USING BLOCKCHAIN TECHNOLOGY FOR PRESERVING DIGITAL EVIDENCE IN DIGITAL FORENSICS

Inda Kreso
Faculty of Criminal Justice, Criminology and Security Studies University of Sarajevo,
Bosnia and Herzegovina, indakreso@fkn.unsa.ba

Abstract: Digital forensics is a forensic discipline that is developing very quickly because it is forced to keep up with the development of technology itself. As technology develops and advances, digital forensics must also develop at the same speed, because criminals actively use the latest technologies to commit crimes. One of the most important phases in digital forensics is the investigative phase, which is carried out by trained personel while investigating certain crimes. In this phase, all data in digital records is collected from all available devices: computers, mobile phones, signals from the phone base station, recorded messages, video files, e-mails, network traffic and other examples of digital evidence. One of the basic and most important processes in digital forensics is the management of digital evidence. Since digital evidence is very delicate by its nature, it is of utmost importance that the integrity of the evidence is fully preserved in the process of collecting evidence and later analyzing the evidence. Blockchain in digital forensics allows the digital evidence collected in the investigative phase not to be damaged or changed during transfer. One of the basic characteristics of blockchain technology is that it enables the confidentiality of data to be maintained. In addition to the above, blockchain guarantees authenticity, immutability and resilience when transferring evidence. Blockchain enables chronological sorting of transactions within blocks. Each block contains an encrypted hash of the previous block in the same chain. Each block in the chain in which data is stored also contains a timestamp and a link to data referring to the previous block. This is crucial, because it allows preserving the authenticity of evidence in the same state in which it was first discovered and collected. In other words, blockchain enables the following: preserving the integrity of the complete transfer of digital evidence, authentication that provides recognizable proof of the identity of the evidence, confidentiality and security that implies preventing unauthorized access or modification of the evidence, and encryption that allows encryption using various algorithms so that the evidence is not compromised. This paper used a systematic literature review to investigate in what ways blockchain technology helps preserve the integrity of digital evidence, and whether this technology makes digital evidence transparent and protected. The three characteristics mentioned in the literature (integrity, transparency and security of digital evidence) are listed as the most important for the proper conduct of digital investigations, and for this reason they were selected for examination in this paper. Blockchain has already been successfully used in other industries and fields, however, its application in digital forensics and forensic science in general is of utmost importance because it enables the development of more secure solutions that can contribute to more fair trial of committed crimes.
Keywords: blockchain, digital forensics, digital evidence, investigation, integrity of evidence

UPOTREBA BLOCKCHAIN TEHNOLOGIJE U SVRHU OČUVANJA DIGITALNOG DOKAZA U DIGITALNOJ FORENZICI

Inda Kreso
Fakultet za kriminalistiku, kriminologiju i sigurnosne studije Univerziteta u Sarajevu,
Bosna i Hercegovina, indakreso@fkn.unsa.ba

Abstrakt: Digitalna forenzika je forenzička disciplina koja se razvija jako brzo jer je primorana da u stopu prati i samo razvijanje tehnologije. Kako se razvija i napreduje tehnologija, tom istom brzinom se mora razvijati i digitalna forenzika, jer kriminalci aktivno koriste najnovije tehnologije za izvršavanje krivičnih djela. Jedan od najbitnijih faza u digitalnoj forenzici jeste istražna faza koju provode obučena lica prilikom istraživanja određenih krivičnih djela. U ovoj fazi se svi podaci u digitalnim zapisima prikupljaju sa svih dostupnih uređaja: računari, mobiteli, signali sa bazne stanice telefona, snimljene poruke, video fajlovi, e-mailovi, mrežni saobraćaj i ostali primjeri digitalnih dokaza. Jedan od osnovnih i najbitnijih procesa u digitalnoj forenzici jeste upravljanje digitalnim dokazima. Kako je digitalni dokaz po svojoj prirodi veoma delikatan, od iznimne je važnosti da se u procesu prikupljana dokaza i kasnije analize dokaza, integritet dokaza u potpunosti sačuva. Blockchain u digitalnoj forenzici omogućava da prikupljeni digitalni dokazi u istražnoj fazi prilikom transfera ne bude oštećen ili izmijenjen. Jedna od osnovnih karakteristika blockchain tehnologija jeste omogućavanje očuvanja povjerljivosti podataka. Pored

