Block Evidence

BLOCK EVIDENCE

Nithin Raj [1015116216]

Nodirbek Islomov[101503673]

Harold Felipe Lara Gonzalez [101532704]

Submitted To: George Petrovic
Submitted On: August 14, 2024

Table of Contents

Introduction

Abstract

Among the biggest problems facing digital forensics is evidence tampering. In the chain of custody, many parties involved in the investigations may have access to the evidence and temporarily control it.

Therefore, the chain of custody must ensure that the evidence is not tampered with during the investigation process, considering that several entities will have access.

Currently, the process in the chain of custody is elaborated manually. This is because some documents must be completed and presented together with the evidence. For this reason, this project aims to use blockchain for the chain of custody procedure. This will help to maintain auditable control of the evidence that is collected. For this project, polygon will be used to elaborate the demo.

The idea behind Block Evidence is to leverage blockchain to create a tamper-proof record of all evidence-related activities. This will ensure that digital evidence is traceable, secure, and unaltered from the point of collection to its presentation in court.

This all arises from the idea of protecting the integrity of digital evidence, which is necessary to properly manage judicial procedures. Furthermore, how collection procedures are handled presents several vulnerabilities, which can compromise the integrity of evidence and lead to judicial errors.

Problem Statement

In digital forensics and cybersecurity, the preservation and authenticity of digital evidence is paramount. The methods currently used in handling and storing digital evidence have many vulnerabilities that can lead to modification, unauthorized access and possible tampering. These vulnerabilities or flaws in the security of proof not only compromise the effectiveness of legal proceedings but also pose a severe risk of miscarriages of justice for those handling the evidence and those involved in the events. Innocent people can be wrongfully implicated or convicted if the evidence presented against them has been altered or tampered with, either intentionally or through negligence. In addition, the lack of a transparent and verifiable chain of custody compounds these problems, making it difficult to trace the origins of tampering or establish the authenticity of evidence beyond doubt, which can cause a lack of trust among interested parties. As cyber threats evolve and digital data becomes increasingly important in investigations, the need for a better system to ensure digital evidence's absolute integrity, security and traceability becomes more apparent. This system must prevent tampering, protect against unauthorized access and provide a transparent and immutable chain of custody record to safeguard all individuals' rights and defend the judicial system.

Solution Overview

Block Evidence proposes to provide a secure, immutable and transparent system of managing digital evidence throughout a legal process to achieve this by creating tamper-proof records of all evidence. Each digital evidence (image) collected is hashed, and these hashes, along with detailed metadata, are recorded on the blockchain, which will ensure that once recorded, evidence cannot be altered without being tampered with, maintaining its integrity and admissibility in legal proceedings.

The use of smart contracts will assist with the interaction of evidence, from collection, analysis, storage and transfer to presentation in court.

Finally, this automated recording mechanism would provide a transparent and auditable trail showing who accessed the evidence and when ensuring that the chain of custody is maintained without tampering.

Business Opportunities

Proper management of the chain of custody is an important issue for various stakeholders, such as law firms, government agencies, and corporate legal departments. Block Evidence proposes using blockchain to guarantee the integrity, security, and transparency of information. For this reason, our strategy for financial projection will be based on subscription-based models.

1. Subscription-Based Model:
- Annual Subscription:
- Target Customers: Law firms, government agencies, corporate legal departments.
- Service: Unlimited access to the platform for evidence management and blockchain-based custody.
- Price per Subscription:
- Year 1-2: $50,000/year
- Year 3-5: $75,000/year
- Tiered Subscription:
- Tier 1 (Basic): Limited storage and user access. $25,000/year

- Tier 2 (Professional): Increased storage, user access, and priority support. $50,000/year
- Tier 3 (Enterprise): Unlimited storage, user access, dedicated support, custom integrations. $100,000/year
Projected Revenue from Subscriptions:
- Year 1: 5 clients $50,000 = $250,000
- Year 2: 12 clients $50,000 = $600,000
- Year 3: 20 clients $75,000 = $1,500,000
- Year 4: 25 clients $75,000 = $1,875,000
- Year 5: 30 clients $75,000 = $2,250,000
2. Pay-Per-Use Model:
- Per Evidence Upload:
- Target Customers: Smaller firms, individual investigators, and consultants.
- Service: Pay-per-upload of evidence to the blockchain.
- Price: $50 per upload.
- Per Transaction (Blockchain Logging):
- Target Customers: Ad-hoc users needing minimal engagement with the platform.
- Service: Pay-per-transaction for blockchain logging of evidence actions.
- Price: $10 per transaction.

Projected Revenue from Pay-Per-Use:
- Year 1:
- 2,000 uploads $50 = $100,000
- 10,000 transactions $10 = $100,000
- Year 2:
- 4,000 uploads $50 = $200,000
- 20,000 transactions $10 = $200,000
- Year 3:
- 8,000 uploads $50 = $400,000

- 40,000 transactions $10 = $400,000
- Year 4:
- 10,000 uploads $50 = $500,000
- 50,000 transactions $10 = $500,000
- Year 5:
- 12,000 uploads $50 = $600,000
- 60,000 transactions $10 = $600,000
3. Consultation and Setup Fees:
- Initial Consultation:
- Target Customers: New clients requiring initial setup and training.
- Service: In-depth consultation, platform customization, and staff training.
- Price: $25,000 per client.
- Custom Integration Fees:
- Target Customers: Enterprises requiring integration with existing systems.
- Service: Custom API development, integration with internal databases.
- Price: $50,000 per integration.
Projected Revenue from Consultation and Setup:
- Year 1: 10 clients $25,000 = $250,000
- Year 2: 15 clients $25,000 = $375,000
- Year 3: 20 clients $50,000 = $1,000,000
- Year 4: 25 clients $50,000 = $1,250,000
- Year 5: 30 clients $50,000 = $1,500,000

4. Licensing Fees:
- Platform Licensing:
- Target Customers: Third-party developers, legal tech companies.
- Service: Licensing the platform for integration into their products.
- Price: $100,000/year.
Projected Revenue from Licensing:

- Year 1: 2 licenses $100,000 = $200,000
- Year 2: 4 licenses $100,000 = $400,000
- Year 3: 6 licenses $100,000 = $600,000
- Year 4: 8 licenses $100,000 = $800,000
- Year 5: 10 licenses $100,000 = $1,000,000

5. Training and Support Services:

- Annual Training Packages:
  - Target Customers: Law firms, government agencies.
  - Service: On-site or virtual training sessions for staff.
  - Price: $10,000 per session.

- Premium Support Packages:
  - Target Customers: High-tier subscription clients.
  - Service: 24/7 support, dedicated account managers.
  - Price: $20,000/year.

Projected Revenue from Training and Support:

- Year 1: 10 sessions $10,000 = $100,000
- Year 2: 20 sessions $10,000 = $200,000
- Year 3: 30 sessions $20,000 = $600,000
- Year 4: 40 sessions $20,000 = $800,000
- Year 5: 50 sessions $20,000 = $1,000,000

6. Cybersecurity and Forensic Analysis Services:

- Cybersecurity Analyst Services:
  - Target Customers: Law firms, government agencies, large corporations.
  - Service: Advanced cybersecurity analysis and consultancy.
  - Price: $700/hour.

- Forensic Analysis Services:

- Target Customers: Forensic firms, private investigators.
- Service: Blockchain-based forensic analysis of digital evidence.
- Price: $500/hour.
Projected Revenue from Cybersecurity and Forensic Analysis:
- Year 3: $500,000 from cybersecurity analysis, $400,000 from forensic analysis.
- Year 4: $700,000 from cybersecurity analysis, $600,000 from forensic analysis.
- Year 5: $1,000,000 from cybersecurity analysis, $800,000 from forensic analysis.

Summary of Financial Projections:	
Total Revenue Projection (Detailed):	Net Profit/Loss:
- Year 1: $1,100,000	- Year 1: $680,000
- Year 2: $2,175,000	- Year 2: $1,515,000
- Year 3: $4,900,000	- Year 3: $3,900,000
- Year 4: $7,425,000	- Year 4: $6,030,000
- Year 5: $9,650,000	- Year 5: $7,860,000
Ongoing Costs (Post-Launch):	
- Year 1: $420,000	
- Year 2: $660,000	
- Year 3: $1,000,000	
- Year 4: $1,395,000	
- Year 5: $1,790,000	

Mission

At Block Evidence, our mission is to secure and simplify digital evidence management. Using blockchain, we guarantee that all digital evidence is protected, traceable, and transparent. By creating a tamper-proof system, we strive to avoid erroneous implications in legal proceedings. Our goal is to provide law enforcement agencies, forensic analysts and legal professionals with a reliable, secure and efficient tool to manage digital evidence, thus enhancing the trust and credibility of the judicial process for all stakeholders.

Use Case

Digital Evidence Chain of Custody and Integrity Verification Use Case

Actors Involved:

- Digital Forensics Analyst (DFA)
- Cybersecurity Analyst (CSA)
- Prosecutor
- Law Enforcement Officer
- Blockchain Platform

Scenario 1: Collection and Documentation of Digital Evidence

Step 1: Identification and Collection

Actor: Digital Forensics Analyst (DFA)

Action: DFA identifies digital evidence, such as files, images, documents, in the process of investigation. This evidence is obtained by forensic tools under write-blocking to ensure that during acquisition, there will be no change.

Blockchain Interaction: Digital evidence is hashed using a algorithm, for example SHA-256, to derive a unique digital fingerprint of the data. The hash and metadata (the collection timestamp, the analyst ID, location, etc.) are posted to the blockchain. The DFA acknowledges that the hash has been posted to the blockchain.

Step 2: Document

Actor: DFA

Action: Complete documentation of the evidence, how it was collected, and any environmental conditions that could possibly be relevant. Hashing will also be done on the documentation, and the hash recorded in the blockchain to be available for validation at any future date.

Blockchain Interaction: Metadata from the report along with the hash are placed on the blockchain. DFA confirms that the hash of the report is safe on the blockchain.

Scenario 2: Evidence Transfer between Analysts

Step 3: Request transfer

Actor: DFA

Action: The DFA should transfer the evidence to a CSA to be further analyzed. The DFA generates a blockchain smart contract for handling this transfer.

Blockchain Interaction: The smart contract utilizes digital signatures of DFA and CSA for verification of identity of both parties. It will record information related to the transfer—e.g., evidence hash, timestamps, and parties involved—in a smart contract.

Step 4: Confirmation of Transfer

Actor: CSA

Action: The CSA receives a notice to accept the transfer of evidence.

Blockchain Interaction: The CSA reviews the transfer information, confirming the receipt; the CSA confirms the details in relation to the evidence hash and other details in the blockchain. The confirmation is registered in the blockchain, updating the chain of custody.

Scenario 3: Authentication and Use in Court

Step 5: Pre-Trial Authentication

Actor: Prosecutor

Action: As a prerequisite for use in court, the Prosecutor shall verify the integrity of evidence. The Prosecutor browses the blockchain to retrieve hash values and transfer history of submitted evidence.

Blockchain Interaction: Chain of custody viewable in full, steps/actions from evidence submission related. The Prosecutor checks whether the current evidence hash matches the original one on the blockchain; the evidence has not been tampered with.

Step 6: Evidence Presentation

Actor: Prosecutor

Behavior: The Prosecutor presents the evidence in the court during the trial. Blockchain records of evidence collection and transfer are presented in the court to validate the integrity of evidence.

Blockchain Interaction: The logs of the blockchain cannot be tampered with and provide proof of the evidence's integrity and chain of custody. The court accepts the fact that the blockchain logs are part of the legal evidence.

Scenario 4: Post-Trial Archiving

Step 7: Long-Term Storage

Actor: Law Enforcement Officer

Action: After the trial, the evidence needs to be archived. The Law Enforcement Officer initiates the archival process through the blockchain.

Blockchain Interaction: A final hash of the archived evidence is created and stored on the blockchain. The evidence status on the blockchain is updated to "Archived" indicating that the chain of custody has ended.

Step 8: Future Retrieval

Actor: Authorized Personnel (e.g., future analysts, legal professionals)

Action: At any point in the future if there is a requirement to retrieve the archived evidence, the integrity can be validated using the blockchain.

Blockchain Interaction: The blockchain enables authorized personnel to verify that the evidence has not been tampered with since its archival.

Error Handling and Security Mechanisms:

Scenario 5: Error in the Evidence Upload Process

Step 9: Error Detection

Actor: DFA or System Administrator

Action: The error has been committed during the execution of the evidence hash file upload (for instance, erroneous hash or metadata mismatch). The system identifies the incongruence between the inputted evidence hash and the anticipated input.

Interaction with Blockchain: The blockchain will disallow the upload, tagging the file as to be reviewed by the DFA. Sends notification to DFA for error correction.

Step 10: Correction of Error

Actor: DFA or System Administrator

Action: The DFA corrects the error (e.g., Regenerate proper hash, Correct metadata) The corrected information is again uploaded to the blockchain.

Interaction with Blockchain: The new corrected hash is entered into the blockchain, updating the chain of custody. A record of the initial error and its resolution is maintained for auditing purposes.

Business Players

For blockchain implementation, the target market consists of various business players who are essential for its operation.

- **Expert Collector:**
  - **Purpose:** First person responsible for collecting, storing, and uploading digital evidence
- **Cybersecurity Experts:**
  - **Purpose:** Specialized team that handles more complex analyses of digital evidence.

- **Legal Professionals**
  - **Purpose:** A group of people would utilize digital evidence in court to build or defend cases.

- **Judges and Court Staff**
  - **Purpose:** Validate the admissibility and treatment of digital evidence in trials.

- **Target Industries and Companies:**
  - **Purpose:** These are the businesses across various sectors that frequently face cyber threats and attacks

Competitor Analysis

1. **Overview of CaseGuard:**
   CaseGuard is a Digital Evidence Management System (DEMS). It provides management tools for digital evidence, including redaction, case management, and secure storage.

   Key Features:

- Offers users an easy-to-use interface with integrated evidence management tools mainly for use by law enforcement users.
- Manages various media types and has built-in compliance capabilities with current legal standards.

- Uses robust encryption to ensure data security but is not based on blockchain.

Weaknesses:

- Limited without blockchain integration.
- Likely not scalable compared to a blockchain solution.

2. **Chainkit Summary:**
   Chainkit is a cybersecurity company using blockchain technology with tamper-evident logs for the protection of digital evidence.

   Strengths:

- Cybersecurity integrated seamlessly with the integrity of blockchain.
- Ideal tamper-evident logging fit for forensics.
- Integration with existing systems for an added layer of security. **Weaknesses:**
- More focused on logging as opposed to a complete evidence management system.
- Limited to certain use cases, which might not be sufficient for the wide set of needs in digital evidence management.

3. **Civic Ledger Overview:**
   Civic Ledger is an Australian company that leverages blockchain in different government services with secure document verification and record management.

   Strengths:

- Strong focus on government use cases that ensure compliance with regulations.
- Uses blockchain with transparency and immutability features for record management.
- Public sector solutions, which can be quite useful in regulated industries.

- **Weaknesses:**
- Lacks the specific tools needed for the domain of digital evidence management within cybersecurity and law enforcement.
- More general for government applications, not focused on the niche of digital evidence.

4. **Everledger Overview:**
   Everledger applies blockchain technology to valuable assets such as diamonds and fine wines for transparency and security in provenance.

   Strengths:

- A track record of successful deployments in using blockchain to prove an asset's authenticity.
- Strong emphasis on transparency and supply chain security that might translate well into evidence management.

Weaknesses:

- Primarily focused on supply chain transparency rather than the digital evidence sector.
- Lacks features specialized for law enforcement or legal enterprises.

5. **Parabon NanoLabs Introduction:**

Parabon NanoLabs is a DNA evidence enterprise that deals with analysis and identification. Although they are not direct competitors, their handling of digital forensic data is somewhat similar to what would be encountered through our tool.

Strengths:

- Specialized in the forensic analysis of genetic material, the most important part of any criminal investigation.
- High accuracy and reliability are ensured in DNA forensics.

Weaknesses:

- Not powered by blockchain technology and specialized only in DNA evidence, without providing broader digital evidence management tools.

Competitive Advantage:

Integration of Blockchain:

Generating an immutable and tamper-proof chain of custody by Block Evidence is a competitive advantage over traditional systems of managing digital evidence. This feature ensures data integrity to the highest order, and it proves to be a make-or-break attribute in legal situations.

Comprehensive Solution:

Unlike competitors, this platform provides a complete solution for the entire lifecycle of digital evidence, from collection through to presentation in court.

Scalability:

Blockchain's decentralized nature is much more scalable compared to conventional centralized systems.

Cybersecurity Focus:

With tamper-evident logs and secure transfer protocols, among others, Our platform strongly leans toward cybersecurity, thus fulfilling one of the core needs in modern digital forensics.

Market Positioning:

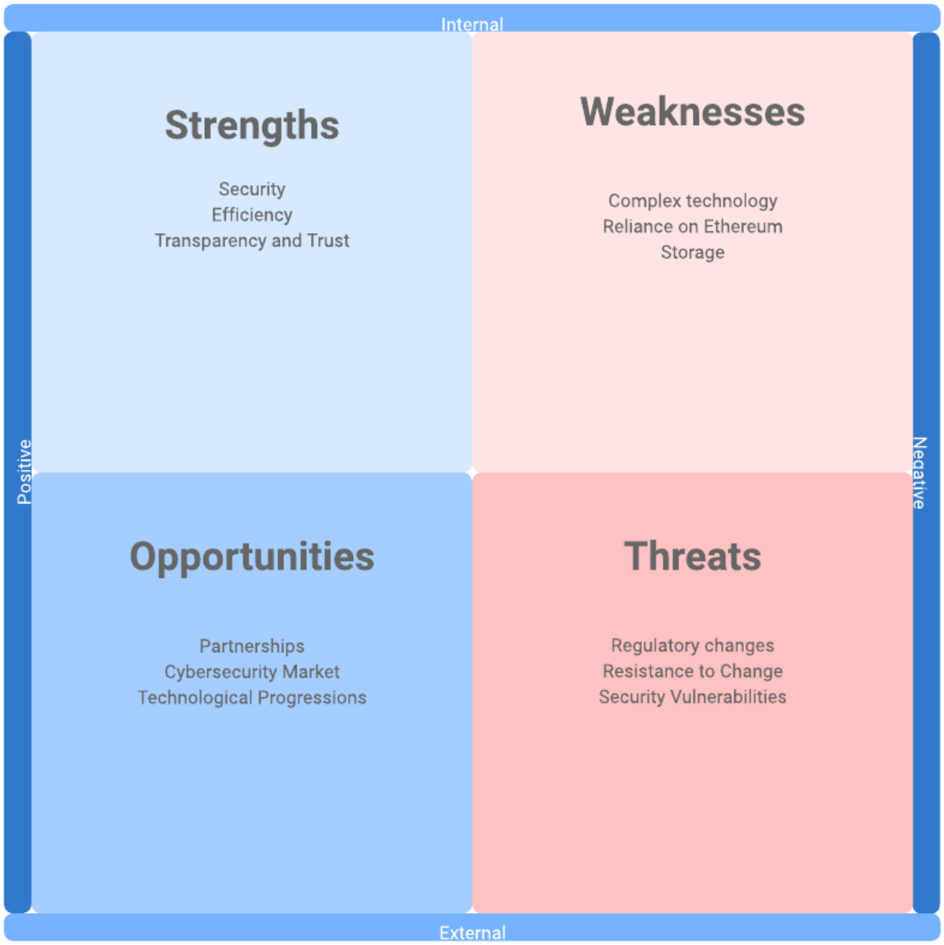
- **Niche Focus:**

Our platform can carve out a niche within the broader digital forensics market by focusing specifically on digital evidence in cyber investigations. Even though solutions like CaseGuard have provided general evidence management in the past, Our solution's blockchain underpinning offers a unique selling proposition to clients where data integrity and transparency are paramount.

- **Legal and Law Enforcement Integration:**

Emphasizing our platform’s use in legal settings can help differentiate it from competitors who may be emphasizing the corporate or government use case too heavily.

SWOT Analysis



Internal

Positive

Negative

Strengths

Security
Efficiency
Transparency and Trust

Weaknesses

Complex technology
Reliance on Ethereum
Storage

Opportunities

Partnerships
Cybersecurity Market
Technological Progressions

Threats

Regulatory changes
Resistance to Change
Security Vulnerabilities

External

Strengths:

- **Security:** blockchain features such as immutability and encryption will be used to protect digital evidence.
- **Efficiency:** The evidence-handling process will be optimized, reducing human error.
- **Transparency and Trust:** The evidence-handling process will be optimized, reducing human error. The chain of custody will be more secure, and its transparency will be verified.

Weaknesses:

- **Complex Technology:** Adopting blockchain technology may pose challenges in terms of implementation, training, and integration with existing systems.
- **Reliance on Ethereum:** For this first stage, we will use Polygon, which leads to specific weaknesses as it relies heavily on the Ethereum core network. If Ethereum faces problems or congestion, this may affect the use of Polygon.
- **Storage:** For this demo, we do not yet have the capacity to store large amounts of evidence, which may lead to bigger problems in the future.

Opportunities:

- **Partnerships:** there is the possibility of forming alliances with government agencies, legal entities and private organizations.
- **Cyber Security Market:** Growing cyber threats increase demand for solutions; this can create good opportunities for new functionality.
- **Technology Progression:** As previously discussed, there are great opportunities to create and implement new functionalities using blockchain.

Threats:

- **Regulatory Challenges:** Changes in data protection regulations could affect the implementation of the application.
- **Resistance to change** there is a possibility that some stakeholders may resist the use of blockchain technology.
- **Security Vulnerabilities:** Blockchain is not immune to all cyber threats that could compromise the integrity of the system and for this first phase we are counting on the weaknesses of using polygon.

Pestel Analysis

Political	Economical	Social	Technological	Legal	Environmental
1. Regulatory Changes 2. Government initiatives.	1. Market Differentiation 2. Cost of Implementation	1. Adoption of target market. 2. Education and training. 3. *Security Threats*	1.Blockchain Development 2. Integration with other systems	1. Data Protection 2Legal admissibility	1. Costly Energy Resources

Political:

- *Regulatory Changes:* If a change in the laws happened, it can compromise how the Smart Contract are developed.
- *Government Initiatives:* There is an opportunity to be funding by government since the project is involved judicial system.

Economical:

- *Market Differentiation:* Economic benefits if the blockchain solution provides a unique selling point.
- Cost of Implementation: the first investment can have a high cost which may affect the development of the project

Social:

- *Adoption of Target Market:* Resistance to change may affect the main users of the platform
- *Education and Training:* there should be training programs to bridge the knowledge gap.
- *Security Threats:* Technological risks, such as unauthorized access and potential attacks on the blockchain network.

Technological:

- Blockchain Development: Technological developments may affect the performance of smart contracts and may cause failures if not upgraded

- Integration with other System: For the future the project will be compatible with other forensics tools

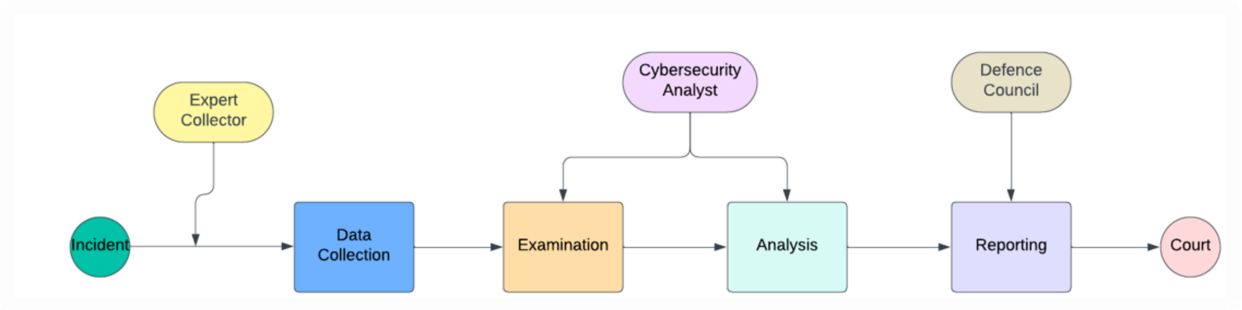
Legal:

- Data Protection: Caution must be taken with the manipulation of the data since the data protection law must be respected when uploading them in the blockchain.

Environmental:
Costly Energy Resources: Depending on the platform the project may consume a higher level of energy which can be an obstacle to public acceptance and environmental sustainability

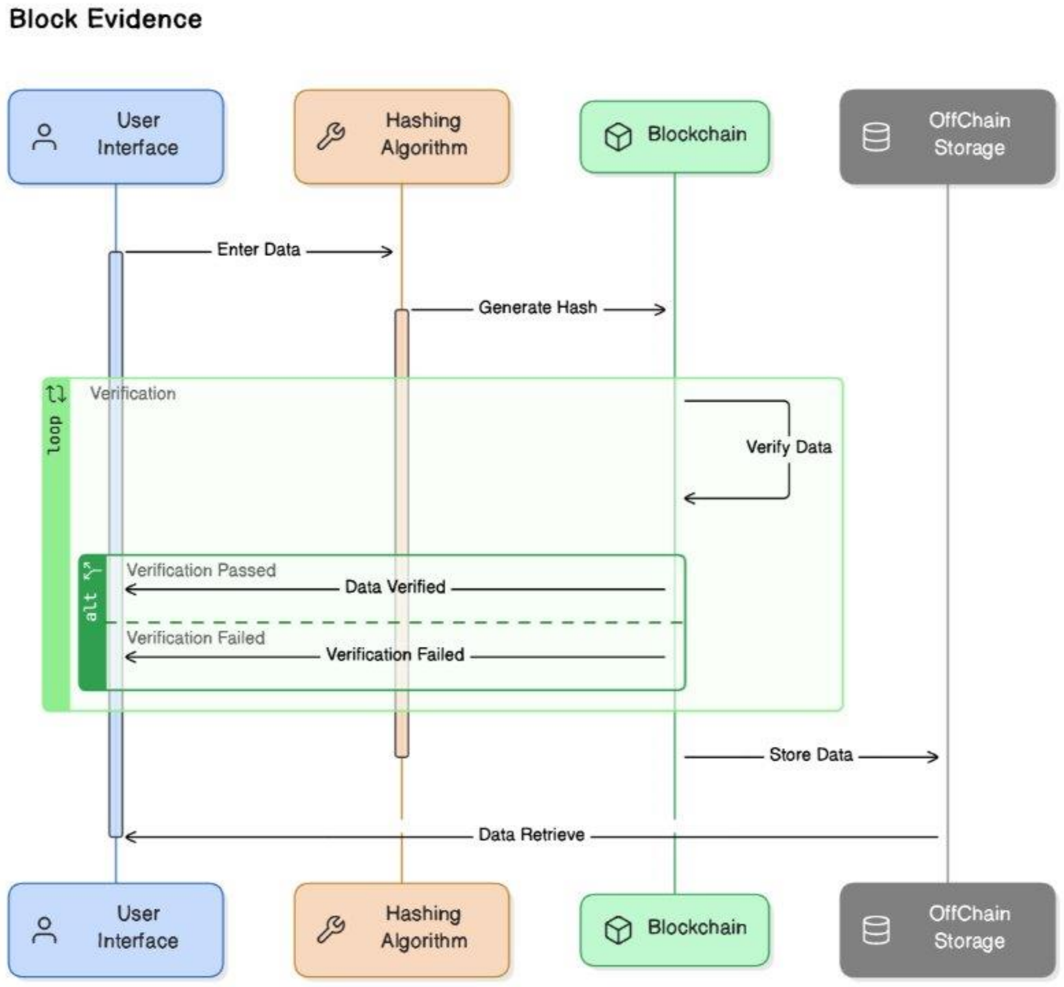
Implementation Details

The process starts after a cyber-attack at this time the company will hire a company that is using our tool to do chain of custody process, at this time an expert will be in charge of collecting the information and uploading it to the system through the application at this time the cyber security team will be in charge of examining and analyzing the information to find any type of evidence that can be used at the end they will have to upload it to the system which will make sure of the validity of the process finally it will be passed to the people in charge of the defense who will finally use the evidence in court and prove the truthfulness of the evidence found.



Technical Diagram

Architecture



Smart contract

1. Structures and Mappings:

Evidence Structure: Stores details about each piece of evidence, including its id, creator, owner, description, associated addresses, timestamps, logs, and an IPFS hash.
evidences Mapping: Maps an evidence ID to its corresponding Evidence structure.
accessControl Mapping: Manages access control for each piece of evidence, allowing the owner to grant or revoke access to specific addresses.

2. Modifiers:

OnlyOwner: Ensures that only the owner of the evidence can execute the function.

OnlyCreator: Ensures that only the creator of the evidence can execute the function.
EvidenceExists: Checks whether a piece of evidence exists or not, depending on the boolean flag mustExist.

3. Functions:

createEvidence: Allows a user to create a new piece of evidence with a unique ID and description. The creator and owner are set to the caller's address.
transfer: Allows the current owner to transfer ownership of the evidence to a new address.
removeEvidence: Allows the creator to remove the evidence record from the blockchain.
addLog: Enables the owner to add a log entry to the evidence, recording additional information.
setIpfsHash: Allows the owner to set or update the IPFS hash associated with the evidence, linking it to external data.
grantAccess: Grants viewing access to the evidence to a specified address.
revokeAccess: Revokes previously granted viewing access from a specified address.
getEvidenceBasic: Returns basic information about the evidence (ID, owner, creator, description) if the caller has access.
getEvidenceDetails: Returns detailed information about the evidence (associated addresses, timestamps, logs, IPFS hash) if the caller has access.

Conclusion

The Block Evidence project focuses on being a robust tool for digital evidence collection, ensuring the integrity, security and transparency of evidence by preventing unauthorized tampering and guaranteeing its authenticity throughout its use cycle. In addition, smart contracts and automated processes significantly reduce manual handling, minimize human error, and enable more efficient case management.

Block Evidence's continued development should focus on expanding its capabilities, improving the user experience and ensuring scalability to meet growing demands. In addition to creating its blockchain, as this project uses polygon as a foundation, collaborations with regulatory bodies can enhance applicability. In addition, the traceability of the chain of custody must always be considered.

References

[1]*Chain Research - How can blockchain technology be applied to CHA*. (n.d.). Chain. https://chain.com/blog/how-can-blockchain-technology-be-applied-to-chain-of-custody

[2]*How Many Innocent People are Jailed Each Year?* (n.d.). https://baldanilaw.com/innocent-people-jailed-each-year/

*[3]*PracticePanther. (2024, January 23). *Chain of custody for evidence using blockchain technology*. PracticePanther. https://www.practicepanther.com/blog/chain-custody-blockchain-technology/

*[4]*Pumphrey, D., Jr. (2022, February 6). *What are Chain of Custody Errors and How can They Impact my Criminal Case?* Pumphrey Law. https://www.pumphreylawfirm.com/blog/what-are-chain-of-custody-errors-and-how-can-they-impact-my-criminal-case/

[5]*What is Chain of Custody in Digital Forensics?* (2024, June 25). https://www.knowledgehut.com/blog/security/chain-of-custody-in-cyber-security

[6]Blockchain Use cases in Digital Sectors: A Review of the literature. (2018, July 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/8726506

[7]*Blockchain Technologies: The foreseeable Impact on society and industry*. (2017). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/8048633

[8]Gimenez-Aguilar, M., De Fuentes, J. M., Gonzalez-Manzano, L., & Arroyo, D. (2021). Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems*, *124*, 91–118. https://doi.org/10.1016/j.future.2021.05.007

[9]Fang, W., Chen, W., Zhang, W., Pei, J., Gao, W., & Wang, G. (2020). Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1). https://doi.org/10.1186/s13638-020-01665-w

[10]Gimenez-Aguilar, M., De Fuentes, J. M., Gonzalez-Manzano, L., & Arroyo, D. (2021b). Achieving cybersecurity in blockchain-based systems: A survey. *Future Generation Computer Systems*, *124*, 91–118. https://doi.org/10.1016/j.future.2021.05.007

[11]König, L., Unger, S., Kieseberg, P., Tjoa, S., Josef Ressel Center BLOCKCHAINS, & St. Pölten University of Applied Sciences. (2020). The Risks of the Blockchain: A review on current vulnerabilities and attacks. In *Journal of Internet Services and Information Security* (No. 3; Vols. 10–10, pp. 110–127). https://doi.org/10.22667/JISIS.2020.08.31.110

[12]Blockchain: Future of financial and cyber security. (2016, December 1). IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/7918009

[13]Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., & Choo, K. R. (2020). A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), 147–156. https://doi.org/10.1016/j.dcan.2019.01.005

[14]CaseGuard AI Redaction Software. (2024, August 9). *Best AI Redaction Solution | CaseGuard*. CaseGuard. https://caseguard.com/

[15]ChainKit Integrity Automation Platform | Carahsoft. (n.d.). Carahsoft. https://www.carahsoft.com/chainkit

[16]Everledger. (2022, October 12). *Main home - Everledger*. https://everledger.io/

Appendix

https://github.com/GBC-BCDV-Capstone-BlockEvidence/block-evidence