APLIKIMI I TEKNOLOGJISË BLOCKCHAIN NË ZINXHIRËT E FURNIZIMIT

ALBANA GORISHTI[1], BLERINA VIKA[2], ERGIN GORISHTI[3]

[1,2] Universiteti i Tiranës, Fakulteti i Ekonomisë, Departamenti i Statistikës dhe Informatikës së Zbatuar

[3]Universiteti i Tiranës, Fakulteti i Ekonomisë, MSHSIE

e-mail: albana.gorishti@unitir.edu.al

Përmbledhje

Blockchain konsiderohet si një inovacion me potencial për të çuar decentralizimin e teknologjisë së informacionit në një stad të ri. Blockchain është një bazë të dhënash e shpërndarë ndërmjet personave apo pajisjeve pjesëmarrëse në rrjet që në gjuhën angleze referohet shpesh me termin "distributed ledger", një përkthim i përshtatshëm i të cilit do të ishte një libër llogarish i shpërndarë. Avantazhi kryesor i blockchain përballë teknologjive të tjera është siguria e shtuar. Elementet të cilët i japin blockchain karakteristika të tilla sigurie, janë jo vetëm në formën e mekanizmave, por dhe në vetë konceptimin e saj si një qendër informacioni pa një zotërues të vetëm. Implementimi i blockchain për krijimin dhe funksionimin e kriptomonedhave shënon një hap shumë të rëndësishëm në zhvillimin e kësaj teknologjie. Gjithsesi perspektiva e blockchain e tejkalon kufirin e kriptomonedhave dhe implementimet e saj mund të shërbejnë për zgjidhjen e një numri të madh problemesh dhe evoluimin e shumë praktikave të cilat kanë hapësirë për përmirësim nga bota e biznesit dhe jo vetëm. Ky artikull ka si qëllim trajtimin dhe demonstrimin praktik të përdorimit të blockchain në përmirësimin e zinxhirit të furnizimit për një biznes, duke paraqitur hapat e implementimit.

Fjalë kyçe: Blockchain, distributed ledger, zinxhiri i furnizimit.

Abstract

Blockchain is considered to be a ground-breaking inovation that has the potential to elevate the information technology world to a new plateau. A blockchain is a databased shared among the network participating devices that is known as a "distributed ledger". The main advantage of using this technology is the increased safety in comparison to other forms of data storage. Blockchain is considered "safe" not only because of the technical mechanism of the technology but also due to blockchain conception as a non-private database itself. Implementing blockchain for the development and the distribution of cryptocurrencies is a very important milestone in the lifecycle of the technology. However the potential of blockchain exceeds the border of cryptocurrenices and its implementation can be the answer to a number of problems and improvement opportunities regarding the business world and beyond. The goal of this paper is to theoretically overview the technology and to practically demonstrate the step-by-step implementation of blockchain in the improvement of a business supply-chain mechanism.

Key words: Blockchain, distributed ledger, Supply-chain.

Hyrje

Blockchain konsiderohet si një inovacion me potencial për të çuar decentralizimin e teknologjisë së informacionit në një stad të ri. Arsyeja përse kjo teknologji njihet kështu është sepse në një nivel bazik ajo i mundëson komunitetit të përdoruesve të regjistrojnë transaksione brenda komunitetit në një mënyrë të sigurt dhe të patjetërsueshme: Yaga., *et al* (2018). Elementet të cilët i japin blockchain karakteristika të tilla sigurie janë në formën e mekanizmave teknike (për shembull: kodimet hash, Proof-of-Work, Proof-of-Stake etj.) por dhe në vetë konceptimin e saj si një qendër informacioni pa një zotërues të vetëm.