navedenog, blockchain garantuje autentičnost, nepromjenjivost i otpornost prilikom prenošenja dokaznog materijala. Blockckhain omogućava hronološko sortiranje transakcija unutar blokova. Svaki blok sadrži krptovani hash prethodnog bloka u istom lancu. Svaki od blokova u lancu u koji se spremaju podaci sadrži i vremensku oznaku i vezu sa podacima koji upućuju na prethodni blok. Navedeno je krucijalno, jer omogućava očuvanje autentičnosti dokaznog materijala u istom stanju u kojem je prvi put otkriven i prikupljen. Drugim riječima, blockchain omogućava slijedeće: čuvanje integriteta kompletnog transfera digitalnih dokaza, autentifikaciju koja omogućava prepoznatljiv dokaz identiteta dokaznog materijala, povjerljivost i sigurnost što podrazumijeva onemogućavanje nevolaštenog pristupa ili izmjene dokaznog materijala, te enkripciju koja omogućava šifriranje putem različitih algoritama kako se dokazni materijal ne bi kompromitovao. U ovom radu korišten je sistematski pregled literature kako bi se istražilo na koje načine blockchain tehnologija pomaže u očuvanju integriteta digitalnog dokaza, te da li ga ova tehnologija čini digitalni dokaz transparentnim i zaštićenim. Navedene tri karakteriste su u literaturi (integritet, transparentnost i sigurnost digitalnog dokaza) navedene kao najvažnije za ispravno provođenje digitalne istrage, te su iz navedenog razloga i odabrane za ispitivanje u ovom radu. Blockchain je već uspješno korišten u drugim branšama i oblastima, međutim njegova primjena u digitalnoj forenzici i forenzičkoj nauci općenito je od iznimne važnosti jer omogućava razvijanje sigurnijih rješenja koji mogu doprinjeti pravičnijem suđenju izvršenih krivičnih djela.
Ključne riječi: blockchain, digitalna forenzika, digitalni dokaz, istraga, integritet dokaza

1. UVOD

Digitalna forenzika, poznata i kao kompjuterska forenzika ili sajber forenzika, jeste proces prikupljanja, čuvanja, analize i predstavljanja digitalnih dokaza prikupljenih sa digitalnih uređaja i elektronskih sistema. Ovaj dokaz se često koristi u pravnoj praksi, odnosno u postupcima istrage sajber kriminala, kršenja sigurnosti, prevara i drugog oblika kompjuterskog kriminala. Evidentno je da je u digitalnoj forenzici od ključne važnosti ispravno upravljanje digitalnim dokazima koji se prikupljaju u fazi istrage. Od iznimne je važnosti zaštititi digitalne dokaze od bilo koje primjene ili uništavanja dokaza, odnosno očuvati integritet dokaza kako bi se prikupljeni digitalni dokaz u svojoj osnovnoj, neizmijenjenoj formi isporučio nadležnim organima (Carrier & Spafford, n.d.; Kebande et al., 2018; Mohammed et al., 2019; Prakash & Sadawarti, n.d.). Ukoliko dođe do bilo koje izmjene ili uništavanja digitalnog dokaza, isti se neće moći primijeniti kao dokazni materijal, što može uticati i na sami ishod suđenja i odluka suda u određenom krivičnom djelu. Kao jedno od rješenja za očuvanje sigurnosti, zaštite i kredibilnosti dokaza u digitalnoj forenzici se primjenjuje blockchain tehnologija. Blockchain tehnologija je zapravo distribuirani sistem za čuvanje podataka koji garantuje sigurnu, transparentnu i nepromjenjiljivu razmjenu informacija između uključenih strana (Ali et al., 2024; Degree Project Bachelor's An Analysis of Using Blockchains for Processing and Storing Digital Evidence, n.d.; S. Li et al., 2019; Mahrous et al., 2021; Muyambo & Omeleze Baror, n.d.; Tsai, 2021; Xiao et al., 2024). Blockchain tehnologija, zahvaljujući svojoj strukturi i dizajnu osigurava očuvanje integriteta, enkripciju, sigurnost i transparentnost digitalnog dokaza. Zbog svojih karakteristika blockchain je u literaturi opisan kao idelano rješenja za upravljanje digitalnim dokaznim materijalom u digitalnoj forenzici. Literatura vezana za korištenje blockchaina u digitalnoj forenzici, a posebno u fazi istrage, je poprilično zastupljena, pogotovo što je blockchain tehnologija od prije prepoznata i već uspješno korištena u drugim oblastima kao što su finansije, energetika, medicina, bankarstvo, osiguranje i ostalim sektorima (AlKhanafseh & Surakhi, 2024; Ekuma & Fon, n.d.; Hamid Lone & Naaz Mir, 2017; Kim et al., 2021; Tian et al., 2019). Kao ključna karakteristika blockchain-a, nepromjenjivost podataka omogućava da digitalni dokazi, pohranjeni u obliku blokova povezanih putem kriptografskih funkcija, ostanu neizmijenjeni i netaknuti tokom cijelog procesa prikupljanja i transfera. Ovaj nepromjenjivi zapis omogućava da svaki pokušaj izmjene dokaza bude odmah uočen, čime se povećava sigurnost i povjerenje u valjanost prikupljenih dokaza.

