World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Strengthening Digital Forensics with Blockchain Technology and Algorithms

Shatakshi Johri *

Assistant Professor (Senior Scale), School of Law, UPES, Dehradun, Uttarakhand, India.

World Journal of Advanced Research and Reviews, 2024, 24(02), 459–467

Publication history: Received on 21 September 2024; revised on 27 October 2024; accepted on 31 October 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.24.2.3317

Abstract

The blockchain technology is fast becoming a crucible of e governance. It is pitched to safeguard privacy and is hard to tamper with as it works using the distributed ledger technology. The digital evidence is secured and strengthened respectively. The regulators are dealing with complex and immense volume of data. To deal with this challenge, one of the possible solutions is cloud computing. The use of blockchain in digital forensics has initiated nuanced understanding of evidence management. There are multiple storage and classification models related to blockchain along with algorithms that are helpful in data handling. This article is an analysis of the evolving models that use blockchain and algorithms. The purpose of this article is to analyse and suggest sustainable and pragmatic solutions for regulators. The algorithmic approaches discussed in this article are efficient in terms of time, cost, access and energy. However, to further the objectives of National Strategy on Blockchain, enhanced efforts are needed to secure digital evidence management.

Keywords: Digital forensics; Blockchain; Algorithm; Blockchain DEF; Blockchain snapshot

1. Introduction

This paper particularly deals with whether blockchain can be used in digital forensics to make the digital ecosystem robust and if so, what are the challenges ahead in using the blockchain technology? Despite blockchain technology being secure and difficult to tamper, how developments in the increasingly datafied space are positing multiple challenges to digital forensics? Academicians and other professionals have interpreted the application of blockchain in the context of explaining the distributed ledger technology, its pros and cons regarding individual use cases in digital evidence management. This paper examines the new trajectories and dynamics of models involving blockchain forensics. The dimension that remains unexplored is what are the problems related to the new approaches? How can these innovative approaches using blockchain technology be used by regulators in handling forensic data? How can the limitation of time, cost and access be reduced with the new models like Block DEF, (Tian et al., 2019) etc.? How can blockchain forensics assist in sustainable digital forensics? The findings provide a reference point for an enabled regulatory response as per the Indian legal framework.

This paper has been divided into five sections. The first section describes the background of this study. It briefly explains the growing relevance of digital forensics, the anatomy of blockchain technology and the process of digital forensics. It touches upon the importance of maintaining integrity in the process of handling digital evidence, also called the Chain of Custody (CoC). (Chawhan et al., 2021) The second section explains the various approaches based on blockchain technology to be used in digital forensics. Thirdly, the limitations and benefits of these approaches has been discussed. This is a conduit between literature on the subject as well as the identification of gaps in the same. The fourth section paves the way for further work regarding the incorporation of blockchain based mechanisms in digital forensics and ameliorates solutions to the challenges regarding blockchain. Lastly, the comprehensive gamut of the above subject matter has been concluded.

* Corresponding author: Shatakshi Johri

The primary sources of this study are- the National Strategy on Blockchain brought out by the Ministry of Electronics and Information Technology (MeitY), in December 2021. (NATIONAL STRATEGY ON BLOCKCHAIN Towards Enabling Trusted Digital Platforms, 2021) Also, the new Digital Personal Data Protection Act,2023(THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023), 2022) the proposed Digital India Act, 2023(Proposed Digital India Act, 2023, 2023), the Information Technology Act,2000, etc. The secondary sources include studies pertaining to developments in blockchain technology and consecutive challenges faced by digital forensics.

2. Expanding Domain of Digital Forensics

The field of digital forensics is transforming very swiftly. A pertinent paradigm is that of upcoming standards. That necessitates that there are distinctly identified techniques of properly executing forensics. At the commencement of computer forensics, most of the investigations were conducted as per the caprices of the investigator instead of a thorough uniform procedure. However, as this field has progressed, it has become quite standardized. In the current scenario, there are transparent, methodized approaches for performing a forensic examination. Yet one more development is regarding who is applying forensics? Earlier, almost all thew forensics, which include computer forensics, used to be the limited realm of law enforcement agencies. That situation no longer exists. Today, there are multiple stakeholders that are actively using and examining digital forensics, including the government, intelligence agencies, law firms, academicians, advocates, judges, corporations, etc. (Mukrimaa et al., 2016)

It is to be noted that digital forensics is valuable in identification and documentation of evidence. Holistically, it deals with the entirety of media, that is a hard disk drive. The information accessed is not confined to what the end user would see, but the forensic expert has all the information for perusal. The analyst examines metadata, that is data regarding information. For example, the structure of partitions in disk, author of a file, modification and updating of the file are crucial facets to be considered by a forensic analyst. The information may also be hidden in an area of the media file, which could be critical for investigation. In the event of examining all the potential aspects of data storage, there is generation of huge volume of data. The analyst must control, examine, and preserve all the abovementioned information for the entire duration of forensic investigation. (Mukrimaa et al., 2016)