Ideja për këtë teknologji është prezantuar për herë të parë në fillimin e viteve 1990 nga Haber dhe Stornetta: (1991). Pavarësisht këtij fakti, fuqia e blockchain nuk do të shfrytëzohej dhe për afërsisht 18 vjet të tjera derisa në vitin 2008 Satoshi Nakamoto aplikoj konceptin e Haber dhe Stornetta në ndërtimin e kriptomonedhës së parë të njohur si "Bitcoin". Në vitet pasuese u krijuan dhe shumë valuta të ngjashme (Etherium", "Dogecoin","Shiba"etj.) dhe popullariteti i tyre në tregjet financiare rrjedhimisht solli njohjen e blockchain dhe përmasave të potencialit të saj për një publik më të gjerë. Gjithsesi mund të thuhet se teknologjia është akoma në fazat e para të saj dhe nuk është adoptuar gjerësisht në fushën e sipërmarrjes: Abeyratne & Monfared (2016).

Përdorimi i blockchain në prodhimin e kriptomonedhave është një temë relativisht e trajtuar në mënyrë të thellë nga studiues dhe artikuj të ndryshëm. Fokusimi i kërkimeve në këtë "sferë" të blockchain është i kuptueshëm duke qenë së rritja e popullaritetit të saj mund ti faturohet këtij lloj implementimi. Gjithsesi, sa vjen e më tepër studiuesit po vënë theksin mbi mundësitë e përdorimit të kësaj teknologjie në një kuadër më të gjerë. Pikërisht këto zhvillime shërbejnë si frymëzim për realizimin e këtij artikulli për të ofruar ide të përdorimit në fusha të industrisë, përtej kripto valutave. Perspektiva e blockchain e tejkalon kufirin e kriptomonedhave dhe implementimet e saj mund të shërbejnë për zgjidhjen e një numri të madh problemesh dhe evoluimin e shumë praktikave të cilat kanë vend për përmirësim nga bota e biznesit dhe jo vetëm. Punimi ndalet në mënyrë më të plotë në aplikimin e blockchain për përmirësimin e zinxhirit të furnizimit (supply-chain) të supozuar të një ndërmarrje, për të cilin është zhvilluar dhe një implementim praktik. Aplikimi ka si qëllim demonstrative që shpjegon me detaje se si do të duhet të aplikohej teknologjia në botën reale. Në mbyllje të punimit janë dhënë konkluzionet si edhe rekomandime për punën e mëtejshme.

Blockchain

Blockchain në vija të gjëra mund të thuhet së është një mënyrë e ruajtjes së të dhënave e cila është e decentralizuar, e patjetërsueshme dhe e sigurt. Pilkington

e përkufizon blockchain si një regjistër i shpërndarë digjital transaksionesh i cili nuk mund të manipulohet për shkak të përdorimit të metodave kriptografike: Pilkington (2016). Këto metoda përfshijnë kodimet Hash dhe mekanizma të tjerë. Kjo teknologji mundëson komunikimin e informacionit në mënyrë të drejtpërdrejt ndërmjet dy pjesëmarrësve në rrjet në atë që njihet si peer-to-peer(p2p). Siguria që ofron ky mekanizëm jep mundësin e krijimit të një rrjeti ku prania e një entiteti ndërmjetësues është e tepërt. Një demonstrim i këtij koncepti vjen nga bota e ekonomisë ku Bitcoin, Etherium etj. shihen si një alternativë ndaj sistemeve tradicionale bankare

Një blockchain mund të jetë publik ose privat në varësi të fushës ku do të përdoret. Një blockchain publik konsiderohet ai i cili i jep të gjithë përdoruesve leje për të kryer veprime mbi të (read and write permissions) ndërsa privat quhet kur vetëm një numër i verifikuar përdoruesish i kanë këto të drejta: Miraz & Ali. (2018).

Blockchain dhe kodet Hash

Një blockchain është i përbërë nga dy komponente: transaksioni dhe blloku: Miraz & Ali (2018). Transaksioni konsiston në aksionin apo veprimin që iniciohet nga përdoruesi, për shembull në rastin e kriptomonedhave mund të jetë transferimi i fondeve nga një portofol në një tjetër. Blloku është një koleksion të dhënash që regjistrojnë transaksionet dhe detaje të tjera të rëndësishme për blockchain si kodet hash apo të dhëna të tjera shtesë si koha e krijimit etj. Ajo çka e bënë këtë mënyrë të ruajtjes së të dhënave të pandryshueshme është lidhja ndërmjet blloqeve për të formuar "zinxhirin". Kjo lidhje arrihet nëpërmjet kodeve Hash. Një funksion Hash është një mekanizëm kriptografie i cili përllogarit një kod për një mesazh të dhënë në mënyrë të tillë që : Thomsen & Knudsen (2009)

a) kodi është unik për mesazhe të ndryshme,

b) të jetë e pamundur që nga një kod i dhënë të arrihet në mesazhin origjinal,

c) të jetë e pamundur që kur jepet një mesazh të gjendet një mesazh tjetër me të njëjtin hash.

Një bllok përfshin disa të dhëna në lidhje me transaksionet. Këto të dhëna (koha, sasia e valutës apo adresa e marrësit të valutave) shërbejnë si argumente për tu futur në funksion dhe për të prodhuar një kod i cili do të identifikojë në mënyrë unike bllokun. Në momentin që një e dhënë e bllokut do të ndryshohet, në mënyrë automatike kodi do të ndryshojë. Secili bllok përveç kodit hash të tij përmban dhe kodin e bllokut paraardhës në zinxhir. Në këtë mënyrë blloqet janë të lidhur në formë të pandashme nga njëri-tjetri. Po ti referohemi figurës së mëposhtme (Figura 1), në qoftë së do të tentohej të ndryshohej përmbajtja e bllokut **n** do të ndryshonte dhe kodi Hash i këtij blloku i referuar në figurë me

emrin "Hash **n**", por regjistrimi i këtij kodi në bllokun **n+1** nuk do të ndryshonte dhe do të dallohej një mospërputhje ndërmjet tyre. Kështu, do të ishte mjaft e lehtë që të kuptohej se në blockchain ka pasur një ndërhyrje. Në mënyrë të ngjashme mund të arsyetohet për çdo bllok të zinxhirit.

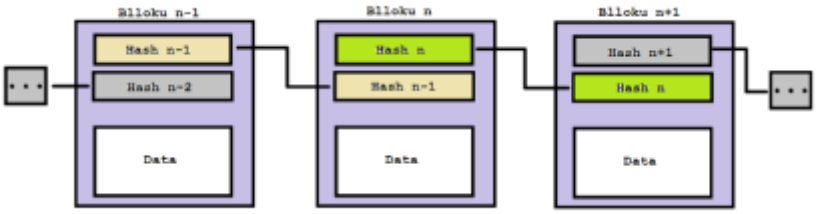

Figura 1: Skema e Blockchain (Burimi: Autori)

