HMD Praxis der Wirtschaftsinformatik
https://doi.org/10.1365/s40702-026-01249-0

SCHWERPUNKT

Digitale Beweissicherung im Verbraucherschutz: Eine DLT-basierte Lösung mit Crowd-Verifikation

Meike Ullrich · Nadja Kruse · Gunther Schiefer · Zina Al-Washash · Steffen Kroschwald · Thomas Schuster

Eingegangen: 30. September 2025 / Angenommen: 29. Januar 2026

Zusammenfassung Verbraucherschutzorganisationen stehen im digitalen Raum zunehmend vor der Herausforderung, Rechtsverstöße gerichtsfest zu dokumentieren. Manipulative Online-Inhalte, unvollständige oder falsche Angaben sowie irreführende Werbung sind flüchtig, leicht veränderbar und daher nur schwer beweiskräftig zu sichern. Herkömmliche Verfahren wie Screenshots sind unzureichend, da sie durch Bildbearbeitung oder minimale Änderungen im Quelltext leicht manipuliert werden können. In diesem Beitrag wird ein hybrides technisches System vorgestellt, das eine zuverlässige und manipulationssichere Beweissicherung solcher Verstöße ermöglicht. Der Ansatz kombiniert Distributed-Ledger-Technologie (DLT) zur

✉ Meike Ullrich · Nadja Kruse · Gunther Schiefer
Institut für Angewandte Informatik und Formale Beschreibungsverfahren (AIFB), Karlsruher Institut für Technologie (KIT), Karlsruhe, Deutschland
E-Mail: meike.ullrich@kit.edu

Nadja Kruse
E-Mail: nadja.kruse@kit.edu

Gunther Schiefer
E-Mail: gunther.schiefer@kit.edu

Zina Al-Washash · Steffen Kroschwald
Institut für Verbraucherforschung und nachhaltigen Konsum (vunk), Hochschule Pforzheim, Pforzheim, Deutschland

Zina Al-Washash
E-Mail: zina.al-washash@hs-pforzheim.de

Steffen Kroschwald
E-Mail: steffen.kroschwald@hs-pforzheim.de

Thomas Schuster
Fakultät für Wirtschaft und Recht, Wirtschaftsinformatik, Hochschule Pforzheim, Pforzheim, Deutschland
E-Mail: thomas.schuster@hs-pforzheim.de

Published online: 23 February 2026

Integritätssicherung der erfassten Daten mit einer verifizierenden Crowd-Absicherung durch Fachpersonal der Verbraucherzentralen. Die Lösung erlaubt es, erkannte Rechtsverstöße automatisiert zu erfassen, indem ein Hashwert des Webseiteninhalts erzeugt und zusammen mit Metadaten und Zeitstempel in einem DLT-System unveränderbar gespeichert wird. Ergänzend bestätigen Arbeitsplatzrechner von Verbraucherschutzmitarbeitenden durch ein automatisiertes paralleles Vorgehen die Existenz der Verstöße, ohne dass aktives Eingreifen erforderlich ist. Dieses Verfahren stärkt den Beweiswert, erhöht die Widerstandsfähigkeit gegen Manipulation und ermöglicht es, nachgelagerte Veränderungen oder Löschungen gerichtsfest nachzuweisen.

Schlüsselwörter Digitale Beweissicherung · Distributed Ledger Technology (DLT) · Verbraucherschutz · Manipulationssicherheit · Crowd-Absicherung

Digital Evidence Preservation in Consumer Protection: A DLT-Based Solution with Crowd Verification

Abstract Consumer protection organizations increasingly face the challenge of providing legally valid evidence of violations in the digital sphere. Manipulative online content, incomplete or false information, and misleading advertising are often ephemeral, easily altered, and therefore difficult to preserve in a legally robust way. Conventional approaches such as screenshots are insufficient, as they can be manipulated through image editing or minimal changes to the source code. This paper presents a hybrid technical system that enables reliable and tamper-proof evidence preservation of such violations. The approach combines distributed ledger technology (DLT) to ensure data integrity with a verifying crowd-based safeguard operated by consumer protection staff. The solution allows recognized violations to be documented automatically by generating a hash of the web content, which is then stored together with metadata and a timestamp in a DLT system in an immutable manner. In addition, workstations of consumer protection employees confirm automatically the existence of the violation through parallel background captures, without requiring active user interaction. This procedure strengthens the evidential value, increases resilience against manipulation, and enables providers' subsequent modifications or deletions to be legally demonstrated.

Keywords Digital Evidence Preservation · Distributed Ledger Technology (DLT) · Consumer Protection · Tamper Resistance · Crowd-based Verification

1 Einleitung

Die fortschreitende Digitalisierung schafft nicht nur neue Chancen für Wirtschaft und Gesellschaft, sondern auch neuartige Risiken. Digitale Inhalte sind jederzeit verfügbar, aber zugleich hochgradig flüchtig, manipulierbar und schwer dauerhaft beweissicher zu dokumentieren. Gerade Verbraucherschutzorganisationen sehen sich mit dieser Problematik täglich konfrontiert. Sie müssen Rechtsverstöße wie irreführ-

rende Werbung, unklare Vertragsbedingungen oder unseriöse Online-Angebote nachweisen, um im Interesse der Verbraucher:innen wirksam einschreiten zu können. In der Praxis stoßen sie dabei jedoch schnell an Grenzen: Screenshots oder Ausdrucke gelten aktuell zwar als naheliegende Dokumentationsformen, erweisen sich aber bei genauerer Betrachtung als unzureichend. Manipulationen können vor der Aufnahme im Quelltext, unmittelbar bei der Erstellung oder nachträglich durch Bildbearbeitung oder den Einsatz von KI-basierten Verfahren wie Deep Fakes erfolgen. Zudem fehlt häufig eine zuverlässige Nachvollziehbarkeit von Zeitpunkt, Kontext und Quelle der Aufnahme. Damit sind die Integrität und Authentizität von Screenshots und Ausdrucken kaum zweifelsfrei belegbar. Sowohl die Rechtsprechung als auch die wissenschaftliche Diskussion betonen daher den geringen Beweiswert dieser Nachweismethoden (Mankowski 2016; Zimmermann 2016; OLG Jena 2018; BGH 2023).

Typische Fälle aus dem Verbraucherschutz betreffen beispielsweise eine produktbezogene Irreführung, etwa wenn Online-Anbieter:innen falsche oder übertriebene Angaben zur Wirkung, zum Zweck oder zur Verwendung von Produkten machen. Solche Täuschungen können nicht nur das Vertrauen von Verbraucher:innen untergraben, sondern auch gesundheitliche, finanzielle oder sicherheitsrelevante Risiken bergen. Klassische Beispiele sind vermeintlich „heilende“ Nahrungsergänzungsmittel oder falsch deklarierte Verbrauchsgüter[1]. Aus technischer und wissenschaftlicher Perspektive ergeben sich vor diesem Hintergrund zentrale Anforderungen an moderne Verfahren der Beweissicherung: Sie müssen Integrität und Authentizität von digitalen Beweismitteln gewährleisten sowie deren Prüfbarkeit und Nachverfolgbarkeit sicherstellen (Casey 2011). Für die Praxis bedeutet dies, dass Verbraucherschutzorganisationen, Behörden und Gerichte dringend auf vertrauenswürdige, skalierbare und zugleich leicht handhabbare Lösungen angewiesen sind. Nur so lassen sich Verbraucherrechte wirksam durchsetzen, Rechtsstaatlichkeit im digitalen Raum sichern und das Vertrauen in digitale Märkte langfristig erhalten.

Um diesem entgegenzuwirken, wird im vorliegenden Beitrag ein Lösungsansatz aus dem Projekt EVIDENTT[2] vorgestellt, das im Rahmen einer Machbarkeitsstudie ein technisches System zur gerichtsfesten Beweissicherung von Rechtsverstößen im digitalen Raum entwickelt hat. Der Lösungsansatz basiert auf einem hybriden Verfahren, das eine Kombination aus DLT zum Nachweis unveränderter Beweise und einer ergänzenden Crowd-Absicherung durch Arbeitsplatzrechner von Fachpersonal der Verbraucherzentralen vorsieht. Die Lösung ermöglicht es, Rechtsverstöße durch eine automatisierte Erfassung zu dokumentieren. Dabei wird von einem Webseitenabzug ein Hashwert erstellt, der zusammen mit Metadaten und Zeitstempel in einem DLT-System manipulationssicher gespeichert wird. Eine verteilte Crowd aus Arbeitsplatzrechnern von Verbraucherschutzmitarbeitenden trägt zur Absicherung des Beweiswerts bei, indem parallel automatisiert gleichartige Sicherungen erstellt werden, ohne aktives Zutun der Beteiligten. Dadurch wird der Beweiswert gestärkt

[1] https://www.verbraucherzentrale.de/vertraege-reklamation/falsche-versprechen-irrefuehrende-angabe-es-kann-schadensersatz-geben-83819, zuletzt zugegriffen am 08.01.2026.

