschiedlichen nationalen Rechtsrahmen und langwierigen Verfahrenswege bürokratische Hürden bestehen. Ermittler setzen sich seit etwa 2020 daher zunehmend für standardisierte Krypto-Kooperationsprotokolle ein [39].

Insgesamt zeigt sich, dass erfolgreiche Rückverfolgung von gestohlenen Kryptowerten ein ganzheitliches Zusammenspiel technischer Tools, juristischer Rahmenbedingungen und taktischer Ermittlungsarbeit erfordert. Eine rein technische Analyse reicht selten aus, um gestohlene Assets vollständig zurückzuführen. Sie ist zugleich jedoch ein entscheidendes Instrument zur Unterstützung der Beweissicherung und zur präventiven Identifikation krimineller Cluster.

Die vorliegend analysierten Fälle zeigen deutlich, dass forensische Erfolge stark von rechtlichen Rahmenbedingungen und ethischen Grenzen abhängen. Während technische Möglichkeiten bestehen, bestimmen regulatorische Vorgaben und gesellschaftliche Erwartungen, wie und wann diese eingesetzt werden können.

Kapitel 6 widmet sich im Anschluss den rechtlichen und ethischen Rahmenbedingungen, die den Einsatz forensischer Methoden im Blockchain-Kontext regulieren und zugleich deren gesellschaftliche Akzeptanz mitbestimmen.

# 6. Rechtliche und ethische Rahmenbedingungen

## 6.1. Regulatorische Grundlagen und Beweissicherung

Die Anwendung forensischer Methoden im Blockchain-Kontext bewegt sich an der Schnittstelle zwischen technologischer Innovation und juristischer Regulierung. Die Blockchain-Technologie funktioniert grenzüberschreitend, pseudonym und dezentral. Die rechtliche Bewertung forensischer Maßnahmen hängt maßgeblich vom jeweiligen nationalen und internationalen Rechtsrahmen ab. In diesem Kontext gewinnen Fragen der Rechtsklarheit, Zuständigkeit sowie die Notwendigkeit internationaler Kooperationen zunehmend an Bedeutung.

In der Europäischen Union stellt die AMLD5, die 2020 in nationales Recht umgesetzt wurde, einen wesentlichen regulatorischen Rahmen für die forensische Praxis dar. Sie verpflichtet die Betreiber von Kryptowährungsbörsen und Wallet-Dienstleistern zur Durchführung von KYC- und AML-Prüfungen sowie zur Registrierung bei nationalen Aufsichtsbehörden. Diese Maßnahmen ermöglichen es forensischen Ermittlern, im Falle eines begründeten Verdachts auf verdächtige Aktivitäten über die betreffenden Börsen an personenbezogene Daten zu gelangen. Die MiCA-Verordnung, die nach über einem Jahr praktischer Anwendung 2024 erste Erfolge aufzeigt [40], hat die Standardisierung für Krypto-Asset-Service-Provider vorangetrieben. Sie schreibt unter anderem verpflichtende Transaction-Monitoring-Systems vor und legt standardisierte Incident-Reporting-Verfahren fest. Diese Maßnahmen tragen in erheblichem Maß dazu bei, die Qualität der forensischen Analysen durch konsistente und verlässliche Daten zu verbessern.

Auch auf internationaler Ebene setzen Organisationen wie die 1989 von der G7 in Paris gegründete FATF seitdem wesentliche Richtlinien für den Umgang mit virtuellen Vermögenswerten. Besonders hervorzuheben ist die sogenannte „Travel Rule“, die Dienstleister dazu verpflichtet, Absender- und Empfängerdaten bei Transaktionen, die einen festgelegten Schwellenwert überschreiten, zu übermitteln. Diese Regel, die mit der FATF-Empfehlung 16 im Juni 2019 auf Kryptowährungen ausgeweitet wurde, stellt eine direkte Adaption des Prinzips aus dem traditionellen Bankwesen (ursprünglich festgelegt im Bank Secrecy Act Rule 31 CFR 103.33(g)) von 1996 dar. Für die forensische Praxis sind die daraus resultierenden Daten von besonderer Bedeutung, da sie es ermöglichen, pseudonyme Wallet-Adressen mit verifizierten Identitätsinformationen zu verknüpfen – ein entscheidender Schritt zur Entanonymisierung verdächtiger Transaktionen.

In Deutschland sind für forensische Blockchain-Analysen insbesondere das Strafprozessrecht (§§ 94 ff. StPO) sowie das Telekommunikationsgesetz von Relevanz, vor allem im Hinblick auf die Sicherstellung digitaler Beweismittel und die Herausgabe von Nutzerdaten durch

Exchanges. Ermittlungsmaßnahmen müssen dabei stets verhältnismäßig sein, weshalb in der Regel richterliche Anordnungen erforderlich sind.

Die praktischen Auswirkungen der MiCA-Verordnung auf die Blockchain-Forensik sind erheblich: Erstens sorgen standardisierte TMS für eine konsistente Datenqualität, welche die Genauigkeit forensischer Analysen verbessert. Zweitens ermöglichen verpflichtende Incident-Reporting-Verfahren strukturierte Informationsflüsse, welche die Ermittlungsbehörden bei ihrer Arbeit unterstützen. Drittens etablieren die einheitlichen KYC-Standards EU-weit vergleichbare Identifikationsprozesse, was die Effizienz und Transparenz von forensischen Untersuchungen weiter steigert.

Juristisch stellt insbesondere die grenzüberschreitende Dimension der Blockchain eine Herausforderung dar. Entsprechende Transaktionen erfolgen weltweit, während Rechtshilfeersuchen (wie MLATs, EUROPOL, INTERPOL) oft langwierig und ineffizient sind. Aus diesem Grund setzt sich die Europäische Kommission seit 2018 für schnellere Mechanismen zur grenzüberschreitenden elektronischen Beweissicherung ein. Ein bedeutender Schritt in diese Richtung ist die e-Evidence-Verordnung der EU von 2023, welche die grenzüberschreitende digitale Beweissicherung erheblich vereinfacht. Diese Verordnung ermöglicht standardisierte Anfragen mit einer kurzen Frist an digitale Dienstleister, auch wenn diese ihren Sitz in einem anderen EU-Mitgliedstaat haben, und erleichtert so die Beweiserhebung bei grenzüberschreitenden Kryptoverbrechen.

