sustainability

MDPI

Article

Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution

Md Hasibul Alam Ratul, Sepideh Mollajafari and Martin Wynn *

School of Business, Computing and Social Sciences, University of Gloucestershire, Cheltenham GL50 2RH, UK; hasib.ratul08@gmail.com (M.H.A.R.); smollajafari2@glos.ac.uk (S.M.)
* Correspondence: mwynn@glos.ac.uk

Abstract: Digital evidence plays a crucial role in cybercrime investigations by linking individuals to criminal activities. Data collection, preservation, and analysis can benefit from emerging technologies like blockchain to provide a secure, distributed ledger for managing digital evidence. This study proposes a blockchain-based solution for managing digital evidence in cybercrime cases in the judicial domain. The proposed solution provides the basis for the development of a new model that leverages a consortium blockchain, allowing secure collaboration among judicial stakeholders, while ensuring data integrity and admissibility in court. An extensive literature review demonstrates blockchain's potential to create a more secure, efficient evidence management system. The proposed model was implemented in a test environment using a localised blockchain for developing and testing smart contracts, as well as integrating a web interface, with off-chain storage for managing evidence data. The system was subsequently deployed in both the Polygon and Ethereum test networks, simulating real-world blockchain environments, revealing that the operational cost in the Polygon network is reduced by 99.96% compared to Ethereum, thereby offering scalability without compromising security. This study underscores blockchain's potential to revolutionise the chain of custody procedures, improving dependability and security in evidence management and providing more sustainable solutions within the criminal justice system.

Keywords: blockchain; chain of custody; data integrity; sustainability; secure distribution; access control

Citation: Ratul, M.H.A.; Mollajafari, S.; Wynn, M. Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution. *Sustainability* **2024**, *16*, 10885. https://doi.org/10.3390/su162410885

Academic Editor: Yang (Jack) Lu

Received: 7 November 2024
Revised: 1 December 2024
Accepted: 9 December 2024
Published: 12 December 2024

1. Introduction

The blockchain concept dates back to 2008, and in 2009, Bitcoin became the first decentralised cryptocurrency using blockchain technology. In recent years, the technology has received a great deal of attention from industry and academia because of its apparent benefits of decentralisation of control, reliability and consistency of data and transactions, immutability, and anonymity [1]. The first generation of blockchain, based on Bitcoin, was largely restricted to simple currency transactions, but Ethereum, an open and decentralised platform, was subsequently introduced in a second generation of the technology and enables users to develop smart contracts [2], enabling mutually distrusted users to complete data exchange, or transactions, without the need of intermediaries [3].

The potential benefits of blockchain are of particular relevance to the storage, analysis, and retrieval of digital evidence due to the rise in cybercrime, necessitating robust security throughout the forensic investigation lifecycle [4]. Digital evidence plays a pivotal role in criminal proceedings, enabling thorough analysis and supporting investigations, and ensuring the privacy, integrity, and equitable distribution of evidence, which is essential for fairness within the criminal justice system. Traditional chain of custody (CoC) methods chronologically record evidence from collection through storage, handling, and distribution, preserving its integrity and ensuring it remains uncontaminated for court proceedings [5]. However, digital evidence storage presents new risks, such as inadequate data encryption, viable storage solutions, access control, and data ownership.

There is much debate concerning the respective environmental costs and benefits of blockchain. PWC [6], in developing an assessment framework to evaluate the environmental footprint of blockchain deployment, recently concluded that "blockchain has significant potential to support sustainability, and it may prove to be a valuable tool to help companies advance environmental aspects of their ESG [Environmental, Social and Governance] goals" (para. 8). This is of significance in the context of the broader research agenda pursued by others to establish how digital technologies can support the transition to sustainability [7] and the circular economy [8]. More specifically, Mulligan et al. [9] (para. 1), in their recent review of the sustainability applications of blockchain, found that "blockchain technology has been proposed to achieve sustainable development through various solutions, such as carbon credit trading, energy systems and supply chain management", but the authors highlight the absence of parallel research in other functions and disciplines. Blockchain's immutability ensures that once data are recorded, they cannot be altered without consensus from the majority of the network, thereby safeguarding data integrity [10]. By leveraging a distributed ledger, blockchain minimises single-point failure risks, enabling comprehensive tracking and verification of evidence transactions through network-wide consensus [11].

This article surveys existing digital CoC solutions, identifying key elements that ensure process integrity. A CoC can be defined as "a process that tracks the movement of evidence through its collection, safeguarding, and analysis lifecycle by documenting each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer" [12] (para. 1). The CoC is of particular significance in criminal cases where the evidence presented in court must be proven to be the same as the evidence found and recorded at the crime scene. A CoC can verify that the evidence was handled properly and not tampered with. The objective here is to present a holistic approach to the digital CoC that guarantees evidence integrity, privacy, admissibility, distribution, and scalability. Ensuring the integrity and admissibility of digital evidence is crucial in this data-driven context. Blockchain's distributed ledger provides strong tracking and verification of transactions and events related to evidence, addressing current weaknesses in the digital CoC. More specifically, this article addresses the following research objectives (ROs):

- RO1: To investigate existing approaches to digital evidence management and assess blockchain's potential to create a more secure and efficient evidence management system.
- RO2: To develop and test a new application model based on blockchain technology that facilitates data integrity and admissibility and the security of digital evidence in the CoC.
- RO3: To evaluate the security and performance aspects of the developed blockchain-based application for managing digital evidence.

In addressing these objectives, this paper contributes to the exiting research literature in several regards. The judicial system's management of digital evidence faces a number of current challenges, and these are set out, and the potential of blockchain in resolving these issues is assessed. More specifically, the proposed solution illustrates how blockchain can be used effectively in the context of criminal justice evidence, highlighting the necessity for, and value of, enhanced encryption algorithms. It provides a worked case example that may be built upon and further developed by other researchers.

Following this brief Introduction section, Section 2 then addresses RO1 by reviewing the existing work related to the CoC, covering both the traditional methods and those that are based on blockchain technology. Section 3 presents the research methodology adopted for this work, being based on a systematic literature review, followed by the development and testing of a blockchain-based model application. Section 4 reports the results, addressing ROs 2 and 3. The proposed solution is outlined, which ensures evidence integrity through data encryption, followed by storage within the blockchain. A comparison of implementing the solution on current blockchain-based networks (Ethereum and Polygon) is then presented and analysed. In Section 5, the results are further reviewed, and some emergent themes are discussed in the context of the existing research literature.

Finally, the concluding Section 6 summarises the contribution of this study, outlines its limitations, and points out some possible future research initiatives in this field of study.

2. Literature Review

This section explores the relevant literature and provides a backdrop to the main research activity. The initial overview sub-section sets out some of the key contextual issues, including particular aspects and challenges related to digital evidence management. The following sub-section then examines the traditional methods of managing digital evidence to ensure integrity and credibility. Sections 2.3 and 2.4 then focus on blockchain-based solutions, first examining the sustainability benefits of blockchain, and then looking in more detail at specific blockchain-based solutions.

2.1. Overview

This review explores the literature related to digital evidence integrity, admissibility, accessibility, processing speed, and timing within the CoC, focusing on factors affecting its performance. The current methods and the limitations of existing approaches to digital evidence preservation and management are highlighted. While the fundamental concept of evidence management applies to both traditional and digital contexts, the unique nature of digital evidence necessitates distinct applications in the digital CoC, especially regarding evidence modification [13]. This underscores the need for a secure system to implement a digital CoC for evidence handling and access by law enforcement during investigations.

The digital evidence lifecycle is crucial in forensic investigations, ensuring accessibility to evidence for all parties involved, including investigators and witnesses [14]. The conventional CoC method records the chronological handling of evidence, ensuring its integrity and admissibility in legal proceedings by establishing a verifiable record of those who have controlled the evidence. Additionally, to ensure admissibility, there are certain standards and best practices that should be followed. Ćosić et al. [15] proposed using file fingerprints, biometrics, timestamps, GPS, reasons, and procedures to address the who, what, when, where, why, and how aspects of digital evidence, forming a comprehensive and chronological representation in the CoC.

Data privacy and protection is clearly of utmost importance in this domain. If evidence is manipulated or fabricated, it may lead to wrongful convictions, and defence lawyers could maintain that such evidence is irrelevant or unlawful. This has produced several initiatives to use new technologies to help improve data privacy in the criminal justice system. Choenni et al. [16], for example, in their research on preserving privacy whilst integrating data in the criminal justice system, maintained that "privacy preserving data integration is of crucial importance", and put forward "an approach for data reconciliation that is based on available schemata of data sources and the content of the sources" (p. 125), which they then applied to a real-life case in the field of police and justice. Ironically, however, more recent digital technologies may exacerbate this problem. As Wexler [17] (p. 212) noted in her research on access to data in criminal defence investigations in the US, "the introduction of artificial intelligence and machine learning tools into the criminal justice system will exacerbate the consequences of law enforcement's and defence counsel's disparate access to data". This only serves to underline the potential of blockchain applications in improving data security and privacy in the criminal justice arena.

Although the CoC process is fundamentally the same for evidence management, it presents unique challenges when dealing with digital evidence. Maintaining data integrity is particularly challenging, as it can be easily altered, unlike physical evidence, which allows for easier control and monitoring of changes [18]. Another core challenge is access control, since different entities access the evidence during the entire duration, from evidence collection to submission to court [5]. While centralisation of storage makes it easier to access and collect data for forensic purposes, centralisation also opens the avenue of single-point failure and will be susceptible to cyber attacks [19]. Without addressing the challenges of the traditional digital CoC, the credibility of evidence cannot be proven and could

be inadmissible in court. The following sub-sections discuss the existing approaches to address these challenges.