[2] Einsatz verteilter Technologien zur beweissicheren Dokumentation von Verbraucherschutzverstößen auf Online-Plattformen, gefördert von der Baden-Württemberg Stiftung im Rahmen des *Ideenwettbewerb Blockchain.*

und Manipulationen werden erschwert. Nachgelagerte „Vertuschungen“ durch Veränderungen oder Löschungen seitens der Online-Anbieter können so zuverlässig nachgewiesen werden. Auf diese Weise entsteht eine praxisnahe, automatisierte und rechtskonforme Lösung, die langfristige Beweisführung etwa im Rahmen von Abmahnungen oder gerichtlichen Auseinandersetzungen ermöglicht.

Dieser Beitrag verfolgt das Ziel, einen rechtskonformen und technisch abgesicherten Lösungsansatz zur Beweissicherung im digitalen Verbraucherschutz vorzustellen. Dazu werden zunächst die rechtlichen Rahmenbedingungen und bestehenden Herausforderungen detailliert analysiert. Anschließend erfolgt eine Vorstellung und Einordnung verwandter Ansätze. Darauf aufbauend wird die Konzeption des Lösungsansatzes sowie die Systemarchitektur von EVIDENTT umfassend beschrieben. Die Machbarkeit der technischen Umsetzung wird mittels eines entwickelten Demonstrators praxisnah dargestellt und erprobt. Abschließend werden offene Herausforderungen diskutiert, ein Fazit gezogen und mögliche Ausblickszenarien skizziert, wie etwa eine Übertragung der Lösung auf weitere Anwendungsfelder wie Urheberrecht, Hate Speech, digitale Bedrohungen oder Mobbing.

Der Beitrag bietet somit gleich doppelten Mehrwert: Er zeigt nicht nur auf, wie eine rechtskonforme, technisch abgesicherte Beweissicherung im digitalen Verbraucherschutz realisiert werden kann, sondern legt auch methodische und konzeptionelle Grundlagen dar, um ähnliche Verfahren in anderen Domänen zu erproben.

2 Rechtliche Rahmenbedingungen

Die Beweissicherung im digitalen Raum wirft erhebliche rechtliche Herausforderungen auf. Zentrale Anforderungen bestehen darin, Integrität, Authentizität und Nachvollziehbarkeit digitaler Beweise sicherzustellen und deren gerichtliche Verwertbarkeit zu gewährleisten. Im Projekt EVIDENTT wurden die rechtlichen Rahmenbedingungen durch eine interdisziplinäre Analyse erarbeitet. Analysiert wurden dazu europäische und nationale Vorschriften zur zivilprozessualen Beweisführung, zu elektronischen Vertrauensdiensten (eIDAS), zum Datenschutz- und zum Urheberrecht. Ergänzt wurde dies durch Interviews mit juristischen Expert:innen, darunter Richter:innen und Vertreter:innen von Verbraucherzentralen, um praxisnahe Einschätzungen zu gewinnen und die Anforderungen aus Sicht relevanter Stakeholder zu erfassen.

2.1 Rechtliche Grundlagen

Die Beweiskette als Schlüsselfaktor Ein zentrales Konzept aus der digitalen Forensik für die gerichtliche Anerkennung ist die Beweiskette (engl. chain of custody) (Giannelli 1996). Sie bezeichnet die lückenlose Dokumentation aller Schritte, die ein Beweisstück von seiner Erhebung bis zu seiner Verwendung im Gerichtsverfahren durchläuft. Für digitale Beweise bedeutet dies, dass jede Interaktion – von der Erfassung über Speicherung bis hin zur Vorlage – nachvollziehbar protokolliert werden muss, um Manipulationen ausschließen zu können.

Einordnung digitaler Beweise Digitale Inhalte wie Webseitenabzüge oder Screenshots werden im Zivilprozess als sog. „Augenscheinsurrogate“ behandelt, deren Beweiswert im Rahmen der freien richterlichen Beweiswürdigung (§ 286 ZPO) individuell beurteilt wird. Dabei spielt die Frage, ob das Gericht von der Integrität und Authentizität des Inhalts zweifelsfrei überzeugt werden kann, eine zentrale Rolle.

Anforderungen aus der eIDAS-Verordnung Die europäische eIDAS-Verordnung (EU 910/2014, EU 2024/1183) verleiht bestimmten qualifizierten Vertrauensdiensten einen erhöhten Beweiswert; Nutzende profitieren von gesetzlichen Vermutungswirkungen. Für DLT-basierte Nachweise gilt dies derzeit nicht unmittelbar, sie sind rechtlich als Augenscheinsurrogate (§ 371 ZPO) einzuordnen. Eine interdisziplinäre Analyse sowie Interviews mit Expert:innen aus Justiz und juristischer Praxis (u. a. Richter:innen und Verbraucherschutzverbände) ergaben jedoch, dass der Beweiswert im Rahmen der freien richterlichen Beweiswürdigung durch den Einsatz von DLT und Crowd-Verfahren gesteigert werden kann. Während herkömmliche Screenshots aufgrund ihrer einfachen Manipulierbarkeit (z. B. durch lokale Quelltextänderungen) angezweifelt werden können, reduziert der EVIDENTT-Ansatz dieses Manipulationsrisiko mittels automatisierter, redundanter Erfassung durch unabhängige Instanzen (Crowd) und sichert die Integrität der Beweiskette mittels kryptografischer Zeitstempel in einer DLT manipulationssicher ab.

Datenschutz- und urheberrechtliche Anforderungen Ein Spannungsfeld ergibt sich auch aus datenschutz- und urheberrechtlichen Vorgaben. Die Speicherung von Webseiten und Screenshots kann zur Verarbeitung personenbezogener Daten führen. Nach der EU-Datenschutzgrundverordnung (DSGVO) braucht es dazu eine Rechtsgrundlage. Hinzu kommt, dass bei der Beweissicherung unter Umständen urheberrechtlich geschützte Werke (mit-)vervielfältigt werden könnten. Im Ergebnis muss technisch und organisatorisch sichergestellt sein, dass alle betreffenden Vorgänge streng auf den Zweck der gerichtlichen Rechtsdurchsetzung beschränkt sind. Außerdem müssen Daten nach DSGVO gelöscht werden, wenn sie nicht mehr erforderlich sind. Eine Löschung steht aber im Widerspruch zur Immutabilität von DLT-Systemen, die eine nachträgliche Veränderung oder Löschung gespeicherter Inhalte technisch ausschließen. In der Literatur wird daher diskutiert, wie sich dieser Zielkonflikt auflösen lässt. Genannte Ansätze sind etwa die ausschließliche Speicherung von Hashwerten anstelle personenbezogener Daten oder die Nutzung von Off-Chain-Speichern, in denen Daten bei Wegfall des Verarbeitungszwecks entfernt werden können (Belen-Saglam et al. 2022; Godyn et al. 2022; Zafar et al. 2024). Für die Beweissicherung im digitalen Raum bedeutet dies, dass bei der konkreten Umsetzung die Vorteile der Unveränderlichkeit mit den datenschutz- und urheberrechtlichen Grenzen sorgfältig austariert werden müssen.

2.2 Erkenntnisse aus Experteninterviews

Im Rahmen von EVIDENTT wurden mehrere Experteninterviews mit Jurist:innen, Richter:innen sowie Vertreter:innen von Verbraucherzentralen durchgeführt, um die rechtlichen Anforderungen praxisnah zu validieren.

Juristische Expert:innen betonten insbesondere die Schwierigkeiten bei der Beweissicherung dynamischer Inhalte. Viele problematische Erscheinungsformen wie Dark Patterns[3], sich verändernde Preisangaben oder situativ eingeblendete Werbung seien nur schwer vollständig zu dokumentieren. Vor diesem Hintergrund wurde der Crowd-Ansatz von EVIDENTT positiv hervorgehoben, da die parallele Absicherung durch mehrere unabhängigen Instanzen eine erhöhte Vertrauenswürdigkeit schafft und den Vorwurf der Manipulation entkräftet. Zudem wurde hervorgehoben, dass eine technische Lösung nur dann Akzeptanz finden kann, wenn sie in ein bestehendes prozessuales Beweisrecht eingeordnet werden kann und sich an etablierten Standards (z. B. Zeitstempel, kryptographische Verfahren) orientiert.

