BLOCKCHAINAPPLICATIONFOR MEDICALDOMAIN

Projectreportsubmittedinfulfillmentoftherequirementforthedegreeof
BachelorofTechnology
in

ComputerScienceEngineering
By

(ShubhamSingh (171305))
(ShashankShukla(171296))

Under the supervision

of(Dr. AmanSharma)

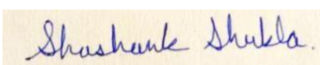
to

DepartmentofComputerScience&EngineeringandInformationTechnolog
y
Jaypee University of Information Technology Waknaghat, Solan-173234,HimachalPradesh

Candidate’sDeclaration

Iherebydeclarethattheworkpresentedinthisreportentitled**“BLOCKCHAINTECHNOLGYAPPLICATION FOR MEDICAL DOMAIN”**in fulfillment of the requirements for the awardof the degree of **Bachelor of Technology in Computer Science and Engineering** submitted inthedepartmentofComputerScience&EngineeringandInformationTechnology**,**JaypeeUniversity of Information Technology Waknaghat is an authentic record of my own work carriedoutoveraperiodfromFebruary2021toMay2021underthesupervisionof**Dr.AmanSharma(**AssistantProfessor(SG)ComputerScienceandEngineeringandInformationTechnology)Thematterembodiedinthereporthasnotbeensubmittedfortheawardofanyotherdegreeor diploma.

ShubhamSingh,171305



ShashankShukla,171296

This is to certify that the above statement made by the candidate is true to the best of myknowledge.

Dr. Aman
SharmaAssistantProfess
or(SG)
Computer Science and Engineering and Information
TechnologyDate: 17/05/2021.

ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to our teacher and mentor **Dr. AmanSharma** who gave us the golden opportunity to do this project on the topic **BLOCKCHAINTECHNOLGY APPLICATION FOR MEDICAL DOMAIN**, which also helped us in doing alot of research and we came to know about so many new things. And also thankful of taking ourweeklyreport on ourproject progress and helpedwith doubts.

Secondly, we would also like to thank Lab assistants who helped us a lot in finalizing this projectwithinthe limited time frame.

ShubhamSingh,171305

ShashankShukla,171296

ABSTRACT

As the Block chain Technology is around for long time now and it has provided us a way to shiftthe tide of traditional centralized system to the new better version of decentralization. And themostpopularversionofthatwehaveseenisthecryptocurrencytheBitcoinandethereumplatformfor the D apps. But now we are way past that now more research on the enterprise application orthebusiness related solution usingthe block chaintechnology.

So for the healthcare system data management we have many frameworks but this project is aapproach to design a methodology to bring out the theoretical model that we have come up withall the research and qualitative analysis on the hyper ledger and block chain application for theenterprise solution. As the traditional system exists and works well but it could be better with theupgraded one with which we tries to achieve transparency but also privacy at the same time, bykeepingallfunctionalandnon-functionalpropertiesandmaintainingtheauthentication,authorizationand the integrityat thesame time.

Dataandtheconsensus-basedmethod of capturing and updating it across distributed nodes arecritical in allowing trustless multi-party transactions in a blockchain-based environment. As aresult, correctly knowing whether and how data is stored and exploited essentially decides theutility,efficiency,andcostofablockchain-basedapplication.Althoughblockchainsimprovedataconsistencybyofferingan open, persistent,and consistentdata base, theplatform alsointroducesnewproblems in data management.

TABLEOFCONTENTS

1 INTRODUCTION 1
1.1 Introduction 1
1.1.1 Overviewof theBlock-chain 1
1.1.2 BlockchainApplicationsin healthcare 4
1.1.3 Dataset 4
1.2 Problem Statement 5
1.3 Objectives 6
1.3.1 Existingsystem 6
1.3.2 ProposedSystem 7
1.4 Methodology 9
1.5 Organization 10
1.5.1 Description 11
1.5.2 FeasibilityStudy 11
1.5.3 Implementationplan 17
2 LITERATURESURVEY 19
3 SYSTEMDEVELOPMENT 35
3.1 AnalysisandDesign 35
3.1.1 System Analysis 35
3.1.2 SystemDesign 36
3.2 ModelDevelopment 38
3.2.1 Analytical 38
4 PERFORMANCEANALYSIS 45
5 CONCLUSIONS 48
5.1 Conclusions 49
5.2 Future Scope 49
REFERENCES 50

LISTOFFIGURES

Fig1-1Feasibilityflowchart 12
Fig1-2StructureofBlock-chain 16
Fig1-3MerkleTree 16
Fig2-1Block-chainanditsmix 19
Fig2-2SymmetricCryptography 22
Fig2-3TruthTableofXOR 23
Fig2-4AESAlgorithm 24
Fig2-5Hashfunction 26
Fig2-6SHA-256construction 27
Fig2-7Bitcoinconsensusalgorithmpoints 29
Fig3-1SmartContractMechanism 37
Fig3-2Workflowwithsmartcontract 39
Fig3-3Smartcontractformedicaldomain 41
Fig3-4labresultsharing 42
Fig3-5communicationlinkbetweenusers 44
Fig3-6Healthcareframework 45
Fig3-7Workingofdataframework 46

1 INTRODUCTION

1.1 Introduction

1.1.1 OverviewoftheBlock-chain

Blockchain technology has recently emerged as a core technology in the digital transformation ofthe healthcare industry, and many academic studies have established blockchain opportunities forthe healthcare ecosystem. It is poised to disrupt the way existing medical services and companieshave operated in the healthcare industry for decades. ICTs and blockchain are important enablingtechnologiesforthedecentralisationanddigitalizationofhealthcareinstitutions,providingpatientsand service providers with a new and digitilized healthcare environment. Blockchain solutions forhealthcare data management include services to patients, physicians, and healthcare institutions intheareasofpatientinformationaccessandmonitoring,claimsandpaymentsmanagement,medicalIoT protection management , and research data authentication and sharing for financial auditingand accountability. Real-time modifications to an encrypted, anonymous blockchain database areperformedintheseapplicationstounderstand,track,andmanagemedicaldata.Whichalsomakesit easier for healthcare institutions to prevent unauthorised individuals from accessing classifiedinformation.

Ayear afterthepopularwhitepaperonBitcoinwaspublished,theBitcoincryptocurrencywasintroduced ,withthetechnologyreleasedasopensource,allowingotherstoadaptandbuildonitandconstructvariousgenerationsofblockchainbasedinnovations.Theinitialversionsofblockchainbasedcryptocurrency,suchasBitcoin,includethefirstwaveofblockchaintechnologies,oftenknownasblockchain1.0.Suchblockchain1.0applicationsinclude,tonameafew,Monero,Dash,andLitecoin.Theimplementationofsmartassetsanddigitalcontractsisalignedwiththesecondwaveofblockchaintechnology.Smartpropertiesareintangiblepropertiesorobjectswhoseownershipcanbegovernedbyablockchainbasednetwork,whilesmartcontractsaresoftwareapplicationsthatencodetherulesfor controllingandmanagingsmartproperties .Ethereum,EthereumClassic,NEO,andQTUMareexamplesofblockchain2.0cryptocurrencies.

Ethereum,EthereumClassic,NEO,andQTUMareexamplesofcryptocurrencies.Buildingontheabove,thethirdwaveofblockchaintechnologiesisnowfocusedonnonfinancialblockchainapplications.Tothatend,attemptshavebeenmadetoadaptthetechnologyoutsideofbanking,sothatothermarketsandusagecaseswillbenefitfromtheintriguingfeatures ofblockchain.Asaresult,blockchainisnowregardedasageneralpurposeplatformwithimplementationsinavariety ofmarketsandusecases,includingidentity protection,conflictsettlement,contractmanagement,supply chainmanagement,banking,andhealthcare,tonameafew.Withtheincreasinginterestinblockchainanditsimplementationinvariouscompaniesandsectors,healthcarehasemergedasasignificantfieldwhereavarietyofusecasesfor blockchainapplicationhave beenestablished.However,sinceblockchainisarelativelyyoung technology,andtherehasbeenalotofexcitementinthepressaswellasingrey mediainthe formofopinionpieces,commentaries,blogposts,interviews,andsoon,thereisalotofmisleadingfacts,speculations,anduncertaintiesaboutitspossibleutilityinthehealthcareindustry.

Members of the research community and clinicians like to learn the particular fields of use or usage cases of blockchain in the healthcare sector, as well as what blockchain based healthcare solutions have been created in response to these described use cases. What are the problems and drawbacksofblockchainbasedhealthcaresystems,howarethesechallengesbeingsolvednow,andwherewilltheybeimproved.

Manyproceduresareincludedinhealthcareadministration,suchasoverseeingbudgets,personnel,patients, regulatory disputes, logistics, inventory, and so on. Medical workflows also includeroutineprocessesrelatingtopatientcarethatcanbediagrammedasasequenceofconditionalsteps. These are intended to increase internal controls and quality, enforcement, and competitiveness, aswellasminimiserisk,tasktimes,andoverheadinhospitalsandotherhealthcareserviceproviders.Multiple patient workflows are built in this paper for various healthcare technology frameworkdomains.

Thispaperdescribesahealthcaresmartcontractstructureformanagingpatientdetailsandstreamlining complicated medical procedures. We addressed cutting-edge blockchain analysis inthe healthcare industry and introduced an ethereum-based healthcare management approach. Theaimofthispaperisalsotodemonstratethepracticalapplicationofblockchaininhealthcare,as wellastheobstaclesandpotentialdirectionsofblockchainscience.Onlyanalysisthatincorporatesa new healthcare approach, algorithm, process, technique, or design is included in this systematicstudy. Review analysis, discussions of possible uses and implementations, and other irrelevantpublications are not permitted. Using practical clinical databases, the paper then investigates theblockchain'sapplicabilitytothesehealthcareworkflowsaswellastheviability ofexistingblockchain implementation in various use cases. The following is how this article is structured:explains the history definition of blockchain technologies and analyses related job explains thepossible advantages of blockchain technologies System architecture and implementation waspresented. In, the cost assessment process and experiment outcomes are presented. The validationoftheworkflowswithactualhealthcaredatasetsisoutlinedinthehighlightsofthepaper'soveral ltopicand overview.Finally, the document comes to aclose.

Decentralization

DefinitionandDefinitionDecentralizationissoughtforanumberofpurposes,includingtechnological, political, and financial considerations. On the technical hand, it is often suggestedas a way of improving managerial and service delivery effectiveness. Decentralization is typicallyused in politics to expand municipal representation and sovereignty, redistribute authority, andreduce political tensions. Decentralization is used in finance to increase cost effectiveness, givemunicipalunitsmoreleverageoverservicesandtaxes,andsharpentransparency.Mills,Vaughan,S mith,andTabibzadehoutlinethemainstructuraldistinctionsbetweenfourtypesofdecentralisation.

DecentralizationintheHealthcaresector

Decentralizationhasbeenasignificantcomponentofperformanceenhancementeffortsasundertaken for strategic purposes. Decentralization, along with health finance restructuring, hasbeenapartofframeworkimprovementsinmanycountriesforatleastadecade.Incountrieswherethepr imarygoalofdecentralisationhasbeenpoliticalandfinancialgain,thehealthsystemhashadto devise coping mechanisms in order to sustain access and advance against health goals. Thebenefits of decentralisation include the development of leadership, the promotion of efficientoversight, management, and regulation, the generation of interest among workers, the promotionofrapid disposal ofjobs,and the lighteningof the upper echelons'workload.

1.1.2 BlockchainApplicationsinhealthcare

Legacyprogrammesusuallyonlysharehealthcareserviceswithinthemedicalandhealthcarefieldsandar eincompatiblewithexternalsystems.Nonetheless,datasuggeststhatcombiningthesenetworksforinteg ratedandimprovedhealthcarehasmultipleadvantages,necessitatinginterconnectionbetweendiversein stitutionsfor healthinformaticsresearchers.Oneofthemostpressingproblemsismultiorganizationalda tasharing,whichrequirespatientdatacollectedfromahealthcareprovidertobereadilyaccessibletoother institutionssuchasapractitionerorresearchinstitute.Blockchaintechnologyisredefiningdatamanage mentandgovernanceinmanyhealthcareapplications.Withadvancementsinelectronichealthrecords,cl ouddatastorage,andpatientdatasecuritylaws,newopportunitiesforhealthdataprocessingareopeningu p,aswellastheeaseforpatientstoviewandsharetheir healthdata.Ensuringdataprotection,storage,trans fers,andseamlessintegrationisextremelyimportanttoanydatadrivenenterprise,particularlyinhealthca re,whereblockchaintechnologyhastheabilitytosolvethesecriticalissuesinarigorousandefficientmann er.Thissectiondelvesintoblockchainbasedtechnologiessuchasdatatransfer,datamanagement,datasto rage,andEHR.

1.1.3 Dataset

Using actual healthcare datasets, we estimated the implementation cost using our existing smartcontract workflows. Figure 10 depicts ethereum blockchain transaction information. Section Acontains a summary of the datasets. The deployment cost is calculated and plotted for differentvariablesin sectionBusingactual datasets.

HSE datasets are culled from the various libraries. The Health Service Executive is in charge ofdelivering health and personal support care for all Irish citizens using public funds. Both outpatientandinpatientwaitinglistsfromvariousdepartments/hospitalsinIrelandisconsideredfor usei nthiswork.TheNationalTreatmentPurchaseFundmanagestheoutpatient,inpatient,andday case waiting lists from data collection to validation. The OP Waiting List survey shows the averagenumberofpatientswhoarewaitingfor afirstappointmentataconsultantledOutpatient clinic across all time bands. Each individual report consists of Each individual report includes the number of people waiting in each specialty at each hospital. To maintain individual anonymity,ifthereare5patientswaitinginacertainspecialty/hospital,thefigureshavebeenaggregatedu ndertheheading‘SmallVolume.'Theentirestudyismadeupofdatacollectedonamonthlybasisoverthec ourseofayear.

Whenitcomestodeployinghealthcareblockchain,thecostofincorporatingsmartcontractsforhealthcar emustbemeasured.Theendaimistoputinplaceaframeworkthatwillprovideall of the benefits of blockchain to a viable medical health system. To prevent network manipulation and to address other computational problems, all programmable calculations on the Ethereum blockchain incur a tax. As a result, all processes, computations, message calls, smart contractcreation/deployment,andstorageonEVMnecessitatetheuseofgas.

