DFRWS

Edinburgh Napier UNIVERSITY
School of Computing, Engineering & the Built Environment

A Bibliometric Analysis and Review of a Blockchain-based Chain of Custody for Digital Evidence Management.

Belinda I Onyeashie, Petra Leimich, Sean McKeown & Gordon Russell.

Abstract

The use of blockchain technology in the management of digital evidence has gained significant attention in recent years due to its potential to increase the security, integrity, and transparency of digital evidence. This study presents a review and a bibliometric analysis of blockchain and digital evidence to illustrate the research trends and the promising opportunities for a blockchain-based chain of custody.

The results suggest that research on blockchain-based chain of custody for digital evidence management has grown rapidly in recent years, with a significant increase in the number of publications since 2018. The reviewed literature demonstrates that blockchain-based systems have the potential to improve the reliability and transparency of digital evidence management. This bibliometric analysis and literature review provides valuable insights into the current state and future directions of research in this rapidly evolving field, indicating promising opportunities for the application of blockchain technology in the management of digital evidence.

1. Introduction and Bibliometric Network

- To address the research question "What is the current knowledge on blockchain-based chain of custody for digital evidence management?", this study presents a bibliometric analysis of the research landscape, highlighting the key contributors, journals, and trends in the field.
- The analysis is used to establish the current gaps, and future research direction which may inform a development of a blockchain based evidence management system that will encompass the entire lifecycle of evidence from acquisition to storage.

The scientific databases and search engines Scopus, Web of Science, and Google Scholar were searched from 2015.

↓

104,324 articles were found (Table 1) and duplicates removed.

↓

The remaining 10,134 distinct articles were evaluated for title-based relevance.

Table 1: *The number of articles based on search terms found in each database.*

Keyword	Google Scholar	Scopus	Web of Science
Blockchain-based	30,700	8,865	11,528
Blockchain and Digital Forensic	7,740	205	132
Blockchain and Digital Evidence	28,200	344	337
Blockchain Chain of Custody	6,730	78	107
Blockchain Chain of Custody Evidence	4,760	34	29
Blockchain Chain of Custody Digital Evidence	4,480	118	24
Total number of Articles	82,610	9,664	12,157

2. Analysis of results

- The unique results for the search term "Blockchain and Digital Evidence Chain of Custody" were broken down by publication year (Figure 1), country of publication (Figure 2) and document type- (Figure 3).

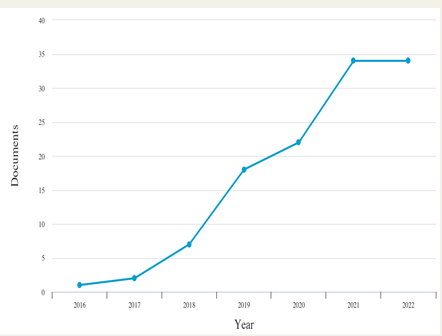

Figure 1: Article Publication year.

Publication Year

The first article addressing the use of blockchain in digital evidence chain of custody was published in 2016. The number of such publications has progressively increased since then, reaching a peak in 2021 with a total of thirty-four articles. The total number of articles published since 2016 is 118.

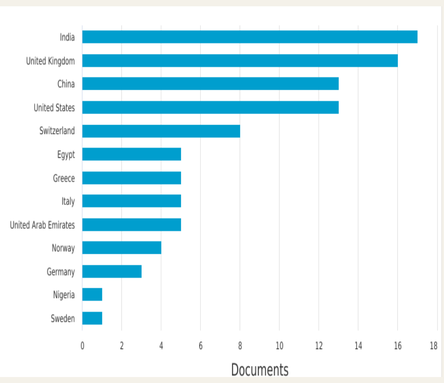

Figure 2: Article publication by country.

Country of Publication:

The paper counts from the Scopus dataset are displayed in Figure 4. The diversity of the countries represented demonstrates that blockchain-based chain of custody is an emerging, promising topic that is garnering interest from researchers all over the world.

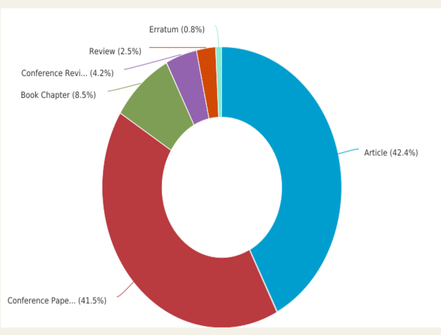

Figure 3: Publications by type.

