JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Evidence Management System Using Blockchain

Sonali Antad
dept. of computer engineering
Vishwakarma Institute of Technology
Pune, India

Harshita Chhangani
dept. of computer engineering
Vishwakarma Institute of Technology
Pune, India

Arwa Bhojawala
dept. of computer engineering
Vishwakarma Institute of Technology
Pune, India

Manas Avachat
dept. of computer engineering
Vishwakarma Institute of Technology
Pune, India

Anshu Maheshkar
dept. of computer engineering
Vishwakarma Institute of Technology
Pune, India

***Abstract*— Evidence Management System is placed at the very forefront of a paradigm shift in evidence handling, using the blockchain as a means to protect and deliver total transparency. As there are safeguarded elements inherent to the blockchain, the EMS will constitute an impenetrable fortress for the evidence, thus doing away with the requirement for oversight from some sort of central authority. Smart contracts flow through the EMS, self-governing the submission, retrieval, and granting of access of the evidence by cultivating accountability and transparency. Such a dynamic framework will allow not only scalability but strict access control. Integration with Metamask further democratizes user interaction with Ethereum smart contracts to such an extent that evidence management is intuitive and inclusive. The EMS is a dawn for evidence management in a new form. Smart contracts, while blockchain innovations are approached through the optics of security and transparency, would act like the orchestra conductors, orchestrating evidence tasks clearly and autonomously. It is the liquid structure that offers adaptability along with strict controls via customizable logic in access. Metamask collaborates to make engagement with Ethereum smart contracts more straightforward and thus evidence management a thing which is intuitive and inclusive in all means. EMS transforms the practices related to evidence and makes sure that its handling is secured and transparent in a decentralized environment, by capitalizing on blockchain's power. Smart contracts ease the process of transparency at every step and reliability in every decision. EMS offers a robust base for effective evidence management with aspects like scalability and strong access controls at the core. The Metamask integration facilitates multiple stakeholders with evidence management in their fingertips and makes it both accessible and user-friendly for all.**

Keywords*— *Evidence Management System, Blockchain, Smart Contracts, Automated Evidence Handling

I. Introduction

It is on the foundation of such a preservation of evidence integrity in the complex legal and regulatory landscape that trust, and justice thrive. However, traditional mechanisms that were used in managing evidence do very little to provide concrete assurance; it instead opens doors for biased manipulation, and leaves it entirely to individuals, as it is about them, rather than truth or reality.

The newly designed Evidence Management System employing blockchain technology for the transformation of the management of evidence into something much more secure as well as transparent helps guarantee each piece of evidence to be treated with the highest integrity. At its core, the EMS attacks the traditional approach in that it decentralizes the custody of evidence. Rather than a single central authority, it relies on a network of users which is distributed using blockchain. The model of decentralization disperses evidence over several nodes, making it impossible to falsify in practice. Also, removing intermediaries increases both speed and integrity of the proof management process.

The core of the effectiveness of EMS is in its smart contracts - those digital agreements residing on the blockchain. They can operate autonomously on every action regarding evidence handling, for instance submission, retrieval, accessing control, and timestamps, completely transparent and independent in their functions- honest and protocol compliant. One such interface is Metamask, which is an easy-to-use interface that has simplified access to Ethereum-based applications. Its intuitive design makes it accessible to users of all expertise levels and democratizes evidence management.

As the EMS moved ahead, with it came changes that not only revamped evidence management, but also opened a new level of transparency, dependability, and trust in legal systems. This research paper explores the intricate workings of the EMS, examining its potential to redefine evidence management in the digital age.