Thecostofdeployingsmartcontractsforhealthcaremanagementsystemshasbeencalculated.Thecostof runninganoperationontheEthereumnetworkisknownasGas.Toruntheservice,alltransactionsneed21, 000gallonsofpetrol.WhenauserinteractswithanEthereumsmartcontract,itrequires21,000electricity, withextragasrequiredforthesmartcontracttooperate.Thegashasbeencompiledformedicalsmartcontr actsforcontractdeploymentandcooperationwithother contracts.Themorecomplicatedthefunctions/o perationsinvolvedinsmartcontracts,themoregasisused,resultinginahigherfee.Fromthestandpointofv iability,itisobviousfromThemorecomplicatedthefunctions/operationsinvolvedinsmartcontracts,the moregasisused,resultinginahigherfee.Intermsofviability,thefindingsshowthatthecostofdeployingas martcontractforahealthcaremanagementsystemisverylimited.Intermsofthemedicalsystem,thispay mentisverylow,andeveryonewillbewillingtopaythissmallamountinordertohaveleverageovertheirE HRandkeeptheirmedicalrecordsfortherestoftheirlives.playsthecostofsmartcontractimplementation foreachpharmacyasmeasuredbyourframework.

1.2 ProblemStatement

Given these difficulties, we think it is necessary to investigate the use of a blockchain as a datastore in the field of data management. A thorough understanding of blockchains in terms of howdataisprocessedandhandledcanhelpprogrammedevelopersanddatabasemanagersproperly planandmaintainacomplexcomputinginfrastructurethatcouldhaveablockchainandanauxiliarydatabase. It can also prevent suboptimal architectures, glitches, and vulnerabilities as a result ofunreasonableexpectations about how blockchainswill behave.

Inotherworks,blockchainhasbeenbrieflycomparedtodatabasesintermsoffeaturesandspecialproperties. Our analysis complements these activities by better conceptualising the differences. Inother works, blockchain has been briefly compared to databases in terms of features and specialproperties. Our analysis supplements these activities by further conceptualising the discrepanciesbasedon how programmedevelopers willnormallyviewtheinformation frameworklayers.

1.3 Objectives

- Toinvestigatethevariousfacetsof Blockchain.
- ToinvestigatetheeffectofBlockchainonvarious industries.
- ToinvestigatetheimpactofBlockchainonvariousindustries.
- Tostudytheeffects ofBlockchain onvarious industries.
- Toinvestigatethelong-termimpactofdemonetizationonaneconomy.
- ToinvestigatehowtheBlockchaindefinitioncan benefita government.

1.3.1 Existingsystem

Centralizedsystem:

Ratherthan youmightthink,centralizationcirclesaroundus.When youusesocialmediasiteslikeFacebook, you are using a centralised structure. Other popular online channels, such as YouTube,arecentralisedas well.

Trust

Whilecentralisedinstitutionsaresafeandtrustworthy,theyarenotfullysecureortrustworthy.Thetrustisa contractbetweentheserviceproviderandthecustomer.However,itisadeal,andthatisquickly broken.Fromtimetotime,largecompaniesfaceconfidenceproblemswiththeircustomers.Whenthereis asecuritybreachinthesystem,customerschoosetoneglecttheserviceforaperiodof timeuntiltheservice providerrestoresfaithbyprovidingremediesandremunerationtothoseaffected.Muchof whichoccursa saresultof centralizationandthefactthatalldataisstoredinasinglearchive.

Singlepointoffailure

Centralizationalsoimpliesthatthewholenetworkisvulnerabletoasinglepointoffailure.Organizationsa reawareofthedownsideandhavetakenstepstomitigateit.However,thepossibility oflossisasignificant drawbackformission-criticalservices.

ScalabilityLimitation

Sinceasingleserverisusedinmostsituations,scalabilityislimited.Unquestionably,centralizationis an efficient method of managing organisations or networks. It has been successfully used bylargecorporationssuchasMicrosoft,Facebook,andYahoo.Inreality,ourgovernmentsdependonacen tralised approach aswell.

Security

The elected executives coordinate authority in the case of a centralised government. You can alsousethepowerindifferentsituations.Centralizationguaranteesthesecurityofalargecorporation'srec ords.Thisisneededtoensurethattheirtradesecretsarenotleaked.However,thereisamodifiedmethod of managing data that includes the possibility of using decentralised networks such asblockchain.Wecanquicklyconcludethatcentralizationisstillverydominantintoday'seconomy.Furth ermore, not all companies would accept decentralisation just for the sake of it. Differentmarketmodelssucceedincentralisednetworks,anditwilltakesometimebeforemorebusinesse smoveto decentralised models.

1.3.2 ProposedSystem:

De-centralizedsystem

Decentralization is a novel concept. It became public after the release of bitcoin in 2009. It alsolaunched a new cool idea that allows for decentralisation, namely blockchain technology. Whenonepersontransfersbitcointoanother,thetransactionisnotroutedthroughacentralisedauthority.T hisdoesnot,however,implythatthetransactionhasnotbeenchecked.Consensusalgorithmsareusedtova lidatethetransactions.Anyonewillconnecttothenetworkusedforbitcoin.Thatmeansit'saccessible.Itals odemonstratedotherimportantcharacteristics,suchasopenness,whichallows everyone to check transactions if necessary. A entity or computer that connects to the network isreferredtoasa"node"insuchanetwork.Eventually,therewillbeanetworkofthousandsofnodescapable of transferringand collectingfunds from oneanother.

Let's look at a real-world situation to better appreciate the definition. A decentralised energynetworkisanetworkthroughwhichindividualscanlinkandpurchaseenergyfromotherindependent entries. They don't have to pay the intermediaries to gain electricity in the first placethisway.Thedistributedenergynetworkisbasedonblockchaintechnologiesanddoesnotrequirea centralised authority. The nodes that generate the energy will distribute it to the network and becompensatedfor it.

CompleteCommand

One of the most important benefits of decentralisation is that consumers have complete autonomyover their transactions. This means they can initiate a contract wherever they choose, rather thanwaiting forauthorizationfromacentralisedauthority.Inlayman'sterms,theauthenticationmechanismisnotreliantonoutsideactors,andadecentralisednetworkusesconsensusmechanismsto validatedata.

Immutabilityof thedata

Blockchain technology's data structure is append only. This means that there is no chance foranyonetomodifyoralter thedataonceitisstored.Thereisanotherblockchaintechnologythatutilizes differentdatamodelssuchasCorda,buttheyalsofollowtheimmutabilityproperty.

Ensure

Becauseofhowthey processdataandtransfers,decentralisednetworksaresafe.They usecryptographytomaintainthesecurityofthedataledgers.Furthermore,thedatainthecurrentblockrequiresdatafrom theneighbouringblock in order to verifythe datausingcryptography.

Censorship

Censorship is often reduced as a result of decentralisation. In a bureaucratic structure, there is agreaterpossibilitythattransparencymaybecensored.However,sincethereisnosingleauthority controllingthedata,thedecentralisednetworkislesssusceptibletocensorship.Let'slookatacaseto better explain the situation. Twitter, for example, is known to delete accounts as it detectsinappropriate tweets or when the government attempts to censor accounts if it contradicts theirpolicy. In the case of decentralisation, peers may communicate directly, resulting in little orminimalcensorship.

1.4 Methodology

The general approach for the creation of a system involves multiple steps that define the life cyclerepresentationoftheproposedforthedevelopmentofasoftwareproject.Notonlydoesthetheoryinv olve forward momentum, but it should also return to an operation that is cycled over to apreviouslyperformed activity.Thisreturnorinputloopmayariseasaresultofafailuretoreachasuccessgoalforthesystemorasaresultofimprovementsintheredefinitionofsystemoperations.The development process of the computer-based system often experiences distinct stages, as withmostsystems.

1. Researchdesign:

My research design will be informative followed by partly exploratory and the whole project willbe based on data gathered from the internet, publications, articles, and analysis, so the project willhave a thorough and concise overview, so there is a combination of interpretation and descriptiondesign.Itwillincludeallofthemainaspectsof Blockchainandwillprovidethereaderwithabett erunderstandingof how itworks.

2. Sourceofdata:

The primary source of information in my project would be secondary data from the internet, suchas facts, statistics, and diagrams, which will be analysed and compiled in the form of this projectpaper.

3. Scopeofresearch:

My project topic is primarily related to industry, banking, and finance. The research's key goal istoraise publicawareness about blockchainand itsapplications in variousindustries.

LimitationsoftheStudy:

- Thesecondarydatagatheredmayhavebeenmanipulated,resultinginabiassedoutcome.•Inexperiencein draftingtheproject study.
- Inadequatetimetocompletethejob.
- Theprocessisnotadaptable.Theoutcomecandeviateifthereisinsufficientorincompleteknowledge.
- It is extremelydifficult to verifythe authenticityof thedata presented.
- Documents may lack authenticity; for example, portions of the document may be absent, and wemaynotevenbeabletovalidatethedocument, whichmeanswecannot determineifitisskewedor not.
- Sincethewayitemsaremeasuredcanvaryovertime,statisticalmeasurementscanbecomplicated.
- As a project report, the scope of study is broad and might not be sufficient to impose anylimitations.

4. CodingPhase:

The coding phase is for translating the design of the system produced during the design phaseinto code in a given programming language, which can be executed by a computer and whichperformsthecomputationspecifiedbythedesign.

5. TestingPhase:

Testing is conducted in different forms, such as algorithm testing, computer code; sample dataanalysisis also one of thetests above.

1.5 Organization

Variousmedicalworkflowsinvolvingvariousmedicaltreatmentshavebeendevelopedandappliedusing theblockchainsmartcontracttechnology.Thisinvolvesissuingsimplemedicalprescriptionsforthetreatmentofcomplexillnessesandtheirprocedures,suchastreatmentproceduresfor surgicalpatients.Theaimofdevelopingthesemedicalsmartcontractsistohelppatients,physicians, and healthcare organisations solve logistical inefficiencies. This method would aid intheretrieval, examination,and maintenanceof complexmedicaldataandprocedures.

1.5.1 Description:

TheMedicalPrescriptionIssuanceandFulfillmentProcedureTheprimaryaimistostreamlinethemedical drug handlingprocessbyminimisinglengthywaittimes,eliminatingbriberyfromthesystem,andloweri ngtheerrorratecausedbydoctormisinterpretations.Adoctorsignsaprescriptionfor apatientandaddsit to thepatient'smedicalhistory using asmartcontract.Thepharmacy thengainsaccesstothismedicationthr oughtheEthereumblockchainsmartcontract,thankstoapprovalgivenbytheprimarydoctorandthecusto mer.Afteraccessingthedrug,thepharmacyissuesthemedicationwiththeexpirydateanddoseusageposte dontothepatient'shealthcarerecordsthroughsmartcontracts,andthemedicineisthenavailableforthepati enttoreceive.Ingeneral,smartcontractfeaturescoordinatemedicationsatisfactionamong doctorsanddr ugstores.Following apatient'sappointment,doctorsdevotelittletimeexplainingmedicationordersor sp eakingwithpharmacyshopsingeneral.Thepatient,primary doctor (GP),andpharmacyareallincludedin thedataflowforadministeringamedicalprescription.Italsoincludes prescriptioninformationsuchasme dicineid,expirydate,patientid,andsoon.

1.5.2 FeasibilityStudy:

Ansignificantstepintheprocessofapplicationdevelopmentisthefeasibilityanalysis.Ithelpsthemanufac turer to provide an evaluation of the software being produced Refers to the product'sfeasibility analysisisintermsof theproduct'sresults,the practicaluseandthe technologicalassistanceneeded for its implementation.

This segment contains the findings of our survey on the viability of using blockchain technologiesin evoting applications. When we talk about viability, we mean a device that is cost-effective,flexible,stable,andsimpletoimplement(orsubsystem).Thoughdetermininggloballmeasurem entsofthesepropertiesisdifficult,wehavefoundcertainthresholdsorvariablestodecideifitisfeasibletosu bstitutecurrent(andprospective)systemswithblockchain-
basedequivalents.Anyblockchainbasedapproachshouldbe(noticeably)lessexpensivethanthealternat ives.Long-term

conventional campaigns, say over a three-year cycle of at least one referendum each year. It couldnot be done. neither more costly nor less expensive than non-blockchain implementations. Basedonthesizeofthedevice, itshouldbeabletoaccommodatemillionsofindividuals.state,companysize, or demographic focus group The standard of protection should not be smaller than that ofnonblockchainsolutions.Informationonprotectionspecificationsareincludedlaterinthedocument.

BlockchainFundamentals

Bydefinition,blockchaincannotbeextendedtoallapplicationsasamodularoff-the-shelfsolution.The flowchart of viability that explains why a blockchain database is useful. This diagram is acondensed version of the flowchart . If blockchain isn't effective or appropriate for a project, itwon'tbefeasible.Wherethefollowingcharacteristicsarepresentinlegacytopicschemes,blockchainsolutions are appropriate.

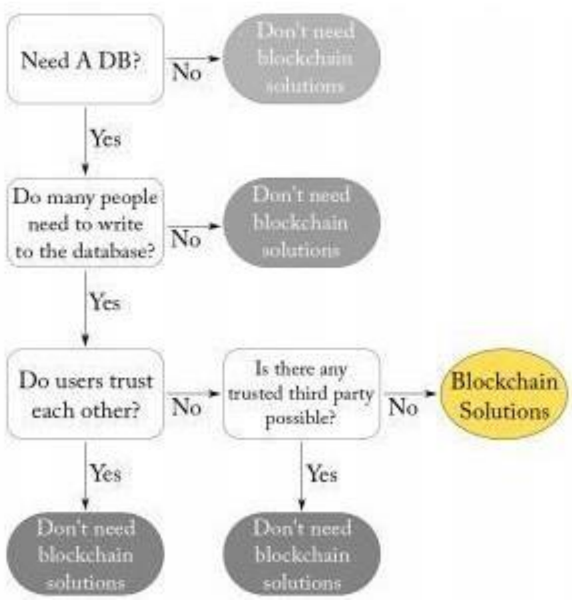


Fig1-1Feasibilityflowchart

- Wherethereiscodedinformationthatcanbeexchangedbetweenpeople,thisisreferredtoasshared data.
- Multipleparties: Wheremorethanoneperson is requiredto read or writedata,
- Lowtrust:Whenthereisnoassumedcompletetrustbetweensystemmembers,

- There is no trusted third party: If it is unavailable or unfavourable due to deploymentchallengesor prices,
- Auditability:Ifwewishthedatatobeunchangeable,wemustensurethattheyareauditable(notto bechanged or deleted after recording).

