A Thesis/Project/Dissertation Report

on

Dropbox using block chain

Submitted in partial fulfillment of the
requirement for the award of the degree of

B.Tech / CSE

(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Under The Supervision of
Name of Supervisor: Dr. Kuldeep Singh Kasan
Designation : Professor

Submitted By

Pratikshit Vashistha
18021180034
Amogh Gupta
18021011446

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING /
DEPARTMENT OF COMPUTERAPPLICATION
GALGOTIAS UNIVERSITY, GREATER NOIDA
INDIA
December, 2021

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY, GREATER NOIDA

CANDIDATE'S DECLARATION

I/We hereby certify that the work which is being presented in the thesis/project/dissertation, entitled **"DROP-BOX USING BLOCKCHAIN "**in partial fulfillment of the requirements for the award of the B.tech submitted in the School of Computing Science and Engineeringof Galgotias University, Greater Noida, is an original work carried out during Aug- Dec, 2021, under the supervision of , Department of Computer Science and Engineering/Computer Application and Information and Science, of School of Computing Science and Engineering , Galgotias University, Greater Noida

The matter presented in the thesis/project/dissertation has not been submitted by me/us for the award of any other degree of this or any other places.

Pratikshit Vashistha -18SCSE1180035

Amogh gupta- 180SCSE1010204

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Dr. Kuldeep Singh Kasan

Professor

CERTIFICATE

The Final Thesis/Project/ Dissertation Viva-Voce examination of Pratikshit vashistha-18021180034, Amogh gupta-18021011446 has been held on _____ and his/her work is recommended for the award of B.tech

Signature of Examiner(s) **Signature of Supervisor(s)**

Signature of Project Coordinator **Signature of Dean**

Date:

Place: Greater Noida

Table of Contents

Abstract

The demand for Blockchain innovation and the significance of its application has inspired ever-progressingexploration in various scientific and practical areas. Even though it is still in the initial testing stage, theblockchain is being viewed as a progressive solution to address present-day technology concerns, such as de-centralization, identity, trust, character, ownership of data, and information-driven choices. Simultaneously,the world is facing an increase in the diversity and quantity of digital information produced by machines andusers. While effectively looking for the ideal approach to storing and processing cloud data, the blockchaininnovation provides significant inputs. This article reviews the application of blockchain technology for se-curingcloudstorage.

CCSConcepts:•**Generalandreference**→**Surveysandoverviews**;•**Computersystemsorganization**→*Peer-to-peerarchitectures*;•**Informationsystems**→*Distributedstorage*;•**Securityandprivacy**→*Securityservices*;

AdditionalKeyWordsandPhrases:Blockchaintechnology,decentralization,cloudcomputing,cloudsecurity,cloudstorage

INTRODUCTION

In recent years, cloud technology has attained an emerging trend by showing a possibility in bothacademia and industry for its efficiency and availability. Although it is a widely accepted technol-ogy,withanoutburstofdataorigins,therehasbeenanincreasedissueofstorageandusageofdata owing to the inability of a conventional data management tool to manage the exponentiallygrowing data. The traditional cloud storage model comprised a back-end platform that could bestorage or server, a front-end platform that could be a mobile device or a client and a network,possibly an intranet or internet. Attention is given to cloud technology with this outburst of dataoriginbytheresearchersinpresentingsolutionsfortheintricaciesofstorageandusabilityincloudstorage technology[1].

Author's addresses: P. Sharma and R. Jindal, Department of Computer Science and Engineering, Delhi Technological Uni-versity, Bawana Road, Delhi-110042, India; emails: pratimasharma1114@gmail.com, rajnijindal@dce.ac.in; M. D. Borah,Department of Computer Science and Engineering, National Institute of Technology Silchar, Fakiratilla, Silchar, Assam788010,India;email:malayaduttaborah@gmail.com.

Cloud computing is usually adopted in military and commercial environments to aid in datastorage. The heterogeneous environments of cloud computing are distributed with various com-ponents of the hardware and software that are obtained from the vendors, which could introduceincompatibility and vulnerabilities. The security affirmation of inter- and intra-cloud transfer andmanagementofinformationemergesasakeyissue[2].Cloudcomputingisapay-per-usemodeltoenableon-demand,convenientavailablenetworkaccessforsharedcomputingresources,suchas storage, servers, applications, and networks, which could be provisioned quickly and releasedwithminimumeffortofmanagementorinteractionwiththeserviceproviders[3,4].

Outsourcingcomputationisavitalserviceprovidedbycloudcomputing,therebyactingasoneofthesignificantadvantagesofthecloud.Withtheapproachofpay-per-use,thecomputingre-sources are used by the cloud, further overcoming the limitations of computationally weak devices[5,6]byoutsourcingtheirdatawithinthecloud.Theusercanrentandpaythestorageservicesorutilitycomputationbasedontherequirementwiththehelpofthecloudservices.Whencomparedwithtraditionalstoragetechniques,thecloudismoreflexibleandhaselasticity[7].Theuserdevicehasalimitedstoragecapacity,sothedataarestoredonthecloud.Fortheclassifieranddata,con-fidentialityisvitalbecauseofprivacyrequirements,andtheserviceproviderisnottrusted[8,9].Themajorchallengeexploredandhighlightedbytheresearchersistheprocessingandstoringofdataintothecloud.Moreover,whilesavingthedata,theissueofheterogeneityisconsideredthemainchallengefortheresearchers. Thisissueofheterogeneityindatastorageistermedasbigdataorlarge-scaledata.Thecloudenvironmentandthetechnologyoftheblockchain[10]areadaptedforthisusability.Therefore,fortheimprovementintheperformanceofexistingapplications,thesetwoapproachesarecombined[11].Therefore,blockchainisadistributedandsafenetworkingsysteminwhichmanycomputerscallednodesarestored.Thistechnologyisoftheutmostimportancewithmanypossibilitiesfortransmittingandstoringavastvolumeofdata.Italsominimizescostsandimprovesaccuracy[12].

Inthissurveyarticle,thefollowingmainpointsarecovered:

- Anoverviewofcloudstorageandblockchaintechnologyisbrieflyhighlightedandanalyzed.
- Existingcloudstoragetechniquesandblockchain-basedstudiesareaddressed,andtheiradvantages,disadvantages areexplained.
- Variousblockchain-basedcloudstorageapplicationsareexplored.
- Blockchain-baseddistributedcloudstoragetechnologiesareanalyzedbasedonvariousparameters,and basic buildingblocks are summarized.
- Inferencesandrecommendationsaregiven.

Figure 1 illustrates an overview of the study in the form of a block diagram. First, the articlepresents an overview of cloud computing and blockchain as separate concepts, reviews the studiesthatintegrateblockchainandcloudstorage,andanalyzesreal-lifeprojectsbasedonblockchainandcloud storage. Finally, some properties of blockchain for secure cloud storage are analyzed, chal-lenges are discussed, inferences are drawn from the study, and some suggestions are made basedontheinferences.Thisarticleisarrangedasfollows:Section2discussestheprocedureforthesystematic literature review. Section 3 covers the background details of cloud storage and blockchaintechnology. The work-related to cloud computing and blockchain technology is explained inSection4.Section5coversthestudyofcurrentblockchain-basedcloudstorage.Section6includesthe various real-life projects related to blockchain-based decentralized cloud storage technolo-gies. Section 7 presents the properties of blockchain-based secure cloud storage. Blockchain

andcloudstorageintegrationrequirementsandchallengesarelistedinSection8.Section9highlights

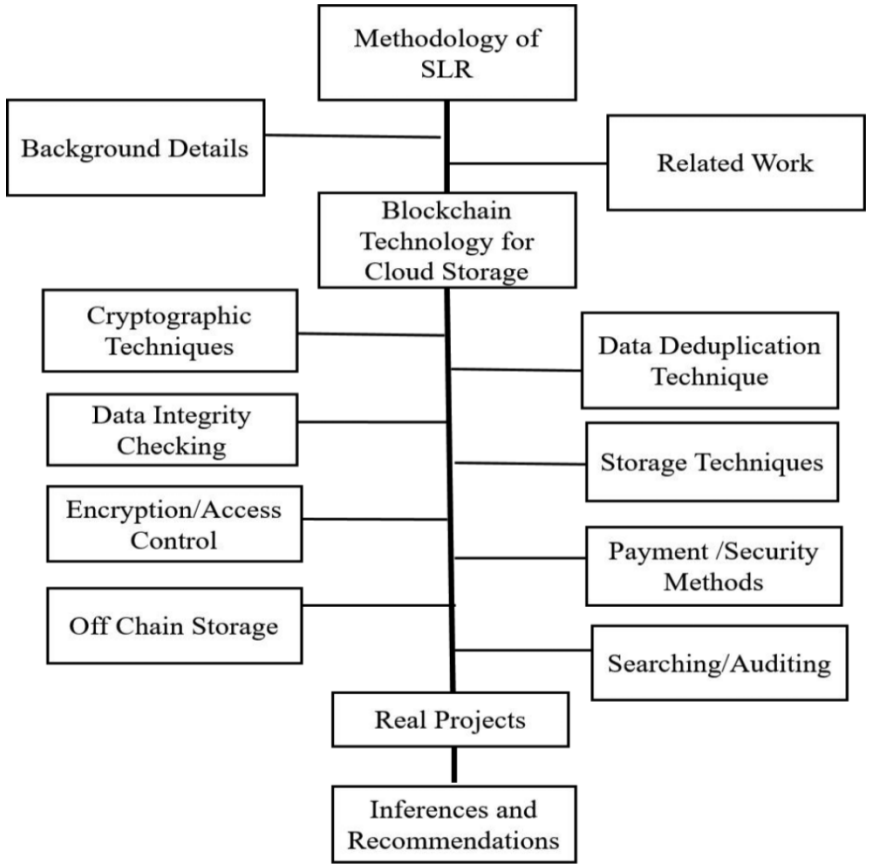

Fig.1.Overall flow of the study.

inferencesandsuggestionsrelatedtoblockchain-basedcloudstorage.Finally,conclusionsarepro-videdinSection10.

1 LITERATURE REVIEW

One of the main research areas of research methodologies is the Systematic Literature Review(SLR). The undertaking of the SLR methodology is crucial for evaluating current cloud storagedetails. The main aim of this review article is to examine or detect the relevant literature based onblockchainforcloud storage.TheSLR processphasesare illustratedasfollows:

As shown in Figure 2, the SLR phases include review protocol, searching queries, selection ofsources, study selection, data extraction, and analysis. Review protocol sets out the strategies thatare to be used in the process of a systematic review. In the current research, the SLR's principalmethodology is used to discover the published papers in the field of blockchain technology andcloud storage. This study's main objective is to provide an overview of the current research onblockchain-basedcloudstoragetechniques.Thus,weexplainedsixresearchqueries.

- RQ1:Whatarethedifferentpreventionmethodsutilizedbycloudstorageproviderswhilesharingi nformationtoanticipatethethreats?

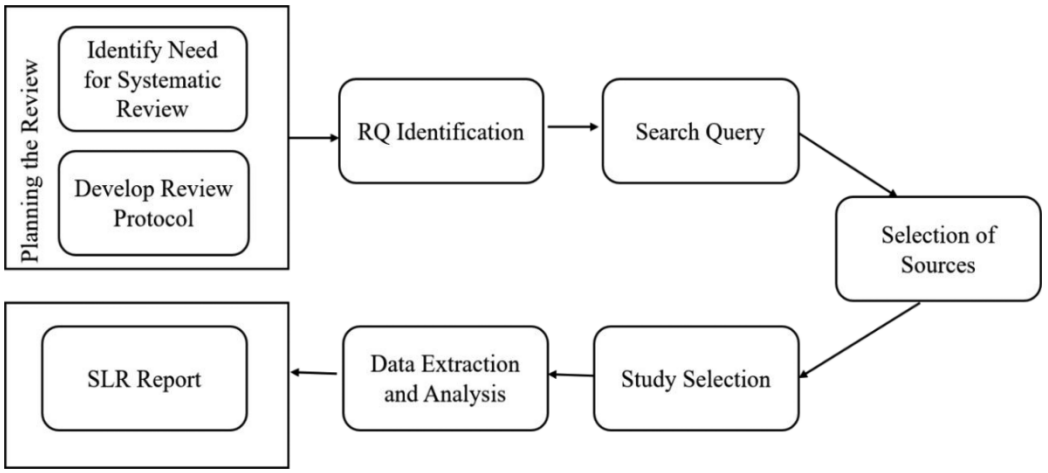

Fig.2.OverviewofSLRprocess.

- RQ2:Whatarethedifferentstrategiesusedforpreventingtheillegaluseofdatastoredonthecloud?

Toidentifythedifferenttechniquesthatareusedforpreventingthestoredinformationinthecloud.

- RQ3:Whatarethemainsecuritydifficultiestobefacedinthefuturebasedoncloudstoragetechnolo gy?

Todiscussfuturecloudcomputingsecuritytechniques.

- RQ4:Whatarethecurrentresearchtopicsofblockchaintechnology?

Tostudyandunderstandtheblockchaintechnology,wetherebycollectedallthecriticalresearchpapersf romlogicaldatabasesandmappedthecurrentresearcharea.

- RQ5:Whatareblockchaintechnology'scurrentresearchtopicsforcloudstorage?

Tostudyandunderstandtheblockchaintechnology-basedcloudstoragetechniques.Thiswould, hence, help the researchers to figure out the present research topics related to blockchaintechnologyforcloudstorage.

- RQ6:Whatarethedifferentmethodsutilizedtosave,delete,andupdatethecloudatausingblockchaintechnology?

To study and understand the methods used to perform the various operation on the cloud datausingblockchaintechnology.

Thesearchwasdirectedfrom2010until2019byutilizingtheonlinelogicaldatabase.Thesearchmethodology for the survey was necessarily coordinated toward finding distributed papers in jour-nals and conference papers through the accepted literature search engines and databases GoogleScholar, Springer Digital Library, ACM Digital Library, IEEE Xplore, Elsevier and Science Direct. In2018, the published articles had the highest rank. Likewise, papers distribution based on publishedarticlesfrom2010–2019appearsinFigure3.

Fig.3.Distributionofpapersfrom2010to2019.

OverviewofCloudStorage

The cloud is described as the chain of servers and connections to give a computing benefit forstoring the user data. Presently, several organizations and internet sources are adopting cloudstorage for individual and organizational users [13]. One of the cloud computing models is cloudstorage, which stores a colossal amount of data and can be retrieved using the internet. Cloudstorageserviceproviderscancontrolanydata,i.e.,organizedorsemi-organized[14].

Cloud storage provides a deliberation to physical capacity gadgets. Also, it presents informationstorage as a service, regularly charged on a user premise. It is this reason for cloud storage, whichenables a client to store and access information records someplace within the cloud, without understandingthepointsofinterestofwheredocumentsaresaved.Moreover,therecordcanbemadeaccessible on a worldwide premise in cloud storage [15]. The expansion of the number of clientswho put their benefits on the cloud has led the cloud storage to become an important theme. How-ever, these clients regularly do not trust the fact where their information will be stored and whowill approach this information. Hence, numerous clients feel the commitment of applying safetyefforts to have an aggregate authority over their information. For this, authentication, integrity,availability, confidentiality, and privacy problems are the requirements that the users look for. Inthe explicit instance of endeavor, these suggest essential contemplation; ought to be incorporatedintoanycloud benefitcontract.