3. Maintaining Integrity of Digital Evidence Chain of Custody

In the area of cyber-crime, just like any other criminal, the miscreants have developed techniques and tools to cover up their actions. The goal of forensic analyst is to trace and recover the “digital footprint”. It pertains to a log of digital activity. The user in such a case tries to alter or destroy their footprint. These practices being used by criminals in cyberspace are designed to counter digital forensics. The phrase assigned to such attempts is termed as “anti-forensics”. (Conlan et al., 2016) Anti-forensics comprise tools and techniques, which attack the digital forensic process at different stages. It is targeted to nullify the process of digital evidence. Anti-forensic practices include the following:(Kaushik et al., 2022) (Conlan et al., 2016)

Firstly, alteration of data, which mostly involves tampering and alteration of metadata, timestamps, header of a file etc. Portions of data or complete datasets are modified to create waste evidence which is done to disrupt the investigation. Secondly, changing the trail by creating false history, varying IP addresses. which is termed as obfuscation. Paired with it, the perpetrators delete their fingerprints using techniques like log cleaners to derail the investigation process. Thirdly, the forensic analyst’s system can be attacked using a malware code. Fourthly, the storage of media file is destroyed to the point that it cannot be rescued. This is a common method. Another method is the use of electromagnets. The electromagnetic pulse disturbs and damages the integrity of storage media and destroys the entire data. This process of degaussing minimizes any chance of recovering the data lost. Furthermore, this data can be swept clean and rewritten many times by spurious data, thereby making tracing the data back a mammoth task for the analyst. Then there are techniques to eclipse the data by hiding it via encryption as well as steganography. This is done by separate digital files like pictures etc. (Kaushik et al., 2022) (Conlan et al., 2016)

Hence, as discussed above, the primary challenge in preserving the integrity of forensic data is safeguarding its authenticity. On considering the integrity of electronic evidence we can see that such evidence needs to be protected from a number of undesirable outcomes, namely, alteration or destruction. We need to guard against these events and others when trying to maintain system integrity and preserve the purity of evidence so that it could be acceptable in court. It is apt to mention here the concept of Chain of Custody (CoC), which pertains to maintaining the digital evidence, chronologically from the time that the incident occurred, till it is submitted before the court of law. (Shrunga et al., 2022) This chain consists of every phase that must be followed in an investigation, to ensure the veracity of information. This is a significant step, because it cannot be guaranteed that the evidence was not tampered with during its journey from

the investigation to the court. In that case, the evidence collected in not of sterling worth and is of questionable credibility. The decentralized nature of blockchain technology assists in providing a secure database by providing hash function to the data and storing the data in blocks.(Agbedanu & Jurcut, 2021)

4. Various Approaches Applying Blockchain: Towards Forensic Security

Blockchain is an exemplary technology that is based on a distributed ledger. This was used firstly in the curation of a virtual currency, named Bitcoin by Satoshi Nakamoto. (Nakamoto, 2009) It is a blend of diverse innovations, with an evident business significance. It facilitates a ledger that is shared among the several participants involved in a transaction of business, which acts as the sole point of truth. Blockchain completely negates the necessity of validation of such transactions by a central unit. This technology can be applied in Permissioned as well as Permissionless models. The models have applications in multifarious domains such as strengthening education, banking, education, wellness, law, energy etc. Internationally and nationwide, various attempts are being made to progressively implement applications that are premised on Blockchain. Many pilot projects and PoC are undergoing execution. To harvest the gains emerging from this technology, there is a pressing need for a national level policy or strategy. Another promising attribute of this distributed ledger technology is that it inherently fosters trust and removes the requirement for a third-party validation of the transactions. Blockchain technology is a combination of different technologies involving cryptography etc. Algorithms ensure that the information that is stored in blockchain are made secure using cryptography hash function. The hash function is the connecting link between these blocks in the chain, thereby building a blockchain. The information in the distributed ledger stores this data in different nodes on a network. The minute details of every transaction are there in every block, along with the hash of the erstwhile block and the timestamp. It is difficult for an adversary to modify the stored details at majority points. Therefore, Blockchain provides better security when compared with a centralized system. A peer-to-peer network is the linchpin of the transactions. The mechanism is consensus centric. It boosts the confidence of users. The speed of processing is faster, it reduces the cost and makes tracking easier. Herein, smart contracts can add an extra feature of automated transactions, with the blockchain. Consequently, the advantages of blockchain technology include efficacy, security, and transparency which make it an emblem of faith in its execution for various applications. (NATIONAL STRATEGY ON BLOCKCHAIN Towards Enabling Trusted Digital Platforms, 2021)