1- Blockchainofferings

- Disintermediation:Transactionsarenotcheckedbyacentralisedcentralgatekeeper,whichmay minimisethecostsofconstructingandmaintainingnetworksandmayresultincertainefficiencyb enefits.
- Transaction interaction: Smart contracts can be used to execute complex and intertwinedtransactions.The blockchain framework offers a simple and scalable foundation for publickeyinfrastructures and blind signatures.
- Auditability: Any record in blockchain keeps track of who is participating in transactions,aswell as the form, number, and valueof thematerial.
- Completeconfidence,sothattheelectionshouldnotbeunderanyone'sinfluence.Itshouldbeensu redthattheelectionresultscannotbedistortedandthattherewouldbenoinconsistencybetween the documents of various intermediatestructures, ifanyexist.
- Transparency greater than legacy internet networks (as well as traditional elections). Mostblockchain applications provide for the listing of all transactions, with a substance and atimestamp, but without exposing the parties concerned. It is also possible to temporarilymask the content. As a result, all casted ballots can be listed in real time, and all votes canbe tallied by each of the observers while preserving the voters' privacy. Additionally, aftercastingtheir ballots, electors havetheright to validatetheir votes.
- Costcutsasaresultoflessdemandsforcostlyserversorcomputers,aswellasopensourceapplicati ons.
- Remote elections, also known as remote absentee voting. If required, it would aid in theturnout rates and make voting more affordable for voters. This is preferable, especially forcompaniesand non-profit organisations.
- Vote histories that are immutable and unchangeable. After the voting is over, no one, notevenmachinetechniciansoroperators,shouldbeabletocontrolthevotes.Duringthe

voting, the ability to update votes could be offered. This can be done in conjunction with aconsensusprotocol.

2- SocialAspects

Applicationssurroundinge-votingandBlockchaintechnologieshavesignificantsocietalimplications.Theseeffectscanbefurtherclassifiedasthemeaningderived fromthegiveneaseofuseandpeople'sperceptionsofconfidenceintheseso-called"hitech"systems.Ingeneral,eGovernment services provided people with broader, quicker, and faster access to governmentservices,especiallythoselivingin rural settlements and thosewho areverybusyand/or mobile.

As a result, it can be seen as a strong instrument that strengthens government citizen partnerships.WhiletheeGovernmentitselfisnotdirectlyrelatedtothedemocracy,theconceptofevoting extendstheeGovernmenttoprovidemeansofdemocracy,callede Democracy.Theeaseof use and financial advantages of such e services are no longer in question, but the sense of confidence, a newer problem brought on by e democracy services, could be overshadowing thesebenefits when it comes to e voting. Independent of the subject and theme, if the majority of electorsdonottrustthecurrentevotingscheme,itshouldnotbeapprovedasthesolemethodofvoting.Thisissoeventhoughtheconcernsarecompletelyfalseandunfounded,oriftheyaretheresultofaplot.

Theuseofblockchaintechnology,whichisusedinthefamouscryptocurrencyBitcoin(andmanyothers),canreinforcetheperceptionoftrust,sinceBitcoinandothercryptocurrencytransactionsarecommonlyconsideredtoprovidetrusttotransactions,includingbetweenuntrustworthyparties,aslongasusersareaware ofcertainsecuritycountermeasures.Ifthesoftwareisopensource(andbetterifitislicencedunderafreesoftwarelicence),publicopinionandconfidencewouldbeevenstronger.Sinceopensourcecodemaybeexaminedbyanyonewhowishestocontributetotheproject(likeinEstonia).Insuchascenario,evenmaliciousindividualsunwittinglyaidinthedevelopmentoftheframework.

3- FinancialAspects

Using digital electronic services, such as online portals and smartphone apps, would undoubtedlyreduceoperatingcostsinthelongrun,consideringtheirhigherinitialinvestmentcosts.Apre viousreport comparing the technology and maintenance costs of conventional and electronic electionswas recently released. According to the report, the benefits of converting to an online votingschemecouldresultinsavingsofuptomanytimesayear.Thedisparitybecomesmorepronounced, particularlyif therearetwo ormoreelections in agivenyear.

AnotherstudyinEstoniaexaminestheexpensefromtheperspectiveoftheelectorate.Thisresearchshowst hatvoterswholiveatleast30minutesawayfromtheirpollingplacesfacehigher(timeandmoney) costs andaretherefore morelikelyto choosevotingonline.However, astheypointedout,elderlypeople'saversionof usingmachinesremains underappreciated.

Standard system expenses are mostly comprised of content, staff, and logistical costs. However,the expense of health-care systems covers the costs of software production, hardware resources,and associated maintenance. Since several blockchain packages are open-source initiatives withcustomised APIs, using blockchain-based technologies can alsoreducethese software costs.Furthermore, combining a blockchain-based healh-care system with a cryptocurrency-paymentsystemcan provide different setups and opportunities.

4- Securityand Reliability

compares the authentication features provided by blockchain to those provided by other databasesolutions. The system's availability and fault tolerance are high because all nodes hold a copy ofthe records and search each other to provide a reliable system. The blockchain allows for bothtransparencyand secrecy. Privacyis not intended,but it can beapplied.

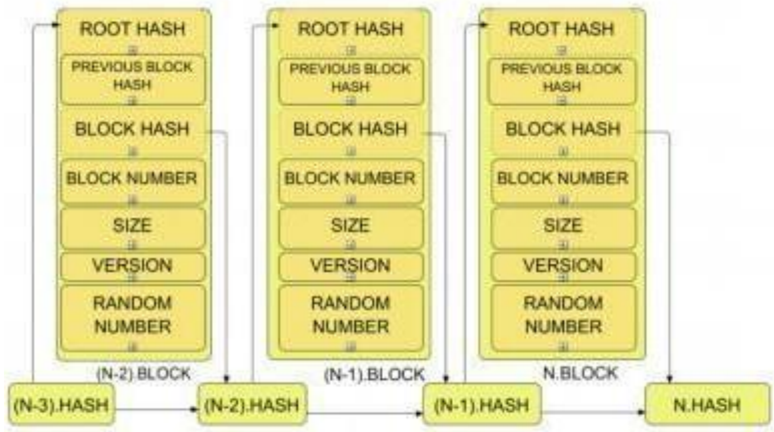


Fig1-2StructureofBlock-chain

TheMerkletreeisused toensuretheaccuracyof thedocuments. Figure3 depictsitscomposition.Eachblockcontainsseveraltransactions.Tobegin,thehashvaluesofeachtransactionareextractedand compared to the hash of the other transaction. Pairs of hashes are then merged until a singleroothash is obtained. This arrangementmakes it simple to verifytransactions.

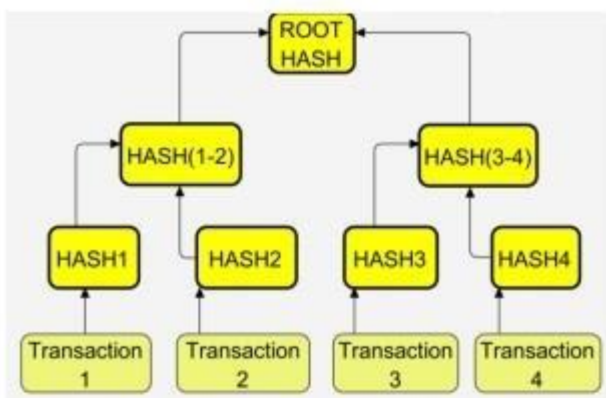


Fig1-3MerkleTree

Whileblockchain-basednetworksaresaidtoholdpermanentrecords,thereisacomplicatedwaytochangetherecords(blocks)thatishandledbytheconsensusprotocols.Asaresult,thesystem'sdependabilityisdeterminedbytheconsensusprotocolused.Theconsensusprotocols(PoW,PoS,andsoon)arethelawsthatgovernwhichnodehastheauthoritytowritetotheblockchain.Bitcoinandminingdrivenblockchainapplicationsmostlyusethe PoW(ProofofWork)algorithm,whichisbasedoncomputationalcapacity.Anyonewhowishestochangeablockshouldchangeitaswellasthesubsequent(next)blocksintheblockchain.Forexample,ina1000blockchain

,Ifauser(orattacker)wishestochange(only)the100thblock,heorshemustchangeallblocksbeginningwiththe100th.untilthe1000thFor anyblock,theattacker(node/computer)should get the writing turn, and in PoW, this requires that It should have at least 51% of the totalprocessingpowergivenby (thenumberof)allthenodesbelongingtothecluster.Thisattackis technically feasible, particularly in small networks, but since all transaction information are registeredinallcopiesoftheblockchain,any maliciousbehaviourwouldbeveryeasytodetect ;additionally,thisnegativeeffectcanbemitigatedquicklybecauseitisnotdifficulttoexcludeanodefrom thenetwork.achain.

1.5.3 Implementationplan:

The primary approach for system improvement is to migrate from the existing system to theproposedsystem. Thenew system hasbeen largelyrevisedto fourproposed approaches.

- Phase-inMethod
- DirectCut-OverSystem
- ParallelRunSystem
- PilotSystem

Parallel Run System: That is the simplest method of converting an old unit to a new one. In thisapproach,alldevicesrunsimultaneouslyforasetperiodoftime.Ifmajorproblemsarediscoveredwhen using the current system, the new system is scrapped and the older system is restarted fromthebeginning.

DirectCut-OverMethod: Inoneareaoftheenterprise,aworkingimplementationofthesystem,such as a single work environment or a single department, is implemented. When the installationisdeemedcomplete,itisinstalledeitherallatonce(directcutting)orgraduallyintheorganisation(phase-in).

Phase-inMethod: Thisstrategybeginsbyimplementingaportionofthearchitectureandgraduallyaddsother components.

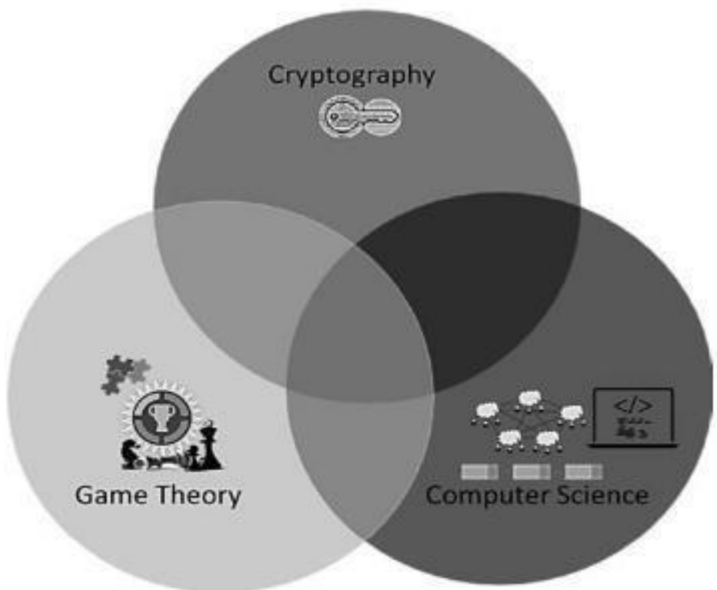
Implementationplanedused: Theprocessmanagementarchitectureisbasedaroundthe"Concurrent Run Method," and we have revised the structure to meet the customer's needs. Theoperationalsystemisreferredto astheoldsystem,andthenewsystemisbasedontheoldsystem, withtheprinciplesprocessedbytheoldersystemretained.Theimprovedmethodworkswellandiseffectiv elyimplemented on thecustomer. For theapplicant's recruitment.

2LITERATURESURVEY

CompositionsofBlockchain

Creating a Blockchain Foundation Blockchain is more than just a technology; it is also linked toenterprisefunctionsandusecases.Itisalsointertwinedwitheconomicvaluesthroughitsblockchain implementations. This segment would mostly concentrate on the scientific aspects.Blockchain is a genius synthesis of ideas from cryptography, game theory, and computer scienceengineering.

Fig2-1Block-chainanditsmix



Let's take a high-level look at the roles these elements perform in the blockchain structure beforedelving further into the basics. Before we get there, let's take a brief look at how conventionalunified systems worked. The standard approach called for a single organisation to keep only onetransaction/modificationhistory.Thegoalwastoexertconcurrencycontrolovertheentiredatabasean d instil confidence in the system through intermediaries. So, what was the issue with such asecure system? A unified structure must be trusted, regardless of whether those concerned aretruthful or not! Often, for obvious reasons, the cost of intermediaries and transaction time can behigher. Consider power centralization; gaining complete oversight of the whole structure allowsthecentralisedauthorities to do about whatever theywish.

Letusnowexaminehowblockchaintacklestheseproblemscausedbycentralisedintermediariesbytheus eofcryptography,gametheory,andcomputer scienceprinciples.Regardlessoftheusecase,cryptograph yisusedtoencryptthetransactions.Cryptographyensuresthatalegitimatepersoninitiatesthetransaction andthatnoonecancounterfeitafaketransaction.ThisensuresthatAlicecannot,cryptographically,make atransactiononbehalfofBobbyforginghissignature.Whatifanodeor ausertriestolaunchadoublespend attack?Keepinmindthatevenifonedoesnothaveenoughfunds,onecanstillinitiateadoublespendattack, whichiscryptographicallycorrect.Theonlywaytoavoiddoublespendisforeachnodetobeawareofalltra nsactions.Thisraisesanotherintriguingproblem.Howwilltheyallconvergeonashareddatabasestateife achnodeisresponsibleformaintainingthetransactiondatabase?Again,howcanthesystemremainresilie nttocircumstancesinwhichoneor morecomputingnodesactivelythreatentosubvertthesystemandinse rtabogusdatabasestate?ThemajorityofsuchissuesfallunderthepurviewoftheByzantineGenerals'Dile mma(describedlater).Ithasgrowninpopularityasaresultofblockchain,butithasbeenaroundforalongti me.Asitcomestodatacentreordistributeddatabasesolutions,theByzantineGenerals'Dilemmaisanobvi ousandwidespreadonethattheymustcontendwithinordertostayfaulttolerant.Suchconditionsandtheirr esolutionsarederivedfromgametheory.Gametheoryoffersafundamentallydifferentapproachtodeter mininghowamechanismcanbehave.Gametheoryapproachesarearguablythemostsophisticatedandpr actical.Theynormallymaynotconsiderwhetheranodeistrustworthy,dishonest,ethical,orhasanyothers uchcharacteristics,andtheyconcludethatparticipantsbehavebasedonthebenefittheyget,notonmoralpr inciples.Theprimegoalofgametheoryinblockchainistoensurethatthemechanismisstable(i.e.,inNash Equilibrium)andthattheplayersareinagreement.