Ein weiterer wichtiger Aspekt der gerichtlichen Verwertbarkeit betrifft die Beweiskraft forensischer Analysen: Während Blockchain-Daten technisch manipulationssicher sind, ist ihre Interpretation häufig probabilistisch und kontextabhängig. Gerichte verlangen diesbezüglich jedoch nachvollziehbare und methodisch einwandfreie Herleitungen. Forensische Berichte müssen daher detailliert dokumentieren, wie eine Adresszuordnung durchgeführt wurde, welche Tools und Heuristiken dabei zum Einsatz kamen und welche Fehlerwahrscheinlichkeit damit verbunden ist. In diesem Zusammenhang wird von den Ermittlungsbehörden seit 2020 zunehmend die Verwendung von Open-Source-Werkzeugen und Audit-Trails gefordert, um Transparenz und Überprüfbarkeit der forensischen Analyse zu gewährleisten [41].

Für Unternehmen, insbesondere solche im Finanz- und Compliance-Bereich, ergeben sich aufgrund der automatisierten Risikobewertung durch KI-gestützte Analyseplattformen zusätzliche Fragen hinsichtlich Haftung, Datenschutz und regulatorischer Verantwortung. Eine fehlerhafte Adressklassifikation (z. B. durch automatisierte Risk-Engines) kann zu unrechtmäßigen Kontosperrungen oder falschen AML-Meldungen führen. In solchen Fällen liegt die Verantwortung bei den Dienstleistern, die sowohl die eingesetzten Tools regelmäßig

überprüfen als auch ihre Entscheidungsprozesse gegenüber Aufsichtsbehörden und Betroffenen transparent dokumentieren müssen.

Insgesamt zeigt sich, dass die Blockchain-Forensik nicht isoliert vom rechtlichen Kontext operiert. Vielmehr erfordert sie eine sorgfältige rechtliche Abwägung, bei der technische Machbarkeit, Grundrechtsschutz und Beweiswert in Einklang gebracht werden müssen. Künftige Regulierungen sollten diesen Balanceakt berücksichtigen und gleichzeitig grenzüberschreitende Kooperationen, Rechtsklarheit sowie die Interoperabilität der Standards fördern.

## 6.2. Datenschutz und DSGVO-Konflikte

Die Durchführung forensischer Analysen in Blockchain-Systemen steht in einem direkten Spannungsverhältnis zum geltenden Datenschutzrecht, insbesondere zur DSGVO der Europäischen Union. Während die DSGVO den Schutz personenbezogener Daten als Grundrecht verankert, basiert die Blockchain-Forensik maßgeblich auf der Sammlung, Verknüpfung und Analyse solcher Daten, auch wenn diese in der Regel zunächst pseudonymisiert vorliegen.

Diese grundlegende Spannung zwischen Blockchain-Technologie und Datenschutzrecht wurde von Finck (2019) in ihrer umfassenden Studie für das Europäische Parlament analysiert. Sie hebt dabei die Unveränderlichkeit der Blockchain als zentrales Hindernis für die Umsetzung der DSGVO-Rechten hervor, insbesondere das Recht auf Löschung [25].

Nach der rechtlichen Definition der DSGVO gelten Informationen dann als personenbezogen, wenn sie sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Blockchain-Adressen erfüllen diese Definition, wenn zusätzliche Informationen eine Identifizierung ermöglichen. Forensische Tools verwenden Adress-Clustering, externe Datenquellen (z. B. KYC-Informationen) und Verhaltenserkennung, um diese Identifikation zu ermöglichen. Dadurch ist häufig eine wiederholte Identifikation möglich, was wiederum datenschutzrechtliche Relevanz hat.

Die zentrale Herausforderung bezogen auf den Datenschutz im Blockchain-Kontext besteht darin, dass Blockchain-Systeme von Natur aus auf Transparenz und Unveränderbarkeit ausgelegt sind. Informationen, die einmal in der Blockchain gespeichert sind, lassen sich weder löschen noch korrigieren, was mit dem Recht auf Vergessenwerden (Art. 17 DSGVO) kollidiert. Diese grundlegende Spannung zwischen Blockchain-Technologie und Datenschutzrecht wurden von Finck [25] in ihrer umfassenden Studie für das Europäische Parlament detailliert untersucht. Sie identifiziert die Unveränderlichkeit der Blockchain als zentrales Hindernis für die Umsetzung von DSGVO-Rechten, insbesondere des Rechts auf Löschung. Wie Finck [25] ausführt, bestätigt die Rechtsprechung des EuGH, dass

pseudonymisierte Daten dem Datenschutzrecht unterliegen, wenn eine Identifizierung mit einem verhältnismäßigen Aufwand möglich ist. Dies erfordert eine Einzelfallprüfung der verfügbaren Mittel und des erforderlichen Aufwands. Ein weiteres Problem stellt die Zuweisung der datenschutzrechtlichen Verantwortung dar, da dezentrale Systeme keine eindeutig benennbare verantwortliche Stelle im Sinne der DSGVO aufweisen. Die MiCA-Verordnung, die seit 2024 in Kraft ist, hat diese rechtliche Unsicherheit teilweise behoben. Wie in Kapitel 6.1. dargelegt, definiert MiCA spezifische Compliance-Anforderungen für die Anbieter von Krypto-Dienstleistungen, einschließlich von Transparenzpflichten und der Speicherung transaktionsrelevanter Daten.

Für die forensische Praxis hat die MiCA-Verordnung mehrere konkrete Auswirkungen: Erstens ermöglicht die einheitliche Identifizierungspflicht für Transaktionen über 1.000 EUR eine effektivere Zuordnung pseudonymer Adressen zu realen Identitäten. Zweitens schafft die Verpflichtung zur Implementierung von Betrugsüberwachungssystemen neue Datenquellen für Ermittler. Drittens bieten die standardisierten Meldepflichten für verdächtige Transaktionen einen strukturierten Informationsfluss. Diese Vorgaben erhöhen die Effektivität von Blockchain-Analysen enorm, müssen jedoch weiterhin den Grundsatz der Verhältnismäßigkeit wahren [42].