It is to be noted that the sequence of ledgers in a blockchain is the same for every node. The public ledger is a repository of blocks collected in the sequence. Thereby storing the sequence of all the transactions on that ledger. An exception to this is a genesis block. This block contains a hash value pointer to the erstwhile block. Miners of the block can create a new block and attach it to the chain by using a type of consensus mechanism. Types of consensus mechanism are for example, proof of work, proof of stake (PoS), PBFT, etc. (Saleh, 2021) Any type of alteration to a block will fracture the hash pointer to that block. Hence, once a transaction is stored, it is difficult to alter it mischievously as against the blockchain. Furthermore, all the individual users that are participating in the blockchain do not use their real identities. In fact, with the help of hash function, cryptography and digital signature, they use several generated addresses. This also secures the privacy aspect of its users to a great extent. Bitcoin was the first application of a decentralized digital asset (Nieto et al., 2017). Bitcoin is highly in use because of its high security and immutability. Besides Bitcoin, multiple alternative currencies were projected, e.g., Ethereum, Zcash, Ripple etc. Overall, blockchain technology has garnered avowed interest from the public. It can be broadly bifurcated in three types, that is public blockchain, private blockchain and consortium blockchain. Because of the above-mentioned reasons, the arena of research involving blockchain is not only limited to alternate currencies but is being strongly pitched as an important concomitant for strengthening security. To this date, this technology has been populated in a wide array of fields, including blockchain-based DNS, security service for cloud (Zhu et al., 2019), IoT security(Khan & Salah, 2018) , and ancillary fields. This stream of technology has also emerged as a favorable approach for verification and management of evidence. (Tian et al., 2019)

In the domain of e-governance, Blockchain technology is being deployed to ensure added vigilance, precision and possibly shield data of high importance on governance issues against attacks. The linchpin attributes of e-governance are accountability, trust and probity, which are very well upheld by Blockchain technology. Because every dataset or transaction that is recorded in Blockchain is nearly impossible to intrude. All the participants in the system of e governance have assurance of truth and security. That makes it an usherer of overhauling measures that the government can take to make an impactful change, especially for the citizens of the digital world. For instance, in the stream of education, student documents like certificates, etc., can be safely stored in a Blockchain network. Many stakeholders, namely social welfare related bodies, institutions that deal with scholarships, administrative bodies can join hands in this initiative and have the records of a student stored on consensus basis. Similarly, in supply chain management, the capacity of blockchain network to track and trace, renders the entire process devoid of any careless mistakes. It is a secure proponent against attach by an insider as regards maintenance of information amongst various stakeholders. (Shukla, n.d.)

In the scheme of electronic governance, once trust is assured, the stakeholders can look forward to streamlining services and access to those services, in a hassle free manner. That is the empowerment which is brought about by digital spaces and their users.

Blockchain can empower the related office bearers to cross-check the proof of existence of documents. This can be done by a comparative analysis of the two set of evidences, originally stored on a blockchain and the one received for analysis. This ensures security. (National Strategy on Blockchain Towards Enabling Trusted Digital Platforms, 2021)

In contemporary times, a few models of blockchain centered digital evidence mechanisms have been offered. (Zyskind et al., 2015) The paper collates and problematizes these approaches to suggest the most sustainable solution for the fast growing legal and administrative framework based upon blockchain. For example, Zyskind et. al have suggested a personal data management platform premised upon blockchain. It is identical to the system of evidence management. In this case, the data pointer along with the access control list are stored in the blockchain itself. Therefore, only the permitted services can have access to the corresponding data. This stresses the fact that the suggested platform ensures privacy of personal data without the involvement of a trusted third-party. The advantage here is that the data cannot be traced. In contrast to the above, Bonomi et al. (Bonomi et al., 2020) have proposed a blockchain-based chain of custody (B- CoC) model. This model employs blockchain to trace the process of investigation of evidence and ensures that evidence is not modified anytime during the course of investigation. This guarantees the traceability and integrity of evidence. However, they also clarify that the application's scenario here is narrow as at every point in time, it is assumed that the evidence has a single owner. On the point of privacy, one may refer to the model suggested by Nieto et al. (Nieto et al., 2017) their model hinges upon digital evidence and the privacy element pertaining to the same. Using a personal device, they gauge the privacy related requirements in the event of digital witnessing, transmitted using a personal device. This is a balancing approach for both the elements. (Kosba et al., 2016); As a tangent to the above-mentioned applications, blockchain can be used in forensics related applications of vehicular networks. Cebe et. al proposed a blockchain- based vehicular forensics system (B4F). That uses VPKI and a ledger that is fragmented, for it to address the concerns of storage overhead and management of membership. This set up suits vehicular regime, as the evidence is stored in a blockchain. However, the authors suggest that this regime is suitable for networking of vehicular management, it may not be overarchingly applied in all scenarios. (Peng et al., 2020)