2. MATERIJALI I METODE

U ovom radu korišten je sistematski pregled literature koja je istraživala benefite upotrebe blockchain tehnologija za očuvanje digitalnih dokaza u digitalnoj forenzici, tačnije u istražnoj fazi, odnosno fazi koja podrazumijeva prikupljanje digitalnih dokaza. Cilj ovog rada jeste identificirati najbitnije karakteristike blockchain tehnologije koje direktno omogućavaju i garantuju nepromjenjivost digitalnog dokaza, te očuvanje integriteta prikupljenog dokaznog materijala. Baze podataka koje su pretražene u svrhu prikupljanja literature su: ResearchGate, Academia.edu i JSTOR. Navedene baze podataka su pretražene koristeći sljedeće ključne riječi: "digital evidence", "investigation", "blockchain technology" i "preserving digital data evidence". Na osnovu pretraga ukupno je prikupljeno, a kasnije i analizirano 37 naučnih radova. Na osnovu provedenog sistematskog pregleda literatura, odgovoreno je na postavljeno istraživačko pitanje. Autor ovog rada je u dijelu Rezultati pokušao odgovoriti na postavljeno pitanje.

Istraživačko pitanje glasi: Koje su osnovne karakteristike blockchain tehnologije koje omogućavaju i garantuju nepromjenjivost digitalnog dokaza, te očuvanje integriteta prikupljenog dokaznog materijala?

3. REZULTATI

Kako bi se ispravno razumjelo na koji način blockchain garantuje očuvanje integriteta digitalnog dokaza u istražnoj fazi, potrebno je kratko predstaviti glavne karakteristike arhitekture blockchain-a. Po definicija blockhain tehnologija je decentralizovana peer-to-peer (P2P) mrežu sa distribuiranom knjigom (eng. distributed ledger) koja je nepromjenjiva i transparentna (Atlam et al., 2024). Druga definicija tvrdi da je blockchain distribuirana baza podataka ili knjiga (eng. ledger) koja se dijeli na čvorovima računarske mreže (Atlam et al., 2024). Arhitektura blockchain-a predstavlja lanac (eng. chain) blokova (eng. block), kao što se da naslutiti iz samog imena ove tehnologije. Blok (eng. block) predstavlja u blockchain mreži jednu kariku u lancu. Lanac u blockchain tehnologiji predstavlja koncept u kojem su svi blokovi povezani jedan sa drugim na osnovu kriptografskih funkcija. Blokovi predstavljaju zapise koji imaju zadatak da skladište transakcije. Transakcije predstavljaju promjene podataka zabilježenih na blockchainu. Oni uključuju ulaze, izlaze i digitalne potpise za verifikaciju (Akter et al., 2020; Ali et al., 2024; Guo & Yu, 2022; Laroiya et al., 2020; Muyambo & Omeleze Baror, n.d.; Ricci et al., 2019; Xiao et al., 2024).