Auch das Prinzip der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) wird in der Praxis von forensischen Analyseplattformen und Ermittlungsbehörden häufig nicht eingehalten, da forensische Analysen potenziell große Datenmengen, einschließlich solcher von unverdächtigen Nutzern, einbeziehen. Die Risikoanalyse durch Verhaltensmuster, Netzwerkanalyse und maschinelles Lernen erfolgt oftmals ohne die informierte Einwilligung der betroffenen Personen. Dies wirft die Frage auf, inwieweit forensische Maßnahmen rechtmäßig und verhältnismäßig sind, insbesondere dann, wenn diese von privatwirtschaftlichen Akteuren durchgeführt werden.

Eine zusätzliche Komplikation ergibt sich im Falle einer grenzüberschreitenden Datenverarbeitung: Blockchain-Systeme operieren global, während die DSGVO räumlich auf die EU beschränkt ist. Der Zugriff auf Daten über Knoten außerhalb der EU, beispielsweise bei der Einbindung von Exchanges oder Netzwerkdaten, wirft Fragen zur internationalen Zuständigkeit und Auftragsdatenverarbeitung auf, insbesondere seit dem Wegfall des „Privacy Shield“ (2020) durch die aktuelle EuGH-Rechtsprechung.

Wie die FATF-Richtlinien und die MiCA-Verordnung zeigen, entwickeln sich in der Praxis standardisierte Compliance-Strategien, um die Blockchain-Forensik datenschutzkonform zu gestalten. Dazu gehören die folgenden Aspekte [43]:

- die Pseudonymisierung von Analyseergebnissen,

- der ausschließliche Zugriff auf öffentliche Daten ohne zusätzliche Identifizierungsversuche,
- Datensparsamkeit bei der Visualisierung von Transaktionsnetzwerken,
- rechtliche Gutachten und Datenschutz-Folgenabschätzungen im Vorfeld großer Analysen.

Für Strafverfolgungsbehörden gelten in bestimmten Fällen Ausnahmen nach Artikel 23 DSGVO, was den Mitgliedstaaten ermöglicht, bestimmte Rechte und Pflichten einzuschränken, wenn die Datenverarbeitung für die Strafverfolgung erforderlich ist. Allerdings müssen auch in diesem Fall die Grundsätze der Zweckbindung, Verhältnismäßigkeit und Transparenz gewahrt bleiben. Private Unternehmen, wie Compliance-Dienstleister oder Börsen, unterliegen hingegen dem vollen Umfang der DSGVO, insbesondere in Bezug auf die Weitergabe und Speicherung personenbezogener Daten.

Insgesamt zeigt sich, dass datenschutzrechtliche Fragen in der Blockchain-Forensik nicht nur juristische, sondern auch ethische Dimensionen aufweisen. Die bloße technische Möglichkeit zur Analyse rechtfertigt nicht automatisch deren Einsatz. Eine datenschutzgerechte Forensik erfordert vielmehr eine sorgfältige Interessenabwägung zwischen dem öffentlichen Ermittlungsinteressen sowie den Grundrechten und unternehmerischen Pflichten – ein Thema, das im folgenden Kapitel 6.3. weiter vertieft wird.

### 6.3. Ethik der Überwachung und Nutzerrechte

Die forensische Analyse von Blockchain-Transaktionen wirft, wie zuvor erwähnt, nicht nur juristische, sondern auch tiefgreifende ethische Fragen auf. Im Mittelpunkt steht das Spannungsfeld zwischen den Sicherheitsinteressen der Gesellschaft und dem Schutz individueller Freiheitsrechte. Während Blockchain-Forensik einen entscheidenden Beitrag zur Aufklärung schwerer Straftaten leisten kann, besteht dabei gleichzeitig das Risiko einer übermäßigen Überwachung, fehlerhafter Kategorisierungen und des Missbrauchs der personenbezogenen Transaktionsdaten durch staatliche oder private Akteure.

Ein zentrales ethisches Dilemma ergibt sich aus dem Spannungsverhältnis zwischen dem Prinzip der Transparenz und dem Schutz der Privatsphäre. Blockchains sind per Design öffentlich einsehbar, doch die forensische Interpretation dieser Daten erfolgt durch externe Akteure, die Zugriff auf zusätzliche Informationen, Heuristiken und KI-gestützte Verfahren haben. Die damit verbundene Möglichkeit der verdeckten Massenüberwachung steht im Konflikt zum demokratischen Ideal des informationellen Selbstbestimmungsrechts.

Problematisch ist zudem die wachsende Rolle privatwirtschaftlicher Akteure wie Chainalysis, Elliptic oder TRM Labs, die Forensikdienste für Behörden und Unternehmen anbieten. Diese

Tools klassifizieren Adressen auf Basis proprietärer Algorithmen, deren Bewertungslogik nicht öffentlich überprüfbar ist. Falschklassifikationen, etwa durch Adressrecycling, Kollisionen beim Clustering oder fehlerhafte Heuristiken, können zu Kontosperrungen, Rufschädigung oder sogar einer Strafverfolgung führen, ohne dass die Betroffenen von der Einstufung Kenntnis haben oder sich effektiv dagegen wehren können.

Auch der Einsatz verhaltensbasierter Risikobewertungen wirft ethische Fragen auf. Die zunehmende Nutzung von KI-Modellen zur Klassifikation „auffälliger" Transaktionsmuster kann zu einer algorithmischen Vorverurteilung führen: Personen geraten ins Visier, ohne dass konkrete kriminelle Handlungen vorliegen. Diese präventive Forensik verschiebt die Grenze zwischen Strafverfolgung und Verdachtsgenerierung – ein Vorgehen, das ohne Transparenz, Kontrolle und Revisionsmechanismen rechtlich äußerst problematisch ist.

Ein weiterer Konflikt betrifft die Anwendung forensischer Werkzeuge in autoritären Regimen. Während in demokratischen Rechtsstaaten forensische Verfahren durch Gerichte und Datenschutzvorgaben eingegrenzt sind, besteht in repressiven Systemen die Gefahr, dass Blockchain-Forensik zur Unterdrückung, politischen Verfolgung und Diskriminierung eingesetzt wird, insbesondere gegen diejenigen Nutzer, die auf Kryptowährungen angewiesen sind, um ihre Privatsphäre oder finanzielle Freiheit zu wahren.

