The importance of Blockchain in cybercrime and digital investigations

Amna Ali MAdkhali

Abstract

Cybercrime has become one of the most critical challenges in the digital age, with traditional security measures proving insufficient in preventing cyberattacks and data breaches. This research explores the role of blockchain technology as a solution to enhance cybersecurity, prevent unauthorized access, and secure sensitive digital records.

Through a comprehensive analysis of real-life cybercrime cases, this study highlights the vulnerabilities in centralized data management systems. A practical implementation was conducted using smart contracts and blockchain-based evidence management, demonstrating the benefits of decentralization, immutability, and transparency in digital investigations. Additionally, the research proposes two innovative blockchain solutions.

While blockchain presents promising advantages in securing digital ecosystems, challenges such as scalability, regulatory compliance, and adoption barriers remain. Addressing these limitations requires collaboration between policymakers, technology developers, and cybersecurity experts to fully integrate blockchain into digital forensics and cybersecurity strategies.

This research concludes that blockchain is not only a tool for financial transactions but a transformative technology capable of reshaping the future of cybersecurity by providing enhanced security, accountability, and trust in digital systems.

Introduction

Digital technology is an essential element in our daily lives, and has become an integral part of our personal and professional dealings alike. With the acceleration of technological development in the modern world, information is now transmitted across digital platforms in real time, which has brought about a radical change in various sectors, from education and health care to business. Digital technology has become the main driver of our current era, as modern technology has come to play a pivotal role in shaping the future of societies.

However, as is the case with any development, this spread has negative side effects, the most prominent of which is the emergence of what is known as cybercrime. Criminals have taken advantage of technological progress to carry out electronic attacks targeting individuals and institutions, with the aim of obtaining sensitive information or making illegal financial gains. These crimes, which include hacking, electronic fraud, and digital espionage, now threaten the security of digital societies and greatly affect trust in digital systems.

Therefore, cybercrime has become one of the most serious challenges facing the digital world in the modern era. As the spread of technology and the dependence of individuals and companies on the Internet in all aspects of life, has led to the emergence of a group of electronic threats targeting personal and financial information and data. Definition of cyber crimes

Cybercrime is any criminal activity carried out using digital technology to target individuals, organizations, or government systems. These crimes differ in their goals and methods, but they all have in common a reliance on the Internet as a means of execution. Forms of cybercrime

Cybercrime includes different types of attacks that can affect individuals and businesses. The most prominent of these forms are:

1. Hacking: Unauthorized entry into electronic systems or accounts, stealing data, or disrupting services.

2. Email fraud: Using fake email or websites to deceive individuals and obtain their financial information.

3. Electronic blackmail: threatening victims with publishing sensitive information in exchange for paying a ransom.

4. Virus and malware attacks: Deploying malicious software to disable devices or steal information.

5. Identity theft: using victims' personal data to commit other crimes, such as opening bank accounts or carrying out financial transactions in their name. Cybercrime greatly affects individuals and businesses alike. On the individual side, these crimes can lead to significant

financial losses and violations of privacy. As for companies, cybercrimes may cause a loss of customer trust, leak sensitive information, and incur huge financial losses.