Shtimi i blloqeve në zinxhir

Shtimi i një blloku në zinxhirin e blloqeve është një element shumë i rëndësishëm pasi është thelbësor për sigurinë, shpërndarjen dhe decentralizimin e tij. Përpara së të shpjegohet procesi i shtimit të bllokut duhet dhënë një përshkrim i shkurtër mbi nyjat (nodes) e një ekosistemi blockchain. Nyjet janë aktorët që marrin pjesë në komunitetin blockchain. Për shembull në rastin e një blockchain publik çdokush mund të bëhet pjesë e këtij "ekosistemi". Roli i këtyre nyjeve është krijimi dhe vlefshmëria e blloqeve. Në momentin që duhet të krijohet një bllok i ri dhe ti shtohet zinxhirit lind pyetja se kush do ta krijojë këtë bllok pasi blockchain u takon të gjithë pjesëmarrësve në këtë rrjet. Për të zgjidhur këtë dilemë hyjnë në veprim mekanizmat e konsensusit të cilat janë të llojeve të ndryshme. Pasi një bllok krijohet ai i komunikohet të gjithë nyjeve të tjera që ato të përditësojnë blockchain-in e tyre me bllokun e ri. Më pas çdo nyje ka mundësin të verifikojë në mënyrë individuale nëse një bllok është i vlefshëm duke kontrolluar kodet hash dhe mekanizmat e tjerë në procesin që quhet validim: Yaga D., et al (2018). Kështu arrihet një sistem në të cilin pjesëmarrësit vendosin se çfarë do ti shtohet bllokut ekzistues dhe se çfarë është e vlefshme në të. Ka disa modele mekanizmash konsensusi ku ndër të cilët mund të përmendim: Proof-of-Work, Proof-of-Stake, Proof-of-Authority, Proof-of-Bandwidth, Delegated Proof-of-Stake etj: Li *et a*l (2020). Dy më të përdorurat janë Proof-of-Work dhe Proof-of-Stake:

Proof-of-Work është mekanizmi që përdoret nga Bitcoin. Ky mekanizëm bazohet në përdorimin e fuqisë kompjuterike të nyjeve si një provë për krijimin e "ndërgjegjshëm" të bllokut: Gervais et al (2016). Supozohet se duke qenë se një kohë dhe një sasi e konsiderueshme e resurseve kompjuterike për krijimin e një blloku, një nyje nuk i intereson të prodhojë një bllok jo të rregullt pasi ai më pas mund të mos-validohet nga nyjet e tjera.

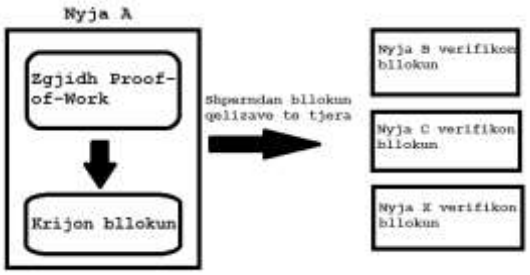

Figura 2: Mekanizmi Proof-of-Work (Burimi: Autori)

Proof-of-Stake, në këtë rast blloku krijohet nga një nyje që përcaktohet në mënyrë rastësore. Në këtë model për të pasur mundësin për të krijuar blloqe secili përdorues duhet të vendos në formë garancie një vlerë të caktuar (stake). Për shembull, në rastin e Etherium nyja duhet të vendosë një sasi të caktuar valute si provë që nuk do të ndërtojë një bllok keqdashës. Nëse blloku i krijuar nuk validohet nga nyjet e tjera atëherë krijuesi do të humbasë vlerën në fjalë. Për këtë arsye përdoruesit janë të interesuar të prodhojnë vetëm nyje të rregullta. Sa më e madhe të jetë vlera e vendosur aq më e madhe është mundësia që nyja të përzgjidhet për të krijuar një bllok.

Implementimi i blockchain në zinxhirin e furnizimit

Një zinxhirë furnizimi është një sistem i përbërë prej tre ose më shumë faktorë të cilët marrin pjesë në mënyrë të drejtpërdrejtë në rrjedhën e mallrave, shërbimeve, financave apo informacionit nga burimi të konsumatori: Mentzer *et al* (2001). Në një mënyrë më të thjeshtuar mund të thuhet se një zinxhirë furnizimi apo siç njihet në gjuhën angleze një "supply chain" është rrjeti i të gjithë firmave apo faktorëve tregtar të cilët kanë një rol në prodhimin, përpunimin, transportin apo shitjen e produktit duke filluar nga furnizuesit e lëndës së parë e deri të tregtarët me pakicë. Sipas Hugos aktorët që përbëjnë një "supply chain" përfshijnë furnizuesit në njërin skaj, konsumatorët në tjetrin, një numër kompanish përgjatë zinxhirit që kanë funksione të tilla si prodhues, shitës me shumicë apo pakicë dhe kompani të cilat ofrojnë shërbime në logjistik, financë, marketing dhe teknologji informacioni: Hugos (2018). Pra, një zinxhirë furnizimi nuk është asgjë tjetër përveç se bashkësia e firmave të cilat bëjnë të mundur që një produkt të vijë në formën e tij komerciale te konsumatori final.