Moving to a forensic integrated model. Lone and Mir propose Forensic-Chain model. This is another model that is based on blockchain centred chain of custody. They have projected the comprehensiveness of blockchain technology in their work. They suggest that the scope and ambit of a blockchain based model holds immense promise for the forensic society. They further suggest that events and actions can be viewed comprehensively to origination and that is the biggest strength of their approach. They are optimistic in the capability of blockchain forensics and are focused on bringing anti-tampering and integrity prone features to forensic investigations. In their work, they have provided Proof of Concept in Hyperledger Composer and then assessed its performance. (Lone & Mir, 2019)

Whereas Tian, Li, Qui et. al are focused on weaknesses or vulnerabilities of a blockchain based forensic evidence management. The authors emphasize upon pre-existing digital evidence management tools which are generally centralized in design. These offer a tamper-resistant mechanism on a single device or a rather centralized system via secure software, a secure hardware, as well as physical separation or admixture of strategies. The centralized design faces many challenges, namely a single spot of failure, which may invalidate the entire system; the issue of scalability, that arises if the amount of evidence is quite voluminous to store. They also attest to the fact that blockchain technology holds promise which can be used to overcome the erstwhile challenges due to its inherently distributed, tamper proof and private. They emphasize that blockchain also faces a pertinent scalability issue, that of blockchain bloat. Eventually, as the length of the blockchain increases, the requirement of storage for each node also increases. Hence, a blockchain that is lightweight is required for creating a secure digital evidence regime. Also, at the same time, to guarantee access and veracity of the evidence, the evidence should be able to be tracked. They highlight the hurdle that tracking the evidence while guaranteeing privacy is also another one of the problems associated with the use of a blockchain. They propose the Block DEF Model. The main contributions of this model are namely- firstly a coupling design that is loose. The pressure of storing evidence is less in this model because only that evidence information is stored in a blockchain, and the impugned evidence is stored on a trusted storage platform. Secondly, two multiple signature mechanisms for submission of evidence and its retrieval are proposed, such that there is balancing of elements of traceability as well as the privacy. Thirdly, to avoid the issue of blockchain bloat, a consensus mechanism is devised in which a lightweight blockchain along with a mixed block structure and an optimized name-based practical byzantine fault tolerance (PBFT) is created. Every node is only required to store all the block headers and a portion of the bodies of the block. The resultant analysis and experiment of these authors has exemplified that this model effectively supports the issue of scalability, integrity, privacy, veracity and the ability to be traced. They further state that the presentation of the Internet has changed from host centric to completely content centric. The primordial demand of users of the internet is retrieving

and publishing and retrieving content. (L. Zhang et al., 2014) (Q. Zhang et al., 2023). In this situation, the content may be a file or a portion of a file that is carried across the internet, for example, images, web pages, audio files or video files. Hence, the security of content becomes a crucial part of cyber security. It mainly hinges upon three properties related to security, that is – non- repudiation, privacy and integrity of evidence. It is highlighted in their work that not all contents are properly protected. Various files are obliterated due to network attacks or other reasons. Such tampering of files has cascading negative effects. For instance, tampering of a web page can be used to design phishing attacks or broadcast illicit information. Malware codes can be infected in executable files by the attacker to monitor the user's behavior or illegally try to access their private data. They further state their limitations that for technical as well as economic and legal reasons, it is often needed to carry out an investigation of the consecutive digital evidence for file tampering. (Tian et al., 2019)

It is to be noted that Bonomi, Casini and Ciccotelli propose B- CoC, a chain of custody which is based on blockchain technology and focusses upon a seamless evidence management system. Their main argument is that one of the crucial issues in digital forensics is the management of evidence. From the time of evidence collection until the time of their assessment in the court, the evidence can pass through various points, thereby increasing the risk of its tampering. This process, as discussed above, is termed as a Chain of Custody (CoC), should guarantee that evidence is not modified during the investigation, despite many entities having owned them, to be admissible in a court of law. Currently CoC of digital evidence is managed entirely in manual mode with entities involved in the chain required to fill in documents accompanying the evidence. This Blockchain-based Chain of Custody (B-CoC) in their model will be based on dematerializing the CoC process. That they suggest guarantees auditable integrity of the collected evidence and owner's traceability. They again explain that the Chain of Custody is the process which validates how evidence has been collected, tracked and carried in a protected means to a court of law. However, it is clarified that the Chain of Custody (CoC) is not a mandatory step in forensic analysis. It is popularly used as evidence, but to be accepted in a court or in legal proceedings, it must be proved to be unaltered during investigations. Hence, a reliable process including CoC must use a standard to deal with and handle the evidence, regardless they are digital or not, and regardless of whether that evidence will be utilized in a trial or not. For experiment, they had used a private permission blockchain and then they implemented a smart contract in order to keep track regarding the ownership changes during the life cycle of the evidence in question. (Bonomi et al., 2020)