II. Literature Review

Sathyaprakasan et al. [1] discussed the use of blockchain technology for managing forensic evidence toward guaranteeing integrity and transparency in handling procedures. A recent study indicates that blockchain could offer an evidence storage system that is decentralized and tamper-proof, while frequent problems arise in the forms of losses and unauthorized access. Li et al. [2] had previously proposed LEChain-a blockchain-based scheme intended to enhance the process of digital forensic. They laid a great emphasis on the concept saying that it authenticated and traced evidence from the blockchain; thus, an effective and secure management process became possible during a digital forensic investigation. Rao et al. [3] conceptualized blockchain to provide managerial support in digital evidence handling. Their framework was based on blockchain's properties in such a way that no one can alter it because of its reliability in dealing with digital evidence handling, and it cannot be tampered with. The concept for development of a blockchain-based digital forensic cabinet was proposed by Yunianto et al. [4]. This approach has provided safe decentralized storage facilities for forensic, and the traceability of this system is completely maintained, ensuring that no evidence tampering or loss takes place throughout the lifecycle. Borse et al. [5] discussed the merits of the integration of blockchain in handling forensic evidence. The authors indicated that blockchain would safeguard evidence integrity through transparency within its procedure for handling, and hence provide it with better security against tampering. Patil et al. [6] highlighted the improving of security in forensic evidence using blockchain. The work presented how the use of blockchain technology prevents unauthorized access, maintains a chain of custody, and increases security for the evidence generally. Tsai [7] discussed contribution from blockchain for maintaining chain of custody in criminal investigations, handling forensic evidence collected from beginning till the presentation in the court. The research article well depicted blockchain capabilities for maintaining integrity in evidence. Billard [8] proposed that a blockchain-based digital inventory system could be utilized in evidence. The use of such a digital inventory system would ensure that pieces of evidence became securely recorded and fully traceable across their lifecycle with no risk of either tampering or mismanagement. Alqahtany and Syed [9] here present an all-rounded approach on the use of blockchain in digital forensics and evidence management. The authors of the method and how it can be applied on to the transparent, accountable, and fair treatment of forensic evidence. Charles et al. [10] designed a security system to protect one form or another from tampering or other types of manipulation, hence keeping it both transparent and secure via blockchain technology. Dhulavvagol et al. [11] had tried applying blockchain sharding and IPFS in evidence management; they successfully achieved impressive scalability and effectiveness with such configuration. Their system was safely shielded and optimized to ensure right evidence management. Billard [12] developed a weighed system for evidence based on blockchain in order to seize forensic relevance as well as importance. This system upgraded the process of evidence management by weighing large volumes of evidence through blockchain technology. Philip and Saravanaguru [13] developed an evidence management framework over a blockchain network based on smart contracts for investigating vehicle accidents. This ensured transparency and accountability in handling digital evidence during the IoT era of Internet of Vehicles. Ahmad et al. [14] have proposed blockchain-based chain of custody with a proof concept ensuring secure, tamper-proof evidence management with the help of private Ethereum blockchain technology. Such framework will hence integrate into digital evidence systems in order to better maintain the integrity of evidence among multiple stakeholders such as law enforcement agencies and forensic professionals. Tian et al. [15] developed a block-based, Blockchain-based Digital Evidence framework- Block-DEF designed to counter the challenge posed by it towards scalability and privacy concerns. Traceability is maintained whilst achieving privacy in evidence management using a lightweight blockchain that also integrates a mixed block structure and multi-signature techniques.