2.2. Current Methods Without Using Blockchain

Researchers have suggested various methods for maintaining evidence integrity and credibility. Saleem et al. [20] implemented the SHA-512 algorithm, which enhances security and integrity. However, there is a possibility of the original data being altered, with the hash being recalculated and replaced, thus compromising data security and the integrity of the evidence. Syed et al. [21] proposed automated tools, like Encase and FTK Imager, for disk imaging, while utilising smart cards to store private keys and generate digital signatures, improving data security and integrity. Similarly, Banwani and Kalra [22] suggested integrating FTK Imager with GPS chips with an MD5 hash value to track evidence from collection to court. However, MD5 hash alone may not sufficiently prove data integrity. In other instances, Ûosiü and Baþa [23] proposed using a third-party timestamp for evidence traceability to validate staff access. This method relies on a consistent time source, so any accidental clock changes could disrupt the process. Ruj and Nayak [24] proposed a decentralised security framework for smart grids that combines data aggregation with access control using homomorphic encryption and attribute-based encryption (ABE). Their framework distributes trust across multiple key distribution centres (KDCs) to avoid single points of failure. Similarly, Buccafurri et al. [25] introduced a decentralised framework using self-sovereign identity (SSI) and verifiable credentials for authentication systems. Their approach also aims to eliminate centralised trust by allowing systems to maintain autonomous security policies while establishing secure dependencies.

In forensic medicine, the RAW image format provides significant benefits for data security and quality when documenting photographic evidence. According to D'Anna et al. [19] (p. 5), "manipulation, understood as tampering, of a RAW image is extremely difficult". However, it presents operational challenges, including substantial storage requirements and cross-platform compatibility issues, which limit its applicability in the context of this research. Romli et al. [26] suggested using a storage area network (SAN) for flexible and accessible digital evidence storage. However, compromised credentials can threaten evidence integrity. Other studies propose digital evidence cabinets with security measures like hash functions, metadata, biometric authentication, and GPS validation. For instance, Ćosić and Bača's [27] framework integrates SHA-2 hash functions, biometric authentication, and GPS validation. However, asymmetric encryption may slow down the CoC process, particularly with larger evidence volumes. Prayudi et al. [18] proposed a digital evidence cabinet framework to enhance evidence availability, integrity, and credibility, noting the importance of metadata, recording methods, and access control.

2.3. The Sustainability Aspects of Blockchain Technology

Blockchain is a decentralised distributed ledger that works on a peer-to-peer network. Consensus algorithms are used to ensure an agreement is reached among nodes regarding the validity of newly generated blocks [28]. Initially, the use of a proof of work (PoW) consensus algorithm became popular due to its use in Bitcoin. Nevertheless, Gervais et al. [29] pointed out that the power consumption and throughput of the PoW algorithm are challenges to the cost, energy consumption, and long-term sustainability of the system. The Ethereum blockchain network moved to proof of stake (PoS) in 2022, which offers a more energy-efficient algorithm with faster consensus and block creation [28]. Moreover, Liu et al. [30] suggested that delegated proof of stake (DPoS) offers more decentralisation, lower energy consumption, and faster confirmation speed. Nevertheless, Manolache et al. [31] suggested that proof of authority (PoA) has the edge over the standard PoS, as it enables block creators to be easily identified, increases accountability, and is also computationally cheaper and more sustainable. Furthermore, Wu et al. [32] proposed a concurrent PoA approach to double the throughput and achieved a 500% reduction in latency when compared to the original PoA. Additionally, Bamakan et al. [33] added that

in a private or consortium blockchain setting, PoA provides more security and integrity of the data, as each validator is predefined, meaning identities are known and trusted. Liu et al. [34] also emphasised the importance of performance metrics, such as transaction speed, in influencing cost efficiency.

Smart contracts are an important component of blockchain. These are self-executing contracts with the terms of the agreement directly written into code [35]. Smart contracts use gas units for tasks. In this context, the term "gas" is used for the fee that is required to successfully conduct a transaction or execute a contract on the blockchain network and is priced in cryptocurrency fractions. Gas is thus used to pay validators for the resources needed to conduct transactions, and amounts fluctuate depending on how operations are conducted [36]. Smart contracts play a pivotal role in upholding data integrity across multiple network nodes. Their functionality encompasses the mitigation of human errors, preservation of privacy, assurance of data reliability, facilitation of traceability, and facilitation of data distribution within the network infrastructure [37]. Another central element in blockchain is cryptography, which ensures secure transactions, authenticates users, links blocks using hash functions, and encrypts data, forming the backbone of security and data integrity in decentralised networks [38]. It safeguards the integrity, confidentiality, and authenticity of information within the decentralised blockchain system. Different types of blockchains are available, such as public, private, and consortium-based, each with their own advantages and disadvantages. For the purpose of this research, a consortium blockchain is proposed. A consortium provides multi-organisational management and data sharing among all the stakeholders, such as law enforcement agencies, forensics laboratories, and the judiciary.

2.4. Blockchain-Based Methods

The existing literature explores various approaches integrating Ethereum into CoC frame works, such as the digital evidence cabinet and digital evidence bag. These approaches differ in focus and methodology, utilising smart contracts for data authentication and authorisation [39,40]. Others employ MAC address verification, predefined access control, and the sharing of unique secret keys and digital signatures [39,41,42]. Role-based access control (RBAC) is commonly implemented across these studies to categorise users into roles with distinct permission levels. Conversely, some innovations include smart locks using Keccak-256 hashed values of IP addresses, evidence names, and contents, alongside private key sharing for evidence access authorisation [39].

Table 1 provides a comparative analysis of blockchain-based CoC solutions, encompassing factors such as data storage methods, features (data integrity, storage, access control), and consensus algorithms. As an example, Li et al. [41] proposed LEChain for managing digital forensic evidence, prioritising witness privacy with short, randomised signatures and employing attribute-based encryption for fine-grained access control, while ensuring juror privacy through secure voting mechanisms. Similarly, Elgohary et al. [42] introduced a blockchain-based paradigm integrating fuzzy hash functions for digital evidence integrity within Hyperledger Composer. Their prototype demonstrates effective CoC management in real-world scenarios, achieving a 54% reduction in pairwise comparison time and 30% faster response compared to conventional hash functions. On the other hand, Bonomi et al. [43] presented B-CoC, a blockchain-based chain of custody using Ethereum private network, focusing on evidence integrity through a hybrid architecture combining traditional databases with blockchain. Their solution addresses dematerialization of the CoC process by guaranteeing auditable integrity of collected evidence and owner traceability, though it faces limitations with fixed validator sets and privacy compromises during consensus.

Table 1. Comparison of blockchain-based chain of custody solutions.

Platform	BC Types	Cons	Access Control		Storage	Features			Authors
			Authentication	Authorisation		DI	DS	AC	
Ethereum	Private	Proof of Authority	N/A	SC	On Chain	*	*	*	[44]
Ethereum	Private	Proof of Validation	SC	SC	Off Chain	*	*	*	[39]
Ethereum	Private	Proof of Authority	SC	SC	Off Chain	*			[43]
HyperLedger Fabric	Public	N/A	N/A	SC	On Chain	*	*		[45]
Ethereum	Public	Proof of Work	SC	SC	Off Chain	*	*	*	[40]
Ethereum	Public	Proof of Work	Unique secret key, access policy	SC	Off Chain	*	*	*	[46]
Ethereum	Private	Proof of Work	MAC address verification	SC	On Chain	*		*	[47]
HyperLedger Fabric	Private	N/A	Access control script	SC	Off Chain	*	*	*	[48]
Ethereum	Consortium	Proof of Authority	Anonymous authentication, digital signature	SC	Off Chain	*	*	*	[41]
HyperLedger Fabric	Consortium	N/A	SC	SC	Off Chain	*	*	*	[4]
Polygon	Public	N/A	SC	SC	Off Chain	*	*	*	[49]
Polygon	Consortium	Proof of Authority	SC	SC	Off Chain	*	*	*	Proposed

Key: BT—blockchain type; Cons—consensus algorithm; SC—smart contract; DI—data integrity; DS—data storage; AC—access control; *— features are present.

Ethereum is frequently utilised as the platform for many current research initiatives (Table 1), despite its inherent drawbacks in performance and scalability as a layer 1 blockchain solution. Layer 1 serves as the foundational platform for blockchain operations, encompassing smart contracts, consensus algorithms, decentralised applications (DApps), and decentralised protocols [50]. Issues like high transaction fees and slow confirmation times have prompted exploration into Polygon, a layer 2 scaling solution integrated with Ethereum [51]. Layer 2 solutions maintain security akin to Ethereum, while enhancing performance and scalability through off-chain methodologies [52].

Rana et al. [49] developed a blockchain solution utilising layer 2 Polygon, emphasising benefits such as improved auditability, reduced dependence on centralisation, enhanced data security, and scalability. Polygon Hermez, a component of the Polygon eco-system, supports 2000 transactions per second and reduces gas fees by 90% compared to Ethereum, significantly lowering operational costs [53]. Diaconita et al. [54] highlighted Polygon's superior speed in B2C applications compared to Ethereum, further supporting its adoption in practical implementations.