Richterliche Perspektiven machten deutlich, dass DLT-basierte Verfahren gegenwärtig noch keine gesetzliche Sonderstellung genießen, wie sie etwa für qualifizierte elektronische Signaturen oder Zeitstempel nach eIDAS besteht. Gleichwohl wurde betont, dass Gerichte im Rahmen der freien Beweiswürdigung (§ 286 ZPO) auch neuartige Verfahren berücksichtigen können. Entscheidend sei, dass Nachvollziehbarkeit und Manipulationsresistenz plausibel dargelegt werden. In diesem Zusammenhang wurde das Konzept der Beweiskette als entscheidendes Kriterium hervorgehoben: Nur wenn die Entstehungsgeschichte eines Beweismittels lückenlos dokumentiert ist, wird es in der gerichtlichen Praxis auch als glaubwürdig bewertet.

Vertreter:innen von Verbraucherzentralen hoben hervor, dass ein praxistaugliches System vor allem den Arbeitsalltag ihrer Mitarbeitenden entlasten müsse. Die Beweissicherung erfolgt bisher oft manuell, ist zeitaufwendig und rechtlich angreifbar. Eine automatisierte Lösung mit dezentraler Absicherung könne hier erhebliche Vorteile bieten. Gleichzeitig wurde deutlich, dass für eine tatsächliche Einführung auch Aspekte wie Bedienfreundlichkeit, Kosten, Integration in bestehende IT-Strukturen sowie die datenschutzkonforme Gestaltung nach DSGVO maßgeblich sind. Ein besonderes Augenmerk legten die Befragten zudem auf die Möglichkeit, Ergebnisse gerichtsverwertbar aufzubereiten und in standardisierte Verfahrensabläufe zu überführen.

Die Gespräche bestätigten damit, dass ein DLT-basierter Ansatz grundsätzlich auf hohe Akzeptanz stößt, jedoch nur dann Wirkung entfalten kann, wenn er eng an die tatsächlichen Bedarfe von Gerichten und Verbraucherzentralen sowie an geltende rechtliche Anforderungen anschließt.

[3] Manipulative Designentscheidungen im User Interface, die Nutzer:innen zu Handlungen verleiten, die ihren eigentlichen Interessen zuwiderlaufen (Gray et al. 2018; Mathur et al. 2019).

3 Verwandte Ansätze

Kapitel 3 gibt einen Überblick über bestehende Ansätze aus der wissenschaftlichen Literatur sowie marktverfügbare Werkzeuge zur digitalen Beweissicherung und zeigt auf, inwieweit diese bereits zentrale Anforderungen wie Integrität, Authentizität und Nachvollziehbarkeit adressieren.

3.1 Publizierte Ansätze

In der Forschung existieren verschiedene DLT-basierte Ansätze zur Sicherung und Verwaltung digitaler Beweise. Ein früher Ansatz wird von Brotsis et al. (2019) im Rahmen des EU-Projekts Cyber-Trust verfolgt. Hier wurde die Sammlung und Sicherung von Beweisen im Kontext von IoT-Umgebungen adressiert, etwa bei kompromittierten Smart-Home-Geräten. Der Ansatz kombiniert Intrusion-Detection-Systeme, also Mechanismen zur automatisierten Erkennung von Anomalien und Angriffsmustern, mit einer sogenannten permissioned Blockchain (Hyperledger Fabric). Da bei dieser Form der DLT Schreib- und Validierungsrechte nur an einen autorisierten Teilnehmerkreis vergeben werden, eignet sie sich besonders, um Metadaten der Beweise sicher zu speichern. Ziel ist es, Integrität, Authentizität und Nachverfolgbarkeit sicherzustellen und eine digitale Beweiskette zu gewährleisten, die insbesondere von Strafverfolgungsbehörden genutzt werden kann.

Chen et al. (2020) untersuchten die Anwendung von Blockchain bei der Generierung elektronischer Beweismittel im justiziellen Umfeld. Im Zentrum steht die Nutzung einer Konsortial-Blockchain, in die Beweisdaten mitsamt Hashwerten und Zeitstempeln eingetragen werden, um Authentizität und Integrität sicherzustellen. In China wurde diese Vorgehensweise bereits gerichtlich anerkannt, etwa in Urheberrechtsstreitigkeiten vor dem Hangzhou Internet Court. Der Ansatz zielt auf die Standardisierung und Institutionalisierung der Beweiserhebung und bietet richterliche Stellen als validierende Knoten der Blockchain. Es bleibt zu untersuchen, ob diese Methode auch vor europäischen bzw. deutschen Gerichten standhält.

Ein prominentes Beispiel ist LEChain von Li et al. (2021). Hierbei handelt es sich um ein Blockchain-gestütztes System für die Beweissicherung in der digitalen Forensik, das den gesamten Lebenszyklus von Beweismitteln abdeckt, von der Sammlung über die Analyse bis hin zu Gerichtsverfahren. Besonderer Wert wird dabei auf die Wahrung der Privatsphäre von Zeug:innen und Geschworenen gelegt, u. a. durch anonyme Signaturen und attributbasiertes Zugriffsmanagement. Das System ermöglicht zudem eine nachvollziehbare Beweiskette und wurde in einem Ethereum-basierten Prototyp erprobt.

Ergänzend zu diesen forensischen Gesamtsystemen existieren etablierte Dienste, die sich primär auf die Integritätssicherung bestehender Dokumente fokussieren, wie etwa OpenTimestamps oder proofofexistence.com. Diese Dienste nutzen die Blockchain zur Attestierung von Dokumenten und Identitäten, bieten jedoch meist keine integrierte Logik zur Erfassung von Web-Inhalten (Härer und Fill 2020). Die hohe Relevanz solcher Verfahren wird auch durch aktuelle Übersichtsstudien unterstrichen: So analysieren Sakshi und Sharma (2024) umfassend, wie Blockchain-Technologien zur Integritätssicherung digitaler Multimedia-Inhalte eingesetzt wer-

den können und zeigen die wachsende Bedeutung fälschungssicherer Nachweise auf.

Diese Arbeiten belegen das Potenzial von DLT für die Beweissicherung. Unterschiede zum EVIDENTT-Lösungsansatz bestehen im Anwendungskontext (digitale Forensik allgemein, gerichtliche Verfahren, IoT-Szenarien) und in den jeweils adressierten Kernanforderungen (Privatsphäre, Institutionalisierung, Angriffserkennung).

3.2 Marktlösungen

In der Praxis erfolgt die Beweissicherung bislang häufig durch einfache Screenshots. Diese gelten zwar als schnell verfügbare, niedrigschwellige Methode, weisen jedoch erhebliche Schwächen auf. Insbesondere fehlen Nachweise zur Authentizität und Integrität, und es bestehen vielfältige Manipulationsmöglichkeiten.

Zur Verbesserung dieses Status quo existieren verschiedene Werkzeuge auf dem Markt, die eine technisch gestützte Beweissicherung anbieten. Hierzu zählen auch etablierte Web-Archivierungsdienste wie beispielsweise perma.cc[4] oder generische „Link-Archive“ (z. B. archive.is[5]). Diese Dienste ermöglichen es, Webseiten zu archivieren und dauerhafte Links zu generieren, um die Flüchtigkeit digitaler Inhalte zu adressieren. Sie erfassen typischerweise Screenshots und den HTML-Code einer Seite.

Ein Beispiel für existierende Beweissicherungsverfahren ist das Netzbeweis[6] Webformular, das sich an Betroffene von Online-Straftaten wie Hassrede, Stalking oder Betrug richtet. Hierbei können Nutzer:innen einen Link einreichen; automatisiert wird anschließend ein Screenshot erstellt, in eine PDF-Datei überführt und mit digitaler Signatur und Zeitstempel versehen. In der kostenpflichtigen Version lassen sich auch nicht-öffentliche Inhalte wie private Webseiten oder Chats sichern, zudem wird eine optionale Browser-Integration angeboten.

Ein weiteres Beispiel ist Rewis WebCapture[7], ein webbasiertes Instrument zur Dokumentation von Inhalten öffentlich zugänglicher Webseiten. Neben Screenshots werden auch der HTML-Code, HTTP-Header und Cookies erfasst sowie ein Hashwert zur Integritätsprüfung generiert. Das Verfahren berücksichtigt dynamisch nachgeladene Inhalte und versucht, die Webseite möglichst realitätsnah zu rendern. Allerdings bestehen technische Einschränkungen: Bei komplexen oder dynamischen Webseiten kann es zu Darstellungsproblemen kommen, sodass die gesicherte Ansicht von der Originaldarstellung abweichen kann.

Beide Ansätze stellen zwar eine Weiterentwicklung gegenüber einfachen Screenshots dar, erreichen jedoch keine vollumfängliche Gewährleistung von Integrität und Authentizität, da die erzeugten Nachweise manipulationsanfällig bleiben und nicht durch unabhängige, technisch abgesicherte Verfahren validiert werden.