BlockchainTechnologyOverview

Blockchain is one of the most hyped advances nowadays and has gained considerable importanceasaninnovationwidelydeployedinvariousareas[16,17].Theblockchainisviewedmainlyasan accounting book or digital distributed database [18]. After its commencement in 2008 [19],blockchain has continued to develop as a disruptive advance that might alter the way we inter-face,makecomputerizedexpenses,followup,andmonitortransactions[20].Blockchaincouldbe cost-effective, removing the centralized authority's need to monitor and regulate transactionsand interactions between different members. In the blockchain, every transfer is cryptographicallymarkedandconfirmedbyotherminingentitiesholdingacopyoftheentirerecordconsisting ofallthe transactions. This makes records step by step, safe, synchronized, and shared time that cannotbe adjusted [21]. Furthermore, blockchain technology is known to be an information technologythatcanbeusedinsoftware,business,andtradesectors[22].Thearchitectureoftheblockchainisillustratedin Figure4.

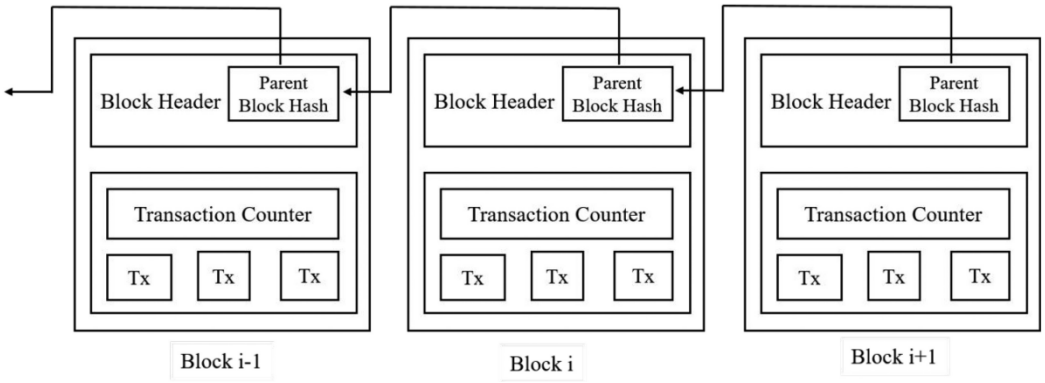

Fig.4.ArchitectureofBlockchain.

KeyCharacteristicsofBlockchain

- *Distributed:* The distributed environment uses the standard protocol, which ensures that every node receives each transaction and uses predefined rules for grouping the transactionsinto blocks after processing. The blockchain is designed for distributing and synchronizingthedataacrossmultiplenetworks.
- *Decentralization:* It is the core strength of blockchain, because each node holds a record ofall transaction data, so there is no need for a central authority. This relief the failure of thesingle point of vulnerability. In the blockchain network, there is no single authority and noservicefees,andtheconsensusalgorithmsareusedtomaintainthedataconsistency.
- *Consensus:* Consensus algorithms maintain the consistency of data within the blockchainand keep incorrect or false transactions away from the blockchain network [23]. All nodesmust agree by executing the standard consensus algorithms to ensure the integrity of trans-action data. Moreover, there must be an assertion between every member, before one canexecutethetransaction,onlythenthetransactionshouldbevalid.Thisprocedureiscalledaconsensus[24,25].
- *Anonymity*:Intheblockchain,everyusercaninteractwithacreatedaddress.Thesystemwillnot disclosetheuser'sactualdetails;however,thememberscanviewtheencodedtrans-actiondetails.
- *Traceable:* The blockchain is time-stamped and digitally signed, which implies that the association can follow back to an explicit time for every transaction and further distinguish the relating party on the blockchain [26]. Consequently, each block is permanently and unquestionably connected to the past block [27].

3 RELATEDWORK

This segment presents research works relating to traditional cloud computing techniques thatproved their significant improvement toward increasing security and academic studies on theblockchainandcloudcomputing.

TraditionalCloudComputingTechniques

Cloud storage is a kind of Internet technology for sharing resources with IT-related capabilities,and it is important to either enterprises or individual users. Traditional security strategies mainlyfocusoninformationencryption[28,38],integritychecking[28–34,36],datadeduplication[30, 39,40],userrevocation[35],datastorage[38],dataauditing[37],andsoon.WhileInformation

and Communications Technology (ICT) and cloud services progressed, numerous scientific workhasbeendedicatedtoincreasingtheperformanceandsafetyofthedata.Toprotectuserdatastored on the cloud, a symmetric cryptographic scheme is used with encrypted bloom filters to allowtheusertorecognizeunauthorizedmodificationsintheoutsourceddata[28].In2018,YunxueYan et al. [29] developed a protection scheme to enhance the security of signature information foruser data. In [30], the authors proposed an integrity assurance algorithm using a standard storagetemplate for various control methods. Tags for validation and process generating proofs relied onthe index pointers. In References [31–34], the authors introduced a novel and efficient integrityverification technique by using various approaches like Merkle hash tree, proof of storage, andpaillier homomorphic cryptography method, respectively. In References [35, 37], the authors il-lustrated a safe group user revocation method with an effective public integrity audit scheme. Itfacilitated public monitoring and the effective removal of users. Yibin Li et al. [38] concentratedontheproblemsofcloudoperatormisuseconcernsaimedtopreventtheclouduser'sdatare-lease from cloud servers. Pooranian et al. [39] proposed a RAndom REsponse (RARE) methodthat removed the cloud storage facilities deduplication response side channel and retained the useof deduplication simultaneously. Chia-Mu Yu et al. [40] proposed a zero-knowledge deduplica-tion response as a side-channel shield that is based on a zero-knowledge cross-user deduplicationresponse structure. Although these schemes provide secure storage, integrity checking, efficientuser revocation, and data duplication removal, there are still some problems existing in the systems,suchascentralizeddatastoragethatseverelyharmsphysicalserversecurityandtheneedfor trusted third-party, which are nightmares for the privacy of users' data. It has been observedthatmostmethodsconsideronlystaticdatasetsanddoesnotapplytoalargevolumeofdata.The issues of cloud storage data security are not resolved through some techniques. Therefore, itseems very meaningful to understand the blockchain-based solutions for cloud storage known sofarand to carry out investigations to conclude.

BlockchainandCloudComputingStudies

A lot of new technologies and frameworks have been introduced with the existing keen interest inblockchaintechnology.Numerousreviewarticleswerepublishedtodemonstratetheadvantagesof blockchain for existing applications. Examples of these studies include the blockchain technologyforbusinessapplications[41,42],e-governance[43],healthcare[44–46],security[47–48, 52, 73], sharding [49], cloud exchange [50], edge computing [51], and so on. Certain studies dealtwith blockchain obstacles, prospects, and plans for the future. For example, References [47, 52,53] address security challenges and opportunities in the blockchains. The research in [81] provides a detailed overview of privacy and security concerns in cloud computing, covering potentialthreatsanddetectionmethodsbasedonblockchain.AuthorsaddressinReferences[45,46]theus e of blockchain technology in the healthcare and medical fields. Reference [49] presents keyconceptsofvariousshardingmechanismfocusedonblockchaintechnology.InReference[50],theaut horsaddressissuesintermsofsafety,security,andtransactionprocessingregardingtheuse of blockchain for cloud exchange. Moreover, Reference [51] is dedicated to blockchains foredge computing systems and their potential uses. All the earlier studies under consideration dis-cuss the safety pattern in cloud storage and plan to incorporate blockchain technology in differentenvironments. This article investigates the use of blockchain technology for cloud storage as awhole without being specific to particular applications, thus addressing its current trends, clas-sifications, and open issues that have not been discussed in the prior surveys. We are aiming toprovideadetailedoverviewoftheusageofblockchaintechnologyincloudcomputing.Tothebestofouru nderstanding,ourresearchsurpassesallthecurrentstudiesmoresystematicallyintermsofthe core principle of blockchain technology for cloud storage.

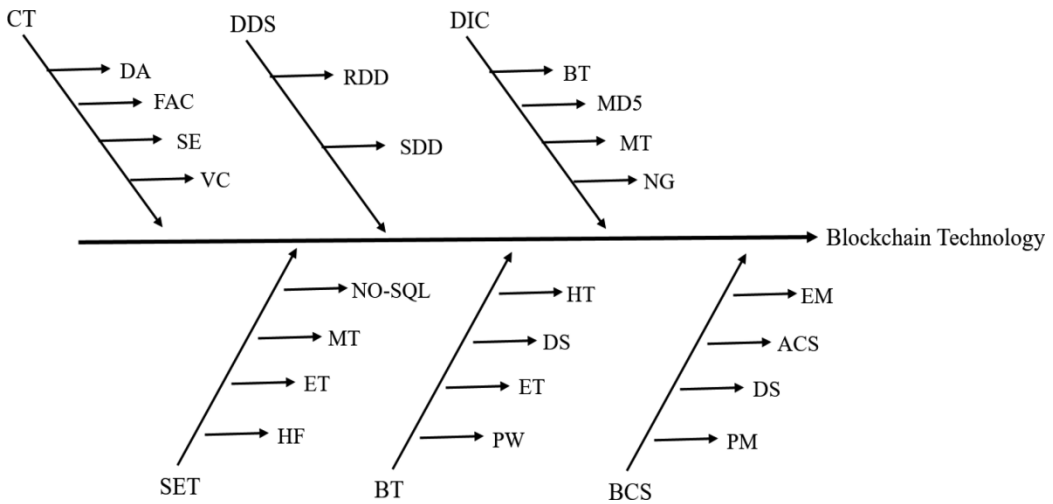

Fig.5.BlockchainmethodsselectedinthisSLR.

4 EXISTING TECHNIQUES OF BLOCKCHAIN FOR CLOUD STORAGE

ThisareagivesthedetailsoftheblockchainmethodsselectedinthisSLR.Basedonselectedstudies,wearra ngedtheblockchaintechniquesutilizedforcloudstorageasfollows:

- CryptographyTechnique(CT)
- DataDeduplicationScheme(DDS)
- Data IntegrityCheckingTechnique(DIC)
- StorageEfficiencyTechnique(SET)

- BitcoinTechnology(BT)
- Blockchain-basedCloudStorage(BCS)

InFigure5,wehaveusedthefollowingabbreviationstorepresentmethodsselectedinthisSLR:FAC,Fine-GrainedAccesscontrol;DA,DataAuditing;SE,SearchableEncryption;VC,VerifiableComputation; RDD, Reliable Distributed Deduplication; SDD, Secure Data Deduplication; BT, Bit-coin Transaction; NG, Non-repudiation Guarantee; MT, Merkle Tree; ET, Ethereum Technology;HF, Hyperledger Fabric; HT, Hash Technology; DS, Digital Signature; PW, Proof of Work; PM,PaymentMethod;DS,DeletionScheme;ACS,AccessControlSystem;ES,EncryptionScheme.

Blockchain-basedCryptographicTechniqueforCloudStorageService

The framework allows the users to transfer their information in encoded form, distribute the information substance to cloud hubs, and ensure the accessibility of information using cryptographicprocedures[55].

Thestructureofcryptographystoragecontainsthreeparts,asshowninFigure6.

- DataProcessor(DP):Processingofinformationbeforesendingittothecloud.DataVeri
- fier(DV):Verificationofthedamagedinformation storedinthecloud.
- TokenGenerator(TG):Forsavingthedocumentsoftheclientsonthecloud,thetokengenerator generates the token for each user.

Figure 6 represents: (1) Master “y” information processor sets the information before sending ittothecloud;(2)Master“x”needsthepermissionofMaster“y”forscanningakeyword;(3)Master

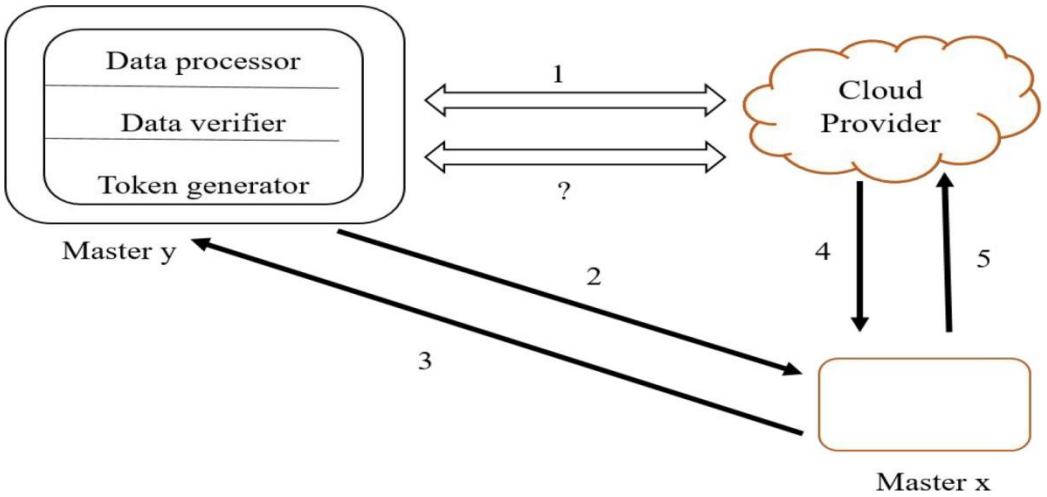

Fig.6.Thearchitectureofcryptographiccloudstorage.

“y”generatesatokenforakeywordandsenditbacktoMaster“x”;(4)Masterxreceivesthetokenand send it to the cloud; (5) To locate the appropriate encoded documents, the cloud utilizes thetoken and send the resultant documents back to Master x. (?) At any time, Master y’s data verifiercanconfirm the integrity of the information.

Blockchain-basedDataDeduplicationSchemeforCloudStorageService

Thedatadeduplicationschemeisusedtoeliminatethesuperfluousdataandtooptimizethestoragespace in the cloud. Additionally, this technique only retains one copy of the indistinguishableinformation to optimize storage capacity. Thus, it can manage data efficiency and save the cost ofphysical devices [56], but there is a chance of increasing data reliability problem. Thus, the filesaredistributedtodifferentserversusingadeduplicationapproach,andthestorageinformationisrecordedontheblockchain.Theprotectionofsystemconfidentialityanddataintegritycanbeachievedbycombiningthedatadeduplicationschemewiththeblockchaintechnique.Also,itis well-suited for distributed storage systems. The blockchain network should be joined by CSPand data owner as a node for related services. Every duplication and transaction data should bedocumented on blockchain for ensuring the data authenticity [57]. The data deduplication methodisclassifiedbasedonData unit,Location,andDisk placement[58].