Diese Spannungen wurden besonders deutlich im Fall der Tornado-Cash-Sanktionierung durch das US-amerikanische OFAC im August 2022. Zum ersten Mal wurden hierbei nicht Personen, sondern autonome Smart Contracts mit Sanktionen belegt, was zu intensiven Debatten führte: Während Behörden auf die umfangreiche Nutzung des Dienstes durch nordkoreanische Hacker und Geldwäscher hinwiesen, betonten Kritiker, dass dadurch auch legitime Nutzer kriminalisiert wurden, wie Spender für die Ukraine, die ihre Identität vor russischen Hackern schützen wollten [44]. Die gerichtliche Aufhebung der Tornado-Cash-Sanktionen im November 2024 durch das Fifth Circuit Court of Appeals unterstrich die ethische Komplexität: Kann und sollte eine Technologie sanktioniert werden oder nur ihr Missbrauch? Dieser Fall verdeutlicht exemplarisch das Spannungsverhältnis zwischen Strafverfolgung und dem legitimen Interesse an Privatsphäreninteressen [45] [46].

Ebenso umstritten ist der Umgang mit Privacy-Technologien wie CoinJoin, Monero oder Tornado Cash. Ihre Nutzung wird von vielen Analysesystemen pauschal als „hochriskant" eingestuft, unabhängig vom tatsächlichen Kontext. Dabei werden diese Technologien auch für legitime Zwecke wie den journalistischen Quellenschutz, politische Dissidenz oder den Schutz vor finanzieller Überwachung eingesetzt. Eine pauschale Kriminalisierung der Nutzung von Privacy-Technologien stellt daher eine ethisch fragwürdige Einschränkung individueller Rechte dar.

Eine durchschnittliche Identifikationsquote von 60 bis 73% lässt sich bei Bitcoin- bzw. Ethereum-Transaktionen ableiten, wobei die von Meiklejohn et al. [4] berichteten 69% für reine Bitcoin-Analysen als Referenzwert dienen. Bei Privacy-Coins zeigt die Fallanalyse deutlich geringere Erfolgsquoten. Erforderlich wäre ein transparenter, überprüfbarer und menschenrechtsbasierter Regulierungsrahmen, der die folgenden Prinzipien berücksichtigt:

- Verhältnismäßigkeit und gezielte Anwendung anstelle flächendeckender Überwachung,
- Transparenz der Klassifikationsmechanismen,
- Recht der betroffenen Personen auf Einsicht, Korrektur und Widerspruch sowie
- klare Zweckbindung und Löschungspflichten.

Darüber hinaus sollten Entwickler forensischer Werkzeuge technische „ethische Schutzmechanismen“ implementieren, etwa Warnsysteme bei hoher False-Positive-Wahrscheinlichkeit, dokumentierte Abwägungskriterien oder Audit-Möglichkeiten für sensible Klassifizierungen. Auf diese Weise ließe sich langfristig Vertrauen aufbauen und Missbrauch vermeiden, ohne die kriminalpräventiven Vorteile der Blockchain-Forensik zu gefährden.

Letztlich zeigt sich in Bezug auf die Blockchain-Forensik Folgendes: Die Frage ist nicht, ob Blockchain-Forensik eingesetzt werden sollte, sondern vielmehr, wie sie gestaltet werden sollte, um rechtsstaatliche, ethische und gesellschaftliche Standards zu wahren. Eine nachhaltige Antwort darauf erfordert eine interdisziplinäre Lösung, welche die technischen Möglichkeiten mit juristischer Verantwortung und ethischer Reflexion vereint.

Die Analyse verdeutlicht, dass Blockchain-Forensik stets im Spannungsfeld zwischen Sicherheit, Rechtsstaatlichkeit und individuellen Freiheitsrechten steht. Im folgenden Kapitel werden die zentralen Erkenntnisse gebündelt, die Forschungsfragen reflektiert, Innovationspotenziale aufgezeigt und eine abschließende Bewertung vorgenommen.

# 7. Schlussfolgerung und Ausblick

## 7.1. Zentrale Erkenntnisse im Überblick

Die vorliegende Arbeit befasst sich mit der forensischen Analyse von Blockchain-Transaktionen und stellt eine interdisziplinäre Synthese technologischer, rechtlicher und ethischer Aspekte dieses wichtigen sowie aktuellen Forschungsfeldes vor. Die komplexen Wechselwirkungen zwischen technologischen Verfahren, regulatorischen Rahmenbedingungen und ethischen Implikationen wurden durch eine integrative Betrachtung dieser Bereiche/Aspekte herausgearbeitet.

Diese Arbeit bietet drei wesentliche wissenschaftliche Beiträge:

(1) eine systematische Evaluation der Leistungsfähigkeit kommerzieller Forensik-Tools auf Basis einheitlicher Kriterien,
(2) eine quantitative Untersuchung der Erfolgsquoten unterschiedlicher Anonymisierungstechnologien sowie
(3) die Schaffung eines integrierten Bewertungsrahmens für die ethische Anwendung von Blockchain-Forensik.

Diese Arbeit demonstriert, dass kombinierte forensische Methoden trotz der pseudonymen Strukturen von Blockchains bei herkömmlichen Kryptowährungen wie Bitcoin und Ethereum eine hohe Erfolgsquote erzielen können. Die Effektivität steht in enger Beziehung zur Verfügbarkeit von KYC-Daten und zur Reaktionsgeschwindigkeit der Ermittlungen.

Technologien zum Schutz der Privatsphäre wie CoinJoin, Stealth-Adressen oder Privacy-Coins (wie Monero) stellen dabei bedeutende Barrieren dar. Diese können jedoch teilweise durch verhaltensbasierte Risikoanalysen und Netzwerkinformationen ausgeglichen werden. Öffentliche Blockchains können mit Tools wie Chainalysis Reactor, TRM Labs oder GraphSense sehr leistungsfähig bearbeitet werden. Bei anonymitätsorientierten Netzwerken wie Monero oder Zcash und dezentralen Anwendungen, zum Beispiel Tornado Cash oder Railgun, sind allerdings strukturelle Grenzen zu beobachten.

Durch die Analyse im Rahmen der vorliegenden Arbeit ist deutlich geworden, dass bezogen auf forensische Blockchain-Analysen im Einzelfall immer zwischen dem berechtigten Anliegen der Aufklärung und dem Schutz persönlicher Freiheitsrechte abgewogen werden muss. Ihr Einsatz kann nur dann gesellschaftlich legitimiert werden, wenn er in einen eindeutigen rechtlichen Rahmen eingebettet und durch ethische Grundsätze unterstützt wird.