Blockchain pruža transparentnost u rukovanju i predstavljanje digitalnih dokaza. Stranke uključene u pravnom postupaku mogu provjeriti integritet i autentičnost dokaza pohranjenih na blockchainu zahvaljujući specifičnoj arhitekturi blockchain tehnologije koja omogućava očuvanje integriteta digitalnog dokaza u istražnoj fazi u digitalnoj forenzici. Blockchain tehnologija u digitalnoj forenzici, konkrento u procesu istrage (prikupljanja digitalnih dokaza) osigurava nepromjenjivost podataka. Podaci su pohranjeni u obliku blokova koji su kriptografski povezani jedan sa drugim i zaštićeni. Kada se digitalni dokaz pohrani u blok, skoro je nemoguće izmijeniti, izbrisati ili na neki drugi način uništiti dokazni materijal, a da se isto ne primijeti u kasnijim koracima. Blockchain osigurava integritet podataka pružajući kriptografski dokaz snimljenih informacija, što ga čini pogodnim za očuvanje forenzičkih dokaza. Slijedeća karakteristika koju blockchain tehnologija nudi jeste decentralizacija. Sve blockchain mreže su decentralizovane, što znači da ne postoji samo jedna tačka kontrole. Navedeno smanjuje rizik od prevara i zaloupotreba, jer su podaci raspoređeni na više lokacija, te kontrola nije isključivo na jednoj strani, te povećava sigurnost digitalnih dokaza (Efanov & Roschin, 2018; Javaid et al., 2022; Patil et al., 2021; Rao et al., n.d.; Sathyaprakasan et al., 2021; Tyagi et al., 2024). Također, u blockchain tehnologiji postoje koncenzusi (eng. Consensus). Također, decentralizacija smanjuje mogućnost manipulacija sa digitalnih dokazima, jer nije moguće jednostavno preuzeti kontrolu nad cijelim sistemom. Decentralizacija također omogućava bolju otpornost na napade, što je od izuzetne važnosti kada je riječ o sigurnosti digitalnih dokaza u forenzičkim istraživanjima. Navedeni koncenzusi predstavljaju mehanizme pomoću kojeg svi učesnici (čvorovi) u blockchain mreži potvrđuju validnost transakcija i stanja knjige (eng. ledger) podataka. Bez sistema koncenzusa, bilo koji učesnik, odnosno čvor, bi mogao pohraniti maliciozan ili pogrešan dokazni materijal. Konceznus u blockchain tehnologiji omogućava očuvanje integriteta, validnosti i zaštitu podataka podataka.

Kada je u pitanju povećana transparentnost, blockchain tehnologija omogućava uvid u kompletnu historiju transakcija što uveliko doprinosi povećanju transparentnosti i pomaže pri verifikaciji autentičnosti dokaznog materijala (AlKhanafseh & Surakhi, 2024; Almutairi & Moulahi, 2023; Ekuma & Fon, n.d.; Hamid Lone & Naaz Mir, 2017; Kim et al., 2021; Pawar et al., 2024; Tsai, 2021). Bitno je napomenuti da je blockchain tehnologija bazirana na kriptografiji, odnosno na posebnim funckijama koje se zovi heš (eng. hash) funkcije. Sve informacije unutar jednog bloka su enkriptovane heš funkcijom. Svaki heš je jedinstven za konkretne podatke, odnosno za konkretan digitalni dokaz, te svaka eventualna promjena istog rezultira u kreiranju potpuno drugačijeg hešoa. Navedno omogućava da se podaci ne mogu promijeniti, što opet upućuje na mogućnost očuvanja digitalnih dokaza.

