International Journal of Multidisciplinary Research and Modern Education (IJMRME)
Impact Factor: 7.315, ISSN (Online): 2454 - 6119
(www.rdmodernresearch.org) Volume 7, Issue 1, 2021

BLOCK CHAIN FORENSICS: A SYSTEMATIC REVIEW OF THE PROSPECTS

Indumathi J
Independent Postdoctoral Fellow, British National university of Queen Mary, Delaware, United States of America & Professor, Department of Information Science and Technology, Anna University, Chennai, Tamilnadu

Cite This Article: Indumathi J, "Block Chain Forensics: A Systematic Review of the Prospects", International Journal of Multidisciplinary Research and Modern Education, Volume 7, Issue 1, Page Number 26-36, 2021.

Abstract:

Among the fastest-growing sectors, health care sector is most sought out one owing to the pandemic. During this pandemic the Healthcare sector is facing lot of complications inclusive of handling the medical record data and contact tracing. Coronavirus disease 2019 (COVID-19) is caused by severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2). Most of the data are stored in the cloud inviting the malicious users to play with. Moreover, a plethora of challenges faced by the investigators related to the new cloud storage technology, are as dispersal of shards, default encryption, defining the position of shards, convalescing files with user credentials, and so on. Among several technologies to tackle the malicious users, block chain tops the list. All the challenges must be met with a forensically sound methodology, identification of artifacts, and a tool to assist investigators in retrieving artifacts and tell-tale evidence.

The Block chain is used a tool to launch an efficient and translucent health care professional model based on sophisticated degrees of accuracy all through this COVID 19 pandemic. Block chain exhibits massive potential health care solution for data provenance, decentralized management, enforcement of health-care regulations, immutable audit trail, interoperable health data access, logistics, medical supply chain efficiency, privacy, redundancy and fault tolerance, remote data collection and logging, robustness, security of EMRs, Integrity of medical records, Storage capacity, unification or standardization of information, value-based payment mechanisms. In the field of block chain-based distributed storage forensics challenges like recovering files and metadata to be of use in a prosecution are yet to be solved. Unless this challenge is tackled there is no guarantee that such data are recoverable on an accused's local storage.

This paper gives a comprehensive overview of the rationalized review of the Block Chain, Block Chain Forensics, rationale for the study of Block Chain Forensics, applications, various open research challenges in Healthcare. This study provokes the inevitability for Block Chain Forensics. Moreover, this study also reveals the need for immediate research that are capable enough to be rendered as solutions. Last but not the least, this paper provides an insight into the latest Block Chain Forensics research trends, which will prove beneficial in the development of Digital forensic investigation process.

Key Words: Anonymity, Autonomy, Block Chain, Block Chain Forensics, Decentralization, Delegated Proof-of-Stake (DPoS) ,Digital artifacts, Immutable, Open Source, Practical Byzantine Fault, Proof of Elapsed Time(PoET),Proof-of-Activity (PoA),Proof-of-Bum (PoB),Proof-of-Stake (PoS),Proof-of-Weight (Po Weight), Proof-of-Work (PoW),Transparency.

1. Block Chain:

Block Chain picks up where IoMT & Cloud technology bites the dust. BC is used to store information securely in safe locations for future information sharing. A Block Chain is a ledger which is dispersed and it operates based on consensus alias validation mechanisms programmed on dissimilar nodes of its networks. The Block Chain is used to generate a tamper-proof digital ledger of transactions; which is shared among the parties. The transactions among the parties are signed using public-key cryptography and these dealings are stockpiled on a circulated ledger. The ledger is encompassed of cryptographically linked blocks of transactions, to form a block chain. Once recorded it is very difficult to remove a block from the Block Chain ledger. Block Chain thus gives a digital version of etching information into solid stone. Block Chain technology further permits dispersed preservation of encrypted data.

2. Characteristics of Block Chain:

The characteristics of block chain are as follows:

- Immutability – The transaction cannot be changed once it is agreed and shared across the distributed network,
- Innovation – There is sample space for new creation of Block Chains,
- Reduced Transaction Expenses – This is made possible with the eradication of the third parties,
- Security – This is made possible due to decentralization,
- Transparency – This is achievable for sure as all the alterations are made public.

- Integrity- Block Chain Data Integrity in Cloud ensures that the data assets stored on the Cloud are intact and nothing has been tampered with. A Keyless Signature Infrastructure (KSI™) via a Restful API is enough to provide the desired integrity.