There are many types of market challenges and circumstances, each of differing degrees of complication. As a result, the underlying crypto and game theoretic consensus protocols can varydependingontheusecase.Thebasicconceptofkeepingareliablerecordor ledgerofchecked transactions, though, remains the same. Though the principles of cryptography andgame theoryhavebeenaroundforalongtime,itiscomputersciencethatconnectsthedotsthroughdat astructuresandpeertopeernetworknetworkingtechniques.Clearly,“smartsoftwareengineering”isneed edtounderstandcertainconceptualormathematicalprinciplesinthemodernworl d.Thecomputerscienceengineeringtechniquesthatembedcryptographyandgametheoreticprinciplesi ntoanapplication,allowingdecentralisedanddistributedcomputationamongnodeswithdatastructurea ndnetworkcommunicationcomponents,arethenused.

Cryptography

Themostcriticalaspectofblockchainiscryptography.Itisunquestionablyascientificareainandofitself,f ocusingonsophisticatedmathematicalmethodsthatareverydifficulttocomprehend.Inthis section, we will try to establish a solid understanding of some of the cryptographic principles,since different problems can necessitate different cryptographic solutions; one size never fits all.You may miss any of the information or refer to them as appropriate, but it is the most criticalcomponent for ensuring system security. Many attacks on wallets and exchanges have beenidentifiedas aresult ofbad architectureor cryptographicimplementation.

Cryptography has existed for over two thousand years. It is the science of keeping informationprivate with the use of encryption techniques. However, secrecy isn't the only goal. There are avariety of other applications for cryptography, which are mentioned below and will be discussedfurther:

- Confidentiality: The message should only be understood by the intended or approvedreceiver.That is also known asconfidentialityor anonymity.
- Data Integrity: Data cannot be forged or changed knowingly or unintentionally by anattacker or by unintended/accidental mistakes. Though data integrity cannot preclude datafrombeingaltered, itcanprovide awayof determiningifthedata hasbeenaltered.
- Authentication:Thesender's legitimacyis guaranteed and verifiablebythe recipient.
- Non-repudiation: After receiving a letter, the sender cannot later dispute that they receivedthemessage.Thisensuresthatanindividual(apersonorasystem)cannotcontinuetoacce ptresponsibilityforapriorpromise oraction.

Plaintextreferstoanymaterialintheformofatextmessage,numericalstatistics,oracomputer programme. The idea is to encrypt the plaintext using an encryption algorithm and a key, resultingintheciphertext.Theciphertextisthensenttotheintendedreceiver,whodecryptsitwiththedecry ptionalgorithmandkey toobtaintheplaintext.

SymmetricKeyCryptography

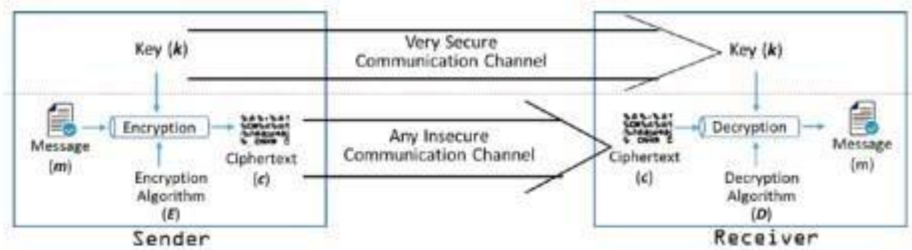


Fig2-2SymmetricCryptography

Symmetrickey cryptographyiscommonlyused;themostpopular applicationsaresecurefiletransfer pr otocols like HTTPS, SFTP, and WebDAVS. Where the data size is large, symmetric cryptosystemsaretypicallyfasterandmoreuseful.Pleasekeepinmindthatsymmetrickeycryptographyc omesintwoflavours:streamcyphersandblockcyphers.Wewilladdressthisinthefollowingpages,butfirs twewilllookatKerchoff'stheoremandtheXORfunctiontoexplainhowcryptosystemsoperate.

XORFunction

Kerckhoff's theorem states that a cryptosystem should be stable even though anything about the scheme except the key is widely available. Furthermore, the general belief is that the message transmitting mediumisneverstableandthatmessagescanbequicklyinterceptedduringtransmissio n.Thismeansthateventhoughthe encryptionalgorithmEanddecryptionalgorithmDare stillpublic,andthereisapossibilitythatthemessagewillbeintercepteddduring transmission,themessage willstillbesecureduetoa sharedsecret.Asa result,ina symmetriccryptosystem,thekeysmustbe kepthidden.TheXORfunctionisthe foundationof manyencryptionanddecryptionalgorithms. .Let'stakea lookatitandsee if itfacilitatescryptography.The XOR,alsoknown as“Exclusive OR,”isrepresentedbythesymbol.

A	B	A ⊕ B
0	0	0
1	0	1
0	1	1
1	1	0

Fig2-3TruthTableofXOR

StreamCiphersvs. BlockCipher

The way plaintext is encoded and decoded differs between stream cypher and block cypheralgorithms. Stream cyphers translate one plaintext symbol to one ciphertext symbol. This ensuresthatencryptionisperformedonebitorbyteofplaintextatatime.Inabitbybitencryptionsituation,a separatekeyiscreatedandusedtoencrypteachbitofplaintext.Asaresult,itemploysaninfinitestream of pseudorandom bits as the key and employs the XOR operation with plaintext input bitsto produce ciphertext. To keep such a device stable, the pseudorandom keystream generator mustbe both secure and unpredictable. Stream cyphers are a close approximation to an establishedcompletecypher knownas "the one-timepad,"which wewill exploreina moment.

Blockcypher,onthe other hand,isbasedontheconceptofdividingtheplaintextintocomparativelylarger blocksoffixedlengthgroupsofbitsandencodingeachoftheblocksindependentlyusingthe samekey.Itis adeterministicalgorithmwithaconstanttransformationthatemploysthesymmetrickey.Thisimpliestha tencryptingthesameplaintextblockwiththesamekeywouldyieldthesameresult.

Eachblockisusually64bits,128bits,or256bitsinlength,andthecorrespondingciphertextblocksare all of the same block length. We choose, say, an r-bit key k to encrypt any block of length n,and note that the permutations of the key k are limited to a very small subset of 2r. This suggeststhattheconceptofa“perfect cypher”doesnotexistin thiscase.Nonetheless,randomselection oftherbitssecret keyis significant,sincemorerandomness impliesgreaterconfidentiality.

AdvancedEncryptionStandard

The AES algorithm, like DES, is a symmetric block cypher that does not use a Feistel network. Ina broader context, the AES employs a substitution-permutation network. It not only providesincreased protection, but it also provides increased speed! According to AES specifications, theblock size is set at 128 bits, and there are three main sizes available: 128 bits, 192 bits, and 256bits. AES is known by various names depending on the key used: AES-128, AES-192, andAES256.

The number of encryption rounds in AES is determined by the key length. There are ten rounds inAES-128,twelveroundsinAES-192,andfourteenroundsinAES-256.Ourdiscussioninthissection,is.restrictedtomainlength128(i.e.,AES128)sincethemechanismisalmostidenticalforotherAESvariants.Theonlydifferenceisthe"maintimetable,"whichwewilldiscusslaterinthissegment.UnlikeDES,AESencryptionroundsareiterative,witheachroundencryptinganentire128bitdatacube.Inaddition,unlikeDES,thedecryptionprocessinAESisnotveryclosetotheencryptionprocess.

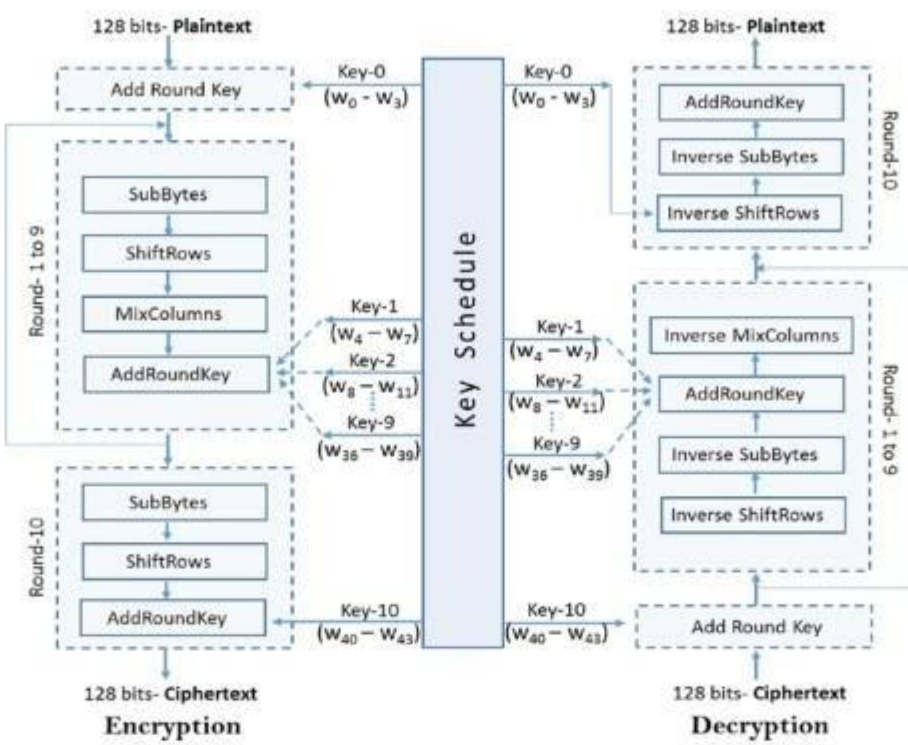


Fig2-4 AESAlgorithm

You'vealreadyfoundthatthedecryptionmechanismisn'tjusttheinverseofencryption.Theproceduresin theroundsarecarried out in arandomorder! SubBytes,ShiftRows,MixColumns,andAddRoundKey areallinvertiblemeasuresintheroundfeature.It'salsoworthnotingthattheroundsareiterativein nature. Rounds 1 through 9 have all four processes, with the final round excluding only the“MixColumns”operation.Letusnowconstructahigh-levelunderstandingofeachprocessthatoccursin around feature.

ChallengesinSymmetricKeyCryptography

Symmetrickeycryptographyhasseveral drawbacks.Amongthemarethefollowing:

- Before any contact can take place, the sender and recipient must exchange the key. Itnecessitates the useof asafekeyestablishment mechanism.
- Sincetheyusethesamesymmetrickey,thesenderandrecipientmusttrusteachother.Thedevice is corrupted if a receiver is hacked by an attacker or if the receiver intentionallysharesthe keywith someoneelse.
- A vast network of,say, nnodes necessitates themanagement ofkeyn(n–1)/2 keypairs.
- Itisbest tochangethe keyforeach contactsession.
- Successful key management also necessitates the use of a trusted third party, which is asignificantconcern in and of itself.

CryptographicHashFunctions

Hashfunctionsarethemostimportantcryptographicprimitivesandareanessentialcomponentofthebloc kchaindatastructure.Theyarecommonlyusedinavarietyofcryptographicprotocolsandcomputersecur ity implementationssuchasdigitalsignaturesandmessageauthenticationcodes(MACs).Sinceitisused inasymmetrickeycryptography,wewillcoveritherebeforemovingontoasymmetriccryptography.Plea sekeepinmindthatthetopicsdiscussedinthissegmentmaydifferfromthoseusedinuniversitytextbooksa ndmaybeskewedagainsttheblockchainecosystem.

Cryptographichashfunctionsareasubsetofhashfunctionsthataresuitableforcryptography,andwewillc onfineourdiscussiontothem.Asaresult,acryptographichashfunctionisaone-way functionthattransformsarbitrary-lengthinputdatatoafixed-lengthoutput.Theoutputiscommonlyreferred to asa"hash value"or"messagedigest."

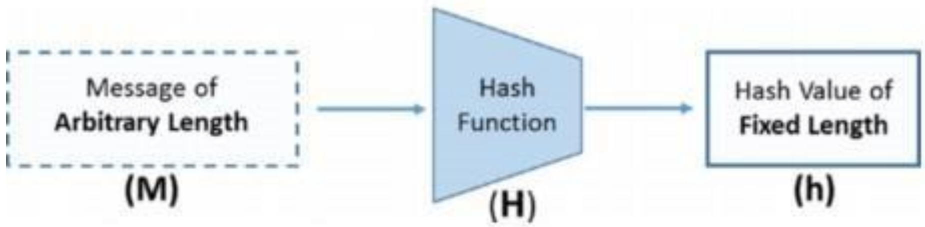


Fig2-5 Hashfunction

SHA-256andSHA-512

Aspreviouslysaid,SHA-256isamemberoftheSHA-2familyofhashfunctions,whichistheoneused in Bitcoins! The name comes from the fact that it generates a 256-bit hash value. As a resultof thebirthdayparadox, it can have2128-bit authentication.

Remember that hash functions accept variable length input and return a fixed size output. Therandomlengthinputisnotfeddirectlytothecompressionfunction;instead,itisdividedintofixedlength blocks before being fed to the compression function. This necessitates the development ofa,mechanism,for.iterating via the compression function by constructing fixed sized input blocksfrom arbitrary length input data and producing a fixed length output. Merkle-Damgrd building,tree construction, and sponge construction are examples of construction techniques. It has beenshown that if the underlying compression mechanism is collision resistant, then the final hashfunction,regardless ofconstruction type, shouldalsobecollisionresistant.