4. DISKUSIJA

Ono što je bitno također predstaviti jeste takozvani lanac nadzora (eng. Chain of Custody (CoC)). Lanac nadzora se može opisati kao proces održavanja i dokumentovanja sekvencijala historijata rukovanja digitalnim dokazima. U digitalnoj forenzici, u različitim procesima, digitalni dokazi uglavnom prolaze kroz različite nivoe hijerarhije (istražitelj, tužitelj, sudije i ostali učesnici), što znači da digitalnim dokazima rukuje više privremenih vlasnika digitalnih dokaza. Ovaj model je fokusiran na različite vlasnike, te prati promjene vlasnika koji rukuju digitalnim podacima. Samo jedan vlasnik podataka u određenom trenutku može imati pristup digitalnih podacima (Batista et al., 2023; Bonomi et al., 2020; Hamid Lone & Naaz Mir, 2017; Khan et al., 2023; Lone & Mir, 2019; Prakash & Sadawarti, n.d.). U literaturi se model lanca nazdora preporučuje kao najefikasniji model rukovanja sa digitalnih podacima.

Primjena blockchain tehnologije u digitalnoj forenzici i dalje zahtijeva dalji razvoj i istraživanje. Iako se već primjenjuje u nekim industrijama, implementacija blockchain-a u digitalnoj forenzici nosi specifične izazove, kao što su pitanje skalabilnosti, tehničke prepreke u integraciji s postojećim sistemima, te moguće zakonske i regulatorne prepreke. Ipak, sa stalnim napretkom u ovoj oblasti, blockchain ima potencijal da postane standardizovano rješenje za upravljanje digitalnim dokazima u forenzičkim istraživanjima, što bi moglo donijeti značajne koristi u borbi protiv cyberkriminala i kriminala uopšteno (Arshad et al., 2018; Dubey et al., 2023; M. Li et al., 2021; van Beek et al., 2020).

5. ZAKLJUČAK

Dokazni materijal je temelj svakog sajber kiminala. Prilikom uviđaja i istražne faze, najbitniji procesi su prikupljane digitalnih dokaza i očuvanje digitalnih dokaza. Upotreba blockchain tehnologije u digitalnoj forenzici predstavlja značajan korak ka osiguravanju integriteta i sigurnosti digitalnih dokaza tokom istražnih procesa. Blockchain nudi ključne prednosti kao što su nepromenljivost, decentralizacija, i transparentnost, koje omogućavaju da se digitalni dokazi prikupljeni u istražnoj fazi sačuvaju u svom izvornom, neizmjenjenom stanju. Tehnička svojstva blockchain-a, kao što su kriptografska zaštita podataka, mogućnost revidiranja pristupa podacima i povećana sigurnost zahvaljujući mehanizmima konsenzusa, smanjuju rizik od manipulacije ili falsifikovanja dokaza, čime omogućavaju njihovu verifikaciju i upotrebu u sudskim postupcima. Ova tehnologija pruža dodatnu sigurnost i transparentnost, što je ključno za pravilno sprovođenje digitalnih istraga i očuvanje povjerenja u forenzičke procese. S obzirom na sve ove karakteristike, blockchain se sve više prepoznaje kao efikasno rešenje za unapređenje digitalne forenzike i postavljanje temelja za buduće inovacije u ovoj oblasti. Korišćenjem blockchain-a, svaki korak u procesu prikupljanja, čuvanja i transfera digitalnih dokaza može biti transparentno zabilježeno, čime se stvara nepobitna evidencija koja omogućava jednostavnu verifikaciju i praćenje toka dokaza. Ovaj nivo sigurnosti i transparentnosti smanjuje mogućnost grešaka ili zloupotreba, te omogućava precizno rekonstruisanje događaja i verifikaciju autentičnosti dokaza, što je od esencijalne važnosti u sudskim procesima. Takođe, upotreba blockchain-a može imati dugoročne koristi za međunarodne forenzičke saradnje, jer omogućava siguran i standardizovan pristup digitalnim dokazima bez obzira na granice i jurisdikcijske razlike. Lanac nadzora (eng. Chain of Custody) ključan za očuvanje integriteta digitalnih dokaza u procesu digitalne forenzike. Ovaj proces osigurava pravilno praćenje i dokumentovanje svakog koraka rukovanja sa digitalnim podacima, te omogućava da se podaci sačuvaju od momenta prikupljanja pa sve do njihovog prezentovanja na sudu. S obzirom na to da digitalni dokazi često prolaze kroz različite faze i različite vlasnike, važno je da se osigura transparentnost u praćenju vlasništva nad dokaznim materijalom. Korištenje modela lanca nadzora smatra se najefikasnijim načinom rukovanja digitalnim dokazima, jer minimizuje rizik od manipulacija i osigurava prihvatljivost tih dokaza u pravosudnom sistemu.

