DIGITAL DOCUMENTS MANAGEMENT FRAMEWORKS: A COMPARATIVE STUDY

Gajanan Badhe, Dr. Maithili Arjunwadkar

Progressive Education Society's Modern Institute of Business Studies, Pune -411044

Abstract: Although there were number of methods and techniques developed for providing security to the digital documents such as cryptography, digital signature but over the existing structure of web applications they found to be very limited to protect the vulnerabilities with the digital documents and the question of originality and trust becomes very critical as even cloud computing technology also have some short falls in providing full flexed data security to the data storage. To overcome such problems the digital ledger technology has emerged into its new form as blockchain technology. Because of its permanent nature of block based storage system and self-executing consensus mechanism it has been applied to ensure the security of digital documents. Blockchain technology is the core technology behind the cryptocurrency or digital currency. This paper focuses on the blockchain technology and application of blockchain technology for the digital document management in terms of storage of digital documents, secured access control for verification and validation of the digital documents stored on the online platform. Also presents a comparative study of various available frameworks for digital document management designed with the help of blockchain and its allied technologies.

IndexTerms - Digital Ledger Technology, Digital Document Management, Blockchain Technology, cryptocurrency, Document storage and verification.

I. Introduction

In earlier days paper documents were very crucial for any issuing and generating kind of certificate, report or any official document till the digitization of paper documents into e-documents or digital documents. Use of these digital or e-documents are safe as long as they are used only for the purpose they are generated; but over time with the advancement of computational technologies related to image processing the forging of online documents and presenting fake documents comes into practice. The security of original documents is the main concern in any kind of communication and it has been proven over the long time that it may be either retention of original documents or transfer of documents from one place to another. Along with the paper based documents e-documents or digital documents were developed although the use of digital documents or e-documents are safe as long as they are used only for the purpose they are generated; but over time with the advancement of computational technologies related to image processing the forging of online documents and presenting fake documents comes into practice. Though there were number of security providing methods and techniques developed such as cryptography, digital signature but over the existing structure of web applications they found to be very limited to protect the vulnerabilities with the digital documents and the question or originality and trust becomes very critical as even cloud computing technology also have some short falls in providing full flexed data security to the data storage. To overcome such problems the digital ledger technology has emerged into its new form as blockchain technology. Because of its permanent nature of block based storage system and self-executing consensus mechanism it has been applied to ensure the security of digital documents. Blockchain technology core is the technology behind the cryptocurrency or digital currency. The paper presents the various concepts involved in blockchain technology and application of blockchain technology for the digital document management in respect of storage of digital documents, secured access control for verification and validation of the digital documents stored on the online platform. A Comparative study of various available frameworks for digital document management designed with the help of blockchain and its allied technologies.

II. Digital Document Management

Digital documents management is very important as over time it is very difficult to manage the documents in paper based forms as well as over the online platform in a secure manner. There are many loopholes that are with the manual system of documents management, authentication and verification. Also somewhat the same scenario with the digital documents system which are

available on the online platform like internet in the form of web based applications and also cloud computing based applications. The existing systems either simple web based or cloud computing based applications are based on the principle and concept of client-server computing model and there are a number of security threats to this kind of computing model especially for the data which has some very high importance in terms of monetary benefits or authoritative benefits. Although the terms like digital document and e-document of electronic documents are mostly used interchangeably or they are considered as synonymous. But there is conceptual and functional difference in these terms as digital documents can be seen as the converted document from its original paper form and e-document can be any transactional document which is exchanged between trading partners in an electronic format and means. They are different from pdf or image files. E-documents are machine readable and typically exchanged via software or online platforms rather than email. Some of the examples of e-documents are purchase orders, Invoices of various types, credit/debit notes, correction invoices, dispatch advice, goods receipt notes and payment instructions etc. Adopting the digital documents allows us to search and track the records very instantly at any point of time from anywhere. It also saves valuable time, expenditure and ensures very improved communication among team and other entities.

III. Blockchain Technology

Satoshi Nakamoto has presented a core concept of blockchain technology in his whitepaper titled as "Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto" (Satoshi Nakamoto, 2008). Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks. Blockchain provides the permanent data storage through its data structure which involves no editing or deletion after writing the data in the blocks. These blocks are linked to each other by storing cryptographic hash of every previous block in the next block that forms the chain of blocks and therefore it is called a blockchain. The hash function helps in managing the security, integrity and immutability of the blockchain. The new block is created and added at the end of the existing blockchain by the process of mining. The blockchain includes components such as transaction, blocks, cryptography, smart contracts, consensus algorithms, peer to peer network.
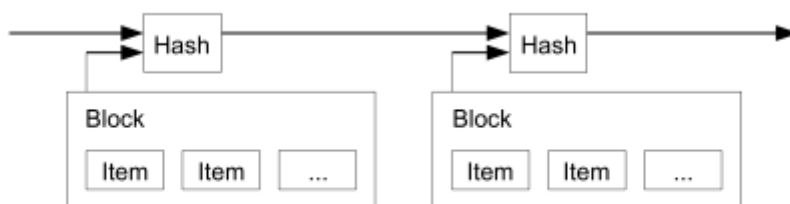
Source (Satoshi Nakamoto, 2008) Figure1: TimeStamp Server

Ethereum is a blockchain-based, public, and open-source distributed computing platform using a Proof-of-Stake (PoS) consensus algorithm including smart contract functionality.