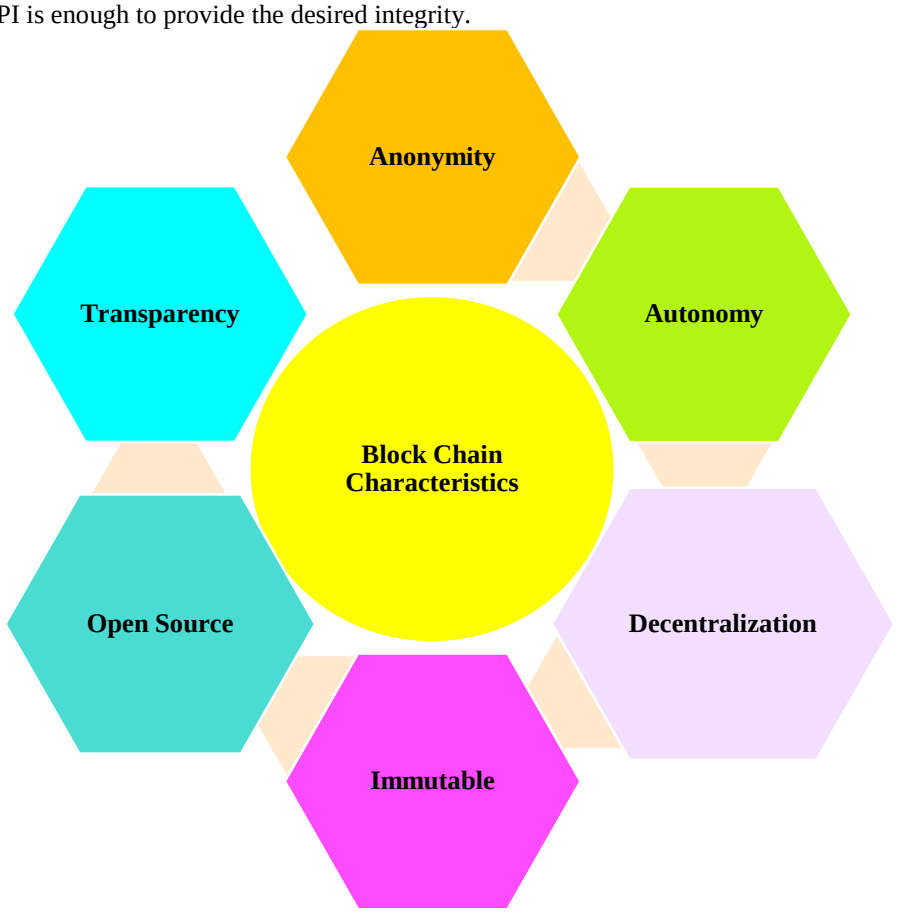

Figure 1: Block Chain - Characteristics

2. Types of Block Chain:

There are many, types of Block Chain (see Table 1), that have emerged such as public, private, semi-private, side-chains etc.

Table 1: Types of Block Chain

Type of Block Chain	Functioning
Public Block Chain	anyone can participate
Private Block Chain	can participate after requesting membership
Semi-Private Block Chain	combination of public and private Block Chains
Side Chains	Concept of running a separate distributed ledger off of the main chain but with transactions able to take place in the same currency

Consensus mechanisms (see Table2) are used for verification of the transactional data between the nodes in a network.

Table 2: Summary of Consensus Algorithms in Block Chain

Algorithm	Characteristics
Proof-of-Work (PoW)	solve a mathematical puzzle to get incentives.
Proof-of-Stake (PoS)	Can own a section of Block Chain and this act as a carter to maintain a version of ledger which is of true state. Should have casing in the game.
Delegated Proof-of-Stake (DPoS)	Owner votes for an agent, who, executes the function of validating transactions and maintaining the Block Chain.
Proof of Elapsed Time(PoET)	Based on a lottery game, a leader is selected; and this Leader picks the next version of the ledger
Practical Byzantine Fault	A consensus algorithm for the enterprise consortiums in which the members are partially Tolerance (PBFT) trusted.

Proof-of-Weight (Po Weight)	PoS algorithm solves the biased nature using "weighted factors".
Proof-of-Bum (PoB)	Miners dispatch coins to an "eater address". The one who burns the coins gets a prize and can pit a new block.
Proof-of-Activity (PoA)	Two consensus algorithms PoW and PoS are mixed to obtain security.

Block Chain platforms are selected based on the subjective assessment of their Activities, ease of prototyping, Popularity, Pricing, supported languages, and Type of network.

The various Block Chain platforms are IBM Block Chain, IOTA, Multichain, Open-chain, Quorum, R3 Corda, Ripple, Stellar, Symbiont Assembly.

3. Block Chain in Health Care:

A vast body of literature is available that converses the use of Block Chain in Health Care. Carlisle, B.G (2014) shows the use of bit coin in medical research. The year 2015, witnessed the popularization of Block Chain as a novel economic model by Swan, M (2015) and the use of Block Chain for decentralizing privacy by Zyskind, G., et al (2015).

The year 2016, further saw the evolution of Block Chain [Baliga, A (2016)], Electronic Patient Record systems (EPRs) [Baxendale, G (2016)], and its utilization in empowering the patient-physician relationship [Baxendale, G (2016)]. Azaria, A, et al., (2016) in their paper described about the utilization of Block Chain for handling authorization in medical domain, with a developed application named as Medrec. Some authors cited the use of Block Chain as solutions for Interoperability [Brodersen, C, et al., (2016)]; provide protocols for medical trustworthiness [Irving, G, Holden, J (2016)]; and for transparency [Nugent, T, et al., (2016)].

In the year 2017, Block Chain evolved rapidly [Dai, F, et al., (2017)]; and it was used in various Health Care applications [Angraal, S, et al., (2017), Benchoufi, M, et al., (2017), Dhillon, V, et al., (2017)]. The Block Chain is substantiated to be very energetic for Health Care [Heston, T (2017)], and for consequently vesting e-health [Dubovitskaya, A, et al., (2017)]. Many preceding works mentions about the challenges and opportunities of Block Chain in e-Health Care [Rabah, K (2017), Karafiloski, E., Mishev, A (2017), Tama,B.A, et al., (2017)].

Esposito, C, et al., (2018) showed how in 2018, Block Chain gained its celebrity status as an assurance for offering security and privacy of eHealth Care. For example, to name a few systems - Blochie [Jiang, S, et al., (2018)], FHIR chain [Zhang, P, et al., (2018)] and Mistore [Zhou, L. (2018)].

Many documentations [WHO (2020); H. Zorbas, et al.,(2003);R. S. Kaplan , et al.,(2011);A. M. Alloubani, et al.,(2020)] have narrated about the problems arising due to the management complexity and the heterogenous nature of the multiple stakeholders. This problem is more intense in developing countries devoid of appropriate infrastructure (deprived of any appropriate systems to preserve the records, human resources and manpower, funding and medical policy [K. Sears, et al.,(2017)]. Amongst the various solutions devised using the latest popular technologies, Block chain exhibits massive potential solution for safeguarding the medical records management problems [World Economic Forum, et al., (2020); Price water house Coopers, 2020)], which was pigeon holed by Gartner, into the top 10 strategic technologies which will change the world in the future years [F. Curbera, et al., (2019)].In short, block chain qualifies the stored data to be secure and improved.