[4] https://perma.cc/, zuletzt zugegriffen am 07.01.2026.

[5] https://archive.is/, zuletzt zugegriffen am 07.01.2026.

[6] https://www.netzbeweis.com/web/, zuletzt zugegriffen am 14.07.2025.

[7] https://rewis.io/service/webcapture/ (derzeit deaktiviert), zuletzt zugegriffen am 14.07.2025.

4 Lösungsansatz und Systemarchitektur

Die in EVIDENTT entwickelte Systemarchitektur für den Lösungsansatz besteht aus mehreren miteinander verzahnten Komponenten. Sie verfolgt das Ziel, einen technisch belastbaren, rechtssicheren und zugleich datenschutzkonformen Prozess zur Dokumentation und Beweissicherung von Rechtsverstößen im Internet bereitzustellen. Digitale Inhalte sind naturgemäß flüchtig und leicht veränderbar; gerade deshalb müssen Verfahren zur Beweissicherung gewährleisten, dass Integrität und Authentizität jederzeit überprüfbar bleiben und eine lückenlose Nachverfolgbarkeit der Beweise sichergestellt ist.

4.1 Systemkomponenten zur Beweissicherung

Die Architektur des Gesamtsystems ist in Abb. 1 dargestellt. Sie zeigt, wie die einzelnen Komponenten zur Erfassung, Verwaltung und Speicherung von Webseitenabzügen zusammenspielen. Auf der unteren Ebene befinden sich die Client-Anwendung und das Browser-Plugin, die gemeinsam für die nutzerfreundliche Erfassung sorgen. Zentral eingebunden ist eine DLT, die als verbindendes Element fungiert. Darüber befinden sich das Crowd-Management, ein dedizierter Datenspeicher für die Webseitenabzüge sowie ein Rechte- und Rollenmanagement. Die beiden letztgenannten Komponenten übernehmen die weitere Verarbeitung, Aufbewahrung und Zugriffssteuerung. Es ist wichtig hervorzuheben, dass diese drei Komponenten (Crowd-Management, Datenspeicher und Rechte-/Rollenmanagement) in der aktuellen Implementierung des Demonstrators zentralisiert umgesetzt sind. Diese bewusste teilweise zentrale Anordnung stellt eine Möglichkeit der Umsetzung dar, die für den beschränkten Anwendungsfall im Demonstrator gewählt wurde. Sie erlaubt die effiziente Erprobung des Lösungsansatzes. Langfristig ist es jedoch denkbar, dass Teile dieser zentralisierten Umsetzung ebenfalls in eine dezentrale Struktur überführt werden könnten, um die Robustheit und Unabhängigkeit weiter zu steigern. Im Folgenden werden die einzelnen Bausteine im Detail erläutert.

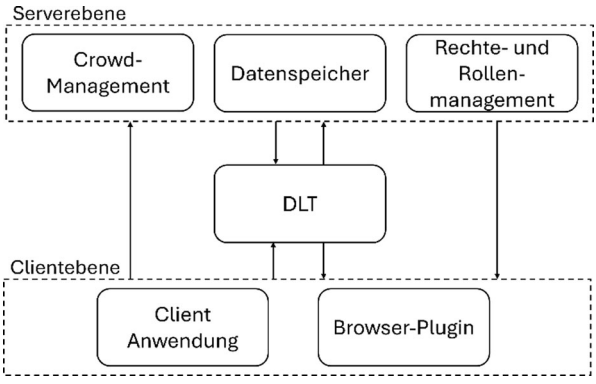

Abb. 1 Systemarchitektur zur Erfassung und Speicherung von Webseitenabzügen

4.1.1 Hybrider Ansatz: Client-Anwendung und Browser Plugin

Für die Erfassung von Webseitenabzügen wurde ein hybrider Ansatz gewählt, der die Vorteile einer Client-Anwendung mit denen eines Browser-Plugins kombiniert. Eine reine Browser-Plugin-Lösung wäre im Hinblick auf Sicherheitsmechanismen zu eingeschränkt. Die Client-Anwendung ermöglicht eine präzise Kontrolle über kryptographische Prozesse, während das Browser-Plugin die Nutzung erheblich vereinfacht: Rechtsverletzungen können direkt aus dem Browser heraus gemeldet werden. Das Plugin übermittelt dabei die jeweilige URL samt relevanter Parameter (z. B. Bannerentfernung ja/nein) an die Client-Anwendung, die anschließend die eigentliche Verarbeitung übernimmt.

Datenschutzrechtlich relevant ist, dass durch das Plugin keine personenbezogenen Daten verarbeitet werden. Es werden ausschließlich die für die Beweissicherung notwendigen Metadaten wie URL und Anzeigeparameter übertragen (vgl. DSGVO Art. 5 Abs. 1).

4.1.2 Crowd-Management

Das Crowd-Management (vgl. Abb. 1, obere Ebene) verteilt Aufgaben an die Crowd-Rechner, koordiniert deren Aktivitäten und sorgt für eine effiziente Lastverteilung. Damit können mehrere unabhängige Abzüge derselben URL erstellt werden, um die Beweissicherheit durch Redundanz zu erhöhen.

Bevor Crowd-Teilnehmende Aufgaben entgegennehmen können, müssen sie sich beim Crowd-Management-Server registrieren. Nach erfolgter Anmeldung wird ein Kommunikationskanal zum Server eröffnet. Neue Aufgaben werden anschließend aktiv vom Server an die verbundenen Clients verteilt. Dieses Push-Prinzip reduziert unnötigen Datenverkehr und ermöglicht eine ressourcenschonende Kommunikation.

Zur Wahrung der Anonymität arbeiten die Crowd-Teilnehmer ausschließlich unter Pseudonymen mit zufällig generierten Identifikatoren (UIDs). Personenbezogene Daten werden nicht gespeichert. Eine Offenlegung der Identität ist nur in vordefinierten Ausnahmefällen und nach Freigabe durch den oder die Systemadministrator:in vorgesehen.

4.1.3 Datenspeicher

Die Verwaltung der gesicherten Webseitenabzüge übernimmt der Datenspeicher (Abb. 1). Eine Ablage direkt in einer DLT ist aus rechtlichen Gründen nicht möglich, da Löschungsansprüche nach Urheberrecht oder DSGVO dort technisch nicht durchgesetzt werden können (Godyn et al. 2022). Der Datenspeicher erlaubt dagegen eine selektive Löschung, wenn Daten nicht mehr erforderlich sind.

Für die Speicherung gelten strenge Vorgaben:

- Der Zugriff auf die gespeicherten Verstoßdaten ist ausschließlich den Beweisführer:innen sowie einem eng begrenzten administrativen Personenkreis vorbehalten.
- Werden Cloud-Dienste genutzt, müssen die Daten verschlüsselt abgelegt werden. Der Speicherort ist innerhalb der Europäischen Union zu wählen, und die techni-

schen und organisatorischen Maßnahmen (TOMs) sind auf Datenschutzkonformität zu prüfen.
- Im Einklang mit dem Grundsatz der Speicherbegrenzung (Art. 5 Abs. 1 lit. e DSGVO) dürfen die Daten nur für eine festgelegte Dauer gespeichert werden. Technische Mechanismen stellen sicher, dass Speicherfristen eingetragen und nach Ablauf automatisch umgesetzt werden.

4.1.4 Rechte- und Rollenmanagement

Ein dediziertes Rechte- und Rollenmanagement stellt sicher, dass nur autorisierte Akteur:innen Zugriff auf die gespeicherten Abzüge erhalten. Dies ist insbesondere mit Blick auf sensible Daten sowie Datenschutzanforderungen unerlässlich.

Das Rollenmodell ist so ausgestaltet, dass insbesondere ausschließlich die jeweiligen Beweisführer:innen Zugriff auf die von ihnen erstellten Verstoßdaten erhalten. Weitergehende Zugriffe sind nur in vorher definierten Ausnahmefällen möglich und werden technisch streng kontrolliert. Auf diese Weise wird die datenschutzkonforme Trennung zwischen Beweisführung und allgemeiner Systemnutzung gewährleistet.

4.1.5 Distributed-Ledger-Integration

Die DLT übernimmt die manipulationssichere Absicherung der erzeugten Nachweise. Zur ressourcenschonenden Speicherung wird ein Merkle-Tree-Ansatz eingesetzt, der es ermöglicht, eine große Zahl von Hashwerten effizient in einer einzigen Transaktion zu bündeln (de Crespo und García 2016). Dadurch lassen sich selbst öffentliche Blockchains mit vertretbarem Aufwand und ressourcenschonend nutzen.

Kennzeichnend für die Integration ist die dezentrale Organisation. Die Validierung der Einträge erfolgt durch eine angemessene Anzahl unabhängiger Teilnehmender

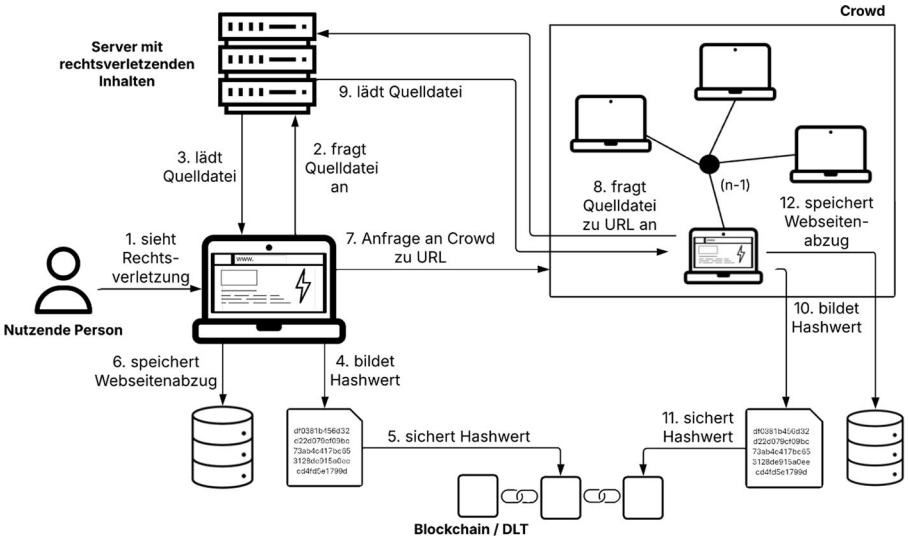

Abb. 2 Prozess der beweissicheren Erfassung und Speicherung von Webseitenabzügen

in einem Peer-to-Peer-Netzwerk. Auf diese Weise verteilt sich die Verantwortung auf viele Akteur:innen, wodurch die Robustheit des Verfahrens erheblich steigt (Nakamoto 2009) und eine Abhängigkeit von einzelnen Instanzen vermieden wird.

Da ausschließlich Hashwerte und keine Originaldaten in der Blockchain gespeichert werden, entstehen keine Risiken im Hinblick auf Urheberrecht und personenbezogene Daten. Damit erfüllt die Distributed-Ledger-Integration die Anforderungen der DSGVO und ist ein manipulationssicheres, datenschutzkonformes Element der Beweiskette.

4.2 Prozess der beweissicheren Speicherung von Webseiten

Der Ablauf der beweissicheren Erfassung ist in Abb. 2 dargestellt.

Identifikation und erste Erfassung Sobald eine nutzende Person beim Surfen im Internet mit ihrem Webbrowser auf einer Internetseite eine potenzielle Rechtsverletzung bemerkt (1), kann mit Hilfe des Browser-Plugins oder direkt über die Client-Anwendung die betreffende Quelldatei vom Quellserver abgefragt und lokal geladen (2–3) werden. Die Client-Anwendung erstellt daraus einen Webseitenabzug, der neben den Quelldateien auch grafische Darstellungen als Bild- und PDF-Export sowie umfassende Metadaten enthält – darunter Seitentitel, Beschreibung, SEO-Informationen, SSL-Status und Port. Zusätzlich umfasst er eine Übersicht aller auf der Seite verfügbaren Ressourcen wie Scripts, Stylesheets, Links, Bilder, Videos und Formulare mit ihren jeweiligen Eigenschaften. Ferner beinhaltet der Abzug technische Daten zu Browser und System der Nutzer:in. Diese einzelnen Komponenten (der Webseitenabzug) werden in einer ZIP-Datei zusammengeführt, über die anschließend ein kryptographischer Hashwert (4) berechnet wird. Schon kleinste Veränderungen am Webseitenabzug würden zu einem anderen Hashwert führen, wodurch Manipulationen sofort erkennbar werden. Anschließend wird der Hashwert in der DLT gesichert (5), während der Webseitenabzug selbst auf dem Speicherserver abgelegt wird (6). Auf diese Weise werden sowohl Nachvollziehbarkeit als auch Prüfbarkeit der Beweise gewährleistet.

Absicherung durch die Crowd Um den Beweiswert zu erhöhen, initiiert die Client-Anwendung zusätzlich eine Anfrage an die Crowd (7). Mehrere Crowd-Teilnehmende rufen die Quelldatei unabhängig voneinander erneut vom Quellserver ab (8–9) und bilden jeweils eigene Webseitenabzüge, die gehasht (10) und in der DLT gesichert werden (11). Die von jedem Crowd-Teilnehmenden erzeugten Webseitenabzüge werden ebenfalls gespeichert (12). Dabei gilt: Erst wenn eine definierte Anzahl N an unabhängigen Webseitenabzügen vorliegt, wird die Beweissicherung als hinreichend validiert betrachtet. Diese redundante Vorgehensweise verhindert, dass der Nachweis ausschließlich auf einer Einzelinstanz basiert. Zugleich wird die Verantwortung auf viele Akteur:innen verteilt, was die Robustheit des Verfahrens erheblich steigert.

Das System geht von einem Bedrohungsmodell aus, bei dem sowohl der oder die ursprüngliche Erfasser:in als auch die Online-Anbietenden als potenziell korrumpierbar betrachtet werden. Um die Integrität zu sichern, wird eine Schwelle von N

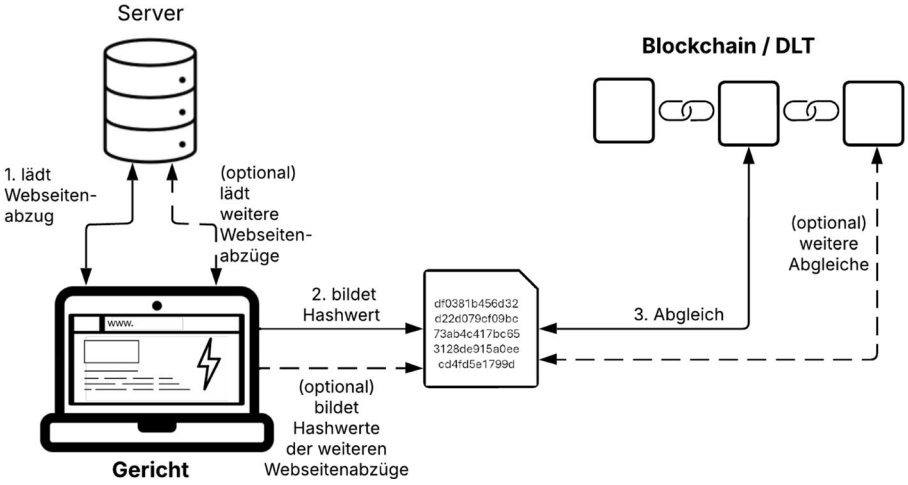

Abb. 3 Prozess der Beweisführung auf Basis abgesicherter Webseitenabzüge

unabhängigen Crowd-Bestätigungen vorausgesetzt (vgl. Abschnitt 6.4). Diese Redundanz minimiert die Angriffsfläche für gezielte Falschdokumentationen oder Absprachen (Collusion), da mit einem Angriff die Mehrheit der zufällig ausgewählten Crowd-Rechner kontrolliert werden müsste, um den Beweiswert zu unterwandern.

Dezentrale Validierung Jeder Hashwert kann unabhängig überprüft werden und belegt damit die Integrität des jeweiligen Webseitenabzugs. Da die Validierung des Rechtsverstoßes durch viele voneinander unabhängige Teilnehmende erfolgt, wird die Authentizität der Beweise gestärkt und Manipulationen lassen sich zuverlässig ausschließen. Gleichzeitig sorgt die unveränderliche Ablage in der DLT dafür, dass die Beweiskette jederzeit nachvollziehbar bleibt und eine lückenlose Prüfbarkeit gewährleistet ist.

4.3 Beweisführung

Neben der Erfassung und dezentralen Absicherung ist auch der gerichtliche Nachweis ein zentraler Bestandteil des Gesamtsystems. Der Ablauf der Beweisführung ist in Abb. 3 dargestellt.

Abruf des Beweismaterials Im Streitfall lädt das Gericht oder eine autorisierte Stelle den zuvor erstellten Webseitenabzug vom Datenspeicher herunter (1). Dieser enthält die vollständige Momentaufnahme der beanstandeten Inhalte.

Berechnung des Hashwerts Anschließend wird lokal ein Hashwert über den gespeicherten Abzug gebildet (2). Da Hashwerte die Integrität der Daten eindeutig repräsentieren, kann durch diesen Schritt überprüft werden, ob der Abzug unverändert vorliegt.