There are three types of blockchains categories (Zheng et al., 2017) as public, private, and consortium. A public blockchain is the standard blockchain network that is open to all and has no central administration, allowing anyone to access the network and participate in reading, writing, and auditing the blockchain. permissionless and decentralized system that allows anyone to create, validate and view transactions at any point in time. The decision-making regarding transaction validation is made by consensus algorithms like Proof-of-Work or Proof-of-Stake. The examples of public blockchains are Bitcoin and Ethereum.

(a) Public Blockchain.   (b) Private Blockchain.   (c) Federated/Consortium Blockchain.
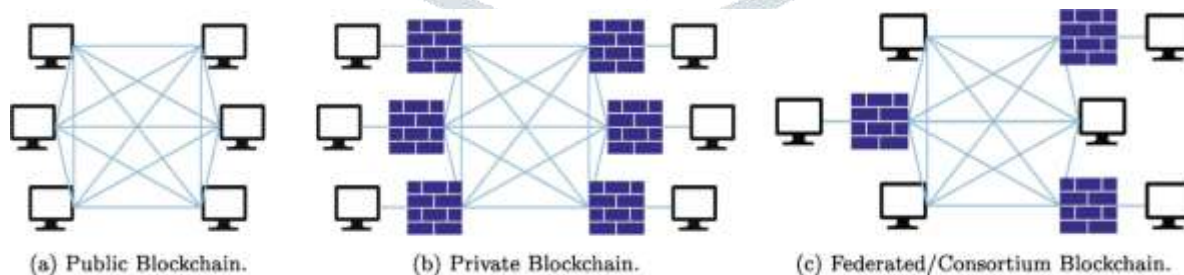
Figure 2. Types of Blockchain networks.

A Private blockchain is a sort of blockchain in which an proprietor of the community can read, write and audit the blockchain. The vital incharge also can offer permissioned get right of entry to choose nodes to validate and think about transactions at designated factor of time only. As it's far an crucial Private consensus is executed on the discretion of the vital incharge to undergo a vote casting and multi celebration consensus set of rules. The instance of a non-public blockchain is Hyperledger Fabric.

A Consortium blockchain is a collection owned device and Permissioned blockchain in which an autonomy is eliminated and there's a couple of vital in charge who will offer right of entry to to pre-decided on nodes to read, write and audit the blockchain. Consensus is received with the aid of using contributors of the consortium via a vote casting and multi celebration consensus set of rules primarily based totally at the consent with the aid of using the participants.

The following figure shows the history of blockchain technology and its evolution over the time to most recent developments.
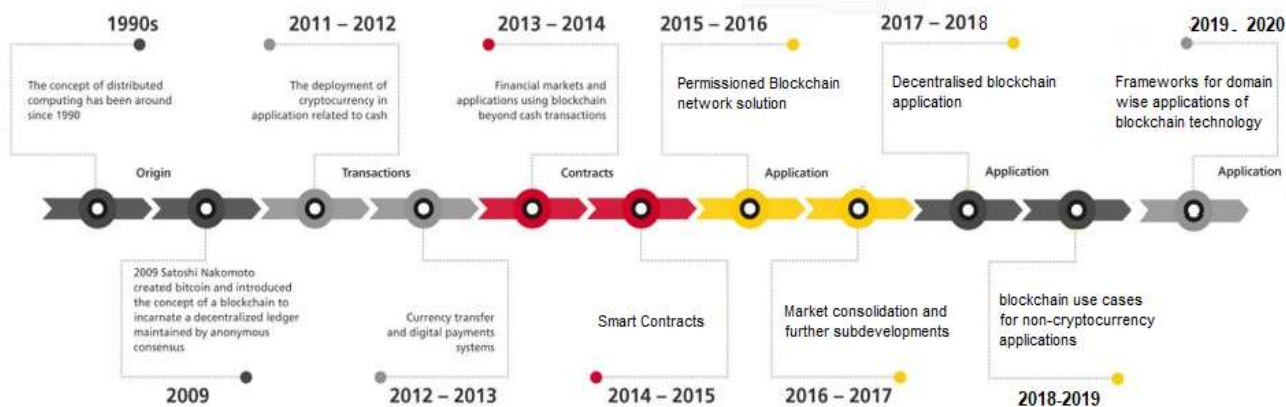
Figure 3: History and Evolution of Blockchain technology (Source: Accenture)