Although many blockchain solutions rely on Ethereum, some also recommend Polygon to minimise scalability issues, but limited research on Polygon impedes thorough evaluation of these solutions. Additionally, a few solutions opt for centralised CoC approaches, posing risks such as single-point failure and dependency on a sole trusted entity. Furthermore, some research studies lack adequate information regarding the employed consensus algorithm, a pivotal factor impacting the overall process and the associated gas fees, as various consensus algorithms have differing permission structures that directly impact blockchain security and data integrity. These factors collectively shape the challenges and constraints of integrating blockchain within the digital CoC domain. To address these

challenges, the proposed solution leverages Polygon's layer 2 scaling capabilities with a proof of authority (PoA) consensus mechanism and an off-chain storage solution. This approach aims to resolve scalability concerns while maintaining robust security. Implementing the solution within a consortium blockchain environment mitigates the risks from centralised architectures while ensuring both data integrity and legal admissibility of the digital evidence.

In summary, the literature review addresses RO1 and reveals significant limitations in current blockchain solutions for digital evidence management. However, it also highlights substantial opportunities for improvement. By addressing these identified issues, there is great potential to develop more secure, efficient, and robust digital evidence management systems leveraging blockchain technology.

3. Research Method

There were three phases to this research project, oriented around the research objectives (Figure 1), each adopting different methods. In Phase 1, a literature review was conducted to explore blockchain technology's role in ensuring the integrity, admissibility, distribution, and scalability of digital evidence throughout the CoC. A literature review can develop a thorough understanding of the current state of knowledge within a specific field and identify gaps in the existing literature. This is reiterated by Hart [55], who observed that "the literature review serves to position the research within the existing body of knowledge, making it possible to highlight areas where further investigation is necessary and to construct a solid foundation for the research framework". Fink [56] similarly made the point that a well-conducted literature review can allow the validity and relevance of prior studies to be assessed, and the findings can support subsequent stages in the research process.

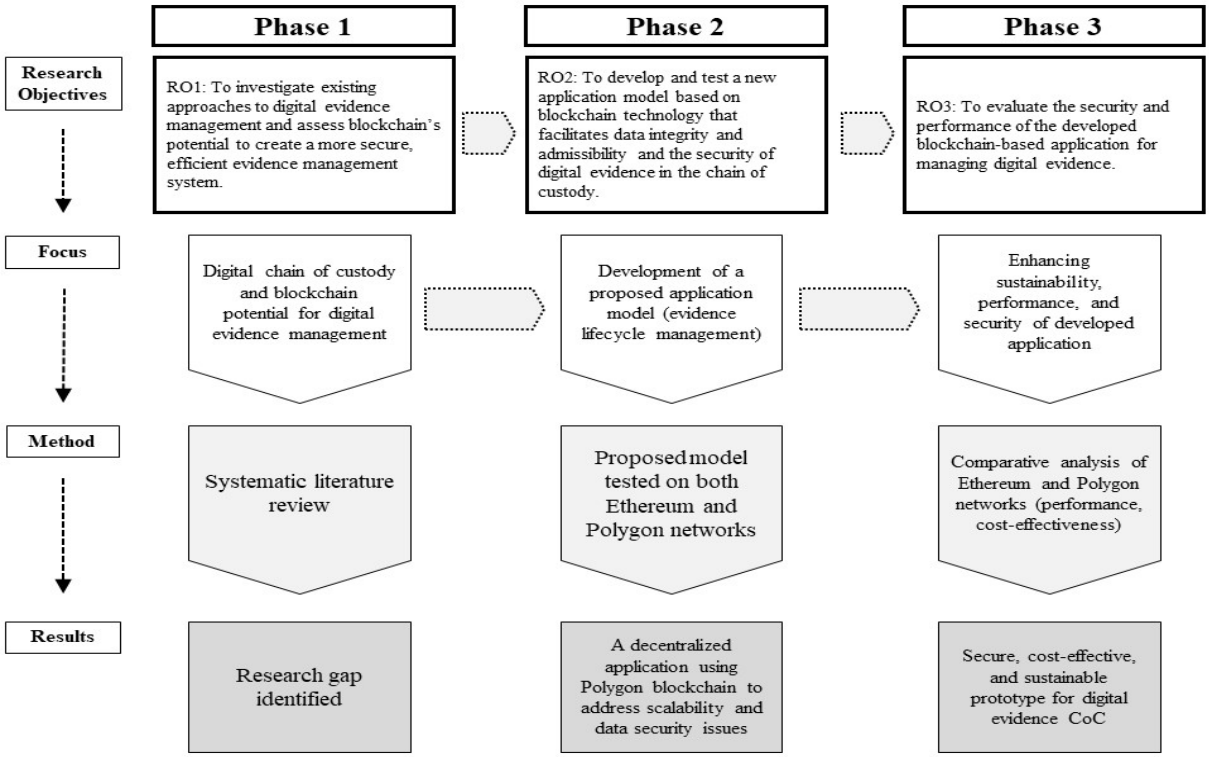

Figure 1. The three phases in the research project.

There are various approaches to conducting a literature review, each with its own strengths and limitations. Here, a systematic literature review (SLR) was undertaken. Such reviews are highly structured, allow reproducibility, and minimise the potential for

researcher bias [57]. Greenhalgh et al. [58] noted that "systematic reviews are generally placed above narrative reviews in an assumed hierarchy of secondary research evidence," and that their advantages are in the transparent and methodical manner in which literature can be found and analysed. As Kitchenham et al. [59] (p. vi) noted, "a systematic review is a means of evaluating and interpreting all available research relevant to a particular research question, topic area, or phenomenon of interest. Systematic reviews aim to present a fair evaluation of a research topic by using a trustworthy, rigorous, and auditable methodology". The Preferred Reporting Items for Systematic reviews and Meta-Analyses (PRISMA) protocol [60] was used to provide an overarching framework for the review (Figure 2). The steps in the PRISMA protocol help determine the search strings, the inclusion and exclusion criteria, executing the search string, selecting articles, extracting data from the articles, synthesising the data, analysing the results, and, finally, writing the research report or thesis.

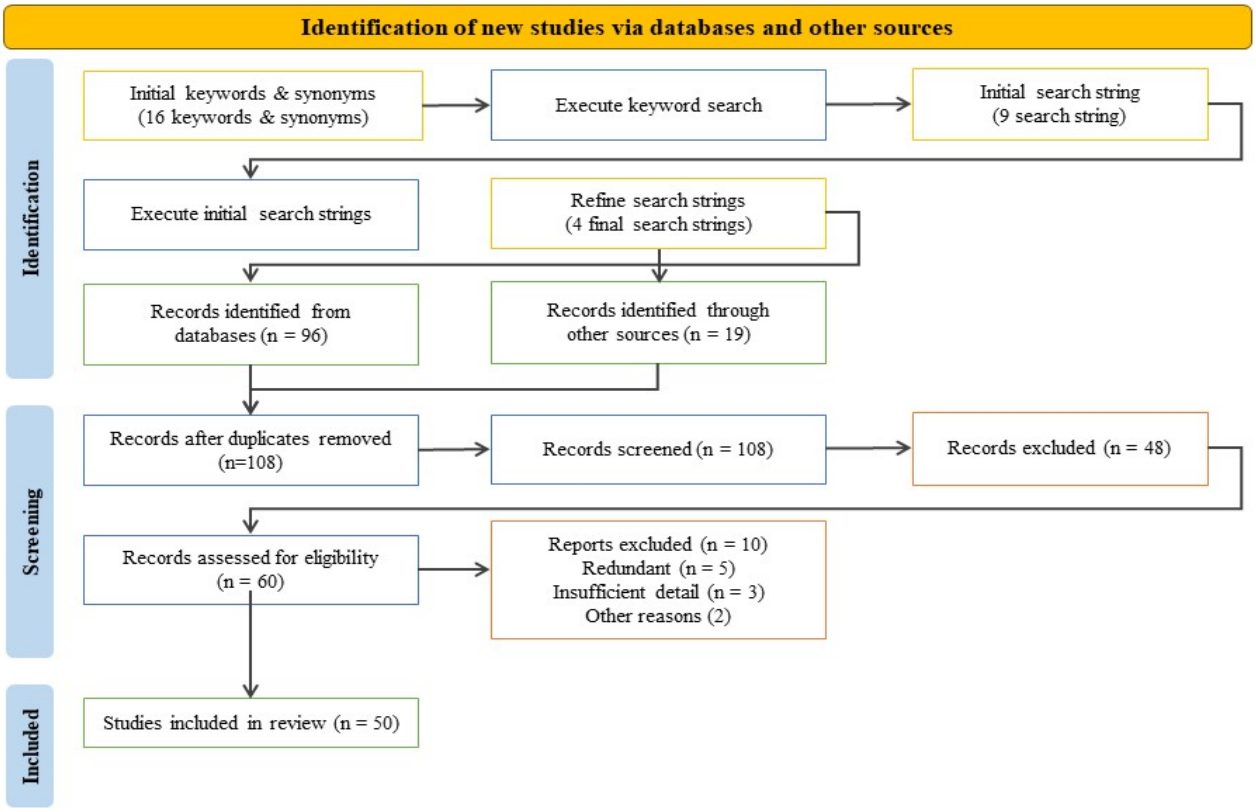

Figure 2. The PRISMA flow diagram for the systematic literature review (Phase 1 of the research process).