Abgleich mit der DLT Der berechnete Hashwert wird mit dem zuvor in der DLT gesicherten Wert abgeglichen (3). Stimmen die Hashwerte überein, ist die Authentizität des Beweismaterials nachgewiesen. Zudem dokumentiert die DLT manipulationssicher den Zeitpunkt der Speicherung des Hashwertes. Optional können zusätzliche Abgleiche mit den Webseitenabzügen und Hashwerten der weiteren Crowd-Teilnehmenden vorgenommen werden, um den Beweiswert weiter zu erhöhen.

Juristische Verwertbarkeit Durch diesen mehrstufigen Prozess entsteht eine manipulationssichere Kette von Nachweisen. Die Kombination aus lokalem Webseitenabzug, Hashwert und DLT-Eintrag gewährleistet, dass das Material in juristischen Verfahren nachvollziehbar und überprüfbar vorgelegt werden kann. Damit wird sowohl den Anforderungen an Integrität und Authentizität als auch den praktischen Bedürfnissen der Beweisführung entsprochen.

5 Technische Umsetzung

5.1 Architektur und eingesetzte Technologien

Auf Basis der in Kapitel 4 beschriebenen Systemarchitektur wurde im Rahmen des Projekts ein Demonstrator entwickelt, der die technische Realisierbarkeit und Praxistauglichkeit des Lösungsansatzes aufzeigt. Der Fokus lag auf einem klar abgegrenzten Anwendungsfall: der Nutzung durch Verbraucherzentralen, die in ihrer täglichen Arbeit systematisch Rechtsverstöße im Internet dokumentieren müssen. Der Demonstrator setzt die einzelnen Komponenten der Architektur prototypisch um und integriert diese zu einem durchgängigen Prozess der Beweissicherung.

Die Client-Anwendung bildet dabei die zentrale Komponente und dient als Hauptschnittstelle, über die das gesamte System von den Nutzenden bedient wird. Von hier aus werden Webseitenabzüge erfasst, an die anderen Komponenten weitergegeben und für die Beweissicherung vorbereitet. Das Rechte- und Rollenmanagement ist als eigenständige Komponente umgesetzt, um den Zugriff auf sensible Daten strikt zu steuern und die Trennung zwischen verschiedenen Rollen sicherzustellen. Die Funktionen von Datenspeicher und Crowd-Management wurden im Demonstrator als ein gemeinsamer Server (Backend) realisiert. Während der Datenspeicher die gesammelten Abzüge verwaltet und datenschutzkonform aufbewahrt, sorgt das Crowd-Management dafür, dass dieselben Inhalte von mehreren Teilnehmenden gesichert werden. Für die Absicherung der Nachweise in der DLT fiel die Wahl auf die leichtgewichtige Lösung OpenTimestamps[8], die eine effiziente Verankerung von Hashwerten in der Bitcoin-Blockchain ermöglicht und die zentralen Anforderungen nach Manipulationssicherheit, Nachvollziehbarkeit und langfristiger Beweisfähigkeit erfüllt.

Die Verifikation der Beweisdaten erfolgt über sogenannte Timestamp-Dateien (OTS-Dateien), die bei der Erfassung automatisch erstellt werden. Diese Dateien enthalten alle notwendigen Informationen, um den ursprünglichen Hashwert eines

[8] https://opentimestamps.org/, zuletzt zugegriffen am 24.09.2025.

gespeicherten Webseitenabzugs zu einem späteren Zeitpunkt mit dem in der Blockchain verankerten Hashwert abzugleichen. Auf diese Weise kann unabhängig und dezentral überprüft werden, ob eine Datei seit ihrer Abspeicherung unverändert geblieben ist. Der Prozess ist nicht auf den Prototypen oder bestimmte Serverinstanzen beschränkt, sondern erlaubt eine langfristige und quelloffen nachvollziehbare Verifikation. Damit wird die Integrität der Beweise gestärkt, auch wenn sie erst Monate oder Jahre nach der Erfassung vor Gericht benötigt werden.

Der Demonstrator folgt einer klaren Client-Server-Architektur: Das Frontend wurde unter Verwendung des Frameworks Vue.js[9] implementiert und ist für die Bereitstellung der Benutzungsoberfläche verantwortlich. Das Backend basiert auf Node.js[10] und übernimmt die serverseitige Logik, insbesondere die Datenverwaltung sowie das Crowd-Management. Für das Identitäts- und Berechtigungsmanagement wurde Supabase[11] integriert, während die Browser-Automatisierung mit Puppeteer[12] realisiert wurde.

5.2 Benutzungsoberfläche des Demonstrators

Der Demonstrator hat bewusst nur eine schlicht und funktional gehaltene Benutzungsoberfläche, da der Fokus in der Machbarkeitsstudie auf der Untersuchung der funktionalen Anforderungen und der technischen Umsetzbarkeit lag. Das Browser-Plugin wurde noch nicht realisiert.

Startseite zur Eingabe der URL Auf der Startseite der Client-Anwendung (siehe Abb. 4) gibt die nutzende Person die Adresse der verdächtigen Webseite ein. Optional kann die automatische Entfernung von Cookie-Bannern und Pop-ups aktiviert werden, sodass störende Overlays die Erfassung nicht beeinträchtigen. Die Banner-Entfernung wird durch einen Adblocker in Kombination mit einem Algorithmus

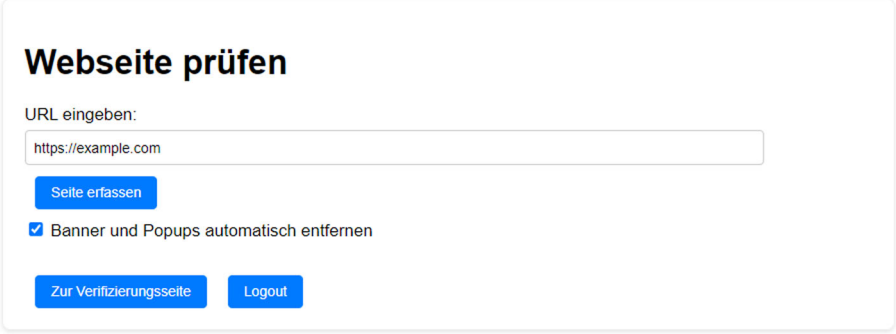

Abb. 4 Startseite im Demonstrator

[9] https://vuejs.org/, zuletzt zugegriffen am 24.09.2025.

[10] https://nodejs.org/en, zuletzt zugegriffen am 24.09.2025.

[11] https://supabase.com/, zuletzt zugegriffen am 24.09.2025.

[12] https://pptr.dev/, zuletzt zugegriffen am 24.09.2025.

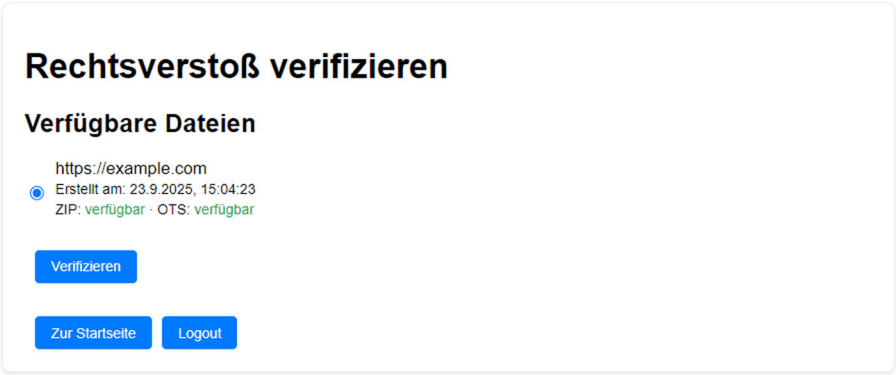

Abb. 5 Verifizierungsseite im Demonstrator mit einem Eintrag in der Liste

realisiert, der Cookie-Banner anhand typischer CSS-Selektoren und Button-Texte identifiziert und automatisch entfernt.

Mit einem Klick auf *Seite erfassen* wird der Prozess gestartet.

Erfassung der Webseite Nach der Eingabe der URL wird die Seite im Hintergrund geladen und unter anderem ein Screenshot als PDF erzeugt. Dieser wird der nutzenden Person zur Überprüfung angezeigt. Nach positiver Bestätigung, dass auf dem Screenshot der vorliegende Rechtsverstoß erkennbar ist, wird der Webseitenabzug auf dem Datenspeicher (Backend) gespeichert und die Speicherung des Hashwertes in die Blockchain initiiert.

