The Influence of Blockchain Technology on Data Security, Attribution and Traceability in Digital Forensics in Extenuating Cybercrime.

Eseyin Joseph B.
Veritas University Abuja Jos Nigeria.
Bwari Abuja, Nigeria.

Onah Juliana Obianuju.
Veritas University Abuja Jos Nigeria.
Bwari Abuja, Nigeria.

Falana Moses O.
Veritas University Abuja Jos Nigeria.
Bwari Abuja, Nigeria.

Ogbonna Chukwudi N.
Veritas University Abuja Jos Nigeria.
Bwari Abuja, Nigeria.

Abstract
Blockchain technology is an innovative database tool that permits obvious information allocation within a business link. A blockchain database stocks records in hunks that are allied together in a fetter. The data is chronologically unswerving as data can't be modified or deleted in the chain lacking consent in the network. Therefore, it produces an irreversible or unassailable ledger for trailing orders, outflows, accounts, and extra dealings. The system has an integrated mechanism that prevents unsanctioned pact items and creates steadiness in the pooled assessment of these transactions. In a centralized network, data security is not efficient and once data is lost digital evidence suffers the effect. However, a decentralized approach is being proposed because each member or participant of the blockchain construction has entree to the unabridged dispersed database. Data provenance makes it conceivable to trail the derivation of every deal inside the blockchain ledger. Blockchain communications are corroborated and reliable due to the multifaceted computations and cryptographic proof among tangled parties. Hence, any annals in a blockchain can't be altered or scrubbed as a result of the immutability technique. This proposal presents a blockchain-based charter for ensuring secure data provenance and traceability in digital forensics. The framework leverages blockchain technology to create an immutable and transparent data origin, processing, and analysis record. The goal is to enhance the reliability and trustworthiness of digital evidence in criminal investigations and legal proceedings. The research aims to contribute to developing a reliable and trustworthy digital forensic process, ultimately supporting the investigation and prosecution of cybercrimes.

Keywords: blockchain, digital forensics, data provenance, traceability, cybersecurity, digital evidence.

Introduction

Blockchain technology, was presented as the core mechanism for Bitcoin, but has moved far beyond cryptocurrency. At its core, blockchain is a distributed ledger that chronicles transactions transversely within computers to ensure it can't be altered without the shift of all successive blocks and the unanimity of the network. This intrinsic feature of immutability sorts blockchain a compelling solution for ensuring data integrity and security.

Presently cryptocurrency has converted a catchphrase in industry and academia. It is explicitly premeditated data stowing structure, dealings in Bitcoin network could ensue deprived of any third party and the

DOI: https://doi.org/10.5281/zenodo.13800859

central technology to construct Bitcoin is blockchain, which came to lime light in 2008 and instigated in 2009. Blockchain can be viewed as an open ledger where all stanch transactions are stockpiled in blocks. This chain develops as new-fangled blocks are affixed to it unremittingly. Asymmetric cryptography and distributed algorithms have been employed for user security and ledger reliability. The blockchain technology mostly has strategic individualities of devolution, tenacity, obscurity, and clarity. With all these, blockchain can critically preclude costs and increase adeptness. Subsequently it allows imbursement to be done deprived of any bank or any arbitrator, blockchain can be castoff in countless business services such as digital assets, remittances, and online payments.

Operation cannot be meddled with when it is chockfull into the blockchain. Activities that require extraordinary consistency and rectitude can practice blockchain to draw customers., Blockchain is distributed and can evade the single point of failure.

In digital forensics, the ability to guarantee the integrity and authenticity of data is crucial. Traditional forensic methods often face challenges related to data tampering and traceability. Blockchain technology propositions is a promising answer to these issues by providing a transparent and tamper-evident record of data transactions.

Blockchain Technology: An Overview

Customary database technologies have numerous encounters for keeping financial transactions. For example, reflect on the auction of a property. When the money is swapped, title of the property is shifted to the buyer. Separately, mutually the buyer and the seller can record the fiscal transactions, but neither basis can be trustworthy. The supplier can easily assert they have not proven receipt of the money even though they have, and the buyer can similarly contend that they have paid the money

To evade impending legal issues, a reliable third party has to oversee and authenticate transactions. The existence of this vital buff not only obscures the transaction but also generates a single point of susceptibility. If the dominant database was conceded, both parties could agonize. Blockchain lessens such issues by crafting a dispersed, tamper-proof system to record transactions. In this scenario, blockchain generates one ledger each for the buyer and the seller. Wholly, all transactions need be sanctioned by both parties and are inevitably rationalized in both of their ledgers in real time. Slightly, venality in antique transactions will corrupt the whole ledger. These feature of blockchain technology have steered its use in numerous sectors, including the creation of digital currency like Bitcoin.

Data provenance and traceability are critical aspects of digital forensics, ensuring the authenticity, integrity, and reliability of digital evidence. Blockchain technology, with its devolved, immutable, transparent ledger, offers a promising solution for enhancing data provenance and traceability in digital forensics.

Data provenance refers to the history of data, including its origins, transformations, and movements over time. In digital forensics, provenance information is crucial for validating the chain of custody and ensuring that digital evidence has not been tampered with.

Blockchain technology can enhance data provenance by providing a distributed and absolute ledger that accounts for all dealings and changes to the data.

Traceability refers to the knack to track and validate the antiquity, position, and application of an entry by means of acknowledged documents. In digital forensics, traceability ensures that the entire interactions with digital evidence are recorded and can be audited.

DOI: https://doi.org/10.5281/zenodo.13800859

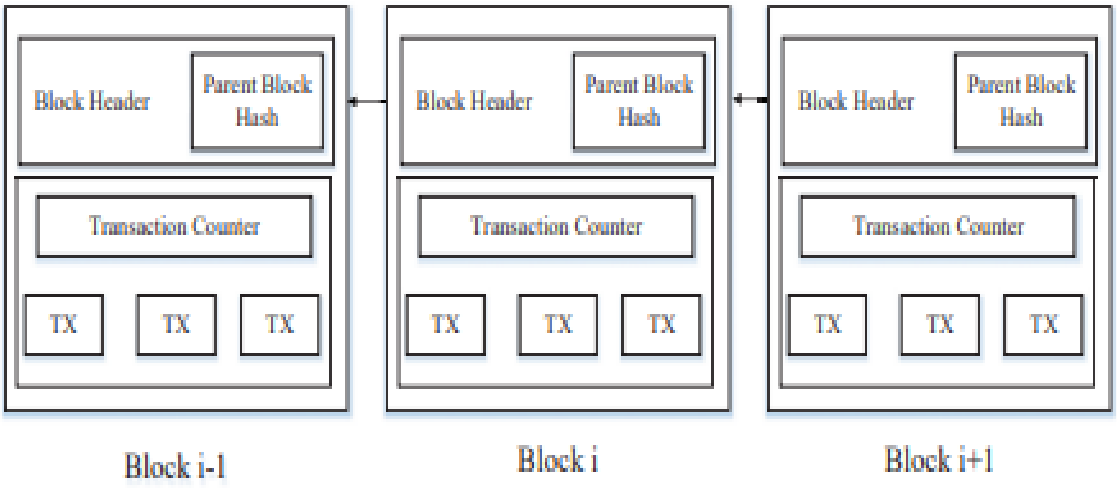
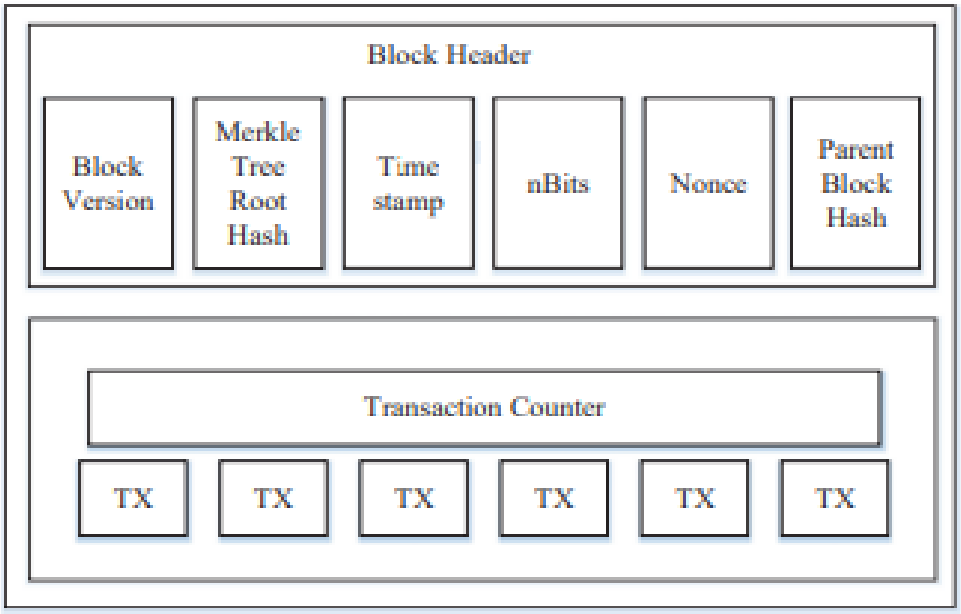


Fig. 1: A Sample blockchain that entails



an unbroken series of blocks

Fig. 2: Block configuration of blockchain

Blockchain is an evolving technology that is being espoused in a ground-breaking manner by several industries such as;

a. **Energy:** To generate peer-to-peer energy interchange platforms and modernize entree to renewable energy.

b. **Finance:** Like banks and stock interactions use blockchain facilities to accomplish virtual payments, accounts and market trading.

c. **Media and Entertainment:** To achieve copyright data.

d. **Retail:** To trail the drive of goods amongst suppliers and buyers.

Blockchain functions on a devolved network where each member has entrée to the whole ledger of transactions.

DOI: https://doi.org/10.5281/zenodo.13800859

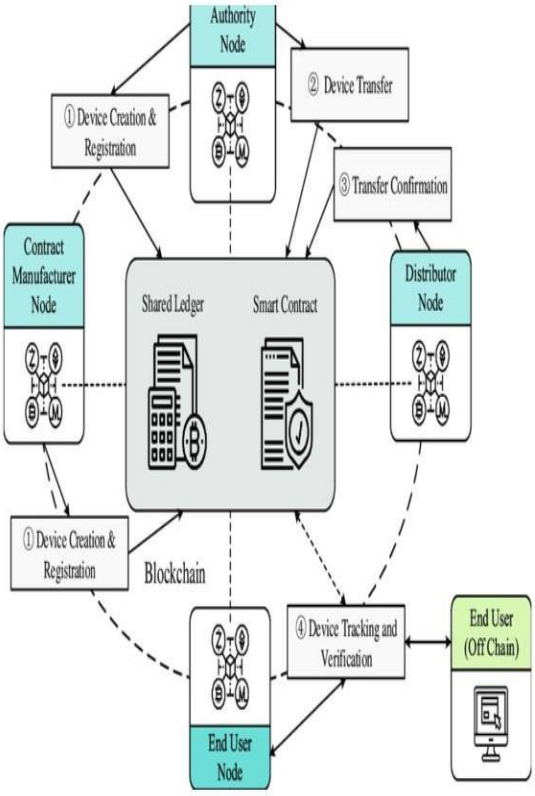


Fig. 3: Blockchain for Supply Chain Provenance

Structures of blockchain:

Decentralization: Distinct from the customary central systems, blockchain drives on a peer-to-peer network, decreasing the risk of a single point of failure.

Immutability: When data is logged in a blockchain, it is awfully hard to adjust, providing a reliable audit trail.

Transparency: All transactions are noticeable to partakers in the network, ornamental trust and accountability.

Security: Cryptographic algorithms safeguard the veracity and privacy of the data.

Data Provenance in Blockchain

The term "data provenance", occasionally named "data lineage," denotes an acknowledged track that accounts for the source of a bit of data and where it has enthused from to where it is now.

Data provenance denotes the extensive accessibility and availability of data. Blockchain technology improves data provenance through the following mechanisms:

a. Decentralized Storage: Data is distributed transversely a network of knobs, certifying idleness and reducing the risk of data loss.

b. Public Accessibility: In public blockchains, data is accessible to anyone with network access, promoting transparency.

c. Interoperability: Blockchain can integrate with various systems, allowing for seamless data exchange across platforms.

The dispersed flora of blockchain warrants that data is not dependent on a single entity, thus enhancing its availability and reliability.

Data Traceability in Blockchain

Data traceability denotes to the capacity to track and smidgen data throughout its lifecycle, from its origin to its current state. This concept is crucial in various industries to ensure data integrity, accuracy, and accountability. Here are the key aspects of data traceability:

a. **Data Origin**: Identifying where the data was created or sourced. This includes the initial input point, whether it's from a sensor, a user, a database, or another system.

b. **Data Lineage**: Tracking the data's journey, including all transformations, movements, and processes it has undergone. This helps in understanding how data has changed over time and the various systems it has passed through.

c. **Data Provenance**: Providing detailed information about the data's history and lifecycle, including who has accessed or modified it, when, and why. Provenance ensures that the data's history is well-documented and transparent.

d. **Audit Trails**: Maintaining logs that capture all actions performed on the data, including creation, modification, and deletion. These logs are essential for compliance, security, and forensic investigations.

DOI: https://doi.org/10.5281/zenodo.13800859

Blockchain In Digital Forensics

Digital forensics is a division of science that emphases on classifying, getting, handling, examining and recording data stored automatically. Electronic confirmation is a constituent of virtually all illicit actions and digital forensics sustenance is crucial for law enforcement inquiry.

It is used to examine cybercrimes but can also aid with unlawful and courteous investigations. For instance, cybersecurity teams may use digital forensics to classify the criminal after a malware bout, while law enforcement agencies may use it to scrutinize data from the maneuvers of a murder suspect.

Digital forensics contains the assortment, conservation, investigation, and staging of digital proof. Blockchain technology can enhance these processes in several ways:

Chain of Custody: Blockchain delivers a safe and unchallengeable record of data transactions, ensuring a clear chain of custody for digital evidence.

Data Integrity: The immutability of blockchain confirms that data remains unaltered from the time it is recorded, providing a reliable basis for forensic analysis.

Traceability: Blockchain's transparency allows forensic experts to trace the origin and history of digital evidence, facilitating more accurate investigations.

Benefits of Blockchain

a. Transparency: Complete transactions are noticeable to all members, augmenting hope and accountability.

b. Security: Cryptographic algorithms and consensus mechanisms protect against fraud and unauthorized changes.

c. Efficiency: Eliminates the necessity for mediators, tumbling costs and speeding up transaction.

d. Traceability: Every transaction is recorded and can be traced back, improving auditing and compliance.

Solicitations of Blockchain

a. **Cryptocurrencies**: The utmost well-known bid of blockchain is in cryptocurrencies like Bitcoin and Ethereum, which use the technology to create decentralized digital currencies.

b. **Supply Chain Management**: Blockchain can be used to trail the drive of things over a supply chain, in case to slide and reducing fraud.

c. **Smart Contracts**: Self-executing contracts with the terms of the treaty rightly transcribed into code. They inevitably impose and implement the terms of a contract when predefined conditions are met.

d. **Voting Systems**: Blockchain can provide safe and apparent voting systems, dipping deception and increasing voter confidence.

e. **Identity Verification**: Blockchain can offer secure and tamper-proof methods for identity verification.

Challenges And Opportunities

While blockchain offers significant advantages for data provenance in digital forensics, it also presents several challenges:

a. Scalability: The size of blockchain networks can grow rapidly, leading to concerns about storage and processing capabilities. That is, as the amount of transactions breeds, the blockchain can become slower and more resource-intensive.

b. Complexity: The technical complexity of blockchain may pose a barrier to its widespread adoption in forensic practices.

c. Legal and Regulatory Issues: The legal status of blockchain records and their admissibility in court remain areas of ongoing debate.

d. Energy Consumption: Some unanimity devices, like Evidence of Work, are energy-intensive.

Despite these challenges, opportunities for blockchain in enhancing data integrity and forensic investigations are substantial. The continued development and adoption of blockchain technology hold promise for more safe and dependable data

DOI: https://doi.org/10.5281/zenodo.13800859

administration practices for forensic experts.

Conclusion

Blockchain technology has the latent to transmute data provenance and digital forensics by ensuring secure, translucent, and indisputable record of data transactions. While there are challenges to its implementation, the benefits of enhanced data integrity, transparency, and traceability make blockchain a valuable tool for forensic experts. As the technology continues to evolve, its integration into digital forensic practices will likely become increasingly prevalent, paving the way for more robust and trustworthy forensic investigations.

References

Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. 2019 IEEE Security and Privacy Workshops.

Kshetri, N. (2019). Can blockchain strengthen the Internet of Things? IT Professional, 19(4), 68-72.

Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81.

J. Bonneau, A. Narayanan, A. Miller, J. Clark, J. A. Kroll, and E. W. Felten, "Mixcoin: Anonymity for bitcoin with accountable mixes," in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2019, pp. 486–504.

T. Ruffing, P. Moreno-Sanchez, and A. Kate, "Coinshuffle: Practical decentralized coin mixing for bitcoin," in Proceedings of European Symposium on Research in Computer Security, Cham, 2019, pp. 345– 364.

A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," arXiv preprint arXiv:1507.06183, 2019.

S. King, "Primecoin: Cryptocurrency with prime number proof-ofwork," July 7th, 2020.

S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proofof-stake," Self-Published Paper, August, vol. 19, 2021.

V. Zamfir, "Introducing casper the friendly ghost," Ethereum Blog URL: https://blog. ethereum. org/2015/08/01/introducing-casperfriendly-ghost, 2022.

DOI: https://doi.org/10.5281/zenodo.13800859