The deduplication process is categorized into three methods based on where the data are processed: data unit deduplication, location deduplication, and disk placement deduplication. Theclassification of deduplication is illustrated in Figure 7. The data unit deduplication is bifurcatedfurther into file-level and chunk level deduplication. The file deduplication uses the unique hashvaluesforcomparingthetwofiles.Ifthehashvaluesareidentical,thenonlyonecopyisstored.In deduplication at the chunk level, the file is split into fixed or variable length blocks and thencheck for the duplicate content. Location-based deduplication is categorized into source and targetdeduplicationprocess.Thetargetdeduplicationprocessisworkedatthesideofareceiverafter the client transmits the files, and it also rejects the additional data. Without influencing theclient's operation, the deduplication process is done by the storage device. The process of dedupli-cation is hidden from users. Before transmitting the data, the source deduplication process is done.Thisdeduplicationhastheadvantageofnetworktrafficbandwidth,becauseitutilizedtheclient's

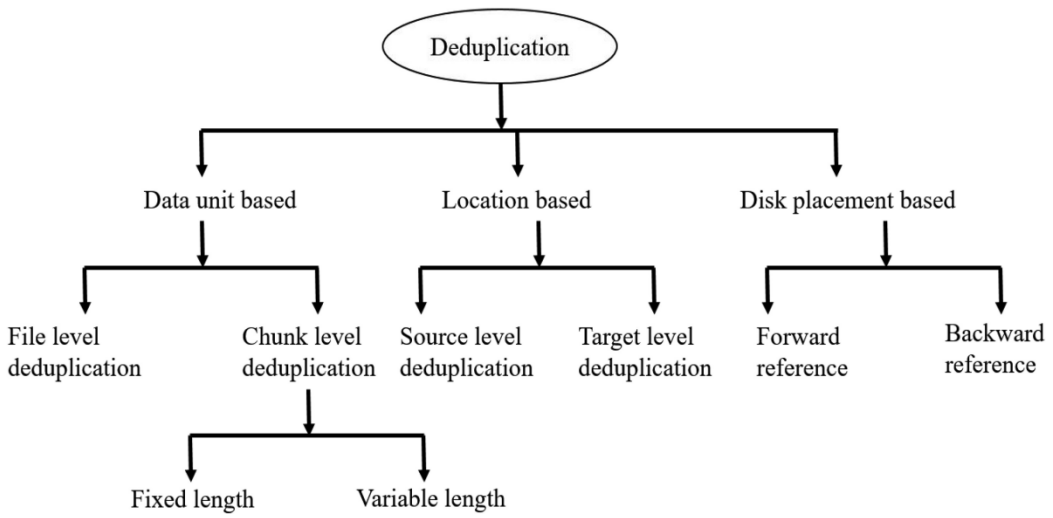

Fig.7.Classificationofdeduplication.

resources. The disk-level deduplication is further divided into two parts; these are forward reference deduplication and backward reference deduplication.

Blockchain-basedDataIntegrityCheckingTechniqueforCloudStorageService

The decentralized data integrity checking is enabled by a blockchain-based structure for cloudstorage services. The integrity checking method is mostly dependent on three components. Theyare the blockchain, the Cloud Storage Service Provider (CSS), to which the information is out-sourced and the data user. Data Integrity Service (DIS) is built on the structure of the blockchain.Theblockchainclientshouldbestartedinitiallyonnodeswhentheis needed[59].Blockchaincan use Merkle trees for data integrity verification. This comprises two phases: the pre-processingstageandthe validationphase.

- Pre-processing phase: Initially, the data are sliced by the data consumer to form differentshards, and these shards are then used for constructing a hash Merkle tree. Then, the con-sumerandCSSwillapprovethehashMerkletrees,andtheconsumerstorestherootofthis hash tree. The user data and public Merkle trees are uploaded on CSS. CSS sends theaddressof the stored user'sdata to the user.
- Verification phase: CSS receives a challenge number from the client, and it is used to selectshards to check. The hash function is used based on challenge number and shard to cal-culate a hash digest. CSS forward digest and the equivalent are supporting statistics to theblockchain. The smart contract calculates a fresh hash root and compares the hash roots.The data integrity will be assured when the hash roots are equal. If not, then data integrityhasbeendegraded.Finally,theverifiedoutputissenttotheclientbytheblockchain[60].

StorageEfficiencyTechniqueforCloud-basedDesign

With the rapid increment of cloud computing, the NoSQL database is the best choice for savingthe information into the cloud. The NoSQL databases are stored and handled by platforms likeMongoDB and Hadoop, Graph Databases, Column-oriented DBs, Document DBs, and Key-valuestores [61]. The cloud stored data in a simple text format; hence, it is a very inefficient way ofstoringdata.Thismakessomeissuesinthecloudandfurtherraisestheoverheadofoperating

system while storing the data. To manage huge volumes of data, the MapReduce method is used,butitisnotsuitableforarelationaldatabasemanagementsystem[62].BigchainDBisamasterless,scalable, decentralized database of cloud data storage. BigchainDB is incorporated on top of aNoSQL RethinkDB database as an additional layer, which is efficient storage for cloud storage. Itutilizes a database underlying and provides blockchain-like functionalities such as hashed blocks,transactions,voting, and record immutability[63].

RedundantArrayofCloudStorage(RACS)

For distributing the data and protecting the network architecture, RACS is used. RACS is performed between the customer and various data repositories [64]. It showed parallel communication with multiple proxies in a distributed manner. It can likewise be kept running on variousintermediaries with a similar arrangement of the vault utilizing strategies. This strategy is primar-ily acquainted with maintaining a strategic distance from seller secure and with decreasing theexpense of exchanging suppliers. The supplier disappointments are endured. The system is basicand straightforward. Since all information must go through a RACS intermediary either to encodeor to decipher, a solitary intermediary could without much of a stretch turn into a bottleneck [65].The users can utilize blockchain-based secured cloud storage architecture [66], where they wouldsplit their documents into several chunks of data and randomly upload those chunks of data to theP2Pnetworkofferingfreestorage capacity.

Blockchain-basedCloudStorageAccessControlSystem

Blockchain technology may be utilized to provide secure access control to the information collectedinanuntrustworthycloudenvironment.Theuntrustedcloudstorageenvironmentneedsthe technique to protect the shared data. Blockchain-based access control provides a method usingthe attribute-based encryption scheme with dynamic attributes for user access [67]. Using the decentralized ledger technology, blockchain keeps the unchanged log for all relevant security events,likerevocation,keygeneration,accesspolicyappointment,andaccessrequest.

A blockchain-based access control technique is developed in Reference [68]. Access control isinclusive of identifying, authenticating, and authorizing procedures. It ascertains the state of beingresponsible wherein client access can be tracked for which specific activity in a framework. Theintroduced framework allows the clients to get to Electronic Health Record (EHR) from the datapools that are shared utilizing blockchain in the wake of checking their cryptographic keys as wellas their identity. To accomplish the client's authentication, validation based on identity is adopted.Banning the malevolent imitation of roles and adaptability, which effectively allows organizationsto participate and consumers from regulating their responsibilities. To guarantee secure access tosensitiveinformation,creatingasmartcontract-basedaccesscontrolmechanismisintendedtobereliable,flexible,anduseful.TheSmartContract-basedRole-basedAccessControl(RBAC-SC)utilizesblockchainandsmartcontractsasversatilesystemstoportraytherelationshipoftrustthat is crucial within the RBAC and for the execution of authenticating the challenge-responseprocess,which willverify theuser's possession ofpositions [69].

Blockchain-EnabledPaymentSystemforCloud

Thesecurityattacksonthepresentpaymentframeworkareincreasingduetoitscomplexityandscattered nature of the transaction facilitators. A client expecting to exchange cash will pay ayearlyparticipationexpensetogetthecardandutilizeittobuymerchandiseorusetheservices.The banks of the client and the dealer associate with one another to settle the charge expecting toutilizethecardobtainedfromthebankanduseditinbuyingthemerchandiseandenterprises.Asimplifiedtransactionisnecessaryasmoreindividualsusecellphonesto buy service or

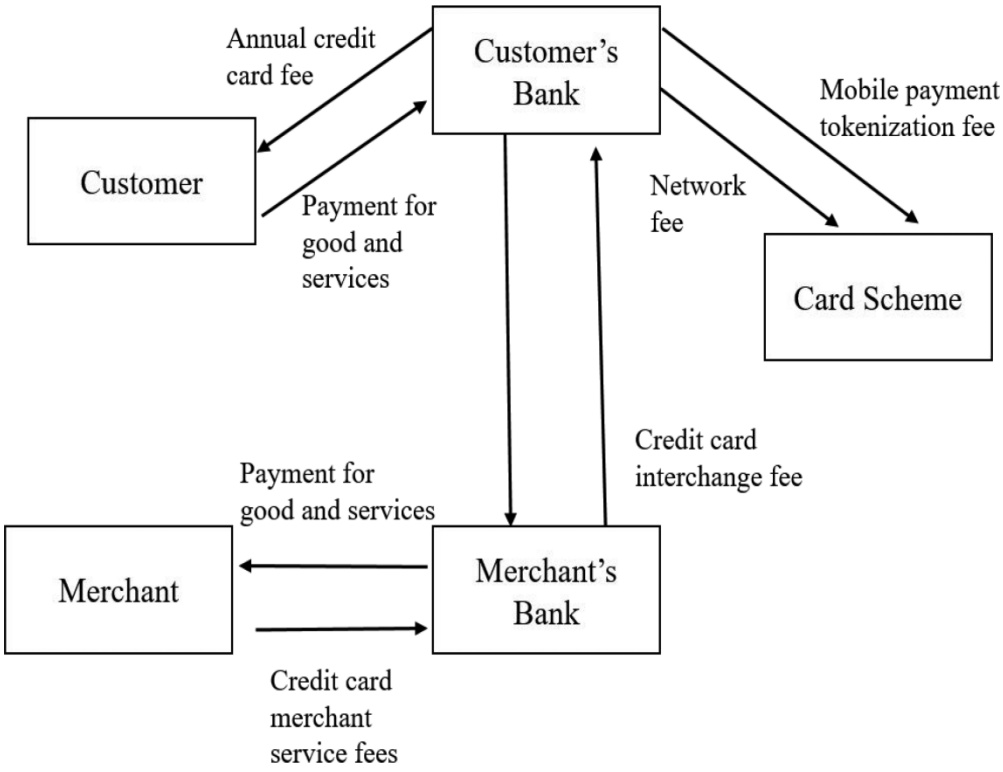

Fig.8.Theprocessofapayment system.

merchandise[70].ConcerningtheadvantagesoftheexecutionofacustomertransactionasaP2P transaction utilizing blockchain, the exchange is not just dependable and unquestionable yetadditionally cost-effective, since there are no outsiders included. Also, the transaction utilizingblockchain could be finished quickly as the physical distance does not influence the transaction,whileregulartransactionsovertheborder couldbeslow.Incontrast,traditional,centrallymanagedtransactions are defenseless against significant information leakage during database managementasallvaluableinformationishandledwithinthecentralserver.Conversely,itisexceptionallyhardfor attacking the transactions based on blockchain, since all of the vital information is conveyed,and an assailant must hack and change 51% of the shared P2P. Outsourcing services generally involveinternetsecurityandpaymentproblemsasanappealingbusinessmodelforcloudcomputing.Mistrust among customers and outsourcing providers may significantly hinder the acceptance ofwide-ranging cloud services. Some present payment techniques, however, only take into consid-eration an outsourcing provider and relying on the trusted third party. For ensuring a safe and fairpayment

service without a trusted party, a blockchain-based online payment method is needed foroutsourcingcloudcomputing services[72].

Blockchain-basedCloudStorageDataDeletionScheme

The cloud server maintains the users' information to reduce the overhead of saving, updating, anddeleting data. Therefore, it is necessary to incorporate the security feature while deleting, storing,and updating the cloud data. Recently, several research works [73] have been carried out to deletethedesiredselecteddatasafely.Mostoftheavailabletechniques,however,canberepresented

using the same "one-bit-return" protocol procedure: The cloud server removes the data and reverses the one-bit result. The owner of the information must trust the outcome, because the ownercannot verify it. Consequently, the deletion scheme based on the blockchain can increase trans-parency in the deletion operation. The data owner may test the deletion result irrespective of howmalevolently the cloud server behaves. Also, the safe deletion technique can obtain public vali-dation without any third party with the application of blockchain [73]. Even though deleting thedata securely has been hypothetically explained; however, the proposed plans still have two char-acteristic constraints. The majority of the proposed plans with overwriting strategy are unable tosupportverification.Insuchprotocols,theowneroftheinformationmustacceptttheframeworkof managing the data, since they cannot check the consequence of data deletion. Despite a fewschemes verifying, they have to introduce a third party that can be trusted. The other innate con-straintsarethattheproposedconventionsarenoteffectiveinthecaseofpracticalapplications.It is considerable for designing secure information deletion plans to erase information effectivelyandpermanently[74].

Blockchain-basedBitcoinTechnologyforCloudStorage

Bitcoin is known as the digital currency, which relies on the P2P payment platform that has beendeveloped as open-source software. The virtual currency is transferred and established within thecryptographiclinks,andbitcoinisalsoknownascryptocurrency[75].Bitcoinbroughtaboutarevolution,sinceitgaveatechniqueforP2Ptransactionswithouttherequirementforintermediatebodieslikethebanks.Thebitcoindependentontheblockchainreliesonthecryptographicalgorithmsthatarehighlysecureandsophisticated P2Ptechniquesthatformthefundamentalsof the democratically sustained and distributed public ledger of transactions. The transactions arevalidated, and a permanent record is maintained by bitcoin while ensuring that the identity-relateduser data is kept incognito [76]. Accordingly, by applying Blockchain or comparative digital currencymethods,theclientsneitherrequireconfidinginoneanothernorrequireanintermediator;instead,thetrustisshowninsidethedecentralizedsystemframeworkitself.

SearchingProcessinBlockchain-basedCloudStorage

Conventional cloud storage depends on only great-sized storage providers, who go about as thirdparties that can be trusted for transferring and storing data. This model represents various issues,including information accessibility, high operational expense, and information security. Variousstudies have presented a framework that influences blockchain technology for providing protecteddistributeddatastoragealongwiththeserviceofkeywordsearches.Theframeworkpermits thecustomer to transfer the information in an encoded manner, transfers the content of data to cloudservers, and guarantees information accessibility utilizing cryptographic strategies [77]. It addi-tionally gives the owner of the data the ability to give authorization for others to search on theinformation. Also, the system allows scanning for private keywords over encoded data

collection[78].

AuditingSchemeinBlockchain-basedCloudStorage

With the fast improvement of cloud computing, an expanding number of companies and peopleshare and store the information on untrusted clouds. Accordingly, the auditing of shared infor-mation has become a major issue in cloud storage, pulling scientific consideration. An open audit(public audit) shared cloud storage information protocol using blockchain and Rank-based MerkleAVL tree (RB-MHT) to achieve privacy conservation and batch auditing to preserve the protec-
tionoftheupdatedblockchainrecordinthescheme[79].ThemainthingthattheTPAneedsforcheckingthe dataevidenceisthegroupmanager'spublickey.Furthermore,thecommunity

managercannotchangethechangedrecordsdiscretionarily.ThePerformanceEvaluationindicatesthepr oposedplanissafe andeffective.