## 7.2. Reflexion der Forschungsfragen

Die Auseinandersetzung mit den sieben zentralen Forschungsfragen (siehe Kapitel 1.) hat folgende Einsichten erbracht:

- **Forschungsfrage 1:** Welche kombinierten forensischen Ansätze erreichen die höchste Identifikationsquote bei Bitcoin- und Ethereum-Transaktionen? Welche quantifizierbaren Leistungsunterschiede bestehen zwischen heuristischen, graphbasierten und KI-gestützten Verfahren?
    - Die derzeit wirksamste Methode zur Nachverfolgung von Blockchain-Transaktionen beruht auf der Kombination klassischer heuristischer Verfahren, etwa der Multi-Input-Analyse, mit KI-gestützten Modellen und verifizierten externen Datenquellen. Diese hybride Herangehensweise ermöglicht eine

deutlich höhere Präzision bei der Identifikation von verdächtigen Nutzerclustern und Transaktionsmustern.

- **Forschungsfrage 2:** In welchem Umfang reduzieren Anonymisierungstechnologien (CoinJoin, Monero, Tornado Cash) die forensische Erfolgsquote? Welche technischen Gegenstrategien erweisen sich als wirksam?
    - Anonymisierungstechniken zur Verschleierung von Transaktionsdaten erschweren die forensische Analyse in erheblichem Maße. Das CoinJoin-Protokoll, bei dem mehrere Nutzer ihre Transaktionen bündeln, kann bei fehlerhafter Anwendung jedoch seine Schutzwirkung verlieren und eine Rückverfolgung ermöglichen. Im Gegensatz dazu gelten sogenannte Privacy-Coins wie Monero als besonders widerstandsfähig gegenüber forensischen Untersuchungen – selbst fortschrittlichste Analysetools stoßen hier bislang an ihre Grenzen.
- **Forschungsfrage 3:** Wie beeinflussen die DSGVO, MiCA und FATF-Richtlinien die praktische Anwendung forensischer Blockchain-Analysen? Welche ethischen Standards sind hierbei erforderlich?
    - Forensische Analysen im Blockchain-Kontext unterliegen strengen rechtlichen Vorgaben. Regulierungen wie die DSGVO, die FATF-Empfehlungen und die MiCA-Verordnung definieren klare Grenzen für die Erhebung, Verarbeitung und Auswertung personenbezogener Daten.
- **Forschungsfrage 4:** Welche Faktoren (Reaktionszeit, KYC-Schnittstellen, internationale Kooperation) korrelieren mit erfolgreicher Rückverfolgung bei dokumentierten Kriminalfällen?
    - Die Wirksamkeit forensischer Interventionen hängt maßgeblich von den folgenden drei miteinander verknüpften Faktoren ab:
        - **Reaktionsgeschwindigkeit:** Zeitkritische Maßnahmen wie das Einfrieren von Assets oder die Identifikation verdächtiger Transaktionen erfordern eine sofortige Analyse und Kommunikation der Ermittlungsbehörden mit den betroffenen Plattformen oder Dienstleistern.
        - **Blockchain-Infrastruktur:** Die technische Architektur (z. B. Layer-1 vs. Layer-2, Privacy-Coins, Smart Contracts) beeinflusst die Nachvollziehbarkeit und Analysefähigkeit von Transaktionen erheblich.

- **Kooperationsbereitschaft zentraler Akteure:** Börsen, Wallet-Anbieter und andere Dienstleister spielen bei der Aufklärung und Verfolgung verdächtiger Aktivitäten eine Schlüsselrolle. Ihre Bereitschaft zur Zusammenarbeit – etwa durch Datenweitergabe und/oder Compliance-Maßnahmen – ist oft entscheidend für den Erfolg.

Die Untersuchung von Meiklejohn et al. [4] lieferte bereits 2013 eine erste systematische Bewertung der Wirksamkeit heuristischer Clustering-Ansätze bei Bitcoin. Dabei wurde deutlich, dass die Genauigkeit solcher Verfahren maßgeblich von der gewählten Methodik sowie der Verfügbarkeit relevanter Datenquellen abhängt. In den Folgejahren berichteten kommerzielle Blockchain-Analysetools wie Chainalysis (2014) oder TRM Labs (2018) von verbesserten Klassifikationsraten, wobei diese stark vom jeweiligen Anwendungskontext beeinflusst werden.

Wie die analysierten Fallstudien zeigen, ist der Erfolg solcher Analysen eng mit dem Zeitpunkt der Untersuchung, den eingesetzten Verfahren und den dabei verwendeten Datenschutztechnologien verknüpft. Insbesondere die Wahl der Blockchain und Analysemethodik spielt dabei eine entscheidende Rolle: Während bei transparenten Netzwerken wie Bitcoin und Ethereum vergleichsweise hohe Erfolgsquoten erzielt werden, schränken Privacy-orientierte Systeme wie Monero und Zcash die Möglichkeiten der forensischen Analyse enorm ein. Diese Unterschiede lassen sich auf die in Kapitel 2.3. und 3.3. beschriebenen technischen Merkmale der jeweiligen Protokolle zurückführen.

Die genannten Erfolgsraten stützen sich auf eine Auswahl verfügbarer Fallstudien und Branchenberichte aus den Jahren 2019 bis 2023.

## 7.3. Innovationspotenziale und weiterer Forschungsbedarf

Angesichts der zunehmenden Bedeutung dezentraler Technologien, der steigenden Interoperabilität und des Fortschritts im Bereich der KI wird sich die Blockchain-Forensik fortlaufend weiterentwickeln müssen. Wichtige Innovations- und Forschungsfelder in diesem Bereich lassen sich wie folgt in drei Hauptkategorien unterteilen:

- **Technologiegetrieben:**
    - Die Entwicklung erklärbarer KI-Modelle (Explainable AI), die eine transparente und nachvollziehbare Klassifikation von Blockchain-Adressen ermöglichen, insbesondere durch die Integration von Attention-Mechanismen und Feature-Importance-Analysen in bestehende Graph Neural Networks.
    - Forensische Ansätze im Zeitalter des Quantum Computings.