Other works that is of interest are: Auth Privacy Chain (block chain-based access control framework with privacy protection) proposed by Yang, C., et al., (2020); block chain-empowered AAA scheme for accessing data of LS-HetNet proposed by Na Shi, et al., (2020) and zkCrowd (an innovative hybrid block chain crowd sourcing platform) named and proposed by, Zhu, S et al.,(2020)

4. Block Chain in Health Care: Rationale:

M. Mettler(2016) enumerated several advantages obtained by applying Block Chain in smart Health Care. For example, health data can be stockpiled on the Block Chain in a safe way. The Characteristics of Block Chain viz., no particular point of failure (as it is distributed), complete pellucidity, strong cryptographic techniques, near 100% immutability and its ability to use insightful contracts, makes it the most preferred mechanism of data integrity in the Cloud. These Characteristics has ignited the Block Chain revolution, which has not only swept the feet of the financial industry by storm, but is also making inroads in every sector like Health Care, energy, retail, governance, supply chain and agriculture, including Data integrity; thereby disrupting the walks of life of people.

The utilization of Block Chain technology, offers reliability (decentralized architecture) and safety in the Health Care system. The Block Chain can alleviate problems arising from the privacy and integrity of patient information, due to the features of Block Chain, such as immutability, transparency and reliability. Block Chain supports in the management of logs and the auditing of the data.

5. Block Chain Applications in Health Care:

The benefits that arise from the integration of Block Chain techniques with Health Care have been documented by several authors [Kshetri, N, et al.,(2018),Azaria, A, et al.,(2016),R. Jayaraman, et al.,(2019)] that is to say, are the computerized execution of services, disparity access control for various user types, the

enactment of health-care regulations, logistics, distant data collection, indexing, the unification or calibration of information, redundancy and fault lenience.

Uniting the Block Chain technology with IoT, it can augment the reliability (due to immutability of the data) of the evidence carried in real time.

Block Chain-Based Health Asset Tracking and Management in The Supply Chain:

The Block Chain assists in the management of drug supply chains, primarily because of its immutability characteristics, which makes the forgery of drug, more challenging (for example the tragic consequences for the Nigeria population). The Block Chain can thus be applied to many areas like control and management of drugs. Block Chain assists in monitoring the dispersal of drugs, and check that the resources trail the supply chain pattern fittingly. Say for example, in drug distribution, cycling through all the stages in the supply chain, assist in combating drug counterfeiters, such as the deviation of pharmaceutical products and theft.

Health Care Information Management:

The Block Chain protocols are used in Health Care information management to control transactions, process of distributing electronic health records, with increased security, immutability of data, and privacy. The Block Chain satisfies the necessities to improve the quality and security of data transfer, as well as the reduction of energy costs. As the consensus protocols are becoming more advanced, they can be used in the resource-constrained devices (e.g., IoMT), as from light consensus protocols such as PBFT and SCP [Imran Makhdoom et al., (2019)]. The Block Chain endorses the sharing and storage of medical big data.

Secure Sharing & Storage of Health Care Data:

All the stakeholders who are into Health Care are to securely share patients' medical Data. The shared untampered data relevant to the patients are necessary to make good Health Care decisions. The speedy development of Block Chain ensures the sharing and stowing of health data on the Block Chain in an absolute, safe and consistent way. The primary protocol that is involved in the network trust building processes are the consensus protocol, which helps to share patient records, images sharing, Log Management in Health Care Systems, managing Health Care information, Patient Monitoring with the aid of personal sensors, reliability and monitoring patients through sensors with limited hardware.

The medical data is to be stored securely, especially with good data honesty, which is a daunting task. The medical data like patients' complete medical histories, are stored and maintained using a Block Chain communally in a decentralized way.

The Block Chain endorses the importance of Block Chain technology in the Health Care industry by utilizing it in a number of other ways – namely, for increased reliability, increased efficiency, privacy, security, developing integration, and lots more.

Privacy and Security in Block Chain for Health Care:

Feng, et al., (2019) has listed about the prevailing challenges of privacy in the Block Chain as (i) Identity privacy - preserve the user's private identity, without linking to the transaction and (ii) Transaction privacy - guaranteeing the inaccessibility to the contents of transaction by unauthorized users.

The striking literatures, citing the utilization of Block Chain to achieve, privacy in health care are : Dwork, C, et al.,(2014) work on differential privacy, Acar, A.,, et al.,(2018) work on homomorphic crypto graphy , Sabt.M, et al.,(2015) work on trusted execution environments (TEE) , and Ben-Sasson, et al.,(2018) work onzk-snarks (derived from the zero-knowledge proof). Several mechanisms and the relevant concepts of preserving privacy are existing in literatures [Indumathi 2012, 2013 (a, b, c), 2020, 2021; Indumathi and Uma 2007(a, b), 2008(a, b, c, d)].

6. Block Chain Forenscis:

Block Chain forensics, is an umbrella term covering issues of Block Chain and Digital Forensics, that may support in investigating Block Chain ecosystems and quickly respond to and report Block Chain security incidents. Moreover, it combats fraud with block chain and crypto-anchors. The block chain is used in an application to secure the data, which is very crucial during this pandemic situation; as it is entrenched in different application stages. [Combating fraud with block chain and crypto-anchors, Provenance: Every product has a story (2017)]. Block chain forensics is yet to develop novel solutions in Retort to Up-and-coming Digital Forensics Challenges.

IoT presents substantial forensic challenges in terms of evidence source identification, artefact acquisition, insufficiency of IoT-specific forensic tools and techniques, and issues in multijurisdictional litigation.

The Block chain is a powerful technology that decentralizes computation and management processes which can solve many of IoT issues, especially security.

Koshy, P., et al.,(2014), established the facility to map Bitcoin addresses straight to IP data. It generates and estimates mappings exclusively by means of real-time transaction traffic garnered over 5 months. The heuristics to detect the ownership relationships between Bitcoin addresses and owners IP addresses was proposed by leveraging anomalous spreading behavior.