A complex challenge for testing the blockchain based forensic evidence has been dealt with by Jurcut and Agbedanu. They propose BLOF, that is a blockchain based forensic model for Internet of Things (IoT). They have problematized the arena of digital forensics for blockchain. The vulnerabilities are higher in this system and are largely unexplored. The forensics in this field deals with cloud, network and device. Their model leverages the decentralized property of blockchain to ensure that the logs produced in IoT environments are stored on the network and are available for verification by any of the participating nodes in the network. To be noted that each block contains a transactional value of hashed values computed from logs. These logs are taken out from the various entities, then attached with a hash function and lastly, written onto the blockchain network as transactions. The nodes here are made up of multiple forensic stakeholders, network and IoT devices and cloud service providers. Here the blocks are only proposed after a consensus has been concluded by the nodes. These logs that are extracted by this mechanism, hashes them. Therein, the hashed values are then written on the block as a individual transaction. They further explain the reason behind the choice of hashing these logs, that these logs might contain sensitive data. Hence, it is not advised by the authors of this model to store these logs as mere plaintext. Secondly, they explain that hashing the logs leads to a reduction of their size which eventually minimizes the time that is needed to process these logs. The last part of this model is the user centre. According to this model, the user centre is comprised of courts as well as the forensic investigators. This component of this model has made it possible for forensic investigators to cross-check the authenticity of the logs presented to them by service providers. Moreover, the forensic investigators can also verify the authenticity of these logs as they are being forwarded from one investigator to another during the chain of custody. In fact, even the court can verify the authenticity of evidence produced by the prosecutors and decipher if such evidence is worthy of being admitted before the court. This prevents the investigators from tampering with logs to either incriminate people that are innocent, or to exonerate the criminals. (Agbedanu & Jurcut, 2021)

5. Analyzing The Existing Studies Employing Blockchain Technology

As described above, blockchain technology affects a decentralized fully replicated, append- only ledger, in a peer-to-peer network that was originally deployed for the cryptocurrency named Bitcoin. In this, all the participating nodes preserve a full local copy of the blockchain. This blockchain consists of a sequence of the blocks that contain the transactions of that ledger. These transactions inside the blocks are categorized in a chronological manner and each block consists of a cryptographic hash of the erstwhile block in the chain. The nodes here create fresh blocks as they receive the transactions that are broadcasted on the network. Hence, once a block is complete, the consensus process

starts to convince fellow nodes to include it in the blockchain. It is to be noted that in the original blockchain technology utilized in Bitcoin, the consensus process was based on concept of Proof-of- Work (PoW). (Nakamoto, 2009). With this, the nodes then compete against each other to confirm transactions and then create new blocks by detangling a mathematical puzzle. This is a computation -based task, hence verification of its validity is easy. But to incentivize this mechanism, solving a block also leads to mining several bitcoins, which is considered as the reward for a block creator, also called as a miner. Many a times, more than one miner can also generate a valid block. This creates forks in that chain. These forks are solved by accepting only the branch which is the longest as the valid continuum of that chain. This then eliminates forks ultimately. Here, the main advantage of PoW, over a traditional consensus algorithm, is that a hacker or an attacker would first need to control much of the computation power of the network and not many of the nodes. This in turn is rather a strenuous task and virtually impossible in public large-scale networks. (Bonomi et al., 2020). A specific type of PoS is Proof-of-Authority (PoA) in which what is under threat is, identity of an individual and not the cryptocurrency. Further, with PoA, the validators must have been authorized by prevention and their identities are then known. Resultantly, acting with malice results in loss of personal reputation and finally in being expelled from the validator set. (Bentov et al., 2016)(Bonomi et al., 2020)

Bonomi et al. also discussed that PoW is more suitable for being used in public networks. However, both PoS and PoA may be deployed for private networks. Moreover, both can be aptly used in permissionless networks, that is the networks where nodes are free to join the network without taking any prior authorization. For example, as needed in Bitcoin and Ethereum. The PoA, is typically used in permissioned blockchain networks, that is the networks in which nodes are not able to freely join and become validators. Here they must be authorized preventively. (Bonomi et al., 2020)