LITERATURA

Akter, O., Akther, A., Uddin, M. A., & Manowarul Islam, M. (2020). Cloud Forensics: Challenges and Blockchain Based Solutions. International Journal of Wireless and Microwave Technologies, 10(5), 1–12. https://doi.org/10.5815/ijwmt.2020.05.01

Ali, M. M., Islam, M. S., Uddin, M. N., Uddin, Md. A., & Kushal, K. S. (2024). A Blockchain-Based Digital Classified Forensic Image Preservation Framework. https://doi.org/10.22541/au.171575721.19694510/v1

AlKhanafseh, M., & Surakhi, O. (2024). A New Evidence Preservation Forensics Model Using Blockchain and Stenography Techniques. https://doi.org/10.20944/preprints202403.0703.v1

Almutairi, W., & Moulahi, T. (2023). Joining Federated Learning to Blockchain for Digital Forensics in IoT. Computers, 12(8). https://doi.org/10.3390/computers12080157

Arshad, H., Jantan, A. Bin, & Abiodun, O. I. (2018). Digital forensics: Review of issues in scientific validation of digital evidence. Journal of Information Processing Systems, 14(2), 346–376. https://doi.org/10.3745/JIPS.03.0095

Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. In Electronics (Switzerland) (Vol. 13, Issue 17). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/electronics13173568

Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., Silva, G. M., & Miranda, F. P. de. (2023). Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. In Journal of Risk and Financial Management (Vol. 16, Issue 8). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/jrfm16080360

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

Carrier, B., & Spafford, E. (n.d.). DIGITAL FORENSIC RESEARCH CONFERENCE An Event-Based Digital Forensic Investigation Framework.

Degree Project Bachelor's An Analysis of Using Blockchains for Processing and Storing Digital Evidence. (n.d.).

Dubey, H., Bhatt, S., & Negi, L. (2023). Digital Forensics Techniques and Trends: A Review. International Arab Journal of Information Technology, 20(4), 644–654. https://doi.org/10.34028/iajit/20/4/11

Efanov, D., & Roschin, P. (2018). The all-pervasiveness of the blockchain technology. Procedia Computer Science, 123, 116–121. https://doi.org/10.1016/j.procs.2018.01.019

Ekuma, N., & Fon, Y. (n.d.). Blockchain Technology for Secure and Transparent Evidence Management in Criminal Investigations.

Guo, H., & Yu, X. (2022). A survey on blockchain technology and its security. Blockchain: Research and Applications, 3(2). https://doi.org/10.1016/j.bcra.2022.100067

Hamid Lone, A., & Naaz Mir, R. (2017). FORENSIC-CHAIN: ETHEREUM BLOCKCHAIN BASED DIGITAL FORENSICS CHAIN OF CUSTODY. In Scientific and Practical Cyber Security Journal (SPCSJ) (Vol. 1, Issue 2).

Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. In BenchCouncil Transactions on Benchmarks, Standards and Evaluations (Vol. 2, Issue 3). Elsevier B.V. https://doi.org/10.1016/j.tbench.2022.100073

Kebande, V. R., Karie, N. M., Michael, A., Malapane, S., Kigwana, I., Venter, H. S., & Wario, R. D. (2018). Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. Proceedings - 2018 IEEE International Conference on Smart Internet of Things, SmartIoT 2018, 93–98. https://doi.org/10.1109/SmartIoT.2018.00-19

Khan, A. A., Shaikh, A. A., & Laghari, A. A. (2023). IoT with Multimedia Investigation: A Secure Process of Digital Forensics Chain-of-Custody using Blockchain Hyperledger Sawtooth. Arabian Journal for Science and Engineering, 48(8), 10173–10188. https://doi.org/10.1007/s13369-022-07555-1

Kim, D., Ihm, S. Y., & Son, Y. (2021). Two-level blockchain system for digital crime evidence management. Sensors, 21(9). https://doi.org/10.3390/s21093051