7. Significance of Block Chain Forenscis:

- Block chain can be integrated into the Digital Investigation Models.
- Block chain can uphold Compliance with Digital Investigation Principles.
- Block chain usage aids to Simplify Multijurisdictional Investigations, Managing Cross-Jurisdictional Disaster-Centered
- Block chain aids to provide more Witnesses.
- Block chain-Based Forensic-Enabled Devices can be used to Support Victims.
- Block chain can be used to Investigate Technology Misuse.
- Building trusted ecosystems for Forensic caseworks using Block chain
- Missing Persons Lists
- Identifying human remains in a disaster
- Managing postmortem (PM) Data Repositories of Found Victims
- Managing ante mortem (AM) Data Repositories for Global Living Citizens

8. Open Research Challenges in Block Chain Digital Forensics:

- Develop a block chain-based forensic framework that aids in gathering heterogeneous digital evidence, forensic procedures in a standardized manner.
- Efficient management of data volume in the chain of custody – Evidence data is voluminous and contains thousands of multimedia files or log files per case. The data storage should offer the raw documents based on off-chain technologies like IPFS, Storj. The hashes or meta-hashes should be used in the block chain, to ease audit ability.
- Enable understandable forensic outcome/reports –There is an accentuating incomplete research in the field of establishing a crystal-clear link between forensic sound procedures and their proper explanations. This can be solved by the block chain as it offers an efficient and provable establishment of data flows. The knowledge salvaging and report formation parts can then be automated so that it is understandable in court.
- Interoperability and cross-border jurisdictions. The international collaborations in the form of international standardized streams and apt data management and sharing agreements will augment the contest of cybercrime, enabling international interoperability.
- Parse forensic sound procedures in block chain systems- Ensure apt sound consistent forensic flows are in proper place, and assure that smart contracts relate the suitable functions; so that it can be used in final court for verification & validation and chain of custody tamper-proof guarantees. The immutable property of Block chain is a proof-of-existence and this can be merged with the block timestamps and hashes, so as to serve as a guarantee that evidence was garnered at a precise moment and that they have not been altered.
- Timeline of events and chronology- In forensic investigations to have an apt reporting and evidence gathering procedures based on the timeline of events is essential as it is used in the future to avoid or minimize them. Moreover, the significance of data acquisition and timeline of events in digital forensics is crucial to recognize patterns and relate to analogous cases.
- Tokenization of pieces from digital evidence – The digital evidence extracted from the crime scene is normally analyzed for the reconstruction of events and this is performed by several individual or group of people. Say for example, when an image of hard disk is obtained then this evidence is divided into a random number of artifacts, analyzed by different people who will look into different parts like log files, file system and a specific binary that necessitates reversing. The broken-down things are normally assigned tokens (one solution) and storing tokenized artifacts in the block chain throughout the progression of a digital investigation still remains as a major unsolved issue.
- Performance Issues-scalability, availability
- Security issues- Majority Attack and Selfish Mining, Anonymity and Privacy, Abuse of Block chain,
- Timeline of events and chronology.
- The creation, presentation and interpretation of forensic reports in numerous occurrences should be prudently handled to eradicate the misapprehensions of the forensic hypothesis or the investigation facts; which is main limitation in the standard.
- The Software-Defined Networks (SDN) paradigm introduces more challenges to digital investigation processes (identification, extraction, and preservation phases). The digital forensic investigation processes are to be revamped for SDN.
- The challenges of precisely identifying, extracting and preserving steadfast potential digital evidence in an SDN is still in infancy. The incessant data storage and physical foraging is to be taken care for well-organized storage process of potential digital evidence.
- The B4F proposed by Cebe, M., et al., (2018) offers a lightweight solution by just possessing hash values, thereby ensuring integrity, fixity of forensic data, and availability of this data. Since, there is a

lacunae in the development of a mechanism to ensure the availability of critical forensic data on block chain; it still remains an open challenge.

- The area of forensic-by-design principle is yet to be researched while propositioning novel systems and mechanisms.
- To get a value-added approach, of high level of forensic readiness a Block chain-based Chain-of-Custody should be established at an identical time pre-identified data (data of interest) that is produced by an IoT device. The data of interest is either about the device itself, or other IoT devices or the environment around.
- Regulations for imposing the partaking of numerous entities to forensic block chains and growth of policies to use such data in illicit cases are probable research issues.
- A perfect check on the Quality and reliability of the evidence obtained from the to open environments (e.g. the internet) through apprehensive communication protocols.
- Devise a mechanism to analyze and handle the heterogeneous evidence collected as medical evidence from medical equipment's, as the healthcare systems adopt diverse technologies.
- Necessity for a digital crime safety enquiry to gather and analyze the various types of evidence got from the network under examination.
- The infinite traces generated by the Medical Laboratory Information System demand infinite storage space when collected over a long period of time and this relates to the devise of mechanism to preserve an immense amount of evidence
- The reliable information integrity property of block chain states that any information, once cast in block chain, cannot be changed or erased.
- Another viable use is to find if it can be trailed in contrary to the initial "deal." How well block chain storage can adapt to the two prerequisites of imaging and treatment plans in healthcare information is yet to be revealed.
- The off-chain storage of information wherein, the medical data remains as the data hashes in the block chain; can be verified, secured, and deleted suitably. These constant hashes are used to prove the legitimacy and precision of the off-chain medical records. This is yet to be standardized and overcome the geographical jurisdictions.
- The person's privacy is yet to follow guidelines, standardization, and cross-border healthcare information strategies, together with data retention and use, is life-threatening and going to be undertaken.
- Yet another line of research is to explore the groundbreaking techniques for the lessening of block chain mining adjournments and how block chain is to store and process large amounts of information access transactions in an opportune time.
- Issues Facing in the Chain of Custody
    - Rising data volume reduces the flexibility and capability of document.
    - Make use of digital evidence and documentation to generate the CoC.
    - CoC documentation, bearing in mind that evidence moves from one party to another.
    - present the information in an understandable ways by the judge/ jury and other law enforcement agencies to take a decision

9. Block Chain Forensics Process:

Digital Forensic Data Identification, Collection and Handling: used to identify, collect, and handle potential Digital Forensic data. Say for example, in a fitness band the forensic digital data can be application logs, configuration logs , monitoring logs, network logs , sensor's physical conditions, security incident and events related logs; along with answers for queries like "who," "when," "what," and "how" questions.