Publications by Type:

There have been one hundred and eighteen documents published for blockchain and digital evidence chain of custody since 2016 and as evident in figure 1, the numbers will continue to grow exponentially. .

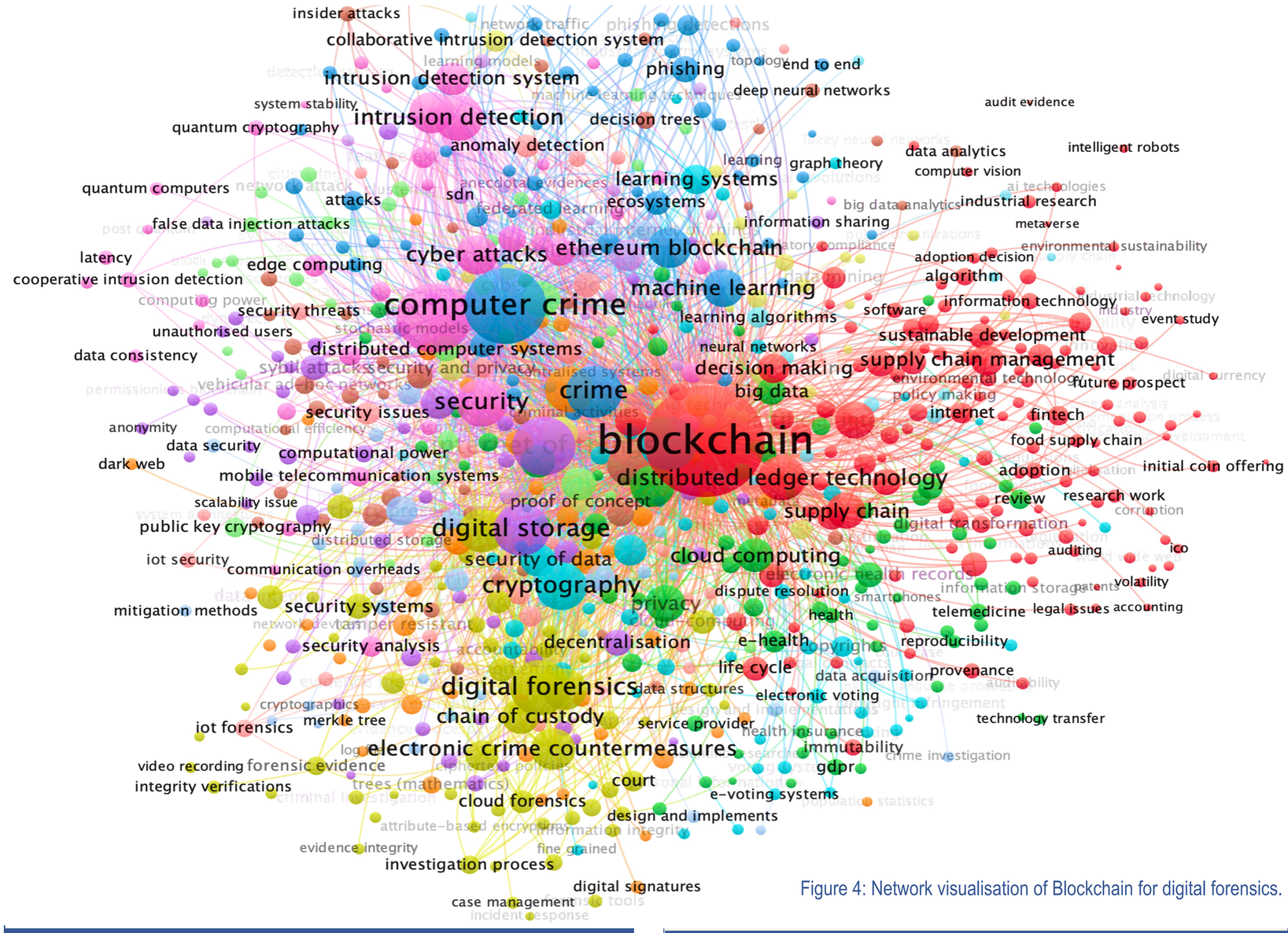

Figure 4: Network visualisation of Blockchain for digital forensics.