A smart and decentralized public auditing plan for cloud storage was proposed in Reference[80]. By bringing the blockchain framework into the plan eliminated the TPA in the frameworkmodel.Stabilityandreliabilityareenhancedbecauseofthecompletelydecentralizeddevelop ment.Likewise, they developed an automatic auditing protocol along with the smart contract, which cancheckperiodicallytheintegrityofthedataintheCloudinsteadoftheownerofthedata.Hencethis ensures that the data owner is rid of the periodic verification burden. Since every single, smartcontractisexecutedandstoredbyallnodesinthesystem,theauditresultscannotbealtered.

SecurityandPrivacyIssuesinBlockchain-basedCloudStorage

A blockchain discarded the server to ban the central authority's association and enabled transac-tions by members who saved the exchange documents collectively and finally endorsed transac-tions using the P2P network technique. The blockchain has a shared framework and makes use ofpeer network and peer resource computation. Specialized estimates, for example, Proof of Work(PoW)andProofofStorage(PoS),wereimplementedforimprovingblockchainsecurity.Event hough blockchain security is continuously improving, problems have continued to be accountedfor, and there are diverse safety assessments. An intruder may make various attempts to access
thepersonalkeysstoredontheclient'sdeviceorcellphone.Investigationsareunderwayonusingasecu re token or storing it securely to protect the personal key. In Reference [81], the authors dis-cussed the advancement of blockchain and related technologies and analyzed the research trend toidentifymoreareasofstudy.TheuseofblockchainintheCloudcomputingenvironmentshouldbeconsid ered for specific current problems. Even now, Blockchain contributes to numerous issues,suchastransactionsecurity,walletandprogramming,andvariousinvestigationshavebeenun -dertaken to resolve these issues. When using blockchain in the cloud computing environment, theanonymityoftheclientdatashouldbeassured,andtheclientdatashouldbecompletelyerasedwhen thesoftwareisdeleted.Theclientdatacanbeinferredfromtherestofthedataincasetheclientdataisnot deletedyetslightlyleftbehind.Itappearsthatefficiencyassessmentsareaddi-tionally required alongside protection, given the environments in which large amounts of data aretransmitted.

EncryptionMethodsUsedinBlockchain-basedCloudStorage

Cloud computing has pulled in an expanding number of people and companies to outsource theirinformation to third-party platforms for boundless storage and computing capacities upon requestwith convenience and inexpensiveness. Since cloud servers cannot be trusted and the informationsecurity of clients, it is important to encode the information before it is outsourced to clouds. But,the immediate utilization of conventional encryption advancements denies clients of

searchabilityand,inthisway,bringsaboutapoorclientexperience.Tosafeguardthissearchservice,accessibleencodingadvancementshavebeencreatedintwodelegatesettings,includingthesettingsofpublickeysandsymmetrickeys[82].

BlockchainTechnologyforOff-ChainCloudStorage

Current-age corporations have handled information as on-chain or off-chain storage structures forblockchain-based solutions. This could be applied as data storage in a blockchain infrastructurethatisprivateorpubliclyavailable.Off-chaindoesnotnecessarilymean“notattheledger,”itsimplymeansit’snotonadatabasethatisopentothepublic.Justasanycompanymightnotmaintainthe information in a publicly accessible repository or archive, off-chain management ensures theinformationisnotavailabletothegeneralpublic[83].Off-chaintransfersareofenormousvalue,

sincetheyhaveimprovedsafetyandarenotconstrainedbythetransactionalspeedrestrictions.Inatraditionalon-chaintransaction,eachtransferwouldhavetobevalidatedbyallpeersinthenetworkbeforethetransferislabelledascomplete,whichkeepsitveryslow.Incontrast,inanoff-chaintransfer,notallpeersneedtowaitforthetransfertobeverifiedbeforeitislabelledassuccessfulorcomplete.

Becauseoff-chainplatformsarenotlinkedtothepublicinternet,itismoreprotected,sinceit is very close to the protection that could achieve by deploying a server or software in the in-tranet as opposed to the internet. The on-chain transaction includes a lot of members checkingtransfers, and all participants’ validation signatures have to be an exact match to be consideredvalid for that transaction. Whereas the details of each exchange are released for inspection on thepublic blockchain so that they are not altered or turned back, this may take longer than for off-chain transactions. Also, there is a very probable possibility for the payment costs to be costly, asparticipantscan choosethe off-chainscheme [84].

In an article published by IBM [85], off-chain transactions deal with “values outside of theBlockchainthatcanbefinishedusingavarietyofmethods.”Bothsidesmustconcuronthetransfer,andthenanotherpartycomesintoverifythetransaction.Becausenon-transactioninformationsuch as images, agreements, PDFs, and private data are not recommended to be stored in the mainblockchain database, some kind of off-chain or sideDB space is required. A hash or signature willbeproducedfortheoff-chainobject,andthatiswhatiskeptintheblockchaindatabase.Theindividual object is stored either in the cloud, on-premises, or in a near-cloud storage network. Theneeded capacity for off-chain data is expected to exceed storage requirements for the blockchaindatabase.Anykindofoff-chaintransactionisprettyfastandimmediate,withoutthehigheron-chaintransactionfees.

The various applications of blockchain technology for cloud storage and their properties aresummarizedinTables1and2.Removalofduplicatedataonthecloud,storageofclouddatausingblockchain, maintaining the security of the cloud data, encryption methods, security and privacyissues, safe deletion of data, secure access control mechanism, off-chain cloud storage, and fairpayment method utilized for cloud services using blockchain technology are presented in thesetables.

5 REAL PROJECTS: BLOCKCHAIN-BASED DISTRIBUTED CLOUD STORAGE TECHNOLOGIES

In this section, we explore and analyze some of the popular distributed storage platforms andhighlight the main contributions. Marketplaces for cloud storage make disk space a commodity.They are the intermediary with those who want to store information and providers who are willingtostoredataforthem.CompaniessuchasMaidsafe,Storj,FileCoin,andSiaallactasmarketplaces. Theyofferquicker,simpler,andsaferstoragethanDropBox,Amazon,orGooglechoices.Figure9showst hevariouscategoriesforanalyzingdistributedcloudstoragetechnologies.

MaidSafe

TheSAFE(SecureAccessForEveryone)NetworkisaP2Pdecentralizednetworkofdataandcommunications built by MaidSafe.net. The framework supports all existing centralized web applicationsanddatacenterswithasecureandconfidentialnetworkofadditionalcomputingresourcesfor their users. SAFE Network is a distributed, independent data storage and communications net-work [97]. The performance, reliability, privacy, and security of the network data are incrediblyhigh. The current server-client-based internet offers information possession to whoever managesthe servers, rather than to the data-creating people. The following categories are selected to analyzethenetwork.

Table1.ApplicationsofBlockchainTechnologyforCloudStorage

Authors	Findin g
Hoang Giang Doetal.[55]	PresentedaBlockDSsystemforprovidingareliabledistributedstorageservicef orsearchingkeywordsusing blockchaintechnology.
JingyiLietal.[56]	Suggestedadeduplicationschemethatallocatesfilestomultipleserversanddoc umentsblockchain storage information. They describe smart contract-based protocols to ensuresecurededuplicationwithoutcentralauthorityparticipants.
BinLiuetal.[59]	Suggested a framework for integrity service based on blockchain. This framework pro-vides a more trustworthy verification of the integrity of data for both consumers anddata holderswithout depending on a trusted party.
Dongdong Yueetal.[60]	In P2P cloud storage, a blockchain-based method for verifying data integrity is intro-duced to make the verification process more effective and open. In this context, theMerkle tree is presented to identify data integrity and evaluate performance and relia-bility under various Merkle tree structures.
Josef Gattermayereta l.[63]	Proposedamulti-levelsystemforclustersdependentoncryptocurrencyprinciplestoobtaina masterlessreputationratingthroughoutthecluster.
JiaxingLietal.[66]	Proposed a blockchain-based system for distributed cloud storage that would allow cus-tomerstodividetheirdocumentsintoencryptedchunksofinformationanduploa dthemrandomlyto a peer-to-peer network.
Ilya Sukhodolskiyet al.[67]	Developedamodelforcontrollingtheaccessdependingonblockchain,store ddatainuntrustworthyspace,andimplementedattributeencryptionbasedo nEthereumsmartcontracts.
Jason Paul Cruzetal.[69]	AnRBAC-SCwasintroducedtoimplementatrans-organizationalframeworkforRBAC.Safe RBAC method (users cannot disguise roles and only allowed users must performtasks), customer-oriented method (customers can report their duties to any agency),testable(everyonecanverifythepositionoftheuser).
Yinghui Zhangetal.[7 2]	IntroducedaBCPay,acloudcomputingservicepaymentsystemfocusedonbloc kchain.Thissystemensuresthatwithoutanytrustedparty,theoutsourcingser vicesarepaidsafelyandreasonably.
Changsong Yangaetal.[73]	Build a novel, data deletion scheme based on blockchain. If the server may not honestlydelete the information, then this scheme allows the data owner to identify the cloudserver'smalevolent operation.
Sharmaetal.[86]	The authors developed a novel architecture based on a decentralized blockchain cloudwith an activated SDN controller at the end of the network to fulfill the essential designprinciples.
Hasan et al.[87]	DevelopedaneffectivemethodtouseblockchainandIFPS(InterPlanetaryFileS ystem)to store provenance information. Users were also able to check the validity of theirresults.
Manzooretal.[88]	Thisstudyproposesablockchain-basedtradingplatformcombinedwithapairingfreeproxyre-encodingschemetotransfersensordatatotheusersecurely.

Zhang etal.[89]	Development of a certificate less public validation technique against the procrastinat-ing auditor, namely, CPVPA, using on-chain currencies. Here, the verification processconductediscombinedwiththeon-chainblockchaincurrencypayment.
Wangetal.[90]	Developed a decentralized scheme for securing cloud storage using access control. Theconventional encryption algorithm based on attributes was modified by the introduc-tion of Ethereum's smart contract technique. The distribution key is not reliant on thecentralauthority,thuspreventingtheattacksonthecentralauthority.
Zhang etal.[91]	A secure technique of Public-key encryption with an option to search for keywords re-ferredtoasSEPSEagainstkeywordguessingattacks(KGA)isdeveloped.Inthisscheme,userscanencryptkeywordsthroughathresholdwiththehelpofspecifickeyservers.

(Continued)

Table1.Continued

Authors	Findin g
Toshetal.[92]	A BlockCloud has been developed for the cloud computing framework, a blockchain-enabled information provenance architecture. Also, a PoS consensus mechanism waspresented for BlockCloud to lessen the overhead of computational necessities that theconventionalPoWconsensus requires.
Chenet al. [93]	Theydevelopedaframeworkforstoringmedicaldatabyusingblockchainandcloudstoragetechnologies sothat thedata could bestored andshared safely.
Caoetal.[94]	AsecureeHealthframeworkassistedbythecloudreferredtoasTP-EHR,whichensuredthe integrity, correctness, and confidentiality of outsourced EHRs without the introduc-tionofatrustedentitywasdeveloped.TheEHRgeneratedbyadoctorduringthep eriodof treatment was unified into the transaction of currencies based on blockchain. Thistechnique employed a key agreement based on a user-friendly password for establish-ingchannelsamongthedoctorsandthepatientsthataresafeandcanpreventattac ksof guessingpasswordswithouttheneed forany extrainvestments.
Wangetal.[95]	A system that combined the attribute-based encryption (ABE), Ethereum blockchain,and decentralized storage system IPFS. The data holder can transmit the secret keyto users and encrypt the shared information by specifying the access policy and thetechniquethathasbeendonewithfine-graineddataaccesscontrol.
Wangetal.[79]	Developed protocol for cloud storage by utilizing blockchain and Rank-based MerkleAVLtree(RB-MHT)toaccomplishpreservationofprivacyandbatchauditingformain-tainingthesecurityofthemodifiedrecordintheschemebasedonblockchain.
Yuetal.[80]	Developedasmartanddecentralizedpublicauditingplanforcloudstorage,whichelim-inatedthe requirementTPAfor auditing.
Chenet al. [96]	Suggested a performance-driven, auction-based reward system based on a blockchainconsortium that ensures belief for both on-chain and off-chain information. Authorsimplementedaconsortiumthatusedasadistributedhyperledgertotackleon-chaindata protection. Using an information performance-driven auction system, the assesseddata performanceusedto maintaintrustinoff-chain data.

Distributed Storage: SAFE network resources are never higher than 1 MB each. Clients operatingwithfilesgreaterthan1MBwouldthenhavetheirdatabrokeninto1MBchunks,whichwillthenbespreadaroundanetwork.Thisspecifiesthatastandardfileconsistsofseveralparts:chunksthat are individual portions of 1 MB after breaking the file and a datamap that stores each portionof the file's identifier. The client maintains a datamap record of the resource identifier. Therefore,theentirefilecanberetrievedbyfirstretrievingtheparticularresource(i.e.,thedatamap)eventhoughitisdistributedovermanyindividualresources.

Consensus: Utilizing a method called Proof of Resource (POR), the system can validate in amathematically verifiable manner which and what provides the resource. It is achieved by thenetwork trying to save and access chunks of data on/from its nodes. A node's ability to performsuch activities will be calculated by a combination of its CPU power, availability of

bandwidth,unusedstorage space,and onlinetime.

Sia:Distributed,Blockchain-basedCloudStorage

Sia, a decentralized-storage network. Sia allows for the creation of peer storage contracts [98].Contracts are treaties between a space supplier and their customer, defining what information willbe contained and at what cost. Contracts are held in a blockchain, which makes them auditablepublicly.Siaprovidestenantswithaccesstodistributedcloudstorageservicestoleveragecheaper,faster ways of using distribution centers accessible to anyone and are not regulated by a singleauthoritative source. Siacoin is based on a separate blockchain from Sia, and there are agreementsbetweenastoragerenterandasupplier[99].Theselectedcategoriesareexplainedbelow.

Table2.StrengthsofWorksonBlockchainTechnologyforCloudStorage

Work	Confidentiality	Integrity	Authentication	AccessControl	Searching	Auditing	Blockchain-baseddistributedclouddata storage
[55]	C	C		C	C		C
[56]	C	C				C	
[59]	C	C	C			C	
[60]		C			C		
[63]	C						
[66]	C					C	C
[67]	C	C	C	C			
[69]	C		C	C			
[72]	C		C				
[73]	C	C	C		C		
[86]	C						C
[87]	C	C				C	C
[88]	C		C				
[89]	C	C				C	
[90]	C		C	C			
[91]	C				C		
[92]		C	C			C	
[93]	C						C
[94]	C	C	C				
[95]	C			C		C	C
[79]	C				C		
[80]	C		C			C	

Confidentiality:C->privacyofinformationachievesthroughencryptionanddataaccessmanagement.Integrity: C->to manage unauthorizedmanipulation of data.
Authentication:C->toidentifythevaliduser.
Access Control: C ->to identify permission to use a resource.Searching:C->processof locating data onthecloud.
Auditing:C ->examinationofrecordstovalidatedatasecurity.
Blockchain-basedcloudstorage:C->decentralizedstorageofclouddatawithouttrustedparties.