Incident Analysis, detection and Monitoring: the organizational processes, data source, and potential forensic data source inputs are detected and used to define incident analysis, detection, and monitoring requirements. Figure 2 validates the framework while integrating knowledge management terms (Navarro-Ortiz et al. 2018) to deliberate the integration of Block chain technology.

IoT Security Processes: Ensures if the information security controls and measures are implemented to protect data identified in the readiness processes are protected as mandated in the organizational processes. Say for example, the IoT proxy, checks if the end-to-end security is employed from the IoT devices to the IoT application, where data is used up.

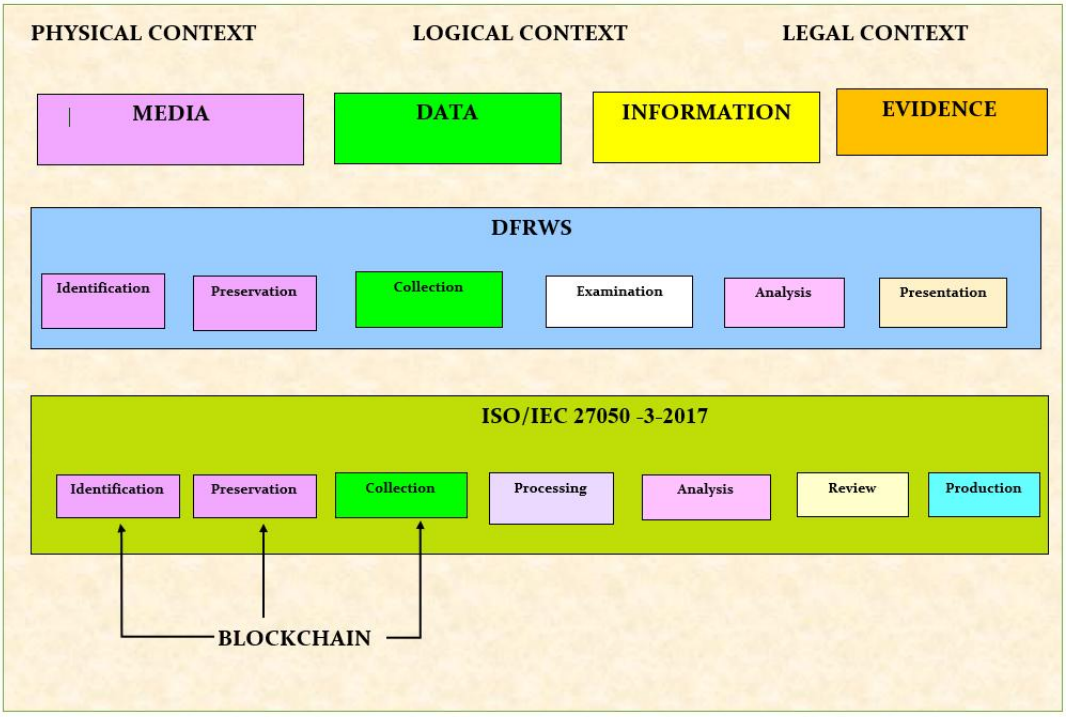

Figure 2: Role of Block Chain in the Digital Investigation Process

A. Identification Phase:

Several authors [M. Spagnuolo, et al.,(2014),C. Zhao , et al.,(2015),D. Neilson, et al.,(2016),L. Van Der Horst, et al.,(2017),J. Bros´eus, et al.,(2017),J. Jose, et al.,(2017),T. Caldwell, (2018),J. Mac Rae , et al.,(2018),M. Wang, et al.,(2018),T. Volety, et al.,(2019)] have mentioned about the proactive steps in the identification phase to be taken for being prepared for the BC DFR .

- Verify and validate all the cases that linked to block chain technology by means of the block chain related keywords.
- Appraise the up-to-date system architecture grounded on reported cases.
- Verify the units that interconnect with the present system as nodes.
- Spot block chain's linked evidences:
  - User's machine, which is demarcated as the machine used by mutually the payer and payee.
  - Crypto currency blocks and ledgers.
  - Use tools like the Bit Cluster, Bit Iodine, Chain analysis, Elliptic, Encase, IEF (Internet Evidence Finder), Numisight.

B. Collection and Preservation Phase:

Several authors [M. Spagnuolo, et al.,(2014),C. Zhao , et al.,(2015),D. Neilson, et al.,(2016), L. Van Der Horst, et al.,(2017),J. Bros´eus, et al.,(2017),J. Jose, et al.,(2017),T. Caldwell, (2018),J. Mac Rae , et al.,(2018),M. Wang, et al.,(2018),T. Volety, et al.,(2019)] have mentioned about the proactive steps in the collection and preservation phase to be taken for being prepared for the BC DFR .

Mas'ud, M. Z.,et al.,(2021)showcased the following Block chain's related evidences:

- Crypto currency's transactions from the crypto currency's ledger
- User's machine (wallet and client's log) - keys (Public + private), transaction id, passphrase, file location.

C. Examination and Analysis Phase:

Several authors [M. Spagnuolo, et al., (2014), C. Zhao, et al., (2015), S. Meiklejohn, et al., (2016), L. Van Der Horst, et al., (2017) have mentioned about the proactive steps in the examination phase to be taken for being prepared for the BC DFR .