- Die Schaffung von Analyseplattformen, die Cross-Chain-Funktionalitäten integrieren, um Interoperabilität zwischen verschiedenen Blockchain-Netzwerken zu gewährleisten.

- **Regulatorisch und normativ:**
  - Die internationale Standardisierung von Forensik-Metriken zur Verbesserung der Beweissicherheit und der Akzeptanz von Blockchain-Beweisen vor Gericht.
  - Die Suche nach einer ausgewogenen Lösung zwischen dem Schutz der Privatsphäre und der Notwendigkeit der Nachvollziehbarkeit, insbesondere im Kontext von DeFi und Layer-2-Lösungen.
  - Regulierung von tokenisierten Vermögenswerte und CBDCs im forensischen Kontext.

- **Ethisch-philosophisch:**
  - Die Entwicklung ethischer Leitlinien für den Einsatz algorithmischer Entscheidungsfindung in Strafverfahren und bei der Strafverfolgung.
  - Die Implementierung von Schutzmechanismen gegen den Missbrauch von Blockchain-Technologien durch autoritäre Staaten und/oder wirtschaftlich mächtige Akteure

Ein erheblicher Forschungsbedarf besteht insbesondere bei Layer-2-Netzwerken (wie dem Lightning Network für Bitcoin [27] oder Optimistic Rollups für Ethereum [28]), bei Privacy-preserving Forensics und bei der forensischen Auswertbarkeit von realweltlich tokenisierten Vermögenswerten. Bei Layer-2-Lösungen wie dem Lightning Network oder den Ethereum Rollups besteht insbesondere die Herausforderung, dass viele Transaktionen außerhalb der Hauptblockchain durchgeführt werden und nur aggregierte Daten im Hauptnetzwerk verankert sind. Neue Forschungsansätze zielen darauf ab, diese Off-Chain-Aktivitäten durch kanal- und netzwerkspezifische Analysetechniken zu erfassen. Besonders vielversprechend erscheinen hierbei Ansätze, die Zero-Knowledge-Proofs nutzen, um eine Blockchain-Analyse zu ermöglichen, ohne dass sensible Transaktionsdaten offengelegt werden müssen. Solche „privacy-preserving forensics“ könnten beispielsweise dazu verwendet werden, nachzuweisen, dass eine Transaktion bestimmten regulatorischen Anforderungen entspricht (wie KYC/AML-Prüfungen), ohne dabei die zugrundeliegenden personenbezogenen Daten preiszugeben und/oder Rückschlüsse auf Transaktionsmuster zu ermöglichen.

## 7.4. Schlussbetrachtung

Die forensische Analyse von Blockchain-Transaktionen illustriert exemplarisch die zunehmende Verschränkung von Technologie, Regulierung und Ethik im digitalen Zeitalter. Die Effektivität Ersterer hängt maßgeblich davon ab, inwieweit es gelingt, innovative technische Ansätze mit rechtsstaatlichen Normen und gesellschaftlichen Erwartungen in Einklang zu bringen. Diese Arbeit zeigt, dass Blockchain-Forensik weder ein Allheilmittel noch eine Gefahrenquelle darstellt, sondern vielmehr ein Werkzeug ist, dessen Potenzial stark vom jeweiligen Kontext abhängt.

Eine fundierte Weiterentwicklung dieses interdisziplinären Forschungsfeldes erfordert koordinierte Maßnahmen aller beteiligten Akteure, wozu vorliegend die folgenden Vorschläge unterbreitet werden:

**Für Strafverfolgungsbehörden:** Investitionen in eine spezialisierte Ausbildung und die Einführung standardisierter forensischer Protokolle, um die Beweiskraft von Blockchain-Analysen vor Gericht zu stärken.

**Für Unternehmen:** Die Implementierung transparenter Risikobewertungssysteme mit Widerspruchsmechanismen, um fehlerhafte Klassifikationen der Transaktionsbeteiligten zu vermeiden und Compliance-Anforderungen zu erfüllen.

**Für Gesetzgeber:** Die Entwicklung international harmonisierter Standards für grenzüberschreitende Ermittlungen bei gleichzeitiger Wahrung von Datenschutz- und Grundrechten.

**Für die Forschung:** Eine Fokussierung auf Privacy-preserving Forensics und erklärbare KI-Systeme, um die Balance zwischen Sicherheit und individuellen Freiheitsrechten zu optimieren.

Nur durch diese koordinierte Herangehensweise kann in Bezug auf den Einsatz forensischer Blockchain-Analyse der legitime Anspruch auf Sicherheit mit dem Schutz individueller Freiheitsrechte in einer zunehmend digitalisierten Welt nachhaltig vereinbart werden.

Mit der fortschreitenden Tokenisierung der Wirtschaft und der Integration von Blockchain-Technologien in alltägliche Finanzprozesse wird die Bedeutung investigativer Transaktionsanalysen stetig weiter zunehmen - nicht nur als Instrument der Strafverfolgung, sondern auch als wesentlicher Baustein für Vertrauen und Integrität im digitalen Finanzsystem der Zukunft.

Die praktische Relevanz dieser Erkenntnisse zeigt sich bereits heute: Führende Krypto-Börsen wie Coinbase implementieren seit 2018 die in dieser Arbeit analysierten forensischen

Methoden in ihre Compliance-Systeme, während Strafverfolgungsbehörden weltweit spezialisierte Blockchain-Analyseeinheiten aufbauen.

Zukünftige Forschungsbemühungen sollten sich insbesondere auf die Entwicklung interoperabler Standards und ethisch vertretbarer forensischer Verfahren konzentrieren, um sowohl die Effektivität der Ermittlungen zu erhöhen als auch die legitimen Datenschutzbedürfnisse der betroffenen Nutzerinnen und Nutzer zu wahren. Die Balance zwischen Transparenz und Privatsphäre wird dabei eine zentrale Herausforderung für die zukünftige Forschung und Praxis bleiben.