Distributed Database: Upon uploading, the Sia program divides files into 30 parts, each targeted towards distribution to hosts worldwide. This distribution means no one host serves a singlefailurepointandincreasesoverallnetworkuptimeandredundancy.

Encryption: Every section of the file is encrypted before entering a renter's machine. It meansthat only authenticated pieces of user data are stored in hosts. It is different from traditional cloudstorageserviceslikeAmazon,whichdoesnotopttoencryptuserdata.SiautilizestheTwofishalgorithm,anopen-sourceandsecureencryptionstandard[115].

Smart Contract: The renters form file contracts with hosts using the Sia blockchain. Thesecontractssetrates,expectationsonuptime,andotheraspectsoftherenters-hostspartnership.The smart contract enables to create cryptographic Service-Level Agreements (SLAs), which are

is saving the data for the renter. It is called proof of storage if the proof of storage appears on theblockchainwithinagiventime,thehostwillbepaid.Ifnot,thenthehostwillbepenalized.

Storj

The Storj network is a reliable store of objects that encodes, fragments, and disperses data forstorage to nodes worldwide. Information is kept and delivered in a way intended to prevent viola-tions. The platform that underlies Storj is a peer-to-peer, implementable space contract. It is a
wayfortwoentities(orcomputers)todecidetotradeacertainamountofstorageformoneywithoutknowing each other. They call the machine-selling space the "farmer," and the computer-buyingspace, the "renter." Storj implements encryption on the client-side, which means that only
thepersonwhouploadsthefilehasaccesstothat.Shardingisusedforthesplittingofdatabetweenseveralnodes[100].Fordecentralizednetworks,thisprovidesstability,preservingconnectivityeven when nodes fall off the network. Also, if a network host could decrypt a file, then they wouldhaveonlyonesmallpiece.Hostsare"audited"continuouslywithanautomatedalgorithmthatverifiesthattheyhavethedocumentsthattheyclaimtohave.

DistributedHashTable(DHT):ADHTissimplyameansoftransformingabunchofself-organized nodes into a functional web. The DHT enables farmers and tenants to transmit theircontractofferstoalargenodecommunityratherthanhavingacentralserverregistereachnodeandmanageallcontracts.

ContractsandAudits:Afixed-termcontract.Overthisperiod,therenterkeepsaneyethatthe farmer is still available. The farmer responds with encoded evidence that the file is still inthem. The renter ends up paying the farmer for every proof they get and verify. This method ofchallenge->evidence->paymentis called an"audit," since the renteraudits the farmer'sstorage.

Swarm:ServerlessHostingIncentivizedPeer-to-PeerStorageandContentDistribution

Swarm is a decentralized storage network and content delivery tool, the ethereum web3 stack'snativebaselayerservice.Swarm'smainobjectiveistoprovidethepublicrecordofEthereumwithasufficientlydecentralizedandrobustarchive,inparticular,tostoreanddistributeDecentralized

WebApplications(dapps)codeanddataandblockchaindata.Fromaneconomicperspective,it allows users to pool their storage and bandwidth resources to provide those utilities to allmembers of the network. At the same time, Ethereum encourages them to do so. Swarm [101]offers a peer-to-peer application and service solution that is fault-tolerant, surveillance-resistant,andauto-sustainingandfacilitatestransactionexchangeresources.Thefollowingselectedcategoriesaresummarized below.

Distributed Database: Uploading data comprises of posting information at local Swarm node,followed by "synchronizing" local Swarm node to the resulting chunks of data with their peers inthe network. In the meantime, downloading content comprises of local Swarm node querying theappropriate chunks of data for its peers in the network and then reconstructing the informationlocally.

Encryption: The encryption feature is intended to protect the data and make the shreddedinformationhardtoreadforanySwarmnodehandling.Toencryptanddecryptthecontent,Swarmusescountermodeencryption.WhenuploadingcontenttoSwarm,theuploadeddataisbrokendowninto4KBchunks.Thesechunksareallencodedwithaseparateencryptionkeycreatedatrandom.

Filecoin

Filecoinisadistributedplatform[102]thattransformsthecloudstorageoveranalgorithmicsector.The platform executes on a blockchain with a proprietary token (also called as "Filecoin"), whichminersareobtainingbysupplyingspaceforstoragetoclients.Instead,customersarespendingFilecoin employing miners to save or circulate data. Filecoin functions as a reward layer on top ofIPFS[103]thatcanprovideanydatastorageinfrastructure.

DecentralizedStorageNetwork(DSN): FilecoinDSNisadistributedstoragesystemthatcan be audited, publicly validated, and incentively built. Customers pay a network of miners forinformation storage and retrieval; in return for fees, miners provide disk space and bandwidth.DSNs cumulative repository provided by numerous individual space suppliers and self-contained,providingcustomers with data storage and access.

Consensus: Storage providers have to persuade their customers in the Filecoin protocol thatthey saved the information they were paying to store; in practice, storage providers must createProofs-of-Storage(PoS)thattheblockchainnetwork(orthecustomersthemselves)verifies.Proof-of-Replication (PoRep) is a novel Proof-of-Storage that enables a server to persuade a customerthat certain information has been repeated into its own unique physical space. Proof-of-storagesystems allow customers to verify whether a storage provider is storing the outsourced data at themoment ofthechallenge.

Smart Contract: Filecoin offers end-users with two core primitives: Get and Put. Theseprimitives enable customers to store information at their preferred price and to retrieve data fromthemarkets.Incontrast,theprimitivesprovidethestandardusecasesforFilecoinbypromotingsmartcontracts.

IPFS:InterPlanetaryFileSystem

The IPFS is a decentralized, peer-to-peer file network designed to link all computer nodes to thesame file system. IPFS integrates a distributed hash table, a block sharing reward, and a self-certification namespace. IPFS has no single point of fault, and nodes do not need to believe eachother.IPFSisaP2Pdocumentsharingmethodaimedatradicallychangingthewayinformationis shared across the globe. IPFS [103] is made up of a variety of developments in communicationprotocols and decentralized systems combined to create a file system like no other. Nodes canstore and share data with the Distributed Hash Table without central coordination. The followingcategoriesareselected foranalyzing theIPFS network.

Table3.BuildingBlocksofDistributedCloudStorageTechnologies

	MaidSafe	Sia	Storj	Swarm	Filecoin	IPFS
CompensationModel	Payment perstorage space,CPU, bandwidth,andonlinetime	Determined byadocumentedcontract betweena storage renteranda provider	The platformcurrently paysstorage providersandbillsstoragerentersmonthly	Decentralized storage network andcontent deliverytool	Peer-to-PeerstoragemarketplacebuiltonIPFS	Data blocksbarteredwithreciprocating file sharing(Bitswap)[119]
WhoProvidesPayments?	Users andgeneratedtokens	Storagerenter	Storage renter (viaStorj)	Built-inincentive	Storagerenter (viaFilecoin)	Filedownloaders
BlockchainFoundation	None uses closegroupsconsensus	Independent Siablockchain	Counterpartybitcoinblockchain	Web3 ethereumstack	Blockchain	None usesbitswap creditprotocol
Target Usecases andScenarios	Encrypted cloudstorage, webhosting,streaming	Encrypted cloudstorage	Encrypted cloudstorage	Messaging, datasharing, peer-to-peerpayment portals,andstoragefacilities	Encryptedcloudstorage	File hosting,versioning, webhosting,andcontentdistribution

DistributedHashTable: Ahashtableisasetofinformationthatgathersdataaskey/valuesets.Information is distributed over a network in DHT and organized effectively to allow fast accessandlookupbetweennodes.Decentralization,faulttolerance,andscalabilityarethekeybenefitsofDHTs.

Merkle DAG: A Merkle DAG is a combination of a Merkle tree and a Directed Acyclic Graph.Merkle trees guarantee right, undamaged and unaltered data blocks exchanged over P2P networks.This test is done by using hash algorithms to group data blocks. Hash is primarily a function thattakes up the input and generates a single alphanumeric (hash) sequence, which refers to that input.Table3 highlighted the basic building blocks of distributedtechnologies.

6 PROPERTIES OF BLOCKCHAIN FOR CLOUD STORAGE

- ***Immutable:*** (tamper-proof and permanent) the blockchain is generally a permanent recordfor the transactions. Hence there is no provision to alter the block once added, thus creatingtrustwithintherecordofthetransaction[104].
- ***Decentralized:***Theblockchain dividesthedataintolittlepiecesandcirculates themwhileuploadingitintothecloudserver.Adecentralizedschemeoffersawiderangeofbenefits overthemoretraditionalcentralizedschemes,includingincreasedsystemreliability,scale,andpri vacy.Hence,afilestoredintheblockchaincanbecopiedoraccessedbyanynodeofthenetwork.Inad ecentralizationnetwork,eachcloudhostingserverisaccountablefortheircloudenvironmentandc ouldinteractandcollaborateviatheblockchainnetworkwith other providers. Blockchain technology is a distributed platform with a secure and dis-tributedledgerforcloudmanufacturing[105].Theblockchainisprimarilyadigitalledgeroftransac tions,sincethecomputerhasacompletecopyoftheledger,sothereisnoresultinthedataloss.Blockc hain'sdigitalledgertechnologyretainsintegrityandconfidentiality,lowersthecostofcomputing, andenhancesprecision.Further,thetransactionprocessissecured,andnootherthirdpartycanacce ssthetransactionusingblockchaintechnology.***DataValidationandEncryption:***As secret
- commercial information is shared on cloudservers,itisessentialtoimplementaneffectiveencryptionmethodtoencodeoutsourceddata. Blockchainencodeseverything,anditisprobablygoingtodemonstratethatinforma-tionhasnotbeenaltered.Furthermore,theuserscancheckorverifythefilesignaturethathasbeench angedornotwhiledistributingthedata.Ifsomeonetriestochangeoralterthe

  file, then the file signature will be invalid. No one can deny that blockchain offers a reliableandsecuresolutionwithindependentinformationconfirmation.
- ***ReliableService:***Blockchain is a representative anonymity technology. Blockchain canbe upgraded to a reliable service in combination with the cloud computing environment[107]. The blockchain makes it unfeasibly hard for attackers to obtain and split networkdata from a storage process. The blockchain's information is distributed, encrypted, andcross-checked.
- ***Obscurity Empowering:*** The public blockchains have gotten the early features and ap-provals for empowering obscurity, making private blockchains that confine access to spe-cific clients. Regardless of this, we understand the advantages of a decentralized distributedsystem. Yet, anybody getting to a private blockchain must validate their personality to ob-tain entrance benefits, which tend to be limited to specific transactions, thereby increasesprivacyprotection[108].
- ***Automationthroughsmartcontracts:***Oneofthemostlikelyconsequencesofblockchaintech nology is companies and individuals' potential to cut off the intermediaries in terms ofinformation monitoring. However, one blockchain-related technology that would improvehow people make a trade is smart contracts, which can potentially automate all transactionsandexchanges.
- ***Verifiability:***Blockchainnotonlystoresdatainadistributedandauthenticatedmannerbut also offers a serial chain with a cryptographic hash of the block in each transaction forthe verification purpose. It connects the blocks, creating a decentralized and tamper-prooftransactionledger.

7 INTEGRATING BLOCKCHAIN WITH CLOUD STORAGE-REQUIREMENTS AND CHALLENGES

Blockchain integration with cloud [109] gathers massive virtualized service structures, includinghardwareandsoftwaretools.Withinthesector,thesesystemsarereferredtoas“Infrastructureas aService” (IaaS), “Platform as a Service” (PaaS), and “Software as a Service” (SaaS). Cloud computingservices are supported in large data centers, sometimes referred to as “data farms.” Public cloudsoffer limitless access to shared information and assets for a broad range of clients, yet there is noassurancethatclients’informationwillbesecured.Accessingthedataandresourcesinprivateclou dsisconfined,andthereisaneedforalltheuserstobevalidatedwiththehelpofstrongau-thentication and authorization processes. Generally, the enterprises are the owners of the privatecloudclustersandworkunderexplicitcloudstandards.Hybridcloudsappeartobeaperfectmodelf orintegratingnumerousprivatecloudsintoacombinedglobalframework.Suchincorporationisdone viathepubliclayeroftheupperlevel.Themainissuewiththatmodelistoreachanun-derstanding among private cloud providers for operating under the unified public cloud standard.A considerably more realistic situation is the “many cloud model,” in which the delegated privatecloudgroupsareconnectedbyusingtheregularP2Porganize(Figure10).

It tends to be seen that an identical model is suitable for blockchain that was the primary explanation behind attempting to incorporate the two conditions to improve the security approaches incloudenvironments.Therearetwoprinciplestrategiesforintegratingthecloudandblockchainplat forms.

- Utilizing cloud for the advancement of blockchain applications and aiding the coordinationwith large business systems (private clouds) encourage replication, storage, and transac-tionaldataaccess.
- Utilizingblockchainstrategiesforimprovingclientsecurity,managingtheinformation,andtaskin thecloud.

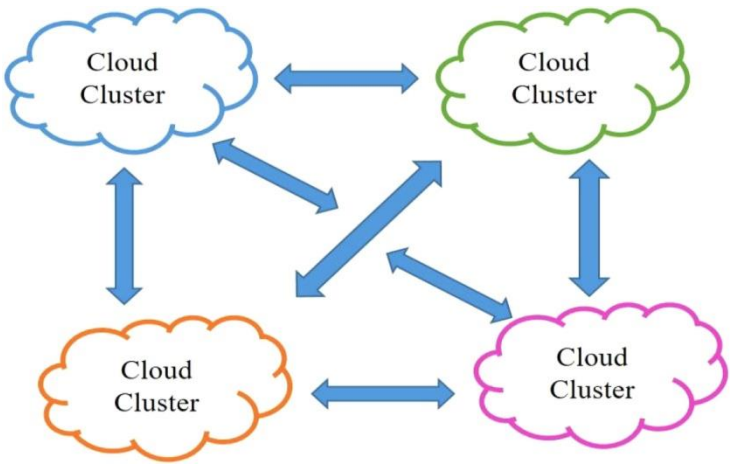

Fig.10.Thearchitectureof“ManyClouds”basedonP2P.

For blockchain systems, the transaction number can be massive. The enormous amounts ofinformationcreatedneedflexibleresourcesininformationhandling.ScalabilityandFlexibilityare perhaps the most critical functionalities within the cloud frameworks to provide dynamicallychangingactivitieswithon-

demandcloudproperties.Publiccloudshavethepotentialtodelivera large-scale resource network that is open to consumers who pay only for those that are beingused.Moreoftenthannot,privatecloudsshouldbeconfiguredtoaccommodateenormousdatasets.Cloud systems can effectively cover the physical area of knowledge from a security perspective.Tuning experiments can be continuously performed with a negligible impact on deployed appli-cations, which is crucial to the successful implementation of most blockchain algorithms. Anyblockchain system must accept data sovereignty rules and store and process the information onlyin areas allowed by the guidelines. This means that the cloud service provider requires its cus-tomers to have control over the areas in which their information is processed and stored.

Anothersignificantproblemwithblockchainsystemsistheresilienceofthearchitectureandthepowertoafault.Thismeansthatevenasinglenodefailureintheblockchainnetworkshouldnotaf-fect the entire framework's work. In these instances, cloud services aid by replicating the storedinformation and usingdifferent programming applications.