IV. Comparison of frameworks for digital document management using blockchain technology

Title of paper / framework	Problem addressed	Blockchain platform and type of blockchain	Consensus mechanism	Major technique/idea used for proposed system	Major components of proposed framework	Advantages of proposed framework	Remarks on proposed framework
Proposing a reliable method of securing and verifying the credentials of graduates through blockchain	Fake certificates and dummy certificates issue	Ethereum test network. Consortium blockchain	Proof of Stake as consensus on Ethereum Platform	Proposed system with every block stores information like Adhar as student-id, marks statement details, time stamp and hash value using SHA256.	Certificate Authority, Certificate verifier, Certificate unique id and aadhar id for verification	mechanism using blockchain technology is proposed to store the genuine certificates in digital form and verify them	Provides adhar based educational credential verification
DMS-XT: a blockchain-based document management system for secure and intelligent archival	Secure Document management,	No specific platform proposed; Any Generic platform for blockchain	No specific Consensus used; its depend upon type of blockchain	Information Extraction techniques, PDF parser, Information extractor, Information-view builder and encryption module	blockchain network, database, IPFS,	to verify the ownership and content by retrieving and decrypting information-view stored in the blockchain	Provides a intelligent archival for document management
Cerberus: A Blockchain-Based Accreditation and Degree Verification System	Credential frauds and certificate verification problems	Parity, Ethereum Virtual Machine	Proof- of- Authority consensus engine	Proposed system addresses the on-chain digital contract and disallows the student to entail digital identity.	Student, University, Accreditation body, Employer, QR code of Certificate, digitally signed transaction to be saved on blockchain	Security for academic Credentials against modifi-cation and manipulation. Provides secured means for verification by legitimate entities	Based on integration with legacy systems, impact of speed of operation as it involves scanning of original documents. Conceptual prototype
Secure E-Documents Storage using Blockchain Ayush	Providing secured storage for documents against tampering	Blockchain api,	No specific Consensus used; its depend upon type of blockchain api	Uses third party hardware named Bottle-server as interface between the blockchain network and the users.	Third party bottle server, adhar number, user, blockchain network	Provides Blockchain based storage for documents, adhar id is used for identification and authentication	Based on blockchain api, system can not able provides additional functionalities
Digital Degrees and Markcards Using Blockchain	forgery and falsification of documents and	Hyperledger Fabric and Hyperledger	RAFT Consensus	Uses web applications to create digital	-front end web application,	permissioned blockchain based solution for	proposed model to restrict forgery and falsification

Technology	verification issue	Composer, permissioned blockchain		certificates in pdf and json format and uses ipfs as distributed storage. With Hyperledger hash pointer link is created to asset.	Interplanetary file system (IPFS) and Hyperledger fabric	forgery and falsification of documents	of certificates.
Online Certificate Validation Using Blockchain	problem of counterfeiting certificate	Ethereum Platform	Proof of Stake as consensus on Ethereum Platform	Web based Electronic Certificate System generates QR code and Serial number which is stored on the blockchain	Electronic Certificate System, smart Contracts, QR Code and Serial Number on Blockchain	proposed blockchain-based system reduces the likelihood of certificate forgery	Provides online generation and verification of certificates by making the process open and transparent.

V. Conclusion

With the varied nature of applicability and availability of various blockchain platforms and tools, its applications are increasing day by day for digital document management in respect of storage of digital documents, secured access control for verification and validation of the digital documents stored on the online platform. The paper presented a detailed comparative study of various available frameworks for digital document management designed with the help of blockchain and its allied technologies. Although this study was mainly limited to the comparison of frameworks for digital documents management using blockchain technology, we are planning to undertake the detailed technological study on various blockchain technology platforms and tools available for the respective platforms, their usability and performance.

References

[1]   Satoshi Nakamoto (2008), Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf.

[2]   T. Rama Reddy, P. V. G. D. Prasad Reddy, R. Srinivas, C. V. Raghavendran, R. V. S. Lalitha, and B. Annapurna, "Proposing a reliable method of securing and verifying the credentials of graduates through blockchain," *EURASIP J. Inf. Secur.*, vol. 2021, no. 1, 2021, doi: 10.1186/s13635-021-00122-5.

[3]   E. Martiri and G. Muça, "DMS-XT: A blockchain-based document management system for secure and intelligent archival," *CEUR Workshop Proc.*, vol. 2280, pp. 70–74, 2018.

[4]   A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," pp. 1–14, 2019, [Online]. Available: http://arxiv.org/abs/1912.06812.

[5]   A. S. Ghanghoria, A. S. A. Raja, V. J. Bachche, and M. N. Rathi, "Secure E-Documents Storage using Blockchain," vol. 07, no. 03, pp. 1972–1974, 2020.

[6]   N. Sarganachari, A. Anjum, and S. IL Christa, "Digital Degrees and Markcards Using Blockchain Technology," pp. 14038–14046, 2020, doi: 10.15680/IJIRSET.2020.0902052.

[7]   N. Swetha and S. Priya, "Online Certificate Validation Using Blockchain," *Spec. Issue Publ. Int. Jnl. Adv. Netw. Appl.*, pp. 132–135.

[8]   J. B. Sastry and B. G. Banik, "A novel blockchain framework for digital learning," Indian J. Comput. Sci. Eng., vol. 12, no. 3, pp. 728–734, 2021, doi: 10.21817/indjcse/2021/v12i3/211203283.

[9]   Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017, July, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85