Es ist zu betonen, dass die Analyse auf öffentlich zugänglichen Quellen und theoretischen Modellen basiert. Eine empirische Untersuchung – etwa durch Interviews mit Ermittlungsbehörden oder Blockchain-Analysten – hätte die Ergebnisse weiter vertiefen können. Auch die rechtliche Bewertung stützt sich auf den Stand der Gesetzgebung zum Zeitpunkt der Erstellung; zukünftige regulatorische Entwicklungen, insbesondere im Rahmen der MiCA-Verordnung, könnten zentrale Aspekte dieser Arbeit verändern. Die interdisziplinäre Herangehensweise hat sich als sinnvoll erwiesen, wenngleich sie auch methodische Spannungen zwischen juristischer Präzision und technischer Komplexität offenbarte. Insgesamt bietet die Arbeit eine fundierte Grundlage, die jedoch durch weitere Forschung ergänzt werden sollte.

# Literaturverzeichnis

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," Oct. 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] V. Buterin, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum White Paper, 2014. [Online]. Available: https://ethereum.org/en/whitepaper/

[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, Berlin Version, 2022. [Online]. Available: https://ethereum.github.io/yellowpaper/paper.pdf

[4] S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of bitcoins: characterizing payments among men with no names," in Proc. 2013 Internet Measurement Conference (IMC '13), Barcelona, Spain, Oct. 2013, pp. 127-140.

[5] D. Ron and A. Shamir, "Quantitative Analysis of the Full Bitcoin Transaction Graph," in Proc. Financial Cryptography and Data Security (FC 2013), Okinawa, Japan, Apr. 2013, pp. 6-24.

[6] M. Harrigan and C. Fretter, "The Unreasonable Effectiveness of Address Clustering," in Proc. IEEE International Conference on Advances in Social Networks Analysis and Mining (ASONAM), San Francisco, CA, USA, Aug. 2016, pp. 368-373.

[7] A. Biryukov, D. Khovratovich, and I. Pustogarov, "Deanonymisation of clients in Bitcoin P2P network," in Proc. 2014 ACM SIGSAC Conference on Computer and Communications Security (CCS '14), Scottsdale, AZ, USA, Nov. 2014, pp. 15-29.

[8] S. Goldfeder, H. Kalodner, D. Reisman, and A. Narayanan, "When the cookie meets the blockchain: Privacy risks of web payments via cryptocurrencies," Proceedings on Privacy Enhancing Technologies, vol. 2018, no. 4, pp. 179-199, 2018.

[9] H. Kalodner, M. Möser, K. Lee, S. Goldfeder, M. Plattner, A. Chator, and A. Narayanan, "BlockSci: Design and applications of a blockchain analysis platform," in Proc. 29th USENIX Security Symposium (USENIX Security 20), Aug. 2020, pp. 2721-2738.

[10] M. Spagnuolo, F. Maggi, and S. Zanero, "BitIodine: Extracting Intelligence from the Bitcoin Network," in Proc. Financial Cryptography and Data Security (FC 2014), Christ Church, Barbados, Mar. 2014, pp. 457-468.

[11] M. Möser and R. Böhme, "Anonymous Alone? Measuring Bitcoin's Second-Generation Anonymization Techniques," in Proc. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Paris, France, Apr. 2017, pp. 32-41.

[12] H. Yousaf, G. Kappos, and S. Meiklejohn, "Tracing transactions across cryptocurrency ledgers," in Proc. 28th USENIX Security Symposium, Santa Clara, CA, USA, Aug. 2019, pp. 837-850.

[13] S. Noether and A. Mackenzie, "Ring Confidential Transactions," Ledger, vol. 1, pp. 1-18, Dec. 2016.

[14] A. Kumar, C. Fischer, S. Tople, and P. Saxena, "A Traceability Analysis of Monero's Blockchain," in Proc. European Symposium on Research in Computer Security (ESORICS 2017), Oslo, Norway, Sep. 2017, pp. 153-173.

[15] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn, "An empirical analysis of anonymity in Zcash," in Proc. 27th USENIX Security Symposium, Baltimore, MD, USA, Aug. 2018, pp. 463-477.

[16] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin," in Proc. European Symposium on Research in Computer Security (ESORICS 2014), Wroclaw, Poland, Sep. 2014, pp. 345-364.

[17] E. Heilman, L. Alshenibr, F. Baldimtsi, A. Scafuro, and S. Goldberg, "TumbleBit: An untrusted Bitcoin-compatible anonymous payment hub," in Proc. Network and Distributed System Security Symposium (NDSS 2017), San Diego, CA, USA, Feb. 2017.

[18] T. Ruffing, P. Moreno-Sanchez, and A. Kate, "P2P mixing and unlinkable Bitcoin transactions," in Proc. Network and Distributed System Security Symposium (NDSS 2017), San Diego, CA, USA, Feb. 2017.

[19] M. Herlihy, "Atomic cross-chain swaps," in Proc. ACM Symposium on Principles of Distributed Computing (PODC 2018), Egham, United Kingdom, Jul. 2018, pp. 245-254.

[20] M. Weber, G. Domeniconi, J. Chen, D. K. I. Weidele, C. Bellei, T. Robinson, and C. E. Leiserson, "Anti-money laundering in bitcoin: Experimenting with graph convolutional networks for financial forensics," in Proc. KDD 2019 Workshop on Anomaly Detection in Finance, Anchorage, AK, USA, Aug. 2019.

[21] D. Y. Huang, M. M. Aliapoulios, V. G. Li, L. Invernizzi, E. Bursztein, K. McRoberts, et al., "Tracking ransomware end-to-end," in Proc. IEEE Symposium on Security and Privacy (S&P 2018), San Francisco, CA, USA, May 2018, pp. 618-631.

[22] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the bitcoin ecosystem," Journal of Cybersecurity, vol. 5, no. 1, 2019.

[23] M. Möser, R. Böhme, and D. Breuker, "An inquiry into money laundering tools in the Bitcoin ecosystem," in Proc. APWG eCrime Researchers Summit, San Francisco, CA, USA, Sep. 2013, pp. 1-14.

[24] M. Conti, A. Gangwal, and S. Ruj, "On the economic significance of ransomware campaigns: A Bitcoin transactions perspective," Computers & Security, vol. 79, pp. 162-189, 2018.

[25] M. Finck, "Blockchain and the General Data Protection Regulation: Can distributed ledgers be squared with European data protection law?" European Parliamentary Research Service, Brussels, Belgium, Study PE 634.445, Jul. 2019.

[26] S. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," in Proc. ACM Conference on Advances in Financial Technologies (AFT 2022), San Francisco, CA, USA, May 2022, pp. 1364-1385.