Menaxhimi i një zinxhiri furnizimi ka të bëjë me koordinimin e pjesëmarrësve në të për sa i përket funksionaliteteve të tilla si prodhimi, inventarizimi, vendndodhja dhe transporti. Kuptohet që një zinxhir furnizimi i mire-organizuar dhe efecient sjell përfitime për të dyja palët e përfshira në tregti: shitësit dhe blerësit. Funksionimi siç duhet i zinxhirit të furnizimit përkthehet në shitje më

të mëdha dhe shpenzime më të ulëta nga perspektiva e firmave por edhe në rritjen e kënaqësisë së blerjes nga ana e konsumatorëve.

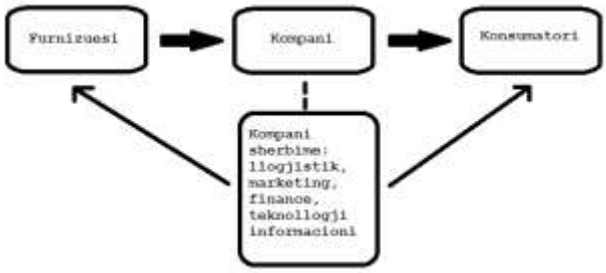

Figura 3: Skema e zinxhirit të furnizimit (Burimi: Autori)

Menaxhimi i zinxhirëve të furnizimit është sot një ndër sfidat më të mëdha të botës së biznesit. Ndonëse nuk është një fushë e re studimi ka akoma mangësi që lidhën me organizimin dhe operimin e zinxhirëve të furnizimit në formën e tyre aktuale. Kryesisht këto problematika lidhen me kompleksitetin dhe natyrën multidimensionale të zinxhirit të furnizimit: Garcia & You (2015). Kompani me përmasa të mëdha e kanë gjithmonë e më të vështirë për të koordinuar dhe menaxhuar proceset dhe aktorët përgjatë zinxhirit. Është mjaft e vështirë të kapen, ruhen, përpunohen dhe transmetohen sasi të mëdha informacioni në një formë të sigurt dhe efecientë në një sistem kaq kompleks. Rezultati është një zinxhirë furnizimi me të meta, jo-transparent dhe jo-efikas. Avantazhet apo përmirësimet që mund të sjell blockchain përballë sistemeve aktuale që përdoren në zinxhirin e furnizimit sipas Timothy Leonard kanë të bëjnë me: eficencën, reduktimin e kostos, sigurinë, transparencën, fleksibilitetin dhe inteligjencën.

Eficenca do të thotë që përdorimi i blockchain në zinxhirin e furnizimit sjell përmirësim dhe bën më të lehtë integrimin e proceseve të ndryshme në sistem. Gjithashtu blockchain mundëson automatizim në një nivel më të lartë. **Reduktimi i kostove** gjithashtu lidhet me efektivitetin por jo vetëm. Teknologjia e blockchain mendohet të ulë nevojën për punë manuale dhe rrjedhimisht të reduktojë faktorin që njihet si gabim njerëzor.

Përgjatë këtij punimi është përcaktuar **siguria** si një ndër karakteristikat kryesore të blockchain. Sigurisht, që firmat mund të përfitojnë nga ky avantazh duke arritur kështu të ruajnë informacionin që vjen përgjatë zinxhirit të furnizimit në një mënyrë të sigurt. Kjo vjen në dy nivele: së pari, informacioni është i sigurt nga ana teknike, në kuptimin që mundësia për tu manipuluar është shumë e vogël; dhe së dyti. i sigurt do të thotë dhe i besueshëm në rastin e blockchain pasi një bllok pasi është krijuar duhet të validohet dhe pas kësaj të dhënat në të nuk mund të ndryshohen në një moment të dytë.

Një tjetër karakteristik, ndoshta më e rëndësishmja që blockchain i "ofron" zinxhirit të furnizimit është **transparenca**. Nëpërmjet këtij implementimi, jo vetëm firma por dhe vet konsumatorët mund të gjurmojnë produktet në kohë reale në një aplikim i cili ofron besueshmëri të lartë.

Së fundmi, **fleksibilitet** në kuptimin që mund të lidh sisteme të ndryshme përgjatë zinxhirit. Gjithashtu kjo teknologji krijon një mundësi më të madhe për grumbullim dhe analizë të dhënash në kuadër të asaj që njihet si **inteligjencë** biznesi.

Aplikimi i blockchain në zinxhirët e furnizimit

Blockchain mund të aplikohet në zinxhirët e furnizimit në degë të ndryshme të industrisë dhe mund të shërbejë për funksione të ndryshme. Gjithsesi ekzistojnë disa parime të cilat kanë vlerë për rastin e përgjithshëm të aplikimit të kësaj teknologjie. Blockchain mendohet të përdoret si një mënyrë për të ruajtur informacion përgjatë ciklit të zinxhirit. Ky informacion në aplikime të ndryshme mund të jetë i ndryshëm dhe arsyeja përse ai duhet të ruhet në blockchain e jo në mënyra të tjera gjithashtu ndryshon. Zinxhirët e furnizimit gjithmonë e më tepër po shihen si procese ciklike e jo në formë lineare siç ka qenë koncepti tradicional: Casado-Vara *et al* (2018). Feedback-u që merret përgjatë etapave të ndryshme të zinxhirit është shumë i rëndësishëm për të gjithë aktorët që marrin pjesë në të. Implementimi i teknologjisë blockchain bën që ky model i zinxhirit të furnizimit (ku transparenca dhe aksesi në informacion merr më tepër rëndësi) të jetë i aplikueshëm për shkak të karakteristikave të vet teknologjisë të përmendura dhe më parë në punim.

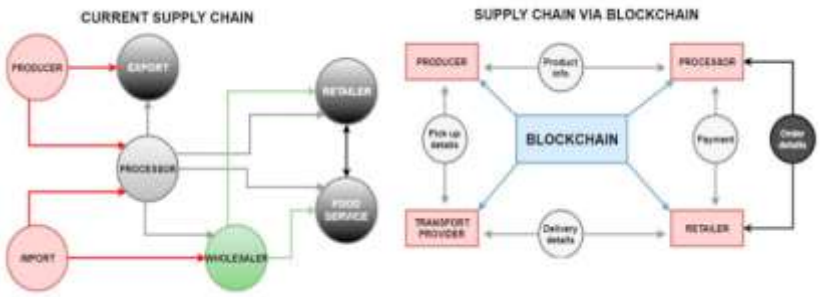

Figura 4: Zinxhiri i furnizimit tradicional përballë atij me blockchain (Burimi: Casado-Vara *et al* (2018)

Në këtë punim, aplikimi është modeluar për një kompani tregtare e cila pjesë të aktivitetit të saj ka transportin ndërkombëtar të mallrave dhe transporti kërkon përfshirjen e aktorëve të ndryshëm. Duhet të kryejnë lëvizjen e produkteve nga prodhuesit apo shitësit me shumicë deri te klienti i cili mund të jetë në anën tjetër të botës. Implementimi i blockchain në këtë proces synon të ruajë të dhënat

e shkëmbimit të produkteve ndërmjet kompanive të ndryshme përgjatë zinxhirit në një mënyrë të sigurt dhe më efektive. Përmendim që ky aplikim ka qëllime tërësisht demonstruese dhe është i papërshtatshëm të përdoret në jetën reale për arsye teknike por kjo edhe për vet procesin e zinxhirit të furnizimit i cili është thjeshtëzuar së tepërmi për t'ju përshtatur formatit të punimit. Ky implementim është punuar në gjuhën e programimit Javascript për kodin burim dhe në Angular për pjesën "front-end".

Ndërtimi i kodit burim të blockchain

Krijimi i aplikimit blockchain fillon me ndërtimin e kodit burim. Fillimisht është shkruar kodi për krijimin e bllokut si një strukturë të dhënash, i cili nuk është asgjë tjetër përveç se një objekt i cili përmban disa atribute ku të domosdoshme janë vlera hash i bllokut dhe vlera hash i bllokut paraardhës. Në këtë aplikim blloku gjithashtu përmban një variabël për të ruajtur kohën e krijimit (time), variablin transactions i cili do të ruajë të dhënat për shkëmbimin e produkteve ndërmjet kompanive transportuese dhe variablin të quajtur fallco i cili shërben për zgjidhjen e mekanizmit Proof-of-Work që do të shpjegohet në vijim. Funksioni calculateHash() përdor funksionin e gatshëm sha256() të librarisë "crypto-js" për të prodhuar një kod hash me të dhënat që përmban blloku.

```
class Block{
  constructor(time, transactions, previousHash=''){
  this.previousHash=previousHash;
  this.time=time;
  this.transactions=transactions;
  this.fallco=0;
  this.hash=this.calculateHash();  }
  calculateHash(){  return
SHA256(this.previousHash+this.time+JSON.stringify(this.transacti
ons)+this.fallco).toString();  }
```

Për të minuar një bllok të ri duhet të zgjidhet mekanizmi Proof-of-Work. Në këtë aplikim është zgjedhur të përdoret i njëjti algoritëm që përdoret për monedhën kripto Bitcoin, i cili kërkon që një numër i caktuar i karaktereve të para të kodit hash të bllokut të jenë zero. Ky numër përcakton dhe vështirësinë e krijimit të një blloku të ri pasi sa më i madh të jetë aq më shumë fuqi kompjuterike kërkohet për zgjidhjen e algoritmit. Për të gjetur një kod hash i cili fillon me një numër **X** zerosh duhet të ndryshohen argumentet e funksionit sha256() por ndryshimi i tyre nënkupton ndryshimin e të dhënave që ruhen në bllok dhe kjo do të ishte e pakuptimtë. Për këtë arsye bllokut i shtohet një varibël (fallco) që ka për funksion të inkrementohet përgjatë një cikli derisa rastësisht kodi hash i prodhuar të përmbushë kushtin e Proof-of-Work. Në kodin mëposhtë argumenti niveli përfaqëson numrin e zerove që kërkohen në fillim të hash-it. Cikli do të

përsëritet për sa kohë karakteret nga 0 deri të niveli të kodit hash janë të ndryshme nga 0. Kur ky kusht nuk plotësohet cikli ndërpritet.

```
mineBlock(niveli){
 while(this.hash.substring(0,niveli)!==Array(niveli+1).join("0")){
 this.fallco++;
 this.hash=this.calculateHash();  }}
```

Duhet përmendur se përdorimi i një mekanizmi Proof-of-Work në këtë aplikim për një zinxhirë furnizimi nuk do të ishte tërësisht kuptimplotë në botën reale. Nën supozimin që minuesit e blloqeve të blockchain-it të një kompanie private do të duhet të ishin entitete të certifikuara nga kompania apo nga aktorë të tjerë dhe besueshmëria e punës së tyre do të sigurohej më mirë nëpërmjet modeleve të tjera ndoshta dhe ligjore. Për nga natyra demonstrative e punimit është arsyetuar se përdorimi i një algoritmi të tillë në këtë punim mund të ketë interes studimor.