Atlast,usingthealgorithmsoftheblockchainmightenhancetheblockchainframeworkse-curity. Within a centralized cloud environment, the program could be managed centrally withinformation being stored on the local data server. Oracle Blockchain Cloud Service venture [110]andiEx.ecventure[111]areongoinginstancesofsucheffectivecoordinationoftheblockchain withcloudstages.

The mapping of blockchain technology features with the safety services supplied to protectcloud information is presented in Table 4. This table shows the case where we can take advantageof the numerous blockchain features to ensure cloud data privacy, confidentiality, accessibility,andtransparency, thus increasing efficiencyand accuracy.

8 SOME IMPORTANT INFERENCES AND RECOMMENATIONS

- ***IdentityManagementSystem:***Theidentitymanagementschemeisvitalfor CSPandcloudcomputingusers.Theusersadopttheiridentitytoaccesstheirdatainthecloud.Differentlimitations oftheidentityadministrationsystemarerecognized.Blockchaintechnologyprovidesameans toavoidthisissuebyprovidingasafemethodwithoutanytrustworthy

Table4.MappingofBlockchainCharacteristicswithSecurityServices

	Secure TransactionsCase (Digital LedgerTechnology)	Safe DataStorage Case(Decentralized)	Authentication Case(Datavalidationandencryption)	MinimizingError Case	SecureBlockchain Solution
Integrity		C			C
Scalability	C		C		C
Confidentiality	C	C	C	C	C
Anonymity		C			C
Efficiency	C		C	C	C
ComputationCost		C		C	C
PrivacyProtection	C		C		C
Availability		C	C	C	C

party. It could be used to create a blockchain-based identity system, making it possible forentities to handle it, offering them more power over who has their data and how they accessit. It is, therefore, necessary to combine the decentralized blockchain principle with identitycontrol to create a digital ID that will function as a digital watermark that can be given toanyinternet transaction[112].

- ***SecureDataClassification:***Cloudcomputingdatacenterscanstorethedataofdistinctiveusers. Based on the importance of information, the characterization of information providessecurity in the cloud. Dependent on the category of data, this scheme offers various aspectssuchasrecurrence,refreshrecurrence,andaccessbydifferentusers[113].Thesecuritylevelincorporates classification, encryption, respectability, capacity, and so on that are chosen todepend on the type of information [114]. The classified information must be secured, sinceit contains the most sensitive information. There is a definite need for a better solutionbasedonblockchainsecuritymethodstosecureacustomer'sclassifiedinformation.
- ***CloudComputingServiceforTrust-basedSecureSolution:***Thesecuritydomainforimplementation of the cloud computing administrations alongside in general security contemplationsisatest.Thecloudcomputingframeworkshouldbefocusedontherequirementof a secure and trusted solution based on blockchain for cloud computing service [115].Blockchainisaconceptaimedatdecentralizationasasecuritymeasure,hasthefunctionof creating a global index for all transactions that take place in a given network and makesthemunchangeable[116].
- ***Infrastructure Security:*** Concerning which party (customer or CSP) provides which protection methods there is a need for transparency. There is likely a need for

agreement,which gives the details about the security capacities and more noteworthy confirmationover the CSP's efforts and capabilities [117]. To address the issues, the identity administra-tionsystemneedstobeadoptedinthecurrentblockchaininfrastructureforresolvingtheinterrelationshipbetweenservicemodel,user,andsystem[118].

- ***Data Storage and Security:*** For the future of cloud computing, information security abilitiesaresignificant.Thisallowsustosaveinformationinthecloudandbesafe.Fordatastorage and security in the future, they combined with the present deficient encryption, keyadministration capacities, and cryptographic research endeavors. For example, to restrainthe amount of information, the predicate encryption can be used to decode the informationinthecloud[119].Cloudcomputing'smainsignificanceishomomorphicencryption, whichinvolvestheprocessofencodinginformationinthecloud.Therefore,thefuturebusiness

Table5.Mapping ofResearchQuestionswith theReferences

ResearchQuestion	Reference
RQ1	[3,4,6,7,14,15,37,38,39,61,65,109]
RQ2	[1,8,9,28,29,30,31,32,33,34,35,36,114,115]
RQ3	[5,13,28,29,30,40,54,57,58,106,116,117,131]
RQ4	[2,10,16,17,18,19,20,21,22,23,24,25,26,27,41,42,43,44,45,46,47,52,53,59,70,71,75,76,93,96,97,98,104,107,108,122,123,124,125,126,128,129,130,132,133,134,135]
RQ5	[11,12,48,49,51,55,56,60,62,63,67,68,69,72,73,74,77,78,79,81,82,83,85,86,90,91,92,93,94,95,99,100,101,102,103,105,110,111,121]
RQ6	[48,49,50,51,60,62,63,64,66,72,74,77,78,79,80,82,83,85,86,87,88,89,90,91,92,93,94,95,99,100,101,102,103,112,113,118,120,127]

practicality of such abilities would be a huge advantage to cloud computing [120]. It needsablock-basedsystemwithasecurebooleansearchforsecurecloudstorage.

- ***SecurityManagement:***Thereisaneedtoinitiatestandardorganizations(e.g.,WorldWideWeb Consortium (W3C), the Internet Engineering Task Force (IETF), the Organization fortheAdvancementofStructuredInformationStandards(OASIS))andstartneweffortsforthe management protocols that interoperate with many clouds [121, 122]. To increase cloudselection, the cloud management standards will be created and supported by the cloud ser-vice provider, which encourages consistent interoperability crosswise over different clouds.Like the customer/server period, guidelines will make a biological system of IndependentSoftwareVendors(ISVs)andspecialistorganizationsthatgiveclientsdecision,adaptability,andgreateragilitybythemethodofcomputerization[123].Also,thereisaneedforSoftware Defined Networking (SDN)-based blockchain to adapt the security without the reviewoftheadministratorautomatically.Itcanalleviatespecificproblemssuchasadaptability,effectiveness,accessibility,andsafety[124].
- ***Privacy:***PrivacyisessentialfortheCSPtounderstandthemainprivacylawstorealizethe data transaction from one place to another. It is yet to solve the type of governmentintercession or the formation of a worldwide security standard that will give reliabilitycrosswise controls. Specific gauges will offer to characterize the way organizations can usecloudcomputing[125].Whencloudcomputingturnsouttobemorestandard,thereportsofregular review increased by specific necessities around protection and security may reviewconcerned with the handling of information and its protection concerns [126]. Blockchain-based data provenance architecture is necessary to ensure the processing of

information incloudstoragewhileatthesametime,increasingprivacyandaccessibility[127]. Table5summarizesthedetailsofthestudiesaddressingeachresearchquestion.

CONCLUSIONS

In this article, a systematic survey (2010–2019) of blockchain technology and cloud computing tosecurecloudstoragehasbeenassessed.Blockchainpresentsnumerousguaranteesforthefutureof cloud data. The first one is that clients could be responsible for controlling their data andthe transactions in various areas. Hence, trust is built that the transactions are being executedprecisely as per the protocol directions, eliminating the trusted third-party requirement. Thisidea can impact cloud data to discover a solution for managing and storing the informationappropriately on a P2P network. Blockchain innovation can be another piece of the
encompassingbiologicalsystemofinstrumentsthatclouddatautilizes.Inreality,itcanassumeavitalj obinsecurityforauthenticatingandpreventingaccessdependingontheuser'srequirementsby

recordingthehistoriesofdataaccessandlegitimateutilizationofencryptionontheinformation.A few challenges are still present, for example, accord models, the computational expenses ofmining blocks, and transaction validation. Additionally, Blockchain applications provide solutionsinvolvingessentialchangesorcompletereplacementofexistingframeworks.Thatisthereasonf or the transaction not being quick and straightforward. In any case, we are still in the beginningstages of the development of Blockchain, and these impediments will, in the end, be overcome,opening the wayfor some energizingpotential outcomes.

REFERENCES

[1] Zhihua Xia, Xinhui Wang, Liangao Zhang, Zhan Qin, Xingming Sun, and Kui Ren. 2016. A privacy-preserving andcopy-deterrencecontent-basedimageretrievalschemeincloudcomputing.*IEEETrans.Info.ForensicsSecur.*11,11(2016), 2594–2608.https://doi.org/10.1109/TIFS.2016.2590944

[2] Xueping Liang, Sachin Shetty, Deepak Tosh, Charles Kamhoua, Kevin Kwiat, and Laurent Njilla. 2017. Provchain:Ablockchain-baseddataprovenancearchitectureincloudenvironmentwithenhancedprivacyandavailability.In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing*. 468–477.https://doi.org/10.1109/CCGRID.2017.8

[3] David S. Linthicum. 2010. *Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide*. PearsonEducation.

[4] Rajnish Choubey, Rajshree Dubey, and Joy Bhattacharjee. 2011. A survey on cloud computing security, challenges,andthreats.*Int.J.Comput.Sci.Engineer.*3(2011),1227–1231.

[5] Bin Feng, Xinzhu Ma, Cheng Guo, Hui Shi, Zhangjie Fu, and Tie Qiu. 2016. An efficient protocol with bidirec-tionalverificationforstoragesecurityincloudcomputing.*IEEEAccess*4(2016),7899–7911.https://doi.org/10.1109/ACCESS.2016.2621005

[6] CongWang,KuiRen,andJiaWang.2016.Secureoptimizationcomputationoutsourcingincloudcomputing:Acasestudyoflinearprogramming.*IEEETrans.Comput.*65,1(2016),216–229.https://doi.org/10.1109/TC.2015.2417542

[7] JinLi,YinghuiZhang,XiaofengChen,andYangXiang.2018.Secureattribute-baseddatasharingforresource-limitedusersincloudcomputing.*Comput.Secur.*72(2018),1–12.https://doi.org/10.1016/j.cose.2017.08.007

[8] PingLi,JinLi,ZhenganHuang,Chong-ZhiGao,Wen-BinChen,andKaiChen.2017.Privacy-preservingoutsourcedclassificationincloudcomputing.*ClusterComput*.21,1(2017),1–10.https://doi.org/10.1007/s10586-017-0849-9

[9] Jianfeng Wang, Xiaofeng Chen, Xinyi Huang, Ilsun You, and Yang Xiang. 2015. Verifiable auditing for outsourceddatabaseincloudcomputing.*IEEETrans.Comput.*1(2015),1–1.https://doi.org/10.1109/TC.2015.2401036

[10] Michael Nofer, Peter Gomber, Oliver Hinz, and Dirk Schiereck. 2017. Blockchain. *Bus. Info. Syst. Engineer*. 59, 3(2017),183–187.https://doi.org/10.1007/s12599-017-0467-3

[11] Chenhan Xu, Kun Wang, and Mingyi Guo. 2017. Intelligent resource management in blockchain-based cloud datacenters.*IEEECloudComput*.4,6(2017),50–59.https://doi.org/10.1109/MCC.2018.1081060

[12] HarleenKaur,M.AfsharAlam,RoshanJameel,AshishKumarMourya,andVictorChang.2018.Approposedsolutionand future direction for blockchain-based heterogeneous medicare data in cloud environment. *J. Med. Syst.* 42, 8(2018),156.https://doi.org/10.1007/s10916-018-1007-5

[13] FaridDaryabar,AliDehghantanha,andKim-KwangRaymondChoo.2017.Cloudstorageforensics:MEGAasacasestudy.*Austral.J.ForensicSci.*49,3(2017),344–357.https://doi.org/10.1080/00450618.2016.1153714

[14] Sushant Rajkumar Patil. 2016. A comparative review on Ceph and Swift open source cloud storage platform, globaltrends in signal processing. In *Proceedings of the IEEE International Conference on Information Computing and Communication(ICGTSPICC'16)*.https://doi.org/10.1109/ICGTSPICC.2016.7955300

[15] DavidBrianFerriera. 2014.Policydrivencloudstoragemanagementandcloudstoragepolicyrouter.5

(2014),8.
[16] A.Maxmen.2018.AIresearchersembracebitcointechnologytosharemedicaldata.*Nature*,555(2018),7696.
[17] Wei Cai, Zehua Wang, Jason B. Ernst, Zhen Hong, Chen Feng, and Victor C. M. Leung. 2018. Decentralized ap-plications:theblockchain-empoweredsoftwaresystem.*IEEEAccess*6(2018),53019–53033.https://doi.org/10.1109/ACCESS.2017
[18] SaveenA.Abeyratne,andRadmehrP.Monfared.2016.Blockchainreadymanufacturingsupplychainusingdistributedledger.*InternationalJournalofResearchinEngineeringandTechnology*5,9(2016).Retrievedfromhttps://repository.lboro.ac.uk/articles/Blockchain_ready_manufacturing_supply_chain_using_distributed_ledger/9566069https://doi.org/10.15623/ijret.2016.0509001.
[19] SantoshiNakamoto.2008.Bitcoin:APeer-to-PeerElectronicCashSystem.Retrievedfromhttps://bitcoin.org/bitcoin.pdf.