An important feature of the above discussed Block DEF model is that it reduces wastage. Waste, in use of blockchain regarding the evidence management. However, there is dearth of literature on critique of this model. (Tian et al., 2019)

In the B CoC model, it can be concluded that it compromises on privacy but is useful for private networks. (Bonomi et al., 2020)

Model named, BLOF- its application has been confined to Internet of Things. It cannot be ignored that such systems are complex and dynamic. The model is based on verification of logs by every stakeholder regarding digital evidence, that is law enforcement agencies, cloud service providers and the courts. It is to be noted in this model that the traditional digital forensics investigators solely depend on the CSPs, network and IoT devices for evidence when it comes to the IoT forensics. This huge dependence on Cloud Service Providers (CSP) may culminate in compromising pieces of evidence at hand. The problem with this proposed model not only ensures the integrity of logs with the use of a decentralized ledger, but also allows logs used as a piece of evidence to be eventually verified by multiple stakeholders in the forensic process. In this model, the forensic investigator relies heavily on the CSP and IoT devices for the evidence. However, this is the quality of hashed evidence which are the logs generated by the cloud instances, network and the IoT devices, after a forensic investigator receives this evidence from a CSP. The hashed value is thereafter compared to the hashes stored as transaction values on the network of blockchain. The task before an investigator then is to search for the hashed value on the blockchain network. Here, if the hash value exists on the blockchain, thereafter, the log is accepted by the investigator. Ultimately, it is forwarded to the court as a credible piece of evidence. On the contrary, if the hash value cannot be found on the blockchain network, in that case, the log is rejected. In this situation, when the court receives a particular evidenced log from a forensic investigator, it is enabled to determine the credibility of that log by similarly hashing that log and then comparing the hashed value to the hash values on the blockchain network. If the value exists, the evidence is accepted by the court, otherwise, it is thereby rejected. (Agbedanu & Jurcut, 2021)

6. Application of Blockchain by Indian Regulators

Firstly, the MeitY has launched a project that involves many entities, it is titled “Distributed Centre of Excellence in Blockchain Technology with C- DAC, Institute for Development & Research in Banking Technology (IDRBT), Hyderabad and Veermata Jijabai Technological Institute (VJTI), Mumbai” as executing agencies. In this initiative, the agencies have conducted research on the use of Blockchain technology in various domains and then developed Proof-of-Concept solutions to the same. In this use case, a Blockchain technology centric solution for property registration has been developed and has been presented as a pilot project at Telangana. Furthermore, the project website states that “Proof-of-Concept solutions have been curated for empowering the Cloud Security Assurance, Central Know Your Customers (CKYC) and trade finance. Here a generic Proof-of Existence (PoE) Framework has been developed to enable PoE for digital artifacts that will be utilized to check the integrity of academic certificates, sale deed documents, MoUs, etc. With the use of PoE framework, an innovative solution has been developed in the process of authentication of academic certificates. This is being piloted at the C-DAC Advanced Computing Training School (ACTS),” another purpose is to issue

the participation certificates in conducting academic events. MeitY has also initiated another project that is premised upon design and development of a National Blockchain Framework (NBF), in order to build a shared Blockchain infrastructure and offer Blockchain as-a- Service (BaaS). (National Strategy on Blockchain Towards Enabling Trusted Digital Platforms, 2021)

Taking the efforts forward, the National Informatics Centre (NIC) along with National Informatics Centre Services Inc. (NICSI) has also established a Centre of Excellence (CoE) in Blockchain technology in Karnataka in 2020. The main objectives of this are "to speed up the adoption and deployment of Blockchain technology in Government, execute the projects which are focused on different use cases, pilot deployment of those, offer Blockchain Platform-as-a-Service to invigorate the design and progress of upcoming solutions, offer consultancy of services and inculcate capacity building. This CoE is looking forward to collaborating across Government, public and private sectors. The areas of application that have been identified and developed through are Digidhan, land documentation, Public Distribution System, land registration, GST's back office and the Excise Management System". (NIC, n.d.-a)(NATIONAL STRATEGY ON BLOCKCHAIN Towards Enabling Trusted Digital Platforms, 2021)

Furthermore, C-DAC, that is the Centre for Development of Advanced Computing, is also developing a unified blockchain framework for offering national blockchain service and creation of a harmonious ecosystem. Potential applications of this are namely, the chain of education certification, supply chain of logistics, enforcement activities regarding the GST, supply chain of State Excise, Public Distribution System, Blood Bank, Government e-Marketplace (GeM), National Health Records, Electronics & Semiconductor supply chain, Trace & Track supply chain applications, Blockchain enabled Digi locker etc. (CDAC, n.d.)