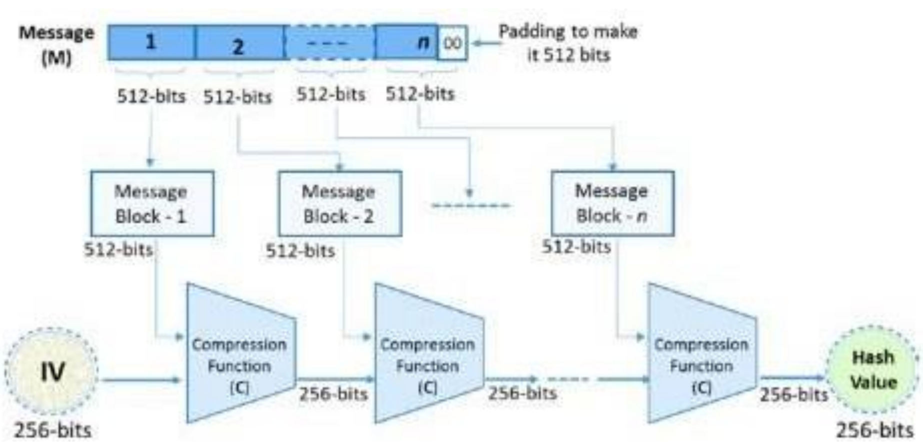


Fig2-6SHA-256 construction

Accordingtothediagram,thefollowing(high-level)stepsarecarriedoutintheorderdefinedtocomputethe final hash value:

- Themessageisfirstseparatedinto512bitblocks,asseeninthediagram.Whenthemessageisnota nexactmultipleof512bits(whichisnormallythecase),thefinalblockispaddedtomakeit512bits.
- The512-bit blocksarefurther subdividedinto 16 32-bitword blocks.
- Eachblockundergoes64roundsofroundwork,witheach32-bitwordundergoingasequenceof operations.Theroundfunctions areamixtureofseveraltypical functions.

Peer-to-PeerNetwork

OntheInternet,BlockChainemploysaP2Pnetworklayer.Eachnodecommunicateswithagroupof neighbour nodes, which in turn communicate with their neighbours, and so on. Every node inthenetworkhastheabilityto access andexitthenetworkat anytime. Thetransfersandblocksarebroadcastoverthepeer-to-peernetwork,andeachreceivingnodeforwardsthemtootherneighbournodes. Full nodes are those that keep a copy of the whole Block Chain. Two Simple PaymentVerificationnodes use only block headers to validate payment. Mining nodes are responsible forthegeneration ofblocks.

Timestamping

When the transfers are chronologically arranged and the majority of nodes agree on a singlehistory,the doublespendingproblemcan beovercome byonlytreatingthefirst transactionfromthesender astrue for the same funds.Timestamping is accomplished by groupingpendingtransactionsintoablockand computing the block hash. Since the transaction is hashed into the block, it can be shown that ithappened.The granularity of this is the time it takes to create a new block, which in Bitcoin is 10minutes.

Consensus

Oneexplanationforthislackofidentitiesisthatthereisnocentralauthorityinapeertopeerschemetodelega teidentitiestoparticipantstoensurethattheyarenotgeneratingnewnodesatwill.A

Sybil assault is the scientific term for this. Sybils are simply copies of nodes that a maliciousadversarymaygeneratetomakeitseemasiftherearesveraldifferentparticipantswhen,inreality,all of those pseudoparticipants are managed by the same adversary. Another justification is thatanonymity is an intrinsic objective of Bitcoin. Even if establishing identities for all nodes orparticipants were feasible or easy, we would not actually want to do so. Although Bitcoin can nothave strong confidentiality guarantees and separate transactions may also be tied together, it doesprovidethepropertythat nooneis requiredtodisclosetheirreallifeidentity,such astheirnameorIPaddress,inorder tojoin.And thisisa crucialproperty anda key functioninBitcoin'sarchitecture.

The architecture would be simpler if nodes had identities. For instance, identities will allow us toprovide protocol instructions such as "Now the node with the lowest numerical ID should takesomeaction."Thesetoffeasibleinstructionsismorelimitedintheabsenceofidentities.However,thereisamuchmoreseriousexplanationfornodestohaveidentities:stability.Ifnodeswereknownand it was not easy to construct new node identities, we might make predictions about the numberofmaliciousnodesanddrawprotectionpropertiesfromthat.Onallofthesecauses,theabsenceofidentitycomplicatesBitcoin's consensus protocol.

Thereisanunspokenagreement.Thisexpectationofrandomnodecollectionallowsforsomethingknown astacitconsensus.Ourprotocolhasseveralrounds,eachofwhichcorrespondstoadifferentblockin the block chain.

Bitcoin consensus algorithm (simplified)

This algorithm is simplified in that it assumes the ability to select a random node in a manner that is not vulnerable to Sybil attacks.

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create

Fig2-7 Bitcoin consensusalgorithmpoints

MerkleTree

Inthepreviouschapter,wediscussedthedefinitionofMerkletrees.Inthispart,wewilljustlookathowBitcoinemploysMerkletrees.EachblockinaBitcoinblockchaincontainsthehashofalltransactions,aswellas theMerklerootofallthesetransactions,whichisincludedintheblock'sheader.Whenwestatethateachblockheadercontainsthehashoftheentirepreviousblock,wemeanitintheliteralsensethatitonlycontainsthe hashofthepreviousblock'sheader.

Nonetheless,itsufficesthattheMerklerootisalreadypresentintheheader.Ifatransactionintheblockischanged,theMerklerootwillnolongerfit,andsuchaconfigurationalsomaintainstheblockchain'slegitimacy.TheMerkletreeisadatastructurethatisatreerepresentationofthehashofthetransactions.TheMerkletree's"LeafNodes"simply formthehashofthetransactions,whiletheMerklerootisthetree'sroot.

Relatedworks

A Block Chain may be permission-less or permissioned, depending on how the nodes in thenetwork join and the constraints imposed on the functions. A public Block Chain is also apermissionless Block Chain. By simply running the node programme, any node will join and exitat any time. Transactions can be submitted by signing them with a private key that peer nodes canverify. Block Chains such as Bitcoin and Ethereum are examples of public permission-less BlockChains.

Bitcoin

Blockchain technology provides cryptocurrency: digital assets. Bitcoin is intended to allow P2Pmoneytransferswithouttheuseoftrustworthyintermediaries,justlikewecantransactwithactualcurrencies without the use of banks or other centralised institutions..Bitcoin is a decentralisedcryptocurrency that is not restricted to any one country and is a global currency. It is autonomousin all aspects—technical, conceptual, and political. New Bitcoins are mined as transactions arevalidated, with a limit of 21 million Bitcoins ever generated. Anyone with a powerful computercanengagein miningand createnewBitcoins.

SinceallBitcoinshavebeencreated,nonewcoinscanbe minted,andonly thoseincirculationcanbe used. Bitcoins,unlike nationalfiatcurrencies,donothave setdenominations.Bitcoins,by definition,canhave anyvaluewitheightdecimalplacesofprecision.As aresult,thesmallestvalueofBitcoinis0.00000001B TC,alsoknownas1Satoshi.

1- Block Structure: A Bitcoin blockchain's block structure is set for all blocks and has uniquefieldswith their correspondingnecessarydetails.

- Bytes from Version 4 It denotes the Bitcoin protocol's version number. Each node runningtheBitcoin protocol should ideallyhavethe sameversion number.
- Thepreviousblockhashwas32bytes.Itholdsthehashofthepreviousblock'sheaderintherow.Wh enallofthefieldsinthepreviousblockheaderarecombinedandhashedwiththe SHA256algorith m,a256-bitresult(32bytes)isgenerated.
- Merkle Root(32bits)By default,thehashesofthetransactionsinablockformaMerkletree,andM erklerootistheMerkletree'sroothash.WhentheMerklerootiscomputed,atransactionthathasbee nupdatedintheblockwouldnotfit.Thismeansthatretainingthehashofthepreviousblock'sheader issufficienttokeeptheblockchainstable.Merkletreesalsoaidindeterminingwhetheratransactio nwaspartoftheblockinO(n)timeandareveryeasy.
- 4bytesforthetimestampIntheBitcoinnetwork,thereisnoconceptofglobaltime.Asaresult,inUni xtimeformat,thisfieldindicatestheapproximatetimeofblockformation.
- TargetDifficulty4bytesWhenthisblockwasmined,theproof-of-work(PoW)complexitylevelwas set.
- asingletimefourbytesThisistherandomnumbergeneratedduringminingtosolvethePoWpuzzle.

2- TheBitcoinNetwork:Aspreviouslysaid,theBitcoinnetworkisapeer-to-peernetwork.Insuch a scheme, there is no centralised server, and each node is handled equally. In such astructure, there is no master–slave relationship and no hierarchy. Since it operates on theInternet,it employs thesame TCP/IPprotocol stack.

TheBitcoinnetworkisadecentralisednetworkwithnosinglepointoffailureorjurisdiction.Howcan you estimate the size of the Bitcoin network for such a design? There is no accurate way toestimate,thissincenodeswilljoinandexitatanytime.

However,someattemptshavebeenmadetostudytheBitcoinnetwork,andsomesaythattherearecloseto1 0,000nodesthataremainly connectedtothenetworkallthetime,andthattherecanbemillionsofnodesata nygiventime.

Ethereum

Byarchitecture,Ethereumisstatefulandkeepstrackofaccountstates,incontrasttoBitcoin,whereeverythin g isatransactionandthereisnointernalpermanentmemory forscripts.Theunderlying complexitiesareshi eldedfromdevelopersthankstoanabstractbaselayer,anddevelopersalsohavethe freedomtocreatetheir o wnstatetransformationfunctionsfor directtransferofvalueandinformation,aswellastransactionformats. Inorder toachievethisgoal,Ethereum'scentralbreakthroughwastheEthereumVirtualMachine(EVM). TheEVM'ssupportfor Turing-completelanguagesmakesitsimplefordeveloperstobuildblockchainapplications.EVMisneededtorun smartcontractsinthesamemannerasaJavaVirtualMachine,(JVM),isrequiredtorunJavacode.For theti mebeing,justrememberthat smartcontractsare Ethereum scripts written in a Turing complete language that are immediately executed when apredefined event happens. In Bitcoin, the “ScriptSig” and “ScriptPubKey” functions are the basicimplementations of smart contracts. We discovered in the previous chapter that the instruction setinBitcoinswasextremelysmall.InEthereum,however,almosteveryapplicationmaybewrittentorun ontheEVMoneachandeverynodeintheEthereumblockchainnetwork.

DApps are the name given to Ethereum's decentralised applications. Ethereum is a worldwideautonomous operating structure. With no centralised server, DApps are programmes that runwithout downtime, fraud, or any kind of control. A peer-to-peer electronic cash system, such asBitcoin, is very simple to create as a DApp on Ethereum. Similarly, any other commodity withinherent value, such as property, vehicles, homes, ballots, and so on, may be easily transacted intheform oftokens from theirrespectiveDAaps onEthereum.

DApps,unlikeconventionalapplicationscreationanddistribution,donotrequirehostingonaback-end server. The "text" is inserted as a payload in transactions, which are then sent to the Ethereumnetwork's mining nodes. Because of the ETH charged as a gas price, certain purchases will beregarded by the mining ecosystem. In Bitcoin, these transfers are broadcast to all those miners inthenetworkthathaveaccesstothem.Whenagreementisreached,thetransactionisaddedtoa block and becomes an everlasting component of the blockchain. Developers are free to create anysolutionand instalit on theEthereum network. Thatis carried outand validated bythenetwork. italso generates the outputs Well, if there had been no fee, the network would not have been viable.Each blockchain transaction has a gas price associated with it, and writing any garbage code andinstallingit into the Ethereum network might bea costlyendeavour.

1- EthereumAccounts

UnlikeBitcoins,Ethereumaccountsdonotconsistofunspenttransactionoutputs(UTXOs).WediscoveredintheBitcoinchapterthatBitcoinsexistintheformoftransactionswithanowner (owner's public key, 20-byte address) and a value. The owner will invest thetransaction provided they have the correct private key for the transaction. As a result,Bitcoinisastatetransfer system, where"state"corresponds totheset ofallUTXOs.

- Externally Controlled Accounts (EOAs): Also known as "easy accounts," these accountsare typically held by individuals or computers that manage them with Private Keys. Bysigning withaprivatekey,EOAsmay transfertransferstootherEOAsorContractAccounts. A contract between two EOAs is typically used to move some kind of value.WhenanEOAmakesadeposittoaContractAccount,theaimistounlockthe"code"insidetheContract Account.
- Contract Accounts: They are only managed by the code that is stored inside them. ThistechnologyinsidetheContract Accounts isknownas "smartcontracts."Theyarenormallyallowed when an EOA or another Contract Account sends a transaction to the ContractAccount.DespitethefactthattheContractAccountscanexecutecomplicatedbusiness logics through the code they contain, they cannot perform new transactions on theirownandmuststilldependontheEOAs.Theycanonlyrespondtoothertransactions(obviouslybymakingtransactions)accordingtothelogiccodedintheir"code."

2- EthereumSmartContracts

Becauseofsmartcontracts,Ethereumissomuchmore.Inthepreviouspages,whentalkingabout Contract Accounts, we got a snapshot of what a smart contract could be. Althoughwe will get into the implementation aspects of smart contracts in the following pages, thissectionwillgointodepthonwhattheyare.Let'sbeginwithwhyit'scalledthat.Pleasekeepinmi ndthatanout-of-the-boxsmartcontractcontainsnothing"smart."Itbecomes intelligentwhensmartlogicisprogrammedintoit,andthemagic of Ethereumallowsyoutodoso.Letusrecapwhatwehavelearned sofar about Ethereumsmart contracts:

- TheEthereumblockchainis hometosmartcontracts.
- Theyhavetheir own account,but theyhavetheir own addressand balance.
- Theyhavetheabilityto transmit messages and receive transfers.
- Theyareenabled whentheyreceiveatransaction andcanalso bedeactivated.
- Theyaresubjecttothesameexecution andstorage feesasothertransactions.

DecentralizedLedger

Bitcoin is an example of the traditional Block Chain protocol. As the first public ledger, it hasdrawnover10,000nodes,establishingthehighest marketcapitalizationofallcryptocurrencies. Inan ideal world, a deployed Dapp would not need any maintenance or governance from the originaldevelopers.Inotherwords,anoptimalBlockChainframeworkoroperationshouldbecapableof functioning without the need for human interaction, forming a Decentralized AutonomousOrganization(DAO).

ADAOisanorganisationthatoperatesaccordingtolawsencodedassmartcontractsthatrunonthe Block Chain. Because of its independent and automated existence, the cost and benefit of aDAOaresharedbyallplayersbymerelyloggingalltasksintoblocks.Bitcoin,themosttraditionalBlockChainprotocol,isanexampleofaDAO.AccordingtothedescriptionofDappsinDappsaredistinguished byfour characteristics, whichare as follows:

- Open Source: Due to the trustworthy nature of Block Chain, Dapps must make their codeopen sourcein orderforthird-partyaudits to befeasible.
- Internal Cryptocurrency Support, internal currency is the vehicle that powers a specificDapp's ecosystem. A Dapp may use tokens to measure all credits and transactions amongdeviceusers, includingserviceproviders andcustomers.
- The basis of transparency is Decentralized Consensus, or agreement among decentralisednodes.
- Thereisnosinglepointoffailure.Sinceallelementsoftheapplicationswillbehostedandimplemented in the Block Chain, a completely decentralised infrastructure can have nosinglepoint of failure.

AReview onBlockchainHealthcareApplications

Legacyprogrammesusuallyonlysharehealthcareserviceswithinthemedicalandhealthcarefieldsandareincompatiblewithexternalsystems.Nonetheless,datasuggeststhatcombiningthesenetworksforintegratedandimprovedhealthcarehasmultipleadvantages,necessitatinginterconnectionbetweendiverseinstitutionsforhealthinformaticsresearchers.Oneofthemostpressingproblemsismultiorganizationaldatasharing,whichrequirespatientdatacollectedfromahealthcareprovidertobereadilyaccessibletootherinstitutionssuchasapractitionerorresearchinstitute.Blockchaintechnologyisredefiningdatamanagementandgovernanceinmanyhealthcareapplications.Thisisduetoitsadaptabilityandunparalleledsegmentation,aswellasthesafeexchangeofpatientdataandresources.Blockchaintechnologyisattheforefrontofnumerouscurrenttrendsinthehealthcaresector.

Withadvancementsinelectronichealthrecords,clouddatastorage,andpatientdatasecuritylaws,newopportunitiesforhealthdataprocessingareopeningup,aswellastheeaseforpatientstoviewandsharetheirhealthdata.Ensuringdataprotection,storage,transfers,andseamlessintegrationisextremelyimportanttoanydatadrivenenterprise,particularlyinhealthcare,whereblockchaintechnologyhastheabilitytosolvethesecriticalissuesinarigorousandefficientmanner.Thissectiondelvesintoblockchainbasedtechnologiessuchasdatatransfer,datamanagement,datastorage,andEHR.

Emergingblockchain,basedhealthcaretechnologiesareconceptuallyseparatedintomultiplelevels,whichincludedatarepositories,blockchaininfrastructure,healthcareimplementations,andstakeholders.CataliniandGordonTheyconcludedtheirdiscussionabouthowblockchaintechnologieswouldallowpatient,centriccontrolofhealthcaredatasharingoverinstitution,centriccontrolinastudyonhealthcareblockchain.Theyinvestigatedhowblockchaintechnologychangesthehealthcareindustrybyallowingdigitalaccessprivileges,patientidentityacrossthenetwork,processingavastamountofhealthcaredata,anddataimmutabilityintheirreport.

DaisukefocusedonmedicalinformationfortheHyperledgerfabricblockchainplatform,sendingmedicaldatatotheHyperledgerblockchainnetwork.Theygatheredsuchmedicalrecordswiththeaidofsmartphones.TheywereattemptingtoensurethathealthcaredataareregisteredtotheBlockchainaspartoftheirwork.

Anuraag investigated blockchain as a means of effectively managing healthcare records. Theyincludeddifferentformsoftrialsintheirresearch,andthemajorityoftheanalysisinthisstudywasaddressing the possible advantages and disadvantages of blockchain technology for healthcarewithoutincludinganyevidenceorframeworkassessment.Theyalsoreachedanagreementonhowblockchaincouldbeaperfectmatch forstoringhealthcareinformationonthecloudinfrastructurewhileprotectingdata protection and privacy.

3SYSTEMDEVELOPMENT

3.1 AnalysisandDesign

3.1.1 SystemAnalysis

The research is a systematic examination of the system's different processes and their interactionsinside.andoutsideof thesystem.Acriticalconcerniswhathastobedonetofixthecrisis.Onepartofthestudyisidentifyingthesystem'sboundariesanddecidingwhetherornottheapplicantsystemcantakeintoaccountothersimilarstructures.Duringtheresearch,informationisgatheredabouttheavailablefiles,decisionpoints,andtransactionsmanagedbythecurrentsystem.

SRS:

The Software RequirementSpecification(SRS) isthe starting pointfor developing software.Throughoutthescheme,itgotmoredifficulttothepointthattheoverallmeaningofthesystemcouldnotbeeasilygrasped.Theprocessofdefiningrequirementswasthenrequired.Thesoftwareprojectisbuiltonthedesiresofcustomers.TheSRSisamethodforconvertingcustomerthoughtsintoaformal document (theinput) (the output oftherequirement phase).

TheSRSphaseconsistsof twobasicactivities:

- Dilemma/RequirementAnalysis:Ahazyandorderedmethodofcomprehendingtheproblem,the target,and the constraints.
- Requirement Specification:Theaimhereisto definethe findings,conductresearchon representation,languages, andequipment, and developtest specifications.

Therequirementprocessconcludesuntilallvalidated SRSdocumentshavebeenproduced.Theprimaryg oal of this procedureis to producethe SRS paper.

Role of SRS:

TheSoftwareRequirement Specification is aformalised formalised formalised formalised formalized.Aimstobridgethegapbetweencustomersanddevelopersthroughcollaboration.Themediu musedtoproperlydefinethecustomeranduserrequirementsisapplicationspecification.Itservesastheba seforappgrowth.Bothparticipatingschememembersshouldbe pleasedwitha good SRS.

3.1.2 SystemDesign

The architecture will be implemented as a decentralised application (DApp) that will support aprivateblockchainnetworkwithadistributedfilesystemonthebackend(DFS).TheEthereumblockchai nsmartcontractprotocolwasusedinthedesignof thehealthcareblockchainsmart contract system. This is an opensource network that is now one of the biggest distributed blockchainnetworks,withathrivingecosystemandasizablepublicDApprepository.Thenetwork currently employs a proof_of_work (PoW) consensus algorithm known as Ethash, but developersareworkingtomovetoaproof-of-stake(PoS)scalabilityalgorithminthenearfuture.

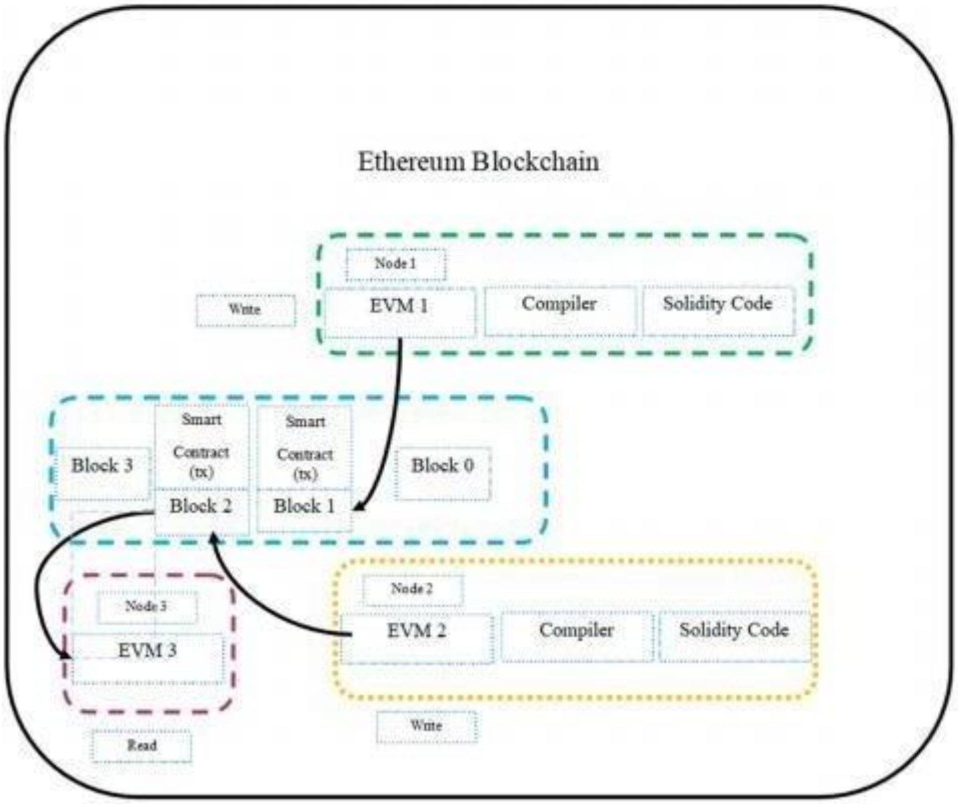


Fig3-1SmartContractMechanism

A consensus algorithm such as or Delegated Proof-of-StakePractical Byzantine Fault Tolerance(PBFT) is ideal for the architecture of distributed applications. The DApp will be able to spotirregularities,unwanteddatainsertions,andmissingpersonsbymatchingDFScontentwithledgerdocuments.Eachphaseislabelled withan auditingtimeline.Thesmartcontracts'keycomponentsarefunctions,events,statevariables,andmodifiers,whicharewritteninthehigh-levelprogramming language solidity. The Remix and Kovan test networks were used to deploy smartcontracts on the testnet and testnet ethers for transaction fee payment. Three phases are involvedin the development of a smart contract using Solidity programming: composing, compiling, andannouncing. Solidity's real-time compiler generates the bytecode. Ethereum Wallet was used topublish smart contracts to the blockchain. Figure 1 depicts the execution of smart contracts withEthereum, without the mining method for simplicity. This smart contract is compiled at thecomputer level into byte code, with each byte representing an operation, and then uploaded to theblockchain.asanEVM-1transaction.AminerpicksitupandconfirmsBlock-

1.Whenausersubmitsarequestthroughthewebinterface,theEVM-2queriesthewebbaseddata,embedsitinTransactiontx,anddeploysittotheblockchain.InBlock,thestateof tr ansactiontxischanged.If node3laterneedstosearchthestatesstoredinthecontract,itmustsynchroniseupt oatleastBlock-2toseethechangescausedbytx.

3.2 ModelDevelopment

3.2.1 Analytical

BlockchainBasedSmartContractsfor Healthcare

We use Ethereum smart contracts to construct smart representations of current medical records,whicharethenstoredonthenetworkwithinindividualnodes.Wecreatecontractsthatprovidemet adataaboutrecordpossession,permissions,anddataintegrity.Theblockchaintransactionsinoursystem containcryptographicallysignedinstructionsforhandlingtheseproperties.

Only legal transactions implementing data alternation allow the contract's statetransition functionscarryoutpolicies.Thislawscanbedesignedtoimplementanysetofguidelinesgoverningasingl emedical record, as long as it can be interpreted computationally. A protocol, for example, canrequire separate approval transactions from patients and healthcare providers before giving third-partyviewingpermission.Fordynamichealthcareworkflows,wecreatedaframeworkfocusedonblockc hainsmartcontracts.Smartcontractshavebeendevelopedtomanagedataaccesspermissions between various institutions in the healthcare environment and for different medicalworkflows.

a smart contract stored on blockchain technologies may be designed that will have all of therequirements from handling various permissions to data access, and it can be shown that a varietyof parties are engaged in this scheme carrying out different tasks. This would aid in improvinginteractionsbetweenphysiciansandpatients.Smartcontractshavedataauthorizationlaws.It willalso assist in monitoring all operations with a special id from their inception to their surrender.Differentscenarioshavebeenplannedandoutlined,andallofthefeaturesandprocessescontain edin the smart contracts are well defined. There will be no need for a centralised agency to overseeand sanction the operation because it will be handled directly by the smart contract, dram aticallyloweringtheadministration expenseof handlingtheprocess.

To ensure performance and economic stability, all medical record data is maintained in local databasestorage,andthehashof thedataisthedatapartof theblockdedicatedtothechain.

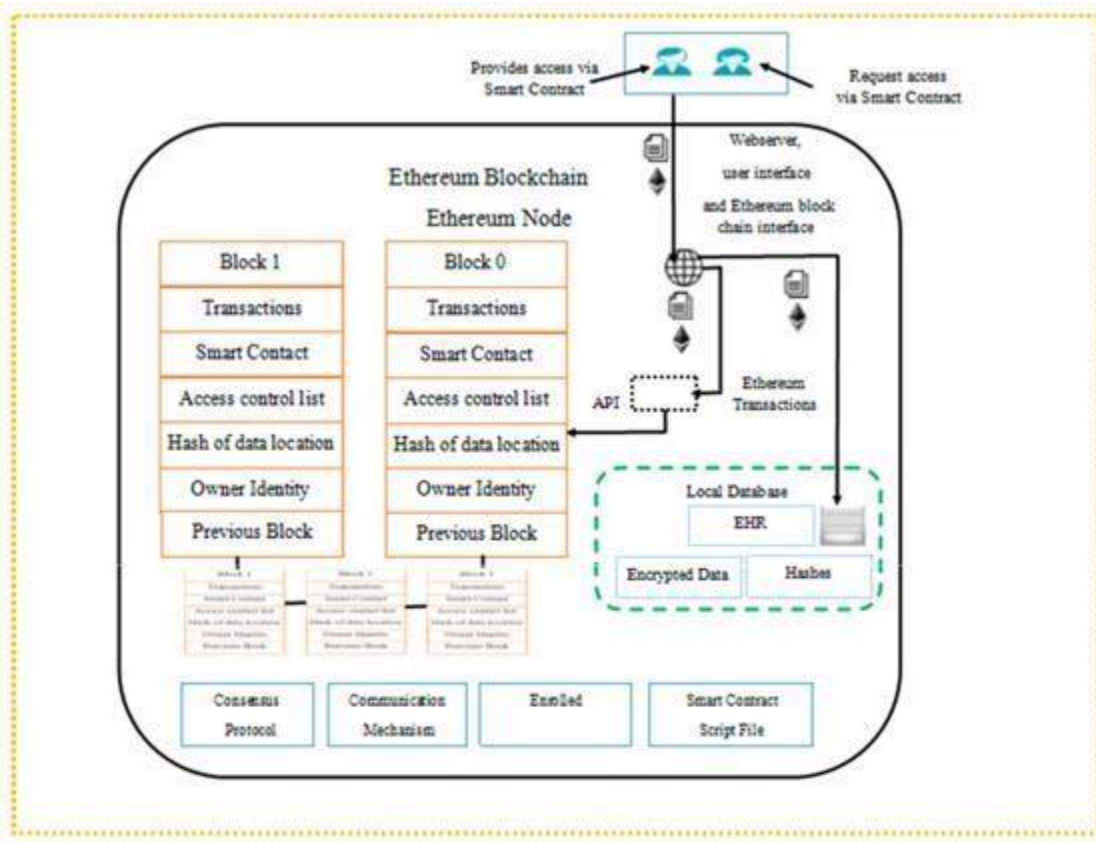


Fig3-2Workflowwithsmartcontract

Theowner'sprivatekeyisusedtosignthedatatransfers(patientordoctor).Thesystem'sblock material reflectsdata ownership and viewing permissionsexchanged byusersof a peerto -peer private network.Smartcontracts,whichenable ustoautomate andmonitorthosestatechanges,aresupportedbyblockchaintechnologies.Welogpatient-providerrelationshipsusing Ethereum smart contracts that link a medical record with viewing rights and data coll ectioninstructions for external server execution. To prevent tampering, we add a crypto graphic hash oftherecord onthe blockchain, preservingdataconfidentiality.

Providerscancreateanewrecordforasinglepatient,andpatientscanconsenttorecordsharing between providers. In all scenarios, the individual processing new material gets an electronicmessageandcancheckthproposedrecorduntilitisapprovedorrefused.Thisl eavesthosewhoareinvolvedintheevolutionof theirdocumentsawareandcommitted.Thisframeworkp rioritisesusability by includingadesignatedcontractthataggregatesconnectionstoallof auser'spatientproviderinteractions, includingacentralpointof referencetoscanonanymedicalbackgro und changes.To manage identity verification, weusepublic key cryptography and a DNSl ike implementation that maps an already existing and widely accepted form of ID,such as auser'snameorsocialsecurity number,totheuser'sEthereumaddress.Asyncingalgorithmmanages“offchain”datasharingbetweenap atientdatabaseandaproviderdatabaseafter returning to the blokchain to validate permissionsthrough our databaseauthentication se rver.

ImplementationDetails

Variousmedicalworkflowsinvolvingvariousmedicaltreatmentshavebeendevelopedandappliedusing theblockchainsmartcontracttechnology.Thiscoverseverythingfromissuingsimplemedicalprescripti onstotreatingcomplicatedillnessesandtheirprocedures,suchassurgicalproceduresforoperationpatien ts.Theaimof developingthesemedicalsmartcontractsistohelppatients,physicians,andhealthcareorga nisationssolvelogisticalinefficiencies.Thismethodwouldaidintheretrieval,examination,andmainten anceofcomplexmedicaldataandprocedures.

FillingofPrescriptions

The primary aim is to streamline the medical drug handling process by minimising lengthy waittimes,eliminatingbriberyfromthesystem,andloweringtheerrorratecausedbydoctormisinterpreta tions. A doctor signs a prescription for a patient and adds it to the patient's medicalhistory using a smart contract. The pharmacy then gains access to this medication through theEthereum blockchain smart contract, thanks to approval given by the primary doctor and thecustomer. After accessing the drug, the pharmacy issues the medication with the expiry date anddose usage posted on to the patient's healthcare records through smart contracts, and the medicineisthenavailableforthepatienttoreceive.Ingeneral,smartcontractfeaturescoordinatemedicati on satisfactionamongdoctorsanddrugstores.Followingapatient'sappointment,doctorsdevotelittletimee xplainingmedication orders orspeakingwith pharmacyshops ingeneral.

Thepatient,primarydoctor(GP),andpharmacyareallincludedinthedataflowforadministeringa medical prescription. It also includes prescription information such as medicine id, expiry date,patientid, and so on.

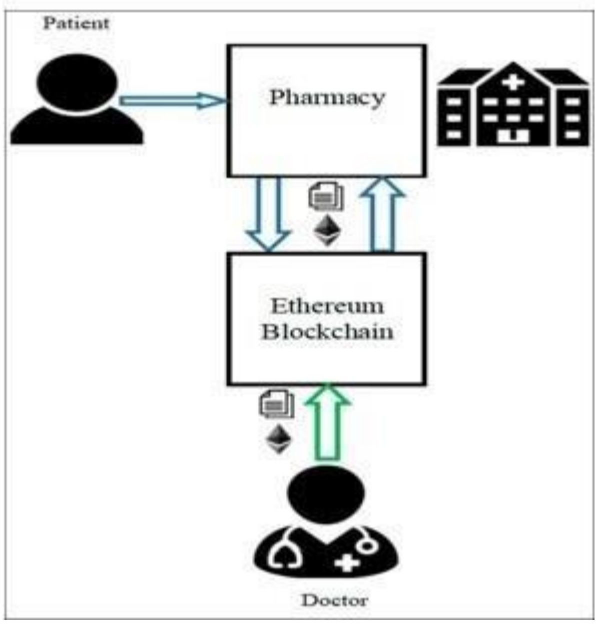


Fig 3-3Smartcontractformedicaldomain

ResultsData

Themaingoalistoexchangeinformationthroughblockchainsmartcontractsbyallowinglaboratories,ph ysicians,emergencyclinics, andothercollaboratorsto effectivelyaccessandshareapatient'stherapeuticinformationamongvariousstakeholders.Considerthe followingscenario:apatient enters a lab for a blood examination. After being processed, the lab will enter the data intothepatient'srecords,andthepatientwillreceiveupdatesviaEthereumblockchain,includinganotetha ttheprocessed resultsofthetestareaccessible,aswellastheoptiontoallowthelabtoencryptthe information and store it on the Ethereum blockchain. The p atient grants permission for theinformation to be posted on the blockchain. If there is an emergency with the patient and he isunresponsive,theemergencyroomwillbeabletoeasilyaccesspatientrecordsfromtheEthereumnetwor kto havepersonalised care.

Allowing patients' medical history to be shared on healthcare blockchain saves patients from havingtotransportlaboratorysamplesorarrangeforrecordstobefaxedtoseparatetreatmentfacilit ies.Healsomaintainsthatallof hishealthcareprofessionalsprovidetheknowledgetheyneedto deliver the best care possible. Laboratories save money on regulatory costs by printing and mailing or faxing each test result to a single supplier. In addition, laboratories and patients have accesstothehealthcareblockchain.

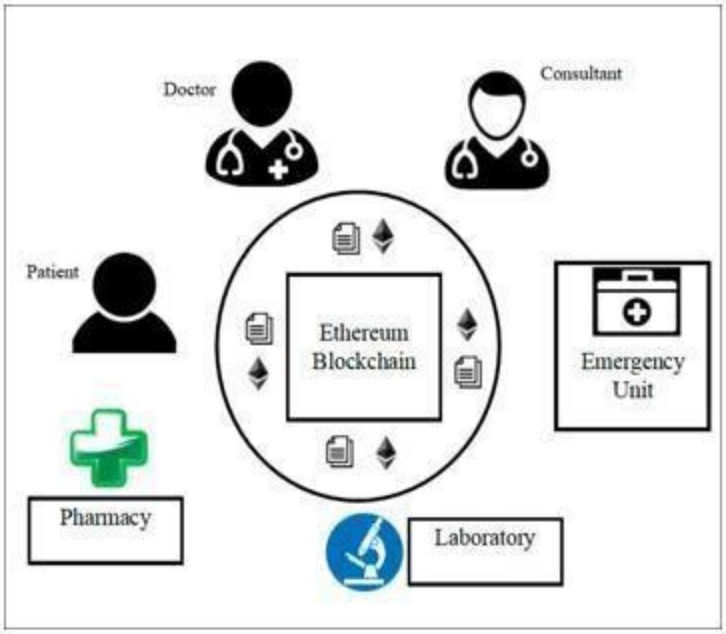


Fig3-4labresultsharing

CommunicationbetweenProviders

In this case, the patient requests treatment for a medical condition. It sends this request to theprimary doctor automatically via the smart contract system. A doctor must assess the referral andrespond with a prescription, as well as refer the patients to a physician for further treatment ifnecessary. Any patient information about treatment history should be documented in the EHR.Please keep in mind that the medical record is held in a local archive where there are strict rulesgoverning who has access to the record and to what degree, and these rules are governed by smartcontractson the Ethereum blockchain.

Another instanceinwhichthepatientrequestsaparticularmedicalprocedure.Asaresult,itsendsthisproposaltotherelevantprofessionalthroughtheagreement'sstrictstructure.Adoctorrecognisesthedemandandanswerswithaprescription,andpatientsaresimplyexchangedforadditionaltreatmentwiththeexpert. Anyhealthrecordspertainingtotreatmentstatusmustbedocumentedinthe EHR.Itisworthnotingthataneighbouringarchiveholdspatient recordswherethereareclear instructionsthatshouldapproachtherecordtowhatextent,andtheseguidel inesaremanagedbythecompetentcontractsontheEthereumblockchain.

Patientsrequestingclinicaladviceaboutaparticulartopicgetmuchmorepersonalisedrecommendationst hanthosegivenbyawebsearch.Seniorphysiciansbenefitfromacreativewayto monetize their experience without overbooking their schedules, while junior physicians gainaccesstoanewpotentialpatient baseand developtheirreputation withintheirspecialisation. Paymentsallowpatients toseekadvicefromjuniorphysicians.

DataFlow

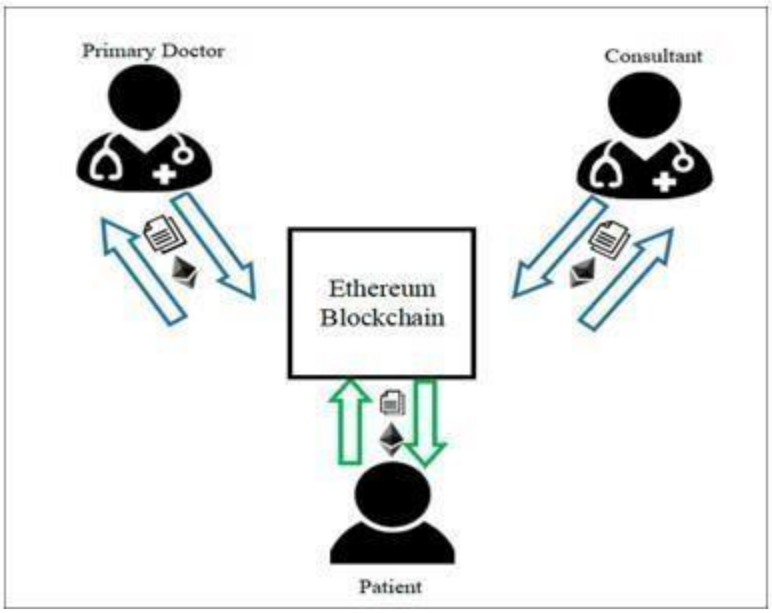


Fig3-5communicationlinkbetweenusers

Theprimarygoalistoexpeditethepaymentprocessforthehealth-caresystem.Physicianswillbeable to continue with treatments more easily as a result of this, rather than trying to place theirpatient's condition on hold while waiting for the payer to respond. The execution of digital smartcontracts will keep a close eye on the whole operation. Reducing, and eventually removing, theerror-prone human activity required to manually evaluate and respond to prior authorizationrequests, as well as reducing appeals caused by inaccurate reading of manually written priorauthorizationforms.

HealthInsuranceCompanypublishestheirpoliciesthroughblockchainsmartcontractsthatincludethepoliciesthatareusedtodecideauthorization.Theproviderthensubmitsanapplicationtotheblockchainforadvancepermissionforadoctorconsultation,medication,orprescription.Thepayer's,smart_contract_basedonthepatient'smedicalrecordsrecordedontheEthereumblockchainandtheinformationintheproposal.Theauthorizationdatawouldthenbeautomaticallyreturnedtothesupplier.Inaddition,thepatient,aswellasanylaboratories,clinics,physicians,orotherpartiestowhichthepatientisgrantedaccess,maychecktheinsuranceauthorizationinrealtime.

Theelectronicpriorauthorizationprocesswillresultinconsiderablecostsavingsforpayers,whonowwastesignificantsumsof timeactivelymonitoringandrespondingtodemands.Doctorswouldbeabletocontinuewithtreatmentmoreefficientlyratherthantryingtopostponecaringfortheirpatientswhilewaitingforthepayer'sresponse.Furthermore,patientswillnothavetoworryaboutwhethertheirinsurerswillcoverthecarethattheirdoctorhasprescribed.Doctorsandpatientscaneffectivelycollaborateonatreatmentpackagecustomiseduniquelyto the patient'sneedsand the necessaryhealth plans if prior consent information isreadil yaccessible.

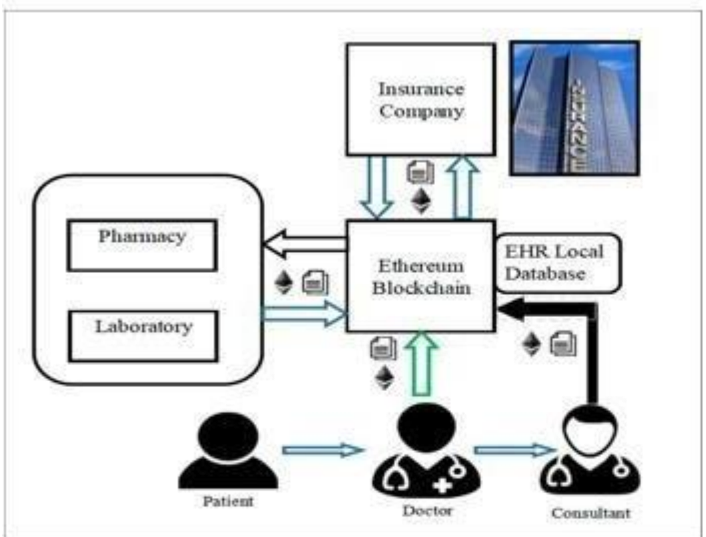


Fig3-6Healthcareframework

SmartContracts

Providingmedicationandmedicalproductsupplierswithaquicker andmorecost_effectivesolutiontotheexistingclinicaltrialprocurementprocess,whichoftennecessitatessignificantexpenditurestopurchasepatientcontactinformationfromseparatedatasourcesandconductextensive pull_marketing strategies.Thekeyaimisforconsumerstobeabletorunclinicaltrial_related smart contractson an Ethereum network, resulting in safer drugsand greater public interestinmedicalscience.Wecanmanagemetadata,suchasprotocolregistration,predefinedresearchinformation,screeningandenrollmentrecords,usingsmartcontractsinthisphase. Toclassifyprospectivecandidatesforclinicaltrials,apharmaceuticalcorporationsearchesformetadatacontainedontheEthereumblockchain.Thecompanythensendsalettertochosenpatients,alongwithanapplicationthatallowsthemtoreadtheirmedicalhistory,andanyrelatedlaboratoryresearchfindings.Ifthepatientagrees,apharmacyindustrypaymentwillbecollectedviasmartcontracts,withaportionofthereceivedchargegoingtothepatientandanotherportiongoingto thelaboratoriesthat reported therequired testfindings for the patient.

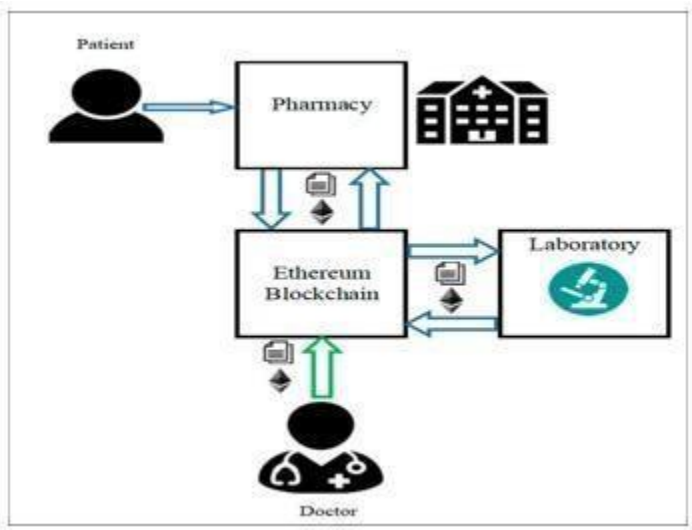


Fig3-7 Workingofdataframework

Drugandmedicaldevicesupplierscangreatlyminimisespendingondatasalesandmarketingcampaignsbyspecificallycontactingqualifyingconsumers.Patients,ontheotherhand,willhaveaccesstoalternativecareoptionsinadditiontoprovidingcreditforparticipationintrials.Laboratoriesinterestedinpostingreportswillbeabletomonetizetheirfindingsinanewway.4PERFORMANCE ANALYSIS

Inthissegment,weevaluateblockchainplatformefficiencyintermsof averageexecutiontime, average latency, and average throughput. It is clear that Hyperledger Fabric outperformsEthereum in all situations. Execution Time Comparison we investigate the variations in execution time of varying numbers of transactions for different platforms and functions.When thenumberof transactionsinthedatacollectiongrows,sodotheexecutiontimes.

Inalldatasets,Hyperledger'sexecutiontimeisconsistentlysmallerthanEthereum's.Ifthenumberoftrans actionsincreases,sodoesthetimedifferencebetweenHyperledgerandEthereum.Weshouldremembert hatCreateAccountmakesuseofanativefeatureofbothsystemssoconstructing,anidentityis_a_nativefu nctiongiven,whileIssueMoneyndTransferMoneyarecustomfunctionswrittenexecutiontimeforCreat eAccount(133.55seconds)issignificantlyfasterthanIssueMoney,(477.71seconds)

andTransferMoneysubtractsmoneyfromoneaccountandtransfersthesamesumtoanother,whileIssue Moneyaddsmoneytooneaccountandsubtractsmoneyfromanother.TheworkloadforIssueMoneyisabo uthalf of theworkloadforTransferMoney.IssueMoneyandTransferMoneytake41.16and62.59secon dsforabatchof 10,000transactions,respectively,forHyperledger,and477.71and485.41secondsforEt hereum.Thefindingsindicateasignificantgapindatacontrolandmaintenancebetweenthetwoplatforms. AverageLatencyComparisonThelogplotof averagelatencyexperiencedbyTransferMoneytransactio nsinfivesetsof experimentsforeachnetworkisshowninFig.5.Theaveragelatencyof Hyperledgeris0. 09secondsandtheaveragelatencyof Ethereumis0.21secondsforthedatacollectionofonetransaction.A tlowtransactionvolumes,Ethereum'slatencyisroughlydoublethatof Hyperledger.Thelatencyof Eth ereumincreasesmuchfasterthanthatof Hyperledgerasthenumberof transactionsinthedatacollection grows. Thelog-logplotof averagelatencyisanalogous.

Averagelatencywasmeasuredinfivesetsof experimentsforeachplatform.Itcanbeshownthatasthenum berof transactionsinthedatasetrises,sodoestheaveragelatencyof bothplatform

s. As the number of transactions is increased from 1000 to 10,000, the average latency of EthereumandHyperledger

increases to 18.67x and 17.09x, respectively. the log-log plot of average throughput experiencedby TransferMoney transactions in five sets of experiments for each network In all data sets,Hyperledger outperformsEthereumintermsofthroughpuWhen the number of transactions

inthedatasetsis100, thetotalthroughputsofbothnetworksmaximise.Thelog-logmapofaverage throughput is analogous to the log-log plot of average throughput.Averagethroughputinfivesetsof experimentsforeachplatformiscompared.Itcanbeseenthatwhenthenumberof transactionsischanged,theshiftinaveragethroughputofHyperledger isgreaterthanthatof Ethereum.LatencyandThroughputinaLargeWorkloadTrialinvestigatehowindividualtransactionsinadatasetfacelatencyandthroughputwhen10,000transactionsareimplemented.BothtransactionsinEthereumhavealongdelay,withthefirsttransactionconfirmedafter361.36secondsandeventuallyconfirmedafterthat.
allsubsequentpurchasesThefirsttransactionisconfirmedbyHyperledgerafter3.57seconds,andsubsequenttransactionsareconfirmedinbatchesof 500.ThehighlatencyexperiencedbyEthereumtransactionspromptsaninquiryintotheminimumlatency.Itcanbeshownthat when thenumberoftransactionsis high, excessivelatencyoccurs.

Maximumconcurrenttransactions

Weimplementedconcurrenttransactionstoassessthecapabilityandlimitationsof eachplatformandreportthemaximumnumberofconcurrenttransactionsthateachplatformcanaccommodate.ThisexercisewouldusetheTransferMoneytransaction.Startingwith10,000,thenumberof concurrenttransactionsismultipliedby10,000beforewereachthelimitof whatthenetworkcanaccommodate.Iftheplatformreports failureorfailstoanswerwithin 10 minutes, this is referred to as failure. According to the findings, Hyperledger Fabric
cansupport20,000concurrenttransactions,whileEthereumcanhandle50,000concurrenttransactions.Furthermore,asthenumberofconcurrenttransactionsgrows,allCPUsarecompletelyused,accordingtoresourceconsumption.

Implications

TheresearchinthispaperdemonstratesthatHyperledgerFabricreliablyoutperformsEthereumintermsof throughputandlatency.Theresultsofthispapersuggestthatasthenumberof transactionsincreases,thedisparitybetweenEthereumandHyperledgerFabricbecomesmuchmorepronounced.

Adirectimplicationisthat,foragivenblockchainapplication,estimatingexpectednumberof transaction swillbeverycrucialinselectingsuitableplatformsastheycanaltersubsequentthroughput,executiontime ,andlatency.Particularly,latencycanplayacrucialroleinapplicationsinvolvingmoneytransferaswellas otherformsof trading.Wenotealsothatthelatenciespresentedinthispapershouldbeconsideredthemini mumpossiblelatencythatcanoccurwhenadoptingthesetwoprivateblockchainplatforms.Attheapplica tionlevel,morecalculation/logicalproces sesmaybeintroducedwhichcaninduceevenlargerlatencies.Lastly,eventhoughHyperledgerFabricout performsEthereuminallaspects,our findingsalsoshowthatEthereumisabletohandlemoreconcurrenttr ansactionsforsimilar computationalresources.

LimitationofthestudyAnalysis

Thesetupforthisevaluationintentionallyanalysestheexecutionlayerof thetargetblockchain platforms. Consensuslayersare excluded from the analysisbyconfiguration. While the di stributed aspect isa crucial part of blockchain platforms,the reasonbehind thisdeliberate ch oiceisbecausethetwotargetplatformsutilisedifferentconsensusprotocols,whichthenatureof theproto colsdirectlyimpacttheperformance.Thenatureof Proof of Workmechanismof Ethereum’sconsens usmechanismismuchslowerthanthenatureof PBFTmechanismthatisdeployedinHyperledgerFabric. Thetestsetupinthispaperteststhecapabilityandlimitationsof both platforms'implementation layer (smart contract infrastructure). The existence of consensusoffersprotectionbutdecreasessystemefficiency;hence,thefindingsprovidedinthispaper representthebestcasescenarioofperformance.Inthefuture,wewillinvestigatetheimplicationsof conse nsusprotocols.Anexaminationof theplatforms'latestversionsThispapertestsandcontraststwoblockc hainplatformsusingthemostrecentimplementationatthetimeof thereview.Whilethisdoesnotreflectw hatblockchainsolutionswouldbeinthefutureduetoongoingimprovements,itdoesbridgeaninformatio nvoidregardingthecapacity and limitations of state.

5 CONCLUSIONS

5.1 Conclusions

SinceitsintroductiontotheworldbyBitcoin,blockchaintechnologyhasdevelopedintoageneral,purpose technologywithapplicationsinavarietyof fields,likehealthcare.Toexplainthecurrentstateof theuseof blockchaintechnologiesinhealthcare,weconductedacomprehensiveanalysisinwhichweusedthesyst ematicmappingstudymethodtobuildamapof allrelatedstudies.Thestudy'saimsweretodefineblockch aintechnologyusecasesinhealthcare,exampleappsdesignedfortheseusecases,problemsanddisadvant agesof blockchain.Basedhealthcareapplications,emergingmethodsusedindesigningtheseapplicatio ns,andareasforpotentialstudies.Ourpapercollectionandsearchprocedureyielded65articles,whichwer eviewedtoanswerthestudyquestions. Accordingtoourfindings,blockchainhas awiderangeofhealthcareapplications,includingtheadministrationofelectronicmedicalrecords,medic ationandpharmacysupplychainmanagement,scientificscienceandeducation,onlinepatientcontrol,an dhealthdataanalytics.Avarietyofblockchain-basedhealthcareprototypeshavebeencreatedbasedonnewblockchainparadigmssuchassmartcontract s,permissionedblockchain,off-chainstorage,andsoon.Moreanalysis,however,isneededtobetterunderstand,define,andassesstheusef ulnessofblockchaintechnologyinhealthcare.Furtherstudyisalsoneededtocomplementongoingefforts toovercomethechallengesofscalability,latency,interoperability,stability,and safetyintheuseofblockchain technologyinhealthcare.

5.2 FutureScope

Asaresultofthetechnology'srapidadoption,ablockchainisoftenusedasanarchitecturalfeatureof a large-scale distributed software system to store data that not only varies greatly in format andcontent, but also expresses a variety of diverse application domain requirements.So there is stillspace for new consueus algorithms that do not need a miner, computing resources, or any otherresourcesas offeringonlyto provethecredibilityof thejob.Then wedesignasingle portalwherewecanallowusersawindowtousethebuiltframeworkfromanydevice.Finally,acompariso nofthe existing system with a cloud-based system to determine the pros and cons of that system and,ifapplicable,howwecanturnitintoourowntomakeitmorecosteffectiveinthelongrun.Aswephase out new modified models, we will also be introducing more pipelines to the grid to includenewfunctional and non-functional functionalities.

REFERENCES

[1] Swan,M.Blockchain,"BlueprintforaNewEconomy,";O'ReillyMediaInc.:Sebastopol,CA,USA, 2015.

[2] Nakamoto, S. Bitcoin, " A Peer-to-Peer Electronic Cash System," March 2019. [Online].Availableat: www.bitcoin.org.

[3] The Monero Project, "the-monero-project", March2019Available at:https://getmonero.org/the-monero-project/.

[4] Paik, Hye-young & Xu, Xiwei & Bandara, Dilum & Lee, Sung & Lo, Sin Kuang. (2019).AnalysisofDataManagementinBlockchain-BasedSystems:FromArchitecturetoGovernance.IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2961404.

[5] Sarmah, Simanta. (2018). Understanding Blockchain Technology.8. 23-29.10.5923/j.computer.20180802.02.

[6] Zheng,Zibin&Xie,Shaoan&Dai,Hong-Ning&Chen,Xiangping&Wang,Huaimin.(2017).AnOverviewofBlockchainTechnology:Architecture,Consensus,andFutureTrends.10.1109/BigDataCongress.2017.85.

[7] Yaga, Dylan & Mell, Peter & Roby, Nik & Scarfone, Karen. (2019). Blockchain TechnologyOverview.

[8] Tasatanattakool, Pinyaphat & Techapanupreeda, Chian. (2018). Blockchain: Challenges andapplications.473-475. 10.1109/ICOIN.2018.8343163.

[9] Kitsantas,Thomas&Vazakidis,Athanasios&Chytis,Evangelos.(2019).AReviewofBlockchainTechnologyandItsApplications in the BusinessEnvironment.

[10] Strebko, Julija & Romanovs, Andrejs. (2018). The Advantages and Disadvantages of theBlockchainTechnology.1-6. 10.1109/AIEEE.2018.8592253.

ORIGINALITY REPORT

24%	14%	14%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

#	Source	%
1	Bikramaditya Singhal, Gautam Dhameja, Priyansu Sekhar Panda. "Beginning Blockchain", Springer Science and Business Media LLC, 2018 Publication	8%
2	www.mdpi.com Internet Source	7%
3	arxiv.org Internet Source	3%
4	Submitted to Jaypee University of Information Technology Student Paper	2%
5	"Applications of Blockchain in Healthcare", Springer Science and Business Media LLC, 2021 Publication	1%
6	Hye-Young Paik, Xiwei Xu, H. M. N. Dilum Bandara, Sung Une Lee, Sin Kuang Lo. "Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance", IEEE Access, 2019	1%

Publication

7	Suporn Pongnumkul, Chaiyaphum Siripanpornchana, Suttipong Thajchayapong. "Performance Analysis of Private Blockchain Platforms in Varying Workloads", 2017 26th International Conference on Computer Communication and Networks (ICCCN), 2017 Publication	1%
8	www.ir.juit.ac.in:8080 Internet Source	<1%
9	hdl.handle.net Internet Source	<1%
10	iugspace.iugaza.edu.ps Internet Source	<1%
11	Martin Feldhofer. "A Case Against Currently Used Hash Functions in RFID Protocols", Lecture Notes in Computer Science, 2006 Publication	<1%
12	Submitted to Universiti Malaysia Sarawak Student Paper	<1%
13	dl.lib.mrt.ac.lk Internet Source	<1%
14	"IC-BCT 2019", Springer Science and Business Media LLC, 2020 Publication	<1%

ulir.ul.ie

15	Internet Source	<1%
16	citeseerx.ist.psu.edu Internet Source	<1%
17	doaj.org Internet Source	<1%
18	dokumen.pub Internet Source	<1%
19	Ken Miyachi, Tim K. Mackey. "hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design", Information Processing & Management, 2021 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		