Übersicht und Verifikation Über einen Button auf der Startseite kann die nutzende Person die Verifizierungsseite aufrufen und dort die Hashwerte der von ihr initiierten Webseitenabzüge im Nachgang überprüfen. Auf der Verifizierungsseite werden alle von dem oder der Nutzer:in erfassten Webseiten aufgelistet. Nach Auswahl eines Eintrags wird die zugehörige Datei aus dem Datenspeicher geladen, ihr Hashwert neu berechnet und mit dem in der Bitcoin-Blockchain verankerten Nachweis verglichen (vgl. Abb. 5). Liegt noch kein Eintrag in der DLT vor, wird dies angezeigt; andernfalls erhält die nutzende Person eine Textausgabe, die bestätigt, dass der ausgewählte Webseitenabzug seit dem dokumentierten Zeitpunkt unverändert geblieben ist.

5.3 Alternative Umsetzungsmöglichkeiten

Neben der gewählten Referenzarchitektur existieren verschiedene technologische Ansätze, die die Leistungsfähigkeit und Effizienz von Systemen zur Beweissicherung im digitalen Raum weiter erhöhen können.

Der Einsatz einer öffentlichen DLT-Infrastruktur wie der Blockchain via OpenTimeStamps ist das Ergebnis einer Abwägung: Das Aufsetzen einer separaten DLT-Infrastruktur wäre mit erheblichem technischem und organisatorischem Aufwand verbunden gewesen und hätte aufgrund der geringen Nutzerbasis des Demonstrators

ihre Vorteile nicht ausspielen können. Als Alternativen wären etwa permissioned Blockchains wie Hyperledger Fabric oder Quorum in Betracht gekommen, die eine stärkere Kontrolle über Governance und Zugriffsrechte ermöglichen und in Unternehmensumfeldern häufig für Nachweis- und Audit-Szenarien eingesetzt werden, z. B. in Regueiro et al. (2021).

Eine weitere Option besteht im Einsatz gerichteter azyklischer Graphen (Directed Acyclic Graphs, kurz DAGs). Anders als die klassische Blockchain, die Transaktionen sequenziell in Blöcken verarbeitet, ermöglichen DAG-Strukturen eine parallele Validierung (Miao et al. 2021). Dadurch könnten sich Skalierbarkeit und Energieverbrauch deutlich verbessern, insbesondere wenn eine große Zahl gleichzeitiger Transaktionen verarbeitet werden muss (Quasim et al. 2020). In einem erweiterten Szenario ließe sich ein DAG zudem mit dem InterPlanetary File System (IPFS) kombinieren, um eine dezentrale, inhaltsadressierte Speicherung zu realisieren. Dateien wären dann über kryptografische Hashes referenziert, sodass Manipulationen unmittelbar erkennbar wären und Redundanz über ein weltweites Peer-to-Peer-Netzwerk sichergestellt würde.

Auch konsortiale und hybride Modelle erscheinen als interessante Alternativen. Konsortiale Architekturen würden es erlauben, dass eine definierte Gruppe vertrauenswürdiger Institutionen – etwa Behörden oder Verbraucherschutzorganisationen – gemeinsam eine Distributed-Ledger-Infrastruktur betreibt. Damit ließe sich eine geteilte Governance etablieren, die zugleich klare Zugriffsrechte wahrt. Darüber hinaus könnten hybride Modelle, die klassische Blockchains mit DAG-Strukturen verbinden, zusätzliche Vorteile eröffnen.

Diese alternativen Ansätze verdeutlichen, dass neben klassischen Blockchain-Implementierungen eine Vielzahl an Weiterentwicklungen existiert, die die Skalierbarkeit, Energieeffizienz und Flexibilität solcher Systeme verbessern könnten. Gleichzeitig erfordern sie – wie auch die Referenzarchitektur – eine sorgfältige rechtliche und organisatorische Einbettung, um Datenschutz, Nachvollziehbarkeit und Akzeptanz sicherzustellen.

Eine Umsetzung muss dabei nicht zwangsläufig auf einer DLT basieren. Das Grundprinzip der manipulationssicheren Archivierung ließe sich ebenso durch verteilte Speichersysteme realisieren, die über kryptografische Hashes und Replikationsmechanismen Integrität und Redundanz gewährleisten. Dateisysteme wie IPFS[13] oder Swarm[14] verdeutlichen, dass eine dezentrale, inhaltsadressierte Speicherung auch unabhängig von klassischen Blockchain-Architekturen möglich ist (Xu 2023).

6 Offene Herausforderungen

Trotz der entwickelten Referenzarchitektur zur beweissicheren Dokumentation bestehen weiterhin verschiedene technische und organisatorische Herausforderungen, die in zukünftigen Arbeiten adressiert werden müssen. Diese betreffen insbesondere

[13] https://ipfs.tech/, zuletzt zugegriffen am 30.09.2025.

[14] https://www.ethswarm.org/, zuletzt zugegriffen am 30.09.2025.

die Aufnahme dynamischer Inhalte, die Beweisführung in geschützten Bereichen sowie die Vergleichbarkeit von Abzügen, die zwangsläufig Unterschiede aufweisen.

6.1 Schwierigkeit bei der Aufnahme bewegter Bilder

Viele Rechtsverstöße im digitalen Raum manifestieren sich nicht in statischen Momentaufnahmen, sondern über den Verlauf einer Interaktion. Ein typisches Beispiel sind sogenannte Dark Patterns, die erst durch die sukzessive Navigation einer Website sichtbar werden, etwa wenn bestimmte Schaltflächen erst nach mehreren Klicks erscheinen oder Inhalte zeitlich verzögert eingeblendet werden, was in den Experteninterviews (siehe Abschn. 2.2) betont wurde. Klassische Screenshots können diese Abläufe nicht vollständig erfassen. Als Lösungsansatz bietet sich der Einsatz von Screen-Recording-Technologien in Kombination mit Metadaten wie Klickpfaden, Zeitstempeln und dem Dokument-Objekt-Modell (zugrunde liegende Struktur und Objekte der Seite) an, um Interaktionen und dynamische Elemente vollständig und nachvollziehbar zu dokumentieren. Allerdings wird dadurch gleichzeitig die Verifikation durch die Crowd erschwert.

6.2 Geschützte Webseitenbereiche

Einige Verstöße treten nicht im frei zugänglichen Internet auf, sondern in durch eine Anmeldung geschützten Bereichen wie Mitgliederportalen oder hinter Bezahlschranken. In diesen Fällen ist eine Verifikation durch die Crowd nicht möglich, da nur ausgewählte Personen Zugriff auf die Inhalte mit dem Rechtsverstoß haben. Damit entfällt ein zentrales Element der redundanten Erfassung. Für derart geschützte Bereiche, in denen eine Crowd-Verifikation nicht möglich ist, müssen alternative Verfahren in Betracht gezogen werden, etwa die Dokumentation durch vertrauenswürdige Instanzen im Auftrag der Betroffenen.

6.3 Unterschiede in den Abzügen und fehlende Vergleichbarkeit

Ein praktisches Problem liegt darin, dass Webseiten dynamische Inhalte einbinden, beispielsweise Werbung oder personalisierte Empfehlungen. Zwei Nutzende, die zeitgleich denselben Webseitenabzug erstellen, insbesondere je nach Region, erhalten daher oft leicht unterschiedliche Inhalte. In der Folge unterscheiden sich auch die Hashwerte, obwohl die relevanten Verstöße in beiden Abzügen enthalten sind. Das erschwert den automatisierten Abgleich und kann den Beweiswert mindern. Um das Problem dynamischer Inhalte zu adressieren, können Verfahren eingesetzt werden, die trotz individueller Unterschiede eine inhaltliche Übereinstimmung erkennen, z. B. durch Textanalyse oder Mustererkennung, durch die Segmentierung von Abzügen in relevante und irrelevante Bereiche oder durch den Einsatz von Fuzzy-Hashing (Kornblum 2006), das auch Ähnlichkeiten zwischen Dateien berücksichtigt.