Data from peer-reviewed academic papers were analysed to investigate the lifecycle of digital evidence, relevant blockchain platforms, and cryptography methods. This analysis identified research gaps and was used in Phase 2 of the research to inform the development of a decentralised application to address scalability issues. The research methodology in Phases 2 and 3 was experimental, which can be defined as "a method of gathering information and data on a subject through observation in controlled settings" [61] (para. 1). The initial developed application in Phase 2 included the key stages of the digital CoC, namely, creation, acquisition, identification, storage, preservation, and access.

This application had a view to achieving the following goals:

- Ensure evidence integrity and admissibility by recording evidence modifications;
- Ensure data privacy and access control, preventing unauthorised access to evidence;
- Provide a cost-efficient decentralised application;
- Provide a viable evidence storage solution.

A range of tools was used for the implementation of the proposed model. Remix IDE, an online development environment, was used for writing, testing, and deploying smart contracts. MetaMask, a cryptocurrency wallet, manages all users and is essential for user authentication. Ganache, a local, customisable blockchain network was engaged for testing and debugging the proposed model. The front-end serves as the user's interface to interact with evidence, enabling access, management, and addition of evidence to case files. It is built on Vue.js, with web3.js and ipfs-http-client.js for functionality. Cryptographic operations are supported by jsencrypt, a Javascript library tool to perform encryption, decryption, and key generation, and vuecryptojs, another library or integration "wrapper". The model underwent initial trialling on both the Ethereum and Polygon networks.

In Phase 3 of the research, the security and performance capabilities of the model were evaluated in the two blockchain test networks. Each of the smart contracts were deployed using Remix to the test networks, which provided the basis for a comparative analysis of the model's performance in the two environments, producing a cost-effective, secure prototype for subsequent development and enhancement.

4. Results

The literature review set out in Section 2 above assessed the existing approaches to digital evidence management and discussed blockchain's potential to create a more secure and efficient evidence management system, and thereby addressed Research Objective 1, providing a conceptual basis for the subsequent research phases. In the following two sub-sections, Research Objectives 2 and 3 are addressed.

4.1. A New Application Model Based on Blockchain Technology That Facilitates Data Integrity and Admissibility and the Security of Digital Evidence in the CoC (Research Objective 2)

In Phase 2 of the research, a new application model based on blockchain technology was developed and tested. There were four main components to the proposed model (Figure 3):

- A decentralised application (DApp) is a blockchain-based application that combines a web-based front-end interface with back-end smart contracts. It can utilise various decentralised or traditional storage solutions depending on specific requirements, while integrating Web3 wallets, like MetaMask, for user authentication and transactions. The communication between front-end and blockchain nodes is facilitated through the JSON-RPC protocol, enabling seamless interaction with blockchain nodes for executing smart contract functions and data exchange. This architecture operates without centralised control through networks such as Polygon or Ethereum.
- IPFS storage is a decentralised off-chain storage solution using a peer-to-peer network. IPFS generates a 256-bit content ID hash (CID) for each file, allowing retrieval through this hash. The encrypted CID is stored on the blockchain to ensure evidence integrity and admissibility. A private IPFS ensures data privacy and restricts unauthorised access. While IPFS traffic is encrypted, metadata like PeerIDs and CIDs on distributed hash tables (DHT) are not [62]. Management of the private IPFS is handled by participating organisations or a designated consortium administrator. The file type evidence was uploaded to a private IPFS node.
- Smart contracts: The back end consists of two smart contracts: "User-Auth", which manages user authentication, registration, and role assignment, and "Management", which controls access to users' digital evidence. Furthermore, the proof of authority (PoA) consensus algorithm was used, which addresses concerns regarding transaction cost, energy consumption, and latency in data processing (as discussed in Section 2.3). Additionally, the smart contract serves as the link between data encryption and distribution. The management contract maintains a list of encrypted ciphers, the users with whom they are shared, and their associated case files. Upon access revocation, it removes the user's key from the case access and shared key list. It also manages user access, case information, and event logging, while the UserAuth contract handles user

registration and validation. Trusted validators, like judicial representatives and forensic experts, are able to efficiently validate transactions in the consortium blockchain, enhancing security and data integrity [33].

- Ethereum/Polygon blockchain: The proposed model was deployed and tested. Initially, testing was performed on Ganache, a localised blockchain network emulator designed for DApp testing and debugging. Following successful local testing, it was deployed to Ethereum Mainnet (Goerli testnet) and Polygon networks (Mumbai testnet). These networks are discussed in Section 2.4 above.

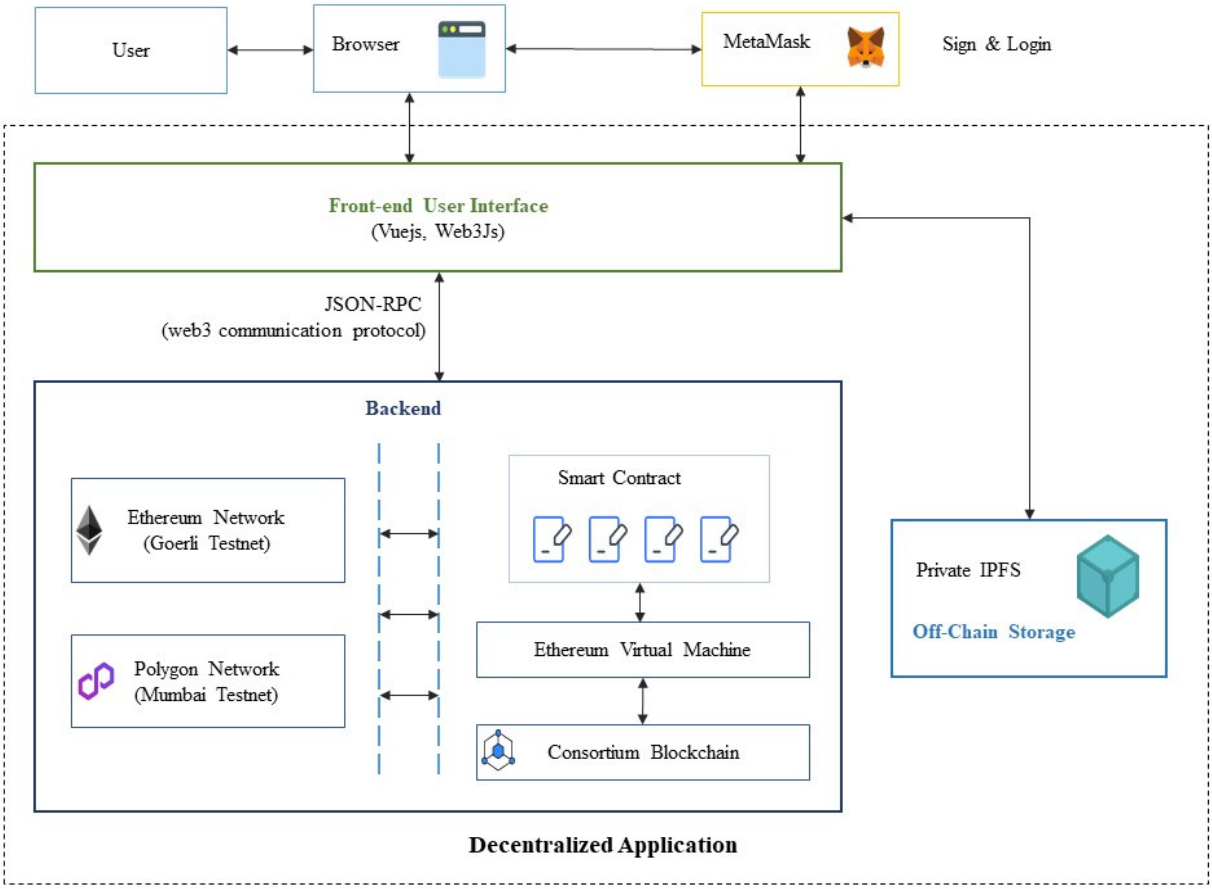

Figure 3. Proposed model structure in Phase 2.

Based on the literature review, user roles were categorised according to their privileges and responsibilities. The user groups reflect real-life case proceedings, with distinct rules for data access and operational capabilities. Each group has specific permissions for adding, viewing, or updating case data, as detailed in Table 2. The admin role possesses elevated authority with specific access and permissions, enabling oversight and management of individual case data and access. In addition, the admin role monitors each user's activity and can revoke access as needed. A management contract updates a revoke list accordingly, which is monitored during operations to prevent unauthorised access or illegal modifications to case data, bolstering platform security. More detail on the access control and evidence creation processing is given in Appendix A.

Table 2. Role based access control table.

Entity	Access Type	Permission		Roles
		Read	Write	
Supervisor	Full	TRUE	FALSE	Admin
Digital Investigator (Owner)	Full	TRUE	TRUE	Investigator
Judge	Partial	TRUE	FALSE	Judge
Jury	Partial	TRUE	FALSE	Jury
Forensic Lab	Partial	TRUE	TRUE	Forensic

Although user access is strictly controlled, data stored in the blockchain requires encryption before distribution. Here, a combination of hashing algorithms was employed—both symmetric (Advanced Encryption Standard-256) and asymmetric (Rivest–Shamir–Adleman)—providing high security capabilities, efficiency in speed, and low computational demands [63]. Further detail on the symmetric and asymmetric encryption is included in Appendix B.

4.2. Evaluation of the Security and Performance Aspects of the Developed Blockchain-Based Application for Managing Digital Evidence (Research Objective 3)

4.2.1. Security Aspects

Symmetric and asymmetric encryption components (such as AES and RSA—see Appendix B) were combined with blockchain's immutability to create a secure method for data maintenance, distribution, and the recording of operations. Smart contracts automate data management, including access control, user registration, verification, and access revocation, protecting data from unauthorised access and ensuring privacy.