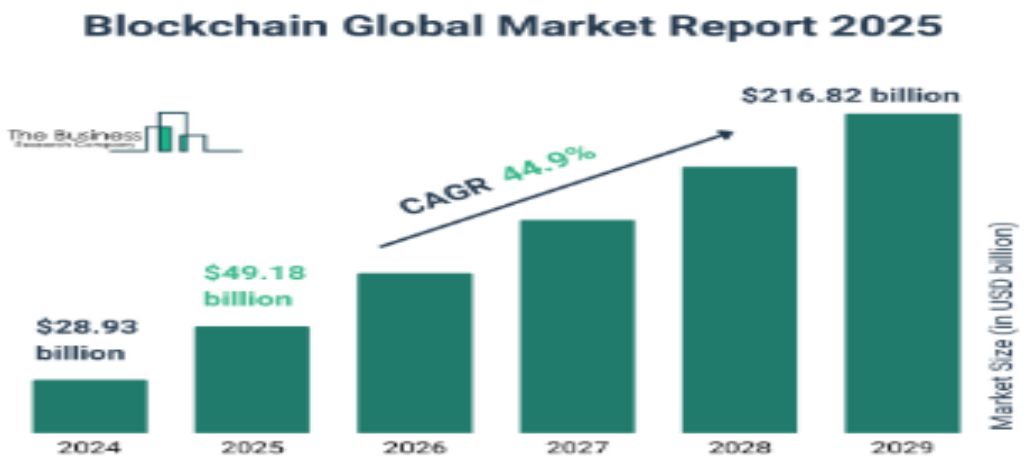
Real-life cases of cybercrime

One of the most prominent examples of cybercrimes that have occurred in recent years is the MOVEit hack case in 2023, which is one of the largest hacks in history. Hackers exploited a security vulnerability in a file transfer service, leaking sensitive information belonging to more than 60 million people around the world.

Such cases are evidence of the importance of protecting digital data and adopting more secure technologies, such as blockchain technology, to reduce cybercrime and secure digital investigations. For businesses, cybercrimes can result in significant financial losses, a decline in client trust, and the leakage of private data.

Blockchain technology has emerged as one of the most revolutionary advancements in the digital age, offering a decentralized and highly secure system for managing and storing data. Originally developed as the backbone for cryptocurrencies like Bitcoin, blockchain has rapidly evolved to become a powerful tool with applications across various fields, including finance, healthcare, supply chain management, and digital security. At its core, blockchain is a distributed ledger technology that records transactions across multiple nodes in a way that ensures transparency, immutability, and protection against unauthorized alterations

Given the increasing challenges posed by cybercrime, blockchain provides a promising solution to secure digital ecosystems. Its decentralized structure eliminates the reliance on a single point of failure, making it resilient to hacking attempts. Moreover, the cryptographic mechanisms employed in blockchain ensure the integrity and confidentiality of sensitive data. These unique features position blockchain as a critical technology capable of transforming the way organizations safeguard information and conduct digital investigations, offering a robust defense against cyber threats while fostering trust in digital platforms. The chart below highlights the rapid growth of the blockchain market, reflecting its increasing adoption as a robust defense mechanism against cyber threats



With the rapid growth of digital technologies, cybercrime has become a major threat to individuals, businesses, and governments. From large-scale data breaches to sophisticated

hacking attacks, these crimes have exposed vulnerabilities in traditional systems and emphasized the need for innovative solutions. Blockchain, with its decentralized and tamper-resistant nature, offers a promising approach to addressing these challenges.

Related Work

Several studies have explored the integration of blockchain technology into cybersecurity and digital investigations. Zyskind et al. (2015) proposed a decentralized personal data management system using blockchain, emphasizing privacy and user control, which laid a foundation for later developments in data security. Similarly, Li et al. (2018) analyzed the applicability of blockchain in healthcare data sharing, highlighting its potential in protecting sensitive records—an approach aligned with this research's case study on healthcare data breaches. In the context of cybercrime, Conti et al. (2018) discussed how blockchain can assist in forensic investigations by providing immutable logging of digital events. Their findings support the idea that blockchain's transparency and traceability offer significant advantages for evidence management, a concept further demonstrated in the smart contract implementation section of this study. Moreover, recent works such as Casino et al. (2019) have conducted systematic reviews of blockchain in cybersecurity, identifying its strengths in resisting data tampering and securing communications across distributed systems. Their analysis also noted challenges such as scalability and legal compliance, issues that are echoed in this research. Despite these valuable contributions, most existing literature either focuses on financial applications of blockchain or general cybersecurity improvements, without providing detailed real-life implementations or sector-specific solutions. This study addresses that gap by presenting practical blockchain-based solutions tailored for cybercrime prevention, such as device registration and secure digital identity, backed by real-world cases like the MOVEit and Shields Health Care Group breaches.

This section explores **real-life cases of cybercrime**, illustrating the weaknesses in current digital infrastructures. It also highlights how blockchain technology can serve as a transformative tool to mitigate these risks, providing secure, transparent, and efficient solutions that restore trust in digital ecosystems.

1. MOVEit Case

Description of the Case:

The MOVEit hack is considered one of the most significant cybercrime incidents in recent history, impacting over 60 million individuals globally. Hackers exploited a vulnerability in the MOVEit file transfer service, which led to the exposure and leakage of sensitive information. This attack highlighted the vulnerabilities in centralized file transfer systems and the growing threat of cyberattacks.

Impact of the Case:

• Financial Losses: Affected organizations incurred massive expenses to mitigate the breach, restore operations, and compensate victims.

• Erosion of Trust: Clients lost confidence in the affected companies, damaging their reputations and customer relationships.

• Increased Fraud Risk: Leaked personal information exposed individuals to risks of identity theft and financial scams.

Solution Using Blockchain Technology:

Blockchain technology offers robust solutions to prevent such breaches:

• Encryption and Access Tracking: Sensitive data can be encrypted and stored securely, ensuring only authorized users can access it. Blockchain provides a tamper-proof record of all access attempts.

• Decentralization: Instead of relying on a centralized system, data is distributed across a blockchain network, reducing the risk of a single point of failure.

• Auditability: Every transaction and access attempt is logged transparently, enabling efficient detection and tracking of unauthorized activities.

Potential Results:

• Enhanced security and reduced likelihood of similar breaches in the future.

• Increased customer confidence due to the transparency and resilience of blockchain systems.

• Significant reduction in fraud risks by limiting unauthorized access to sensitive data.

Critical Analysis:

While blockchain offers promising solutions, implementing it on a large scale may face challenges such as:

• High initial deployment costs.

• Integration issues with existing systems.

• Need for widespread adoption and technical expertise to maximize its potential.

2. Shields Health Care Group Data Breach

Description of the Case:

In 2023, Shields Health Care Group experienced a data breach that exposed sensitive data of over 2.3 million patients. The leaked information included Social Security numbers, dates of birth, and health records, highlighting the vulnerabilities of centralized data storage systems in the healthcare sector.

Impact of the Case:

• Privacy Violations: The breach compromised patients' confidentiality, leading to significant distress and loss of trust.

• Operational Challenges: The company faced lawsuits and regulatory scrutiny, straining its resources.

• Healthcare System Risks: This incident undermined public trust in digital health systems, causing reluctance among patients to share their personal data.

Solution Using Blockchain Technology in the Healthcare Sector:

• Storing Sensitive Data on Blockchain:

• Blockchain provides encrypted and decentralized storage for sensitive data, reducing the risk of breaches.

• Key features: 1. Encryption: Ensures only authorized individuals can view the data.

2. Decentralization: Eliminates single points of failure by distributing data across the network.

3. Immutability: Prevents unauthorized modifications to patient records.

• Data Access Management Using Smart Contracts:

• Patients control access to their data using private keys.

• Smart contracts allow temporary access for healthcare providers, which expires automatically after a predefined period.

• All access attempts are transparently logged on the blockchain.

• Practical Example:

• A patient visiting a new doctor can use a smart contract to grant temporary access to specific medical records. The doctor cannot exceed the granted permissions, and the system ensures traceable interactions.

Potential Results:

• Restored trust in digital health systems due to enhanced transparency and security.

• Minimized risk of privacy violations by empowering patients with control over their data.

• Reduced financial and legal liabilities for healthcare providers.

Critical Analysis:

Although blockchain is highly effective, its adoption in the healthcare sector comes with challenges:

• Scalability: Storing large volumes of data on the blockchain can be expensive.

• Regulatory Compliance: Adapting blockchain solutions to comply with healthcare laws (e.g., HIPAA) requires careful design.

• Interoperability: Integrating blockchain with existing healthcare systems requires technical advancements.

By applying blockchain technology, both cases demonstrate how this innovation can provide secure, transparent, and tamper-proof systems to combat cybercrime. While challenges exist, the potential benefits significantly outweigh the obstacles, paving the way for a more secure digital future.

Practical Implementation of Blockchain Technology

To further demonstrate the practical application of blockchain technology in addressing cybercrimes, this section presents a real-world implementation using a smart contract. The primary goal of this implementation is to illustrate how blockchain can be utilized to secure

sensitive data, track access, and ensure transparency in digital investigations. Tools and Environment The implementation was carried out using the following tools:

• Remix IDE: A browser-based integrated development environment for writing, compiling, and deploying smart contracts written in Solidity.

• Ganache: A personal blockchain for Ethereum development that allows for testing and deploying smart contracts locally before moving to a live network. Building the Smart Contract The developed smart contract focuses on creating a registry for managing sensitive data securely. The contract allows for adding, retrieving, and tracking evidence or sensitive records in a decentralized manner, ensuring that no single entity has control over the data. Key functionalities of the smart contract include:

1. Data Registration: Authorized users can add sensitive records to the blockchain.

2. Data Access: Users can retrieve records through unique identifiers, ensuring that only authorized individuals can access the data.

3. Transparency: Every transaction and modification is recorded on the blockchain, creating a tamper-proof history of activities. Example Code Below is a simplified snippet of the smart contract:

pragma solidity ^0.8.0; contract EvidenceRegistry { struct Evidence { string description; uint256 timestamp; address addedBy; } mapping(uint256 => Evidence) public evidences; uint256 public evidenceCount; function addEvidence(uint256 id, string memory description) public { evidences[id] = Evidence(description, block.timestamp, msg.sender); evidenceCount++; } function getEvidence(uint256 id) public view returns (string memory, uint256, address) { Evidence memory evidence = evidences[id]; return (evidence.description, evidence.timestamp, evidence.addedBy); } }

Deployment and Testing

1. Deploying the Contract: The smart contract was deployed using Remix IDE on a local Ethereum blockchain provided by Ganache.

2. Adding Evidence: After deployment, the addEvidence function was tested by adding sample records. The records included a description of the data, a timestamp, and the user's address.

3. Retrieving Evidence: The getEvidence function was used to verify the data stored on the blockchain. Each retrieval was logged and could be traced back to the original entry.

Results and Analysis The implementation demonstrated the following:

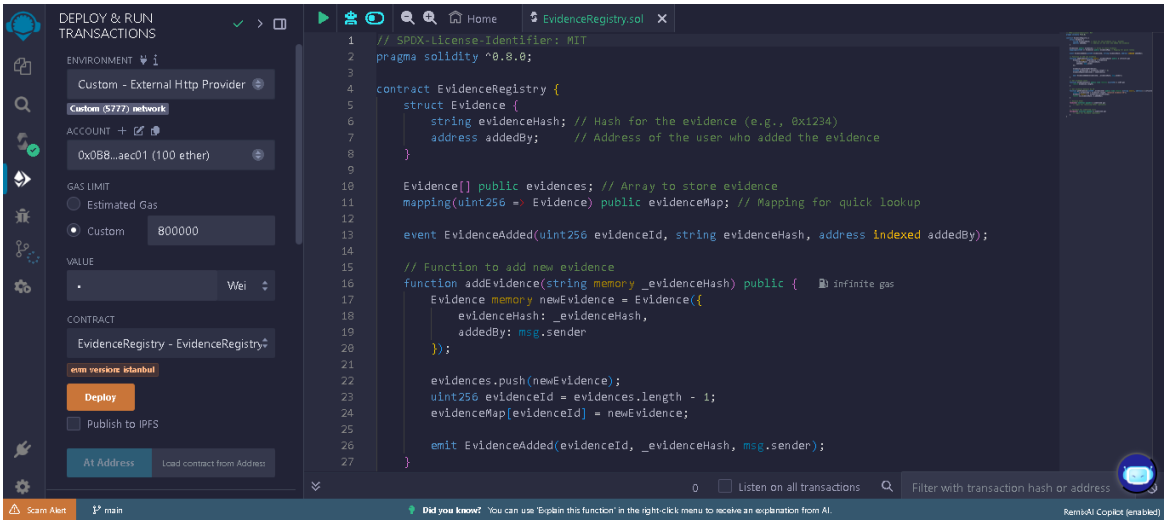
1. Decentralization: Sensitive data was stored across multiple nodes, eliminating the risk of a single point of failure.

2. Transparency: Each interaction with the smart contract was recorded on the blockchain, ensuring accountability and traceability.

3. Data Security: The use of cryptographic hashing and decentralization protected the data from unauthorized access and tampering. Limitations and Future Enhancements While the smart contract effectively secured and tracked sensitive data, there are some limitations:

1. Scalability: Storing large amounts of data on the blockchain can be inefficient due to storage costs. Future implementations could use off-chain storage with blockchain integration.

2. Access Control: Advanced mechanisms, such as multi-signature access and role-based permissions, could further enhance security. The practical implementation of a blockchain-based smart contract illustrates its potential to revolutionize data security in digital investigations. By ensuring decentralization, transparency, and immutability, blockchain provides a robust solution to combat cybercrimes and protect sensitive information.



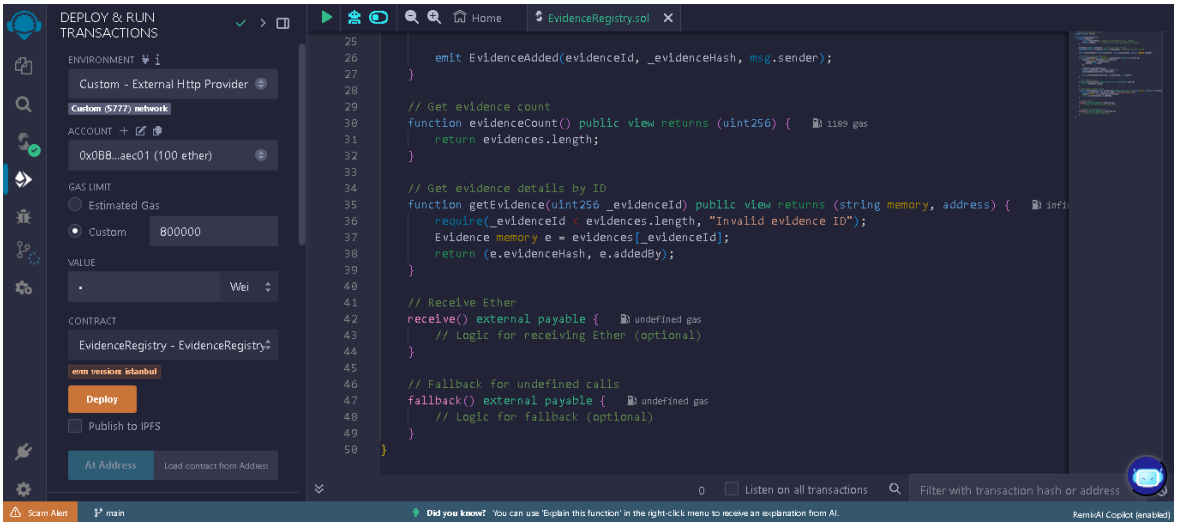


Figure 1 and 2: Deployment.

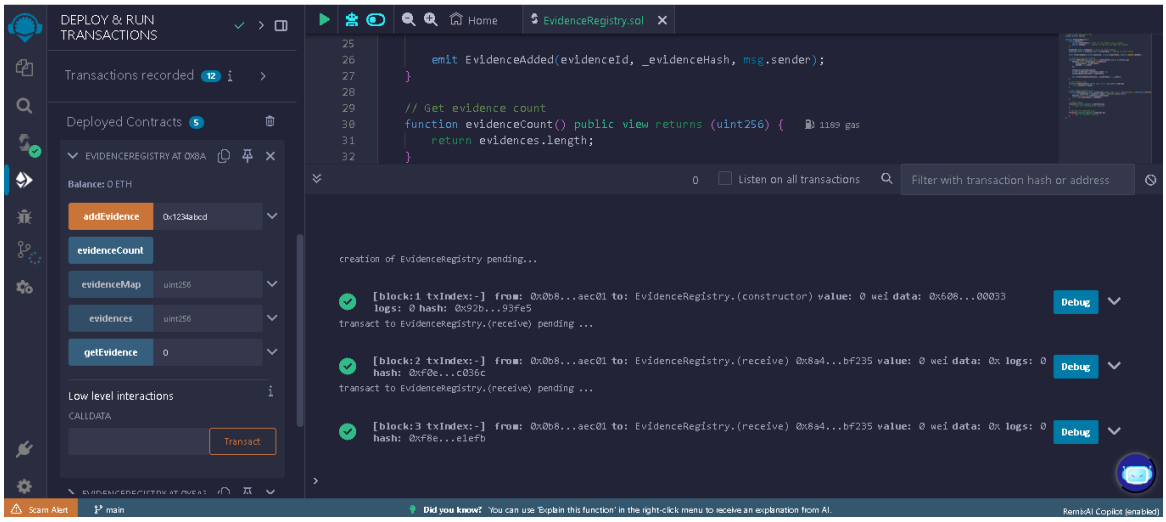


Figure 3: Output Successfully.

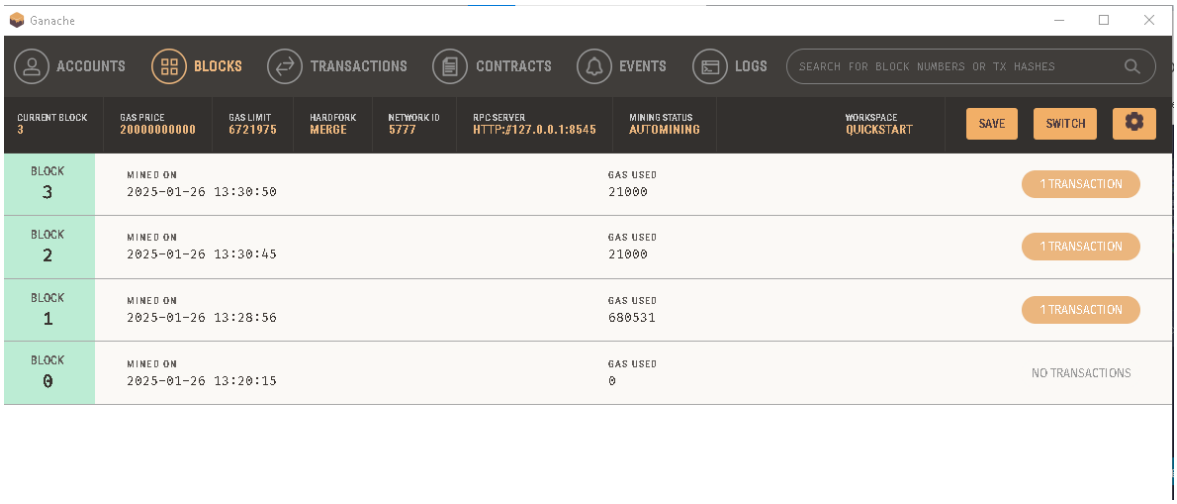


Figure 4: Execution of the smart contract on Ganache.

Blockchain-Based Solutions

As cybercrime continues to evolve, traditional security measures have proven insufficient in preventing unauthorized activities such as digital fraud, device misuse, and identity theft. Blockchain technology offers innovative solutions to enhance security, ensure data integrity, and improve accountability in digital systems. This section explores two proposed blockchain-based solutions: 1- registering electronic devices on a blockchain network to prevent criminal misuse and 2- creating secure digital identities to eliminate fake accounts on social media platforms.

1. Device Registration on Blockchain

Concept and Implementation

One of the major challenges in digital investigations is identifying the device used in cybercrimes, especially when criminals use unregistered or stolen devices. By integrating blockchain technology into the registration process of electronic devices, such as laptops

and smartphones, their serial numbers can be securely linked to the owner's verified identity.

How It Works

1. When purchasing a new device, its serial number is recorded on a blockchain ledger, linked to the owner's digital identity.

2. The record is encrypted and stored in a decentralized network, ensuring that it cannot be altered or deleted.

3. In case of a cybercrime incident, law enforcement agencies can request access to the blockchain database to trace the device ownership and investigate its usage.

4. If a device is reported stolen or misused, the blockchain network can prevent unauthorized resale by verifying ownership history.

Potential Impact

• Enhanced Cybercrime Investigations: Allows authorities to trace and identify devices used in illegal activities.

• Reduced Device Theft & Resale Fraud: Blockchain records ensure stolen devices cannot be resold without detection.

• Strengthened Digital Accountability: Ensures that individuals are responsible for the devices linked to their identity.

Challenges & Considerations

• Privacy Concerns: Users may hesitate to link their personal identity to their devices due to privacy risks.

• Integration with Law Enforcement: Authorities must develop secure access mechanisms to request information without violating data privacy.

• Adoption by Manufacturers: Device manufacturers need to adopt blockchain-based registration as a standard practice.

2. Creating Encrypted Digital Identities

Concept and Implementation

Social media platforms struggle with the rise of fake accounts, which are often used for scams, misinformation, and cyberbullying. Traditional verification methods, such as email or phone number authentication, are easily bypassed. Blockchain-based digital identities offer a secure and tamper-proof solution to eliminate fake accounts while preserving user privacy.

How It Works

1. Users create a blockchain-based identity that serves as a unique, verifiable credential.

2. Instead of storing personal details on centralized databases, the identity is stored on a decentralized ledger, reducing the risk of data breaches.

3. When signing up for an online service (e.g., a social media account), users verify their identity through a zero-knowledge proof system, confirming authenticity without revealing personal data.

4. Each account is linked to a verified blockchain identity, preventing the creation of multiple fraudulent accounts.

Potential Impact

• Eliminating Fake Accounts: Ensures that only real individuals with verified identities can create accounts.

• Protecting User Privacy: Unlike traditional identity verification, blockchain verification does not expose sensitive personal data.

• Enhancing Trust in Digital Interactions: Increases credibility across online platforms by reducing identity fraud.

Challenges & Considerations

• User Adoption: Encouraging widespread adoption of blockchain-based identities may require collaboration between governments and private sectors.

• Platform Integration: Social media companies must integrate blockchain verification systems without compromising user experience.

• Regulatory Compliance: Ensuring blockchain-based digital identity systems comply with global data protection laws.

Blockchain technology presents groundbreaking solutions to long-standing cybersecurity challenges. By implementing device registration systems and digital identity verification, it is possible to improve accountability, reduce cyber fraud, and enhance digital security. However, for these solutions to be effective, collaboration between technology providers, regulators, and law enforcement agencies is essential to ensure a balance between security, privacy, and usability.

Conclusion

As cyber threats continue to evolve, traditional security measures have proven inadequate in protecting digital assets and sensitive information. This research has highlighted the increasing risks of cybercrime, as seen in real-world cases such as the MOVEit hack and the Shields Health Care Group data breach. These incidents underscore the vulnerabilities present in centralized systems and the urgent need for more secure and transparent solutions. Blockchain technology offers a promising alternative by providing decentralization, immutability, and enhanced security. Through practical implementation, this study demonstrated how smart contracts and blockchain-based solutions can improve data protection, prevent unauthorized access, and strengthen digital investigations. Additionally, novel approaches such as device registration on blockchain and secure digital

identities were proposed to further enhance accountability and reduce cyber fraud. Despite its potential, blockchain adoption faces challenges, including scalability, regulatory compliance, and integration with existing infrastructures. Overcoming these obstacles requires collaboration between governments, businesses, and technology providers to develop standardized frameworks that balance security, privacy, and efficiency. In conclusion, blockchain is not merely a financial tool but a transformative technology capable of reshaping cybersecurity and digital forensics. As organizations and institutions seek more resilient security solutions, integrating blockchain into cybersecurity strategies will play a crucial role in safeguarding digital ecosystems against future threats.