6.4 Systemsicherheit

Eine zentrale Herausforderung bleibt die Absicherung des gesamten Erfassungsprozesses gegen gezielte Manipulationen. Angriffsflächen finden sich dabei auf verschiedenen Ebenen: Lokal könnten Angreifende versuchen, den Webseiteninhalt unmittelbar vor der Erfassung zu verfälschen, etwa durch den Einsatz von Proxies. Weiterhin besteht das Risiko, dass infizierte Endgeräte (Malware) den Dokumentationsprozess unbemerkt korrumpieren, oder dass durch gezielte *Sybil-Angriffe* (Erstellung multipler Scheinidentitäten in der Crowd) versucht wird, den Konsensmechanismus zu unterwandern. In diesem Kontext ist die Bestimmung der notwendigen Schwelle N an unabhängigen Bestätigungen ein entscheidender Faktor, der im Rahmen weiterer Forschungsarbeiten validiert werden muss. Die Festlegung dieses Wertes stellt dabei keine rein technische Entscheidung dar, sondern erfordert eine interdisziplinäre Abwägung:

- Technisch muss N groß genug sein, um die statistische Wahrscheinlichkeit erfolgreicher Absprachen oder Manipulationen (Collusion) zu minimieren
- Juristisch ist zu klären, welche Anforderungen an eine „Vielzahl“ unabhängiger Bestätigungen zu stellen sind, um die freie richterliche Beweiswürdigung (§ 286 ZPO) positiv zu beeinflussen und den Beweiswert eines „Augenscheinsurrogats“ zu festigen

Die Ermittlung eines ausreichend großen N muss daher sowohl die technische Resilienz als auch die prozessrechtliche Akzeptanz berücksichtigen.

7 Ausblick

Die aktuelle Umsetzung ist zunächst auf den Anwendungsfall der Verbraucherzentralen beschränkt, um die Machbarkeit auf einem klar abgegrenzten Feld nachzuweisen. Mittel- bis langfristig besteht jedoch die Möglichkeit einer Skalierung auf breitere Nutzergruppen. Neben Verbraucherzentralen könnten auch andere Organisationen, Unternehmen oder sogar Einzelpersonen die Infrastruktur nutzen, um Rechtsverstöße im digitalen Raum zu dokumentieren. Besonders relevant wäre dies etwa bei der Dokumentation von Hassrede, Desinformation, Urheberrechtsverletzungen, unlauteren Geschäftspraktiken oder digitalem Mobbing in sozialen Medien. Eine solche Erweiterung setzt allerdings ein differenziertes Rechte- und Rollenmanagement voraus, um sensible Daten zu schützen und rechtliche Vorgaben einzuhalten. Parallel dazu eröffnet sich ein Entwicklungspfad in Richtung erhöhter Datensicherheit, etwa durch serverseitige Verschlüsselung mit speziellen Verfahren, sodass Inhalte zwar von allen gespeichert, aber nur von wenigen autorisierten Stellen entschlüsselt werden können. Dadurch ließen sich externe Speicherdienste (z. B. AWS Cloud) flexibler einbeziehen und Kosten reduzieren, ohne die Integrität der Beweise zu gefährden.

Auch technologische Weiterentwicklungen bieten Potenzial: Proof-of-Stake- oder DAG-basierte Systeme versprechen eine energieeffizientere Verarbeitung, während konsortiale Architekturen und hybride Modelle die Skalierbarkeit und Governance flexibilisieren könnten. Ergänzend wären Smart Contracts zur Automatisierung von

Prüf- und Zugriffsprozessen sowie der Einsatz von IPFS für eine dezentrale, inhaltsadressierte Speicherung denkbar. Diese Optionen würden die Funktionsweise erheblich erweitern, erfordern jedoch eine sorgfältige rechtliche und organisatorische Einbettung.

Über die technische Weiterentwicklung hinaus sind die gesellschaftlichen Implikationen zentral. Eine breitere Anwendung könnte das Vertrauen in die digitale Rechtsdurchsetzung stärken und Transparenz im Umgang mit Online-Verstößen fördern. Gleichzeitig stellen sich Fragen nach Datenschutz, Verantwortungszuschreibung und der Wahrung demokratischer Prinzipien, um Missbrauch zu verhindern und Akzeptanz zu sichern.

Damit zeigt sich, dass die vorgeschlagene Architektur nicht nur eine kurzfristige Lösung für spezifische Herausforderungen im Verbraucherschutz bietet, sondern auch methodische und konzeptionelle Grundlagen bereitstellt, um ähnliche Verfahren in anderen Anwendungsdomänen wie Urheberrecht, Hate Speech oder digitalen Bedrohungen zu erproben. Der Beitrag verdeutlicht somit sowohl den praktischen Nutzen einer rechtskonformen, technisch abgesicherten Beweissicherung als auch das Potenzial für weiterführende Forschungs- und Entwicklungsarbeiten.

Danksagung Die Autor:innen danken der Baden-Württemberg Stiftung für die Finanzierung des Projekts EVIDENTT -– „Einsatz verteilter Technologien zur beweissicheren Dokumentation von Verbraucherschutzverstößen auf Online-Plattformen“ im Rahmen des Forschungsprogramms „Ideenwettbewerb Blockchain“, das neuartige, datenschutzkonforme und gesellschaftlich relevante Anwendungen von Distributed-Ledger-Technologien unterstützt. Diese Arbeit wurde von den KASTEL Security Research Labs, Karlsruhe unterstützt.

Funding Open Access funding enabled and organized by Projekt DEAL.

Interessenkonflikt M. Ullrich, N. Kruse, G. Schiefer, Z. Al-Washash, S. Kroschwald und T. Schuster geben an, dass kein Interessenkonflikt besteht.

Literatur

Belen-Saglam R, García-Bañuelos L, Matulevičius R (2022) A systematic literature review of the tension between the GDPR and public blockchain systems. arXiv preprint

BGH (2023) Beschluss vom 10. Okt. 2023 – XI ZB 1/23

Brotsis S, Kolokotronis N, Limniotis K et al (2019) Blockchain Solutions for Forensic Evidence Preservation in IoT Environments. In: 2019 IEEE Conference on Network Softwarization (NetSoft). IEEE, Paris, S 110–114

Casey E (2011) Digital evidence and computer crime: forensic science, computers and the Internet, 3. Aufl. Elsevier

Chen S, Zhao C, Huang L et al (2020) Study and implementation on the application of blockchain in electronic evidence generation. Forensic Sci Int Digit Investig 35:301001. https://doi.org/10.1016/j.fsidi.2020.301001
de Crespo ASP, García LIC (2016) Stampery Blockchain Timestamping Architecture (BTA). Stampery / Aragon
Giannelli PC (1996) Chain of custody. Case Western Reserve University, School of Law
Godyn M, Wojciechowski M, Gregorczyk M (2022) Analysis of solutions for a blockchain compliance with GDPR. PeerJ Comput Sci 8:e1062. https://doi.org/10.7717/peerj-cs.1062
Gray CM, Kou Y, Battles B et al (2018) The dark (patterns) side of UX design. In: Proceedings of the 2018 CHI conference on human factors in computing systems, S 1–14
Härer F, Fill H-G (2020) Blockchain-basierte Attestierung von Identitäten und Dokumenten
Kornblum J (2006) Identifying almost identical files using context triggered piecewise hashing. Digit Investig 3:91–97. https://doi.org/10.1016/j.diin.2006.06.015
Li M, Lal C, Conti M, Hu D (2021) LEChain: a blockchain-based lawful evidence management scheme for digital forensics. Future Gener Comput Syst 115:406–420. https://doi.org/10.1016/j.future.2020.09.038
Mankowski (2016) Kapitel zu § 12 UWG. In: Fezer B, Obergfell (Hrsg) Lauterkeitsrecht: UWG, 3. Aufl. Bd 1. C.H. Beck, München
Mathur A, Acar G, Friedman MJ et al (2019) Dark patterns at scale: findings from a crawl of 11K shopping websites. Proc Acm Hum Comput Interact 3:81:1–81:32. https://doi.org/10.1145/3359183
Miao Z, Ye C, Yang P et al (2021) Blockchain-based electronic evidence storage and efficiency optimization. In: 2021 International Conference on Artificial Intelligence and Blockchain Technology (AIBT), S 109–113
Nakamoto S (2009) Bitcoin: a Peer-to-Peer electronic cash system
OLG Jena (2018) Urteil vom 28.11.2018–2 U 524/17
Quasim M, Ayoub M, Algarni F et al (2020) Blockchain Frameworks, S 75–89
Regueiro C, Seco I, Gutiérrez-Agüero I et al (2021) A blockchain-based audit trail mechanism: design and implementation. Algorithms. https://doi.org/10.3390/a14120341
Sakshi MA, Sharma AK (2024) A survey on blockchain based IoT forensic evidence preservation: research trends and current challenges. Multimed Tools Appl 83:42413–42458. https://doi.org/10.1007/s11042-023-17104-z
Xu S (2023) Dissecting IPFS and Swarm to demystify distributed decentralized storage networks. École Polytechnique Fédérale de Lausanne (EPFL)
Zafar A, Buckley P, Camilleri MA, Andriotis P (2024) Reconciling blockchain technology and data protection laws. J Cybersecur 11:tyaf2. https://doi.org/10.1093/cybsec/tyaf002
Zimmermann (2016) § 371. In: Münchener Kommentar zur Zivilprozessordnung (ZPO). C.H. Beck, München