Mas'ud, M. Z.,et al.,(2021)also showcased the following:

- Examine client process memory-back-up locations, contacts, passphrase, public and private key, transaction data (address, label, transaction id, amount, fee and timestamps),
- User's machines-Wallet (registry, wallet.dat, log files, debug.log, peers.dat)
- Crypto currency' s ledgers and blocks- Crypto currency addresses, Crypto currency transaction signature schemes

Analysis:

- User's memory and hard disk analysis

- Graph-based analysis and clustering
- Based the crypto currency addresses
- clustering Bitcoin's addresses[S. Meiklejohn, et al.,(2016)]
- find groups of addresses that belong to the same user based on blocks and transactions from the local Bitcoin [M. Spagnuolo, et al.,(2014)

Probe-IoT of M. Hossain, et al., [2018] and FIF-IoT of M. Hossain, et al., [2018] are two models using block chain technology to acquire and preserve evidence in IoT-based systems. They provide a tamper-evident scheme to store evidence in a trustworthy manner. They use the digital ledger to maintain a track record of all the transactions in an IoT-based system, including transactions between things and users, between things and cloud, and between things to things. Due to the nature of block chain, Probe-IoT and FIF-IoT can ensure the confidentiality, anonymity, and non repudiation of publicly available evidence.

D. Presentation or Report Phase:

N.H. Ab Rahman, et al., (2015), emphasised that the standardised procedures and specifications for formulating forensic reports, should comply with the processes defined in existing investigation models and standards like the ISO/ISEC 27043:2015 international standard.

In the milieu of the ISO/IEC 27043, report creation is a process is captured inside the exploratory process which is one of the classes of digital investigation processes [V.R. Kebande, et al.,(2018) , V.R. Kebande, et al.,(2015)]. V. Kebande, et al.,(2016), showed that the report generation is not a part of the main process of investigation, but it is a process that shows or interprets the findings.

10. Conclusion:

The purpose and demand for the use of BC in digital forensic investigations is very apparent; whether it be used for criminal inquiries by bodies or for meeting compliance requirements at exchanges. The use of BC digital forensics is very challenging to the investigators have to not only antagonize with the ingenious gangs of cybercriminals but also to cope with the core technical issues. The increase in computer storage has grown leaps and bounds paving way to an alarming increase in various challenges in regard to digital forensics. The evolution of services of storage from the local storage devices to cloud-based storage services, has only increased the burden on the investigators posing several challenges related to evidence recovery. Several of these have been dazed with inventiveness and tools to aid in the process of recuperating incriminating data. Most of the research on Block Chain in the Internet of Medical Things (IoMT) is focused only on privacy, data integrity, concealment and authentication. But it doesn't tackle the problems arising out of big data stream produced by resource-constrained IoMT devices. However, more laborious research is also desirable in the development of novel algorithms to decrypt provenance of crypto currencies and other parameters. It is necessary to bring to light the potential of BC technology is and what can be done to assist in digital forensic investigations. This is a comparatively new area and consequently has a lot of prospects besides a range of challenges.

14. References:

1. M. Alloubani, M. Almatari, and M. M. Almukhtar, 'Review: Effects of Leadership Styles on Quality of Services in Healthcare', European Scientific Journal, ESJ, Vol. 10, No. 18, Jun. 2014, Accessed: May 06, 2020. [Online]. Available: https://eujournal.org/index.php/esj/article/view/3586.
2. Acar, A., Aksu, H., Uluagac, A. S., & Conti, M. (2018). A survey on homomorphic encryption schemes: Theory and implementation. ACM Computing Surveys (CSUR), 51(4), 1-35.
3. Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Block chain technology: applications in health care. Circulation: Cardiovascular quality and outcomes, 10(9), e003800.
4. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016, August). Medrec: Using block chain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data (OBD) (pp. 25-30). IEEE.
5. Baliga, A. (2016). The block chain landscape. Persistent Systems, 3(5).
6. Baxendale, G. (2016). Can block chain revolutionize EPRs?. ITNow, 58(1), 38-39.
7. Benchoufi, M., & Ravaud, P. (2017). Block chain technology for improving clinical research quality. Trials, 18(1), 1-5.
8. Ben-Sasson, E., Bentov, I., Horesh, Y., & Riabzev, M. (2018). Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptol. ePrint Arch., 2018, 46.
9. Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., Truscott, A., & Accenture, L. (2016). Blockchain: Securing a new health interoperability experience. Accenture LLP, 1-11.
10. C. Zhao and Y. Guan, "A graph-based investigation of bitcoin transactions," in IFIP Advances in Information and Communication Technology, vol. 462. Springer, Cham, 2015, pp. 79–95. [Online]. Available: http://link.springer.com/10.1007/978-3-319-24123-4 5
11. Carlisle, B. G. (2014). Proof of prespecified endpoints in medical research with the bit coin block chain. The Grey Literature [Internet], 25.