The NITI Aayog has announced that "it is currently working on various Blockchain related use cases. In collaboration with the Gujarat Narmada Valley Fertilizers and Chemicals Limited (GNFC), it has curated a blockchain based system regarding the fertilizer subsidy. This team has also partnered with PwC and Intel to further optimize the supply chain for the subsidy regarding fertilizers". (Ayog, 2018)

This is the junction where the research gap is crucial on this subject and the relevance of this study lies.

7. Further Work

Recently, the Lieutenant Governor of Delhi launched Blockchain Technology in an Inter-Operable Criminal Justice System for Delhi Forensic Science Laboratory. This is intended to become the first in India to collect information and evidence with minimum intervention of humans. It also makes the former the first institution of this category to use blockchain technology for transparent, tamper-proof digital recording of concerned evidence. The officials stated that this step would augment and automate the entirety of forensic flow of work, that starts from the police to the FSL. This would render data entry by the Investigating Officer at the police station level, available to the FSL directly, without disclosure of crucial details such as the FIRs or names of parties to make sure that there is confidentiality and privacy. This is a welcome step in application of blockchain in governance. (NIC, n.d.-b)

Subsequently, the Government of India has also started a "Future Skills Prime program that envisages upskilling as well as reskilling around blockchain to address the urgent need for growing the skilled talent pool. This involves NIELIT and C-DAC".(NIELIT, n.d.)(NATIONAL STRATEGY ON BLOCKCHAIN Towards Enabling Trusted Digital Platforms, 2021)

This is in juxtaposition to the vision and mission of the National Strategy on Blockchain, towards enabling trusted digital platforms, introduced by the Ministry of Electronics and Information Technology (MeitY) in December, 2021. (NATIONAL STRATEGY ON BLOCKCHAIN Towards Enabling Trusted Digital Platforms, 2021)

8. Conclusion

As suggested by a study conducted, "By 2030, Blockchain would be used as a foundational technology for 30% of the global customer base that will be made up of things, and these things will be used for conducting commercial activities. By 2025, Blockchain would add a business value that will grow to over $176 billion. This would increase further to $3.1 trillion by 2030". (Lovelock et al., 2017) (NATIONAL STRATEGY ON BLOCKCHAIN Towards Enabling Trusted Digital Platforms, 2021)

It can be concluded that the transactions involving a blockchain platform consume time. They are also computation wise consuming immense energy. This highlights a threat to sustainability aspect on this subject. Hence, it is furthered that

any application or use case which is envisioning its implementation via this technology should necessarily first conduct a survey or audit of its transaction related time and then produce an estimated expenditure on the challenges highlighted in the above discussion. Relying on the credibility of smart contracts, further study can be conducted to understand the mushrooming problems to security for forensic investigations that are based upon this novel technology.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Agbedanu, P., & Jurcut, A. D. (2021). BLOFF: A Blockchain based Forensic Model in IoT. March, 59–73. https://doi.org/10.4018/978-1-7998-7589- 5.ch003

[2] Ayog, N. (2018). NITI Aayog partners with GNFC Ltd to implement Fertilizer Subsidy Disbursement through Blockchain Technology.

[3] Bentov, I., Gabizon, A., & Mizrahi, A. (2016). Cryptocurrencies without proof of work. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 9604 LNCS(February), 142–157. https://doi.org/10.1007/978-3-662-53357- 4_10

[4] Bonomi, S., Casini, M., & Ciccotelli, C. (2020). B-CoC: A blockchain-based chain of custody for evidences management in digital forensics.OpenAccess Series in Informatics, 71. https://doi.org/10.4230/OASIcs.Tokenomics.2019.12

[5] CDAC. (n.d.). Design and Development of a Unified Blockchain Framework for offering National Blockchain Service and creation of Ecosystem.

[6] Chawhan, G., Patole, D., Borse, Y., Kukreja, G., Parekh, H., & Jain, R. (2021). Advantages of Blockchain in Digital Forensic Evidence Management.SSRNElectronicJournal. https://doi.org/10.2139/ssrn.3866889

[7] Conlan, K., Baggili, I., & Breitinger, F. (2016). Anti-forensics: Furthering digital forensic science through a new extended, granular taxonomy. DFRWS 2016 USA - Proceedings of the 16th Annual USA Digital Forensics Research Conference, 18(December 2015), S66–S75. https://doi.org/10.1016/j.diin.2016.04.006

[8] THE DIGITAL PERSONAL DATA PROTECTION ACT, 2023 (NO. 22 OF 2023), (2022).

