UNIVERSITETI “ISA BOLETINI”

FAKULTETI I INXHINIERISË MEKANIKE DHE KOMPJUTERIKE

DEPARTAMENTI: INFORMATIKË INXHINIERIKE

PUNIM DIPLOME

Mentori: Kandidati:

Prof.Ass.Dr. Artan Rexhepi Njiazi Ferati

Mitrovicë, Shtator, 2021

UNIVERSITETI “ISA BOLETINI”

FAKULTETI I INXHINIERISË MEKANIKE DHE KOMPJUTERIKE

DEPARTAMENTI: INFORMATIKË INXHINIERIKE

PUNIM DIPLOME

Bazat e teknologjisë blockchain dhe zbatimet e saj

Mentori: Kandidati:

Prof.Ass.Dr Artan Rexhepi Njiazi Ferati

Mitrovicë, Shtator, 2021

Deklaratë e Origjinalitetit

Unë deklaroj që kjo paraqitje është puna ime dhe për sa kam njohuri nga unë nuk përmban materiale të botuara më parë ose të shkruara nga një person tjetër, përveç kur bëhet njohja e duhur në tezë. Çdo kontribut i dhënë nga hulumtimi, pranohet shprehimisht në tezë. Unë gjithashtu deklaroj që përmbajtja intelektuale e kësaj teze është produkt i punës sime personale, përveç në masën që pranohet ndihma nga të tjerët në hartimin dhe konceptimin e projektit ose në stilin, prezantimin dhe shprehjen gjuhësore.

Statement of Originality

I declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, except where due acknowledgement is made in the thesis. Any contribution made by researching, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

Falenderim

Falenderojë familjen time, shoqërinë dhe stafin e mrekullueshëm akademik për mbështetjen e plotë dhe këshillat e shumta që më kanë ofruar gjatë gjithë viteve të studimeve. Puna, përkushtimi dhe suksesi im i përkushtohet gjithë atyre që punuan pa hezitim me mua. Për fund falenderojë përzemërsishtë mentorin tim Prof.Ass.Dr. Artan Rexhepi, për këshillat, rekomandimet dhe mbështetjen në të gjitha etapat e projektit tim.

TABELA E PËRMBAJTJES

REGJISTRI I ILUSTRIMEVE

1 Hyrja në temë

Librat, shfaqjet televizive, dhe filmat kanë bërë parashikime ambicioze të së ardhmës për dekada, shumica nga të cilat janë konsideruar absurde. Ndryshimi eksponencial është bërë një fjalë me trend, por fuqia e një lakese eksponenciale është konsideruar rrallë herë. Çdo vit do të sjellë ndryshime më të mëdha se një vit më parë. Një koncept i tillë ndryshon në mënyrë drastike nga një normë lineare e ndryshimit, ku e ardhmja do të ndryshojë po aq shpejt sa e kaluara. Fatkeqësisht, shumica e portofoleve të investimeve po menaxhohen me një pamje lineare në mbarë botën, me indekse të lidhura me të kaluarën që drejtojnë investimet tona në të ardhmen. Asgjë nuk mund të jetë më dritëshkurtër ose potencialisht e rrezikshme në një kohë të ndryshimit eksponencial. Interneti ka ndryshuar në mënyrë të pakthyeshme botën dhe vazhdon ta bëjë këtë ndërsa zhvilluesit krijojn në platformën që interneti krijon. Në fillimet e para interneti u pa si një rrjet që do të i shërbente ushtrisë të krijonte sisteme komunikuese që do të ndihmonin shtetet e bashkuara të Amerikës të i mbijetonin një katastrofe nukleare. Disa shkenctarë e menduan internetin si një mundësi për të lidhur të gjithë botën në një rrjet të decentralizuar për qëllime të shumta, e që jo shumë vite më vonë edhe ndodhi. Sot vihet në pyetje decentralizimi i internetit pasi shumë shërbime kalojnë nga disa kompani gjigande si Facebook, Google e Amazon. Tani po shfaqet një teknologji e re që kthehet në moralin e decentralizuar të Internetit origjinal me potencialin për të revolucionarizuar infrastrukturën tonë llogaritëse dhe transaksionare, teknologjia e blockchain. Çdo sekondë, miliona pako informacioni transaktohen midis njerëzve dhe makinerive duke përdorur internetin, dhe teknologjia e blockchain po na detyron të rimendojmë kostot, sigurinë dhe pronësinë e këtyre transaksioneve. Blockchain teknologjia ka lindur bashkë me paranë e programueshme digjitale *Bitcoin.* Blockachain sot ka një zhvillim dhe vision shumë më të gjërë dhe mund të mendohet si një teknologji me qëllime të përgjithshme. Blockchain është teknologjia themelore që mbështet kriptovalutat. Për gati katër dekada, ne kemi internetin e informacioneve. Ai përmirësoi jashtëzakonisht rrjedhën e të dhënave brenda dhe midis kompanive dhe njerëzve, por nuk ka transformuar mënyrën se si ne bëjmë biznes. Kjo sepse interneti është krijuar për të lëvizur informacionin - jo vlerën. Ne nuk mund t'i dërgojmë para me email direkt dikujt jo vetëm sepse kopjimi i parave është i paligjshëm, por sepse nuk mund të jemi 100 për qind të sigurt se marrësi ynë është ai që thotë se është. Informacioni në lidhje me identitetin duhet të jetë i shkurt, i përhershëm dhe i pandryshueshëm. Kështu që sot ne kalojmë nëpër ndërmjetës të fuqishëm për të vendosur besimin dhe për të ruajtur

integritetin. Bankat, qeveritë dhe madje kompanitë e mëdha të teknologjisë konfirmojnë identitetin tonë dhe na mundësojnë transferimin e aseteve, ato pastrojnë dhe shlyejnë transaksionet dhe mbajnë shënime për këto transferime. Por kufizimet e këtyre ndërmjetësve - fshehtësia e tyre operacionale dhe cenueshmëria e tyre ndaj hakerave dhe punonjësve mashtrues, po bëhen më të dukshme. Blockchain zgjidh problemin e shpenzimit të dyfishtë, siç e quajnë kriptografët. Tani për herë të parë ndonjëherë kemi një medium dixhital vendas për vlerën, përmes të cilit mund të menaxhojmë, ruajmë dhe transferojmë çdo pasuri - nga paratë dhe muzika te votat dhe veturat, te kolegët e tjerë në një mënyrë të sigurt dhe private. Besimi arrihet jo domosdoshmërisht nga ndërmjetësit por nga kriptografia, bashkëpunimi dhe kodi i zgjuar. Përdorimi i kontratave të menquara është një temë e rëndësishme në teknologjinë blockchain, në këtë raport janë trajtuar edhe kontratat e menqura dhe mënyra se si ato funksionojn.

1.1 Motivimi

Mënyra se si blockchain ka hapur një dimension të ri për shtrirjen e ideve dhe teknologjive të reja, më ka shtyrë shumë që të i përvishem hulumtimit të kësaj teknologjie dhe zbatimeve të saj. Ajo që më magjeps mua është se si kjo teknologji arriti të i shtyej të mendojnë ndryshe edhe gjigandët më të mëdhënjë ekonomik dhe teknologjik të kohës drejt ndryshimit të disa normave që kanë qenë të rregulluara mjaftë mirë ndërë vite, sidomos këtu kur flasim për paranë.

1.2 Qëllimi i punimit

Punimi synon të hedh dritë në parimet dhe zotimet e teknologjisë blockchain. Për hulumtuesit e teknologjisë blockchain, punimi sygjeron që duhet kushtuar më shumë kujdes mbrojtjes së privacisë dhe qështjeve të sigurisë. Në mënyrë të vazhdueshme, pyetja se si të i shpërndajmë të dhënat e transaksioneve në të njejtën kohë duke i mbrojtur ato, është çështje vitale si për nivelin akademik ashtu edhe për praktikimin social. Punimi i përgjigjet pyetjes - *Cila është mënyra që përmes teknologjisë të ndërveprojm me njëri-tjetrin pa përfshirjen e një pale të tretë?*

Kontratat inteligjente janë një pjesë e rëndësishme e një kornize blockchain. Duke përdorur ato, njerëzit mund të tregtojnë në Internet pa pasur nevojë për një ndërmjetës. Punimi ka për qëllim të spjegoj se si këto kontrata qëndrojnë të vetme pa qeversije nga autoritet qendrore dhe as nga ndërhyrja njerëzore. Si funksionojnë këto kontrata dhe si ekzekutohen është çështje e rëndësishme e cila duhet shtruar në mënyrë që të kuptojmë

zbatimet e tyre. Në punim gjendet përgjigjja e pyetjes - *Cilat janë mundësitë dhe sfidat e kontratave intelegjente në teknologjinë blockchain?*

1.3 Struktura e punimit

Punimi është i ndërtuar në gjashtë kapituj. Kapitulli i parë "Hyrja në temë" paraqet pjesët kryesore drejt ndërtimit të temës. Në këtë kapitull gjenden edhe nënkapitujt lidhur me motivimin dhe qëllimin e punimit. Kapitulli dy na njofton me teknologjinë blockchain dhe mënyrën se si lindi kjo teknologji. Në këtë kapitull paraqitet një nënkapitull shumë i rëndësishëm për teknologjinë blockchain "Sistemi i regjistrit të shpërndarë", poashtu njoftohemi me infrastrukturën në blockchain. "Bitcoin - valuta digjitale" është kapitulli i radhës që na njofton me zbatimin më të rëndësishëm të teknologjisë blockchain - *Bitcoin*, në këtë kapitull diskutohet edhe për pjesën e kriptografisë pjesë kjo që i jep sigurinë teknologjisë blockchain. Në kapitullin e katërt "Ethereum dhe kontratat e mençura" flitet për një zbatim të ri dhe mjaft interesant të blockchain teknologjisë, për kontratat e mençura. Një nënkapitull i rëndësishmë i kapitullit të katërt është nënkapitulli "Aplikacionet e Decentralizuara (DApps)", që na njofton me një natyrë ndryshe të aplikacioneve, atë të decentralizuar dhe krijimin e një uebi të ri të quajtur *web3*. Në kapitullin pesë si thotë edhe vetë titulli "Mundësitë dhe sfidat e kontratave intelegjente në teknologjinë blockchain", paraqiten disa zbatime të kontratave të mençura dhe sfidat që i kanë këto zbatime në teknologjinë blockchain. Në kapitullin e fundit të këtij punimi, kapitullin gjashtë është paraqitur një listë që përmbanë referencat e punimit.

2 Teknologjia Blockchain

Ju do të shihni frazën teknologjia “blockchain”, ose zakonisht vetëm “blockchain”, në shumë kontekste të ndryshme dhe mund të jetë konfuze sepse njerëz të ndryshëm përdorin këto fjalë për të kuptuar gjëra të ndryshme [1]. Kur teknologjia Blockchain filloj të ekzistoj, aplikacioni i parë që u testua në këtë platformë ishte **Bitcoin.** Pasi Bitcoin ishte aplikacioni i parë në teknologjinë blockchain, disa mund të thonë se Bitcoin është Blockchain, sidoçoftë Blockchain nuk është Bitcoin. Blockchain është teknologji shumë komplekse që shumë pak e kuptojnë në tërësi. Në fakt, blockchain është aq e komplikuar sa që çdo ditë gjejmë ideja të reja që kjo teknologji mund të i implementoj [2]. Vetë termi i teknologjisë blockchain na jepë një kuptim të lidhjes së blloqeve në zinxhirë qofshin këto blloqe pjesë softuerike të kodit ose pjesë harduerike të sistemit. Ekzistojnë disa lidhje të blloqeve “blockchain”, dhe shumë variacione se si ato funksionojnë. Në qoftë se e shikojmë në anën hierarkike, të gjitha platformat në teknologjinë blockchain bien nën kategorinë e “regjistrave të shpërndarë” (eng distributed ledgers). Ne duhet të bëjmë dallimin në mes teknologjive blockchain dhe regjistrave specifik blockchain. Teknologjitë blockchain janë rregullat ose standardet se si një regjistër (eng ledger) duhet krijuar dhe mirëmbajtur. Teknologjitë e ndryshme kanë rregulla të ndryshme për pjesmarrje, rregulla të ndryshme të rrjetit, specifikime të ndryshme se si duhet të krijohen transaksionet, metoda të ndryshme për të ruajtur të dhënat dhe mekanizma të ndryshëm të konsensusit. Kur një rrjet krijohet, blockchain ose regjistri i rekordeve është inicialishtë i zbrazët pa asnjë transaksion, ashtu si nyja fizike e regjistrit e cila poashtu është e zbrazët. Disa shembuj të teknologjisë blockchain janë: Bitcoin, Etherum, NXT, Corda, Fabric dhe Quorum. Blockchain regjistrat janë instanca të regjistrave që përmbajnë transaksionet ose rekordet përkatëse [1].

2.1 Sistemi i regjistrit të shpërndarë

Në qoftë se e paraqesim sistemin e regjistrit si një trung të familjes, në vend të emrave të familjarëve regjistri i madhë mban informacione për vlerat e pagesave dhe adresat. Në lidhje me vlerat e shumës, regjistri mban të gjitha rekordet e pagesave qysh nga transaksioni i parë që është bërë ndonjëherë. Në lidhje me adresat, nuk ka adresa URL ose adresa vendndodhje. Në vend të kësaj, këto janë adresa bitcoin, ose ndonjë kriptomonedhë tjetër. Regjistri mban një seri transaksionesh të të gjitha kriptovalutave. Vlerat aktuale llogariten në vazhdimësi nga transferimet e mëparshme. Një pjesë e

regjistrit paraqet vlerën që është shoqëruar, kurse pjesët e tjera paraqesin datën dhe kohën e secilit transaksion. Ju mund të shihni se kush ka transferuar te cila llogari, datën dhe kohën, poashtu vlerën se sa ka qenë transaksioni, sidoçoftë regjistri nuk ka banker. Adresat nuk prezantojnë emra të individëve e as nuk tregojnë se kush e mbanë atë shumë, kështu që ne mund ta quajmë këtë sistem si regjistër anonim. Në qoftë se ju aksidentalishtë e humbni fjalkalimin e kuletës tuaj bitcoin që ai regjistër mbanë, qfardo vlere që është në atë kuletë do të humb përgjithmonë. Regjistri është i dukshëm (eng visible) për të gjithë pasi është komplet i decentralizuar.

Në teknologjinë blockchain, çdo transaksion konfirmohet për validitetin e tij dhe pastaj vendoset në një bllok, pastaj secili bllok do të i bashkohet një blloku të validuar më parë, dhe eventualishtë të gjithë këto blloqe do të formojnë një zinxhir të blloqeve që ne e quajmë blockchain. Secilit pjesmarrës në rrjetin e caktuar blockchain i kërkohet ta mbajë një kopje të zinxhirit të blloqeve, pas çdo blloku që krijohet nga sistemi, secili anëtarë në blockchain pranon një bllok të mbyllur (eng sealed). Pastaj sistemi kontrollon secilin bllok automatikisht dhe shton secilin bllok te secili pjesmarrës. Kjo është mënyra se si blockchain mban çdo transaksion dhe çdo vlerë që është krijuar. Këto metoda sigurojnë legjitimitetin dhe korrektësinë e secilit transaksion pa një autoritet qendrorë. Secili transaksion, pasi vërtetohet, mbyllet në regjistër, ky proces kryhet nga minatorët. Kur arrin një bllok i ri i vërtetuar, çdo bllok i ri duhet të shtohet në bllokun e çdo pjesmarrësi, megjithatë, para se të pranojnë bllokun e ri, të gjithë kontrollojnë vazhdimin logjik të të gjitha vlerave në bllokun e ri, për t'u siguruar që të gjitha transferimet e kostove janë të ligjshme. Kjo gjithashtu parandalon çdo replikim të transferimeve ose ndonjë falsifikim të bërë nga hakerët, ose njerëzit me qëllime të këqija, duke u përpjekur të vjedhin bitcoin ose ndonjë kriptomonedhë tjetër. Ky është një hap vendimtar, pasi ky vërtetim do të mbetet përgjithmonë brenda regjistrit të madh dhe brenda blockchain. Ky proces përdor hash funksionet për konkurrencë, për të vërtetuar çdo bllok dhe për t'u siguruar që secili qytetar të marrë të njëjtin rekord [2].

2.2 Blockchain, jo Bitcoin

Termi blockchain, i pavarur nga Bitcoin, filloi të përdoret më gjerësisht në Amerikën e Veriut në vjeshtën e vitit 2015 kur dy revista të shquara financiare kristalizuan vetëdijen për konceptin blockchain. Duhet të bëjmë disa dallime në mes Bitcoin blockchain dhe blockchain teknologjisë. Bitcoin me një shkronjë të madhe B i referohet softuerit që

lehtëson transferimin dhe ruajtjen e Bitcoin monedhës, e cila fillon me një shkronjë të vogël b. Bitcoin është gjeneza e lëvizjës së teknologjisë blockchain. Është e zakonshme të krahasohen blockchain platformat e krijuara rishtas me Bitcoin sepse blockchain Bitcoin është pika referencuese më e gjatë. Ne e dimë se Bitcoin blockchain është një nga platformat blockchain më të rëndësishme që ekzistojnë, dhe që i ka dhënë lindjen një teknologjie me qëllim të përgjithshëm që shkon përtej Bitcoin. Teknologjitë e qëllimit të përgjithshëm janë të përhapura, duke prekur përfundimisht të gjithë konsumatorët dhe kompanitë. Si një teknologji e qëllimit të përgjithshëm, teknologjia blockchain përfshin blockchain platformat private që do të kenë një ndikim të thellë në shumë industri dhe blockchain platformat publike përtej Bitcoin që po rriten me të madhe. Fusha e blockchain platformave publike dhe aseteve të tyre vendase është më e rëndësishme për investitorin inovativ, pasi blockchain platformat private nuk kanë dhënë një klasë krejtësisht të re të aseteve që është e investueshme për publikun. Deri më tani do të jetë e qartë për investitorin inovativ që hapësira e teknologjisë blockchain po punon ende në vetën e vetë dhe do të vazhdojë ta bëjë këtë për vitet që vijnë [3].

2.3 Në kërkim të protokollit të mirëbesimit

Në përgjithësi, interneti ka mundësuar shumë ndryshime pozitive - për ata që kanë qasje në të - por ai ka kufizime serioze për biznesin dhe aktivitetin ekonomik. Në internet, ne ende nuk kemi mundur të krijojmë një mënyrë të besueshme për të vërtetuar identitetin e njëri-tjetrit ose t'i besojmë njëri-tjetrit për të bërë transaksione dhe për të shkëmbyer para pa vërtetuar nga një palë e tretë si një bankë ose një qeveri. Këta ndërmjetës të njëjtë mbledhin të dhënat tona dhe pushtojnë privatësinë tonë për përfitime tregtare dhe siguri kombëtare. Edhe me internet, struktura e kostos së tyre përjashton rreth 2.5 miliardë njerëz nga sistemi financiar global. Pavarësisht premtimit të një bote të fuqizuar nga rrjeti i decentralizuar peer-to-peer, përfitimet ekonomike dhe politike janë provuar të jenë asimetrike - me fuqi dhe prosperitet. Qysh në vitin 1981, shpikësit po përpiqeshin të zgjidhnin problemet e privatësisë në Internet, sigurisë dhe përfshirjes me kriptografi. Pavarësisht se si e riinxhinieruan procesin, gjithmonë kishte rrjedhje sepse palët e treta ishin të përfshira. Pagesa me karta krediti përmes internetit ishte e pasigurt sepse përdoruesit duhej të zbulonin shumë të dhëna personale, dhe tarifat e transaksionit ishin shumë të larta për pagesa të vogla. Në vitin 1993, një matematikan i shkëlqyer me emrin David Chaum doli me një sistem *eCash*, një sistem dixhital pagese që ishte një produkt teknikisht i përsosur që bëri të mundur pagimin e sigurt dhe anonim në Internet. Ishte

shumë e përshtatshme për të dërguar qindarka elektronike, nikel dhe monedha në Internet. Ishte aq e përsosur sa që Microsoft dhe të tjerët ishin të interesuar të përfshinin *eCash* si një tipar në softuerin e tyre. Problemi ishte se, blerësit në internet nuk kujdeseshin për privatësinë dhe sigurinë në internet atëkohë. Kompania Hollandeze e Chaum DigiCash falimentoi në vitin 1998. Të bësh biznes në internet kërkon një hap të madh besimi. Për shkak se infrastrukturës i mungon siguria aq e nevojshme, ne shpesh kemi pak zgjedhje, përveçse t'i trajtojmë ndërmjetësit sikur të ishin perëndi.

Një dekadë më vonë në vitin 2008, industria globale financiare u rrëzua. Ndoshta në mënyrë të favorshme, një person ose persona pseudonim të quajtur Satoshi Nakamoto përshkroi një protokoll të ri për një sistem të parave elektronike peer-to-peer duke përdorur një kriptovalutë të quajtur bitcoin. Kriptomonedhat (monedhat dixhitale) janë të ndryshme nga monedhat tradicionale fiat (parat e letrës) sepse ato nuk janë krijuar ose kontrolluar nga vendet. Ky protokoll vendosi një sërë rregullash - në formën e llogaritjeve të shpërndara - që siguruan integritetin e të dhënave të shkëmbyera midis këtyre miliarda pajisjeve pa kaluar përmes një pale të tretë të besuar. Një platformë globale e besueshme për transaksionet tona është diçka shumë e madhe. Po e quajmë *Protokolli i Mirëbesimit*. Ky protokoll është themeli i një numri në rritje të regjistrave globalë të shpërndarë të quajtur blloqe të lidhura në zinxhir - prej të cilave Bitcoin blockchain është më i madhi. Në bazën më themelore, ky protokoll është një kod me burim të hapur: çdokush mund ta shkarkojë atë falas, ta ekzekutojë dhe ta përdorë për të zhvilluar mjete të reja për menaxhimin e transaksioneve në internet. Si i tillë, ai mban potencialin për lëshimin e aplikacioneve të reja të panumërta dhe aftësive ende të parealizuara që kanë potencialin për të transformuar shumë gjëra. Blockchain teknologjia është e enkriptuar, ajo përdorë kriptim të rëndë që përfshinë çelësa publikë dhe privatë për të ruajtur sigurinë virtuale [4].

2.4 Infrastruktura në blockchain

Blockchain është një teknologji e re, sidoqoftë pasi e shikojmë nga afër mund ta shohim se përbërësit e kësaj teknologjie veqse kanë ekzistuar, e gjitha që është dashur ka qenë bashkimi i këtyre përbërësve [2]. Çdo sistem kompleks kërkon infrastrukturën e duhur, ose burimet dhe një kornizë themelore, për të funksionuar [5].

2.4.1 Rrjeti Peer-to-peer

Një rrjet peer-to-peer është një model i decentralizuar i komunikimit midis dy palëve të njohura gjithashtu si nyje, të cilat mund të komunikojnë me njëri-tjetrin pa pasur nevojë për një server qendror. Ndryshe nga sistemi klient / server, në të cilin një klient bën kërkesën dhe një server e plotëson kërkesën, modeli i rrjetit P2P lejon që secila palë të funksionojë si një klient ashtu edhe si server. Rrjeti, sapo të formohet, mund të përdoret nga pjesëmarrësit për të ndarë dhe ruajtur skedarë pa ndihmën e një ndërmjetësi. Një model peer-to-peer mirëmbahet nga një rrjet i shpërndarë kompjuterash. Këta kompjuterë nuk kanë një server ose administrator qendror pasi secila nyje mban një kopje të skedarëve - duke vepruar si server ashtu edhe klient. Prandaj, secila nyje mund të ngarkojë skedarë për nyjet e tjera ose të shkarkojë skedarë prej tyre. Këto nyje përdorin disqet e tyre për të ruajtur të dhënat e tyre në vend të një serveri qendror. Meqenëse secila nyje ka aftësi të përbashkëta për të ruajtur, transmetuar dhe marrë skedarë, rrjetet P2P priren të jenë më të shpejta dhe më efikase. Ndryshe nga arkitekturat tradicionale në të cilat ekziston një pikë e vetme e dështimit, një rrjet P2P ka një arkitekturë të shpërndarë që e bën atë jashtëzakonisht rezistent ndaj sulmeve kibernetike [6].

Për të mbajtur në lëvizje blockchain-nin, kërkohet një rrjet që banon në internet. Për më tepër, brenda rrjetit, ka shkëmbime të caktuara, për qëllime të përditësimit. Këto përditësime kërkohen për të mbajtur vazhdimisht të përditësuar sistemin e regjistrit të shpërndarë me bllokun e fundit. Nëse ndizni kompjuterin tuaj dhe filloni të ekzekutoni protokollin e blockchain në të, ai do të bëhet pjesë e rrjetit të blockchain [5].

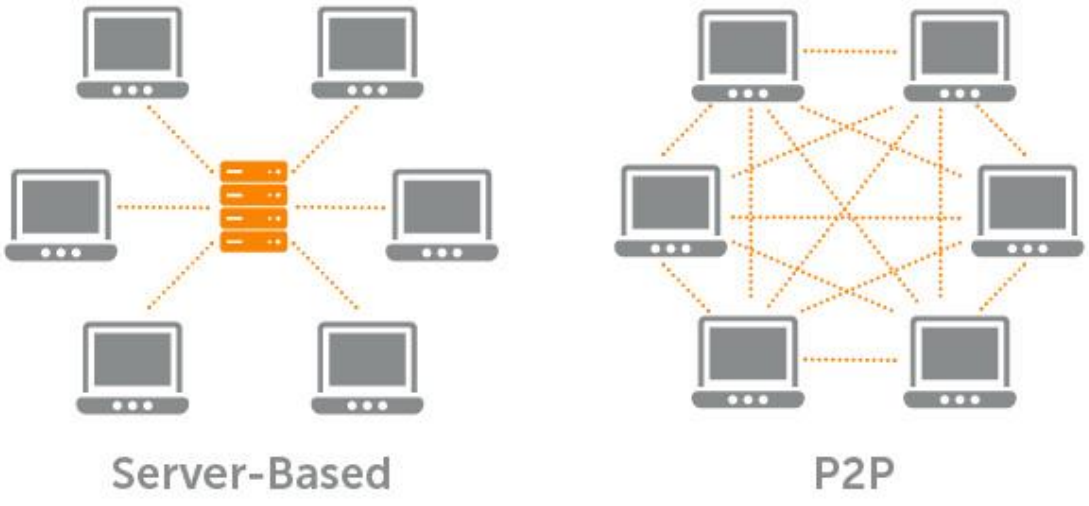

Figura 1. Rrjeti i bazuar në server kundrejt rrjetit P2P [7]

Figura 1 e ilustron formën e lidhjes së pjesmarrësëve në një rrjet i cili bazohet në një server si nyjeve komunikimi në mes të gjithë pjesmarrësve, në anën e djathtë të figurës është paraqitur rrjeti peer-to-peer, rrjet ky ku secili pjesmarrës është i lidhur me secilin pjesmarrës dhe paraqet nyje në rrjet.

Teknologjia themelore blockchain përdor fuqinë e rrjeteve P2P dhe siguron një regjistër të përbashkët dhe të besueshëm të transaksioneve. Si një teknologji e regjistrit të shpërndarë, blockchain regjistron transaksionet si një bllok dixhital i stampuar i pandryshueshëm që tregon dërguesit dhe marrësit. Asnjë autoritet i centralizuar nuk menaxhon rrjetet e blockchain dhe vetëm pjesëmarrësit mund të vërtetojnë transaksionet midis tyre. Teknologjia lejon që njerëzit dhe institucionet të besojnë në rezultatet pa u besuar pjesëmarrësve. Kjo formë e re e ruajtjes dhe menaxhimit të të dhënave të shpërndara (të decentralizuara) vepron si një regjistër kryesor që regjistron publikisht të gjitha transaksionet dhe aktivitetet [6].

Një problem me rrjetet e centralizuara është se nëse një nyje është gati për të shpërndarë përditësimet me të reja me pjesën tjetër të rrjetit, së pari do të i duhet ta dërgojë këtë trafik në nyjen menaxhuese ose server, pastaj kjo nyje menaxhuese qendrore do të mund të bënte shumë gjëra. Serveri mund ta manipulonte trafikun para se ta dërgoj tek nyjet tjera. Një tjetër problem mund të ishte se serveri do të vendoste të dërgonte trafikun vetëm tek një pjesë e rrjetit. Në këto raste teknologjia blockchain në këtë rrjet nuk do të kishte avantazhe. Mënyra e vetme për funksionimin e sistemit është përdorimi i rrjetave të decentralizuara P2P. Rrjetet peer-to-peer janë të dobishme sepse zvogëlojnë rrezikun e mashtrimit dhe manipulimit të të dhënave dhe zvogëlojnë interferimin e një pale të tretë [3].

Në blockchain ka filluar të përdoren edhe rrjetet rrufe (eng Lightning Networks). Rrjeti i rrufesë është një rrjet i shtresës 2, i njohur gjithashtu si rrjeti i shtresës së të dhënave. Ai synon të shkallëzojë rrjetet peer-to-peer nga miliona në miliarda transaksione në sekondë, duke përdorur njëkohësisht kontrata inteligjente [2].

2.4.2 Minatorët në blockchain

Qka është Bitcoin minimi (eng Bitcoing mining)? Bitcoin minimi kryhet nga kompjuterë me fuqi të lartë që zgjidhin probleme komplekse llogaritëse të matematikës, këto probleme janë aq komplekse sa që nuk mund të zgjidhen me dorë dhe janë mjaft të komplikuara edhe për kompjuterë tepër të fuqishëm. Rezultati i minimeve të bitcoin është

i dyfishtë. Së pari, kur kompjuterët zgjidhin këto probleme komplekse të matematikës në rrjetin bitcoin, ato prodhojnë bitcoin të ri, dhe së dyti, duke zgjidhur probleme matematikore llogaritëse, minatorët e bitcoin e bëjnë rrjetin e pagesës së bitcoin të besueshëm dhe të sigurt duke verifikuar informacionin e tij të transaksionit. Kur dikush dërgon bitcoin kudo, quhet transaksion. Transaksionet e bëra në dyqan ose në internet dokumentohen nga bankat, sistemet e pikave të shitjes dhe faturat fizike. Minatorët e Bitcoin arrijnë të njëjtën gjë duke grumbulluar transaksione së bashku në "blloqe" dhe duke i shtuar ato në një rekord publik të quajtur "blockchain". Nyjet pastaj mbajnë shënime për ato blloqe në mënyrë që ato të mund të verifikohen në të ardhmen. Kur minatorët e bitcoin vendosin një bllok të ri transaksionesh në blockchain, një pjesë e punës së tyre është të sigurohen që ato transaksione janë të sakta. Në veçanti, minatorët e bitcoin sigurohen që bitcoin nuk po kopjohet, një ndodhi unike e monedhave dixhitale e quajtur "shpenzimi i dyfishtë" [8]. Shpenzimi i dyfishtë është procesi i kryerjes së dy pagesave me të njëjtën njësi dixhitale të vlerës. Pamundësia për të parandaluar shpenzimet e dyfishta ishte arsyeja kryesore që skemat elektronike të parave të gatshme ishin të pasuksesshme derisa Bitcoin të dilte me një zgjidhje. Bitcoin e zgjedhi problemin e shpenzimit të dyfishtë duke përdorurë blockchain teknologjinë, teknologjinë e rrjetit të decentralizuar ku vetë pjesmarrësit e garantojnë vlerën e njesisë digjitale dhe nuk është nevoja e përfshirjes së një pale të tretë [9].

Minatorët mund të jenë individë por me kohë janë formuar edhe shumë kompani të mëdha si Genesis Mining, ku ju si individë mund të bashkoheni dhe të merrni me qera pajisjet për minim [2]. Me deri në 300,000 blerje dhe shitje që ndodhin në një ditë të vetme, verifikimi i secilës prej këtyre transaksioneve mund të jetë një punë e madhe për minatorët. Si kompensim për përpjekjet e tyre, minatorët shpërblehen me bitcoin sa herë që shtojnë një bllok të ri transaksionesh në blockchain. Shuma e bitcoin-it të ri të lëshuar me çdo bllok të minuar quhet "shpërblimi i bllokut". Shpërblimi i bllokut përgjysmohet çdo 210,000 blloqe (ose afërsisht çdo 4 vjet). Në vitin 2009, ishte 50. Në 2013, ishte 25, në 2018 ishte 12.5, dhe në maj të vitit 2020, u përgjysmua në 6.25. Ky sistem do të vazhdojë deri rreth vitit 2140. Në atë moment, minatorët do të shpërblehen me tarifa për përpunimin e transaksioneve që përdoruesit e rrjetit do të paguajnë. Këto tarifa sigurojnë që minatorët të kenë akoma stimuj për të minuar dhe mbajtur rrjetin. Ideja është që konkurrenca për këto tarifa do të bëjë që ato të mbeten të ulëta pasi të kenë përfunduar përgjysmimet. Me këtë normë përgjysmimi, numri i përgjithshëm i bitcoin në qarkullim

do të arrijë një kufi prej 21 milion, duke e bërë monedhën plotësisht të fundme dhe potencialisht më të vlefshme me kalimin e kohës [8].

2.4.3 Krijimi i bllokut në blockchain

Një bllok është një listë e transaksioneve të regjistruara në regjistër (eng ledger) për një periudhë të caktuar. Madhësia, periudha dhe ngjarja nxitëse (eng triggering event) për blloqet është e ndryshme për çdo blockchain. Jo të gjithë blockchain platformat regjistrojnë dhe sigurojnë një rekord të lëvizjes së kriptovalutës së tyre si objektivin e tyre kryesor. Por të gjithë blockchain platformat regjistrojnë lëvizjen e kriptomonedhës ose shenjës së tyre (eng token)[1]. Transaksioni është thjesht regjistrimi i të dhënave. Caktimi i një vlere (siç ndodh në një transaksion financiar) përdoret për të interpretuar se çfarë do të thotë kjo e dhënë [10].

Shpjegimi i secilit krijim të bllokut mund të bëhet në shumë mënyra, megjithatë, disa tingëllojnë shumë konfuze, por kjo gjithashtu varet nga sa e kuptoni teknologjinë. Në seksionet e mësipërme paraqitëm rolin e jashtëzakonshëm që minatorët kanë për të vërtetuar çdo transaksion në formën e një blloku. Në vijim, paraqesim hapat, se çfarë duhet për të krijuar çdo bllok.

1. Fillimi i një blloku të ri. Edhe nëse minatorët janë duke bërë gjysmën e vlerësimit të një blloku, përfundimisht, ata do të heqin dorë nga gjithçka dhe do të përqendrohen në fillimin e një blloku të ri.
2. Zgjidhja e një transaksioni të ri. Kjo ndodhë kur minatorët po zgjedhin nga mijëra operacione që transmetohen në rrjet.
3. Kontrollimi i përparësinë së transaksionit. Këtë herë minatorët mund të kthehen në numrin një duke filluar një bllok të ri nëse zbulojnë se transaksioni që ata kanë zgjedhur më parë nuk është aq i rëndësishëm. Sidoqoftë, nëse përparësia është e lartë, minatorët mund të vazhdojnë dhe të kalojnë në hapin tjetër.
4. Kontrollimi nëse transaksioni është i vlefshëm. Ky është një proces që çdo minator duhet ta kontrollojë, nuk ka përjashtim të shmangies së këtij hapi për çdo minator. Sidoqoftë, nëse zbulohet se transaksioni është i falsifikuar, ose jo i vlefshëm, minatorët duhet të ndalojnë procesin dhe të kthehen në numrin 1 dhe të fillojnë një bllok të ri dhe të marrin një tjetër transaksion të vlefshëm.

[1] Token - një copë (pjesë) që i ngjan një monedhe të lëshuar për përdorim (si tarifa në një autobus) nga një grup i veçantë me kushte të specifikuara [11]

5. Pranimi i transaksionit. Nëse transaksioni i mëparshëm është testuar si një transaksion i vlefshëm, duhet të pranohet.
6. Vulosja (mbyllja) e transaksionit. Përsëri, nëse transaksioni është gjetur i vlefshëm dhe i pranuar, tani është koha ta nënshkruajmë (vulosim) atë transaksion.
7. Shtimi i transaksionit në pemën e transaksionit brenda bllokut. Ky proces mund të bëhet vetëm pasi të jenë verifikuar të gjithë hapat e mëparshëm.
8. Kontrollimi i madhësisë së transaksioneve. Minatorët duhet të kontrollojnë nëse ka transaksione të mjaftueshme brenda pemës së transaksionit, për të vulosur bllokun. Nëse nuk ka ende transaksione të mjaftueshme, minatori nuk do të jetë në gjendje të vulos bllokun derisa të ketë mjaft transaksione. Prandaj, minatorët duhet të kthehen në hapin numër 2 të zgjedhjes së një transaksioni të ri përsëri, derisa të ketë transaksione të mjaftueshme për mbylljen e bllokut.
9. Kontrollimi i ndërprerjeve. Ky është procesi kur minatori duhet të sigurohet që asnjë minator tjetër nuk e ka vulosur bllokun ndërkohë me të njëjtat transaksione brenda bllokut.
10. Mbyllja e bllokut. Sapo të ketë mjaft transaksione për mbylljen e bllokut, minatorët do të vulosin bllokun.
11. Transmetimi i bllokut. Minatorët duhet të transmetojnë bllokun e ri që është vulosur, megjithatë, nëse minatorët janë ndërprerë brenda procesit të mbylljes së bllokut, atyre mund t'u duhet të fillojnë përsëri një bllok të ri.
12. Fillimi i një blloku të ri. Ky është hapi tjetër në proces, megjithatë, siç e shihni, ne tani jemi kthyer në hapin numër 1. Siç e përmenda, minatorët mund të ndërpriten ndërsa po vulosin bllokun dhe pasi ta transmetojnë atë, nëse një bllok tjetër është vulosur nga një minator tjetër me të njëjtat transaksione brenda në bllok, blloku nuk do të pranohet. Prandaj, duhet të filloni një bllok të ri.

Çdo bllok krijohet rreth 10 minutave. Si rezultat, krijohen 144 blloqe çdo ditë. Siç e përmenda më parë, minatorët të cilët kanë shtuar me sukses një bllok të ri në një blockchain marrin një shkallë të bitcoin. Shpërblimi për çdo krijim të bllokut të ri ishte 50 bitcoin nga 2008 deri në 2012. Shpërblimi për një bllok të ri përgjysmohet çdo katër vjet; prandaj, nga 2012, deri në 2016, çmimi për secilin bllok të ri ishte 25 bitcoin. Aktualisht, që nga viti 2016, deri në vitin 2020, shpërblimi për një minator për një bllok të ri që i shtohet blockchain është 12.5 bitcoin, megjithatë nga viti 2020, do të jetë vetëm

6.25 bitcoin deri në vitin 2024. Ky proces do të vazhdojë deri në 2140 derisa të krijohet bitcoin i fundit.

Të gjitha blloqet në zinxhirin kryesor numërohen, duke filluar me numrin 0, pastaj 1, 2, 3, 4, 5, etj. Blloku i gjelbër është blloku i parë që u krijua, dhe njihet gjithashtu si një bllok i gjenezës, dhe ka një numër bllok zero [2].

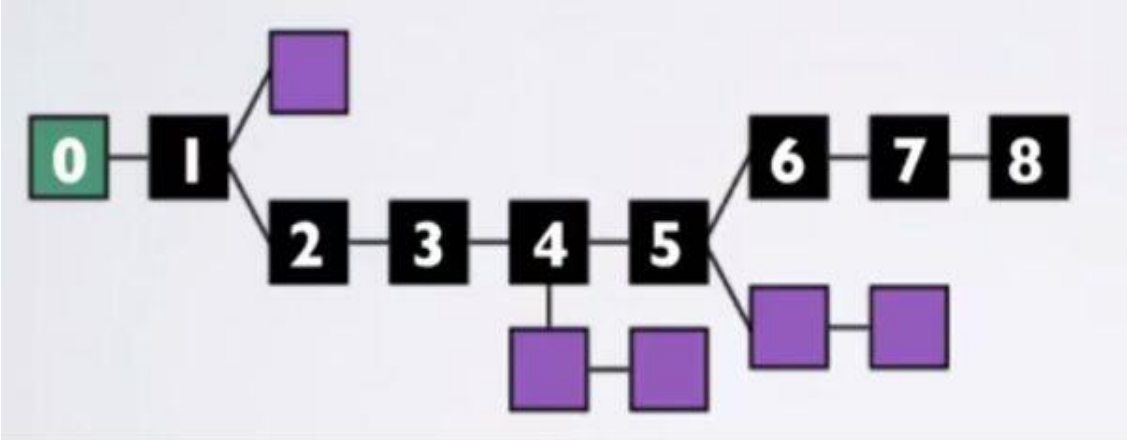

Figura 2. Krijimi i zinxhirëve në teknologjinë blockchain duke përfshirë edhe pirunët anësor[2]

Në figurën 2 paraqitet një zinxhirë i blloqeve të lidhura në blockchain, me ngjyrë të gjelbërt është paraqitur blloku i parë i njohur si blloku i gjenezës kurse me ngjyrë të zezë blloqet valide në blockchain. Në figurë shihen edhe pirunët anësorë të cilet krijohen nga blloqet jo valide në blockchain, blloqe këto që më vonë do të largohen. Blloqet vjollcë janë ato që po formojnë zinxhirë të shkurtër dhe të pavlefshëm, ato quhen pirunë të bllokut. Pirunët në blockchain paraqiten shumë shpesh, përveç kësaj këta pirunë anësorë, njihen gjithashtu si pirunë jetimë.

Një bllok Bitcoin krijohet mesatarisht çdo dhjetë minuta, megjithatë, blloqet Ethereum vendosen mesatarisht në çdo 17 sekonda. Lartësia e bllokut është shuma e blloqeve në një zinxhir midis tij dhe bllokut të gjenezës minus 1. Blloqet në pirunët anësorë mund të kenë të njëjtën lartësi blloku si blloqet në zinxhirin kryesor. Nyje të veçanta në rrjetin peer-to-peer krijojnë këto blloqe. Këto nyje quhen minatorë. Të gjithë minatorët po mbledhin çdo transaksion që njerëzit i dërgojnë njëri-tjetrit përmes rrjetit, dhe vetëm transaksionet e vlefshme transferohen në nyjet e tjera. Secili minator merr një numër të këtyre operacioneve të mbledhura dhe i vendos ato në një bllok të sapoformuar. Këto lista të transaksioneve numërohen tx0, tx1, tx2,… etj. Tx qëndron për transaksion, i ndjekur nga numri. Transaksioni i parë (tx0) njihet gjithashtu si transaksioni i monedhës. Ky është

transaksioni kur minatori cakton një shpërblim bllok në adresën e tij. Kështu krijohen bitcoin valutat. Për minatorët e Bitcoin, që nga viti 2017, shpërblimi i bllokut është 12.5 bitcoin, megjithatë, përsëri në ditën e bllokut të gjenezës, shpërblimi ishte 50 bitcoin për secilin krijim të bllokut. Për Bitcoin, shpërblimi i bllokut përgjysmohet pas çdo 210,000 blloqesh. Pasi të ketë pasur 64 përgjysmime, shpërblimi i bllokut do të jetë zero. Do të ketë një numër maksimal prej 21 milion Bitcoin në qarkullim në vitin 2140. Transaksione të tjera Bitcoin, të tilla si tx1 ose tx2, janë transaksioni i zakonshëm ku bitcoin transferohen nga adresa e pronarit në një adresë të marrësit. Çdo transaksion kërkon një tarifë të vogël transaksioni. Kjo tarifë do të vazhdojë të rritet si një nxitje për minatorët për të krijuar blloqe të reja sepse shpërblimi i bllokut do të vazhdojë të ulet.

Kur minatori ka ndërtuar bllokun, ai duhet të zgjidhë një enigmë hash që zbatohet në listën e tij të transaksioneve. Minatori i cili së pari zgjidh enigmën hash lejohet të transmetojë bllokun e tij në rrjetin peer-to-peer. Blloku gjithashtu përfshin zgjidhjen e enigmës, e quajtur ndryshe edhe *nonce* (eng number once), në kokën e bllokut. Kjo është, sigurisht, e disponueshme për këdo që dëshiron ta shohë atë dhe detajet për secilin bllok mund të gjenden në *www.blockchain.info*. Minatorët e tjerë në rrjet do ta marrin këtë bllok dhe do ta vërtetojnë bllokun para se ta bashkojnë atë në zinxhirin e tyre të blloqeve. Ndodh rregullisht që një tjetër bllok i vlefshëm transmetohet në rrjet sepse një minator tjetër ka zgjidhur enigmën gati në të njëjtën kohë. Kur kjo të ndodhë, krijohen pirunë të përkohshëm. Minatorët duhet të punojnë gjithmonë në zinxhirin më të gjatë [2].

2.4.4 Zinxhiri

Zinxhiri paraqet një hash që lidh një bllok në tjetrin, duke "zinxhiruar" matematikisht ata së bashku. Ky është një nga konceptet më të vështira për t'u kuptuar në blockchain. Është gjithashtu magjia që ngjit blockchain teknologjitë bashkë dhe i lejon ato të krijojnë besim matematikor. Hash-i në blockchain krijohet nga të dhënat që ishin në bllokun e mëparshëm. Hash është një gjurmë gishtash (eng fingerprint) e këtyre të dhënave dhe bllokon blloqet në mënyrë dhe kohë. Edhe pse blockchain teknologjitë janë një risi relativisht e re, hashing nuk është. Hash funksioni u shpik mbi 30 vjet më parë. Kjo risi e vjetër është duke u përdorur sepse krijon një funksion të njëanshëm që nuk mund të deshifrohet. Një funksion hash krijon një algoritëm matematik që harton të dhënat e çdo madhësie në një varg bit të një madhësie fikse. Një varg bit është zakonisht 32 karaktere i gjatë, i cili më pas paraqet të dhënat që janë shkëputur (hash-uar). Algoritmi i sigurt

Hash (SHA) është një nga disa funksione kriptografike të hashit të përdorura në bllok-zinxhirët. SHA-256 është një algoritëm i zakonshëm që gjeneron një hash pothuajse unik, me madhësi fikse 256-bit (32-bajt) [10].

2.4.5 Siguria në blockchain

Blockchain është një teknologji e lartë që do ta ndryshojë botën për të mirë. Një nga pyetjet kryesore që mbetet për këtë teknologji është ajo, se sa e sigurtë është kjo teknologji? Për shkak se kompanitë i mbajnë të gjitha të dhënat e tyre të centralizuara, hakerët duhet të ndjekin vetëm një organizatë të veçantë për të kompromentuar sistemet e saj, kjo është arsyeja pse hakerët e dinë me siguri se gjithçka mund të depërtohet. Për të sulmuar çdo sistem, është vetëm çështje kohe dhe planifikimi i duhur, megjithatë, kur bëhet fjalë për një sistem si blockchain, nuk ka shumë gjasa. Edhe pse ekspertët thonë se nuk është e pamundur, gjithsesi do të kërkonte një sasi të madhe të fuqisë informatike. Blockchain nuk ka firewalls[2] ose ndonjë sistem zbulimi ose parandalimi që do ta mbronte atë. Në vend të kësaj, fuqia e blockchain-it vjen nga fakti që është plotësisht e decentralizuar [2].

2.4.5.1 Çelësat asimetrik

Blockchain përdor algoritme të çelësit asimetrik si pjesë e algoritmeve të tjerë që përdor. Për të zbatuar algoritmin e çelësit asimetrik, kërkon që të kesh dy çelësa të ndryshëm. Njëri prej tyre quhet çelës "Publik" dhe tjetri quhet çelës "Privat". Arsyeja për të pasur dy çelësa është e thjeshtë. Një nga çelësat do të jetë përgjegjës për kriptimin e informacionit për t'u bërë një tekst shifror (eng cipher text), dhe tjetri është për të deshifruar informacionin për t'u bërë një tekst i thjeshtë. Çelësi privat do të gjenerohet nga krijuesi, ai që do të kriptonte informacionin, dhe ky çelës privat duhet të mbahet sekret në çdo kohë. Sidoqoftë, çelësi publik do të ishte i disponueshëm për këdo, kjo është arsyeja pse quhet çelësi publik. Algoritmi i çelësit asimetrik është shumë më i ngadaltë se algoritmi i çelësit simetrikë, megjithatë, siguria është më komplekse. Prandaj, është më e vështirë të thyhet. Të dy, çelësat publikë dhe privatë janë të ndërlidhur matematikisht njëri me tjetrin, që do të thotë se secili çelës publik ka vetëm një çelës privat përkatës [2]. Varësishtë nga sistemet që veprojnë në teknologjitë blockchain, ekzistojnë edhe teknika të ndryshme më të komplikuara të kriptografisë të përdorura në to.

[2] Firewall - Firewall është një pajisje e sigurisë në rrjet që monitoron trafikun hyrës dhe dalës të rrjetit dhe lejon ose bllokon paketat e të dhënave bazuar në një sërë rregullash të sigurisë [12].

2.5 Blockchain sistemet publike, pa leje

Ne kemi eksploruar që kriptovalutat dhe disa shenja (eng token) të tjera përdorin blockchain sistemet publike si mediumin e tyre të regjistrimit - domethënë, transaksionet e tyre përkatëse regjistrohen në blloqe në një regjistër të kopjuar. Blockchain sistemet publike përshkruhen gjithashtu si pa leje kryesisht sepse çdokush mund të krijojë blloqe ose të jetë një mbajtës i regjistrave pa pasur nevojë për leje nga një autoritet. Në këto rrjete publike, ekziston edhe palejueshmëri në një kuptim tjetër - çdokush mund të krijojë një adresë për marrjen e fondeve dhe të krijojë transaksione për dërgimin e fondeve [1].

2.6 Instancat private të blockchain sistemeve publike

Ju mund të ekzekutoni softuer blockchain në një rrjet privat për të krijuar një regjistër të ri. Për shembull, mund të merrni kodin Bitcoin dhe ta ekzekutoni, por në vend që të drejtoni nyjën tuaj te disa kompjuterë që tashmë ekzekutojnë në sistemin blockchain publik të Bitcoin, mund ta drejtoni atë në vend të disa kompjuterëve të tjerë që nuk janë në rrjetin publik të Bitcoin. Sa i përket të gjithë këtyre kompjuterave, ata po fillojnë me një regjistër të ri pa shënime. Në rrjetin e vogël privat që drejtohet nga Bitcoin, ju mund të minoni disa bitcoin por nuk do të mund t'i dërgoni tek rrjeti publik. Edhe pse ky rrjet privat do të përdorte të njejtën grup rregullash si blockchain sistemi publik, ky rrjet ka të dhëna të ndryshme për bilancet e llogarive. Nyjet në secilin rrjet mund të vërtetojnë vetëm atë që shohin në sistemin e tyre blockchain, dhe këto nyje nuk janë në gjendje të shohin vlera në blockchain sistemet tjera [1].

2.7 Blockchain sistemet me leje

Disa platforma janë krijuar për të lejuar grupet e pjesëmarrësve të krijojnë blockchain sistemet e tyre në një kontekst privat. Ato nuk kanë një rrjet publik global. Këto quhen blockchain sisteme private dhe ato janë krijuar për të lejuar pjesëmarrjen vetëm të pjesëmarrësve të aprovuar paraprakisht. Ndryshe nga rrjetet pa leje si Bitcoin dhe Ethereum, blockchain sistemet me leje nuk kanë nevojë për shenjën e tyre amtare (eng native token). Ato nuk kanë nevojë të stimulojnë krijuesit e blloqeve dhe nuk kanë nevojë për provën e punës si faktor për të lejuar pjesëmarrësit të shkruajnë në regjistrin e përbashkët. Në vend të kësaj, kur bizneset kryejnë transaksione, ato po kërkojnë të dhëna për të cilat mund të besohet se janë të azhurnuara (eng updated), të rëna dakord dhe të nënshkruara nga palët e përshtatshme [1].

3 Bitcoin - valuta digjitale

Bitcoin është një koleksion konceptesh dhe teknologjish që formojnë bazën e një ekosistemi digjital parash. Njësitë e monedhës së quajtur bitcoin përdoren për të ruajtur dhe transmetuar vlerën midis pjesëmarrësve në rrjetin bitcoin. Përdoruesit e Bitcoin komunikojnë me njëri-tjetrin duke përdorur protokollin bitcoin kryesisht përmes internetit, megjithëse mund të përdoren edhe rrjete të tjera transporti. Grumbulli i protokolleve Bitcoin, i disponueshëm si softuer me burim të hapur, mund të drejtohet në një gamë të gjerë pajisjesh kompjuterike, duke përfshirë llaptopë dhe telefona inteligjentë, duke e bërë teknologjinë lehtësisht të arritshme. Përdoruesit mund të transferojnë bitcoin përmes rrjetit për të bërë gjithçka që mund të bëhet me monedhat konvencionale, përfshirë blerjen dhe shitjen e mallrave, dërgimin e parave te njerëzit ose organizatat ose dhënien e kredisë. Bitcoin mund të blihet, shitet dhe shkëmbehet për monedha të tjera në shkëmbimet e specializuara të monedhave. Bitcoin në një kuptim është forma përfekte e parave për internet sepse është e shpejtë, e sigurt dhe pa kufij. Ndryshe nga monedhat tradicionale, bitcoin janë tërësisht virtuale. Nuk ka monedha fizike apo edhe monedha digjitale në vetvete. Monedhat nënkuptohen në transaksione që transferojnë vlerën nga dërguesi te marrësi. Përdoruesit e bitcoin posedojnë çelësat që u lejojnë atyre të dëshmojnë pronësinë e bitcoin në rrjetin Bitcoin. Me këto çelësa ata mund të nënshkruajnë transaksione për të zhbllokuar vlerën dhe për ta shpenzuar atë duke e transferuar te një pronar i ri. Çelësat shpesh ruhen në një portofol digjital në kompjuterin ose smartphone-in e secilit përdorues. Zotërimi i çelësit që mund të nënshkruajë një transaksion është i vetmi parakusht për të shpenzuar bitcoin, duke e vendosur kontrollin plotësisht në duart e secilit përdorues. Bitcoin është një sistem i shpërndarë, peer-to-peer. Si i tillë nuk ka server "qëndror" ose pikë kontrolli. Bitcoin valutat janë krijuar përmes një procesi të quajtur "minim", që përfshin konkurrencën për të gjetur zgjidhje për një problem matematikor gjatë përpunimit të transaksioneve bitcoin. Çdo pjesëmarrës në rrjetin bitcoin (d.m.th., kushdo që përdor një pajisje që ekzekuton protokollin e plotë të protokollit bitcoin) mund të funksionojë si minator, duke përdorur fuqinë përpunuese të kompjuterit të tyre për të verifikuar dhe regjistruar transaksionet. Protokolli i bitcoin përfshin algoritme të integruara që rregullojnë funksionimin e minierave në të gjithë rrjetin. Vështirësia e detyrës së përpunimit që minatorët duhet të kryejnë rregullohet në mënyrë dinamike, në mënyrë që mesatarisht, dikush të ketë sukses çdo 10 minuta pavarësisht se sa minatorë (dhe sa përpunim) konkurrojnë në çdo moment.

Bitcoin përfaqëson kulminacionin e dekadave të kërkimit në kriptografi dhe sistemet e shpërndara dhe përfshin katër inovacione kryesore të bashkuara në një kombinim unik dhe të fuqishëm. Bitcoin përbëhet nga:

- Një rrjet i decentralizuar peer-to-peer (protokolli i bitcoin)
- Regjistri kryesor i transaksioneve publike (blockchain)
- Një grup rregullash për vërtetimin e transaksionit të pavarur dhe lëshimin e monedhës (rregullat e konsensusit)
- Një mekanizëm për arritjen e konsensusit global të decentralizuar për blockchain-in e vlefshëm (algoritmi i provës së punës) [13].

3.1 Satoshi Nakamoto

Bitcoin u krijuar nga një person anonim (ose grup personash) të njohur si *Satoshi Nakamoto.* Fitimi i një kuptimi të mendësisë së personit misterioz (ose grupit të personave) prapa kësaj teknologjie të re të mrekullueshme do të ishte me siguri interesante. "Jeta publike" dyvjeçare e Satoshi që mbivendoset me zhvillimin e Bitcoin dhe fillimin i tij, filloi me botimin e letrës së tij "Bitcoin: A Peer to - Peer Electronic Cash System", të cilën ai e njoftoi më 1 nëntor 2008, në listën postare të kriptografisë. Në atë kohë, ky punim mund të shkarkohej në domainin *bitcoin.org,* i cili ishte regjistruar disa muaj më parë me 18 Gusht 2008, përmes *anonymousspeech.com*. Më 9 nëntor 2008, projekti Bitcoin u regjistrua në *SourceForge.net* dhe në fillim të vitit 2009 u krijua blloku i gjenezës (zanafillës). Gjashtë ditë më vonë, më 9 janar 2009, Nakamoto publikoi kodin burimor të versionit Bitcoin 0,01 në *SourceForge.net*. Disa nga komentet e Satoshi kanë të bëjnë me mbulimin e lajmeve që u zhvilluan kur Bitcoin filloi të tërheqë vëmendjen e mediave. Një ngjarje e tillë ishte kur PayPal ndaloi përpunimin e pagesave për WikiLeaks, një organizatë jofitimprurëse gazetareske kushtuar botimit të informacioneve të zgjedhura sekrete dhe të klasifikuara të siguruara nga burime anonime. Një artikull pasues i botuar në revistën *PC World* supozoi se si WikiLeaks mund të përfitonte nga Bitcoin. Shumë gazetarë dhe studiues janë përpjekur të identifikojnë se kush mund të jetë personi që qëndron pas Satoshi Nakamoto. Zgjedhje tipike kanë qenë shkencëtarë të njohur në fushën e kriptografisë, emrat e vërtetë të të cilëve nuk janë Satoshi Nakamoto. Të gjithë janë provuar të rremë, dhe të gjithë janë mohuar të jenë Satoshi Nakamoto gjithashtu [14].

3.2 Paratë

Bitcoin është teknologjia më e re për të shërbyer funksionin e parave - një shpikje që shfrytëzon mundësitë teknologjike të epokës digjitale për të zgjidhur një problem që ka vazhduar për të gjithë ekzistencën e njerëzimit, si ta zhvendosim vlerën ekonomike në kohë dhe hapësirë. Në mënyrë që të kuptohet Bitcoin, duhet së pari të kuptohen paratë, dhe për të kuptuar paratë, nuk ka asnjë alternativë tjetër përveç se studimit të funksionit dhe historisë së parave.

Mënyra më e thjeshtë për njerëzit për të shkëmbyer vlerë është shkëmbimi i mallrave të vlefshme me njëri-tjetrin. Ky proces i shkëmbimit të drejtpërdrejtë referohet si shkëmbim (eng barter), por është praktik vetëm në një qark të vogël me vetëm disa mallra dhe shërbime të prodhuara. Të jesh një mjet shkëmbimi është funksioni themelor që përcakton paratë - me fjalë të tjera, është një e mirë e blerë që të mos konsumohet (një e mirë e konsumit), as të përdoret në prodhimin e mallrave të tjerë (një investim ose një e mirë kapitale), por kryesisht për hir të shkëmbimit me mallra të tjera. Në parim nuk ka asgjë që përcakton se çfarë duhet ose nuk duhet të përdoret si para. Çdo person që zgjedh të blejë diçka jo për hir të vetvetes, por me qëllim për ta shkëmbyer atë me diçka tjetër, po i bën ato de facto[3] para dhe ndërsa njerëzit ndryshojnë, ndryshojnë edhe mendimet e tyre dhe zgjedhjet e asaj që përbën para. Gjatë gjithë historisë njerëzore, shumë gjëra i kanë shërbyer funksionit të parave: ari dhe argjendi, veçanërisht, por edhe bakri, lëvozhgat e detit, gurët e mëdhenj, kripa, bagëtia, letra qeveritare, gurët e çmuar, madje edhe alkooli dhe cigaret në kushte të caktuara. Zgjedhjet e njerëzve janë subjektive, dhe kështu nuk ka zgjedhje "të drejtë" dhe "të gabuar" të parave.

Ndërsa kapaciteti teknik njerëzor për prodhimin e mallrave u sofistikua dhe përdorimi ynë i metaleve dhe mallrave u rrit, shumë metale filluan të prodhoheshin në sasi mjaft të mëdha dhe ishin mjaft të kërkuara për t'i bërë ato shumë të shitshme dhe të përshtatshme për t'u përdorur si media monetare. Dendësia dhe vlera relativisht e lartë e këtyre metaleve e bëri lëvizjen e tyre më të lehtë, më të lehtë se kripa ose bagëtia, duke i bërë ato shumë të shitshme në hapësirë. Prodhimi i metaleve fillimisht nuk ishte i lehtë, duke e bërë të vështirë rritjen e shpejtë të furnizimit të tyre dhe duke u dhënë atyre aftësi të mira për kalimin e kohës. Për shkak të qëndrueshmërisë dhe vetive fizike, si dhe bollëkut relativ në tokë, disa metale ishin më të vlefshme se të tjerat. Hekuri dhe bakri, për shkak të

[3] de facto - një gjendje e gjërave që është e vërtetë në fakt, por që nuk është sanksionuar zyrtarisht [16].

bollëkut të tyre relativisht të lartë dhe ndjeshmërisë së tyre ndaj korrozionit, mund të prodhohen në sasi në rritje. Rezervat ekzistuese do të zhvlerësoheshin nga prodhimi i ri, duke shkatërruar vlerën në to. Këto metale zhvilluan një vlerë relativisht të ulët të tregut dhe do të përdoren për transaksione më të vogla. Nga ana tjetër, metalet më të rralla të tilla si argjendi dhe ari, ishin më të qëndrueshme dhe kishte më pak të ngjarë të gërryheshin ose shkatërroheshin, duke i bërë ato më të shitshme me kalimin e kohës dhe më të dobishme si një depo me vlerë në të ardhmen.

Në shekullin e nëntëmbëdhjetë, me zhvillimin e bankave moderne dhe përmirësimin e metodave të komunikimit, individët mund të bënin transaksione me para letre dhe çeqe të mbështetura nga ari në thesaret e bankave të tyre dhe bankave qendrore. Kjo bëri që transaksionet e mbështetura nga ari të ishin të mundshme në çdo shkallë, duke shmangur kështu nevojën për rolin monetar të argjendit dhe duke mbledhur të gjitha vetitë thelbësore të standardit të arit. Standardi i arit lejoi akumulimin dhe tregtinë e paparë globale të kapitalit duke bashkuar shumicën e ekonomisë së planetit në një zgjedhje të shëndoshë parash të bazuar në treg. E meta e saj tragjike, sidoqoftë, ishte se duke përqendruar arin në qemerët e bankave, dhe më vonë bankat qendrore, u bëri të mundur bankave dhe qeverive që të rrisnin furnizimin e parave përtej sasisë së arit që ata mbanin, duke zhvlerësuar paratë dhe duke transferuar një pjesë të vlerës së saj nga mbajtësit e ligjshëm të parave te qeveritë dhe bankat [15].

3.2.1 Bitcoin si para digjitale

Bitcoin përfaqëson zgjidhjen e parë me të vërtetë digjitale për problemin e parave dhe në të gjejmë një zgjidhje të mundshme për problemet e veçueshmërisë, qëndrueshmërisë dhe sovranitetit. Bitcoin ka funksionuar praktikisht pa asnjë dështim për 12 vitet e fundit, dhe nëse vazhdon të veprojë kështu për 88 vitet e ardhshme, do të jetë një zgjidhje bindëse për problemin e parave, duke u ofruar individëve sovranitet mbi paratë që është rezistent ndaj inflacionit të papritur ndërsa gjithashtu duke qenë shumë i shitshëm në hapësirë, shkallë dhe kohë.

Para shpikjes së Bitcoin, pagesat e ndërmjetme përfshinin (megjithëse nuk ishin të kufizuara) të gjitha format e pagesave digjitale. Natyra e objekteve digjitale, që nga fillimi i kompjuterëve, është se ato nuk janë të pakta (eng scarce). Ato mund të riprodhohen pafund, dhe si të tilla ishte e pamundur të bëhej një monedhë prej tyre, sepse dërgimi i tyre vetëm do t'i kopjonte ato. Çdo formë e pagesës elektronike duhej të kryhej përmes

një ndërmjetësi për shkak të rrezikut të shpenzimit të dyfishtë, nuk kishte asnjë mënyrë për të garantuar që paguesi ishte i sinqertë me fondet e tij, dhe nuk i përdorte ato më shumë se një herë, përveç nëse kishte një palë të tretë të besuar që mbikëqyr llogarinë dhe është në gjendje të verifikojë integritetin e pagesave të kryera. Pas viteve të provave dhe gabimeve inovative nga shumë programues, dhe duke u mbështetur në një gamë të gjerë teknologjish, Bitcoin ishte zgjidhja e parë inxhinierike që lejoi pagesa digjitale pa pasur nevojë të mbështetesh te një ndërmjetës i besuar i palës së tretë. Duke qenë objekti i parë digjital që burimi i tij është vërtet i verifikueshëm, Bitcoin është shembulli i parë i parave të gatshme digjitale. Nakamoto hoqi nevojën për besim tek një palë e tretë duke ndërtuar Bitcoin në një themel të provës dhe verifikimit shumë të plotë dhe të hekurt. Është e drejtë të thuhet se tipari qendror operativ i Bitcoin është verifikimi, dhe vetëm për shkak të kësaj Bitcoin mund të heqë plotësisht nevojën për besim. Sasia e bitcoin-ëve të krijuara është e paraprogramuar dhe nuk mund të ndryshohet pavarësisht se sa përpjekje dhe energji harxhohen për provën e punës (eng proof of work). Kjo arrihet përmes një procesi të quajtur rregullimi i vështirësisë, i cili është ndoshta aspekti më i zgjuar i dizajnit të Bitcoin. Rregullimi i vështirësisë është teknologjia më e besueshme për të bërë para solide (eng hard money) dhe për të kufizuar rritjen e raportit të aksioneve në qarkullim, dhe kjo e bën Bitcoin-in thelbësisht të ndryshëm nga çdo para tjetër. Ndërsa rritja e vlerës së çfardo paraje çon në më shumë burime të dedikuara për prodhimin e saj dhe kështu një rritje në furnizimin e saj, ndërsa vlera e Bitcoin rritet, më shumë përpjekje për të prodhuar bitcoin nuk çojnë në prodhimin e më shumë bitcoin-ave. Në vend të kësaj, thjesht çojnë në një rritje të fuqisë përpunuese të nevojshme për të kryer transaksione të vlefshme në rrjetin Bitcoin, i cili shërben vetëm për ta bërë rrjetin më të sigurt dhe më të vështirë për kompromis. Bitcoin është paraja më e komplikuar e shpikur ndonjëherë, rritja e vlerës së saj nuk mund të rrisë furnizimin e saj, vetëm mund ta bëjë rrjetin më të sigurt dhe më imun ndaj sulmeve. Përdoruesit, minatorët dhe operatorët e nyjeve shpërblehen të gjithë ekonomikisht nga bashkëveprimi me Bitcoin dhe kjo është ajo që e mban atë në lëvizje. Vlen të shtohet se të gjitha palët që e bëjnë Bitcoin të funksionojë individualisht janë të disponueshme për funksionimin e saj. Askush nuk është thelbësor për Bitcoin, dhe nëse dikush dëshiron të ndryshojë Bitcoin, Bitcoin është krejtësisht i aftë të vazhdojë të funksionojë ashtu siç është pa ndonjë kontribut që ka dikush për këtë [15].

3.2.2 A është Bitcoin vegël për kriminelët?

Një nga keqkuptimet shumë të zakonshme në lidhje me Bitcoin që nga fillimi i tij është se ajo do të bënte një monedhë të shkëlqyer për kriminelët dhe terroristët. Një listë e gjatë e artikujve për shtyp janë botuar me pretendime të pabazuara se terroristët ose bandat kriminale po përdorin Bitcoin për veprimtarinë e tyre. Realiteti është se regjistri kryesor i Bitcoin është globalisht i arritshëm dhe i pandryshueshëm. Ai do të mbajë regjistrin e çdo transaksioni për aq kohë sa Bitcoin është ende funksional. Është e pasaktë të thuash vërtet se Bitcoin është anonim, pasi është më tepër pseudonim. Është e mundur, megjithëse nuk është e garantuar, të vendosni lidhje midis identiteteve të jetës reale dhe adresave të Bitcoin, duke lejuar kështu gjurmimin e plotë të të gjitha transaksioneve nga një adresë pasi të përcaktohet identiteti i saj. Kur bëhet fjalë për anonimitetin, është e dobishme të mendoni se Bitcoin është anonim sa internet, kjo varet nga sa mirë fshiheni dhe sa mirë duken të tjerët. Megjithatë, blockchain i Bitcoin e bën fshehjen shumë më të vështirë në web. Është e lehtë të disponosh një pajisje, adresë emaili ose adresë IP dhe të mos e përdorësh më kurrë, por është më e vështirë të fshish plotësisht gjurmët e fondeve në një adresë bitcoin. Nga vetë natyra e saj, struktura blockchain e Bitcoin nuk është ideale për privaci. E gjithë kjo do të thotë që për çdo krim që ka në të vërtetë një viktimë, do të ishte e padukshme që krimineli të përdorë Bitcoin. Natyra e tij pseudonuese do të thotë që adresat mund të lidhen me identitete të botës reale, madje edhe shumë vite pasi është kryer krimi. Bitcoin është një teknologji për para, dhe paraja është diçka që mund të përdoret nga kriminelët në çdo kohë. Çdo formë parash mund të përdoret nga kriminelët, por regjistri i përhershëm i Bitcoin e bën atë veçanërisht të papërshtatshëm për krime me viktima që mund të përpiqen të hetohen. Bitcoin mund të jetë i dobishëm në lehtësimin e "krimeve pa viktima", ku mungesa e viktimës do të thotë se askush nuk përpiqet të përcaktojë identitetin e "kriminelit". Me fjalë të tjera, Bitcoin ka të ngjarë të rrisë lirinë e individëve ndërsa jo domosdoshmërisht u'a bën më të lehtë për të kryer krime. Nuk është një mjet për tu pasur frikë, por një për t'u përqafuar si një pjesë integrale e një të ardhme paqësore dhe prosperuese [15].

3.3 Bërthama e Bitcoin - Zbatimi i referencës

Bitcoin është një projekt me burim të hapur dhe kodi burimor është në dispozicion nën një licencë të hapur (MIT), falas për t'u shkarkuar dhe përdorur për çdo qëllim. Burim i hapur do të thotë më shumë sesa thjesht i lirë për t'u përdorur. Do të thotë gjithashtu se bitcoin është zhvilluar nga një komunitet i hapur vullnetarësh. Në fillim, ai komunitet

përbëhej vetëm nga Satoshi Nakamoto. Deri në vitin 2016, kodi burimor i bitcoin kishte më shumë se 400 kontribues me rreth një duzinë zhvilluesish që punojnë në kod pothuajse me kohë të plotë dhe disa dhjetëra më shumë me kohë të pjesshme. Bërthama Bitcoin është zbatimi referues i sistemit bitcoin, që do të thotë se është referencë autoritare se si duhet të implementohet secila pjesë e teknologjisë. Bërthama Bitcoin zbaton të gjitha aspektet e bitcoin, përfshirë portofolët, një transaksion dhe motorin e vlerësimit të bllokut dhe një nyje të plotë të rrjetit në rrjetin peer-to-peer bitcoin.

Nëse jeni një zhvillues, do të dëshironi të krijoni një mjedis zhvillimi me të gjitha mjetet, libraritë dhe softuerin mbështetës për të shkruar aplikacione bitcoin. Në disa shembuj në këtë kapitull do të përdorim mjedisin e ndërfaqes së rreshtit komandues të sistemit operativ (CLI) e njohur ndryshe edhe si *SHELL*, e cila mund të qaset përmes terminalit [13].

3.3.1 Përpilimi i Bërthamës Bitcoin nga Kodi Burimor

Kodi burimor i Bitcoin (Bitcoin Core) mund të shkarkohet si një arkiv ZIP ose duke klonuar depon e autorizuar të burimit nga GitHub. Në këtë shembull, ne jemi duke përdorur komandën git për të krijuar një kopje lokale ("clone") të kodit burimor:

```
$ git clone https://github.com/bitcoin/bitcoin.git
Cloning into 'bitcoin'...
remote: Counting objects: 66193, done.
remote: Total 66193 (delta 0), reused 0 (delta 0), pack-reused 66193
Receiving objects: 100% (66193/66193), 63.39 MiB | 574.00 KiB/s, done.
Resolving deltas: 100% (48395/48395), done.
Checking connectivity... done.
```

Kur të ketë përfunduar operacioni i klonimit të git, do të keni një kopje të plotë lokale të depozitës së kodit burimor në direktorinë bitcoin [13].

3.3.2 Përzgjedhja e një versioni stabil të bërthamës së Bitcoin

Si parazgjedhje, kopja lokale do të sinkronizohet me kodin më të fundit, i cili mund të jetë një version i paqëndrueshëm ose beta i bitcoin. Para se të përpiloni kodin, zgjidhni një version specifik duke kontrolluar një etiketë të lëshimit. Së pari, për të gjetur etiketat e disponueshme, ne përdorim komandën git tag:

```
$ git tag
v0.1.5
v0.1.6test1
```

```
v0.10.0
...
v0.11.2
v0.11.2rc1
v0.12.0rc1
v0.12.0rc2

...
```

Lista e etiketave tregon të gjitha versionet e lëshuara të bitcoin. Sipas konventës, kandidatët për lëshim, të cilët janë të destinuar për testim, kanë prapashtesën "rc". Lëshimet e qëndrueshme që mund të ekzekutohen në sistemet e prodhimit nuk kanë prapashtesë. Nga lista paraprake, zgjidhni versionin më të lartë të lëshuar, i cili në kohën e shkrimit ishte v0.11.2. Për të sinkronizuar kodin lokal me këtë version, përdorni komandën git checkout:

```
$ git checkout v0.11.2
HEAD is now at 7e27892... Merge pull request #6975
```

Ju mund të konfirmoni që keni versionin e dëshiruar të "checkout" duke shtypur komandën e statusit [13]:

```
$ git status
HEAD detached at v0.11.2
nothing to commit, working directory clean
```

3.3.3 Konfigurimi i versionit të bërthamës së Bitcoin

Kodi burimor përfshin dokumentacionin, i cili mund të gjendet në një numër skedarësh. Rishikoni dokumentacionin kryesor të vendosur në *README.md* në direktorinë e bitcoin duke shtypur *more README.md* në kërkesë dhe duke përdorur hapësirën për të vazhduar në faqen tjetër. Rishikoni me kujdes parakushtet e ndërtimit (eng build), të cilat janë në pjesën e parë të dokumentacionit të ndërtimit. Këto janë libraritë që duhet të jenë të pranishme në sistemin tuaj para se të filloni të përpiloni bitcoin. Nëse këto parakushte mungojnë, procesi i ndërtimit do të dështojë me një gabim. Nëse kjo ndodh sepse keni humbur një parakusht, mund ta instaloni dhe më pas të rifilloni procesin e ndërtimit nga aty ku e keni ndaluar. Duke supozuar se parakushtet janë instaluar, ju filloni procesin e ndërtimit duke gjeneruar një sërë skriptash ndërtimi duke përdorur skriptën *autogen.sh*.

```
$ ./autogen.sh
...
glibtoolize: copying file 'build-aux/m4/libtool.m4'
glibtoolize: copying file 'build-aux/m4/ltoptions.m4'
glibtoolize: copying file 'build-aux/m4/ltsugar.m4'
glibtoolize: copying file 'build-aux/m4/ltversion.m4'
...
configure.ac:10: installing 'build-aux/compile'
configure.ac:5: installing 'build-aux/config.guess'
configure.ac:5: installing 'build-aux/config.sub'
configure.ac:9: installing 'build-aux/install-sh'
configure.ac:9: installing 'build-aux/missing'
Makefile.am: installing 'build-aux/depcomp'
...
```

Skripta *autogen.sh* krijon një sërë skriptash automatike konfigurimi që do të marrin në pyetje sistemin tuaj për të zbuluar cilësimet e sakta dhe për të siguruar që keni të gjitha bibliotekat e nevojshme për përpilimin e kodit. Më e rëndësishmja nga këto është skripta e konfigurimit që ofron një numër opsionesh të ndryshme për të personalizuar procesin e ndërtimit. Shtypni. /configure –help për të parë opsionet e ndryshme:

```
$ ./configure --help
`configure' configures Bitcoin Core 0.11.2 to adapt to many kinds of systems.
Usage: ./configure [OPTION]... [VAR=VALUE]...
...
Optional Features:
--disable-option-checking ignore unrecognized --enable/--with options
--disable-FEATURE do not include FEATURE (same as --enable-FEATURE=no)
--enable-FEATURE[=ARG] include FEATURE [ARG=yes]
--enable-wallet enable wallet (default is yes)
--with-gui[=no|qt4|qt5|auto]
...
```

Këtu janë disa opsione të dobishme që mbishkruajnë sjelljen e paracaktuar të skriptës së konfigurimit:

--prefix=$HOME: Ky opsion mbishkruan vendndodhjen e paracaktuar të instalimit. Përdorni *$HOME* për të vendosur gjithçka në direktorinë tuaj, ose në ndonjë vend tjetër.

--disable-wallet: Ky opsion përdoret për të çaktivizuar zbatimin e kuletës referuese.

--with-gui=no: Mos ndërtoni ndërfaqen grafike të përdoruesit, e cila kërkon librarinë *Qt*. Kjo ndërton bitcoin vetëm në server dhe në rresht komandash.

Pastaj, ekzekutoni skriptin e konfigurimit për të zbuluar automatikisht të gjitha libraritë e nevojshme dhe për të krijuar një skript të personalizuar të ndërtimit për sistemin tuaj:

```
$ ./configure
checking build system type... x86_64-unknown-linux-gnu
checking host system type... x86_64-unknown-linux-gnu
checking for a BSD-compatible install... /usr/bin/install -c
checking whether build environment is sane... yes
checking for a thread-safe mkdir -p... /bin/mkdir -p
checking for gawk... gawk
checking whether make sets $(MAKE)... yes
...
[many pages of configuration tests follow]
...
$
```

Nëse gjithçka shkoi mirë, komanda e konfigurimit do të përfundojë duke krijuar skriptet e personalizuara të ndërtimit që do të na lejojnë të përpilojmë bitcoin. Nëse ka ndonjë librari që mungon ose ndonjë gabim, komanda e konfigurimit do të përfundojë me një gabim në vend që të krijojë skriptet e ndërtimit [13].

3.3.4 Ndërtimi i skriptave ekzekutuese Bërthamë të Bitcoin-it

Në vazhdim, ju do të përpiloni kodin burimor, një proces që mund të zgjasë deri në një orë, në varësi të shpejtësisë së CPU-së tuaj dhe memories në dispozicion. Gjatë procesit të përpilimit duhet të shihni rezultatet çdo disa sekonda ose çdo disa minuta, ose një gabim nëse diçka shkon keq. Nëse ndodh një gabim, ose procesi i përpilimit ndërpritet, ai mund të rifillojë në çdo kohë duke përpiluar përsëri kodin.

```
$ make
Making all in src
CXX crypto/libbitcoinconsensus_la-hmac_sha512.lo
CXX crypto/libbitcoinconsensus_la-ripemd160.lo
CXX crypto/libbitcoinconsensus_la-sha1.lo
CXX crypto/libbitcoinconsensus_la-sha256.lo
CXX crypto/libbitcoinconsensus_la-sha512.lo
CXX libbitcoinconsensus_la-hash.lo
CXX primitives/libbitcoinconsensus_la-transaction.lo
CXX libbitcoinconsensus_la-pubkey.lo
CXX script/libbitcoinconsensus_la-bitcoinconsensus.lo
CXX script/libbitcoinconsensus_la-interpreter.lo
[... many more compilation messages folloë ...]
$
```

Nëse gjithçka shkon mirë, bërthama Bitcoin tani është përpiluar. Hapi i fundit është instalimi i ekzekutuesve të ndryshëm në sistemin tuaj duke përdorur komandën *sudo make install*. Mund t'ju kërkohet fjalëkalimi juaj i përdoruesit, sepse ky hap kërkon privilegje administrative: [13]

```
$ sudo make install
Password:
Making install in src
../build-aux/install-sh -c -d '/usr/local/lib'
libtool: install: /usr/bin/install -c bitcoind /usr/local/bin/bitcoind
libtool: install: /usr/bin/install -c bitcoin-cli /usr/local/bin/bitcoin-cli
libtool: install: /usr/bin/install -c bitcoin-tx /usr/local/bin/bitcoin-tx
...
$
```

3.3.5 Përdorimi i bërthamës Bitcoin në një nyje

Drejtimi i një nyje, sidoqoftë, kërkon një sistem të lidhur përgjithmonë me burime të mjaftueshme për të përpunuar të gjitha transaksionet me bitcoin. Në varësi të faktit nëse vendosni të indeksoni të gjitha transaksionet dhe të mbani një kopje të plotë të bllokut, mund t'ju duhet gjithashtu shumë hapësirë në disk dhe RAM. Që nga fundi i vitit 2016, një nyje me indeks të plotë ka nevojë për 2 GB RAM dhe 125 GB hapësirë në disk në mënyrë që të ketë vend për t'u rritur. Nyjet Bitcoin gjithashtu transmetojnë dhe marrin transaksione dhe blloqe bitcoin, duke konsumuar gjerësi të madhe bandwidth-i të internetit. Nëse lidhja juaj e internetit është e kufizuar, ka një kapacitet të ulët të të dhënave ose matet (ngarkohet nga gigabit), ju ndoshta nuk duhet të ekzekutoni një nyje bitcoin mbi të, ose ta ekzekutoni në një mënyrë që kufizon gjerësinë e saj të bandwidth-it. Pavarësisht nga këto kërkesa për burime, mijëra vullnetarë drejtojnë nyje bitcoin. Disa janë duke funksionuar në sisteme aq të thjeshta sa një Raspberry Pi (një kompjuter prej $35 me madhësinë e një pakete kartash). Shumë vullnetarë gjithashtu ekzekutojnë nyje bitcoin në serverat me qira, zakonisht një variant i Linux. Një server privat virtual (VPS) ose serveri kompjuterik cloud mund të përdoret për të ekzekutuar një nyje bitcoin. Serverë të tillë mund të merren me qira për $25 deri $50 në muaj nga një shumëllojshmëri ofruesish [13].

3.4 Çelësat dhe Adresat në Bitcoin

Pronësia e bitcoin vendoset përmes çelësave digjitalë, adresave të bitcoin dhe nënshkrimeve digjitale. Çelësat digjitalë nuk ruhen në të vërtetë në rrjet, por në vend të

kësaj krijohen dhe ruhen nga përdoruesit në një skedar, ose në një bazë të dhënash të thjeshtë, të quajtur portofol. Çelësat digjitalë në portofolin e një përdoruesi janë plotësisht të pavarur nga protokolli Bitcoin dhe mund të gjenerohen dhe menaxhohen nga softueri i portofolit të përdoruesit pa i'u referuar zinxhirit blockchain ose qasjes në internet. Çelësat mundësojnë shumë nga vetitë interesante të bitcoin, duke përfshirë besimin dhe kontrollin e decentralizuar, vërtetimin e pronësisë dhe modelin e sigurisë me kriptografi. Shumica e transaksioneve me bitcoin kërkojnë një nënshkrim të vlefshëm digjital për t'u përfshirë në blockchain, i cili mund të gjenerohet vetëm me një çelës sekret, prandaj kushdo që ka një kopje të këtij çelësi ka kontrollin e bitcoin. Nënshkrimi digjital i përdorur për të shpenzuar fonde është referuar gjithashtu si një dëshmitar, një term i përdorur në kriptografi. Të dhënat e dëshmitarëve në një transaksion me një monedhë të vogël dëshmojnë për pronësinë e vërtetë të fondeve që shpenzohen. Çelësat vijnë në çifte të përbëra nga një çelës privat (sekret) dhe një çelës publik. Mendoni se çelësi publik është i ngjashëm me një numër të llogarisë bankare dhe çelësi privat, si i ngjashëm me PIN-in sekret, ose nënshkrimin në një çek, që siguron kontroll mbi llogarinë. Këto çelësa digjitalë shihen shumë rrallë nga përdoruesit e bitcoin. Për pjesën më të madhe, ato ruhen brenda skedarit të portofolit dhe menaxhohen nga softueri i portofolit bitcoin. Në pjesën e pagesës së një transaksioni bitcoin, çelësi publik i marrësit përfaqësohet nga gjurma e tij e gishtit (eng fingerprint), e quajtur një adresë bitcoin. Në shumicën e rasteve, një adresë bitcoin gjenerohet nga dhe korrespondon me një çelës publik. Sidoqoftë, jo të gjitha adresat e bitcoin përfaqësojnë çelësat publik. Në këtë mënyrë, bitcoin adreson abstraktin e marrësit të fondeve, duke i bërë destinacionet e transaksioneve fleksibël, të ngjashme me kontrollet në letër, një instrument i vetëm pagese që mund të përdoret për të paguar në llogaritë e njerëzve, për të paguar në llogari të kompanisë, për të paguar fatura ose për të paguar në para të gatshme. Adresa e bitcoin është paraqitja e vetme e çelësave që përdoruesit do të shohin në mënyrë rutinore, sepse kjo është pjesa që ata duhet të ndajnë me botën [13].

3.4.1 Kriptografia e çelësit publik dhe kriptomonedha

Që nga shpikja e kriptografisë së çelësit publik, janë zbuluar disa funksione të përshtatshme matematikore, të tilla si eksponentimi i numrit kryesor dhe shumëzimi i kurbës eliptike (eng eliptic curve). Këto funksione matematikore janë praktikisht të pakthyeshme, që do të thotë se ato janë të lehta për t'u llogaritur në një drejtim dhe të parealizueshme për t'u llogaritur në drejtim të kundërt. Bazuar në këto funksione matematikore, kriptografia mundëson krijimin e sekreteve digjitale dhe nënshkrimeve

digjitale të paharrueshme. Bitcoin përdor shumëzimin e kurbës eliptike si bazë për kriptografinë e saj. Në bitcoin, ne përdorim kriptografinë e çelësit publik për të krijuar një çift kyç që kontrollon qasjen në bitcoin. Çifti i çelësave përbëhet nga një çelës privat dhe - që rrjedh prej tij - një çelës unik publik. Çelësi publik përdoret për të marrë fonde, dhe çelësi privat përdoret për të nënshkruar transaksione për të shpenzuar fondet. Ekziston një marrëdhënie matematikore midis çelësit publik dhe privat që lejon që çelësi privat të përdoret për të gjeneruar nënshkrime në mesazhe. Ky nënshkrim mund të vërtetohet përkundër çelësit publik pa zbuluar çelësin privat. Kur shpenzon bitcoin, pronari aktual i bitcoin paraqet çelësin e tij publik dhe një firmë (të ndryshme çdo herë, por të krijuar nga i njëjti çelës privat) në një transaksion për të shpenzuar ato bitcoin. Përmes prezantimit të çelësit publik dhe nënshkrimit, secili në rrjetin bitcoin mund të verifikojë dhe pranojë transaksionin si të vlefshëm, duke konfirmuar që personi që transferon bitcoin i zotëronte ato në kohën e transferimit [13].

3.4.2 Çelësat publik dhe privat

Mënyra se si funksionojnë çelësat publikë dhe privatë është thelbësore për të kuptuar se si funksionojnë transaksionet e kriptovalutave. Kur thoni se keni kriptovalutë, ajo që jeni duke thënë në të vërtetë është se ju keni një çelës privat që vërteton pronësinë e asaj kriptomonedhe [17]. Një portofol bitcoin përmban një koleksion çelësash, secili i përbërë nga një çelës privat dhe një çelës publik. Çelësi privat (k) është një numër, zakonisht zgjidhet rastësisht. Nga çelësi privat, ne përdorim shumëzimin e kurbës eliptike, një funksion kriptografik në një drejtim, për të gjeneruar një çelës publik (K). Nga çelësi publik (K), ne përdorim një funksion hash kriptografik njëkahësh për të gjeneruar një adresë bitcoin (A) [13].

3.4.2.1 Çelsi privat

Një çelës privat ju jep mundësinë të dëshmoni pronësinë ose të shpenzoni fondet e lidhura me adresën tuaj publike. Një çelës privat mund të marrë shumë forma si: kod binar i gjatë 256 karakteresh, kod heksadecimal 64 shifror, QR kod, frazë menemonike (grup fjalësh). Pavarësisht nga forma e tij, një çelës privat është një numër i madh astronomikisht dhe është i madh për një arsye të mirë. Ndërsa mund të gjeneroni një çelës publik me një çelës privat, të bësh të kundërtën është praktikisht e pamundur për shkak të funksionit njëkahësh. Mund të keni një numër çelësash publikë të lidhur me një çelës privat [17]. Softueri Bitcoin përdor gjeneratorët e numrave të rastësishëm të sistemit operativ

themelor për të prodhuar 256 bit entropie (rastësi). Zakonisht, gjeneratori i numrave të rastit në OS (sistemi operativ) inicializohet nga një burim njerëzor i rastësisë, prandaj mund t'ju kërkohet të lëvizni miun për disa sekonda. Më saktësisht, çelësi privat mund të jetë çdo numër ndërmjet 1 dhe n - 1, ku n është një konstante (n = 1.158 * 10^{77}, pak më pak se 2^{256}) e përcaktuar si rendi i kurbës eliptike të përdorur në bitcoin.

3.4.2.2 Çelësi publik

Një çelës publik ju lejon të merrni transaksione kriptovalutash. Është një kod kriptografik që shoqërohet me një çelës privat. Ndërsa çdokush mund të dërgojë transaksione në çelësin publik, ju duhet çelësi privat për t'i "zhbllokuar" ato transaksione dhe për të dëshmuar që ju jeni pronari i kriptovalutës së marrë në transaksion [17]. Çelësi publik llogaritet nga çelësi privat duke përdorur shumëzimin e kurbës eliptike, i cili është një funksion i pakthyeshëm: K = k * G, ku k është çelësi privat, G është një pikë konstante e quajtur pikë gjeneratori, dhe K është çelësi publik që rezulton. Operacioni i kundërt, i njohur si "gjetja e logaritmit diskret" - llogaritja e k nëse e dini K - është po aq e vështirë sa provimi i të gjitha vlerave të mundshme të k, d.m.th., një kërkim me forcë brutale (eng brute force attack) [13].

3.5 Shpjegimi i kriptografisë së kurbës eliptike

Kriptografia e kurbës eliptike është një lloj kriptografie asimetrike ose çelësi publik i bazuar në problemin e logaritmit diskret, siç shprehet me mbledhjen dhe shumëzimin në pikat e një kurbe eliptike. Bitcoin përdor një kurbë specifike eliptike dhe një grup konstantesh matematikore, siç përcaktohet në një standard të quajtur *secp256k1*, themeluar nga Instituti Kombëtar i Standardeve dhe Teknologjisë (NIST). Lakorja *secp256k1* përcaktohet nga funksioni i mëposhtëm, i cili prodhon një kurbë eliptike:

$y^2 = \frac{(x^3+7)}{F_p}$ ose

$y^2 \; mod \; p = (x^3 + 7) \; mod \; p$

Mod p (modulo numër kryesor p) tregon se kjo kurbë është mbi një fushë të fundme të rendit të parë p, e shkruar gjithashtu si p, ku p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1, një numër i madh i thjeshtë (eng prime number). Për shkak se kjo kurbë përcaktohet mbi një fushë të fundme të rendit të parë në vend të numrave realë, duket si një model i pikave të shpërndara në dy dimensione, gjë që e bën të vështirë vizualizimin. Sidoqoftë, matematika është identike me atë të një kurbe eliptike mbi numrat realë [13].

3.6 Bitcoin Adresat

Një adresë Bitcoin është një identifikues unik që shërben si një vendndodhje virtuale ku mund të dërgohet kriptovaluta. Vetë adresa përbëhet nga 26-35 karaktere alfanumerike. Ky varg është gjysma publike e një çifti çelësash asimetrik. Formati standard për një adresë Bitcoin është *P2PKH* (pay to public key hash). Portofolët digjitalë ose klientët Bitcoin krijojnë adresa përmes operacioneve kriptografike, softueri gjeneron një çelës privat përmes një algoritmi nënshkrimi asimetrik dhe më pas nxjerr çelësin publik nga ai privat. Përdoruesi nënshkruan me çelësin privat dhe verifikon atë nënshkrim me çelësin publik [18]. Adresat e prodhuara nga çelësat publikë përbëhen nga një varg numrash dhe shkronjash, duke filluar me shifrën "1". Këtu është një shembull i një adrese bitcoin: *1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy*.

Një adresë bitcoin mund të përfaqësojë pronarin e një çifti çelësash privat/publik, ose mund të përfaqësojë diçka tjetër, të tillë si një skript pagese. Adresa e bitcoin-it rrjedh nga çelësi publik përmes përdorimit të hashimit kriptografik në një drejtim. Një "algoritëm hashing" ose thjesht "algoritmi hash" është një funksion me një drejtim që prodhon një gjurmë gishtash ose "hash" të një hyrje me madhësi arbitrare. Funksionet e hashit kriptografik përdoren gjerësisht në bitcoin: në adresat e bitcoin, në adresat e skriptave dhe në algoritmin e nxjerrjes së provës së punës. Algoritmet e përdorura për të bërë një adresë bitcoin nga një çelës publik janë *Algoritmi i Sigurt Hash* (SHA) dhe përmbledhja e mesazhit të vlerësimit të primitiveve të integritetit *RACE* (RIPEMD), specifikisht *SHA256* dhe *RIPEMD160.* Duke filluar me çelësin publik K, ne llogarisim hashin SHA256 dhe pastaj llogarisim hash RIPEMD160 të rezultatit, duke prodhuar një numër 160 bit (20 bajt):

A = RIPEMD160(SHA256(K))

ku K është çelësi publik dhe A është rezultati adresa bitcoin.

Adresat e Bitcoin janë të enkoduara pothuajse gjithmonë si "Base58Check", sistem i cili përdor 58 karaktere dhe një përmbledhje kontrolli për të ndihmuar lexueshmërinë njerëzore, për të shmangur paqartësinë dhe për të mbrojtur nga gabimet në transkriptimin dhe hyrjen e adresës [13].

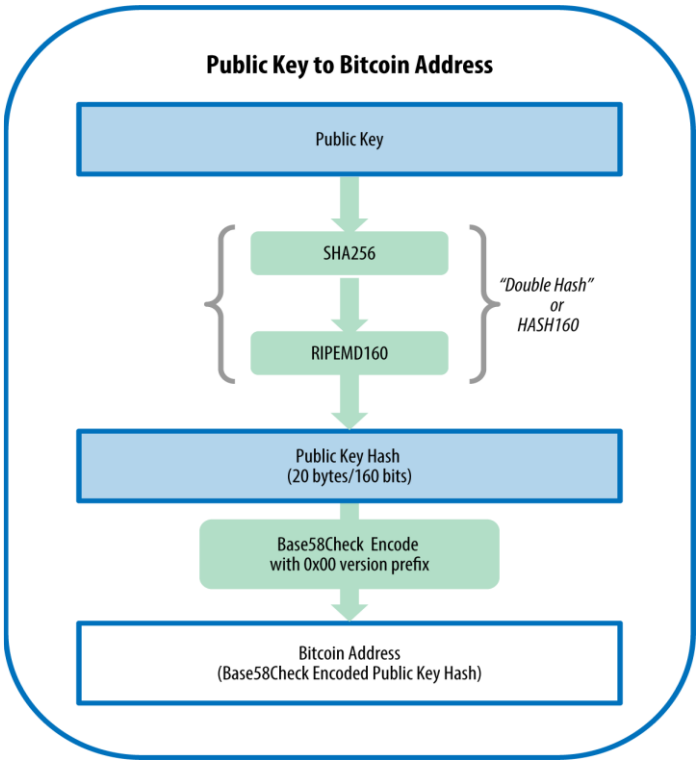

Figura 3. Çelësi publik në adresën e bitcoin, shndërrimi i një çelësi publik në një adresë bitcoin

Figura 3 paraqet procesin e shëndrrimit të një çelsi publik në një adresë Bitcoin, në fillim me anë të procesit të hashimit nga çelsi publik krijohet çelsi publik i hashuar dhe pastaj me anë të procesit të enkodimit me sistemin *Base58Check* fitohet adresa Bitcoin.

3.7 Portofoli Bitcoin

Portofoli Bitcoin paraqet një ndërfaqje elektronike të një përdoruesi në bitcoin-at e tij. Portofoli Bitcoin është softuer në kompjuterin ose pajisjen mobile të përdoruesit. Mund të jetë gjithashtu një pajisje harduerike që bashkëvepron me softuerin në kompjuter dhe mund të jetë një portofol letre. Shumë portofole që mbështesin Bitcoin përdoren gjithashtu për *Ethereum*, *Litecoin* dhe monedha të tjera digjitale. Portofoli mban ekuilibrin Bitcoin të përdoruesit, por nuk përmban monedha. Ai ruan adresën Bitcoin dhe çelësin privat të përdoruesit për të hyrë në Bitcoin blockchain. Kur njerëzit kryejnë pagesa, portofolët përdorin çelësin për të nënshkruar digjitalisht transaksionet që dëshmojnë pronësinë e monedhave të tyre në rrjet, të njohura si "rezultate të transaksioneve të pashpenzuara" UTXO [19]. Nga perspektiva e një programuesi, fjala "portofol" i referohet strukturës së të dhënave që përdoret për të ruajtur dhe menaxhuar çelësat e një përdoruesi [13].

Ekzistojnë dy lloje kryesore të kuletave, të dalluara nga fakti nëse çelësat që ato përmbajnë kanë lidhje me njëri-tjetrin apo jo. Lloji i parë është një portofol jodeterministik, ku secili çelës gjenerohet në mënyrë të pavarur nga një numër i rastësishëm. Çelësat nuk janë të lidhur me njëri-tjetrin. Ky lloj portofoli njihet gjithashtu si një portofol JBOK nga fraza "Just a Bunch Of Keys". Lloji i dytë i portofolit është një portofol përcaktues, ku të gjithë çelësat rrjedhin nga një çelës i vetëm kryesor, i njohur si fara (eng seed). Të gjithë çelësat në këtë lloj portofoli janë të lidhur me njëri-tjetrin dhe mund të gjenerohen përsëri nëse dikush ka farën origjinale. Ekzistojnë një numër metodash të ndryshme kryesore të derivimit të përdorura në kuletat përcaktuese. Metoda e derivimit që përdoret më shpesh përdor një strukturë të ngjashme me pemën dhe njihet si një portofol hierarkik përcaktues ose portofoli HD (eng hierarcic directory). Kuletat përcaktuese u krijuan për ta bërë më të lehtë nxjerrjen e shumë çelësave nga një "farë" e vetme. Forma më e përparuar e kuletave përcaktuese është portofoli HD i përcaktuar nga standardi BIP-32. Kuletat HD përmbajnë çelësa që rrjedhin nga një strukturë peme, e tillë që një çelës prind mund të nxjerrë një sekuencë çelësash për fëmijë, secila prej të cilave mund të nxjerrë një sekuencë çelësash të nipërve, dhe kështu me radhë. Kuletat HD ofrojnë dy avantazhe kryesore ndaj çelësave të rastësishëm (jodeterministik). Së pari, struktura e pemës mund të përdoret për të shprehur kuptimin shtesë organizativ, të tilla si kur një degë specifike e nën-çelësave përdoret për të marrë pagesa hyrëse dhe një degë tjetër përdoret për të marrë ndryshim nga pagesat në dalje. Degët e çelësave mund të përdoren gjithashtu në mjediset e korporatave, duke alokuar degë të ndryshme në departamente, filiale, funksione specifike ose kategori të kontabilitetit. Avantazhi i dytë i kuletave HD është se përdoruesit mund të krijojnë një sekuencë çelësash publikë pa pasur qasje në çelësat përkatës privatë. Kjo lejon që kuletat HD të përdoren në një server të pasigurt ose në një kapacitet vetëm të marrjes, duke lëshuar një çelës tjetër publik për çdo transaksion. Çelësat publikë nuk kanë nevojë të ngarkohen paraprakisht ose të nxirren paraprakisht, megjithatë serveri nuk ka çelësat privatë që mund të shpenzojnë fondet [13].

Një nga portofolët Bitcoin më të mira në treg është *Exodus* i cili është falas për t'u blerë. Exodus është një portofol desktop dhe celular me një ndërfaqe përdorimi shumë të thjeshtë dhe një shkëmbim të integruar. Një nga tiparet më të njohura të Exodus është aftësia për të ndërruar një numër në rritje të kriptovalutave. Exodus aktualisht lejon shkëmbime midis mbi 100 monedhave të ndryshme virtuale. Ndërsa është i shkëlqyeshëm për fillestarët, përdoruesit më të përparuar mund ta shohin se mungon një veçori e

rëndësishme. Së pari, Exodus është një portofol me burim të mbyllur. Një tjetër portofol me përdorim të madhë është edhe *Electrum*, portofol ky që është në përdorim qysh nga viti 2011, dy vjet pas krijimit të Bitcoin, dhe që nga atëherë ka pak ndryshime. Ndërsa ky portofol është i zhveshur për sa i përket ndërfaqes së tij të përdoruesit dhe angazhimit të tij vetëm për Bitcoin, ai shkëlqen në këtë funksion kryesor. Electrum është gjithashtu më i përshtatshëm për përdoruesit e përparuar për shkak të opsioneve të tij komplekse [20]. Përveç këtyre portofoleve ekzistojnë edhe shumë portofole tjera Bitcoin të cilat japin opsione të ndryshme për operimin me bitcoin.

3.8 Bitcoin Transaksionet

Transaksionet janë pjesa më e rëndësishme e sistemit bitcoin. Çdo gjë tjetër në bitcoin është krijuar për të siguruar që transaksionet mund të krijohen, përhapen në rrjet, vërtetohen dhe më në fund shtohen në regjistrin kryesor të transaksioneve (blockchain). Transaksionet janë struktura të të dhënave që kodifikojnë transferimin e vlerës midis pjesëmarrësve në sistemin bitcoin. Çdo transaksion është një hyrje publike në bllokun-zinxhiror Bitcoin. Blloku themelor i një transaksioni me bitcoin është një transaksion i daljes (eng transaction output). Daljet e transaksionit janë pjesë të pandashme të monedhës bitcoin, të regjistruara në blockchain dhe të njohura si të vlefshme nga i gjithë rrjeti. Nyjet e plota Bitcoin ndjekin të gjitha daljet e disponueshme dhe të harxhueshme, të njohura si rezultate të transaksioneve të pashpenzuara, ose UTXO. Mbledhja e të gjithë UTXO është e njohur si grupi UTXO dhe aktualisht numëron në miliona UTXO. Seti UTXO rritet ndërsa UTXO të reja krijohen dhe zvogëlohet kur konsumohen UTXO. Çdo transaksion përfaqëson një ndryshim (tranzicion gjendje) në grupin UTXO. Kur themi se portofoli i një përdoruesi ka "marrë" bitcoin, ajo që duam të themi është se portofoli ka zbuluar një UTXO që mund të shpenzohet me një nga çelësat e kontrolluar nga ai portofol. Kështu, "bilanci" bitcoin i një përdoruesi është shuma e të gjithë UTXO që mund të shpenzojë portofoli i përdoruesit dhe që mund të shpërndahet midis qindra transaksioneve dhe qindra blloqeve. Koncepti i një ekuilibri krijohet nga aplikacioni i portofolit. Portofoli llogarit ekuilibrin e përdoruesit duke skanuar Bitcoin blockchain dhe duke grumbulluar vlerën e çdo UTXO që portofoli mund të shpenzojë me çelësat që kontrollon. Shumica e kuletave mbajnë një bazë të dhënash ose përdorin një shërbim të bazës së të dhënave për të ruajtur një grup të shpejtë referimi të të gjithë UTXO-ve që ata mund të shpenzojnë me çelësat që kontrollojnë. Nëse një UTXO është më i madh se vlera e dëshiruar e një transaksioni, ai përsëri duhet të konsumohet në tërësinë e tij dhe ndryshimi duhet të

gjenerohet në transaksion. Me fjalë të tjera, nëse keni një UTXO me vlerë 20 bitcoin dhe doni të paguani vetëm 1 bitcoin, transaksioni juaj duhet të konsumojë të gjithë UTXO me 20 bitcoin dhe të prodhojë dy rezultate: një që paguan 1 bitcoin te marrësi juaj i dëshiruar dhe një tjetër që paguan 19 bitcoin në ndryshim përsëri në portofolin tuaj. Si rezultat i natyrës së pandarë të rezultateve të transaksioneve, shumica e transaksioneve me bitcoin do të duhet të gjenerojnë ndryshime. Përjashtim nga zinxhiri i prodhimit dhe hyrjes është një lloj i veçantë transaksioni i quajtur transaksioni i monedhës (eng coinbase transaction), i cili është transaksioni i parë në secilin bllok. Ky transaksion vendoset atje nga minatori "fitues" dhe krijon një bitcoin të ri të pagueshëm për atë minator si shpërblim për minimet. Ky transaksion i veçantë i monedhës nuk konsumon UTXO; në vend të kësaj, ai ka një lloj të veçantë të hyrjeve të quajtura "baza e monedhës". Kjo është mënyra se si krijohet furnizimi i parave të bitcoin gjatë procesit të minimeve [13].

3.8.1 Validimi i Transaksioneve

Një nga gjërat më të ndërlikuara për t'u koduar në Bitcoin është vërtetimi i transaksioneve. Një tjetër është krijimi i transaksioneve. Çdo nyje, kur merr transaksione, sigurohet që secili transaksion t'i përmbahet rregullave të rrjetit. Ky proces quhet vërtetim i transaksionit. Këto janë gjërat kryesore që një nyje kontrollon:

1. Hyrjet e transaksionit janë shpenzuar më parë.

2. Shuma e hyrjeve është më e madhe ose e barabartë me shumën e daljeve.

3. ScriptSig (nënshkrimi digjital ose çelsi privat) zhbllokon me sukses ScriptPubKey (çelsin publik) e mëparshme.

1 parandalon shpenzimet e dyfishta. Çdo hyrje që është shpenzuar (d.m.th., i përfshirë në bllok zinxhir) nuk mund të harxhohet përsëri.

2 siguron që nuk krijohen bitcoin të reja (përveç në një lloj të veçantë transaksioni të quajtur transaksioni i monedhës).

3 siguron që skripta e kombinuar është e vlefshëm. Në shumicën dërrmuese të transaksioneve, kjo do të thotë të kontrollosh që një ose më shumë nënshkrime në ScriptSig janë të vlefshme [21].

3.8.1.1 Kontrollimi i shpenzimeve të hyrjes

Për të parandaluar shpenzimet e dyfishta, një nyje kontrollon çdo hyrje që ekziston dhe nuk është shpenzuar. Kjo mund të kontrollohet nga çdo nyje e plotë duke parë setin UTXO. Ne nuk mund të përcaktojmë nga vetë transaksioni nëse është shpenzim i dyfishtë. Mënyra e vetme për të ditur është të kesh akses në grupin UTXO, i cili kërkon llogaritjen nga i gjithë grupi i transaksioneve. Në Bitcoin, ne mund të përcaktojmë nëse një hyrje po shpenzohet dyfish duke mbajtur nën kontroll UTXO-të. Nëse një hyrje është në grupin UTXO, ajo hyrje e transaksionit ekziston si dhe nuk është me shpenzime të dyfishta. Nëse transaksioni kalon pjesën tjetër të testeve të vlefshmërisë, atëherë ne heqim të gjitha hyrjet e transaksionit nga grupi UTXO. Klientët e ri që nuk kanë qasje në blockchain duhet të kenë besim në nyjet e tjera për shumë informacione, përfshirë këtu nëse një hyrje është shpenzuar tashmë [21].

3.8.1.2 Kontrollimi i shumës së hyrjeve kundër shumës së daljeve

Nyjet gjithashtu sigurohen që shuma e hyrjeve është më e madhe ose e barabartë me shumën e daljeve. Kjo siguron që transaksioni nuk krijon monedha të reja. Një përjashtim është transaksioni i monedhës. Meqenëse hyrjet nuk kanë një fushë sasie, kjo duhet të shikohet në blockchain. Edhe një herë, nyjet e plota kanë qasje në shumat e shoqëruara me prodhimin e pashpenzuar, por klientët e ri duhet të varen nga nyjet e plota për t'u furnizuar me këtë informacion [21].

3.8.1.3 Kontrollimi i nënshkrimit digjital

Ndoshta pjesa më e ndërlikuar e vërtetimit të një transaksioni është procesi i kontrollit të nënshkrimeve të tij. Një transaksion zakonisht ka të paktën një nënshkrim për hyrje. Algoritmi i nënshkrimit kërkon çelësin publik P, nënshkrimin hash z dhe nënshkrimin (r, s). Pasi të dihen këto, procesi i verifikimit të nënshkrimit është shumë i thjeshtë [21].

3.8.2 Krijimi i Transaksioneve

Ne mund të krijojmë transaksione që përshtaten me procesin e verifikimit. Transaksionet që ne krijojmë do të kërkojnë që shuma e hyrjeve të jetë më e madhe ose e barabartë me shumën e daljeve. Në mënyrë të ngjashme, transaksionet që ne krijojmë do të kërkojnë një ScriptSig që, kur kombinohet me Script-PubKey, do të jetë i vlefshëm. Për të krijuar një transaksion, na duhet të paktën një dalje që kemi marrë.

Ndërtimi i një transaksioni kërkon përgjigjjen e disa pyetjeve themelore:

1. Ku duam të shkojnë bitcoin?

2. Çfarë UTXO mund të shpenzojmë?

3. Sa shpejt duam që ky transaksion të futet në blockchain?

Pyetja e parë ka të bëjë me atë se sa duam të paguajmë kë. Ne mund të paguajmë një ose më shumë adresa. Për shembull, ne do të paguajmë 0.1 testnet bitcoin (tBTC) tek adresa mnrVtF8DWjMu839VW3rBfgYaAfKk8983Xf nga adresa jonë në këtë shembull, mzx5YhAH9kNHtcN481u6WkjeHjYtVeKVh2.

Pyetja e dytë ka të bëjë me atë që ka në portofolin tonë. Çfarë kemi në dispozicion për të shpenzuar? Në këtë shembull, ne kemi një dalje të shënuar me një ID të transaksionit që në shembull ka 0.44 tBTC testnet bitcoin vlerë dhe posedon indeksin e prodhimit: 0d6fe5213c0b3291f208cba8bfb59b7476dffacc4e5cb66f6eb20a080843a299: 13

Meqenëse kjo është më shumë se 0,1 tBTC, ne do të dëshirojmë që pjesën tjetër ta kthejmë tek vetja. Megjithëse është praktikë e keqe e privatësisë dhe e sigurisë për të ripërdorur adresat, ne do të i dërgojmë bitcoin valutat tona përsëri në adresën tonë mzx5YhAH9kNHtcN481u6WkjeHjYtVeKVh2 për ta bërë më të lehtë ndërtimin e transaksionit.

Pyetja e tretë ka të bëjë me tarifat. Nëse duam ta marrim më shpejt transaksionin në zinxhirin e bllokut, do të duhet të paguajmë më shumë tarifa; nëse nuk e kemi problem të presim, mund të paguajmë më pak. Në shembullin tonë, ne do të përdorim 0,01 tBTC si tarifë [21].

3.9 Prova e punës – Proof-of-Work

Prova e punës është ajo që siguron sistemin Bitcoin dhe, në një nivel të thellë, lejon që të funksionojnë minierat e decentralizuara të Bitcoin. Gjetja e një prove për punën i jep një minatori të drejtën të vendosë bllokun e bashkangjitur në blockchain. Meqenëse prova e punës është shumë e rrallë, kjo nuk është një detyrë e lehtë. Por për shkak se prova e punës është objektive dhe e lehtë për t'u verifikuar, çdokush mund të jetë minator nëse zgjedh kështu. Prova e punës quhet "minim" për një arsye shumë të mirë. Ashtu si me minierat fizike, ka diçka që minatorët po kërkojnë. Një operacion tipik i minierave të arit përpunon 45 ton papastërti dhe gurë përpara se të grumbullojë 1 gram ar. Kjo sepse ari është shumë i rrallë. Sidoqoftë, sapo të gjendet ari, është shumë e lehtë të verifikoni që

ari është i vërtetë. Ekzistojnë teste kimike, gurë prekës dhe shumë mënyra të tjera për të treguar relativisht lirë nëse minerali i gjetur është ari. Në mënyrë të ngjashme, prova e punës është një numër që siguron një rezultat shumë të rrallë. Për të gjetur një provë të punës, minatorët në rrjetin Bitcoin duhet të rrëmbejnë ekuivalentin numerik të papastërtisë dhe shkëmbit. Ashtu si me arin, verifikimi i provës së punës është shumë më i lehtë sesa gjetja e tij. Procesi i gjetjes së provës së punës kërkon që ne të përpunojmë rreth 10^{22} copa numerike të papastërtive dhe shkëmbinjve për të gjetur copën tonë numerike të arit [21].

Gjetja e provës fituese të punës është kaq e vështirë, mënyra e vetme për të siguruar punën e minatorëve për të fituar bitcoin është me kompjutera të shtrenjtë dhe të specializuar. Minatorët do të fitojnë bitcoin nëse punojnë për një llogaritje që përputhet. Sa më shumë llogaritje të krijojnë, aq më shumë bitcoin ka të ngjarë të fitojnë.

Çfarë llogaritjesh po bëjnë minatorët saktësisht? Në Bitcoin, minatorët nxjerrin të ashtuquajturin "hash", i cili kthen një hyrje në një varg shkronjash dhe numrash që duken rastësisht.

Qëllimi i minatorëve është të krijojnë një hash që përputhet me "synimin" aktual të Bitcoin. Ata duhet të krijojnë një hash me zero mjaftueshëm përpara. Mundësia për të marrë disa zero rresht është shumë e ulët. Por minatorët në të gjithë botën po bëjnë triliona llogaritje të tilla në sekondë, kështu që u duhen rreth 10 minuta mesatarisht për të arritur këtë objektiv.

Kushdo që arrin qëllimin i pari fiton një grumbull kriptomonedha bitcoin. Pastaj protokolli Bitcoin krijon një vlerë të re që minatorët duhet të hash-ojnë, dhe minatorët fillojnë garën për gjetjen e provës së punës fituese përsëri [22].

4 Ethereum dhe kontratat e mençura

Nga perspektiva e shkencës kompjuterike, Ethereum është praktikisht një makinë me gjendje të pakifizuar, duke konsistuar në një gjendje të çasshme globalishtë dhe një makinë virtuale që zbaton ndryshimet tek ajo gjendje. Nga një perspektivë më praktike, Ethereum është një burim i hapur, infrastrukturë kompjuterike e decentralizuar globalisht që ekzekuton programe të quajtura kontrata inteligjente. Ethereum përdor një bllok zinxhir (Ethereum blockchain) për të sinkronizuar dhe ruajtur ndryshimet e gjendjes së sistemit, së bashku me një kriptovalutë të quajtur *ether* për të matur dhe kufizuar kostot e burimeve të ekzekutimit. Platforma Ethereum u mundëson zhvilluesve të ndërtojnë aplikacione të fuqishme të decentralizuara me funksione të integruara ekonomike. Ndërsa siguron disponueshmëri të lartë, auditueshmëri, transparencë dhe neutralitet, ajo gjithashtu zvogëlon ose eliminon censurimin dhe zvogëlon rreziqet e caktuara të palës tjetër. Qëllimi i Ethereum nuk është kryesisht të jetë një rrjet i pagesave të monedhës dixhitale. Ndërsa valuta digjitale ether është integrale dhe e domosdoshëme për funksionimin e Ethereum, ether është menduar si një monedhë e dobishme për të paguar për përdorimin e platformës Ethereum [23].

Në fillim, blockchain kishte të bënte me një lloj të ri të monedhës elektronike. Por tani, pjesërisht falë Ethereum, blockchain është shumë më tepër sesa një mënyrë e re për të paguar gjërat. Është një mënyrë e re për të menduar për gjërat. Kjo u mundëson njerëzve dhe bizneseve të kryejnë biznes pa shumë nga pengesat që kanë ekzistuar në marrëdhëniet tregtare me shekuj [24]. Ethereum është dizenjuar të jetë një platformë blockchain e programueshëme me qëllim të përgjithshëm që drejton një makinë virtuale të aftë për të ekzekutuar kod me kompleksitet arbitrar dhe të pakufizuar. Ethereum u krijua në një kohë kur njerëzit njohën fuqinë e modelit Bitcoin dhe po përpiqeshin të lëviznin përtej aplikacioneve të kriptovalutave [23]. Në vitin 2013, *Vitalik Buterin* një programer i ri dhe entuziast i Bitcoin teknologjisë, themeluesi i *Bitcoin Magazine,* botoi një letër që propozoi një zbatim të ri, më funksional të blockchain teknologjisë. Ky propozim i ri ishte për zinxhirin blockchain të Ethereumit. Vitalik Buterin, filloi të mendojë për zgjerimin e mëtejshëm të aftësive të Bitcoin dhe *Mastercoin* (një protokoll mbivendosje që zgjeroi Bitcoin për të ofruar kontrata të mençura). Në tetor të atij viti, Vitalik propozoi një qasje më të përgjithësuar për ekipin *Mastercoin*, një qasje që lejoi kontrata fleksibile dhe të shkruara për të zëvendësuar gjuhën e specializuar të kontratës së *Mastercoin*. Ndërsa ekipi i *Mastercoin* ishte i impresionuar, ky propozim ishte një ndryshim shumë radikal për t'u

futur në hartën e tyre të zhvillimit [23]. Pas fitimit të interesit dhe tërheqjes së mbështetjes teknike dhe financiare, *Ethereum Foundation*, një organizatë zvicerane jofitimprurëse, u themelua dhe u bë zhvilluesi i Ethereum. Ethereum nuk u krijua vetëm për të shkëmbyer kriptovaluta. Në fakt, ai ishte projektuar që nga fillimi për të qenë i ndryshëm. Karakteristikat thelbësore të Ethereum janë kontrata inteligjente dhe etheri. Ether është kriptovaluta vendase që mbështet Ethereum-in, edhe pse mund të krijoni vlerat (eng tokens) tuaja për të shkëmbyer vlerën në shumë forma të tjera. Kontratat inteligjente sigurojnë një mjedis ekzekutimi që siguron integritetin në të gjitha nyjet. Çdo kod që ekzekutohet në një nyje ekzekutohet në të njëjtën mënyrë në të gjitha nyjet. Kjo garanci bën të mundur vendosjen e një game të gjerë aplikimesh nëpër mjedise të pasigurta. Ethereum është një platformë aplikimi gjithëpërfshirëse, e decentralizuar që zgjeron gamën e aftësive përtej asaj që ishte e mundur para teknologjisë blockchain. Ndërsa zgjidhjet e trashëguara për të dhënat dhe ndarjen e proceseve kërkonin autoritetet e palëve të treta për të zbatuar integritetin, Ethereum siguron procesin dhe integritetin e të dhënave, së bashku me opsionin që të dhënat të shkëmbehen pa palën e tretë [24].

Ethereum është gjithashtu një makinë e gjendjes së shpërndarë. Por në vend që të gjurmojë vetëm gjendjen e pronësisë së monedhës, Ethereum gjurmon tranzicionet e gjendjes së një dyqani të dhënash me qëllim të përgjithshëm, d.m.th. një dyqan që mund të mbajë çdo të dhënë të shprehshme si një palë me vlerë kryesore. Një dyqan i të dhënave me vlerë kyçe mban vlera arbitrare, secila referohet nga ndonjë çelës, për shembull, vlera "Produkti 100" referohet nga çelësi "Emri i dyqanit". Në disa mënyra, kjo shërben për të njëjtin qëllim si modeli i ruajtjes së të dhënave të memories (RAM) i përdorur nga shumica e kompjuterëve me qëllim të përgjithshëm. Ethereum ka memorie që ruan kodet dhe të dhënat, dhe përdor Ethereum blockchain për të gjurmuar se si ndryshon kjo kujtesë me kalimin e kohës. Ashtu si një kompjuter me program të ruajtur për qëllime të përgjithshme, Ethereum mund të ngarkojë kodin në makinerinë e tij të gjendjes dhe ta ekzekutojë atë kod, duke ruajtur ndryshimet e gjendjes që rezultojnë në blockchain-in e tij. Dy nga ndryshimet kritike nga shumica e kompjuterëve me qëllim të përgjithshëm janë se ndryshimet e gjendjes Ethereum rregullohen nga rregullat e konsensusit dhe gjendja shpërndahet globalisht. Ethereum përgjigjet në pyetjen: "Po sikur të mund të gjurmonim ndonjë gjendje arbitrare dhe të programonim makinerinë e gjendjes për të krijuar një kompjuter në të gjithë botën që funksionon nën një konsensus?". Risia e Ethereum është ndërthurja e arkitekturës informatike me qëllim të përgjithshëm të një

kompjuteri të programit të ruajtur me një blockchain të decentralizuar, duke krijuar kështu një kompjuter botëror të shpërndarë në një gjendje [23].

Ethereum përcakton etherin si kriptomonedhën e tij. Ju mund të transferoni ether midis llogarive ose ta fitoni atë duke bërë punën e vështirë për të shtuar blloqe në bllokun e zinxhirit Ethereum. Mekanizmi Ethereum PoW (Proof-of-Work) kërkon që nyjet të gjejnë një numër që, kur kombinohet me të dhënat e kokës së bllokut, prodhon një vlerë hash kriptografike që përputhet me synimin aktual, e cila është një vlerë që rregullohet për të mbajtur prodhimin e bllokut të ri në një normë të qëndrueshme. Gjetja e një vlere hash që përputhet me synimin aktual është e vështirë. Duhet të provosh mesatarisht më shumë se një kuadrilion vlera për të gjetur atë të duhurën. Përdorimi i një mekanizmi PoW e bën kaq të vështirë dorëzimin e një blloku kështu që dorëzohen më pak blloqe, gjë që zvogëlon numrin e përplasjeve. Nyja që gjen vlerën e duhur merr një pagesë të vogël etheri për përpjekjen. Ky proces quhet minim, dhe nyja që fiton çmimin është minatori i atij blloku. Minimi rregullon shpejtësinë me të cilën blloqet e reja paraqiten si blloqe kandidate dhe rezulton në një numër që është i lehtë për t'u vërtetuar. Gjetja e numrit të duhur për të zgjidhur enigmën është e vështirë, por verifikimi i numrit është i shpejtë dhe i lehtë. Një aspekt tjetër interesant i minimeve është se koka e çdo blloku përmban një hash nga blloku i mëparshëm. Nyjet Ethereum përdorin hashin për të zbuluar lehtësisht ndryshimet e bllokut të paautorizuar. Nëse një bllok ndryshon, rezultati i hashit nuk përputhet dhe blloku bëhet i pavlefshëm. Minimi është gjithashtu një mënyrë për të fituar para duke përdorur teknologjinë blockchain. Minimet janë bërë konkurruese dhe shumica e minatorëve të sotëm investojnë në pajisje me performancë të lartë me GPU të shumta për të kryer operacionet komplekse. Për ta mbajtur të drejtë procesin e minimeve, Ethereum përdor një vlerë kompleksiteti që e bën procesin e minimeve edhe më të vështirë ndërsa minatorët bëhen më të shpejtë. Rregullimi i kompleksitetit lejon Ethereum të rregullojë frekuencën e bllokut të ri në një mesatare prej një blloku të ri çdo 14 sekonda [24].

4.1 Prova e Aksioneve – Proof-Of-Stake (PoS)

Prova e aksioneve është një lloj mekanizmi konsensual i përdorur nga rrjetet blockchain për të arritur konsensusin e shpërndarë. Kërkon që përdoruesit të marrin pjesë në Ethereum për t'u bërë një vlerësues në rrjet. Vlerësuesit janë përgjegjës për të njëjtën gjë si minatorët në provën e punës: renditjen e transaksioneve dhe krijimin e blloqeve të reja

në mënyrë që të gjitha nyjet të mund të bien dakord për gjendjen e rrjetit. Prova e aksioneve vjen me një numër përmirësimesh nga sistemi i provës së punës:

- efikasitet më të mirë të energjisë - nuk keni nevojë të përdorni shumë energji të blloqeve
- pengesa më të ulëta për hyrje, kërkesa të reduktuara për pajisje - nuk ju nevojiten pajisje elitare për të patur një shans për të krijuar blloqe të reja
- imunitet më i fortë ndaj centralizimit - prova e aksioneve duhet të çojë në më shumë nyje në rrjet
- mbështetje më e fortë për zinxhirët veçmas - një azhurnim kryesor në shkallëzimin e rrjetit Ethereum

Ndryshe nga prova e punës, vlerësuesit nuk kanë nevojë të përdorin sasi të konsiderueshme të fuqisë llogaritëse sepse ata janë zgjedhur në mënyrë të rastësishme dhe nuk konkurrojnë. Ata nuk kanë nevojë të minojnë blloqet, ata thjesht duhet të krijojnë blloqe kur zgjidhen dhe të vërtetojnë blloqet e propozuara kur nuk janë të zgjidhur [26].

4.2 Kontratat e mençura

Kontratat inteligjente janë një pjesë e rëndësishme e një kornize blockchain. Duke përdorur ato, njerëzit mund të tregtojnë në Internet pa pasur nevojë për një ndërmjetës. Ato nuk qeverisen nga autoritetet qendrore dhe as nga ndërhyrja njerëzore. Kontratat inteligjente janë kontrata vetë-ekzekutuese me kushtet e kontratës ndërmjet blerësit dhe shitësit të shkruara drejtpërdrejt në rreshta të kodit. Kontratat inteligjente lejojnë që transaksionet dhe marrëveshjet e besueshme të kryhen midis palëve të ndryshme, anonime pa pasur nevojë për një autoritet qendror, sistem ligjor ose mekanizëm të jashtëm të zbatimit. Ato i bëjnë transaksionet të gjurmueshme, transparente dhe të pakthyeshme [25]. Termi kontratë inteligjente është përdorur gjatë viteve për të përshkruar një larmi të gjërave të ndryshme. Në vitet 1990, kriptografi *Nick Szabo* shpiku termin dhe e përcaktoi atë si "një grup premtimesh, të specifikuara në formë dixhitale, përfshirë protokollet brenda të cilave palët kryejnë premtimet e tjera". Që atëherë, koncepti i kontratave inteligjente ka evoluar, veçanërisht pas prezantimit të platformave të decentralizuara me shpikjen e Bitcoin blockchain në vitin 2009. Në kontekstin e Ethereum, termi në të vërtetë është pak i gabuar, duke pasur parasysh se kontratat inteligjente Ethereum nuk janë as kontrata të zgjuara dhe as ligjore, por termi ka ngecur [23]. Kontratat inteligjente ju ndihmojnë të zbatoni rregulla kur shkëmbeni ndonjë gjë me vlerë në Ethereum. Mënyra

më e thjeshtë për të përshkruar kontratat inteligjente është se ato janë programe që ekzekutohen kur ndodhin transaksione të caktuara. Për shembull, nëse krijoni një kontratë inteligjente për blerjen e pijeve freskuese, ai kod softueri do të ekzekutohet sa herë që dikush blen një pije freskuese. Kodi i kontratës inteligjente është ruajtur në blockchain, kështu që të gjitha nyjet kanë një kopje të tij. Gjithashtu, nuk ka rëndësi se ku ekzekutohet softueri, të gjitha nyjet janë të garantuara për ta ekzekutuar njësoj dhe për të marrë të njëjtat rezultate si çdo nyje tjetër. Kontratat inteligjente ofrojnë qeverisjen dhe parashikueshmërinë e Ethereum. Pa to, Ethereum do të ishte thjesht një teknikë magazinimi e shpërndarë (eng distributed storage technique). Por me to, Ethereum është një platformë e qëndrueshme e decentralizuar që mbështet bashkëveprimet dhe shkëmbimet midis përdoruesve jo besues, duke përfshirë transaksione jashtëzakonisht komplekse. Është e lehtë të shohësh hapat e nevojshëm për të blerë një pije freskuese. Transaksionet e tjera, të tilla si transaksionet e pasurive të patundshme, janë shumë më komplekse, kanë shumë varësi dhe kërkesa, dhe zakonisht përfshijnë disa njerëz dhe organizata. Kontratat inteligjente Ethereum mund të ndihmojnë zhvilluesit të krijojnë softuer që eliminon ndërmjetësuesit, rregullon proceset komplekse dhe zvogëlon koston e përgjithshme dhe kohën e nevojshme për të përfunduar edhe shkëmbimet më komplekse [24].

Kontratat inteligjente zakonisht shkruhen në një gjuhë të nivelit të lartë, siç është *Solidity*. Por në mënyrë që të ekzekutohen, ato duhet të përpilohen në nivel të ulët të kodit "*bytecode"* që ekzekutohet në EVM (Ethereum Virtual Machine). Pasi të përpilohen, ato vendosen në platformën Ethereum duke përdorur një transaksion të veçantë për krijimin e kontratës, i cili identifikohet si i tillë duke u dërguar në adresën speciale të krijimit të kontratës. Çdo kontratë identifikohet nga një adresë Ethereum, e cila rrjedh nga transaksioni i krijimit të kontratës si funksion i llogarisë origjinuese dhe numrit identifikues (nonce). Adresa Ethereum e një kontrate mund të përdoret në një transaksion si marrës, duke dërguar fonde në kontratë ose duke thirrur një nga funksionet e kontratës. Kontratat ekzekutohen vetëm nëse ato thirren nga një transaksion. Një kontratë mund të thërrasë një kontratë tjetër që mund të thërrasë një kontratë tjetër, dhe kështu me radhë, por kontrata e parë në një zinxhir të tillë të ekzekutimit do të jetë thirrur gjithmonë nga një transaksion në një nga nyjet në Ethereum blockchain. Kontratat nuk funksionojnë kurrë "më vete" ose "në prapavijë". Kontratat në mënyrë efektive qëndrojnë në gjumë derisa një transaksion të shkaktojë ekzekutimin, qoftë direkt ose indirekt si pjesë e një

zinxhiri thirrjesh të kontratës. Transaksionet janë atomike, pavarësisht nga sa kontrata ato thërrasin ose çfarë bëjnë ato kontrata kur thirren. Transaksionet ekzekutohen në tërësinë e tyre, me çdo ndryshim në gjendjen globale (kontrata, llogari, etj.) Të regjistruara vetëm nëse i gjithë ekzekutimi përfundon me sukses. Përfundimi i suksesshëm do të thotë që programi ekzekutohet pa ndonjë gabim dhe ka arritur në fund të ekzekutimit. Nëse ekzekutimi dështon për shkak të një gabimi, të gjitha efektet e tij (ndryshimet në gjendje) "rikthehen përsëri" sikur transaksioni të mos ekzekutohej kurrë. Kodi i kontratës nuk mund të ndryshohet. Sidoqoftë, një kontratë mund të "fshihet", duke hequr kodin dhe gjendjen e saj të brendshme nga adresa e saj, duke lënë një llogari të zbrazët. Çdo transaksion i dërguar në atë adresë llogarie pasi kontrata është fshirë nuk rezulton në ndonjë ekzekutim të kodit, sepse atje nuk ka më asnjë kod për t'u ekzekutuar [23].

4.2.1 Solidity – gjuha e kontratave të mençura

Kontratat inteligjente janë programe softuerike. Me burime të mjaftueshme, kontratat inteligjente mund të bëjnë gjithçka që mund të bëjë çdo softuer tjetër. Ju mund të shkruani kontrata inteligjente Ethereum në disa gjuhë si: LLL, Serpent, Bamboo, Viper, Solidity e disa të tjera. Solidity është gjuha më e njohur e përdorurë për kontratat inteligjente dhe që ka më shumë të ngjarë të hasni në kontratat e mençura [24]. Solidity është gjuha zyrtare dhe më e përdorur gjerësisht në rrjetin Ethereum, duke e përdorur atë, shkruhen kontrata inteligjente për të cilat bien dakord dy palë [25]. Në shembullin vijues paraqitet një kod shumë i thjeshtë i kontratës intelegjente.

```
pragma solidity ^0.4.25;

contract helloWorld {

    function printHelloworld () public constant returns (string) {

        return 'Hello World!';

    }

}
```

Kështu duket një kontratë inteligjente në gjuhën Solidity. Pas titullit, ju përcaktoni kontratën tuaj, dhe pastaj çdo funksion që përbëjnë funksionimet e brendshme të programit. Pasi të shkruani dhe testoni një kontratë inteligjente, mund ta vendosni në një blockchain dhe më pas ta ekzekutoni. Kur të merrni të gjitha daljet në rregull, kontrata juaj e zgjuar do t'ju tregojë mesazhin ikonik "Hello World!". Ndërsa mësoni më shumë

rreth Solidity, do të shihni se duket shumë si JavaScript por gjithashtu ndihet pak si C ++ dhe Python. Zhvilluesit e Solidity e bazuan gjuhën në të tre gjuhët. Ajo mbështet trashëgiminë, libraritë dhe llojet e përcaktuara nga përdoruesit që mund të jenë mjaft komplekse. Është gjithashtu një gjuhë me tipe statike të të dhënave, që do të thotë që ju duhet të siguroni lloje të dhënash të qarta për variablat që krijoni dhe përdorni. Mbi të gjitha, Solidity është një gjuhë e zgjuar e zhvillimit të kontratës. Edhe pse duket si gjuhët e tjera programuese, ajo përfshin tipe primitive dhe një orientim të krijuar për të bashkëvepruar me rrjetin Ethereum blockchain [24]. Solidity vjen me përpiluesin (eng compiler) e vet që gjeneron kod të nivelit *bytecode* që mund të ekzekutohet në EVM [25].

4.3 Makina Virtuale Ethereum

Gjuhët programuese të tilla si *Java* dhe *Solidity*, ekzistojnë ndërmjet gjuhëve të përpiluara dhe të interpretuara. Ju përpiloni programet që shkruani në të dyja këto gjuhë, por përpiloni kodin tuaj burimor në *opcode*, i quajtur gjithashtu *bytecode*. *Opcode* është një sekuencë e optimizuar e operacioneve që mund të kuptojë mjedisi i kohës së gjuhës suaj (eng machine environment). Mjedisi i kohës së funksionimit shpesh quhet si makina virtuale e gjuhës. Në Java, programet ekzekutohen në makinën virtuale Java (JVM). Të gjitha kontratat inteligjente të Solidity funksionojnë në makinerinë virtuale Ethereum (EVM) [24]. Ethereum Virtual Machine është një makinë llogaritëse, jo shumë e ndryshme nga makinat virtuale të Microsoft .NET Framework [23]. EVM është i pranishëm në të gjitha nyjet. Kur instaloni Ethereum, ju merrni automatikisht EVM, dhe ekzekutohet sa herë që përdorni Ethereum. Kjo do të thotë se çdo herë që ekzekutohet një kontratë inteligjente, ajo ekzekutohet në të gjitha EVM në të gjithë rrjetin Ethereum. Ethereum siguron që kontratat inteligjente funksionojnë në të njëjtën mënyrë në të gjitha nyjet dhe marrin të njëjtat rezultate. Kështu Ethereum blockchain mbetet i qëndrueshëm në të gjitha nyjet. EVM përdor një arkitekturë të bazuar në stack[4] dhe ka zonën e vet në kujtesë për kodin që ekzekuton dhe të dhënat që ruan përveç hapësirës lokale të secilës kontratë inteligjente. Edhe pse EVM është një makinë virtuale e plotë Turing (Turing complete machine)[5], ekzekutimi i saj është i kufizuar nga sasia e gazit të lejuar nga çdo kontratë inteligjente. Ky kufizim shmang përdorimin e fuqisë së tepërt të llogaritjes për

[4] Stack - është një strukturë lineare e të dhënave e cila ndjek një renditje të veçantë në të cilën kryhen operacionet. Rënditja mund të jetë LIFO (Last In First Out) ose FILO (First In Last Out) [28]

[5] A Turing completeness system - Një sistem i plotë Turing nënkupton një sistem në të cilin mund të shkruhet një program që do të gjejë një përgjigje [27]

nyjet në të gjithë rrjetin Ethereum [24]. Gazi është karburant që fuqizon një rrjet Ethereum. Në një rrjet publik të Ethereum blockchain, për të joshur gjithnjë e më shumë minatorë për të punuar në vërtetimin e transaksionit, krijuesi i transaksionit cakton një sasi të veçantë të gazit në transaksion, i cili duhet t'i paguhet minatorit që minon transaksionin. Ethereum është një kornizë e plotë blockchain Turing, pasi u jep një themel gjuhëve programuese ashtu që duke përdorur këto gjuhë mund të shkruani kontrata që mund të zgjidhin ndonjë problem të arsyeshëm llogaritës. Rrjeti blockchain Ethereum është një grup EVM, ose nyje të lidhur me çdo nyje tjetër në një mekanizëm peer-to-peer [25]. EVM është pjesa e Ethereum që merret me vendosjen dhe ekzekutimin e kontratës inteligjente. Transaksionet e thjeshta të transferimit të vlerës nga një adresë Ethereum në tjetrën nuk kanë nevojë ta përfshijnë atë, duke folur praktikisht, por gjithçka tjetër do të përfshijë një azhurnim të gjendjes së llogaritur nga EVM. Në një nivel të lartë, EVM që funksionon në blockchain Ethereum mund të mendohet si një kompjuter global i decentralizuar që përmban miliona objekte të ekzekutueshme, secili me ruajtjen e tij të të dhënave të përhershme. EVM punon me një madhësi fjale prej 256 bit (kryesisht për të lehtësuar operacionet vendore të hasheve dhe kurbave eliptike) dhe ka disa përbërës të dhënash të adresueshëm:

- Një kod programi i pandryshueshëm ROM, i ngarkuar me *bytecode* të kontratës inteligjente që do të ekzekutohet
- Një kujtesë e paqëndrueshme, me çdo vendndodhje të iniciuar në mënyrë të qartë në zero
- Një depo e përhershme që është pjesë e gjendjes Ethereum, gjithashtu inicializuar zero

Detyra e EVM është azhurnimi i gjendjes Ethereum duke llogaritur tranzicionet e vlefshme të gjendjes si rezultat i ekzekutimit të kodit inteligjent të kontratës, siç përcaktohet nga protokolli Ethereum. Ky aspekt çon në përshkrimin e Ethereum si një makinë gjendje e bazuar në transaksione, e cila pasqyron faktin se aktorët e jashtëm (d.m.th., mbajtësit e llogarive dhe minatorët) fillojnë tranzicionet e gjendjes duke krijuar, pranuar dhe urdhëruar transaksione. Në nivelin e lartë, ne kemi gjendjen botërore Ethereum. Gjendja botërore është një hartëzim i adresave të Ethereum (vlera 160 bit) në llogari. Në nivelin më të ulët, çdo adresë Ethereum përfaqëson një llogari që përmban një bilanc ether, një *nonce* (që përfaqëson numrin e transaksioneve të dërguara me sukses nga

kjo llogari, ose numri i kontratave të krijuara prej saj nëse është një llogari kontrate), hapësira e ruajtjes së llogarisë (e cila është një depo e përhershme e të dhënave, e përdorur vetëm nga kontratat inteligjente), dhe kodi i programit të llogarisë [23].

4.4 Aplikacionet e Decentralizuara (DApps)

Që nga ditët e para të Ethereum, vizioni i themeluesve ishte shumë më i gjerë se "kontratat e mençura", jo më pak sesa rishpikja e uebit dhe krijimi i një bote të re të aplikacioneve DApps, e quajtur me të drejtë ***web3***. Kontratat inteligjente janë një mënyrë për të decentralizuar logjikën kontrolluese dhe funksionet e pagesave të aplikacioneve. Web3 DApps kanë të bëjnë me decentralizimin e të gjitha aspekteve të tjera të një aplikacioni: hapësira ruajtëse, mesazhet, emërtimet, etj.

Një DApp është një aplikacion që është kryesisht ose plotësisht i decentralizuar. Merrni parasysh të gjitha aspektet e mundshme të një aplikacioni që mund të jenë të decentralizuara:

- Softueri Backend (logjika e aplikimit)
- Softueri Frontend
- Ruajtja e të dhënave
- Komunikimet e mesazheve
- Rezolucioni i emrit (DNS)

Ka shumë përparësi për krijimin e një DApp që një arkitekturë tipike e centralizuar nuk mund t'i sigurojë:

- Qëndrueshmëri
    - Për shkak se logjika e biznesit kontrollohet nga një kontratë inteligjente, një mbështetje DApp do të shpërndahet dhe menaxhohet plotësisht në një platformë blockchain. Ndryshe nga një aplikacion i vendosur në një server të centralizuar, një DApp nuk do të bie nga sistemi asnjëherë dhe do të vazhdojë të jetë i disponueshëm për sa kohë që platforma të funksionoj.
- Transparenca
    - Natyra në zinxhirin e një DApp lejon të gjithë të inspektojnë kodin dhe të jenë më të sigurt për funksionin e tij. Çdo ndërveprim me DApp do të ruhet përgjithmonë në blockchain.

- Rezistenca e censurës
    - Për sa kohë që një përdorues ka qasje në një nyje Ethereum (duke ekzekutuar një nëse është e nevojshme), përdoruesi do të jetë gjithmonë në gjendje të ndërveprojë me një DApp, pa ndërhyrje nga ndonjë kontroll i centralizuar. Asnjë ofrues i shërbimit, apo edhe pronari i kontratës inteligjente, nuk mund ta ndryshojë kodin sapo të vendoset në rrjet.

Ndërsa shumë aplikacione sot e quajnë veten "DApps", shumica nuk janë plotësisht të decentralizuara. Sidoqoftë, tashmë është e mundur të ndërtohen aplikacione që janë pothuajse plotësisht të decentralizuara. Me kalimin e kohës, ndërsa teknologjia piqet më tej, gjithnjë e më shumë aplikacione tona mund të decentralizohen, duke rezultuar në një rrjet më elastik, rezistent ndaj censurës dhe falas [23].

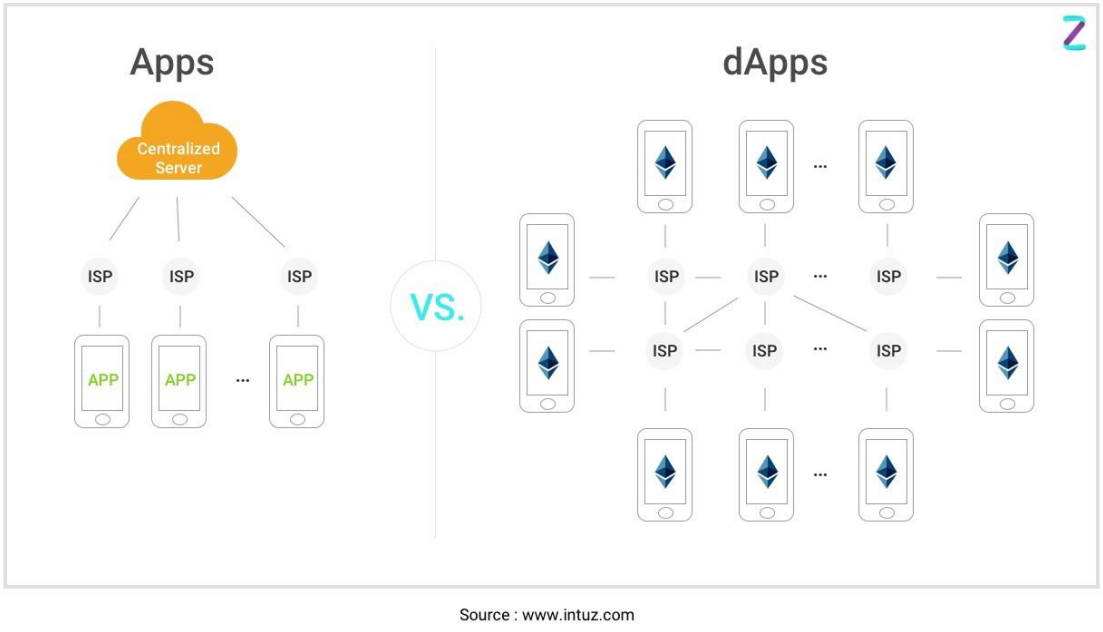

Figura 4. Aplikacionet e centralizuara kundrejt aplikacioneve të decentralizuara [29]

Në figurën 4 është paraqitur modeli i aplikacioneve të centralizuara *CApps* kundrejtë modelit të aplikacioneve të decentralizuara *DAaps*. Nga figura mund të vërejmë se aplikacionet e centralizuara kanë një serverë bazë nga i cili marrin të dhëna me anë të siguruesëve të tyre të çasjes në internetit, kurse në anën e djathtë të figurës paraqiten nyjet tek aplikacionet e decentralizuara të cilat shërbejnë si server por edhe si klientë për të gjitha nyjet tjera në rrjet, poashtu ato vetë sigurojnë transportin e të dhënave tek të gjitha nyjet në blockchain sistemin, pa nevojën e përfshirjes së një pale të tretë.

5 Mundësitë dhe sfidat e kontratave intelegjente në teknologjinë blockchain

Kontratat inteligjente lehtësojnë zbatimin e kontratës, marrëveshje me transparencë të integruar dhe krijojnë rezistencë. E tiparet dalluese të kontratave të zgjuara e bëjnë atë të përshtatshme në shumë aplikacione. Janë bërë shumë kërkime në industri si dhe akademi për të hetuar pikat e forta dhe zbatueshmërinë e kontratave të zgjuara në fusha të ndryshme aplikimesh. Për më tepër, përmirësimet e aspekteve teknike u përqëndruan shumë për të rregulluar mirë kontratat inteligjente për rritjen e përputhshmërisë së kontratave të zgjuara. Ka shumë platformat të kontratave të zgjuara që dalin në treg me veçori të veçanta dalluese që i përshtaten aplikimeve të veçanta.

Kontratat inteligjente mund të transformojnë rregullat e biznesit në programet kompjuterike. Platformat e kontratave të ndryshme inteligjente janë zhvilluar për të adresuar kërkesat specifike në secilën industri. Çdo platformë e kontratës inteligjente përfshin një sërë veçorish specifike të synuara për aplikacionin e veçantë. Për shembull, Ethereum është zhvilluar kryesisht për aplikacionet që kërkojnë tokenizim. Pothuajse të gjitha platformat përmbajnë tiparet themelore të një sistemi të zgjuar të kontratave duke përfshirë kodin e pandryshueshëm të programit, regjistrin kryesor të decentralizuar dhe shtresën e konsensusit.

5.1 Aplikimet e kontratave të mençura

Në këtë pjesë do të paraqesim disa nga fushat dhe rolet më të rëndësishme të aplikimit të kontratave intelegjente. Fusha këto që kanë të bëjnë me sistemin shëndetësor dhe menaxhimin e logjistikës.

5.1.1 Shërbimet që lidhen me kujdesin shëndetësor

Hulumtimi dhe zhvillimi në fushën e kujdesit shëndetësor kanë rritur jetëgjatësinë. Si rezultat, numri i të moshuarve në botë që do të kërkojnë kujdes periodik mjekësor po rritet gradualisht. Trajtimi me dorë i një vëllimi kaq të paparë të të dhënave të pacientit është një proces i rëndë. Proceset manuale pësojnë shpenzime të konsiderueshme administrative dhe janë të prirura ndaj gabimeve kritike njerëzore. Transformimi dixhital do të eliminojë këto çështje që lidhen me procesin manual, por të ekspozuar ndaj një sërë kërcënimesh për sigurinë e të dhënave. Prandaj, përfshirja e kontratave të zgjuara në ekosistemin e kujdesit shëndetësor do të jetë dukshëm efektive në dimensione të ndryshme [30].

5.1.1.1 Menaxhimi i informacionit shëndetësor

Shumica e sistemeve në disa vende nuk janë në përputhje me standardet ndërkombëtare siç është Akti i Transportueshmërisë dhe Privacisë i Sigurimeve Shëndetësore (HIPAA). Disa sisteme janë ende të ngurtë dhe ende mund të kërkojnë disa shkresa. Sistemi i informacionit shëndetësor duhet të sigurojë privatësinë dhe integritetin e të dhënave, si dhe disponueshmërinë. Këto shërbime janë më të domosdoshme në kontekstin shëndetësor sesa në industritë e tjera, sepse informacioni mjekësor është shumë i rëndësishëm në pasuritë e paçmueshme të jetës. Teknologjia blockchain dhe kontratat inteligjente mund të aplikohen për të mundësuar sistemet e menaxhimit të informacionit shëndetësor për të siguruar privatësinë, integritetin dhe kontrollin e aksesit për të arritur pajtueshmërinë rregullatore së bashku me përvojën e shtuar të pacientit.

Azaria paraqiti ***MedRec***, një sistem i decentralizuar i menaxhimit të regjistrave elektronikë të shëndetit i cili u mundëson pacientëve të kenë qasje në të dhënat e tyre mjekësore nëpër vende të shumta trajtimi. Sistemi po shfrytëzohet nga blockchain dhe kontratat e zgjuara, të zhvilluara në platformën Ethereum dhe menaxhon vërtetimin, konfidencialitetin, llogaridhënien dhe ndarjen e të dhënave me një konsideratë vendimtare mbi informacionin e ndjeshëm të pacientit. Sistemi është i ndërveprueshëm me ekosistemet ekzistuese të regjistrave mjekësorë [30]. MedRec është kombinimi i një nevoje sociale me një aftësues teknologjik: një sistem që i jep përparësi agjencisë së pacientit, duke dhënë një pamje transparente dhe të arritshme të historisë mjekësore. Për të vazhduar analogjinë bankare, sistemet financiare mund të përmbajnë depozitues të shumtë të ndryshëm të monedhës, ndoshta një për secilin rrjet ofrues. Problemi është se të dhënat shëndetësore nuk janë të shkëmbyeshme, secila është gjurmë unike e një individi. Nuk ka asnjë tregti të ngjashme, siç mund të bëjmë me paratë. Ndërsa konkurrenca dhe shumësia shpesh rezultojnë në kosto më të ulëta të konsumatorit, këtu rrezikon një masë pengesash të papajtueshme ose të paarritshme për shkëmbimin dhe kontrollin. Ne propozojmë një alternativë: një sistem aksesi të shpërndarë dhe vlefshmërie duke përdorur blockchain për të zëvendësuar ndërmjetësit e centralizuar [31].

5.1.1.2 Mbrojtja e të dhënave të kërkimit klinik

Integriteti i të dhënave të provave klinike është një shqetësim kryesor në mjekësi. Integriteti i të dhënave përcaktohet si masa në të cilën të dhënat elektronike dhe të bazuara në letër janë të plota, të qëndrueshme, të sakta, dhe të besueshme gjatë gjithë ciklit të jetës

së të dhënave. Problemet domethënëse të besueshmërisë së të dhënave shkencore janë humbja e të dhënave, ndërrimi i pikës përfundimtare, pastrimi i të dhënave dhe publikimi selektiv. Trajtimet për shkak të të dhënave të shtrembëruara do t'i ekspozojnë pacientët në një rrezik për jetën [30]. Nugent në punimin e tij nënkuptonte zbatimin e kërkesave rregullatore dhe besimin në të dhënat e kërkimit klinik me anë të kontratave të zgjuara të bazuara në blockchain duke përdorur platformën Ethereum. Kontratat inteligjente, duke u emërtuar si kontrata rregullatore dhe kontratat e provës vepruan si administratorë të besuar të sistemit. Autorët përdorën dy kontrata të zgjuara. Kontrata rregullatore mban një strukturë të dhënash për autorizimin e provës klinike ndërsa kontrata e provës është ndërtuar duke përdorur funksione brenda kontratës së autorizimit [32].

5.1.1.3 Monitorimi dhe trajtimi i automatizuar i pacientit

IoT (eng Internet of things) dhe pajisjet që mund të vishen janë përqafuar nga njerëzit nga orët e mençura në Wireless Body Area Network (WBAN). Objektivi kryesor i WBAN është të përmirësojë shpejtësinë e komunikimit, saktësinë dhe besueshmërinë e sensorëve të lidhur në afërsi të trupit të njeriut. Sensorët WBAN mund të gjenerojnë një sasi masive të të dhënave të tilla si niveli i glukozës në gjak, shkalla e pulsit, presioni i gjakut, etj. Zgjerimi i sistemeve të tilla ngriti kërkesën e privatësisë, kontrollit të aksesit dhe integritetit të të dhënave. Kontratat inteligjente do të jenë zgjidhja e gjeneratës së ardhshme për të eliminuar rreziqet duke kontrolluar aksesin dhe ekzekutimin e sigurt autonom të trajtimeve në sistemet e automatizuara të monitorimit dhe trajtimit të pacientëve [30]. Griggs propozoi një sistem i cili përdor blockchain privat Ethereum dhe modelin e vendosjes së pajisjeve mjekësore të modelit master-slave. Sensorët e lidhur me pajisjen inteligjente, të tilla si një smartphone ose tabletë. Sensorët mund të lidhen me aparate të tillë si aktivizuesit e insulinës dhe monitorët e presionit të gjakut për të ekzekutuar kontrata të zgjuara dhe përfundimisht regjistrimet do të transferohen në librin kryesor të pandryshueshëm. Të dhënat e marra nga pajisja inteligjente dërgohen në kontratën inteligjente, së bashku me vlerat e pragut të personalizuar dhe kontratat inteligjente vlerësojnë të dhënat dhe shkaktojnë njoftime për pacientin, ofruesin e kujdesit shëndetësor dhe udhëzon nyjet e aktivizimit për trajtim të automatizuar nëse kërkohet [33].

5.1.2 Menaxhimi i Logjistikës

Industria e logjistikës dhe zinxhirit të furnizimit u ndërlikua për shkak të kërkesave të larmishme të klientëve. Prodhimi global rregullohet sipas përparësive ekonomike dhe shumica e vendeve kontribuojnë në importin dhe eksportin e tregtisë. Ngarkesat ajrore dhe detare janë të ndryshme nga pjesa më e madhe e mallrave të tilla si gaforret e gjalla, perimet e freskëta etj. Që kur mallrat u rimodeluan, poashtu kërkesat e magazinimit dhe kushtet mjedisore në dorëzim, magazinimi është bërë një konsideratë jetike. Konsumatorët zakonisht përqendrohen nëse produkti specifik i dorëzuar në raft është brenda kushteve të kërkuara siç janë kërkesat rregullatore. Sigurimi i shpërndarjes së mallrave brenda kushteve të rekomanduara është një sfidë e madhe në logjistikën dhe zinxhirin e furnizimit. Kontratat e zgjuara dhe teknologjia blockchain premtuan të zgjidhin shumë probleme me natyrën e saj të shpërndarë dhe autonome ekzekutive [30].

5.1.2.1 Sigurimi i cilësisë dhe pajtueshmërisë së zinxhirit të furnizimit të mallrave detar/ajror

Pajtueshmëria me zinxhirin e furnizimit është një shqetësim i madh në mallra të caktuara, siç janë artikujt ushqimor, përfshirë perimet, frutat dhe gaforret e gjalla. Standardet janë të vendosura nga organizata të tilla si Këshilli i Mbikëqyrjes Detare. Autoritetet kryejnë auditime të forta për të siguruar që palët e interesuara të certifikuara të ushqimit të detit të sigurojnë standardet. Kostoja e gjerë dhe përpjekjet mund të eliminohen duke u mundësuar kontratave të zgjuara të marrin përsipër veprimet e kërkuara brenda zinxhirit të furnizimit. Për shembull, kushtet specifike që kërkohen të përmbushen për një transferim të vlefshëm të kujdestarit të prodhimeve të detit të përcaktuara nga autoritetet rregullatore dhe përfshirja e tyre si një kontratë e zgjuar. Nëse është kështu, autoritetet mund të sigurohen që transferimet e kujdestarit të ekzekutohen sapo të plotësohen kushtet e përcaktuara nga autoritetet rregullatore. Prandaj kërkesa e auditimit eksplicit eliminohet. Kontrata e zgjuar, si një program i pandryshueshëm i kushteve do të sigurojë transparencën e ekzekutimit me kusht [30]. Chen dhe disa autorë të tjerë propozuan aplikimin e kontratave inteligjente të bazuara në blockchain për të menaxhuar cilësinë e zinxhirit të furnizimit. Autorët theksuan se kontratat inteligjente mund të përdorin një mori teknikash optimizimi për të përmirësuar shpërndarjen, siç është përdorimi i koordinatave GPS dhe planifikimi i itinerarit. Ata autorë gjithashtu theksuan rëndësinë e konfidencialitetit në blockchain, i cili korrespondon me informacionin e ndjeshëm të biznesit [34].

5.1.2.2 Pajtueshmëria rregullatore e zinxhirit të furnizimit bujqësor

Organizata të tilla si Organizata e Ushqimit dhe Bujqësisë (FAO) nga Kombet e Bashkuara (OKB) krijuan standarde të rëndësishme për të mbajtur në rregull zinxhirin e furnizimit me ushqim. Për shembull, kushtet termike të kontejnerit me perime ose ushqime brenda duhet të jenë të lidhura me standardet e paracaktuara brenda shpërndarjes, në mënyrë që të parandalohet zhvillimi i baktereve. Ndonjëherë, personeli duhet të rregullojë manualisht temperaturën, i cila është një operacion intensiv i burimeve njerëzore. Kostoja e rregullimeve manuale të kushteve të temperaturës eliminohet kur përfshihen kontratat inteligjente. Kushtet e vendosura nga autoritetet rregullatore dhe saktësia e kushteve të temperaturës, garantohen me kontratat inteligjente. Kim në bashkpunim me disa autorë të tjerë në punimin "*Integrating Blockchain, Smart Contract-Tokens, and IoT to Design a Food Traceability Solution*" prezantoi Harvest Network, një zgjidhje teorike e gjurmueshmërisë së ushqimit "farm-to-fork" me integrimin të platformës Ethereum së bashku me pajisjet IoT që shkëmbejnë standardet e mesazheve GS1. Autorët propozuan që të tokenizohen asetet bujqësore në shenja ERC-721 për t'u transferuar brenda zinxhirit të furnizimit. Softueri i krijuar për kontrata të zgjuara në blockchain Ethereum ndërton një rrjetë mesh për të përmirësuar gjurmueshmërinë e ushqimit, kursimet e kostos dhe efikasitetin e përmirësuar brenda zinxhirit të furnizimit bujqësor. [30]

5.1.2.3 Gjurmueshmëria e zinxhirit të furnizimit të mallrave të veçanta

Prejardhja e historisë së disa mallrave është shumë efektive në vlerën e saj monetare. Për shembull, gurët e çmuar dhe diamantet janë shembuj domethënës. Regjistrimet e vazhdueshme të lëvizjes nga miniera në sallë ekspozite sigurojnë që perla të mos jetë ndryshuar ose të dhënat të mos jenë modifikuar gjatë transportit. Certifikatat e lëshuara nga autoritetet qeveritare janë shtesa me vlerë për mallin. Natyra e decentralizuar dhe transparente e blockchain është përshtatja ideale për kërkesën e gjurmimit të mallrave të veçanta [30]. Cartier ofron njohuri të rëndësishme të zbatueshmërisë së kontratave të zgjuara të bazuara në blockchain për industrinë e gurëve të çmuar, diamantit, gurit me ngjyra dhe perla. Faktet thelbësore të një guri të çmuar, të tilla si vendndodhja gjeografike dhe specifikimet e prerjes dhe lustrimit të kërkuara për t'u regjistruar në regjistrin kryesor. Kur ndodhë fitimi i parave nga gurët e çmuar, rregullat e biznesit mund të përcaktohen si kontrata e zgjuar dhe gurët e çmuar dhe pronësia e aseteve mund të transferohen sapo të përmbushen kushtet e kontratës së zgjuar [35].

5.2 Sfidat Teknike në Kontratat e mençura

Përfundimisht, kontratat inteligjente përbëhen nga programe kompjuterike dhe algoritme. Çështjet që lidhen me programet kompjuterike, si dhe ciklin jetësor të zhvillimit të softuerit klasik janë të zbatueshme për kontratat inteligjente. Metodologjitë e vlefshmërisë të cilat janë të zbatueshme për të vlerësuar programet kompjuterike dhe algoritmet do të jenë të zbatueshme për kontratat inteligjente. Përveç kësaj, janë identifikuar disa sfida domethënëse të cilat do të lënë boshllëqe në funksionalitetin e aplikacionit [30].

5.2.1 Verifikimi dhe vërtetimi për të zgjidhur çështjet e korrektësisë

Sjellja e devijuar nga specifikimet e tyre funksionale të kontratave të zgjuara do të jetë një problem domethënës në aplikimet e kontratave të zgjuara. Verifikimi formal i një programi kompjuterik konstaton se programi i veçantë funksionon sipas sjelljes formale për inputet e përcaktuara dhe dëshmon korrektësinë (e pjesës harduerike dhe të algoritmeve). Verifikimi formal ekziston me dy nivele parimesh gjuhësore. Verifikimi formal mund të kryhet në nivelin gjuhësor dhe në nivelin e ulët bytecode. Nga testimi i njësisë në zbatimin e funksioneve komplekse matematikore, ka një mori teknikash të përdorura në kontekst. Verifikimi formal i kontratës së zgjuar është i spikatur me vetitë e tij operacionale. Kontratat inteligjente janë të pandryshueshme sapo të vendosen dhe nuk mund të rregullohen lehtë. Përveç kësaj, kontratat inteligjente mund të kenë vlera financiare në aplikacione të ndryshme dhe do të jenë të arritshme për këdo. Prandaj, verifikimi formal është parësor në kontekstin e kontratave të zgjuara [30].

5.2.2 Dobësitë e sigurisë

Dobësitë e sigurisë i ekspozojnë sistemet në rreziqe të ndryshme. Meqenëse sistemet blockchain për aplikimet përkatëse janë të ndërtuara në programet kompjuterike, të metat e sigurisë të zakonshme për sistemet kompjuterike pritet të hetojnë dhe eliminojnë për funksionimin e sigurt të sistemeve. Operacionet e ri-vendosjes pas rregullimeve të dobësive të sigurisë janë të ndryshme nga cikli i jetës tradicionale i vendosjes së softuerit dhe sfiduese me shpenzime të gjera. Sidomos, kur një aplikacion i veçantë integrohet me një rrjet publik blockchain, korrigjimi i një defekti do të jetë një operacion i shtrenjtë [30].

5.2.3 Gabimet e softuerit (bugs)

Testimi i softuerit është një praktikë thelbësore në inxhinierinë e softuerit. Cilësia e kodeve të softuerit dhe pozicioni i tyre me specifikimet që pritet të vlerësohen para integrimit të prodhimit. Ekzistojnë teknika dhe mjete të ndryshme në treg për të identifikuar gabimet e softuerit dhe për të vlerësuar cilësinë. Sidoqoftë, disa kërkime kanë menaxhuar për të zhvilluar mjete dhe teknika për sigurimin e cilësisë së kontratave të zgjuara në mënyrë specifike. Gao prezantoi SmartEmbed i cili mund të përdoret për të identifikuar defektet e lidhura me klonimin në kontratat inteligjente të qëndrueshmërisë. Zgjidhja e propozuar mbështet identifikimin e defekteve në shkallë individuale, si dhe në shkallë të madhe [30].

5.2.4 Çështjet e privatësisë dhe teknikat e përmirësimit

Privatësia e të dhënave është një shqetësim jetik në pothuajse të gjitha aplikacionet. Parimet kryesore të blockchain përfshijnë regjistrin publik të decentralizuar i cili përfshin të dhënat e transaksioneve. Sidoqoftë, këto të dhëna të transaksioneve publike mund të ngrenë çështje të privatësisë në perspektivën e pronarëve të të dhënave. Këto kërkesa për privatësi duhet të adresohen me kujdes pa ndikim në veçoritë e tjera të blockchain, përfshirë kërkesat e performancës. Zbatimi i privatësisë së të dhënave mund të zvogëlojë hendekun midis shumicës së aplikacioneve aktuale dhe blockchain për integrim të përsosur [30].

5.2.5 Kufizimet e performancës

Faktorët e performancës janë konsiderata thelbësore në perspektivën e aplikimit. Kërkesat e performancës të përpunimit të transaksioneve me vëllim të lartë janë të detyrueshme për aplikime të tilla si sistemet e pagesave dixhitale. Kohët e verifikimit të transaksioneve për platformat kryesore blockchain si Ethereum dhe Bitcoin penguan zbatueshmërinë për pagesat me pakicë. Në të kundërt, rrjetet e pagesave të tilla si Visa sigurojnë 7000 transaksione në sekondë. Sidoqoftë, shumë kërkime janë në progres për të hetuar teknikat për të rritur karakteristikat e performancës së blockchain [30].

PËRFUNDIMI

Nevoja e një rritje eksponenciale drejt zhvillimit teknologjikë e shfaqur qysh herët me paraqitjen e kompjuterëve të parë, duket se pati ngecje në shekullin XXI deri sa u paraqit një teknologji me emrin Bitcoin që për herë të parë arriti ta gjejë një zgjidhje reale për të zëvendësuar paranë e letrës dhe atë digjitale në pronësi të bankave apo qeverive, vlera këto që kontrollohen nga palët e treta. Duke e bërë kështu këtë teknologji, një risi që hap një dritare të re për botën e teknologjisë përveç shpikjes së mënyrave të ndryshme të komunikimit. Garanca e kësaj teknologjie që ka sjellë një valutë të re krejtësisht virtuale, është rrjeti i gjërë P2P dhe kriptografia e jashtzakonshme. Përmes kriptografisë Bitcoin i zgjidh problemet si besueshmëria në rrjet, krijimi i adresave valide dhe shumë të sofistikuara, krijimi dhe validimi i transaksioneve dhe poashtu arrin ta mbaj aktiv rrjetin duke mbrojtur të gjithë pjesmarrësit në rrjet. Bitcoin është valuta e parë që me anë të rrjetit të saj dhe kriptografisë, arriti ta zgjedh problemin e shpenzimit të dyfisht, problem ky që mbante peng për vite inxhinierët që të krijojnë vlera për bartje në Internet. Edhe pse ende nuk dihet krijuesi i kësaj teknologjie, çdo ditë e më shumë kjo teknologji po adaptohet dhe po kontribohet në kodin e saj, nga shumë inxhinierë dhe programues, kod ky që është i hapur për publikun.

Me Bitcoin erdhi edhe teknologjia blockchain, teknologjia e blloqeve të lidhura në zinxhirë, që si e thotë edhe emri mban një zigjirë me blloqe të lidhura në të, blloqet janë të lidhura dhe të regjistruara falë një regjistri të shpërndarë, regjistër ky që jeton në të gjitha nyjet e pjesmarrësëve në blockchain. Ky regjistër përmban të gjitha blloqet që krijohen në blockchain që nga blloku i parë e deri tek blloku më i fundit që e kanë krijuar minatorët. Minatorët janë një rol tjetër mjaft i rëndësishëm në blockchain, ata përveq se janë nyje në rrjet, ndryshe nga nyjet tjera që vetëm kryejn transaksione, krijojnë valuta virtuale, validojnë transaksionet e nyjeve në rrjet dhe mirmbajnë rrjetin, në bazë të protokolleve që ndodhen në rrjet dhe për këtë zakonisht edhe shpërblehen.

Blokchain nuk solli vetëm pajisjet dhe mundësinë për krijimin dhe lëvzjen e valutave virtuale, por solli edhe një hapsirë krejtësisht të re të ideve inovative që mund ta ndryshojnë për të mirë botën viteve në vijim. Një ide si kjo është edhe Ethereum që na prezantoj me konceptin e kontratave të mençura dhe me aplikacionet e decentralizuara DApps.

6 LITERATURA

[1] Antony Lewis, The Basics Of Bitcoins And Blockchains, ISBN: 978-1-63353-800-9

[2] Keizer Söze, Blockchain Novice to Expert, Copyright © 2017 Keizer Söze

[3] Chris Burniske & Jack Tatar, Cryptoassets The inovative investor's guide to Bitcoin and beyond, ISBN: 978-1-26-002668-9

[4] Don Tapscott, Alex Tapscott, Blockchain Revolution How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, ISBN: 9781101980149

[5] https://bisontrails.co/blockchain-infrastructure/ qasur me 13/06/2021

[6] https://coinmarketcap.com/alexandria/article/what-is-peer-to-peer-p2p qasur me 13/06/2021

[7] https://www.wowza.com/resources/guides/p2p-unicast-streaming qasur me 13/06/2021

[8] https://www.investopedia.com/terms/b/bitcoin-mining.asp qasur me 13/06/2021

[9] https://www.gemini.com/cryptopedia/double-spending-problem-crypto qasur me 13/06/2021

[10] Tiana Laurence, Blockchain for dummies, ISBN: 978-1-119-36559-4

[11] https://www.merriam-webster.com/dictionary/token qasur me 18/06/2021

[12] https://www.forcepoint.com/cyber-edu/firewall qasur me 20/06/2021

[13] Andreas M. Antonopoulos, Mastering Bitcoin programming the open Blockchain, ISBN: 978-1-491-95438-6

[14] Phil Champagne, The book of Satoshi, ISBN: 978-0-9960613-0-8

[15] Saifedean Ammous, The Bitcoin Standard, The Decentralized Alternative to Central Banking, ISBN: 9781119473862

[16] https://onlinelaw.wustl.edu/blog/legal-english-de-factode-jure/ qasur me 03/07/2021

[17] https://www.gemini.com/cryptopedia/public-private-keys-cryptography qasur me 04/07/2021

[18] https://whatis.techtarget.com/definition/Bitcoin-address/ qasur me 04/07/2021

[19] https://www.pcmag.com/encyclopedia/term/bitcoin-wallet qasur me 05/07/2021

[20] https://www.investopedia.com/best-bitcoin-wallets-5070283 qasur me 05/07/2021

[21] Jimmy Song, Programming Bitcoin Learn How to Program Bitcoin from Scratch, ISBN: 978-1-492-03149-9

[22] https://www.coindesk.com/what-is-proof-of-work qasur me 05/07/2021

[23] Andreas M. Antonopoulos, Dr. Gavin Wood, Mastering Ethereum Building Smart Contracts and DApps

[24] Michael G. Solomon, Etherum for dummies, ISBN: 978-1-119-47412-8

[25] Debajani Mohanty, Etherum for Architects and Developers ISBN: 978-1-4842-4074-8

[26] https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ qasur me 14/07/2021

[27] https://chortle.ccsu.edu/StructuredC/Chap01/struct01 qasur me 14/07/2021

[28] https://www.geeksforgeeks.org/stack-data-structure/ qasur me 14/07/2021

[29] https://medium.com/hackernoon/what-are-decentralized-applications-dapps-explained-with-examples qasur me 14/04/2021

[30] Hewa, Tharaka, Ylianttila, Mika, Liyanage, Madhusanka, Survey on blockchain based smart contracts: Applications, opportunities and challenges, 2021-03-01

[31] https://medrec.media.mit.edu/ qasur me 18/08/2021

[32] T. Nugent, D. Upton, M. Cimpoesu, Improving Data Transparency in Clinical Trials using Blockchain Smart Contracts, 2016

[33] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, T. Hayajneh, Healthcare Blockchain System using Smart Contracts for Secure Automated Remote Patient Monitoring, 2018

[34] S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, J. Zhang, A Blockchain-Based Supply Chain Quality Management Framework, 2017

[35] L. E. Cartier, S. H. Ali, M. S. Krzemnicki, Blockchain, Chain of Custody and Trace Elements: An Overview of Tracking and Traceability Opportunities in the Gem Industry, 2018