12. D. Neilson, S. Hara, and I. Mitchell, "Bit coin forensics: A tutorial," in Communications in Computer and Information Science, vol. 630. Springer, Cham, 2016, pp. 12–26. [Online]. Available: http://link.springer.com/10.1007/978-3-319-51064-4 2
13. Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017, November). From Bitcoin to cyber security: A comparative study of block chain application and security issues. In 2017 4th International Conference on Systems and Informatics (ICSAI) (pp. 975-979). IEEE.
14. Daryabar, F., Dehghantanha, A., & Choo, K. K. R. (2017). Cloud storage forensics: MEGA as a case study. Australian Journal of Forensic Sciences, 49(3), 344-357.
15. Dhillon, V., Metcalf, D., & Hooper, M. (2017). Block chain enabled applications. Apress, Berkeley, CA, 72.
16. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M., & Wang, F. (2017). Secure and trustable electronic medical records sharing using block chain. In AMIA annual symposium proceedings (Vol. 2017, p. 650). American Medical Informatics Association.
17. Dwork, C., & Roth, A. (2014). The algorithmic foundations of differential privacy. Foundations and Trends in Theoretical Computer Science, 9(3-4), 211-407.
18. Esposito, C., De Santis, A., Tortora, G., Chang, H., & Choo, K. K. R. (2018). Block chain: A panacea for healthcare cloud-based data security and privacy?. IEEE Cloud Computing, 5(1), 31-37.
19. F. Curbera, D. M. Dias, V. Simonyan, W. A. Yoon, and A. Casella, 'Block chain: An enabler for healthcare and life sciences transformation', IBM Journal of Research and Development, vol. 63, no. 2/3, pp. 8:1-8:9, Mar. 2019, doi:10.1147/JRD.2019.2913622.
20. Feng, C., Yu, K., Aloqaily, M., Alazab, M., Lv, Z., & Mumtaz, S. (2020). Attribute-based encryption with parallel outsourced decryption for edge intelligent IoV. IEEE Transactions on Vehicular Technology, 69(11), 13784-13795.
21. Feng, C., Yu, K., Bashir, A. K., Al-Otaibi, Y. D., Lu, Y., Chen, S., & Zhang, D. (2021). Efficient and secure data sharing for 5G flying drones: a block chain-enabled approach. IEEE Network, 35(1), 130-137.
22. Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy protection in block chain system. Journal of Network and Computer Applications, 126, 45-58. FIF-IoT [2018] by M. Hossain, et al., [2018]
23. Hossain, M., Karim, Y., & Hasan, R. (2018, July). FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. In 2018 IEEE International Congress on Internet of Things (ICIOT) (pp. 33-40). IEEE.
24. H. Zorbas, K. Rainbird, K. Luxford, B. Barraclough, and S. Redman, 'Multidisciplinary care for women with early breast cancer in the Australian context: what does it mean?', Medical Journal of Australia, vol. 179, no. 10, pp. 528–531, Nov. 2003, doi: 10.5694/j.1326-5377.2003.tb05678.x.
25. Heston, T. (2017). A case study in block chain healthcare innovation.
26. https://enterprise.gem.co/health/
27. Huang, C. H., & Cheng, K. W. (2014). RFID technology combined with IoT application in medical nursing system. Bulletin of Networking, Computing, Systems, and Software, 3(1), 20-24.
28. Huang, C. H., & Cheng, K. W. (2014). RFID technology combined with IoT application in medical nursing system. Bulletin of Networking, Computing, Systems, and Software, 3(1), 20-24.
29. Indumathi J (2012) A generic scaffold housing the innovative modus operandi for selection of the superlative anonymisation technique for optimized privacy preserving data mining. Data mining applications in engineering and medicine, 133–156
30. Indumathi J (2013a) Amelioration of anonymity modus operandi for privacy preserving data publishing (Chap. 7). In: Network Security Technologies: Design and Applications, vol 330, pp 96–107
31. Indumathi J (2013b) An enhanced secure agent-oriented burgeoning integrated home tele health care framework for the silver generation.
32. Indumathi J (2013c) State-of-the-art in reconstruction-based modus operandi for privacy preserving data dredging. Int J Adv Netw Appl 4(4):9–15 (Special Issue on "Computational intelligence— a research perspective" held on "21st–22nd February, 2013")
33. Indumathi J, Uma GV (2007a) Customized privacy preservation using unknowns to stymie unearthing of association rules. J Comput Sci 3(12):874–881
34. Indumathi J, Uma GV (2007b) Using privacy preserving techniques to accomplish a secure accord. Int J Comput Sci Netw Security 7(8):258–266
35. Indumathi J, Uma GV (2008a) A bespoked secure framework for an ontology-based data-extraction system. J Softw Eng 2(2):1–13
36. Indumathi J, Uma GV (2008b) A new flustering approach for privacy preserving data fishing in tele-health care systems. Int J Healthcare Technol Manag 9(5–6):495–516 (Special Issue on: "Tele-Healthcare System Implementation, Challenges and Issues.")

37. Indumathi J, Uma GV (2008c) A novel framework for optimized privacy preserving data mining using the innovative desultory technique. Int J Comput Appl Technol 35(2/3/4):194–203 (Special Issue on: "Computer Applications in Knowledge-Based Systems")
38. Indumathi J, Uma GV (2008d) An aggrandized framework for genetic privacy preserving pattern analysis using cryptography and contravening— conscious knowledge management systems. Int J Mol Med Adv Sci 4(1):33–40
39. Irving, G., & Holden, J. (2016). How block chain - time stamped protocols could improve the trustworthiness of medical science. F1000Research, 5.
40. J. Bros´eus, D. Rhumorbarbe, M. Morelato, L. Staehli, and Q. Rossy, "A geographical analysis of trafficking on a popular darknet market," Forensic Science International, 2017.
41. J. Jose, K. Kannoorpatti, B. Shanmugam, S. Azam, and K. C. Yeo, "A critical review of Bit coins usage by cybercriminals," in 2017 International Conference on Computer Communication and Informatics, ICCCI 2017, 2017. Authorized
42. J. MacRae and V. N. Franqueira, "On locky ransom ware, Al Capone and Brexit," in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 2018.
43. Jayaraman, I., & Mohammed, M. (2020). Secure privacy conserving provable data possession (SPC-PDP) framework. Information Systems and e-Business Management, 18(3), 351-377.
44. Jayaraman, I., & Panneerselvam, A. S. (2021). A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud. Journal of Ambient Intelligence and Humanized Computing, 12(5), 4911-4924.
45. Jiang, S., Cao, J., Wu, H., Yang, Y., Ma, M., & He, J. (2018, June). Blochie: a block chain-based platform for healthcare information exchange. In 2018 ieee international conference on smart computing (smartcomp) (pp. 49-56). IEEE.
46. K. Sears, D. Stockley, and D. Stockley, Influencing the Quality, Risk and Safety Movement in Healthcare: In Conversation with International Leaders. CRC Press, 2017.
47. Karafiloski, E., & Mishev, A. (2017, July). Block chain solutions for big data challenges: A literature review. In IEEE EUROCON 2017-17th International Conference on Smart Technologies (pp. 763-768). IEEE.
48. Koshy, P., Koshy, D., & McDaniel, P. (2014, March). An analysis of anonymity in bitcoin using p2p network traffic. In International Conference on Financial Cryptography and Data Security (pp. 469-485). Springer, Berlin, Heidelberg.
49. Kshetri, N. (2018). Block chain and electronic healthcare records [cyber trust]. Computer, 51(12), 59-63.
50. L. Van Der Horst, K. K. R. Choo, and N. A. Le-Khac, "Process Memory Investigation of the Bit coin Clients Electrum and Bitcoin Core," IEEE Access, 2017.
51. M. Hossain, R. Hasan and S. Zawoad, "Probe-IoT: A public digital ledger based forensic investigation framework for IoT," IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2018, pp. 1-2, doi: 10.1109/INFCOMW.2018.8406875
52. M. Mettler, "Blockchain technology in healthcare: The revolution starts here," Proceedings of IEEE 18th International Conference on e-Health Networking, Applications and Services, 2016.
53. M. Spagnuolo, F. Maggi, and S. Zanero, "Bitiodine: Extracting intelligence from the bit coin network," in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2014.
54. M. Wang, Q. Wu, B. Qin, Q. Wang, J. Liu, and Z. Guan, "Lightweight and Manageable Digital Evidence Preservation System on Bitcoin," Journal of Computer Science and Technology, Vol. 33, No. 3, pp. 568–586, may 2018. [Online]. Available: http://link.springer.com/10.1007/s11390-018-1841-4
55. Ma A (2018) Thousands of people in Sweden are embedding microchips under their skin to replace ID cards. http://uk.businessinsider.com/swedish-people-embed-microchips-under-skin-to-replace-id-cards-2018-5?r=US&IR=T
56. Mas'ud, M. Z., Hassan, A., Shah, W. M., Abdul-Latip, S. F., Ahmad, R., Ariffin, A., & Yunos, Z. (2021, January). A Review of Digital Forensics Framework for Block chain in Crypto currency Technology. In 2021 3rd International Cyber Resilience Conference (CRC) (pp. 1-6). IEEE.
57. MedRec. In: MedRec. https://medrec.media.mit.edu/. Accessed 25 May 2019
58. N.H. Ab Rahman, K.-K. R. Choo, A survey of information security incident handling in the cloud, (Comput. Secur. 49 (2015) 45–69.
59. Nakamoto, Y., Abe, I., Osaki, T., Terada, H., & Moriyama, Y. (2008, October). Toward integrated virtual execution platform for large-scale distributed embedded systems. In IFIP International Workshop on Software Technologies for Embedded and Ubiquitous Systems (pp. 317-322). Springer, Berlin, Heidelberg.