Laroiya, C., Saxena, D., & Komalavalli, C. (2020). Applications of Blockchain Technology. In Handbook of Research on Blockchain Technology (pp. 213–243). Elsevier. https://doi.org/10.1016/B978-0-12-819816-2.00009-5

Li, M., Lal, C., Conti, M., & Hu, D. (2021). LEChain: A blockchain-based lawful evidence management scheme for digital forensics. Future Generation Computer Systems, 115, 406–420. https://doi.org/10.1016/j.future.2020.09.038

Li, S., Qin, T., & Min, G. (2019). Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems. IEEE Transactions on Computational Social Systems, 6(6), 1433–1441. https://doi.org/10.1109/TCSS.2019.2927431

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

Mahrous, W. A., Farouk, M., & Darwish, S. M. (2021). An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash. IEEE Access, 9, 151327–151336. https://doi.org/10.1109/ACCESS.2021.3126715

Mohammed, K. H., Mohammed, Y. D., & Solanke, A. A. (2019). Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. The International Journal of Cybersecurity Intelligence and Cybercrime, 2(1), 56–63. https://doi.org/10.52306/02010519zjrk2912

Muyambo, E., & Omeleze Baror, S. (n.d.). Systematic Review to Propose a Blockchain-Based Digital Forensic Ready Internet Voting System.

Patil, S., Kadam, S., & Katti, J. (2021). Security enhancement of forensic evidences using blockchain. Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021, 263–268. https://doi.org/10.1109/ICICV50876.2021.9388486

Pawar, P. P., Kumar, D., Bhujang, R. K., Pareek, P. K., Manoj, H. M., & Deepika, K. S. (2024). Investigation on Digital Forensic Using Graph Based Neural Network with Blockchain Technology. 2nd IEEE International Conference on Data Science and Network Security, ICDSNS 2024. https://doi.org/10.1109/ICDSNS62112.2024.10691122

Prakash, F., & Sadawarti, H. (n.d.). Blockchain-Based Chain Of Custody: A Secure Digital Evidence Framework For Digital Forensics Investigation.

Rao, S., Syed, S., Fernandes, S., & Raorane, S. (n.d.). A Novel Approach for Digital Evidence Management using Blockchain. https://ssrn.com/abstract=3683280

Ricci, J., Baggili, I., & Breitinger, F. (2019). Blockchain-Based Distributed Cloud Storage Digital Forensics: Where's the Beef? IEEE Security and Privacy, 17(1), 34–42. https://doi.org/10.1109/MSEC.2018.2875877

Sathyaprakasan, R., Govindan, P., Alvi, S., Sadath, L., Philip, S., & Singh, N. (2021). An Implementation of Blockchain Technology in Forensic Evidence Management. Proceedings of 2nd IEEE International Conference on Computational Intelligence and Knowledge Economy, ICCIKE 2021, 208–212. https://doi.org/10.1109/ICCIKE51210.2021.9410791

Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. Information Sciences, 491, 151–165. https://doi.org/10.1016/j.ins.2019.04.011

Tsai, F. C. (2021). The application of blockchain of custody in criminal investigation process. Procedia Computer Science, 192, 2779–2788. https://doi.org/10.1016/j.procs.2021.09.048

Tyagi, A. K., Balogun, B. F., & Tiwari, S. (2024). Role of blockchain in digital forensics: A systematic study. In Global Perspectives on the Applications of Computer Vision in Cybersecurity (pp. 197–222). IGI Global. https://doi.org/10.4018/978-1-6684-8127-1.ch008

van Beek, H. M. A., van den Bos, J., Boztas, A., van Eijk, E. J., Schramp, R., & Ugen, M. (2020). Digital forensics as a service: Stepping up the game. In Forensic Science International: Digital Investigation (Vol. 35). Elsevier Ltd. https://doi.org/10.1016/j.fsidi.2020.301021

Xiao, N., Wang, Z., Sun, X., & Miao, J. (2024). A novel blockchain-based digital forensics framework for preserving evidence and enabling investigation in industrial Internet of Things. Alexandria Engineering Journal, 86, 631–643. https://doi.org/10.1016/j.aej.2023.12.021