[20] Zachary Baynham-Herd, 2017. Enlist blockchain to boost conservation. *Nature* 548, 7669 (2017), 523–523. https://doi.org/10.1038/548523c
[21] Selena Ahmed, and Noah ten Broek. 2017. Blockchain could boost food security. *Nature* 550, 7674 (2017), 43–43.https://doi.org/10.1038/550043e
[22] Jong-HyoukLeeandMarcPilkington.2017.Howtheblockchainrevolutionwillreshapetheconsumerelectron-ics industry [future directions]. *IEEE Consumer Electron. Mag.* 6, 3 (2017), 19–23. https://doi.org/10.1109/MCE.2017.2684916
[23] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. 2017. An overview of blockchaintechnology: Architecture, consensus, and future trends. In *Proceedings of the IEEE International Congress on Big Data(BigData'17)*.557–564.https://doi.org/10.1109/BigDataCongress.2017.85
[24] MosakheilandJamalHayat.2018.Securitythreatsclassificationinblockchains.*CulminatingProjectsinInformationAssurance*. Retrievedfromhttps://repository.stcloudstate.edu/msia_etds/48.
[25] Lakshmi Siva Sankar, M. Sindhu, and M. Sethumadhavan. 2017. Survey of consensus protocols on blockchain ap-plications. *Proceedings of the 4th IEEE International Conference on Advanced Computing and Communication Systems(ICACCS'17)*.https://doi.org/10.1109/ICACCS.2017.8014672
[26] AoLei,HaithamCruickshank,YueCao,PhilipAsuquo,ChibuezeP.AnyigorOgah,andZhiliSun.2017.Blockchain-baseddynamickeymanagementforheterogeneousintelligenttransportationsystems.*IEEEInternetThingsJ*.4,6(2017),1832–1843.https://doi.org/10.1109/JIOT.2017.2740569
[27] ChinmayA.VyasandMunindraLunagaria.2014.Securityconcernsandissuesforbitcoin.In*ProceedingsoftheNationalConferencecumWorkshoponBioinformaticsandComputationalBiology(NCWBCB'14)*.
[28] LucaFerretti,MircoMarchetti,MauroAndreolini,andMicheleColajanni.2018.Asymmetriccryptographicschemefordataintegrityverificationinclouddatabases.*Info.Sci*.422(2018),497–515.https://doi.org/10.1016/j.ins.2017.09.033
[29] Yunxue Yan, Lei Wu, Ge Gao, Hao Wang, and Wenyu Xu. 2018. A dynamic integrity verification scheme of cloudstorage data based on lattice and Bloom filter. *J. Info. Secur. Appl.* 39 (2018), 10–18. https://doi.org/10.1016/j.jisa.2018.01.004
[30] GuangweiXu,MiaolinLai,JingLi,LiSun,andXiujinShi.2018.Agenericintegrityverificationalgorithmofversionfilesforclouddeduplicationdatastorage.*EURASIPJ.Info.Secur*.12(2018),1.https://doi.org/10.1186/s13635-018-0083-x

[31] Hao Jin, Ke Zhou, Hong Jiang, Dongliang Lei, Ronglei Wei, and Chunhua Li. 2018. Full integrity and freshness forclouddata.*FutureGen.Comput.Syst.*80(2018),640–652.https://doi.org/10.1016/j.future.2016.06.013

[32] RajatSaxenaandSomnathDey.2016.Cloudaudit:Adataintegrityverificationapproachforcloudcomputing. *ProcediaComput.Sci.*89(2016),142–151.https://doi.org/10.1016/j.procs.2016.06.024

[33] Jian Mao, Yan Zhang, Pei Li, Teng Li, Qianhong Wu, and Jianwei Liu. 2017. A position aware Merkle tree for dynamicclouddataintegrityverification.*SoftComput.*21,8(2017),2151–2164.https://doi.org/10.1007/s00500-015-1918-8

[34] Yuan Zhang, Chunxiang Xu, Xiaohui Liang, Hongwei Li, Yi Mu, and Xiaojun Zhang. 2017. Efficient public verifi-cation of data integrity for cloud storage systems from indistinguishability obfuscation. *IEEE Trans. Info. ForensicsSecur.*12,3(2017),676–688.https://doi.org/10.1109/TIFS.2016.2631951

[35] TaoJiang,XiaofengChen,andJianfengMa.2016.Publicintegrityauditingforshareddynamicclouddatawithgroupuserrevocation.*IEEETrans.Comput.*65,8(2016),2363–2373.https://doi.org/10.1109/TC.2015.2389955

[36] Marcus Brandenburger, Christian Cachin, and Nikola Knežević. 2017. Don't trust the cloud, verify: Integrity andconsistencyforcloudobjectstores.*ACMTrans.PrivacySecur.*20(2017),3.https://doi.org/10.1145/3079762

[37] JiaweiYuanandShuchengYu.2015.Publicintegrityauditingfordynamicdatasharingwithmultiusermodification. *IEEETrans.Info.ForensicsSecur.*10,8(2015),1717–1726.https://doi.org/10.1109/TIFS.2015.2423264

[38] Yibin Li, Keke Gai, Longfei Qiu, Meikang Qiu, and Zhao Hui. 2017. Intelligent cryptography approach for securedistributedbigdatastorageincloudcomputing.*Info.Sci.*387(2017),103–115.https://doi.org/10.1016/j.ins.2016.09.005

[39] Zahra Pooranian, Kang-Cheng Chen, Chai-Mu Yu, and Mauro Conti. 2018. RARE: Defeating side channels basedondata-deduplicationincloudstorage.In*ProceedingsoftheInfocomWorkshop*.https://doi.org/10.1109/INFCOMW.2018.8406888

[40] Chia-Mu Yu, Sarada P. Gochhayat, Mauro Conti, and Chun-Shien Lu. 2018. Privacy aware data deduplication forsidechannelincloudstorage.*IEEETrans.CloudComput.*1(2018),1–1.https://doi.org/10.1109/TCC.2018.2794542

[41] IoannisKonstantinidis,GeorgiousSiaminos,ChristosTimplalexis,PanagiotisZervas,VassiliosPeristeras,andStefanDecker. 2018. Blockchain for business applications: A systematic literature review. In *Proceedings of the InternationalConference on Business Information Systems*. Springer, Cham, 384–399. https://doi.org/10.1007/978-3-319-93931-5_28

[42] Qalab E. Abbas, and Jang S. Bong. 2019. A survey of blockchain and its applications. In *Proceedings of the Inter-national Conference on Artificial Intelligence in Information and Communication (ICAIIC'19)*. 1–3. https://doi.org/10.1109/ICAIIC.2019.8669067

[43] F. Rizal Batubara, Jolien Ubacht, and Marijn Janssen. 2018. Challenges of blockchain technology adoption for e-government: A systematic literature review. In *Proceedings of the 19th Annual International Conference on DigitalGovernmentResearch:GovernanceintheDataAge*.1–9.https://doi.org/10.1145/3209281.3209317

[44] Cornelius C. Agbo, Qusay H. Mahmoud, and J. Mikael Eklund. 2019. Blockchain technology in healthcare: A sys-

tematicreview.*HealthcareMultidisc.DigitalPublish.Inst.*7,2(2019),56.https://doi.org/10.3390/healthcare7020056

[45] Seyednima Khezr, Md Moniruzzaman, Abdulsalam Yassine, and Rachid Benlamri. 2019. Blockchain technology inhealthcare: A comprehensive review and directions for future research. *Appl. Sci.* 1–28. https://doi.org/10.3390/app9091736

[46] AsadA.Siyal,AishaZ.Junejo,MuhammadZawish,KainatAhmed,AimanKhalil,andGeorgiaSoursou.2019.Ap-plications of blockchain technology in medicine and healthcare: Challenges and future perspectives. *Cryptography*3,1(2019),1–16.https://doi.org/10.3390/cryptography3010003

[47] Rui Zhang, Rui Xue, and Ling Liu. 2019. Security and privacy issues on blockchain. *ACM Comput. Surveys* 52, 3(2019),1–35.https://doi.org/10.1145/3316481

[48] JoannaKołodziej,AndrezejWilczyński,DamianF.Cerero,andAlejandroF.Montes.2018.Blockchainsecurecloud:A new generation integrated cloud and blockchain platforms-general concepts and challenges. *Eur. Cybersecur. J*.28–34.

[49] GuangshengYu,XuWang,KanYu,WeiNi,J.AndrewZhang,andRenP.Liu.2019.Survey:Shardinginblockchains.
*IEEEAccess*8(2019),14155–14181.https://doi.org/10.1109/ACCESS.2020.2965147

[50] ShaoanXie,ZibinZheng,WeiliChen,JiajingWu,HongN.Dai,andMuhammadImran.2019.Blockchainforcloudexchange:Asurvey.*Comput.Electric.Engineer*.81(2019),1–20.https://doi.org/10.1016/j.compeleceng.2019.106526

[51] Ruizhe Yang, F. Richard Yu, Pengbo Si, Zhaoxin Yang, and Yanhua Zhang. 2018. Integrated blockchain and edgecomputing systems: A survey, some research issues and challenges. *IEEE Commun. Surveys Tutor*. 21, 2 (2018), 1–22.https://doi.org/10.1109/COMST.2019.2894727

[52] Tara Salman, Maede Zolanvari, Aiman Erbad, Raj Jain, and Mohammed Samaka. 2019. A security services usingblockchains:Astateoftheartsurvey.*IEEECommun.SurveysTutor*.21,1(2019),858–879.https://doi.org/10.1109/COMST.2018.2863956

[53] BhabenduK.Mohanta,DebasishJena,SoumyashreeS.Panda,andSrichandanSobhanayak.2019. Blockchaintech-nology:Asurveyonapplicationsandsecurityprivacychallenges.*InternetThings*8(2019),1–19.https://doi.org/10.1016/j.iot.2019.100107

[54] YoungjooShin,DongyoungKoo,andJunbeomHur.2017.Asurveyofsecuredatadeduplicationschemesforcloudstoragesystems.*ACMComput.Surveys*49(2017),4.https://doi.org/10.1145/3017428 54=137

[55] HoangGiangDoandWeeKeongNg.2017.Blockchain-basedsystemforsecuredatastoragewithprivatekey-word search. In *Proceedings of the IEEE World Congress on Services (SERVICES'17)*. 90–93. https://doi.org/10.1109/SERVICES.2017.23

[56] Li, Jingyi,JigangWu, LongChen,and JiaxingLi.2018. Deduplicationwithblockchainfor securecloudstorage. In *ProceedingsoftheCCFConferenceonBigData*.Springer,558–570.https://doi.org/10.1007/978-981-13-2922-7_36

[57] Xiao-LongLiu,Ruey-KaiSheu,Shyan-MingYuan,andYu-NingWang.2016.Afile-deduplicatedprivatecloudstor-ageservicewithCDMIstandard.*Comput.Stand.Interfaces*44,18–27.https://doi.org/10.1016/j.csi.2015.09.010

[58] S. Supriya and S. Mythili. 2017. Study on data deduplication in cloud computing. *Int. J. Adv. Res. Comput. Sci.* 8 (2017),8.https://doi.org/10.26483/ijarcs.v8i8.4689

[59] Liu, Bin, Xiao Liang Yu, Shiping Chen, Xiwei Xu, and Liming Zhu. 2017. Blockchain based data integrity serviceframeworkforIoTdata.In*ProceedingsoftheIEEEInternationalConferenceonWebServices(ICWS'17)*.468–475.https://doi.org/10.1109/ICWS.2017.54

[60] Yue, Dongdong, Ruixuan Li, Yan Zhang, Wenlong Tian, and Chengyi Peng. 2018. blockchain based data integrityverification in p2p cloud storage. In *Proceedings of the IEEE 24th International Conference on Parallel and DistributedSystems(ICPADS'18)*.561–568.https://doi.org/10.1109/PADSW.2018.8644863

[61] Deka Ganesh Chandra, Ravi Prakash, and Swati Lamdharia. 2012. A study on cloud database. In *Proceedings of the4th IEEE International Conference on Computational Intelligence and Communication Networks (CICN'12)*. 513–519.https://doi.org/10.1109/CICN.2012.35

[62] VandanaBhatiaandAjayJangra.2014.SETiNS:StorageefficiencytechniquesinNo-SQLdatabaseforCloudbaseddesign. In *Proceedings of the IEEE International Conference on Advances in Engineering and Technology Research(ICAETR'14)*.https://doi.org/10.1109/ICAETR.2014.7012839

[63] JosefGattermayerandPavelTvrdik.2017.Blockchain-basedmulti-levelscoringsystemforP2Pclusters.In*Proceed-ings of the 46th International Conference on Parallel Processing Workshops (ICPPW'17)*. 301–308. https://doi.org/10.1109/ICPPW.2017.50

[64] HussamAbu-Libdeh,LonniePrincehouse,andHakimWeatherspoon.2010.RACS:Acaseforcloudstoragediversity. In*Proceedingsofthe1stACMSymposiumonCloudComputing*.https://doi.org/10.1145/1807128.1807165

[65] AmbarishKumarPatel.2017.Cloudstorageanditssecuretechniques.*Int.J.Engineer.Sci*.7(2017),6603.

[66] JiaxingLi,JigangWu,andLongChen.2018.Block-Secure:BlockchainbasedschemeforsecureP2Pcloudstorage. *Info.Sci.*465,219–231.https://doi.org/10.1016/j.ins.2018.06.071

[67] Ilya Sukhodolskiy and Sergey Zapechnikov. 2018. A blockchain-based access control system for cloud storage. In*Proceedings of the IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus'18)*.1575–1578.https://doi.org/10.1109/EIConRus.2018.8317400

[68] Qi Xia, Emmanuel Sifah, Abla Smahi, Sandro Amofa, and Xiaosong Zhang. 2017. BBDS: Blockchain-based datasharing for electronic medical records in cloud environments. *Information* 8, 2 (2017), 44. https://doi.org/10.3390/info8020044

[69] Jason Paul Cruz, Yuichi Kaji, and Naoto Yanai. 2018. RBAC-SC: Role-based access control using smart contract. *IEEEAccess*6(2018),12240–12251.https://doi.org/10.1109/ACCESS.2018.2812844

[70] IttayEyal,AdemE.Gencer,EminG.Sirer,andRobbertVanRenesse.2016.Bitcoin-ng:Ascalableblockchainpro-tocol.In*Proceedingsofthe13thUSENIXSymposiumonNetworkedSystemsDesignandImplementation(NSDI'16)*.45–59.

[71] Christopher Natoli and Vincent Gramoli. 2016. The blockchain anomaly. In *Proceedings of the IEEE 15th InternationalSymposiumonNetworkComputingandApplications(NCA'16)*,310–317.https://doi.org/10.1109/NCA.2016.7778635

[72] Yinghui Zhang, Robert H. Deng, Ximeng Liu, and Dong Zhen. 2018. Blockchain based robust and efficient fairpayment for outsourcing services in cloud computing. *Info. Sci.* 462 (2018), 262–277. https://doi.org/10.1016/j.ins.2018.06.018

[73] S.Pavithra,S.Ramya,andS.Prathibha.2019.Asurveyoncloudsecurityissuesandblockchains.In*P*

roceedingsof the 3rd International Conference on Computing and Communication Technologies (ICCCT'19), 136–140. https://doi.org/10.1109/ICCCT2.2019.8824891

[74] ChangsangYang,XiaofengChen,andYangXiang.2018.Blockchain-basedpubliclyverifiabledatadeletionschemeforcloudstorage.*J.Netw.Comput.Appl.*103(2018), 185–193.https://doi.org/10.1016/j.jnca.2017.11.011

[75] Pasquale Giungato, Roberto Rana, Angela Tarabella, and Caterina Tricase. 2017. Current trends in sustainability ofbitcoinsandrelatedblockchaintechnology.*Sustainability*9,12(2017),2214.https://doi.org/10.3390/su9122214

[76] MahdiH.MirazandMaarufAli.2018.Applicationsofblockchaintechnologybeyondcryptocurrency.*InternationalAssociationofEducatorsandResearchers(IAER)*2,1(2018),1–6.https://doi.org/10.33166/AETiC.2018.01.001

[77] HuigeLi,HaiboTian,andJiejieHe.2018.Blockchain-basedsearchablesymmetricencryptionscheme.*Comput. Electric.Engineer*.73(2018),32–45.https://doi.org/10.1016/j.compeleceng.2018.10.015

[78] Hong Giang Do and Wee Keong Ng. 2017. Blockchain-based system for secure data storage with private keywordsearch. In *Proceedings of the IEEE World Congress on Services (SERVICES'17)* 90–93. https://doi.org/10.1109/SERVICES.2017.23

[79] Han Wang, Xu An Wang, Shuai Xiao, and Zichen Zhou. 2019. Blockchain-based public auditing scheme for shareddata.In*ProceedingsoftheInternationalConferenceonInnovativeMobileandInternetServicesinUbiquitousComputing*. Springer,Cham,197–206.https://doi.org/10.1007/978-3-030-22263-5_19

[80] HiayangYuandZhenYang.2018.DecentralizedandsmartpublicauditingforcloudStorage.In*ProceedingsoftheIEEE9thInternationalConferenceonSoftwareEngineeringandServiceScience(ICSESS'18)*(491–494).IEEE.https://doi.org/10.1109/ICSESS.2018.8663780

[81] JinHoParkandJongHyukPark.2017.Blockchainsecurityincloudcomputing:Usecases,challengesandsolutions. *Symmetry*9,8(2017),1–13.https://doi.org/10.3390/sym9080164

[82] Yinghui Zhang, Robert H. Deng, Jiangang Shu, Kan Yang, and Dong Zheng. 2018. TKSE: Trustworthy keywordsearch over encrypted data with two-side verifiability via blockchain. *IEEE Access* 6 (2018), 31077–31087. https://doi.org/10.1109/ACCESS.2018.2844400

[83] Jacob Eberhardt and Stefan Tai. 2017. On or off the blockchain? Insights on off-chaining computation and data. In*Service-OrientedandCloudComputing(ESOCC'17)*,F.DePaoli,S.Schulte,andJohnsenE.Broch(Eds.).LectureNotesinComputerScience,Vol.10465,Springer,Cham.https://doi.org/3-15.10.1007/978-3-319-67262-5_1.