Evidence integrity is ensured in two ways. Firstly, AES encryption secures the evidence, which is then stored within the blockchain. The blockchain's immutability prevents tampering, safeguarding the integrity of the encrypted data. Blockchain records all subsequent evidence updates, allowing authorised users to trace it back to its original form at creation, thereby enhancing its admissibility in legal proceedings. Secondly, to fortify data security, the solution employs a role-based access control model, as outlined above, ensuring restricted access for unauthorised users. RSA encryption (see Appendix B) securely transfers cipher keys among authorised users, enhancing data security protocols. Using IPFS storage mitigates centralisation risks, ensuring both scalability and reliability.

4.2.2. Performance Aspects

Research indicates that over 90% of Ethereum smart contracts are affected by gas-costly patterns, including useless code- and loop-related anti-patterns [64]. Functions involving storage, arrays, and loops impact gas usage, leading to out-of-gas exceptions [65]. Other factors, like bytecode analysis and deployment challenges [62], contribute to high gas fees. However, the gas cost varies due to several factors affecting usage. According to Li [65], removing storage use, avoiding struct variables, and refactoring without converting the byte32 variable reduced the gas fee for the RegisterUser function from 0.000465383 Matic to 0.000464245 Matic. These data were gathered using the Remix IDE on the Polygon Mumbai testnet. While the reduction is minor, optimising the entire smart contract can lead to significant improvements. Appendix C provides a comparison between unoptimised and optimised user register functions.

Based on the applied optimisation strategies, the contracts achieved notable gas fee reductions (3.54% for UserAuth and 11.64% for the Management contract) compared to their initial values, as shown in Table 3. These optimisations aim to lower gas usage, thereby reducing overall costs. The literature review (see Section 2.4) highlights Polygon as a particularly efficient platform for transactions and cost, with its Layer 2 scaling solutions enabling faster processing and lower fees. To illustrate Polygon's cost-effectiveness, Table 3

shows the calculation of the gas usage values, considering the standard prices of Matic (on the Polygon network) and Ether (on the Ethereum network).

Table 3. Contract deployment cost comparison: Polygon (matic) vs. Ethereum (eth).

Platform	Contracts	Gas Used	Gas Fee (GWei)	Gas Fee (Matic/Eth)	Total Gas Fee (Matic/Eth)	Exchange Rate (USD)	Platforms
Polygon	User Auth	938,945	2.500000015	0.002347363	0.010456068	0.77	0.008051172
	Management	3,243,482	2.500000015	0.008108705			
Ethereum	User Auth	938,945	2.500000008	0.002347363	0.010456068	2076.68	21.71390633
	Management	3,243,482	2.500000008	0.008108705			

Figure 4 illustrates the inverse relationship between transaction costs and network throughput for Ethereum and Polygon networks. The network performance is measured in transactions per second (TPS), with Ethereum processing 12–14 TPS, while Polygon achieves 65,000 TPS ([54], Table 4). The figure compares exchange rates (blue line) and TPS (green bars), and shows how total deployment costs (orange line) decrease from Ethereum (USD 21.71) to Polygon (USD 0.008), highlighting the efficiency gains of higher transaction speeds and indicating that using Matic for transactions can save about USD 21 per contract deployment compared to Ether, representing a significant 99.96% cost efficiency improvement, making Matic a more financially viable and sustainable option.

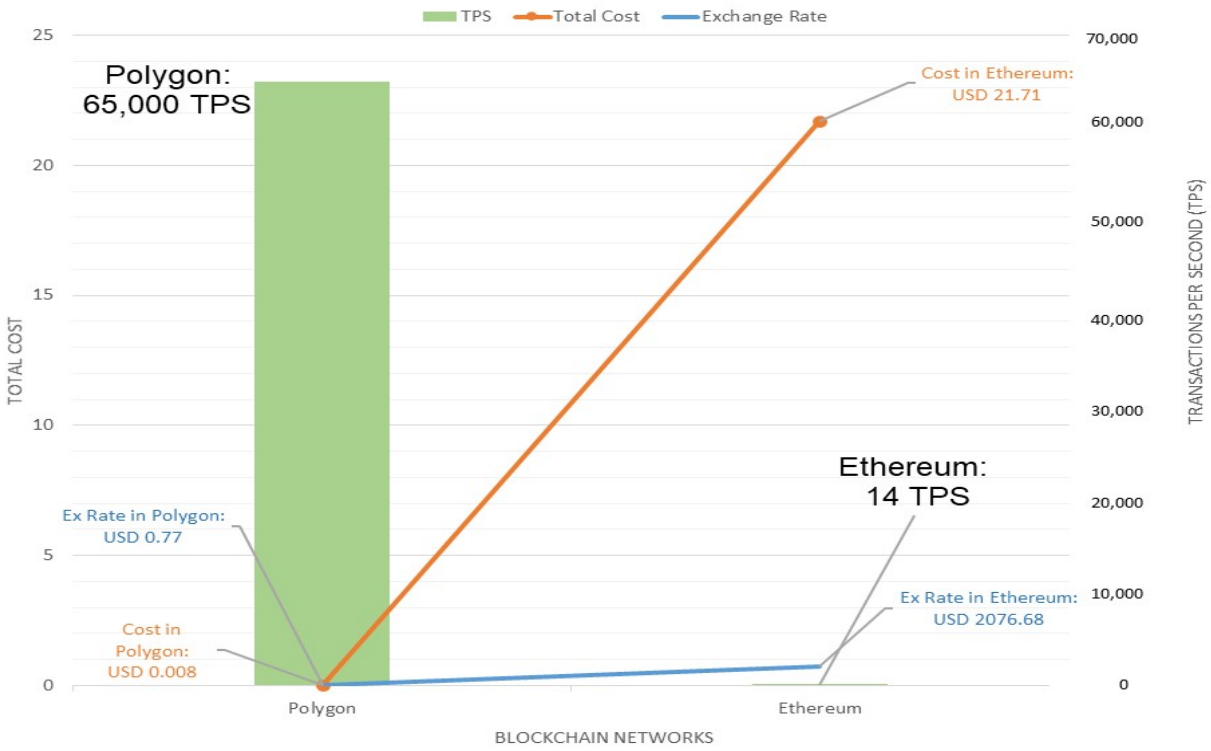

Figure 4. Relationship between transaction costs and network performance for Polygon and Ethereum networks.

5. Discussion

The results set out above raise some issues worthy of further discussion. Firstly, the results provide a new perspective on blockchain-based data security. Rana et al. [49] presented a decentralised architecture on Polygon to improve auditability and data security, reducing reliance on centralised institutions. However, the study does not specify the

blockchain type and implements user roles for access management. While focusing on data integrity and auditability, the architecture lacks encryption, storing data in plaintext on the block-chain visible to all participants. Additionally, in Rana et al.'s work [49], IPFS content identifiers (CIDs) are stored without encryption, risking unauthorised data access if CIDs are obtained, compromising privacy and legal admissibility. The creator admin oversees user creation, evidence approval, and ownership transfers, with the authority to appoint super admins or admins for request approval. This hierarchical structure enhances security, although it may introduce bottlenecks and delays.

Secondly, the proposed solution contributes to the potential management of digital evidence through the use of a consortium blockchain, smart contracts, and IPFS. It features a role-based access control model tailored for judicial processes, where data access requires approval from the data owner. Unlike private blockchains commonly used in similar contexts (see Table 1), the consortium blockchain is selected for its trustworthiness, lower latency, and reduced operational costs. Smart contracts streamline role assignments, offering enhanced flexibility and control over data management. Crucially, privacy concerns are addressed by encrypting evidence and IPFS CIDs before storage on the blockchain, ensuring confidentiality even if accessed.

Thirdly, cryptographic methods used in this study secure key exchange for safe data distribution among authorised users, significantly enhancing data privacy and security compared to the findings of Rana et al. [49]. The implementation of advanced encryption protocols for both evidence data and IPFS CIDs provides multiple layers of security. Nevertheless, smart contract vulnerabilities remain a concern, as several crucial issues required careful consideration during implementation. Re-entrancy attacks, which take advantage of vulnerabilities in smart contracts, pose a significant risk when malicious contracts exploit callback functions to recursively re-enter the original contract before previous executions are completed, potentially leading to unauthorised resource drainage and state manipulation. To mitigate this vulnerability, implementations must incorporate robust re-entrancy guards and follow established security patterns. Equally concerning are integer overflow and underflow vulnerabilities, which occur when arithmetic operations exceed the maximum or minimum bounds of their data types [28]. Another vulnerability is timestamp dependency, which arises from contracts that rely on block timestamps for key operations. Since miners can manipulate these timestamps within certain bounds, malicious actors can exploit this flexibility to execute front-running attacks by strategically positioning their transactions before legitimate ones [66].

Fourthly, in terms of cost efficiency, Polygon offers a more economic option. The PoA consensus algorithm it employs achieves low computational intensity by leveraging trusted validators, such as judicial representatives and forensic experts, to validate transactions. This cost advantage does not compromise security but rather enhances system sustainability and scalability compared to the findings of Rana et al. [49], which have scalability limitations.

Fifthly, the proposed solution effectively tackles critical challenges previously identified in blockchain-based evidence management systems. While Bonomi et al. [43] highlighted limitations with fixed validator sets and privacy compromises during consensus in their B-CoC architecture, the solution presented here leverages a consortium blockchain model that enables dynamic validator management. This approach allows multiple judicial stakeholders to participate in network validation while maintaining strict authentication through smart contracts and enhanced privacy through encrypted evidence storage. The consortium design overcomes the inflexibility of fixed validator structures while ensuring both security and operational efficiency in judicial evidence management processes.

In summary, the proposed solution demonstrates sustainability by leveraging Polygon's layer 2 scaling capabilities with a PoA consensus, and off-chain storage provides increased performance with reduced resource consumption, ensuring long-term operational viability while maintaining environmental responsibility.

6. Conclusions

Blockchain is a technology that is receiving growing attention from many researchers, scientists, and application developers. Data are stored in a transparent, shared distributed ledger, which is verified and maintained by the nodes in a decentralised network. The data in blockchain are immutable, as the blockchain is guarded by cryptography to ensure security, integrity, and privacy. This innovative tool promises a secure digital world and offers more reliable and convenient services. This advanced technology has the potential to radically change the way in which businesses and public services operate and the way transactions are conducted in everyday life.

This is of particular relevance to the management of criminal evidence, in which the CoC presents inherent complexities that demand specialised approaches. Existing solutions often target specific stages but lack comprehensive coverage. Blockchain technology emerges as a promising way forward due to its immutability, traceability, and transparency, crucial for maintaining evidence integrity and admissibility, thereby underpinning more sustainable solutions. More specifically, the solution put forward here integrates a consortium blockchain with IPFS to establish robust evidence maintenance capabilities. IPFS provides scalable storage to accommodate increasing evidence data volumes, ensuring long-term system sustainability. In addition, this study implements role-based access control mechanisms to manage permissions based on user roles, enhancing access control and protecting data privacy against unauthorised access. Emphasising scalability, cost-efficiency, and transaction speed, the approach set out here leverages Polygon for developing decentralised applications. Polygon addresses scalability concerns more effectively than Ethereum, offering a PoA consensus algorithm and smart contracts to ensure secure and reliable digital evidence management.

This study contributes to a number of areas: the identification of challenges in the judicial system's management of digital evidence and the benefits of adopting blockchain technology; proposing and implementing a blockchain-based solution to address these challenges; and providing an efficient, sustainable, and practical storage solution for digital evidence. The solution presented here can act as a basis for further development by other researchers in exploring how blockchain can be deployed to enhance data security and integrity in the management of criminal justice evidence.

This study has its limitations. First, it must be recognised that blockchain technology, despite its many advantages, still faces significant security challenges and vulnerabilities, specifically within smart contracts, where a notable number of issues remain unexplored. While blockchain promotes decentralisation, smart contracts can introduce centralisation risks, creating a critical vulnerability. Second, and more specifically as regards this project, while testnets offer a valuable environment for developing and testing decentralised applications, they have limitations that impact development and performance effectiveness. Testnets often fail to accurately replicate real-world main-net conditions, making it challenging to assess actual network loads and user interactions. Issues such as network congestion, transaction delays, and test token shortages can impede testing and may not fully capture the diverse scenarios faced in production. Moreover, current solutions typically lack the ability to set user-specific access permissions, a feature that could be beneficial in certain scenarios. These limitations can lead to unforeseen challenges when deploying smart contracts on main nets.

In this context, this study points to a number of possible areas for future research. Taking a broad perspective, one area that could profitably be pursued is to explore how blockchain applications, like the one developed here, can be made more accessible to developers than is currently the case. This would enhance both the development potential and testing and verification rigor. A further area for future research is the integration of artificial intelligence techniques and tools to analyse smart contract's behaviour and data transactions. Indeed, the proposed solution in this study emphasises the need for enhanced encryption algorithms. Future research could also explore elliptic curve cryptography as an alternative to the RSA public-key encryption algorithm to bolster security,

offering efficiency benefits with comparable security levels. Real-world testing and integration of user-specific permission features would further fortify security and refine data access controls. Enhancing user-specific permissions could offer finer granularity in access management capabilities. Furthermore, addressing privacy concerns inherent in CoC procedures might involve incorporating zero-knowledge proofs (ZKPs) to ensure evidence verifiability while safe-guarding anonymity [67]. Such research initiatives would serve to further the provision of sustainable solutions for digital evidence storage, recording, and analysis using blockchain technology.

Author Contributions: Conceptualization, M.H.A.R. and S.M.; methodology, M.H.A.R. and S.M.; software, M.H.A.R.; validation, M.H.A.R., S.M. and M.W.; formal analysis, M.H.A.R.; investigation, M.H.A.R.; resources, M.H.A.R., S.M. and M.W.; data curation, M.H.A.R., S.M. and M.W.; writing—original draft preparation, M.H.A.R., S.M. and M.W.; writing—review and editing, M.H.A.R., S.M. and M.W.; visualization, M.H.A.R., S.M. and M.W.; supervision, S.M.; project administration, M.H.A.R., S.M. and M.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The test data used in this research are held within a university environment. Further enquiries can be directed to the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Access Control and Evidence Creation Processes in Proposed Model

Access Control Process:

1. Admins can specify user access levels to case files, excluding the owner's access.
2. The owner of evidence is typically the user who created it, such as those with an investigator role.
3. To access a case file, the jury, judge, and forensic need approval from the admin and the owner of that evidence.
4. Only forensic users can add or update evidence but require approval from the admin and owner of that case file.

Evidence Creation:

1. If (user = investigator), then the user is allowed to create a case file.
2. Otherwise, "you do not have permission to create case file".
3. Case file requires a password to proceed (generates AES key from password) to add evidence into it.
4. Only the investigator and forensic can add or update evidence of a case file.
5. After adding evidence, it is encrypted with the AES key and then stored on the blockchain via management contract.
6. File-based evidence is uploaded to IPFS, and the CID is added to the case file.
7. The CIDs are then encrypted and stored in the blockchain, same as step 5.
8. To update existing case files, the owner of that case file needs to decrypt it using the AES key of that case file.

This details the workflow explaining the roles, permissions, and encryption methodologies employed throughout the management and handling of evidence within this pro-posed decentralised system.

Appendix B. Symmetric and Asymmetric Encryption Detail

Symmetric Encryption

This study utilised PBKDF2 to generate a cipher key by combining hash algorithms (like SHA-256) with a salt and iteration count, enhancing security against brute-force attacks [68]. Each investigator initiates encryption of new case files by providing a password, which derives the AES-256 key, ensuring confidentiality of the encrypted data stored on the blockchain through a management contract (Figure A1).

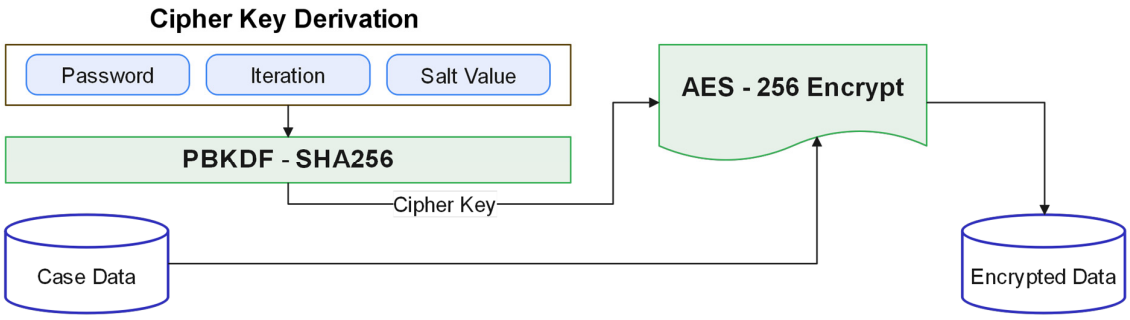

Figure A1. Key derivation and data encryption process.

Asymmetric Encryption

Storing cipher keys on the blockchain poses security risks, potentially allowing unauthorised access and decryption of data. Instead, RSA encryption securely distributes cipher keys among authorised users using the recipient's public key. The complete process of data encryption–decryption and distribution can be represented mathematically, which is shown below in Figure A2.

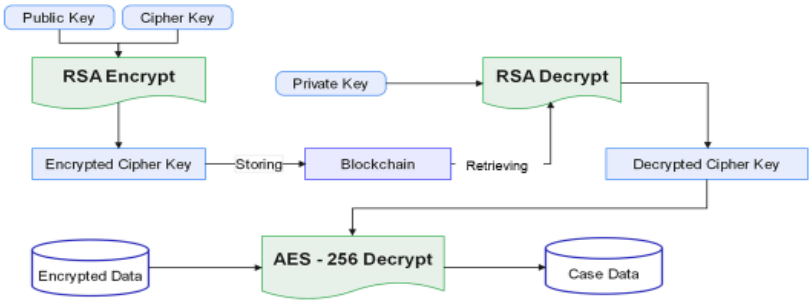

Figure A2. Key distribution and data decryption process.

The variables used in the formalisation are described below:

- P denotes the password;
- S denotes the salt (a random value used to increase the complexity of the derived key);
- C denotes the iteration count (number of iterations);
- K_{Length} denotes the desired length of the derived key;
- *M* represents the original data;
- C_{AES} represents the cipher text obtained by encrypting the data *M* using the *AES*;
- K_{AES} is the key used for AES encryption;
- C_{RSA} represents the cipher text obtained by encrypting the *AES* key K_{AES} using the *RSA* algorithm;
- K_{RSA} is the RSA public key used for encryption;
- $K_{AES\ -\ decrypt}$ is the *AES* key obtained by decrypting C_{RSA} using the *RSA* private key.

The mathematical representation is as follows:

1. K_{AES} = PBKDF2 (P, S, C, K_{Length});

2. *AES* Encryption:
   a. $C_{AES} = AES_{Encrypt}(M, K_{AES})$;
3. *RSA* Encryption of *AES* Key: $C_{RSA} = RSA_{Encrypt}(K_{AES}, K_{RSA})$;
4. Transmission of C_{AES} and C_{RSA} to User B;
5. *RSA* Decryption to Obtain *AES* Key:
   a. $K_{AES-decrypt} = RSA_{decrypt}(C_{RSA}, RSA_{PrivateKey})$;
6. *AES* Decryption:
   a. $M_{decrypt} = AES_{decrypt}(C_{AES}, K_{AES-decrypt})$.

Here $AES_{Encrypt}$, $RSA_{Encrypt}$, $RSA_{Decrypt}$, and $AES_{Decrypt}$ are functions representing the encryption and decryption processes for *AES* and *RSA*.

Appendix C. Comparison Between Unoptimised and Optimised User Register Function

Figures A3 and A4 below show a comparison between unoptimised and optimised user register functions.

```
function registerUser(
  string memory _name,
  string memory _email,
  string memory _password,
  Roles _role
) external {
  // convertion of string to byte32 variable
  bytes32 name = stringToBytes32(_name);
  bytes32 email = stringToBytes32(_email);
  bytes32 password = stringToBytes32(_password);
  // (reqired) checking for existing users
  require(!userExists[email], "Email address is already registered");
  users[msg.sender] = UserProfile(name, email, password, _role, "");
  userExists[email] = true;
  allUsers.push(msg.sender);
  emit UserRegistered(msg.sender, name, email, _role);
 }
```

Figure A3. Unoptimised user register function.

```
function registerUser(
  string memory _name,
  string memory _email,
  string memory _password,
  Roles _role
) external onlyNewUser(_email) {
  // No convertion of string to byte32 variable
  // required method replaced with onlyNewUser modifier (
  //(performs same task)
  users[msg.sender] = UserProfile(_name, _email, _password, _role, "");
  userExists[_email] = true;
  allUsers.push(msg.sender);
  // removed unneccary emit event
}
```

Figure A4. Optimised user register function.

Figure A3 (unoptimised) and Figure A4 (optimised) show the same function from the UserAuth contract.

References

1. Ul Hassan, M.; Rehmani, M.H.; Chen, J. Differential privacy in Blockchain technology: A futuristic approach. *J. Parallel Distrib. Comput.* **2020**, *145*, 50–74. [CrossRef]
2. Chen, H.; Pendleton, M.; Njilla, L.; Xu, S. A Survey on Ethereum Systems Security. *ACM Comput. Surv.* **2020**, *53*, 1–43. [CrossRef]
3. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y.T. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1432–1465. [CrossRef]
4. Lone, A.H.; Mir, R.N. Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. *Digit. Investig.* **2019**, *28*, 44–55. [CrossRef]
5. Prayudi, Y.; SN, A. Digital Chain of Custody: State of The Art. *Int. J. Comput. Appl.* **2015**, *114*, 1–9. [CrossRef]
6. PWC. Embracing Sustainable Innovation: Understanding the Environmental Impacts of Blockchain Technology. 2024. Available online: https://www.pwc.com/us/en/services/digital-assets/blockchain-environmental-impact.html (accessed on 20 October 2024).
7. Costa, I.; Riccotta, R.; Montini, P.; Stefani, E.; de Souza Goes, R.; Gaspar, M.A.; Martins, F.S.; Fernandes, A.A.; Machado, C.; Loçano, R.; et al. The Degree of Contribution of Digital Transformation Technology on Company Sustainability Areas. *Sustainability* **2022**, *14*, 462. [CrossRef]
8. Wynn, M.; Jones, P. Digital Technology Deployment and the Circular Economy. *Sustainability* **2022**, *14*, 9077. [CrossRef]
9. Mulligan, C.; Morsfield, S.; Cheikosman, E. Blockchain for sustainability: A systematic literature review for policy impact. *Telecommun. Policy* **2024**, *48*, 102676. [CrossRef]
10. Le, T.V.; Hsu, C.L. A Systematic Literature Review of Blockchain Technology: Security Properties, Applications and Challenges. *J. Internet Technol.* **2021**, *22*, 789–802. [CrossRef]
11. Wang, H.; Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352. [CrossRef]
12. NIST Computer Security Resource Centre Glossary. Chain of Custody. 2024. Available online: https://csrc.nist.gov/glossary/term/chain_of_custody (accessed on 30 September 2024).
13. Gopalan, S.H.; Suba, S.A.; Ashmithashree, C.; Gayathri, A.; Andrews, V.J. Digital forensics using blockchain. *Int. J. Recent. Technol. Eng.* **2019**, *8*, 182–184. [CrossRef]
14. Ćosić, J.; Ćosić, Z. Chain of Custody and Life Cycle of Digital Evidence. *Comput. Technol. Appl.* **2012**, *3*, 126–129. Available online: https://www.academia.edu/15316907/Chain_of_custody_and_life_cycle_of_digital_evidence (accessed on 1 October 2024).
15. Ćosić, J.; Ćosić, Z.; Bača, M. An Ontological Approach to Study and Manage Digital Chain of Custody of Digital Evidence. *J. Inf. Organ. Sci.* **2011**, *35*, 1–13. Available online: https://www.academia.edu/15316908/An_ontological_approach_to_study_and_manage_digital_chain_of_custody_of_digital_evidence (accessed on 20 October 2024).
16. Choenni, S.; van Dijk, J.; Leeuw, F. Preserving privacy whilst integrating data: Applied to criminal justice. *Inf. Policy* **2010**, *15*, 125–138. [CrossRef]
17. Wexler, R. Privacy Asymmetries: Access to Data in Criminal Defense Investigations. *UCLA Law Rev.* **2021**, *212*, 212–287.
18. Prayudi, Y.; Ashari, A.; Priyambodo, T.K. Digital Evidence Cabinets: A Proposed Framework for Handling Digital Chain of Custody. *Int. J. Comput. Appl.* **2014**, *107*, 30–36. [CrossRef]
19. D'Anna, T.; Puntarello, M.; Cannella, G.; Scalzo, G.; Buscemi, R.; Zerbo, S.; Argo, A. The Chain of Custody in the Era of Modern Forensics: From the Classic Procedures for Gathering Evidence to the New Challenges Related to Digital Data. *Healthcare* **2023**, *11*, 634. [CrossRef]
20. Saleem, S.; Popov, O.; Dahman, R. Evaluation of security methods for ensuring the integrity of digital evidence. In Proceedings of the 2011 International Conference on Innovations in Information Technology IIT, Abu Dhabi, United Arab Emirates, 25–27 April 2011; pp. 220–225. [CrossRef]
21. Shah, M.S.; Saleem, S.; Zulqarnain, R. Protecting Digital Evidence Integrity and Preserving Chain of Custody. *J. Digit. Forensics Secur. Law* **2017**, *12*, 12. [CrossRef]
22. Banwani, D.; Kalra, Y. Maintaining and Evaluating the Integrity of Digital Evidence in Chain of Custody. *Int. J. Recent Technol. Eng. IJRTE* **2021**, *10*, 90–96. [CrossRef]
23. Ûosiü, J.; Baþa, M. (Im)Proving Chain of Custody and Digital Evidence Integrity with Time Stamp. In Proceedings of the 33rd International Convention MIPRO, Opatija, Croatia, 24–28 May 2010. Available online: https://ieeexplore.ieee.org/abstract/document/5533653 (accessed on 20 October 2024).
24. Ruj, S.; Nayak, A. A decentralized security framework for data aggregation and access control in smart grids. *IEEE Trans. Smart Grid* **2013**, *4*, 196–205. [CrossRef]
25. Buccafurri, F.; Angelis, V.D.; Lazzaro, S.; Pugliese, A. Enforcing security policies on interacting authentication systems. *Comput. Secur.* **2024**, *140*, 103771. [CrossRef]
26. Romli, M.A.; Prayudi, Y.; Sugiantoro, B. Storage Area Network Architecture to support the Flexibility of Digital Evidence Storage. *Int. J. Comput. Appl.* **2019**, *182*, 30–35. Available online: https://www.ijcaonline.org/archives/volume182/number41/30368-2019918496/ (accessed on 20 October 2024).
27. Ćosić, J.; Bača, M. A Framework to (Im)Prove Chain of Custody in Digital Investigation Process. In Proceedings of the 21st Central European Conference on Information and Intelligent Systems, Varazdin, Croatia, 22–24 September 2010. Available online: https://www.researchgate.net/publication/279175021 (accessed on 1 October 2024).

28. Mollajafari, S.; Bechkoum, K. Blockchain Technology and Related Security Risks: Towards a Seven-Layer Perspective and Taxonomy. *Sustainability* **2023**, *15*, 13401. [CrossRef]
29. Gervais, A.; Karame, G.O.; Wüst, K.; Glykantzis, V.; Ritzdorf, H.; Capkun, S. On the security and performance of Proof of Work blockchains. In Proceedings of the ACM Conference on Computer and Communications Security 2016, Vienna, Austria, 24–28 October 2016; pp. 3–16. [CrossRef]
30. Liu, J.; Xie, M.; Chen, S.; Ma, C.; Gong, Q. An improved DPoS consensus mechanism in blockchain based on PLTS for the smart autonomous multi-robot system. *Inf. Sci.* **2021**, *575*, 528–541. [CrossRef]
31. Manolache, M.A.; Manolache, S.; Tapus, N. Decision Making using the Blockchain Proof of Authority Consensus. *Procedia Comput. Sci.* **2022**, *199*, 580–588. [CrossRef]
32. Wu, X.; Chang, J.; Ling, H.; Feng, X. Scaling proof-of-authority protocol to improve performance and security. *Peer Peer Netw. Appl.* **2022**, *15*, 2633–2649. [CrossRef]
33. Bamakan, S.M.H.; Motavali, A.; Bondarti, A.B. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert. Syst. Appl.* **2020**, *154*, 113385. [CrossRef]
34. Liu, J.; Zhang, Q.; Xie, M.; Lin, M.; Xu, Z. A blockchain platform selection method with heterogeneous multi-criteria Decision-Making based on hybrid distance measures and an AHP-EWM weight method. *Expert. Syst. Appl.* **2024**, *256*, 124910. [CrossRef]
35. Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J. Smart contract-based access control for the internet of things. *IEEE Internet Things J.* **2019**, *6*, 1594–1605. [CrossRef]
36. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [CrossRef]
37. Ali, O.; Jaradat, A.; Kulakli, A.; Abuhalimeh, A. A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities. *IEEE Access* **2021**, *9*, 12730–12749. [CrossRef]
38. Zhai, S.; Yang, Y.; Li, J.; Qiu, C.; Zhao, J. Research on the Application of Cryptography on the Blockchain. *J. Phys. Conf. Ser.* **2019**, *1168*, 032077. [CrossRef]
39. Ahmad, L.; Khanji, S.; Iqbal, F.; Kamoun, F. Blockchain-based chain of custody: Towards real-time tamper-proof evidence management. In Proceedings of the ACM International Conference Proceeding Series 2020, Dublin, Ireland, 25–28 August 2020. [CrossRef]
40. Sultana, T.; Almogren, A.; Akbar, M.; Zuair, M.; Ullah, I.; Javaid, N. Data Sharing System Integrating Access Control Mechanism using Blockchain-Based Smart Contracts for IoT Devices. *Appl. Sci.* **2020**, *10*, 488. [CrossRef]
41. Li, M.; Lal, C.; Conti, M.; Hu, D. LEChain: A blockchain-based lawful evidence management scheme for digital forensics. *Future Gener. Comput. Syst.* **2021**, *115*, 406–420. [CrossRef]
42. Elgohary, H.M.; Darwish, S.M.; Elkaffas, S.M. Improving Uncertainty in Chain of Custody for Image Forensics Investigation Applications. *IEEE Access* **2022**, *10*, 14669–14679. [CrossRef]
43. Bonomi, S.; Casini, M.; Ciccotelli, C. B-CoC: A blockchain-based chain of custody for evidences management in digital forensics. *arXiv* **2020**, arXiv:1807.10359. [CrossRef]
44. Yunianto, E.; Prayudi, Y.; Sugiantoro, B. B-DEC: Digital Evidence Cabinet based on Blockchain for Evidence Management. *Int. J. Comput. Appl.* **2019**, *181*, 22–29. [CrossRef]
45. Burri, X.; Casey, E.; Bollé, T.; Jaquet-Chiffelle, D.O. Chronological independently verifiable electronic chain of custody ledger using blockchain technology. *Forensic Sci. Int. Digit. Investig.* **2020**, *33*, 300976. [CrossRef]
46. Wang, S.; Zhang, Y.; Zhang, Y. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems. *IEEE Access* **2018**, *6*, 38437–38450. [CrossRef]
47. Kamboj, P.; Khare, S.; Pal, S. User authentication using Blockchain based smart contract in role-based access control. *Peer Peer Netw. Appl.* **2021**, *14*, 2961–2976. [CrossRef]
48. Hanafi, J.; Prayudi, Y.; Luthfi, A. IPFSChain: Interplanetary File System and Hyperledger Fabric Collaboration for Chain of Custody and Digital Evidence Management. *Int. J. Comput. Appl.* **2021**, *183*, 24–31. [CrossRef]
49. Rana, S.K.; Rana, A.K.; Rana, S.K.; Sharma, V.; Lilhore, U.K.; Khalaf, O.I.; Galletta, A. Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain. *IEEE Access* **2023**, *11*, 83289–83300. [CrossRef]
50. Yadav, J.; Shevkar, R. Performance-Based Analysis of Blockchain Scalability Metric. *Tehnički Glasnik* **2021**, *15*, 133–142. [CrossRef]
51. Bafandehkar, M.; Yasin, S.M.; Mahmod, R.; Hanapi, Z.M. Comparison of ECC and RSA algorithm in resource constrained devices. In Proceedings of the 2013 International Conference on IT Convergence and Security ICITCS, Macao, China, 16–18 December 2013. [CrossRef]
52. Neiheiser, R.; Inacio, G.; Rech, L.; Montez, C.; Matos, M.; Rodrigues, L. Practical Limitations of Ethereum's Layer-2. *IEEE Access* **2023**, *11*, 8651–8662. [CrossRef]
53. Thibault, L.T.; Sarry, T.; Hafid, A.S. Blockchain Scaling Using Rollups: A Comprehensive Survey. *IEEE Access* **2022**, *10*, 93039–93054. [CrossRef]
54. Diaconita, V.; Belciu, A.; Stoica, M.G. Trustful Blockchain-Based Framework for Privacy Enabling Voting in a University. *J. Theor. Appl. Electron. Commer. Res.* **2023**, *18*, 150–169. [CrossRef]
55. Hart, C. *Doing a Literature Review: Releasing the Research Imagination*; Sage Publishing: Thousand Oaks, CA, USA, 2018.
56. Fink, A. *Conducting Research Literature Reviews: From the Internet to Paper*; Sage Publishing: Thousand Oaks, CA, USA, 2019.

57. Moher, D.; Liberati, A.; Tetzlaff, J.; Altman, D.G. Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *Int. J. Surg.* **2010**, *8*, 336–341. [CrossRef]
58. Greenhalgh, T.; Thorne, S.; Malterud, K. Time to challenge the spurious hierarchy of systematic over narrative reviews? *Eur. J. Clin. Investig.* **2018**, *48*, e12931. [CrossRef]
59. Kitchenham, B.; Charters, S.; Budgen, D.; Brereton, P.; Turner, M.; Linkman, S.; Jørgensen, M.; Mendes, E.; Visaggio, G. *Guidelines for Performing Systematic Literature Reviews in Software Engineering, EBSE Technical Report*; University of Keele: Keele, UK; University of Durham: Durham, UK, 2007; EBSE-2007-01. Available online: https://legacyfileshare.elsevier.com/promis_misc/525444systematicreviewsguide.pdf (accessed on 12 October 2024).
60. Page, M.J.; McKenzie, J.E.; Bossuyt, P.M.; Boutron, I.; Hoffmann, T.C.; Mulrow, C.D.; Shamseer, L.; Tetzlaff, J.M.; Akl, E.A.; Brennan, S.E.; et al. The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ* **2021**, *372*, n71. [CrossRef]
61. Indeed Editorial Team. Experimental Research: Definition, Types and Examples. 2024. Available online: https://www.indeed.com/career-advice/career-development/experimental-research (accessed on 18 October 2024).
62. IPFS. Privacy and Encryption. IPFS Docs. 2023. Available online: https://docs.ipfs.tech/concepts/privacy-and-encryption/#what-s-public-on-ipfs (accessed on 12 October 2023).
63. Khanezaei, N.; Hanapi, Z.M. A framework based on RSA and AES encryption algorithms for cloud computing services. In Proceedings of the 2014 IEEE Conference on System, Process and Control ICSPC, Kuala Lumpur, Malaysia, 12–14 December 2014; pp. 58–62. [CrossRef]
64. Chen, T.; Li, X.; Luo, X.; Zhang, X. Under-optimized smart contracts devour your money. In Proceedings of the 24th IEEE International Conference on Software Analysis, Evolution, and Reengineering 2017 SANER, Klangenfurt, Austria, 20–24 February 2017; pp. 442–446. [CrossRef]
65. Li, C. Gas Estimation and Optimization for Smart Contracts on Ethereum. In Proceedings of the 2021 36th IEEE/ACM International Conference on Automated Software Engineering ASE, Melbourne, Australia, 15–19 November 2021; pp. 1082–1086. [CrossRef]
66. Antonopoulos, A.M.; Wood, G. *Mastering Ethereum: Building Smart Contracts and DApps*; O'reilly Media: Sebastopol, CA, USA, 2019; p. 424. Available online: https://www.google.co.uk/books/edition/Mastering_Ethereum/nJJ5DwAAQBAJ (accessed on 18 October 2024).
67. Lourinho, L.; Kendzierskyj, S.; Jahankhani, H. Securing the digital witness identity using blockchain and zero-knowledge proofs. In *Strategy, Leadership, and AI in the Cyber Ecosystem. The Role of Digital Societies in Information Governance and Decision Making*; Academic Press: Cambridge, MA, USA, 2021; pp. 159–194. [CrossRef]
68. Choi, H.; Seo, S.C. Optimization of PBKDF2 Using HMAC-SHA2 and HMAC-LSH Families in CPU Environment. *IEEE Access* **2021**, *9*, 40165–40177. [CrossRef]