Author(s)	**Research Focus**	**Key Contributions**	**Differentiation**
R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip, and N. Singh [1]	Blockchain-based forensic evidence management	Focus on integrity and transparency; decentralized and tamper-proof storage	Emphasis on user-friendly interfaces for evidence handling and reporting.
M. Li, C. Lal, M. Conti, and D. Hu, "LEChain [2]	LEChain scheme for digital forensic evidence	Authentication, tracking, and evidence tracing can be done with improved secure management process.	It incorporates AI-driven analytics in order to generate real-time insights into handling evidence.
S. Rao, S. Fernandes, S. Raorane, and S. Syed [3]	Managerial support through blockchain	Reliability and tamper-proof handling of digital evidence can be achieved through a blockchain architecture	Custom workflows designed to specific forensic investigations.
E. Yunianto, Y. Prayudi, and B. Sugiantoro. [4]	Blockchain digital forensic cabinet	The decentralized storage provides the benefit of traceability and prevents it from being altered.	Implication of interoperability that goes hand-in-hand with the existing tools and systems of forensic analysis
Y. Borse, D. Patole, G. Chawhan, G. Kukreja, H. Parekh, and R. Jain. [5]	Blockchain-based forensic evidence handling	It ensures integrity due to transparency and enhances tamper-proofing	Focus on training and educating users to have a more effective and high-potential system
S. Patil, S. Kadam, and J. Katti [6]	Enhance forensic evidence security	Locks out unauthorized access and maintains the chain of custody.	Provide more advanced encryption techniques for sensitive evidence data
F. Tsai [7]	Chain of custody in criminal investigation	Exploiting the potential of blockchain to maintain an integrity of evidence	Determine a user-friendly application that makes the history of evidence traceable in real time
D. Billard [8]	Digital inventory of the evidence	Evidence with no lacuna for tracing and in its lifecycle	Automate reporting and alert at event lifecycle

S. S. Alqahtany, and T. A. Syed [9]	Co-existence of holistic blockchain approach in digital forensic	Transparency, accountability and treatment in an evidence fair manner	Community driven feedback input developed on continuous basis according to usability.
] A. O. Charles, A. Oguntimilehin, and O. A. Bello. [10]	Technological protection and safety system for evidence	It uses blockchain for clarity and tamper resistance.	Hybrid approach integrating two-factor authentication to block unauthenticated access
P. M. Dhulavvagol, S. G. Totad, and A. Anagal [11]	Blockchain sharding and IPFS for the management of evidence	It gives scalability, while its design is user-centered with ease of usability and accessibility.	The system utilizes the IPFS for redundancy and protection purposes with data, which makes it scalable with tamper-proof evidence handling.
D. Billard [12]	Blockchain-based evidence management weighing scale	It allows a huge volume of evidence to be managed using blockchain.	Focuses to encourage the availability of data for useful decision making concerning evidence.
A. O. Philip, and R. K. Saravanaguru [13]	Framework to implement an accident vehicle evidence management	It guards the extension of the framework for managing forensic evidence related to everything but vehicles.	The IoT-enabled system with blockchain smart contracts ensures that real-time evidence capture and secure tamper-proof storage occur.
Liza Ahmad, Salam Khanji, Farkhund Iqbal, and Faouzi Kamoun [14]	Blockchain-based chain of custody framework	Taps the private Ethereum for secure evidence management among stakeholders.	Find public blockchain-based solutions to increase accessibility and trust.
Zhihong Tian, Mohan Li, Meikang Qiu, Yanbin Sun, Shen Su [15]	Block-DEF framework for digital evidence	It addresses scalability as well as privacy issues while ensuring traceability with a lightweight blockchain.	Inclusion of machine learning in predicting tampering of evidence by certain patterns should be studied.

III. PROPOSED ARCHITECTURE

The EMS is, in fact, a beacon of change with regards to how evidence will be processed using blockchain technology; thus, it increases integrity, security, and access to evidence across the legal and regulatory spectrum. Conceptually, these structures decentralized storage infrastructure with smart contract functionalities, user-friendly interfaces, and more stringent network and hardware requirements. Let's take an in-depth look at the EMS architecture, exploring its core components, design principles, and operational mechanics.

Fig 1. Proposed System Architecture

A. *Decentralized Storage Infrastructure:*

Imagine that EMS has a decentralized storage infrastructure, anchored on blockchain technology. Such infrastructure would disperse evidence across a network of nodes, making the same redundant, resilient, and immutable. Each node, therefore, will have an in-sync copy of the evidence ledger; entry and retrieval of data are guaranteed to be both accurate and accessible when the nodes fail or the network faces disruptions.

For instance, building of this infrastructure requires careful selection of the right blockchain platform for things such as scalability, security, as well as developer support. Cryptographic hashing techniques and encryption mechanisms are then applied to prevent records from unauthorized access and alteration. Therefore, careful planning and execution will ensure that the decentralized storage infrastructure becomes the hub of trust and confidence in evidence management. A diagram of a diagram of a document

B. *Smart Contract Functionality:*

Therefore, the second one - smart contracts - the magic wand of the EMS. As I'll describe here, they deploy the functions of the EMS on the blockchain to automate the evidence management process. In such contracts, all the logic and commands for what must be done with evidence from its submission until its retrieval, access control, verification, and so forth. Indeed, smart contracts automate any process and enforce predefined rules, which makes them smooth out the workflows, ensures consistency, and transparency.

Therefore, creating and deploying smart contracts is a multi-dimensional process. Such constitutes designing, coding, testing, and deployment of the contracts so that they could be functional and robust with reliability and integrity. We do audits and code reviews to identify and fix vulnerabilities in the EMS ecosystem so that their smart contracts can be robust. We also implement mechanisms for upgrading and maintaining smart contracts so that they adapt

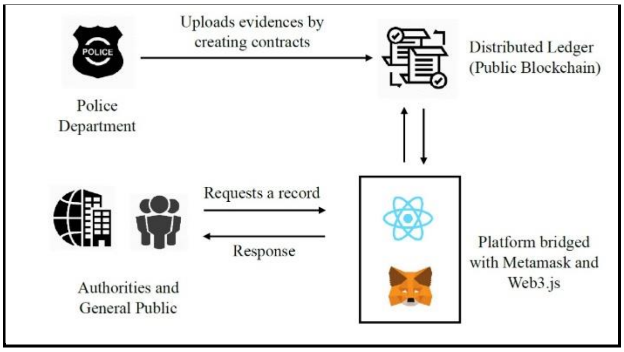

Fig 1. Proposed System Architecture

to the change and regulations in the future. Through rigorous development and testing, the smart contracts turn to be the only witnesses of trust and accountability to evidence management.

C. *User Interface Integration:*

Therefore, creating and deploying smart contracts is a multi-dimensional process. Such constitutes designing, coding, testing, and deployment of the contracts so that they could be functional and robust with reliability and integrity. We do audits and code reviews to identify and fix vulnerabilities in the EMS ecosystem so that their smart contracts can be robust. We also implement mechanisms for upgrading and maintaining smart contracts so that they adapt to the change and regulations in the future. Through rigorous development and testing, the smart contracts turn to be the only witnesses of trust and accountability to evidence management. 3. User Interface Integration:

Imagine availing of the EMS with a user-friendly interface-it is like a comfortable ride on a road that is well paved. This is a gateway for the submission, retrieval, verification, and audit trails of evidence. It is so designed that it is simple and accessible so that users will confidently navigate the EMS, confident in the process, of course.

The development of this interface is based on user-centric principles. We gather the feedback from users and conduct usability testing to polish it for it to be intuitive and more effective. Integrating the interface with tools like Metamask increases security and usability as authentication and transaction signing processes are made easier. With endless refinement and improvement, the user interface is that the bridge for connecting users with the EMS thus enhancing engagement and satisfaction.

D. *Network and Hardware Requirements:*

Now, some details about the nuts and bolts of EMS: network and hardware. We are building on top of the Ethereum blockchain and use Ethereum as a platform to keep records of evidence. Smart contracts issued in Solidity take care of evidence management. Of course, we support Clarity too for writing contracts on the Stacks blockchain. For optimal operation and reliability, we possess powerful resources in terms of computing capabilities, along with plenty of storage capacity.

Provisioning of network and hardware resources is quite a comprehensive task. We determine the appropriate configuration of infrastructure by assessing the scalability, performance, and security requirements. Load testing and capacity planning ensure that all the peak usage scenarios are provided for, which would then scale seamlessly with the EMS. Such investment in scalable infrastructure ensures operations of the EMS are efficiently scalable, reliable, and secure.

In essence, therefore, it represents an integrated and robust framework of evidence management that addresses many of the pressing issues but inculcates transparency, reliability, and trust in legal and regulatory processes.

IV. METHODOLOGY

The design and implementation methodology of the Evidence Management System is like choreographed dance, where every move is a step toward efficiency, effectiveness, and reliability every step of the way. Let's break down this methodology into six unified phases: every step along the road to shape the EMS into what it should be.

A. *Conceptualization and Requirements Analysis:*

EMS forming process is based on the definition of scope and objectives. In this phase, there is a collaborative effort between the stakeholders, that are lawyers, regulatory agencies, and end-users, that help paint the needs and expectations for the system. Workshops, interviews, and

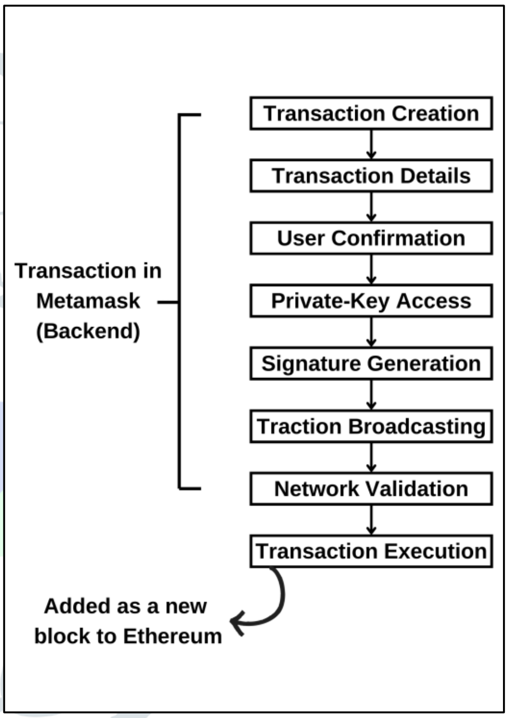

Fig 2. Transaction Initialization Phase.

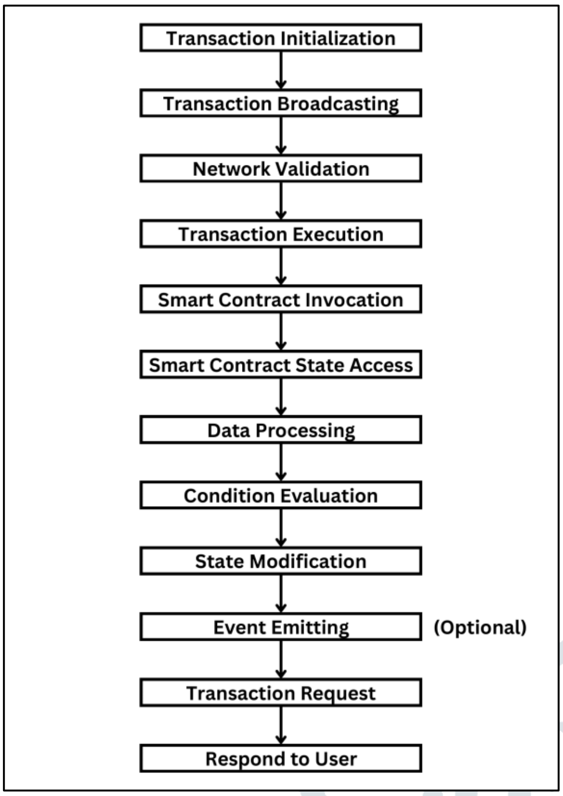

Fig 3. Smart Contract Execution Flow.

surveys it assists in the assembly of informed knowledge regarding the complexity of evidence management in various settings.

In requirements analysis, we take stakeholder inputs and transform them into explicit and actionable requirements. We differentiate functional requirements-the what of the EMS-from the non-functional requirements, which describe a quality of performance, security, or scalability, for example. We prioritize our requirements and line them up with the organizational goals we wish to obtain for effective implementation of the EMS.

B. Design and Architecture Planning:

We design the architecture of EMS with a keen knowledge of the stakeholder's requirements. As always, there is a blueprint delineating the structural elements and interfaces along with guidelines on how to work with this system. We use architectural patterns and designs that are modular, scalable, and maintainable along with good architectural and engineering practices.

All the decisions taken at the architecture planning level about the technology, platform compatibility, and points of integration are going to be very important. Considerations will include the blockchain platform chosen upon which we will operate - whether to be Ethereum or Stacks, the program language, the choice of which is being specifically used on the blockchain platforms: Solidity for Ethereum and Clarity for Stacks - and the UI framework. In this case, given the need for something like React, we evaluate what would best fit these EMS requirements in laying down a strong and scalable system by appropriately aligning the choices of technology with both the project goal and constraint.

C. Development and Implementation:

Now that we have set up the architecture, we are in the development stage where EMS is realizing as code and configuration. We use an approach that splits the functionalities of the system into smaller bits called user stories or features that we then implement piece by piece to receive continuous feedback and adapt the functionalities appropriately.

Agile methodologies, such as Scrum or Kanban, guide the development process to encourage teamwork, flexibility, and responsiveness to change. Designer/developer/domain expert cross-functional teams work within iterations/sprints to deliver incremental values. Continuous integration and deployment practices are followed; each increment of the EMS is thoroughly tested and thus ready for deployment.

D. Testing and Quality Assurance:

Testing and quality assurance are involved in the whole process in the cycle of development. This is for the assurance that EMS will operate at desired quality levels. In most methods of testing, there exist unit testing, integration testing, system testing, and acceptance testing. During unit tests, specific parts of a system may be verified to be working correctly; however, during integration tests, it verifies that interaction between those parts functions as it should. These are done to verify the complete behavior of the EMS, whether for functionality or performance, UI.User acceptance tests also engage stakeholders in validation that verifies whether the EMS meets the expected requirements of the stakeholders.

E. Deployment and Rollout:

Once testing is done and the EMS satisfies all the quality criteria, it is deployed into the production environment. The rollout plan also depends on the factors of system complexity and risk tolerance, considering that it impacts the users. There are two basic types of rollout strategies available: phased rollout, also sometimes referred to as blue-green deployment.

It becomes easier on how to deploy a system and ensures uniformity across different environments with the help of Ansible, Terraform, and others that stabilize a deployment script or an automation tool. Continuous monitoring and logging mechanisms will provide real-time visibility into the performance and health of the system with the help of tools like Prometheus and Grafana, while being initially rolled out and integrated.

F. Monitoring and Maintenance:

After deployment, EMS moves to a maintenance phase, which is merely just continuous monitoring and keeping in ideal performance and reliability of the system. Tools such as monitoring, including Datadog or New Relic, exist in that metrics and logs from various components of EMS will be collected in order to immediately notice and analyze a fault.

Regular activities include software updates, security patches, as well as database migrations to close the vulnerability, thus improving the stability of the system. There are also incident procedures: for example, on critical issues, and escalation protocols take care of minimizing downtime.

EMS stays agile and responsive in response to changing demands and challenges by monitoring and maintaining. The efforts of performance tuning and optimization ensure continuance in delivering value over time to satisfy stakeholder expectations.

Finally, the EMS design and implementation methodology calls for a structured and iterative approach to ensure that any system under development meets stakeholder needs effectively as well as delivers value in a consistent manner through best practices in every phase of the development lifecycle.

V. Results and Discussion

Deployment of the Evidence Management System, in essence, reveals its cost management and operational efficiency. The system is actually rather of a balance approach: it deals with high security and reliability, and even so, with resource usage at the low level. The balance at the initial stage is 0.24122754 ETH, while the total expense of deployment is only 0.02103833 ETH. Thus, it is shown that EMS is quite both resource-saving and secure.

Such an EMS based on the data obtained during deployment has been optimized for minimal use of gas directly contributing to saving cost. For instance, for the case of "Contracts" deployment, 922144 units of gas were consumed, equating to a value of 0.01877246 ETH, and with the "Migrations" contract, 226587 gas units were utilized in costing 0.00226587 ETH (Fig. 4. Cost Output). Such outputs manifest optimal use of gas that is critical to sustaining the overall cost-efficiency of blockchain operations.

In addition, the transaction details, as in Fig. 5. Transaction Details of these processes reiterate the kind of transactions that these processes conduct and ensure to optimize the cost aspect correctly. For example, a Sepolia Testnet transaction charged at 2.506898602 Gwei resulted in only 0.000473157055938684 ETH as the fee for that transaction, thus confirming that the system is indeed focused on cost optimization.

Low cost of deployment merged with high security and reliability, the EMS promises to be employed in a legal and regulatory environment where cost and security feature much. Unlike most systems, the EMS produces an immutable and verifiable record of all the actions, therefore keeping the integrity of the evidence because any change can trace back to a certain user. Additionally, the transparency feature combined with decentralization allows the system to find its place as a transformative tool in managing modern evidence.

This is what makes it stand out, given its focus on gas optimization, an approach that significantly lowers the operating cost without taking quality and dependability away. Among blockchain applications, the price of gas fees is one of the major operational costs, so this approach adopted by the EMS is rather useful for them. Considering all these synergistic aspects related to cost efficiency, security, and transparency gives the EMS an edge well above other evidence management solutions.

In summary, it is a true low-cost solution for evidence management that offers efficient deployment, strong security, and reliability at a very low cost, an excellent low-cost evidence management solution coupled with modern legal and regulatory environments, owing to its innovative gas optimization strategy coupled with a decentralized feature.

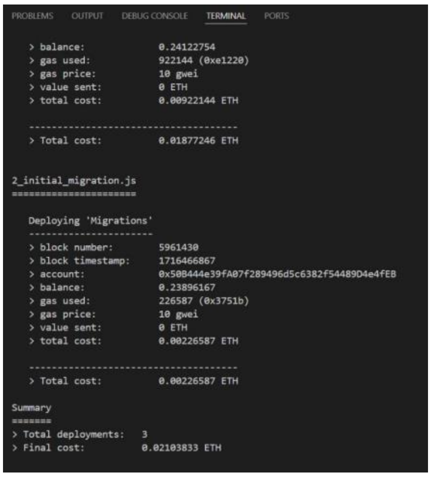

Fig 4. Cost Output

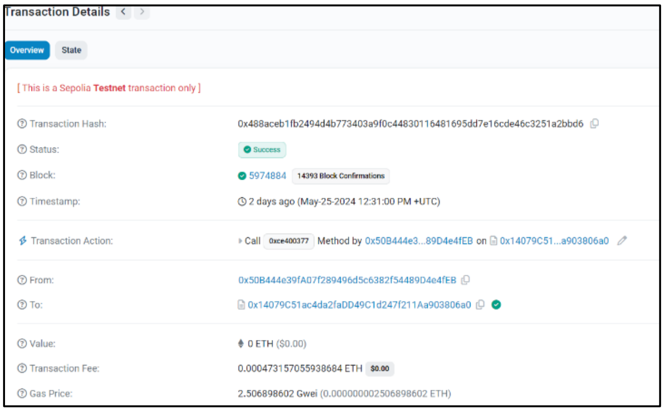

Fig 5. Transaction Details

VI. CONCLUSION

In short, the Evidence Management System is the greatest leap for evidence handling - pertaining to blockchain technology that manipulates integrity, security, and accessibility within a legal or regulatory sphere. Some of the most challenging problems in traditional evidence management systems are addressed through a carefully designed framework: transparency, reliability, and trust. Decentralized storage infrastructure, smart contracts that automate most of the processes, easy interfaces for users, and robust requirements of the network and hardware help this EMS to be a breakthrough standard in evidence management in the digital age. Looking forward, the EMS holds much promise to bring about widespread revolution in evidence management practices. Thus far, the EMS is scalable, reliable, and transparent for use by stakeholders across sectors. The system remains flexible and adaptable for more innovation as technology continues to advance and regulatory environments evolve.

VII. REFERENCES

[1] R. Sathyaprakasan, P. Govindan, S. Alvi, L. Sadath, S. Philip, and N. Singh, "An implementation of blockchain technology in forensic evidence management," in *2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, pp. 208-212, IEEE, 2021.

[2] M. Li, C. Lal, M. Conti, and D. Hu, "LEChain: A blockchain-based lawful evidence management scheme for digital forensics," *Future Generation Computer Systems*, vol. 115, pp. 406-420, 2021.

[3] S. Rao, S. Fernandes, S. Raorane, and S. Syed, "A novel approach for digital evidence management using blockchain," in *Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT)*, 2020.

[4] E. Yunianto, Y. Prayudi, and B. Sugiantoro, "B-DEC: Digital evidence cabinet based on blockchain for evidence management," *Int. J. Comput. Appl.*, vol. 181, no. 45, pp. 22-29, 2019.

[5] Y. Borse, D. Patole, G. Chawhan, G. Kukreja, H. Parekh, and R. Jain, "Advantages of blockchain in digital forensic evidence management," in *Proceedings of the 4th International Conference on Advances in Science & Technology (ICAST2021)*, 2021.

[6] S. Patil, S. Kadam, and J. Katti, "Security enhancement of forensic evidences using blockchain," in *2021 Third*

International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 263-268, IEEE, 2021.

[7] F. Tsai, "The application of blockchain of custody in criminal investigation process," *Procedia Computer Science*, vol. 192, pp. 2779-2788, 2021.

[8] D. Billard, "Blockchain-based digital evidence inventory," *Journal of Advances in Information Technology*, 2019.

[9] S. S. Alqahtany, and T. A. Syed, "ForensicTransMonitor: A comprehensive blockchain approach to reinvent digital forensics and evidence management," *Information*, vol. 15, no. 2, p. 109, 2024.

[10] A. O. Charles, A. Oguntimilehin, and O. A. Bello, "Forensic Evidence Security System using Blockchain Technology."

[11] P. M. Dhulavvagol, S. G. Totad, and A. Anagal, "SHARD-FEMF: adaptive forensic evidence management framework using blockchain sharding and IPFS," *Int. Arab J. Inf. Technol.*, vol. 21, no. 2, pp. 179-190, 2024.

[12] D. Billard, "Weighted forensics evidence using blockchain," in *Proceedings of the 2018 International Conference on Computing and Data Engineering*, pp. 57-61, 2018.

[13] A. O. Philip, and R. K. Saravanaguru, "Smart contract based digital evidence management framework over blockchain for vehicle accident investigation in IoV era," *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 7, pp. 4031-4046, 2022.

[14] Liza Ahmad, Salam Khanji, Farkhund Iqbal, and Faouzi Kamoun. 2020. Blockchain-based chain of custody: towards real-time tamper-proof evidence management. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES '20). Association for Computing Machinery, New York, NY, USA, Article 48, 1–8. https://doi.org/10.1145/3407023.3409199

[15] Zhihong Tian, Mohan Li, Meikang Qiu, Yanbin Sun, Shen Su, Block-DEF: A secure digital evidence framework using blockchain,Information Sciences,Volume 491, 2019, Pages 151-165, ISSN 0020-0255. https://doi.org/10.1016/j.ins.2019.04.011.

.