[84] Xiaolong Liu, Riqing Chen, Yu-Wen Chen, and Shyan-Ming Yuan. 2018. Off-chain data fetching architecture forethereum smart contract. In *Proceedings of the International Conference on Cloud Computing, Big Data and Blockchain(ICCBB'18)*.1–4.https://doi.org/10.1109/ICCBB.2018.8756348

[85] StorageNeedsforBlockchainTechnology.2019.IBMstorage.RetrievedfromhttpsIBMstorage.Retrievedfromhttps://www.ibm.com/blogs/systems/storage-for-blockchain-and-modern-distributed-database-processing/.

[86] PradipK.Sharma,Mu-YenChen,andJongH.Park.2017.AsoftwaredefinedfognodebaseddistributedblockchaincloudarchitectureforIoT.*IEEEAccess*6(2017),115–124.https://doi.org/10.1109/ACCESS.2017.2757955

[87] SyedS.Hasan,NazatulH.Sultan,andFerdousA.Barbhuiya.2019.Clouddataprovenanceusingipfsandblockchaintechnology.In*Proceedingsofthe7thInternationalWorkshoponSecurityinCloudComputing*.5–12.https://doi.org/10.1145/3327962.3331457

[88] Ahsan Manzoor, Madhsanka Liyanage, An Braeke, Salil S. Kanhere, and Mika Ylianttila. 2019, May. Blockchainbasedproxyre-encryptionschemeforsecureIOTdatasharing.In*ProceedingsoftheIEEEInternationalConferenceonBlockchainandCryptocurrency(ICBC'19)*.99–103.https://doi.org/10.1109/BLOC.2019.8751336

[89] Yuan Zhang, Chunxiang Xu, Xiaodong Lin, and Xuemin S. Shen. 2019. Blockchain-based public integrity verifica-tion for cloud storage against procrastinating auditors. *IEEE Trans. Cloud Comput*. https://doi.org/10.1109/TCC.2019.2908400

[90] Shangping Wang, Xu Wang, and Yaling Zhang. 2019. A secure cloud storage framework with access control basedonblockchain.*IEEEAccess*.7(2019),112713–112725.https://doi.org/10.1109/ACCESS.2019.2929205

[91] Yuan Zhang, Chunxiang Xu, Jianbing Ni, Hongwei Li, and Xuemin S. Shen. 2019. Blockchain-assisted public-keyencryption with keyword search against keyword guessing attacks for cloud storage. *IEEE Trans. Cloud Comput*.https://doi.org/10.1109/TCC.2019.2923222

[92] DeepakTosh,SachinShetty,XuepingLiang,CharlesKamhoua,andLaurentL.Njilla.2019.Dataprovenanceinthecloud:Ablockchain-basedapproach.*IEEEConsumerElectron.Mag*.84,38–44.https://doi.org/10.1109/MCE.2019.2892222

[93] YiChen,ShuaiDing,ZhengXu,HandongZheng,andShanlinYang.2019.Blockchain-basedmedicalrecordssecurestorageandmedicalserviceframework.*J.Med.Syst*.43,1(2019),5.https://doi.org/10.1007/s10916-018-1121-4

[94] Sheng Cao, Gexiang Zhang, Pengfei Liu, Xiaosong Zhang, and Ferrante Neri. 2019. Cloud-assisted secure eHealthsystemsfortamper-proofingEHRviablockchain.*Info.Sci*.485,427–440.https://doi.org/10.1016/j.ins.2019.02.038

[95] Shangping Wang, Yinglong Zhang, and Yaling Zhang. 2018. A blockchain-based framework for data sharing withfine-grained access control in decentralized storage systems. *IEEE Access* 6, 38437–38450. https://doi.org/10.1109/ACCESS.2018.2851611

[96] Wuhui Chen, Yufei Chen, Xu Chen, and Zibin Zheng. 2019. Toward secure data sharing for the IoV: A quality-drivenincentivemechanismwithon-chainandoff-chainguarantees.*IEEEInternetThingsJ*.7,3(2019),1625–1640.https://doi.org/10.1109/JIOT.2019.2946611

[97] NickLambert,QiMa,andDavidIrvine.2015.Safecoin:Thedecentralizednetworktoken.Retrievedfromhttps://docs.maidsafe.net/Whitepapers/pdf/Safecoin.pdf.

[98] Vitalik Buterin. 2013. Ethereum white paper: A next generation smart contract and decentralized application platform.Retrievedfromhttps://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

[99] DavidVorick.andLukeChampine.2014.Sia:Simpledecentralizedstorage.NebulousInc.Retrievedfromhttps://sia.tech/sia.pdf.

[100] Storj Labs, Inc. 2018. Storj: A decentralized cloud storage network framework. Retrieved from https://storj.io/storj.pdf.

[101] Swarm.2017.Retrievedfromhttps://swarm-guide.readthedocs.io/en/latest/introduction.html.

[102] ProtocolLabs.2017.Filecoin:ADecentralizedStorageNetwork.Retrievedfromhttps://filecoin.io/filecoin.pdf.

[103] JuanBenet.IPFS:ContentAddressed,Versioned,P2PFileSystem.RetrievedfromhttpsIpfs.io/ipfs/QmR7GSQM93Cx5eAg6a6yRzNde1FQv7uL6X1o4k7zrJa3LX/ipfs.draft3.pdf.

[104] KarimSultan,UmarRuhi,andRubinaLakhani.2018.Conceptualizingblockchains:Characteristicsandapplications.Retrievedfromhttps://arxiv.org/abs/1806.03693v1.

[105] Barenji, Ali Vatankhah, Hanyang Guo, Zonggui Tian, Zhi Li, W. M. Wang, and George Q. Huang. 2019. Blockchain-basedcloudmanufacturing: decentralization.Retrieved from https://arxiv.org/abs/1901.10403.

[106] Emil Stefanov, Marten van Dijk, Ari Juels, and Alina Oprea. 2012. Iris: A scalable cloud file system with efficientintegritychecks.In*Proceedingsofthe28thAnnualComputerSecurityApplicationsConference*.229–238.https://doi.org/10.1145/2420950.2420985

[107] Jesus Emanuel Ferreira, Vanessa R. L. Chicarino, Célio VN de Albuquerque, and Antônio A. de A. Rocha. 2018. Asurvey of how to use blockchain to secure internet of things and the stalker attack. *Secur. Commun. Networks* 7(2018),1–27.https://doi.org/10.1155/2018/9675050

[108] Nurzhan Aitzhan, Zhumabekuly, and Davor Svetinovic. 2018. Security and privacy in decentralized energy tradingthroughmulti-signatures,blockchainandanonymousmessagingstreams.*IEEETrans.Depend.SecureComput.*15,5(2018),840–852.https://doi.org/10.1109/TDSC.2016.2616861

[109] Lizhe Wang, Rajiv Ranjan, Jinjun Chen, and Boualem Benatallah. 2011. Cloud computing: Methodology, systems,andapplications.CRCPress. https://doi.org/10.1201/b11149

[110] Oracle.2017.Oracleblockchaincloudservice project. Retrievedfromhttps://cloud.oracle.com/blockchain.

[111] iEx.ec.2018.Retrievedfromhttps://iex.ec/.

[112] Jacobovitz, Ori. 2016. Blockchain for identity management. *The Lynne and William Frankel Center for ComputerScienceDepartmentofComputerScience.*Ben-GũrionUniversity,BeerSheva.Retrievedfromhttps://www.cs.bgu.ac.il/frankel/TechnicalReports/2016/16-02.pdf.

[113] Hassan Saad Alqahtani and Ghita Kouadri-Mostefaou. 2014. Multi-clouds mobile computing for the secure storageofdata.In*IEEE/ACM7thInternationalConferenceonUtilityandCloudComputing(UCC'14)*.IEEE.https://doi.org/10.1109/UCC.2014.68

[114] Jia Yu, Kui Ren, Cong Wang, and Vijay Varadharajan. 2015. Enabling cloud storage auditing with key-exposureresistance.*IEEETrans.Info.ForensicsSecur.*10,6(2015),1167–1179.https://doi.org/10.1109/TIFS.2015.2400425

[115] CongWang,ShermanS.M.Chow,QianWang,KuiRen,andWenjingLou.2013.Privacy-preservingpublicauditingforsecurecloudstorage.*IEEETrans.Comput.*62,2(2013),362–375.https://doi.org/10.1109/TC.2011.245

[116] Yannan Li, Yong Yu, Willy Susilo, Jianbing Ni, and Kim-Wang Raymand Choo. 2017. Fuzzy identity-based dataintegrityauditingforreliablecloudstoragesystems.*IEEETrans.Depend.SecureComput*.16,1(2017),72–83.https://doi.org/10.1109/TDSC.2017.2662216

[117] Yi-Sheng Su. 2017. Constructions of fractional repetition codes with flexible per-node storage and repetition de-gree. In *Proceedings of the IEEE Global Communications Conference (GLOBECOM'17)*. 1–6. https://doi.org/10.1109/GLOCOM.2017.8255008

[118] Pradip Kumar Sharma, Mu-Yen Chen, and Jong Hyuk Park. 2018. A software defined fog node based distributedblockchaincloudarchitectureforIoT.*IEEEAccess*.6,115–124.https://doi.org/10.1109/ACCESS.2017.2757955

[119] Anjia Yang, Jia Xu, Jian Weng, Jianying Zhou, and Duncan S. Wong. 2018. Lightweight and privacy-preservingdelegableproofsofstoragewithdatadynamicsincloudstorage.*IEEETrans.CloudCom*

put.

[120] LiehuangZhu,YuluWu,KekeGai,andKim-KwangRaymondChoo.2018.Controllableandtrustworthyblockchain-basedclouddatamanagement.*FutureGen.Comput.Syst*.91(2018),527–535.https://doi.org/10.1016/j.future.2018.09.019

[121] JingyiLi,JigangWu,LongChen,andJiaxingLi.2018.Deduplicationwithblockchainforsecurecloudstorage. In *ProceedingsoftheCCFConferenceonBigData.Springer*.https://doi.org/10.1007/978-981-13-2922-7_36

[122] RiponPatgiri,IraniAcharjamayum,andDhruwajitaDevi.2018.Blockchain:Ataleofpeer-to-peersecurity.In*Pro-ceedings of the IEEE Symposium Series on Computational Intelligence*. IEEE SSCI, 18–21. https://doi.org/10.1109/SSCI.2018.8628826

[123] JesseYli-Huumo,DeokyoonKo,SujinChoi,SooyongPark,andKariSmolander.2016.Whereiscurrentresearchonblockchaintechnology?—Asystematicreview.*PloSOne*11,10.https://doi.org/10.1371/journal.pone.0163477

[124] Roy,Shanto,MdAshaduzzaman,MehediHassan,andArnabRahmanChowdhury.2018.BlockchainforIoTsecurityand management: Current prospects, challenges and future directions. In *Proceedings of the 5th IEEE InternationalConferenceonNetworking,SystemsandSecurity(NSysS)*.1–9.https://doi.org/10.1109/NSysS.2018.8631365

[125] WilliamJ.Luther.2016.BitcoinandthefutureofdigitalpaymentsTheIndependentReview20,3(2016),397–404.https://www.jstor.org/stable/24562161.

[126] Trent J. MacDonald, Darcy W. E. Allen, and Jason Potts. 2016. Blockchains and the boundaries of self-organizedeconomies: Predictions for the future of banking. In *Banking Beyond Banks and Money*. Springer, 279–296. https://doi.org/10.1007/978-3-319-42448-4_14

[127] Liang,Xueping,SachinShetty,DeepakTosh,CharlesKamhoua,KevinKwiat,andLaurentNjilla.2017.Provchain:Ablockchain-baseddataprovenancearchitectureincloudenvironmentwithenhancedprivacyandavailability.In *Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*. 468–477.https://doi.org/10.1109/CCGRID.2017.8

[128] Walid Al-Saqaf and Nicolas Seidler. 2017. Blockchain technology for social impact: Opportunities and challengesahead.*J.CyberPolicy*.2,3(2017),338–354.https://doi.org/10.1080/23738871.2017.1400084

[129] Bayu Adhi Tama, Bruno Joachim Kweka, Youngho Park, and Kyung-Hyune Rhee. 2017. A critical review ofblockchainanditscurrentapplications.In*ProceedingsoftheInternationalConferenceonElectricalEngineeringandComputerScience(ICECOS'17)*.109–113.https://doi.org/10.1109/ICECOS.2017.8167115

[130] CharalamposAlexopoulosetal.2018.BlockChaintechnologiesingovernment3.0:Areview.EGOV-CeDEM-ePart.In*ProceedingsoftheInternationalConferenceEGOV-CeDEM-ePart,DanubeUniversityKrems,Austria*.Retrievedfromhttp://depts.washington.edu/egcdep18/documents/Virkar_et_al_2018.pdf.

[131] YanZhu,HongxinHu,Gail-JoonAhn,YujingHan,andShiminChen.2011.Collaborativeintegrityverificationinhy-brid clouds. In *Proceedings of the 7th International Conference on Collaborative Computing: Networking, Applications,andWorksharing(CollaborateCom'11)*.IEEE,191-200.

[132] AaronWrightandPrimaveraDeFilippi.2015.Decentralizedblockchaintechnologyandtheriseoflexcryptographia.

[133] Lin,Iuon-Chang,andTzu-ChunLiao.2017.Asurveyofblockchainsecurityissuesandchallenges.*Int.J.Netw.Secur.*

19, 5(2017), 653–659. https://doi.org/10.6633/IJNS.201709.19(5).01

[134] Yong Yuan and Fei-Yue Wang. 2016. Towards blockchain-based intelligent transportation systems, in intelligenttransportationsystems(ITSC).In*Proceedingsofthe19thInternationalConferenceonIEEE*,2663–2668.https://doi.org/10.1109/ITSC.2016.7795984

[135] Xiaoqi Li, Peng Jiang, Ting Chen, Xiapu Luo. 2017. A survey on the security of blockchain systems, *Future Gen.Comput.Syst*.107(2017),841–853.https://doi.org/10.1016/j.future.2017.08.020