[9] Kaushik, K., Tanwar, R., Dahiya, S., Bhatia, K. K., & Wu, Y. (2022). Unleashing the Art of Digital Forensics. In Unleashing the Art of Digital Forensics. https://doi.org/10.1201/9781003204862

[10] Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. Future Generation Computer Systems, 82, 395– 411. https://doi.org/10.1016/j.future.2017.11.022

[11] Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts. Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016, 839–858. https://doi.org/10.1109/SP.2016.55

[12] Lone, A. H., & Mir, R. N. (2019). Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digital Investigation, 28, 44–55. https://doi.org/10.1016/j.diin.2019.01.002

[13] Lovelock, J.-D., Reynolds, M., Granetto, B. F., & Kandaswamy, R. (2017). Forecast : Blockchain Business Value, Worldwide, 2017-2030. In Gartner Inc. (Issue March). https://ssofed.gartner.com/sp/startSSO.ping?PartnerIdpId=urn:federation:accenture&TargetResource=https%3A%2F%2Fwww.gartner.com%2Fdocument%2F3627117%3Fref%3Dd- linkShare

[14] NATIONAL STRATEGY ON BLOCKCHAIN Towards Enabling Trusted Digital Platforms, 1 (2021).

[15] Proposed Digital India Act , 2023, GOI (2023). https://www.meity.gov.in/writereaddata/files/DIA_Presentation 09.03.2023 Final.pdf

[16] Mukrimaa, S. S., Nurdyansyah, Fahyuni, E. F., YULIA CITRA, A., Schulz, N. D., Taniredja, T., Faridli, E. M., & Harmianto, S. (2016). Digital Forensics, Investigation, and Response. In Jurnal Penelitian Pendidikan Guru Sekolah Dasar (Vol. 6, Issue August).

[17] Nakamoto, S. (2009). Bitcoin: A peer to peer electronic currency. 1–4.

[18] NIC. (n.d.-a). Centre of Excellence - Blockchain Technology. https://blockchain.gov.in/home.html

[19] NIC. (n.d.-b). Launch of Blockchain Technology in Inter-Operable Criminal Justice System for Delhi Forensic Science Laboratory . 1–4.

[20] NIELIT. (n.d.). Future Skills PRIME.

[21] Nieto, A., Rios, R., & Lopez, J. (2017). Digital witness and privacy in IoT: Anonymous witnessing approach. Proceedings - 16th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 11th IEEE International Conference on Big Data Science and Engineering and 14th IEEE International Conference on Embedded Software and Systems, 642–649. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.295

[22] Peng, C., Wu, C., Gao, L., Zhang, J., Yau, K. L. A., & Ji, Y. (2020).Blockchain for vehicular internet of things: Recent advances and open issues. Sensors (Switzerland), 20(18), 1–37. https://doi.org/10.3390/s20185079

[23] Saleh, F. (2021). Blockchain Without Waste: Proof-of-Stake. Review of Financial Studies, 34, 1156. https://doi.org/10.2139/ssrn.3183935

[24] Shrunga, H. S., M, A., U, D., R, S., & K R, R. (2022). A Survey on Blockchain Based Digital Forensics Framework. International Journal for Research in Applied Science and Engineering Technology, 10(4), 2542–2549. https://doi.org/10.22214/ijraset.2022.41841

[25] Shukla, S. K. (n.d.). Blockchain for E-Governance and Other Applications What problems we are addressing ?

[26] Tian, Z., Li, M., Qiu, M., Sun, Y., & Su, S. (2019). Block-DEF: A secure digital evidence framework using blockchain. Information Sciences, 491, 151–165. https://doi.org/10.1016/j.ins.2019.04.011

[27] Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Claffy, K. C., Crowley, P., Papadopoulos, C., Wang, L., & Zhang, B. (2014). Named data networking. Computer Communication Review, 44(3), 66–73. https://doi.org/10.1145/2656877.2656887

[28] Zhang, Q., He, Y., Lai, R., Hou, Z., & Zhao, G. (2023). A survey on the efficiency, reliability, and security of data query in blockchain systems. Future Generation Computer Systems, 145, 303–320. https://doi.org/10.1016/j.future.2023.03.044

[29] Zhu, L., Wu, Y., Gai, K., & Choo, K. K. R. (2019). Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 91, 527–535. https://doi.org/10.1016/j.future.2018.09.019

[30] Zyskind, G., Nathan, O., & Pentland, A. S. (2015). Decentralizing privacy: Using blockchain to protect personal data. Proceedings - 2015 IEEESecurity and Privacy Workshops, SPW 2015, 180–184. https://doi.org/10.1109/SPW.2015.27