60. Navarro-Ortiz J, Sendra S, Ameigeiras P, Lopez-Soler JM (2018) Integration of LoRaWAN and 4G/5G for the industrial internet of things. IEEE Commun Mag 56(2):60–67. https://doi.org/10.1109/MCOM.2018.1700625
61. Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using block chain smart contracts. F1000Research, 5. Price water house Coopers, 2020
62. R. S. Kaplan and M. E. Porter, 'How to solve the cost crisis in health care', Harv Bus Rev, vol. 89, no. 9, pp. 46–52, 54, 56-61 passim, Sep. 2011.
63. Rabah, K. (2017). Challenges & opportunities for block chain powered healthcare systems: A review. Mara Res J Med Health Sci, 1(1), 45-52.
64. S. Meiklejohn, M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A fistful of Bitcoins," Communications of the ACM, 2016.
65. Sabt, M., Achemlal, M., & Bouabdallah, A. (2015, August). Trusted execution environment: what it is, and what it is not. In 2015 IEEE Trustcom/BigDataSE/ISPA (Vol. 1, pp. 57-64). IEEE.
66. Sabt, M., Achemlal, M., & Bouabdallah, A. (2015, August). Trusted execution environment: what it is, and what it is not. In 2015 IEEE Trustcom/BigDataSE/ISPA (Vol. 1, pp. 57-64). IEEE.
67. Shi, N., Tan, L., Li, W., Qi, X., & Yu, K. (2020). A block chain-empowered AAA scheme in the large-scale HetNet. Digital Communications and Networks.
68. Swan, M (2015) and the use of Block Chain for decentralizing privacy by
69. Swan, M. (2015). Block chain: Blueprint for a new economy. " O'Reilly Media, Inc.".
70. T. Caldwell, "The miners strike – addressing the crypto-currency threat to enterprise networks," Computer Fraud and Security, 2018.
71. T. Volety, S. Saini, T. McGhin, C. Z. Liu, and K. K. R. Choo, "Cracking Bitcoin wallets: I want what you have in the wallets," Future Generation Computer Systems, 2019.
72. Tama, B. A., Kweka, B. J., Park, Y., & Rhee, K. H. (2017, August). A critical review of block chain and its current applications. In 2017 International Conference on Electrical Engineering and Computer Science (ICECOS) (pp. 109-113). IEEE.
73. The Gem Health Network [https://enterprise.gem.co/health/}
74. V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in Proc. 4th IEEE Int. Conf. Future Internet Things Cloud (FiCloud), Vienna, Austria, Aug. 2016, pp. 356–362.
75. V.R. Kebande, H.S. Venter, Adding event reconstruction to a Cloud Forensic Readiness model, 2015 Information Security for South Africa (ISSA), IEEE, August, 2015, pp. 1–9.
76. V.R. Kebande, H.S. Venter, Novel digital forensic readiness technique in the cloud environment, (Aust. J. Forensic Sci. 50 (5) (2018) 552–591.
77. WHO (2020)
78. World Economic Forum, et al., (2020)
79. Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). Auth Privacy Chain: A block chain-based access control framework with privacy protection in cloud. IEEE Access, 8, 70604-70615.
80. Zhang, P., Schmidt, D.C., White, J., Lenz, G.: Block chain technology use cases in healthcare. In: Advances in Computers Block chain Technology: Platforms, Tools and Use Cases, pp. 1–41(2018)
81. Zhou, L., Wang, L., & Sun, Y. (2018). MIStore: a block chain-based medical insurance storage system. Journal of medical systems, 42(8), 1-17.
82. Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using block chain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE.