Spring 4-2020

IOT SECURITY WITH BLOCKCHAIN SOLUTION

Arber Murati
University for Business and Technology - UBT

Programi për Shkenca Kompjuterike dhe Inxhinierisë

IOT SECURITY WITH BLOCKCHAIN SOLUTION

Niveli Bachelor

Arber Murati

Prill / 2020
Prishtinë

Fakulteti i Shkencave Kompjuterike dhe Inxhinierisë

Punim Diplome
Viti akademik 2017 – 2018

Arber Murati

IOT SECURITY WITH BLOCKCHAIN SOLUTION

Mentori: Phd. Can. Blerton Abazi

Prill / 2020

Ky punim është përpiluar dhe dorëzuar në përmbushjen e kërkesave të pjesshme për Shkallën Bachelor

ABSTRAKT

IoT është një teknologji me një potencial, impakt dhe rritje të jashtzakonshme. Sot, prodhimi momental i të dhënave nga paisjet teknologjike llogaritet të jetë rreth 2.5 quintillion bytes gjdo ditë. Për të pasur një kuptim më figurativ, 2.5 quntillion cent në monedha do të mbulonin sipërfaqën e globit për rreth 5 herë nëse token do ta përcaktonim si të sheshtë. Sipas hulumtimeve të fundit, deri në vitin 2025 diku rreth 41.6-miliard paisje IoT do të jenë online si dhe 30 % e të gjitha të dhënave do të duhen të procesohen në real-time. Hakerët shpesh fitojnë qasje në pajisje fundore si routers dhe switches, duke shfrytëzuar dobësitë e këtyre sistemeve. Paisje të tjera si termostati, zilja e derës apo kamerat e sigurisë gjithashtu janë të rrezikuara. Qëllimi i këtij punimi ka qenë që të bëhet një studim mbi integrimin e Blockchain teknologjisë në sistemet e sigruisë së IoT paisjeve. Më e rëndësishme, do të diskutojmë mbi impaktin e teknologjisë së Blockchain (BC) si njëra ndër teknologjitë e cila mundë të ofrojë zgjidhje për disa nga problemet e sigurisë. Studimi është bazuar në hulumtimin e materialeve online rrespektivisht e ndikuar nga botimet prej profesionisteve të sigurisë informative, gjithashtu dhe nga analizimi i të dhënava, trendeve dhe statistikave të fundit.

Rezultatet e këtij studimi paraqesin nevojën imediate dhe të vazhdueshme për të ndërmarrë masa në mënyre që paisjet të cilat i përdorim të jenë më të sigurta. Mbi të gjitha, bëhet e qartë që teknologjitë e ndryshme mundë të bashkohen dhe të hapin horizonte të reja. Në fund, ky studim përpos aspekteve pozitive gjithashtu shtjellon disa nga mangësitë me te cilat paraqiten.

Fjalët kyqe: Internet of things, Blockchain, Smart Contract.

FALENDERIME

Unë falënderoj mentorin tim, PhD. Can. Blerton Abazi në rradhë të parë si profesor të sukseshëm gjatë studimeve si dhe për udhëzimet, mbështetjen dhe këshillat e tij gjatë mentorimit të këtij punimi.

Gjithashtu falënderoj të gjithë miqtë e mi të studimeve dhe stafin akademik me të cilët kaluam momente të bukura përgjatë këtyre viteve se bashku.

Në fund, falënderim të përzemërt dhe të veqantë gjithë familjes sime të cilët me besimin dhe mbi të gjitha me dashurinë dhe sakrificën e tyre të vazhdueshme, ishin mbështetja ime më e madhe përgjatë gjithë këtij rrugëtimi. Do të ju mbetem gjithmonë mirënjohës sepse pa ju nuk do të ishte i mundur realizimi i kësaj ëndrre për mua.

Faleminderit të gjithëve!

PËRMBAJTJA

LISTA E FIGURAVE

LISTA E TABELAVE

FJALORI I TERMAVE

IoT - Internet of Things

IT - Information Technology

Hacker - A person who uses computers to gain unauthorized access to data

Firewall - A part of a computer system or Network that is designed to block unauthorized

BC - Blockchain

SC - Smart Contract

PII - Personally Identifiable Information

SPOF - SPOF is a part of a system that, if it fails, will stop the entire system

PoW - Proof-Of-Work

Merkle Root - Is the hash of all the hashes of all the transactions

Mining - The process of adding transaction records to BC ledge

Hash - Hash function is any function that can be used to map data of arbitrary fixed size

Ledger - A book containing accounts in which the classified and summarized information

TEE - Trusted Execution Environment

SGX - Software Guard Extensions

Smart Home - Home setup where internet appliances and devices can be controlled

Overlay Network – Is a telecommunications network that is built on a another network

Cloud Storage - Computer data storage in which the digital data is stored in logical pools

DHT - Distributed Hash Table

1 HYRJE

Biliona paisje të Internet of Things (IoT) mundë të transformojnë shtëpi, qytete dhe jetën në përgjithësi. Zhvillimi i teknologjise 5G gjithashtu do të ndikon në një transformim të shpejtë duke zvogëluar vonesën e internetit. Nje raport i International Data Corporation (IDC), parashikon që IoT paisjet të pësojnë një rritje prej 28.5 % prej vitit 2018 deri në vitin 2025 kurse video mbikqyrjet do të rriten deri në 60 %. E gjithë kjo dinamikë e shpejtë e zhvillimit të teknologjisë do rrisë varsinë e njerzëve ndaj teknologjisë. Siguria dhe mbrojtja e të dhënave do të jetë një ndër sfidat dhe qëllimi kryesorë me të cilën do të përballemi. Duke analizuar faktet nga e kaluara, vërejmë që është e vështirë që të ketë sistem përfekt ose të pathyeshëm të cilin mundë ta përdorim dhe se gjithmonë do të ketë një vektor i cili mundë të paraqes një rrezik potencial. Jo gjithmonë rreziku vjen nga jashtë, në fakt rreziku më i lartë gjendet përbrenda njerzëve të një kompanie apo organizate të caktuar. Motivet për sulmet në të dhëna mundë të jenë nga më të ndryshmet duke filluar prej motiveve financiare, politike, konkurencës apo asnjëra nga ato por vetëm që të shkaktohet një dëm i caktuar pa asnjë arsyje. Për të mos ndodhur kjo është me rëndësi që në mënyre të vazhduar të hulumtohen apo të zhvillohen sisteme të avancuara të sigurisë të cilat na mbrojnë nga këto rreziqe që paraqiten gjatë përdorimit të internetit apo teknologjisë në përgjithësi.

Trendi i zhvillimit tregon që siguria është duke kërkuar zgjidhjen tek decentralizimi i të dhënave dhe gjithmonë duke tentuar që të shmangim një single point failure që do të kompremententonte të gjithë sistemin e centralizuar. Për këtë arsyje do të diskutojmë mbi IoT paisjet, impaktin dhe trendin e zhvillimit për të ardhmën. Studimi si i tillë do të bazohet në shqyrtimin dhe analizimin e litaraturës dhe shkrimeve aktuale sa i përket temës rrespektive. Fokus të veqantë do ti kushtojme Blockchain (BC) teknologjisë, për të cilën si të tillë do të tregojmë se si funksionon, cili është parimi mbrapa asaj teknologjie dhe se si do të mundë të gërrshetojmë atë si model të sigurisë së IoT paisjeve. Do të paraqesim disa prej aplikimeve interesante të disa projekteve të cilat përdorin BC për të rritur sigurinë në IoT.

2 SHQYRTIMI I LITERATURËS

2.1 Sulmet në IoT

Internet of Things (IoT) luan një rol shumë të rëndësishëm duke mundësuar një jetë më dinamike dhe më të rehatshme. Megjithatë, siguria e këtyre paisjeve është një nga qështjet që kërkon prioritet dhe angazhim të veqantë duke pasur parasysh natyrën heterogjene, shpërndarjen e madhe dhe gjenerimi enorm i të dhënave që gjenerohen nga këto pasije gjdo sekond. Authentifikimi dhe kontrolli i qajes janë ndër faktorët dhe sfidat kryesore e në IoT. Përkundër angazhimit të vazhdueshëm në zhvillimin e arkitekturave dhe teknologjive të ndryshme të sigurisë, algoritme të ndryshme kriptografike, kontrolle të qasjes dhe shumë masave të tjera të sigurisë prapë nuk arrijmë që të kemi një sistem të pathyeshëm. Të dhënat tona përsonale, transaksionet bankare dhe madje të dhëna dhe statistika nga jeta jonë për të cilat nuk jemi as vetë në dijeni, analizohen nga sisteme të ndryshme.

Shkelja e të dhënave nuk ka filluar vetëm kur kompanitë filluan të konvertonin të dhënat e tyre ne formë digjitale. Shkeljet e të dhënave filluan të rriten pikerisht në vitet e 1980-ta deri në kohet aktuale. Sulmet kanë pësuar një rritje drastike nga fillimi i vitit 2005 deri në ditët e sotme. Këto sulme kanë pasuar si rrjedhojë e zhvillimit të hovshëm të tëknologjisë dhe sistemeve të komunikimit. Duke u adaptuar në jetën tonë të përditshme IoT paisjet përmbajnë informacione të rëndësishme të jetës sonë. Ky aspekt i përdorimit të teknologjise është kuptuar herët nga individë të caktuar me qëllime të përvetësimit të atyre të dhënave për qëllime kryesisht të përfitimit të lehtë të të dhënave.

Rrjedhja e të dhënave në ditet e sotme mundë të kenë pasoja shumë të rënda për individin apo kompaninë, deri në atë mase sa që e gjithë kompania mundë të mos arrijë të rimëkëmbet nga incidenti i cili e ka pësuar. 43% e sulmeve kanë për qëllim bizneset apo kompanite e vogla dhe 60 % e atyre bizneseve duhet të mbyllin veprimtarinë vetëm 6 muaj nga sulmi i pësuar (Small Business Trends, 2019).

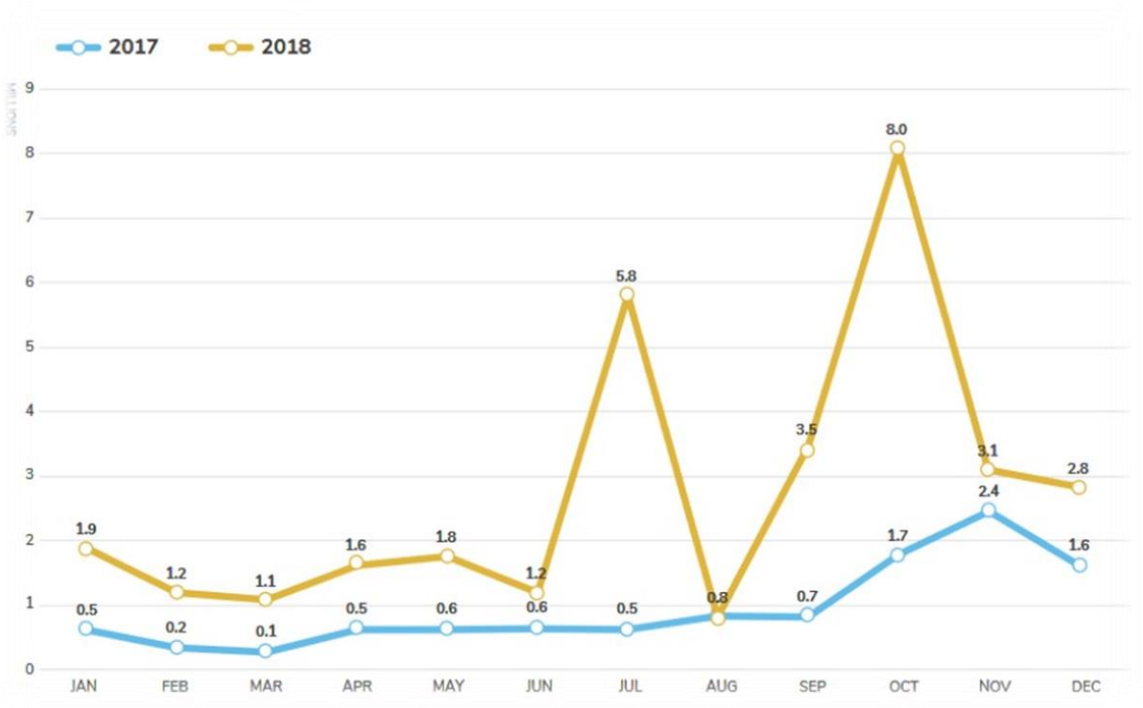


Figure 1. IoT sulmet përgjatë viteve 2017/2018

Fig 1 paraqet një ngritje për rreth 600 % të sulmeve të cilat janë evidentuar. Vërehet se ngritja më e madhe e sulmeve në vitin 2018 ka ndodhur përgjatë gjysëmvitit të 2018-tës dhe pastaj trendi ka vazhduar më rritje enorme përgjatë muajve në vazhdim. Nëse analizojmë shkeljet e të dhënave dhe privatësisë vetëm përgjatë dy viteve të fundit, mundë të verejmë një dallim dhe tendencë drastike të sulmeve të IoT paisjeve nga viti 2017 dhe 2018. Shqetësuese është fakti që ky trend nuk ka pësuar një ulje por vetem disa pauza përgjatë muajve ky prapë sulmi i rradhës ka dhënë rezultate më të mëdha se ai paraprak dhe se këto janë vetem disa të dhëna të cilat janë evidentuar dhe të cilat me gjasë të madhe nuk paraqesin numrin total të sulmeve.

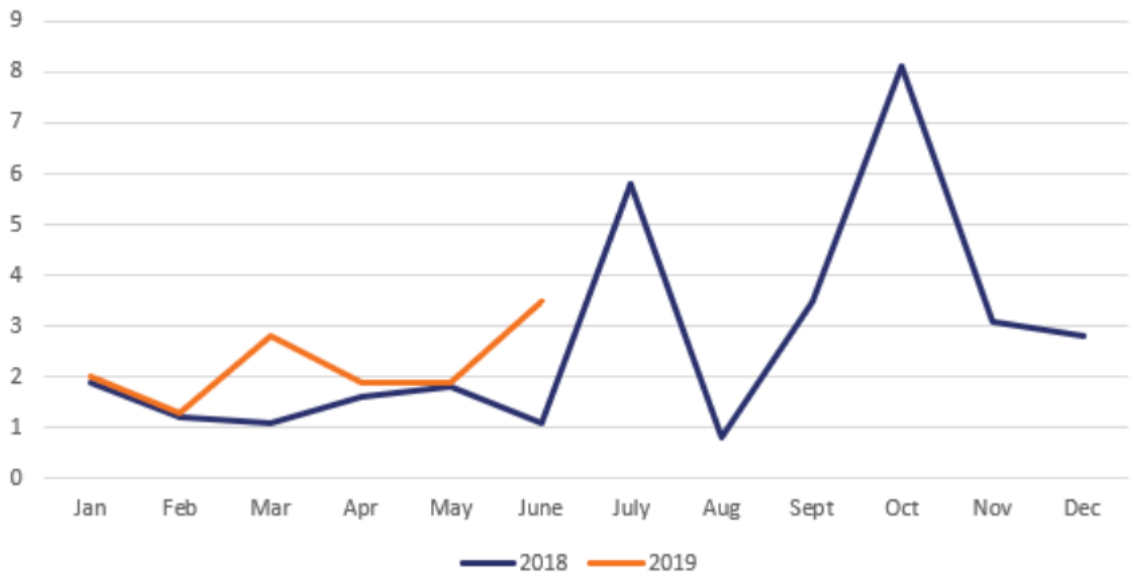


Figure 2. Sulmet malware ndaj paisjeve IoT

Fig 2 paraqet nje diagram i cili tregon rritjen e sulmeve kundrejt vitit paraprak. Sulmet ndaj IoT pasijeve përgjatë gjysëm vitit 2019 nuk kanë pësuar ndonjë tendence të rënies përkundrazi nga muaji shkurt deri në muajin qershorë kemi pësuar një rritje të sulmeve dhe e cila rritje llogaritet të jetë dikund rreth 217 % nga viti praprak 2018 Nëse vazhdon me këtë trend atëhere do të arrihet një record tjeter i sulmeve ndaj IoT paisjeve. Me pak se 20 % të përsonelit profesional mundë të identifikojnë sulmet në IoT paisje (Security Boulevard, 2019) kurëse 75% e sulmeve ndaj paisjeve IoT llogariten të jenë sulme në paisjet fundore si routers (Symantec data, 2019). Sipas një raporti të Avast në shkurt të këtij viti, 40.8 % të smart homes do të kenë në mesin e tyre të paktën një paisje IoT e cila është e ekspozuar ndaj rrezikut. Këto pasije janë në rrezik shkaku i softuereve jo të përditesuar kurse 2/3 e paisjeve të tjera do të jenë në rrezik shkaku i një fjalëkalimi të dobët. Rreth 92 % e të gjithë përdoruesëve duan që të PII të tyre të mbetet në kontroll (Economist Intelligence Unit), kurëse rreth 74 % e përdoresëve kan frikë nga humbja e të drejtave civile nga ndërhyrjet në të dhënat përsonale. IoT është një mundësi e madhe e bërjes biznes nga kompanitë e ndryshme por gjithashtu një mundësi e madhe për kriminelët kibernetik për të arritur qëllimet e tyre.

2.2 Blockchain në IoT

Teknologjia e Blockchain (BC) konsiderohet nga shumë profesionist dhe inxhinierë të sigurisë si pjesa e fundit e teknologjisë e cila ka munguar gjatë gjithë kësaj kohe. Shumë prej tyre bien dakort se një zgjidhje potenciale dhe premtuese është përdorimi i BC e cila teknologji është fundamenti i të gjitha kryptovalutave. Monedha e parë digjitale, Bitcoin e cila është formuar në vitin 2008 përdorë BC e cila nënkupton se është komplet e decentralizuar.

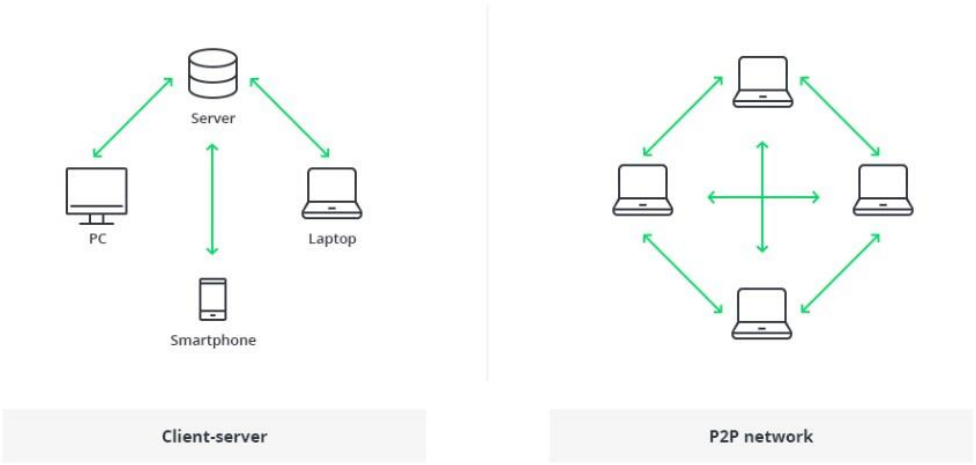


Figure 3. Dallimi i sistemit Client-Server dhe P2P

Fig 3 paraqet dallimet dhe vërehet se arkitektura Client-server dhe P2P janë plotesisht të ndryshme në substancë. Për dallim nga sistemet e centralizuara të cilat përdorin një autoritet të përbashkët të kontrollit Client-server, BC nuk përdorë sistem të centralizuar për të validuar të dhënat apo transaksionet por përdorë një sistem të decentralizuar Peer-to-peer ku secili host komunikon me secilin.

Pikërisht për faktin se sistemi decentral nuk ka nevojë për një autoritet qëndror i cili i merr të gjitha përgjithësitë e kontrollit, e bën këtë arkitekturë me interes të veqantë në aspektin e sigurisë. Ndër argumentet më të forta për të ju përgjigjur pyetjes se pse BC është zgjidhje potenciale e problemeve të sigurisë qëndron në faktin se duke eliminuar një autoritet qëndror të kontrollit gjithashtu eliminohet problemi i Single point failure, i cili problem është një ndër shqetësimet më të mëdha e të një inxhinieri të sigurisë. Nëse e shprehim ndryshe, kjo do të thotë se një sulmues për të fituar qasje të plotë të një sistemi BC, ai duhet të përfitojë qasje në të gjitha blloqet. Teorikisht është e mundur që të thyhet algoritmi por praktikisht me fuqinë më të madhe kompjuterike do të duheshin rreth 0.60 bilion vite që të realizohet kjo hipotezë. Supozojmë se ligji i Moore do të vlen ende dhe se algoritmi i enkriptimit mbetet i njejtë gjatë gjithë kohës, prapë do të duheshin rreth 60 vite për të thyer një bllok të vetëm në BC.

2.3 Llojet e Blockchain

Në bazë të kërkesës Blockchain mundë të përdoret për qëllime të ndryshme. Është e një rëndësie të veqantë që të aplikohet arkitektura e duhur për qëllimin e duhur. Jo të gjitha arkitekturat përshtaten për qëllime të ndryshme. Në vazhdim do të diskutojmë llojet e arkutekturave të BC.

Në përgjithësi Blockchain ndahet në tri arkutektura kryresore, por nuk kufizohet vetëm në këto tri arkitektura pasi që ka mundësi të shkallëzimit të arkitekturës për kërkësa specifike. Arkitekturat kryesore e ndahen në:

I. Blockchain publik
II. Blockchain privat
III. Blockchain me consortium

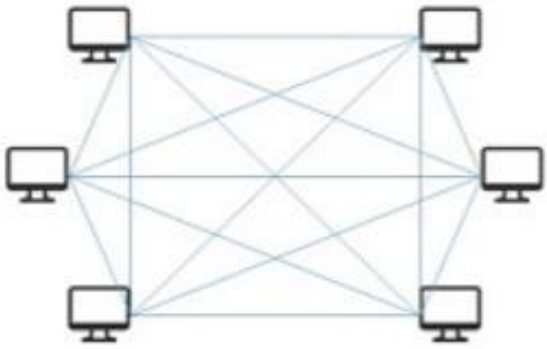


Figure 4. Blockchain public

Fig 4 paraqet një ilustrim të rrjetit të një Blockchain public. Ky koncept bazohet në idenë e një decentralizimi të plotë. Të gjitha nyjet mundë të marrin pjesë në shtimin e një blloku të ri në Ledger kryesorë dhe të përmbajë një kopje të përmbajtjes. Në arkitekturën publike të një BC, nuk ka kufizime për pjestarët e tjerë të rrjetit. Kjo arkitekturë është e dizajnuar që të përmbajë në vetë shumë nyje në të njëjten kohë. Të gjitha nyjet janë të sinkronizuara nëpërmjet një algoritmi të quajur Consensus, për të cilën do të flasim në vazhdim. Shkaku i numrit të madh të nyjeve të cilat marrin pjesë, shpejtësia e transaksioneve është më e ulët në krahasim më një arkitekturë private. Gjithashtu është më e shpejtë dhe me kosto më të ulët se sistemet e sotme që përdoren nga industria financiare.

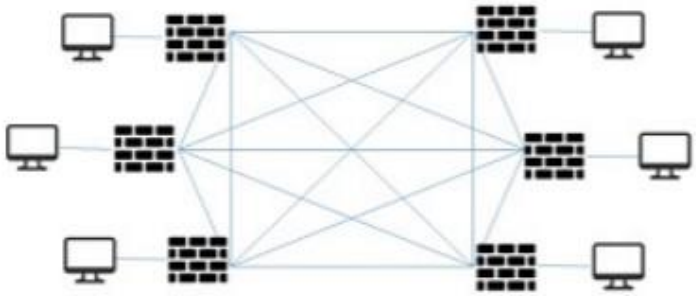


Figure 5. Blockchain privat

Fig 5 paraqet një ilustrim të rrjetit të një Blockchain privat. BC privat ka një dallim të qartë për nga mënyra e punës prej një BC publik. Përderisa arkitektura publike lejon qasjen në rrjet të seciles nyje pa kushte, arkitektura private nuk lejon qasje në rrjet të qfarëdo nyje. BC privat është një zgjerim i atij publik, për arsyje se zgjeron sigurinë duke impelemtuar një acces control layer në mënyrë që vetëm përsonat e njohur të mundë të qasen në BC. BC private janë më të lehta se ato publike dhe transaksionet kanë një shpejtësi më të madhe. Acces control layer i arkitekturës private eliminon nevojën e një konsensusi të besimit e cila zbatohet tek BC publik. Blockchain privat janë të përshtatshm për një implementim apo zgjidhje jo shumë të zgjeruar, shembull të një kompanie. Të gjithë antarët e kompanisë janë të njohur dhe në këtë mënyrë kontrolli i qasjes është më lehtë i implementueshëm.

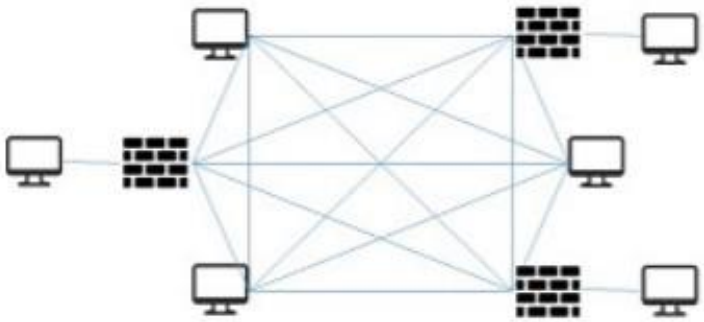


Figure 6. Blockchain me consortium

Fig 6 paraqet modelin hybrid të një arkitekture të BC e cila quhet arkitektura me consortium. Arkitekturën me consortium ndryshe mundë ta përshkruajmë si një lloj arkitekture në mes arkitekturës publike dhe asaj private. Arkitektura me consortium është një arkitekturë shumë fleksibile e cila lejon që Blockchain të përmbajë karakteristika më shumë publike por në të njejtën kohë mundë të vendoset që të përmbajë më shumë veti private, pra nuk ka ndonjë linjë të kuqë e cila në mënyrë të qartë definon se qfare veti do të përdorë. Kjo realizohet duke vendosur se cilat nyje do të marrin në përgjithësi shtimin e blloqeve të reja, cilat nyje do të bëjnë PoW apo në të njëjtën anë do të jenë në funksion të shtresës së kontrollit. Shpejtësia e transaksioneve është më e madhe se e asaj publike dhe me afër asaj private.

2.4 Veqoritë dhe struktura e një Blockchain

Në mënyrë që të kuptojmë potencialin e plotë të teknologjise BC dhe aplikimin e saj në IoT, është e rëndësishme që të kuptojmë principet e punës së një BC teknnologjie dhe sesi arrihet decentralizimi i saj. Blockchain është një teknologji komplekse, jo vetëm për njerzit të cilet nuk kanë njohuri të thella të teknologjisë por edhe për vet profesionistët e IT-së. Për këtë fakt nuk është gjithmonë e lehtë që të implementohet një teknologji e tillë.

Në vijim paraqesim një listë të karakteristikave kryesore e të një BC arkitekture:

I. **Decentralizimi** – në sistemet e centralizuara client-server, transaksionet apo të dhënat validohen dhe kontrollohen nga një autoritet central. Kjo mënyrë e trajtimit të të dhënave është e kushtueshme sepse serveri kërkon mirëmbajtje të vazhdueshme si dhe ka pengesa në përformancë. Në një infrastrukturë të decentralizuar eliminohet kërkesa për të pasur një autoritet central të validimit dhe kontrollit. Dy nyje apo hosts kanë mundësinë e shkëmbimit të të dhënave ndërmjet vete pa pasur nevoje për autoritet central.

II. **Pandryshueshmëria-** të gjithë antarët përmbajnë një kopje të Blockchain përkatës dhe kjo mundëson që antarët mundë të qasen në të gjitha transaksionet e bëra në Blockchain. Kjo është një veqori me benefit shumë të madh pasi që lejon që për të gjitha transaksionet të mundë të verifikohet prejardhja, pra Blockchain është shumë transparent.

III. **Anonimiteti** – të gjithë antarët e një Blockchain nuk ruhen më emer të identitetit të pronarit por me një shifer të gjeneruar, pra një pseudo emer. Kjo mundëson anonimitet, pasi që nëse një përdorues ka një interaksion më një Blockchain tjetër për ndonjë transaksion të caktuar atëherë ruhet privatesia e emrit të tij të vërtetë dhe në këtë mënyrë mundësohet që të mos dihet se në mes kujt është bërë transaksioni.

IV. **Toleranca e gabimeve** – gjdo antarë i Blockchain ruan nga një kopje të të gjitha transaksioneve ndërmjet tyre. Nëse ndodhë që të ketë ndonjë gabim apo një transaksion të korruptuar, atëhere gabimi në rrjet identifikohet më anë të një konsensusi nëpërmjet të cilit duke krahasuar të dhënat mundë të identifikohet saktë se në cilin bllok gjendet gabimi dhe pastaj të korigjohet.

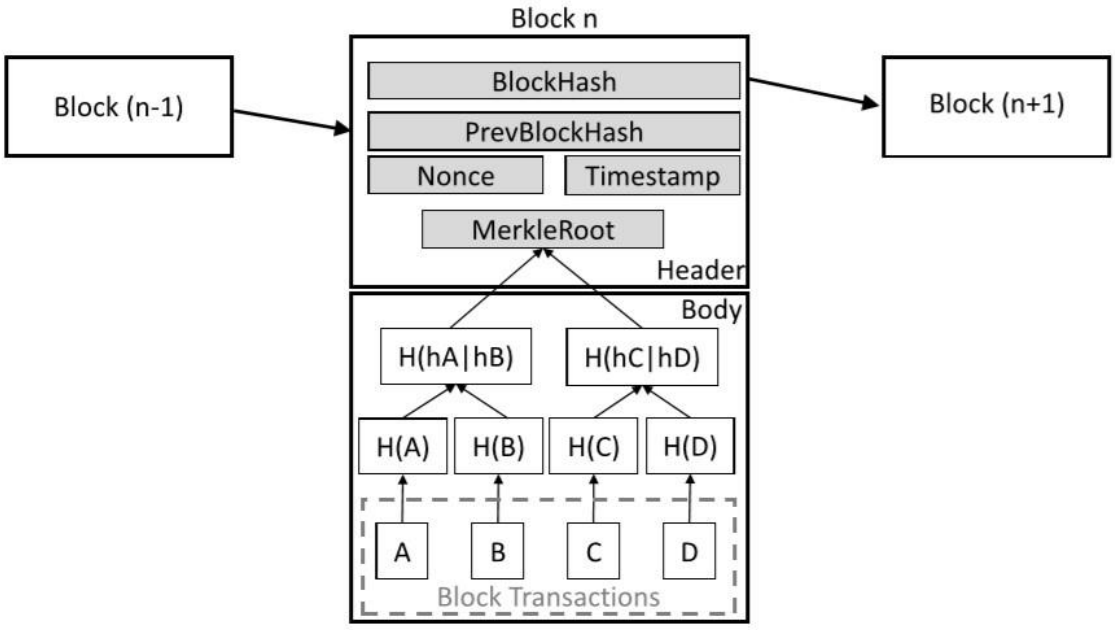


Figure 7. Reprezentimi logjik i nje blloku të Blockchain

Fig 7 paraqet në mënyrë logjike pjesët përbërse të një blloku në BC dhe mënyrën sesi përpunohet transaksioni. Një bllok është një set i transaksioneve, i ndërtuar me një strukturë të qartë të transaksioneve të cilat janë të rënditur në mënyrë kronologjike një nga një. Blloku i parë i zingjirit quhet **Genesis**. Struktura e një blloku përbëhet prej dy pjesëve:

I. **Header** - kryen një operacionin kriptografik dhe e bën punën të komplikuar dhe në këtë mënyrë arrihet që të mbrohet nga manipulimet. Merkle root ben hash të të gjithë transaksioneve në body. Merkle root redukton shumë kohen e verifikmit të një blloku pasi që përmban shifren e të gjithë hash funksioneve, kështu që kur të bëhet krahasimi i hash funksioneve për të garantur pandrysheshmerinë e një transaksioni përdorim merkle root. Nëse ndodhë që të kemi një bllok të korruptuar atëherë duke përdorur merkle root, ne mundë të garantojmë pandryshueshmërinë pa humbur shumë kohë dhe fuqi kompjuterike. Timestamp përmban kohën dhe datën e gjdo blloku të gjeneruar. Nonce është një numer i cili përdoret për të zgjidhur Proof-of-Work (PoW).

II. **Block content** – përbëhet prej të gjitha transaksioneve të cilat ruhen në mënyrë kronologjike. Gjdo transaksion përmban një ID të veqantë dhe e cila përbëhet prej një funksioni kriptografik të informatës e cila gjindet në të. Në këtë mënyrë arrihet që informata e cila gjindet në transaksion dhe e cila mundë të përbëhet dhe prej emrit të pronarit të transaksionit të mbetet anonime dhe private.

Shihet se struktura e brendshme e një blloku të BC është një strukturë më një kompleksitet të theksuar dhe e cila duhet analizuar dhe kuptuar mirë para se të bëjmë ndryshimet të cilat duhen për të adaptur teknologjinë në fjalë për nevojat tona të sigurisë.

Blochchain teknologjia është një proces i cili përbëhët prej katër koncepteve:

I. **Peer-to-peer network** – në Fig3 nënkupton eliminimin e një autoriteti qëndror për authentifikim dhe validim të të dhënave. Në këtë pjesë, nyjet e një rrjeti Blockchain komunikojnë ndërvete në mënyrë të lirë dukuë përdorur qelësat publik dhe privat të tyre.

II. **Databazë të hapur dhe të decentralizuar** – databaza ka një strukturë të caktuar në mënyrë kronologjike, pra të gjitha transaksionet ruhen në mënyrë kronologjike. Kjo strukturë është e hapur për të gjithë dhe nuk ka ndonjë autoritet qëndror për të shtuar ose fshirë transaksionet. Të gjitha nyjet e rrjetit kanë nga një kopjë të kësaj strukture dhe kjo mundëson që të gjitha nyjet të gjejnë asetin e tyre në strukturë dhe të shohin poashtu dhe asetet e nyejeve të tjera. Për më tepër të gjitha nyjet mundë të përcaktojnë në mënyre autonomë nëse një transaksion është valid apo jo.

III. **Sinkronizimi i databazës** – në mënyrë që struktura ku ruhen transaksionet të jetë e saktë, ajo duhet sinkronizuar. Sinkronizimi arrihet në tre hapa:
    a. Të transmetohen transaksionet e reja në rrjet
    b. Transaksionet e reja të validohen
    c. Transaksionet e validuara të shtohen në databazë

IV. **Mining** – mining është procesi i validimit dhe i shtimit të blloqeve në databazen kryesore. Para se transaksioni të shtohet në databazën kryesore, duhet të bëhet nënshkrimi i transaksionit, ndryshe njihet si Proof-of-Work (PoW).

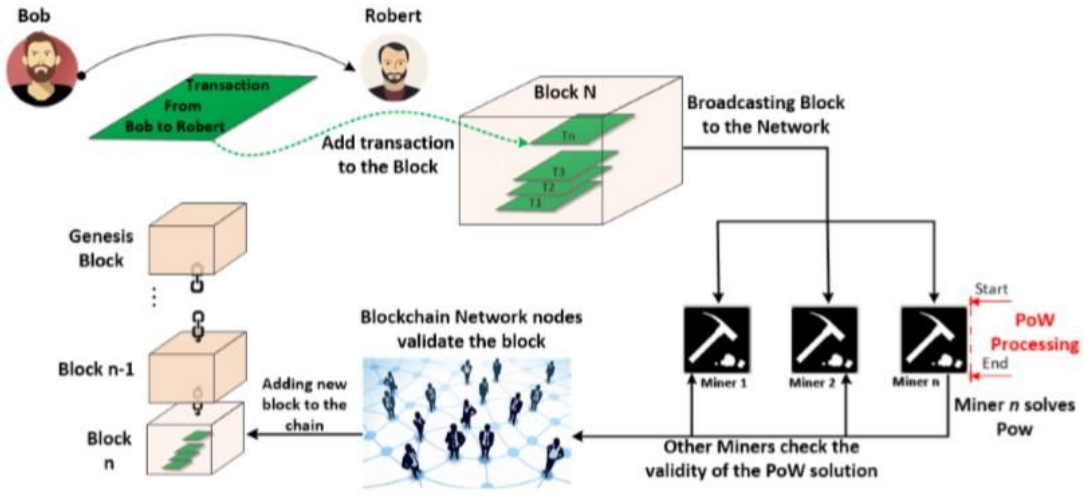


Figure 8. Transaksioni në Blockchain

Në Fig 8 simulohet rasti i inicimit të një transaksioni në BC deri në përfundimin e tij. Në këtë rast, Bob dëshiron që të bëjë një transaksion në llogarinë e Robertit. Supozojmë se asnjëri prej tyre nuk njeh njëri tjetrin, pasi që llogaritë e tyre ne BC përmbajnë një hash të të dhënave të tyre dhe jo të dhënat personale si identifikim. Transaksioni fillon duke enkriptuar transaksionin e Bob me qelsin publik të Robertit. Bob pastaj krijon në signaturë digitale duke marrë hash të të dhënave që do të dërgohen dhe pastaj enkriptohen me qelësin privat të tij. Të dhënat strukturohen në formë të bllokut si në Fig 4 me të gjitha informatat të cilat janë të nevojshme për të vazhduar me procesin. Pasi të enkriptohen të dhënat me qëlësin privat të Bob, të gjitha blloqet transmetohen në rrjet. Roberti decrypton signaturen digitale me qëlësin publik të Bobit dhe të dhënat me qëlësin privat të Bobit. Verifikimi bëhet kur të krahasohen hash e të dhënave me signature digitale të Bobit. I gjithë ky process njihet ndryshe si merkle root dhe gjendet në head bllok. Procesi i PoW përfshin validimin e të dhënave pra të Merkle root dhe gjejten e një numri Nounce për ta përfunduar procesin. Vërshtirësia e gjejtes së numrit Nounce Fig 5 varet direkt prej konfigurimit të blloqëve në një variablël të quajtuar difficulty apo dhe Nounce, gjendet në dy termet në literatura të ndryshme. Pasi të gjendet Nounce atëherë përfundimisht blloqet validuara kalojnë në databazen kryesore që njihet si Ledger.

Pasi të dhënat kalojnë në Ledger kryesorë, askush më nuk mundë të ndryshojë, fshijë apo te mohoj transaksionin e bërë pasi që të gjithë antarët e rrjetit e përmbajnë nga një kopjë të Ledger dhe kështu në këtë mënyrë evitohet gjdo gabim me apo pa qëllim i cili mundë të ndodhë. Detektimi i gabimeve në BC është një proces mjaft i shpejtë falë Merkle root e cila është e parallogaritur para se të futen të dhënat në Ledger kryesorë.

Deri në këtë pjesë kemi shtjelluar në mënyrë mjaft analitike strukturën dhe funksionimin e një BC dhe kemi listuar benefitët dhe veqoritë kryësore të një BC teknologjie. Falë këtyre vetive, BC rrëmben interes të veqantë në fushen e sigurisë. Në vazhdim do të shohim disa nga llojet e BC teknologjisë dhe pastaj do të flasim për konsensusin e besimit në BC. Aspektet kryesore janë shpejtësia dhe aftësia adaptive e BC teknologjisë në IoT. Pasi që IoT ka një dinamike shumë të shpejtë të shkëmbimit të të dhënave duhet një shpejtësi e duhur dhe performance të mjaftueshme të BC në mënyrë që të mundë të gërrshetohen të dy teknologjitë për të plotësuar nevojat e tregut.

2.5 Problemi i konsensusit

Për të zgjedhur se cila arkitekturë është më e përshtatshme dhe e cila i plotëson nevojat dhe kërkësat e tregut apo të kompanisë duhet të merren parasysh disa fakte. Një ndër faktet kryesore është shpejtësia, pra sa më shpejtë të bëhen transaksionet aq më mirë. Për të arritur këtë qëllim duhet pasur një ide të qartë të implementimit.

Një konsensus mundë ta paramendojmë si një protokol i cili ka tri veqori kryresore, si:

I. **Siguri** – protokolli i konsensusit ofron siguri atëherë kur të gjitha nyjet prodhojnë të njëjtin rezultat.
II. **Vlerë -** protokolli i konsensusit merr vlerë vetëm nëse të gjitha nyjet jo boshe eventualisht prodhojnë një vlerë të caktuar.
III. **Tolerancë të gabimit** – një protokoll i konsensusit prodhon tolerancë të gabimit vetëm nëse është në gjendje të rikuperohet prej ndonjë gabimi eventual.

Duke u bazuar në këto vlera të cekuara më lartë, të gjitha modelet e konsensuseve duhet që në mënyrë strikte të ju përmbahen karakteristikave, përndryshe nuk mundë të trajtohen si modele valide. Në vazhdim do të shtjellojmë disa nga modelet e konsensuseve, por lista nuk kufizohet vetëm me kaq sepse ekzistojnë ende modele të tjëra që fatkeqësisht në këtë punim nuk do të trajtohen.

Proof-of-Work (PoW) punon shumë mirë në një arkitekturë publike ku ka shumë nyje të cilat marrin pjesë. Përdoret nga Bitcoin dhe Ethernum, dy platformat më të mëdha të monedhave kriptografike. Në mënyrë që të mundë të shtohet një bllok, të gjitha nyjet duhet të vërtetojnë se kanë berë një punë. PoW bazohet në kalkulimin e një problemi shumë kompleks kriptografik. Për të zgjidhur ketë problem, kompjuterëet duhet të gjejnë një numer Nounce i cili përcaktohet nga protokolli i BC dhe është i ndryshëm për secilin bllok. Procesi i gjetjes së këtij numri ndryshe njihet si Mining. Një kompjuter i vetëm mundë të bëjë mining dhe shumë kompjuterë së bashku të krijojnë një Pool. Kompjuteri apo pool i cili zbërthen i pari problemin kriptografik, merr automatikisht të drejtën të shtoj bllokun në databazën kryesore e dhe në këtë mënyrë merr një shpërblim për punën e kryer. Qëllimi është që të krijohet një problem i vështirë kriptografik i cili kërkon fuqi të madhe procesorike dhe energji për ta zgjidhur. Kushti është që të gjendet një numer Nounce i cili plotësohen shkallen e vërshtirësisë së hash funksionit. Shkalla e vërshtirsisë përcaktohet në header të bllokut në mënyrë të pavarur.

Nëse kushti kërkon që të gjendet një Nounce i cili pasi të enkriptohet të gjenerojë tetëmbdhjetë zero rradhazi në header të shifrës së enkriptuar, atëhërë kompjuteri fillon që në mënyrë rastësishme të përcaktojë një numër dhe të fillon procesin e PoW në mënyrë që të plotësojë kushtin e vërshtirsisë që të mundë të shtohet në databaze. Nëse marrim në mënyrë të rastësishme numrin dy, atëhere supozojmë se do të gjenerohet ky hash rezultat si në figuren e mëposhtme.

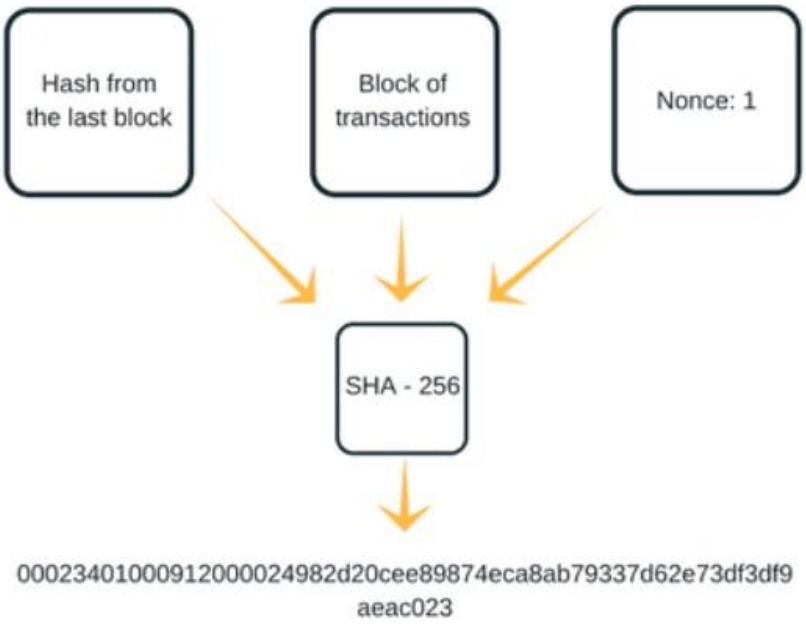


Figure 9. PoW jo valid

Hash rezultati në Fig 9 nuk është rezultati të cilin e kërkojmë me tetëmbdhjetë zero në header por gjeneron vetëm tre zero. Kompjuteri do të kërkon me rradhë të gjitha numrat deri sa të plotësohet kushti i dhënë.

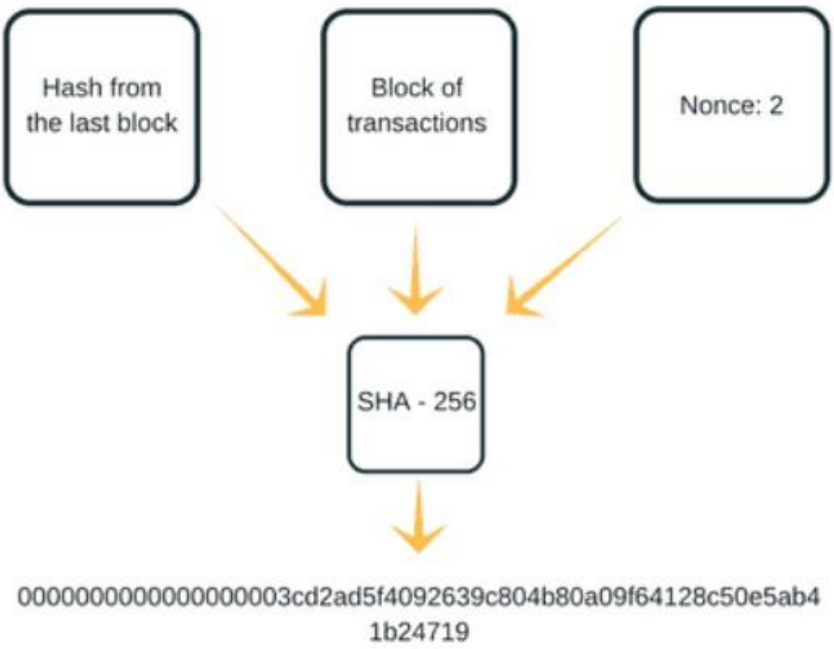


Figure 10. PoW valid

Në Fig 10 shihet se pas disa kalkulimeve të cilat kanë marrë X kohë dhe kanë bërë Y raste të kalkulimeve të Nounce të rastësishëm, më në fund ka arritur që të gjejë një Nounce i cili ploteson kushtin e vërshtirësisë i cili pason më tetëmbëdhjetë zero në header të vlerës së enkriptuar.

Megjithatë, përkundër faktit që ky protokoll punon shumë mirë, ekziston mundësia e sulmit të quajtur ’51 %’. Ky lloj i sulmit funksionon nëse një nyje ka më shumë se 51 % fuqi kompjuterike se të gjitha nyjet tjera së bashku. Kjo nënkupton se kjo nyje do të kalkulojë gjithmonë më shpejt se të gjitha nyjet tjera dhe se mundë të shton cilin do bllok në databazen kryesore e dhe ta transmetojë atë nëpër rrjet. Sulmuesi mundë të dyfishojë të gjitha transaksionet e veta dhe të bën një mohim të shërbimit ndaj transaksioneve reale. Pra

teorikisht është e mundur që të manipulohet me këtë protokoll dhe se duhet të sigurohet që askush të mos ketë 51 % të fuqisë.

Nëse e shikojmë nga një kënd tjeter, ky lloj protokolli prodhon një vonesë të madhe dhe që e bën të papërshtatshme për paisjë IoT të cilat kanë dinamike të madhe të shkëmbimit të të dhënave. Llogaritet që shpejtesia e PoW është afër 7 transaksione/sekond e cila është vlerë shumë e vogel duke marre parasysh sasisnë e të dhënave që prodhojnë paisjet IoT, madje nuk është e mjaftueshme as për sektorin financiar.

Proof-of-Stake (PoS) ka qëllim të njejtë, pra të arrihet konsensusi por ka një metodë tjetër të punës. PoS është dizajnuar që të eliminojë problemet të cilat i paraqet PoW, veqanërisht me shpenzimin e madh të energjisë elektrike. PoS eliminon nevojën e mining pasi që nuk ka nevojë që të zgjidhet një algoritëm komplex i cili garanton siguri dhe kështu në këtë mënyrë eliminon problemin e shpenzimit të madh të energjisë. Në algoritmin PoS nyjet që shtojnë blloqët në Ledger quhen validorë. Validorët duhet të bëhën pjesë e një rrjeti dhe të depozitojnë një vlerë të caktuar të parave në këtë rast mundë të supozojmë se mundë ta adaptojmë sistemin që validori të depozitojë të dhëna me vlerë. Shtrohet pyetja, pse?

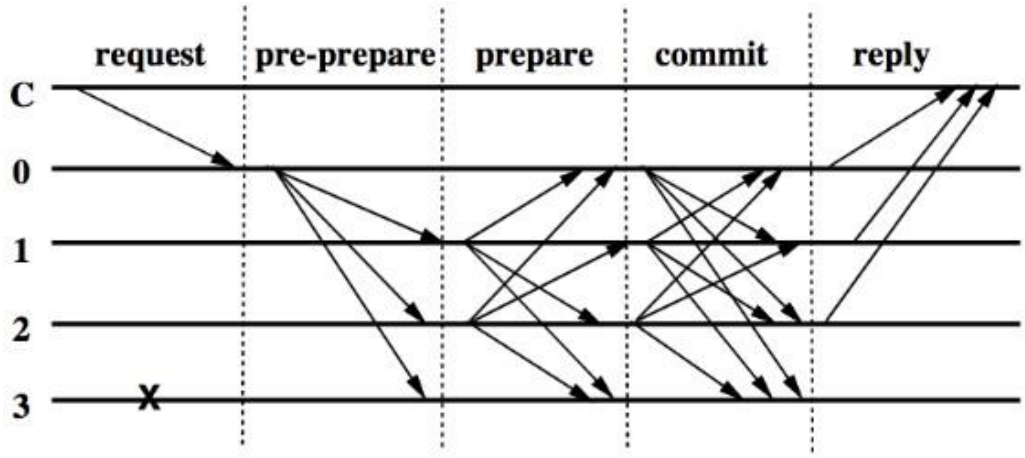
Kjo bëhët për shkak të sigurisë në rastin nëse një validor nuk kryen punën e tij në mënyrë korrekte duke shtuar blloqe të korruptuara në ledger. Nëse një validor bën gabimin e shtimit të një blloku të korruptuar në Ledger atëherë ai penalizohet duke humbur paratë apo të dhënat të cilat i ka depozituar si masë të sigurisë. Depozita e cila duhet të bëhët duhet të jetë gjithmonë më e madhe se sa vlera e cila mundë të fitohet. Teorikisht dhe praktikisht një validor do të humbë më shumë sesa fiton nëse korrupton një bllok. Zgjedhja e validorit bëhet në mënyrë të rastësishme përbrenda rrjetit, në këtë mënyrë askush nuk mundë të ketë dijeni se cila do të jetë nyja e ardhshme e cila do të zgjidhet për validim. Në fakt nuk është dhe tepër e rastësishmë sepse nyja e cila ka depozitën dhe mundësinë e humbjës së asteve më të madhe se të tjerët, ajo zgjidhet. Kjo shqetëson për faktin sepse praktikisht zgjidhet nyja e cila ka pasuri më të madhe dhe bëhet edhe më e pasur. PoS ka dhe një problem tjetër me sulmin

e ‘51 %’ por natyra e punës e bën më të lehtë sepse teorikisht për tu realizuar një sulm i tillë, nyja duhet të posedojë 51 % të të gjitha aseteve të rrjetit. Kjo është më e pazakontë që të ndodhe pasi që duhet një shumë tepër e madhe e aseteve që të realizohet, por teorikisht është e mundur. PoS ka pësuar disa ndryshme duke u avancuar me disa nën modele tjera, por të cilat nuk do të përfshihen në këtë diskutim pasi që nuk është qëllimi jonë primar.

Proof-of-Elapsed-Time (PoET) është një platformë u hapur e zhvilluar nga kompania Intel. Në mënyrë që të mundë të jesh pjesë e kësaj platforme nyjet duhet të shkarkojnë dy softuer të cilët janë: Trusted Execution Environment (TEE) dhe Software Guard Extensions (SGX). Algortimi funksionon duke zgjedhur në mënyrë të rastësishme një lider të grupit i cili do të merr përgjithësinë e shtimit të bllokut në Ledger. Kjo mundësohet duke përdorur SGX protokollin. Në mënyrë që ky protokoll të funksionojë lideri i grupit duhet të zgjidhet nga i gjithë rrjeti në mënyrë të rastësishme dhe të gjitha nyjet tjera duhet të verifikojnë se lideri është zgjidhur në mënyrë korrekte. Kjo mundësohet duke përdorur TEE. Ky algoritëm funksionon në atë mënyrë që nyja kërkon një kohë të ekzekutimit nga kodi i cili ekzekutohet në TEE. Nyja e cila ka kohën më të shkurtë fiton të drejtën e liderit. Intel garanton se TEE nuk mundë të manipuloet nga sofuer të jashtëm të cilët duan ta ndryshojnë kohën e ekzekutimit.

Practical Byzantine Fault Tolerance (pBFT) është njëra prej varienteve të Byzantin Fault Tolerance (BFT) algoritmeve e cila është një platformë e konsensusit dhe e cila përdorë një arkitekturë private të Blockchain. Identitetet në BFT jo vetëm që janë të njohura por janë gjithashtu të regjistruara në një regjistër qëndror përbrenda sistemit. Qëllimi kryesorë i BFT është që në një sistem të shpërndarë të nyjeve të arrihet një konsensus i mjaftueshëm ndërmjet nyjeve përkundër nyjeve të falsifikuara që duan të japin vlera false, duke parandaluar një dështim total të sistemit. BFT përdoret në sistemin ajrorë, impiante nukleare dhe në shumë sisteme tjera ku kërkohen veprime të bazauara në shumë sensorë. pBFT është një variant i BFT i zhvilluar nga Miguel Castro dhe Barbara Liskov në vitin 1999. pBFT punon më konceptin e replikimit të gjendejve të makinerisë (State Machine) dhe rezultateve që merr prej replikave. Duket e komplikuar në shikim të parë por do ta shtjellojmë në vazhdim.

Table 1. Hapat e pBFT



Në Table 1 kemi paraqitur një tabele me disa gjendje. Gjithesej kemi katër nyje të cilat janë 0 deri 3. Shkronja C paraqet një kerkesë apo klient, pastaj kemi tri gjendje të algoritmit pBFT: pre-prepare, prepare dhe commit. Gjithmonë nyja e pare është nyja kryesore. Transaksoni fillon kur prej klientit marrim një kërkesë dhe shkon tek nyja kryesore e 0. Nyja kryesore e 0 pastaj dërgon kërkesën tek të gjitha nyjet tjera 1,2 dhe 3 dhe keshtu fillon faza pre-prepare.

Nyjet përmbajnë numer sekuence, signatur dhe metadata të tjera për të verifikuar validitetin e pre-prepare kërkesës. Pasi të marrin mesazhin pre-prepare të gjitha nyjet vazhdojnë ta dërgojnë mesazhin tek nyjet e tjera. Në këtë mënyrë verifikohet nëse nyja kryesore ka berë kërkesën e njejtë tek të gjitha nyjet, nëse jo atëherë kërkesa është false. Nyja llogaritet nëse kalon fazen prepare dhe nëse ka parë kërkesën originale prej nyjes kryesore, është bërë pre-prepare dhe ka marre reply se paku **2f** mesazhe nga nyjet tjera. Duke llogaritur nyjen kryesore gjithësej bëhen **2f+1** mesazhe të marra. **F** është numri i byzantine faults.

Pasi nyjet kalojnë fazen prepare, ata dërgojnë një mesazh commit. Nëse nyjet marrin **f+1** commit kërkesa valide, atëherë ato kalojnë mesazhin tek klienti. Klienti pret prapë të marrë f+1 reply valide dhe kur kjo të arrihet atëherë përfundon transaksioni dhe klienti merr

përgjigjen e saktë. Prat e gjitha nyjet marrin pjesë në verifikimin e transaksionit. Nyja kryesore e propozon një sekuence dhe të gjitha nyjet tjera presin që të bien dakort për propozimin e bërë.

Federated Byzantine Agreement është një tjetër protokoll i konsensusit i zhvilluar nga Stellar. Në vend që pres për një përgjigjë të të gjitha nyjeve të rrjetit, nyja ka autonomi që të krijojë një nëngrup të tij të nyjeve të besueshme. Nyja merr vendimet duke u bazuar në një konsensus të rrethit të tij të besueshëm. Nëse ndodh një gabim, atehërë nyja penalizohet që të mbetet jashtë rrethit të besueshmërisë dhe të mos ketë të drejtë të marrë vendime.

Table 2. Krahasimi ndërmjet modeleve të konsensuseve

	PoW	PoS	PoET	BFT and variants	Federated BFT
Blockchain type	Permissionless	Both	Both	Permissioned	Permissionless
Transaction finality	Probabilistic	Probabilistic	Probabilistic	Immediate	Immediate
Transaction rate	Low	High	Medium	High	High
Token needed?	Yes	Yes	No	No	No
Cost of participation	Yes	Yes	No	No	No
Scalability of peer network	High	High	High	Low	High
Trust model	Untrusted	Untrusted	Untrusted	Semi-trusted	Semi-trusted
Adversary Tolerance	<=25%	Depends on specific algorithm used	Unknown	<=33%	<=33%

2.6 Smart Contracts

Smart Contracts (SC) për herë të parë është paraqitur në vitin 1994 nga Nico Szabo kur është marrë me sigurinë e rrjetave. Për shkak të teknologjisë së limituar të asaj kohe nuk ka gjetur zbatim në atë kohë. Smart contracs mundë të konvertohen, ruhen dhe të replikohen nga nyjet në BC.

Një smart contract është si një lloj marrëveshje tradicionale në mes dy palëve të cilët bien dakort për një shkëmbim të caktuar. Implementimi tradicional i BC ka mundësi të limituara të programimit. Smart contract është shumë më fleksibile se një BC tradicional dhe për këtë arsyje është quajtur dhe si një BC i programueshëm.

Një smart contract mundë të programohet në atë mënyrë që të kryej një punë të caktuar pa ndihmën e një pale të tretë TTP. Kodi i shkruar për smart contract mundë të vendoset në një BC dhe në këtë mënyrë të gjithë antarët mundë të thërrasin SC për funksionin të cilin e kryen. SC funksionon në atë mënyrë që garanton se palët do të marrin për atë që kanë rënë dakort. SC bazohet në një set të protokolleve ku secili prej pjesmarrësve duhet të pranojë rregullat.

Identiteti i palëve të cilat marrin pjesë në një SC garantohet nëpërmjet signaturës digitale. E gjithë kontrata praktikisht përkthehet në kod dhe i cili ruhet pastaj në BC. Pasi të ruhet në BC nuk mundë të mbishkruhet apo të ndryshojë. Algoritmi funksionon duke plotësuar kushtet **if-else**. Nëse plotesohet kushti i caktuar atëherë jepet shërbimi. Smart contratat kanë një veqori shumë të veqantë pasi që asnjëra palë nuk mundë të mohoj palën tjetër duke mos kryer obligimet pasi që sistemi nuk e lejon një gjë të tillë. Gjithë puna është e automatizuar dhe nuk mundë të interferohet më në të.

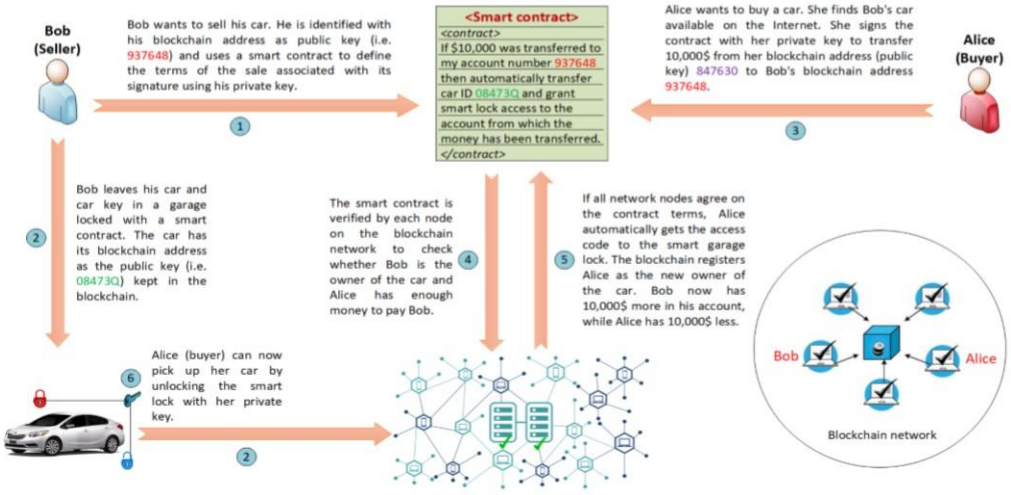


Figure 11. Implementimi i një Smart Contract

Fig 11 paraqet shembullin sesi realizohet një SC midis dy palëve. SC mundësojnë zgjidhje për shumë probleme me të cilat përballemi. Duke marrë parasysh potencialin e mbishkrimit të protokoleve mundë të supozojmë se në aspektin e sigurisë mjafton nëse shkruajmë protokolle të cilat identifikojnë përdoruesit përbrenda një rrjeti të caktuar. Kombinimi i teknologjinë BC dhe SC mundë të rezulton me zgjidhje premtuese të problemeve të sigurisë. Më vonë do të adresojmë disa zgjidhje potenciale.

2.7 Arkitektura e IoT Cloud Storages

Në hulumtimet e ndryshme që janë bërë për integrimin e BC në IoT paisjet, gjejmë disa lloje të arkitekturave të ndryshme. Në përgjithësi arkitekturat kategorizohen në tri domene të ndryshme:

I. Smart Home
II. Overlay Network
III. Cloud Storages

Që të tri kanë të bëjnë me transmetimin e të dhënave nëpërmjet IoT paisjeve. Në pamundësi që të trajtohen të tri domenet, në vazhdim do të flasim për cloud storages apo si cloud of things që ndryshe njihet nëpër disa literatura. Do të trajtojmë një arkitekturë konceptuale e cila mundë të aplikohet në disa skenare të ndryshme si dhe do të listohen projekte apo startups të cilat kanë implementuar në këtë drejtim.

Cloud of Things zakonisht janë data center të mëdha të shpërndarë nëpër vende të ndryshme. Decentralizimi i kësaj infrastruktre ka venë në pah se zgjeron largësinë ndërmjet klientit dhe provider më përkatësisht është rritur vonesa në komunikim. Për të ju përshtatur mevojës për të pasur një shpejtësi dhe fleksibilitet të lartë në komunikim janë zhvilluar cloud të decentralizuar që quhen Cloudlets. Cloudlets janë server më të vegjël të cilët gjenden më afër klientit dhe që zgjidh problemin e vonesës dhe garanton bandëidth të lartë.

IoT paisjet posedojnë zakonisht resurse të vogla të fuqisë së CPU nga disa MHz, 10s KB RAM dhe 100s KB ROM. Gjithashtu për të mbështetur disa enkriptime në disa paisjet IoT mundë të gjenden dhe module për enkriptim e cila mundëson një shtresë të sigurisë. Në vazhdim do të analizojmë arkitekturen e një IoT Blockchain koncepti të propozuar nga hulumtuesit e Universitetit të ETH Zürich në Zvicer.

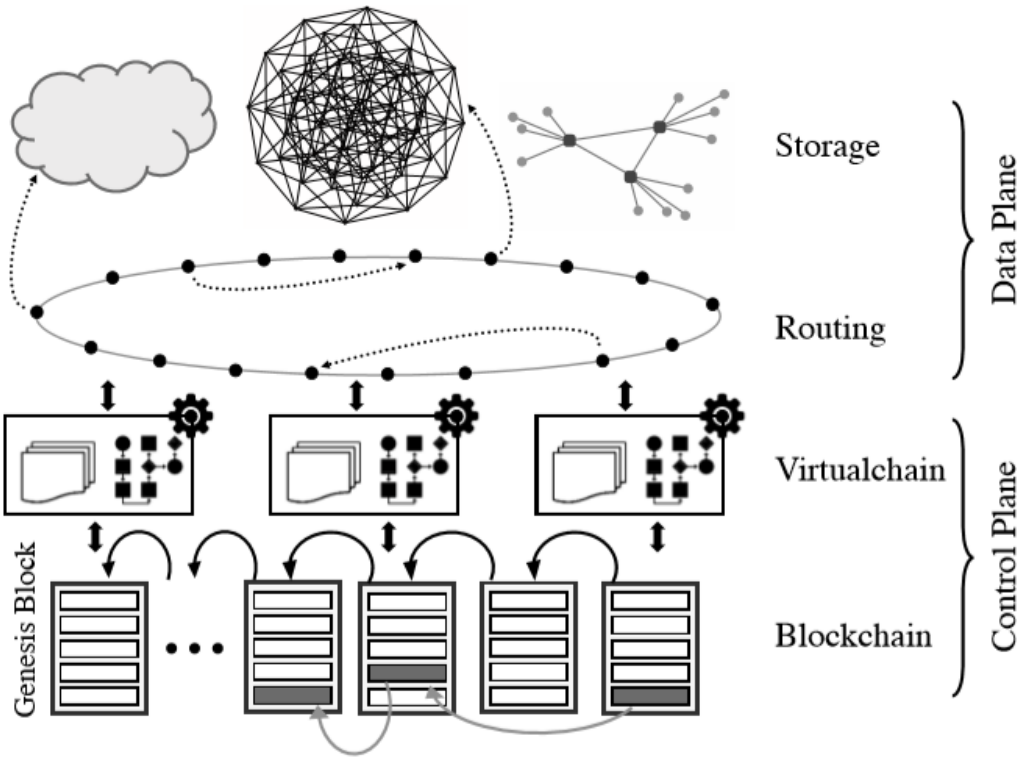


Figure 12. ***System design***

Fig 12 paraqet një arkitekturë të propozuar të një rrjeti cloud of things duke e ndarë atë në dy shtresa.

Arkitektura përbëhet prej:

I. Control Panel
   a. Blockchain
   b. Virtualchain

II. Data Plane
   a. Routing
   b. Storage

Control Panel: Në këtë pjesë logjike trajtohen problemet e *Access Control, Key Management dhe Revocation.* Për të siguruar siguri, anonimitet dhe mbi të gjitha një ndërveprim pa një kontroll central, hulumtuesit kanë zbatuar një koncept të decentralizuar të ruajtes së të dhënave. Koncepti për tu realizuar në praktikë përdorë Bitcoin por është e

mundur që të përdoren dhe valuta të tjera. Përdorimi i valutave të ndryshme është shumë praktike pasi që lejon fleksibilitet të lartë në strukturen e BC. E gjitha kjo mundësohet nga një Virtualchain (VC) e cila lejon shtimin e veqorive në transaksione në këtë rast monedhën më të cilen kryhet transaksioni por pa pasur nevojë që të ndryshohet struktura e përgjithshme e shtresës bazë së BC. Për qasje në të dhëna është përdorur një BC publik i cili menaxhon në mënyrë të sigurt kontrollin e qasjes. Të dhënat janë të ndara në të streams të veqantë.

Për të ndarë të dhënat më një service të caktuar kur të paraqitet nevoja, pronari në këtë rast inicon një transaksion i cili përmban një stream identifier dhe qelësin publik të marrësit. Kurse në rastin kur paraqitet nevoja për të marrë të dhëna të caktuara nyja e cila e përmban të dhënën së pari kontrollon në BC për të drejta në qasje nga nyja e caktuar.

Koncept tjeter shumë interesant që është paraqitur në këtë arkitekturë është koncepti i ***Key Management***. Ky koncept nënkupton implementimin e një algoritmi i cili gjeneron qelësa të ri për një qelës **Kt** në një kohë të caktuar ***t***. Kjo veoqri lejon përditësimin e qelsave aktual me qelësa të rinj dhe shpërndarjen e qelësave të rinj vetëm me nyje të cilat janë të besueshme. Për të parandaluar që nyja shpërndarëse të bëhet një ***bottleneck*** përdoret një tjetër objekt kriptografik i cili quhet rotation **scheme**.

Një problem tjetër të cilin e hasim në shpërndarjen e qelsave është koha e shpërndarjes ***O(n)*** për ***Kn*** shpërndarje të qelësit. Për të ardhur në kohen ***O(1)*** është propozuar teknika e ri-enkriptimit e cila realizohet duke ri-enkriptuar një ciphertext më një qeles publik të Alice ***PKa*** tek një ciphertext të Bob ***PKb*** pa pasur qasje në plaintext. Alice pastaj enkripton qelësat ***Kt*** me një one-time qelës ***(PKa, SKa)***. Për gjdo servis ***Si*** i cili kërkon qasje, Alice prap ri-enkripton tokenin ***(TSKa-PKs)*** duke u bazuar në qelësat public të serviseve ***PKs***. Gjdo servis ***Si*** prap ri-enkripton ***ENCPKa(Kt)*** në **ENCPKs*(Kt)***, duke përdorur qelësat e tyre privat ***(SKSi)*** për tu qasur në qelësat e rinj **Kt**. Pas kësaj Alice vetëm duhet të ndërron ***ENCPKa(Kt+1)*** për gjdo servis për të mundësuar qasje në qëlësat e fundit të gjeneruar.

Revocation bëhet me qëllim të revokimit të së drejtës që të lexohen të dhënat një nyje e caktuar ose ndryshe e shprehuar si ndalim i qasjes dhe komunikimit. Kjo realizohet duke përditësuar qëlësin ***Kt*** në ***Kt+1***. Pastaj bëhet përditësimi i ***ENCPKa'(Kt+1)***. Ky opëracion shkakton një vonese O(n) pasi që duhet të përditësohen të gjitha enkriptimet. Për siguri shtesë pronari mundë të inicon një transaksion të ri në BC që të mbishkruhet e gjithë lista e kontrollit të qasjes. Nyjet të cilat i ruajnë të dhënat nuk do të ndajnë më as të dhënat e vjetra në të cilat dikur një nyje e caktuar ka pasur qasje.

Data Plane përbëhet prej dy shtresave: Routing plane dhe një Storage të sigurt. Storages të tanishëm nuk janë të përshtatshëm për ruajtjen e të dhënave të IoT paisjeve dhe për këtë arsyje është propozuar që të dhënat të ruhen si copëza të vogla dhe jo gjdo të dhënë veqmas. Të gjitha copëzat e vogla janë të lidhur ndër vete në mënyrë kriptografike ku secila copëz përmban një pointer të copëzës tjetër dhe i cili pointer ruhet në BC. Gjdo copëz enkriptohet në source me një algoritmëm simetrik. Algoritmi i cili përdoret është ***AES-GCM*** i kategorisë së algoritmeve të authentifikimit. Me algoritmin e authentifikimit garantohet integriteti dhe authentifikimi i të dhënave. Për të siguruar autorsinë e të dhënave gjdo e dhënë përmbanë një **ID** të paenkriptuar e cila korrenspondon me një transaksion në shtresën e access control.

Për të kursyer bandwidth dhe hapsirë IoT të dhënat kompresohen para se të ruhen në copëza të vogla. Rezultatet e para kan treguar se kjo metodë funksionon shumë mirë përkundër se të dhënat janë të ruajtura në copëza të vogla. Search i të dhënave bëhet duke i ruajtur të dhënat duke kalkuluar hash të të dhënave si në vijim: **< *stream-ID, oëner-ID, timestamp*-hash >**, të gjitha ID janë stringje unike. Për të pasur një search effizicent dhe të shpejt përdoret një teknike e thjeshtë duke kalkuluar timestamp të copëzës e cila e përmban të dhënen dhe kështu evitojmë kërkimin e dyfishtë nëpër copëza të cilat nuk përshtaten me atë se qfarë kërkojmë. Për ruajtje të të dhënave siq është cekuar mundë të përdoret një cloud apo një on-përmise cloud në bazë të nevojës. Gjithashtu përdoret një IoT getëay server si një

nyje para se të dhënat të ruhen në storage. Getway merr kërkesat për ruajtje të të dhënave dhe i rendit ato në një **FIFO** rënditje për tu ruajtur pastaj në cloud. Gjithashtu getway serverët mundë të përdoren si një lloj cache për të dhënat të cilat thirren më shpesh. IoT aplikacionet e tanishme ruajnë të gjitha të dhënat njëherësh në cloud dhe pastaj prap i thërrasin ato për shtresën e prezantimit duke shkaktuar një vonesë të paarsyeshme.

Për storage të decentralizuar koncepti bazohet në *P2P Routing* teknikë dhe në ***Distributed Hash Table*** (*DHT*). *DHT* mundëson një ruajtje të replikuar dhe të rastësishmë të të dhënave përgjatë 160 bit hapsirë të adresave si dhe gjetjen e shpejtë të të dhënave i cili korrenspondon me qëlësin e caktuar dhe gjithashtu mundëson shtim dhe fshirje të të dhënave me një minimum të fuqisë kompjuterike. **Sloopy hashing** do të përdorej për të instancuar DHT. Në fund do të kishim një infrastrukturë në të cilën të dhënat do të ishin më afër servisit dhe pronarit në këtë rast.

2.8 Mekanizmat e sigurisë së IoT paisjeve të bazuara në Blockchain

Siguria në kuptimin gjenerik nënkupton mbrojtjen e të dhënave tona. Rreziku shfaqet nga shumë faktorë të ndryshëm por në thelb dallojmë dy faktorë kryesorë ë: faktorin njeri dhe faktorin natyrë. Tek rreziqet e faktorit njeri mundë të rendësimin të gjitha sulmet të cilat përbëjnë shkelje të llojit të qasjes së paautorizuar në të dhëna, kodet e dëmshme, vjedhja apo vandalizmi i të dhënave dhe kështu më rradhë. Kurse tek faktori natyrë mundë të cekim të gjitha katastrofat natyrore si uji, era apo zjarri dhe deri tek ndërpreja e energjisë elektrike.

Për të standartizuar këtë disciplinë janë krijuar protokolle dhe udhëzues të ndryshëm në mbrojtjen e fjalëkalimeve, firewall, procedura të enkriptimit etc. Në mënyrë që ky standartizim të gjejë zbatim në sistemet tona, siguria është ndarë në disa kategori që ndryshe njihet si trekëndëshi CIA.

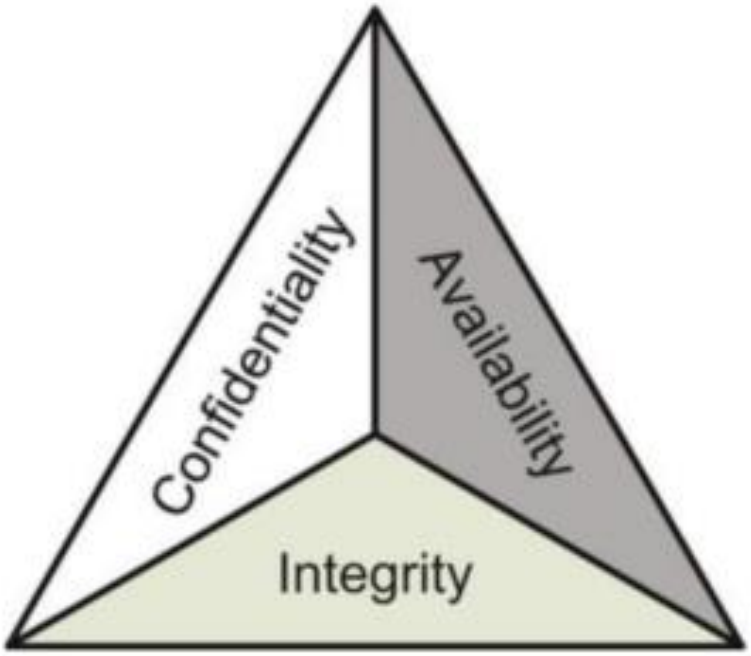


Figure 13. CIA Triad

Availability garanton se paisjet apo të dhënat janë të disponueshme në gjdo kohë dhe paisjet mundë të komunikojnë dhe të shkëmbejnë të dhënat pa pasur ndonjë ndërprerje të shërbimit.

Confidentiality garanton se të dhënat mundë të qasen vetëm nga përsona të autorizuar duke përdorur një set të rregullave. Pasi që IoT pasijet përmbajnë të dhëna kritike është e një rëndësie të veqantë mbrojtja e tyrë nga qasjet e paautorizuara.

Integrity garanton një servis të besueshëm ku pasijet të cilat përdorin protokollet e komunikimit për qëllim të shkëmbimit të të dhënave përcjellin mesazhet apo të dhënat në gjendjen e tyre origjinale përgjatë udhetimit për tek destinacioni.

Por karakteristikat e trekendëshit të CIA-as nuk mjaftojnë për të gjitha sulmet moderne që përgjatë zhvillimit të shpejtë të paisjeve IoT. Për të plotësuar këtë handicap nëse mundë ta quajmë ashtu është krijuar një standart i ri i cili quhet IAS-OCTAVE dhe ku fjala OCTAVE ka kuptimin e "**O**perationally **C**ritical **T**hreat, **A**sset and **V**ulnerability **E**valuation" dhe i cili mundë të përdoret si një plotësim i standartit të CIA.

Table 3. Standarti OCTAVE

Requierment	**Definition**
Confidentiality	Garanton se vetëm përsonat e autorizuar kanë qasje në informacion
Integrity	Garanton se të dhënat janë origjinale dhe të pandryshuara
Availability	Garanton se të dhënat janë të disponueshme në gjdo kohë
Accountability	Sistemi mban përgjegjës përdoruesin për veprimet e tij
Auditability	Sistemi monitoron të gjitha veprimet në mënyrë përsistente
Trustworthiness	Sistemi verifikon dhe ndërton besueshmëri me plaët e treat
Non-repudiation	Sistemi konfirmon nëse një veprim ka ndodhur apo jo
Privacy	Siguron se të gjitha të dhënat përsonale të përdoruesit trajtohen sipas procedurave dhe protokolleve

Table 3 paraqet standartin e zgjeruar OCTAVE për të përmbushur kërkesat e sigurisë së IoT paisjeve. Nga tabela kuptojmë se janë shtuar shumë veqori tjera të cilat përmbajnë në vetë disa kërkesa shumë me rëndësi dhe se në rastin ideal të një sistemi të sigurisë të gjitha këto kërkesa do të plotësoheshin.

Table 4. Blockchain IoT Services

Zonat gjenerale të IoT sigurisë më Blockchain	Zgjidhjet e propozuara	Funksionet kryesore
Acces Control	**Axon et al.**	PKI i bazuar në Blockchian
	Hashemi et al.	BC i veqantë për Data Storage dhe Data Acces
	Zhang et al. **FairAccess**	Qasje e priviligjuar me token për off-chain të dhëna
	Novo et al. **Enigma**	Qasje e priviligjuar me token për on-chain të dhëna
	Capchain	Funksione të smart contract për acces control shtresën
	Hamza et al.	Funksioni i acces control për big data
	Dorri et al.	Acces control protokollet e shkruara në header të bllokut
	Ali et al.	Acces control protokolle për IPFS data të shkruara në Smart contract
	Shafagh et al.	Smart contract

Data Integrity	**Biswas et al.**	Blockchain për të dhëna të pakomprementuara
	Dorri et al.	Blockchain multi shtresorë i cili mirëmbanë të dhënat në cloud based
	Enigma **Shafagh et al.**	Blockchain për të dhëna të pakomprementuara të ruajtura në DHT
	Liu et al.	Query të bazuar në Blockchain për verifikimin e integritetit të dhënave në cloud based
	Yang et al.	Sistem i cili garanton besueshmërine e mesazheve
	Lee et al.	Transaksione të bazuara në Blockchain i cili mundëson updatë të paisjeve embedded
	Steger et al.	Mundëson përditësimin e smart automejeteve duke përdorur Blockchain
		Ruan softëare përditesimet e IoT paisjeve në Blockchain

Confidentiality	**Axon et al.**	PKI i bazuar në Blockchian
	Aitzan et al.	DSO për adresimin e Blockchain
	Alphand et al.	Protokolle të sigurisë së Smart contract me OSCAR modelin e sigurisë
	Cha et al.	Getway i bazuar në Blockchain për komunikimin e paisjeve BLE
	Dorri et al.	Mundëson shkëmbimin e të dhënave ndërmjet përdoruesëve në një arkitekturë multi shtresore
	Ali et al.	Të dhënat e enkriptura IPFS shkëmbehen ndërmjet përdoruesve në një BC publik
	FairAcces	Qasjet e priviligjuara autorizohen me transaksione të verifikuara
	Hardjono et al.	Blockchain me kontroll të qasjes për komisionimin e IoT resruseve

Availability	**Alphand et al.**	Model i fault tolerance për modelin e autorizimit i bazuar në Blockchain
	Chakraborty et al.	Ndërlidh IoT paisjet nëpërmjet nyjeve të fault tolerance të Blockchain
	Ali et al.	IPFS transaksionet behen nëpërmjet një Blockchain publik
	Bagha et al.	Paisjet smart të prodhimit ndërlidhen me një Blockchain infrastrukturë

Table 4 tregon aplikimin e Blockchain dhe Smart Contract teknologjisë në katër standartet e sigurisë të cilat mbrojnë sistemet tona. Përkunder faktit se Blockchain është një teknologji me një teori dhe aplikim të ndërlikuar, shohim se disa startups apo kompani kanë arritur që të krijojnë disa projekte apo sisteme të bazuara në BC. Rëndësi të veqantë është fakti se ekzistojnë tashmë mjaft projekte me të cilat mundë të punojmë dhe se duke i kombinuar njohuritë të fitojmë një model të ri të sigurisë. Zgjedhjet e propozuara kanë të bëjnë specifikisht vetëm me sigurinë por nuk duhet të harrojmë faktin se ekzistojnë shumë projektë tjera të të cilat kanë të bëjnë me jetën tonë të përditshmë të cilat janë realizuar duke përdorur Blockchain apo Smart Contracts por fatkeqësisht janë jashtë fokusit të këtij hulumtimi.

3 DEKLARIMI I PROBLEMIT

Duke e pasur parasysh që siguria e të dhënave është duke u kthyer në një temë shumë të rëndësishme në ditët e sotme, diskutohet gjithnjë e më shumë që të gjenden zgjidhje të reja dhe inovative prandaj hulumtuesit gjithnjë janë përpiqur që gjetjet e tyrë të jenë sa më afër kërkesave të tregut në mënyrë që ti përmbushin ato. Mangësia e mbrojtjes së të dhënave ka një ndikim të madh në të gjithë shoqërinë duke nisur nga organizatat e ndryshme biznesore dhe ato jo biznesore, konsumatorët e rregullt global që përdorin internetin për blerje dhe komunikim të përditshëm e deri tek sistemet qeveritare. Impakti për të cilin paguajnë qmimin është shumë i lartë pasi që shpesh here të dhënat të cilat rrjedhin në mënyrë jo të ligjshme nuk kan vlerë të parasë më të cilin mundë të ishin paguar dhe si rrjedhojë e kësaj humbja apo rrjedhja e të dhënave ka një impakt shumë të madh si në jetën përsonale të individit gjithashtu vetëm pak organizata biznesorë mundë të rikupërohen nga dëmtimi financiar dhe të rindërtojnë imazhin e tyre pas ndonjë humbje të të dhënave. Nëse nuk punohet që të zgjidhjet problemi ateherë në mundë të parashikojmë një ngecje të zhvillimit të teknologjise së komunikimit pasi që sistemet do të ishin jo të sigurta për përdorim. Dukë marrë parasysh të gjitha ato që i cekëm më lart për fat të mirë hulumtuesit dhe inxhinierët punojnë gjdo ditë që të kenë një zgjidhje sa më adekuate dhe që përmbush kërkesat. Me aplikimin e teknologjisë së BC në sistemet e sigurisë, dhe pse jo të gjitha shqetësimet do të mbaronin me kaq por do të kishim një zgjidhje premtuese me të cilin do të mundë të punonim tutje për përshtatjen dhe gërrshetim sa më të mirë të sistemeve ndër vete me qëllim të arritjës së një sigurie e cila na mundëson përdorim dhe më të madh të teknologjisë.