3. Analysis of Blockchain and Digital Forensic Bibliometric Network

- Fig 4 shows the visual representation of contents' co-occurrence networks.
- Each cluster of highly related keywords is represented by a different colour. Each circle signifies a different keyword. The greater the size of a circle, the greater the number of articles that include the matching term in their keywords. Keywords that appear together frequently are clustered in close proximity.
- The keywords were categorised, and the size of the group including the word "Blockchain" was exceptionally large. It belonged to cluster 1, had a total of 752 links, and a total link strength of 7,179. This highlights that blockchain is linked to all keywords analysed in the digital forensic, evidence management, chain of custody papers analysed.

4. Review of Literature

Many researchers have incorporated blockchain technology with the chain of custody or evidence life cycle to improve the management process.

This has established that Blockchain, a distributed, tamper-resistant ledger, can be leveraged to provide a decentralised secure digital evidence system.

- Bonomi et al. (2018) propose a Blockchain based chain of custody based on Ethereum to dematerialize the chain of custody process and ensure auditable evidence integrity and owner traceability.
- Lone and Mir (2018, 2019) propose a blockchain-based system (Forensic-chain) designed to bring integrity and tamper-resistance to the digital forensics chain of custody. This is followed by a proof-of-concept (PoC) implementation of Forensic-chain using Hyperledger Composer.
- Xiong and Du (2019) propose a blockchain-based electronic evidence preservation model to ensure the integrity of data. Their model aims to address the data security and trust issues associated with the storage of electronic evidence in a centralised database.
- Tian et al. (2109) proposes "Block-DEF" a secure chain of custody framework using blockchain technology to store evidence metadata while the evidence is stored in a reliable storage medium and integrated with the digital evidence system where it is physically stored and locked with smart locks.
- Burri et al. (2020) present a chain of custody system for timestamping digital evidence hash values using a blockchain-based electronic chain of custody system. A public blockchain ledger is used to verify the integrity of the secure ledger.
- Jaquet-Chiffelle et al. (2020) build on and extend prior work to trace the provenance of digital data using a blockchain-based registry. This work provides a tamper-proof, time-stamped provenance ledger using a public, pre-existing, trusted blockchain.
- Yan (2020) presents a protocol for digital evidence chain of custody based on revocable ciphertext-policy attribute-based encryption, Boneh-Lynn-Shacham (BLS) signature, and blockchain technology to manage evidence privacy and traceability.
- Li et al. (2021) propose digital witnesses and a blockchain-based lawful evidence management scheme called "LEChain" to manage the entire chain of evidence in digital forensics with transparency and verifiability. They use short randomizable signatures to authenticate witnesses' identities anonymously.

5 : Research Gap

Blockchain-based chains of custody for digital evidence management are still in their preliminary stages with gaps and room for future work:

- Most proposed works are theoretical rather than experimental.
- User acceptance and adoption can be improved by understanding and researching how different stakeholders such as investigators, forensic analysts, and lawyers, perceive and use these systems.
- The legal and regulatory framework for using blockchain for tracking the chain of custody of digital evidence lacks clarity and there is no standardized framework.
- Scalability and performance issues with blockchain-based systems for digital evidence management have been identified in literature and more research is needed to understand these limitations and potential solutions.
- A chain of custody system should cover the entire lifecycle of evidence, from acquisition to storage, but many blockchain based chain of custody-evidence management papers have inconsistent methods for storing digital evidence.

6. Conclusion

This study presents a bibliometric analysis and review of literature, highlighting the application of blockchain technology for digital evidence management.

- Growing interest in this area is reflected in an increase in publications since 2016.
- Additional research is needed to investigate its applicability, effectiveness, and interoperability with existing technologies.
- Future research opportunities include more experimental studies, understanding user acceptance, addressing legal and regulatory frameworks, and scalability and performance issues.
- A standardised framework covering the entire lifecycle of a blockchain-based evidence management system is necessary for effective implementation.
- Further research is required to investigate storage architectures that can scale effectively with the blockchain in order to store evidence and interoperate with the evidence meta data recorded on the blockchain.
- This study provide insights for future researchers and practitioners to advance the development and application of a blockchain-based chain of custody in digital evidence management.

References

Acknowledgement

The authors wish to express their gratitude to the Edinburgh Napier SCE group and the organisers of the Women in Forensic Computing Workshop 2023 for their support.

belinda.onyeashie@napier.ac.uk