[27] S. Tikhomirov, P. Moreno-Sanchez, and M. Maffei, "A Quantitative Analysis of Security, Anonymity and Scalability for the Lightning Network," in Proc. IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Sep. 2020, pp. 387-396.

[28] L. Gudgeon, P. Moreno-Sanchez, S. Roos, P. McCorry, and A. Gervais, "SoK: Layer-Two Blockchain Protocols," in Proc. Financial Cryptography and Data Security (FC 2020), Kota Kinabalu, Malaysia, Feb. 2020, pp. 201-226.

[29] CoinGecko, "2024 Annual Crypto Industry Report," Jan. 2025. [Online]. Available: https://www.coingecko.com/research/publications/2024-annual-crypto-report

[30] U.S. Securities and Exchange Commission, "SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FTX," Press Release 2022-219, Dec. 13, 2022. [Online]. Available: https://www.sec.gov/news/press-release/2022-219

[31] Europol, "ChipMixer: Cryptomixer platform shut down for facilitating money laundering on a large scale," Press Release, Mar. 15, 2023. [Online]. Available:

https://www.europol.europa.eu/media-press/newsroom/news/chipmixer-cryptomixer-platform-shut-down-for-facilitating-money-laundering-large-scale

[32] U.S. Department of Justice, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside," Press Release, Jun. 7, 2021. [Online]. Available: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

[33] M. Bartoletti, B. Pes, and S. Serusi, "Cryptocurrency scams: Analysis and perspectives," IEEE Access, vol. 9, pp. 148353-148373, 2021.

[34] Analytics Yogi, "List of Blockchain Platforms & Examples", Nov. 2022. [Online]. Available: https://vitalflux.com/list-different-blockchain-platforms-examples/

[35] BlessedTechnologist, "Understanding Solana and Proof of History in Blockchain," Feb. 2022. [Online]. Available: https://dev.to/blessedtechnologist/understanding-solana-and-proof-of-history-in-blockchain-43i3

[36] Avalanche Builder Hub, "Avalanche Consensus," [Online]. Available: https://build.avax.network/docs/quick-start/avalanche-consensus

[37] A. Alexandre, "Silk Road-Gründer: BTC erreicht 2020 bis zu 100.000 US-Dollar," Cointelegraph, 13. Dez. 2019. [Online]. Available: https://de.cointelegraph.com/news/silk-road-darknet-marketplace-founder-btc-will-reach-100-000-in-2020

[38] IDnow, "Wie Kriminelle nicht-konforme Kryptobörsen für Geldwäsche nutzen," IDnow Blog, 2023. [Online]. Available: https://www.idnow.io/de/blog-de/wie-kriminelle-nicht-konforme-kryptoboersen-fuer-geldwaesche-nutzen

[39] M. Ackermann, "Internationale Kooperation: Rechtshilfe als Schlüssel im Wallet-Tracing," anwalt.de, Aug. 2024. [Online]. Available: https://www.anwalt.de/rechtstipps/internationale-kooperation-rechtshilfe-als-schluessel-im-wallet-tracing-252745.html

[40] M. Pussar, "MiCAR – Was die neue EU-Verordnung für Krypto-Dienstleister und Emittenten bedeutet," KPMG Law, Dec. 2024. [Online]. Available: https://kpmg-law.de/micar-neue-eu-verordnung-fuer-krypto-dienstleister-und-emittenten

[41] K. Weber, "Ausgetretene Pfade verlassen: Forschungsprojekt erprobt Blockchain-Technologie für Audit Trails," DHChannel, DHC Business Solutions, Sept. 2019. [Online]. Available: https://dhchannel.dhc-vision.com/dhc-insights/ausgetretene-pfade-verlassen-forschungsprojekt-erprobt-blockchaintechnologie-fuer-audit-trails

[42] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), "Europäische MiCA-Verordnung: Regel-Fundament für Kryptowerte," BaFinJournal, 17. Mai 2023. [Online]. Available: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2023/fa_bj_2305_Mica.html

[43] M. Härtel, "Blockchain in der digitalen Forensik: Einsatzfelder, Beweiswert und Datenschutzgrenzen," itmedialaw.com, Apr. 2024. [Online]. Available: https://itmedialaw.com/blockchain-in-der-digitalen-forensik-einsatzfelder-beweiswert-und-datenschutzgrenzen/

[44] U.S. Department of the Treasury, "U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash," Press Release, Aug. 8, 2022. [Online]. Available: https://home.treasury.gov/news/press-releases/jy0916

[45] United States Court of Appeals for the Fifth Circuit, Van Loon v. Department of Treasury, ca5.uscourts.gov, Nov. 2024. [Online]. Available: https://www.ca5.uscourts.gov/opinions/pub/23/23-50669-CV0.pdf

[46] Reuters, “Court overturns US sanctions against cryptocurrency mixer Tornado Cash,” reuters.com, Nov. 2024. [Online]. Available: https://www.reuters.com/legal/court-overturns-us-sanctions-against-cryptocurrency-mixer-tornado-cash-2024-11-27/

[47] J. J. McShane, “In-Depth Look at Chainalysis, Elliptic, and CipherTrace: Forensic Science in Blockchain Analysis,” The Truth About Forensic Science, May 4, 2023. [Online]. Available: https://thetruthaboutforensicscience.com/in-depth-look-at-chainalysis-elliptic-and-ciphertrace-forensic-science-in-blockchain-analysis

[48] Chainalysis Team, “Introducing Cross-Chain Investigations in Reactor: Enhancing Crypto Tracing,” Chainalysis Blog, Mar. 9, 2022. [Online]. Available: https://www.chainalysis.com/blog/cross-chain-investigations

[49] Elliptic, Preventing Financial Crime in Cryptoassets: Typologies Report 2024, Elliptic, London, UK, May 2024. [Online]. Available: https://www.elliptic.co/hubfs/Elliptic%20Typologies%20Report%202024.pdf

[50] B. Haslhofer, R. Stütz, M. Romiti, and R. King, “GraphSense: A General-Purpose Cryptoasset Analytics Platform,” arXiv preprint arXiv:2102.13613, Feb. 2021. [Online]. Available: https://arxiv.org/pdf/2102.13613

## Eidesstattliche Erklärung

„Ich versichere, dass ich vorliegende Arbeit ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quelle kenntlich gemacht."

Datum: .....  Unterschrift: