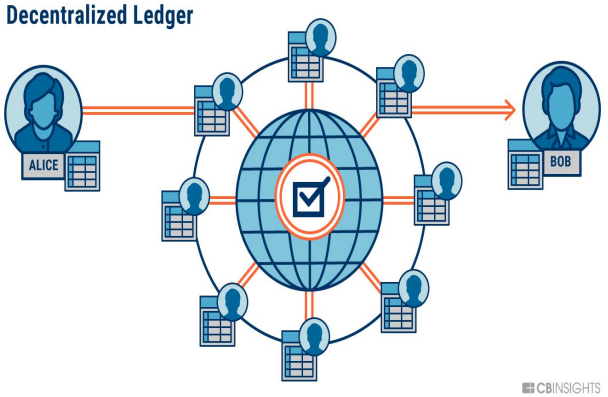
Application of Blockchain in Digital Forensics (CIS 5396)

By: Samuel Babatunde

Digital Forensics

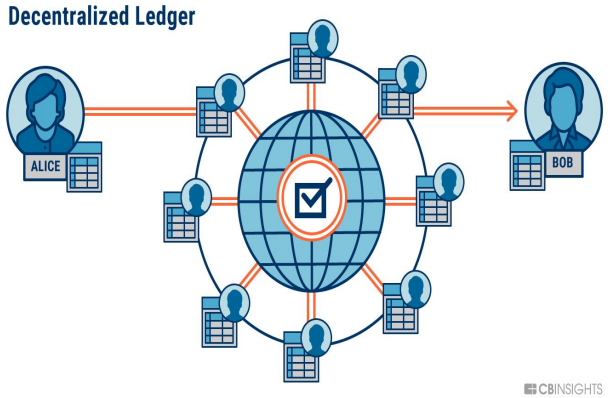
Digital forensics is a legal procedure to *collect, analyze, store, and report digital evidence*



Blockchain

Blockchain is a type of database (a collection of information stored electronically on a computer system).

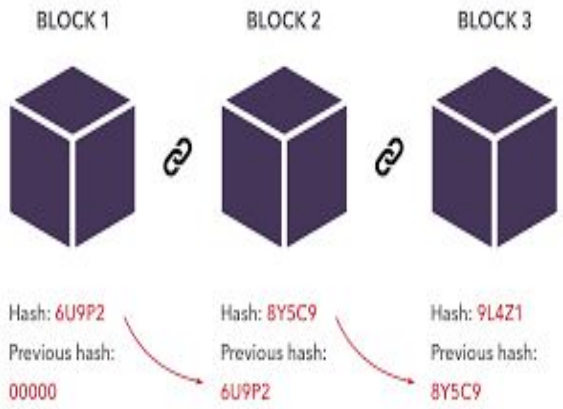
Unlike the traditional database, Blockchain is a distributed and append-only database of time-stamped records that are cryptographically linked.



Blockchain cnt'd

The blockchain network comprises several nodes (computing machines) that validate each transaction request and store the information (states) verified transaction.

Some blockchain supports smart contracts (e.g., ethereum), allowing developers to encode and publish logic to the network.



Pros

BC's Immutability and the irreversible feature ensure the integrity of information stored on the blockchain. (modified states can be audited by indexing the network and contract event logs)

BC's decentralization eliminates the centralized control or rules as it is in a traditional database.

BC provides security, efficiency, and transparency when used in information exchange.

The anonymity feature and data encryption (SHA 256)

Evidence Mgmt & Appn of BC in DF

Blockchain provides a secure, tamper-resistant data platform for forensic evidence storage.

Access to stored data can be controlled using smart contracts

Elliptic Curve Digital Signature Algorithm(ECDSA) data encryption and identity (privacy) protection

Evidence is protected against confiscation (immutability)

Off-chain and on-chain data encryption and decryption

Blockchain forensic

BMW leverages blockchain (PartChain) technology to track component's journey from the origin to the factory.

BMW suppliers are included on the PartChain network as participant which enables traceability for compliance and historic data audit.

"PartChain enables tamper-proof and consistently verifiable collection of data in our supply chain," said Andreas Wendt (member of the Board of Management of BMW AG)

Blockchain forensic

PartChain creates a timestamped transaction object representing the changes along the supply chain (e.g., component movement, raw material processing, etc.).

Application of Blockchain forensic in automotive industry include: Finances, vehicle safety and data security, vehicle maintenance and accident history, manufacturing process, telematics and infotainment, and smart insurance.

Env setup for private BC

Node/npm

waffle, web3 & ethersjs

Remix IDE

Smart Contrat (Ethereum Solidity)

Open source Tools for private BC

Hardhat

Truffle

Ganache

IPFS for media evidence storage (Immutable file system)

Go-Ethereum (Geth)

Puppet

???