4 METODOLOGJIA

4.1 Dizajni i kërkimit

Për këtë studim është përdorur metodologjia e hulumtimit nëpërmjet studimit të literaturës ekzistuese. Studimi është realizuar duke kombinuar literaturën kërkimore me atë induktive. Qëllimi i këtij studimi ka qenë që të hulumtohen aspeketet kryesore të problemit i cili është hulumtuar pak. Duke kombinuar literaturën kërkimore dhe atë induktive së bashku është tentuar që të paraqitet një teori për problemin e caktuar e cila ofron një zgjidhje adekuate dhe të realizueshme. Duke pas parasysh se inputi i të dhënave që kam analizuar dhe procesuar ka qenë si rrjedhë e analizimit të literatures ekzistuese, nuk kam pas ndonjë kontroll në mënyrën sesi janë gjeneruar të dhënat. Gjithashtu është shpenzuar kohë dhe procesim shtesë për analizat e bëra duke marrë në konsideratë që fusha nuk është hulumtuar dhe prefeksionuar shumë dhe të dhënat kanë qenë ekspërimentale dhe teori të ndryshme për zgjidhje të problemit. Është analizar një numer i madh i dokumenteve në formë tekstuale si dhe gjithashtu të dhënat në mënyrë vizuale. Nëpërmjet analizës së mirëfillt është tentuar që të balancohet përshkrimi i teorive si një bahkësi konceptesh me interpretimin të qartë dhe të thellë.

Ky studim ka përdorur këto metoda:

a) Metoda përshkruese – është përdorur për të përshkruar të gjeturat e studimit të literaturës si dhe përshkrimit të tabelave dhe paraqitjeve vizuale.

b) Metoda krahasuese – është përdorur për të bërë krahasimin e të dhënave me qëllim të definimit sa më të saktë të koncepteve të disa pjesëve më të ndërlikuara.

4.2 Burimi i të dhënave

Burimi i të dhënave për këtë studim ka qenë kërkimi në internet, literatura e gjetur online, libra si dhe artikuj të ndryshëm në relevancë me llojin e probemi të cilin e kemi trajtuar. Të gjitha të dhënat shkencore të përdorura në këtë studim bazohen në punime shkencore profesionale të punuar nga njerëz profesional të fushes së sigurisë së të dhënave dhe të cilat punime janë të viteve të fundit dhe aktuale. Si bazë kryesore e e këtij studimi janë marre disa nga punimet shekncore të cilat janë analizua dhe prej të cilave rrjedhin të dhënat më të rëndësishme dhe teoritë të cilat ndërtojnë një bazë teorike dhe praktike të zgjidhjes së problemit. Përpunimi dhe selektimi i burimit të të dhënave nuk ka qenë proces i lehtë pasi që është dashur që të analizohet me kujdes përmbajtja e cila pastaj duhet të jetë relevante me rrjedhën e hulumtimit. Nuk ishte e lehtë që të gjenden punime të thukta me informacion të bollshëm pasi që infrastruktura është ende duke u zhvilluar sipër dhe se ka projeksone të shumta sesi mundë të gërrshetohen teknologjitë së bashku.

5 PËRMBLEDHJE

IoT si koncept është paraqitur ne fillim të punimit dhe vazhdon me një historik kronologjik të rritjes së sulmeve dhe shtjellimin e statistikave të sulmeve kundrejt IoT paisjeve në kapitullin 2.1. Kapitulli 2.2 vazhdon me prezantimin e Blockchain si një koncept në tërsi dhe pastaj duke diferencuar sistemet tradicionale prej sistemeve të decentralizuara me qëllim të kuptimit të qartë të konceptit të decentralizimit. Në kapitullin 2.3 studimi vazhdon duke kategorizuar arkitekturat e ndryshme të Blockchain teknologjisë.

Nga kapitulli 2.4 punimi vazhdon duke prezantuar karakteristikat kryesore e të cilat duhet të ofron një Blockchain teknologji dhe pastaj në mënyrë vizuale dhe shpjegim logjik studimi vazhdon me paraqitjen e një blloku të Blockchain duke vënë theks të veqantë në strukturën e tij të brendshmë, duke trajtuar të gjitha komponentet dhe funksionet e tyre. Pastaj janë trajtuar në tërsi të gjitha fazat prej gjenerimit të një transaksioni deri në përfundimin e tij, paraqitur në Fig 8.

Pas ndërtimit të njhurive bazë për Blockchain si teknologji, kapitull 2.5 trajton një problematikë me një kompleksitet më të lartë të problemit dhe atë të problemit të koncensusit. Pasi është shtjelluar problemi i konsensusit si koncept, studimi vazhdon me trajtimin e llojeve të konsensuseve dhe veqorive të cilët duhet të ju përmbahen. Duke analizuar studimin bëhet shumë e qartë se problemi i konsensusit ka një rendësi shumë të veqantë dhe se e gjithë logjika e shfrytëzimit të resurseve qëndron për faktin se qfarë modeli të konsensusit përdorë një Blockchain i caktuar. Duhet të përmendet fakti se modelet e konsensuseve të e listuara në këtë punim nuk përfundojnë me aq dhe se ekzistojnë variantë të ndryshmë të tyre. Kapitulli 2.6 vazhdon trajtimin e Smart Contract duke prezantuar në fillim konceptin bazë dhe pastaj në mënyrë vizuale dhe logjike procesin e punës në Fig13.

Kapitulli 2.7 fillon me trajtimin e arkitekturave të ndryshme të IoT paisjeve me Blockchain dhe vazhdon pastaj duke prezantuar dhe shtjelluar një arkitekturë të një IoT Cloud Storage të propozuar nga disa hulumtues të ETH University Zürich.

Për fund, kapitulli 2.8 vazhdon me trajtimin e mekanizmave të sigurisë të standartit CIA dhe zgjerimin e këtij standarti për të plotësuar kërkesat e sigruisë së IoT pasijeve. Pastaj vijon duke paraqitur në mënyrë tabelare disa nga projektet e bazuara në Blockchain dhe Smart Contract për të plotësuar kërkësat e standarteve të sigurisë me të cilat ne punojmë që të mbrojmë sistemet tona.

6 PËRFUNDIME

Përderisa teknologjitë e shkëmbimit të informacionit gjdo ditë dhe më shumë po pësojnë një rritje dhe avancim në aspketin teknologjik, varësia e njerzëve kundrejt këtyre teknologjive po rritet së bashku në mënyrë paralele me avancimin e tyre sikurse rrezikshmëria e ekspozimit të informacioneve të ndjeshme. Pas hulumtimit sekondar dhe analizimit të informacioneve është evidente se sulmet ndaj sistemeve të ndryshme dhe me theks të veqantë ndaj sistemeve IoT nuk po pësojnë ndonjë rënie por po ndodh e kundërta. Sulmet nuk po bëhen vetëm ndaj pasijeve të ndryshme por edhe ndaj vet protokolleve të komunikimit të cilat janë përgjegjëse për mbledhjen dhe transmetimin e të dhënave.

Hulumtimi si tërsi është i një niveli teorik. Pjesa teorike unifikoi modelin e Blockchain teknologjisë e cila ishte qelës për të identifikuar mundësitë e shumta që ofron kjo teknologji sa i përket aspektit të inkorperimit të saj në sistemet tona të sigurisë. Gjithashtu është treguar se qfarë duhet të përmbajë një Blockchain infrastructure. Megjithatë modifikimi i një teknologjie të tillë dhe aplikimi i saj në skenare ku rreziku është me i madh sesa benefitet, mbetet një rrezik i cili mundë të anashkalohet lehtë. Pritshmëritë janë se Blockchain do të bejë revulucion në industrinë e IoT dhe se integrimi i këtyre dy teknologjive duhet të adresohet mëtutje.

Problemi i konsenësusit luan nj rol shumë të rëndësishëm sa i përket procesit të mining të cilin kritikët e shohin si konsumues të madh të resurseve të energjisë i cili pastaj krijon ndotje më të madhe të ambientit kur bëhet fjalë për të prodhuar atë sasi të energjisë. Mendimi im përsonal është se ka modele eficiente të konsensuseve të cilat mundë të japin zgjidhje potenciale me zero ndotje të ambientit dhe prapë ti shftytëzojmë benefitet potenciale. Skepticizem shfaqet gjithashtu kur bëhet fjale për shkallzueshmërinë e Blockchain, pasi që është bërë punë e vogel sa i përket kësaj asaj fushe.

Duke marrë parasysh zhvillimin e shpejtë të IoT pasijeve dhe integrimin e tyre në jetën tonë të përditshme, është duke u berë një punë e ngadaltë sa i përket zhvillimit dhe standartizimit të protokolleve të sigurisë për IoT pasijet. Kjo nënkupton që kompanitë e mëdha teknologjike dhe kompanitë e prodhimit të IoT pasijeve duhet të konsiderojnë më seriozisht kërkimin në këtë fushë, përndryshe gjithë kjo rritje e përdorimit të pasijeve të reja IoT vetëm do të simulonte sulme të tjera.

Gjithashtu, përpara se kjo teknologji të mundë të aplikohet në masë të madhe duhen të adresohen disa qështje me rëndësi, si: shpejtësia e transaksioneve, konsumi i energjisë, avancimi i standarteve të implementimit, mungesa e konizave ligjore, krijimi i ekosistemit të përshtatshëm të BC si dhe të krijohet zgjidhje në rast të aplikimit të Quantum Computing, e cila mendohet se në një të ardhme jo shumë të largët mbetet një ndër kërrcënimet kryesore kundrejt sistemeve kriptografike pasi që fuqia kompjuterike e cila mundë të prodhohet nga ky sistem kompjuterik qëndron shumë më lartë në krahasim me kompjuterët të cilët përdoren në ditët e sotme për sistemet e ndryshme.

7 REFERENCAT

[1] Ali, I., Sabir, S., & Ullah, Z. (2019). ”Internet of things security, device authentication and access control: a review”. Cornell University. (Online article). https://arxiv.org/abs/1901.07309

[2] Ali, M. S., Vecchio, M., Pincheira, M., Dolui, K., Antonelli, F., & Rehmani, M. H. (2018). “Applications of blockchains in the Internet of Things: A comprehensive survey”. IEEE Communications Surveys. (Online article). https://ieeexplore.ieee.org/abstract/document/8580364/citations?tabFilter=papers#citations

[3] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). “Blockchain for IoT security and privacy: The case study of a smart home”. IEEE Communications Surveys. (Online article). https://ieeexplore.ieee.org/abstract/document/7917634

[4] Kaulartz, M., & Heckmann, J. (2016). “Smart Contracts-Anwendungen der Blockchain-Technologie“. ProQuest. (Online article). https://search.proquest.com/openview/b5d2fe75babb6e2f20860d49717079e7/1?pq-origsite=gscholar&cbl=2038913

[5] Khan, M. A., & Salah, K. (2018). “IoT security: Review, blockchain solutions, and open challenges”. ScienceDirect. (Online article). https://www.sciencedirect.com/science/article/abs/pii/S0167739X17315765

[6] Lin, I. C., & Liao, T. C. (2017). “A survey of blockchain security issues and challenges”. (Online article). http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf

[7] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2019).” Integration of Blockchain and Cloud of Things: Architecture, Applications and Challenges”. Cornell University. (Online article). https://arxiv.org/abs/1908.09058

[8] Panarello, A., Tapas, N., Merlino, G., Longo, F., & Puliafito, A. (2018). “Blockchain and iot integration: A systematic survey”. MDPI. (Online article). https://www.mdpi.com/1424-8220/18/8/2575

[9] Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research handbook on digital transformations*. ElgarOnline. (Online article). https://www.elgaronline.com/abstract/edcoll/9781784717759/9781784717759.00019.xml

[10] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). "On blockchain and its integration with IoT. Challenges and opportunities." ScienceDirect. (Online article). https://www.sciencedirect.com/science/article/pii/S0167739X17329205

[11] Shafagh, H., Burkhalter, L., Hithnawi, A., & Duquennoy, S. (2017, November). "Towards blockchain-based auditable storage and sharing of iot data". ACMDL. (Online article). https://dl.acm.org/doi/abs/10.1145/3140649.3140656