Për krijimin e këtij aplikimi është adoptuar modeli i transaksioneve siç përdoret në kriptomonedha, por në dallim nga to në këtë implementim një transaksion nënkupton kalimin e pronësisë së produktit nga një aktorë përgjatë zinxhirit të furnizimit te një tjetër dhe jo një shkëmbim monetar. Një transaksion është një objekt i tipit Javascript i cili përmban disa atribute: produktin (mund të përfaqësohet nga emri i produktit, tipi apo numri serial), zotëruesin e mëparshëm të produktit (fromAddress), zotëruesin e ri të produktit (toAddress), sasinë që do të shkëmbehet dhe një variabël për të ruajtur komente shtesë që mund të kenë palët pjesëmarrëse.

```
class Transaction{
 constructor(fromAddress,toAddress,amount,time,produkt, koment){
 this.fromAddress=fromAddress;
 this.toAddress=toAddress;
 this.amount=amount;
 this.time=new Date();
 this.produkt=produkt;
 this.koment=koment;  }
```

Siç është përmendur dhe më parë përgjatë punimit transparenca është një element kyç i teknologjisë blockchain. Është e vërtetë që blockchain është publik dhe mbështet një nivel të lartë transparence por kjo nuk do të thotë që të dhënat që ruhen në një bllok mund të arrihen nga kushdo. Për të siguruar një standard privatësie dhe sigurie në këtë sens blockchain inkorporon metoda kriptografike për të nënshkruar të dhënat brenda blloqeve. Në këtë aplikim autori përdor funksionet e librarisë "elliptic" për të nënshkruar transaksionet e blockchain.

```
signTransaction(signingKey){
        if(signingKey.getPublic('hex')!==this.fromAddress){
```

```
throw new Error('Nuk mund të nënshkruaj transaksione për të tjerë');
}
const hashTx = this.calculateHash();
const sig= signingKey.sign(hashTx, 'base64');
this.signature= sig.toDER('hex');  }
```

Funksioni signTransactions() ndodhet brenda klasës **Transaction** dhe kërkon si argument një objekt (signingKey) që ka për atribute një çift çelësash kriptografik (publik dhe privat). Variabli fromAddress që përfaqëson adresën apo entitetin i cili është zotërues i produktit para shkëmbimit në vetvete do të jetë një çelës publik. Arsyeja për këtë është se për të kryer një shkëmbim duhet të konfirmohet një lloj autentifikimi ndërmjet palëve pjesëmarrëse dhe prandaj adresat e tyre janë trajtuar si një çift çelësash në mënyrë të ngjashme siç ndodh me portofolët në rastin e kriptomonedhave. Kështu përpara se të bëhet nënshkrimi i një transaksioni bëhet një kontroll për të parë nëse personi i cili po kryen procesin është vërtet pala pjesëmarrëse në shkëmbim. Më pas përllogaritet kodi hash i transaksionit dhe ky i fundit nënshkruhet dhe ruhet në variablin signature. Funksionet getPublic(), sign() dhe toDER() janë funksione të gatshme të librarisë ELLIPTIC. Gjithashtu për të verifikuar vlefshmërinë e transaksionit është ndërtuar funksioni isValid() i cili përdor pikërisht nënshkrimin digjital të gjeneruar nga metoda e mësipërme.

```
isValid(){
        if(!this.signature || this.signature===0)
        {throw new Error('Transaksioni nuk ka nënshkrim digjital'); }
          const publicKey = ec.keyFromPublic(this.fromAddress,'hex');
          return publicKey.verify(this.calculateHash(),this.signature);
        }
```

Në fillim kontrollohet nëse transaksioni ka apo jo një nënshkrim. Më pas në variablin publicKey do të ruhet një objekt që do të jetë një çift çelësash që për çelës publik do të ketë fromAddress. Kjo mundësohet nga funksioni i gatshëm keyFromPublic(). Funksioni isValid() do të rikthejë vlerën TRUE në rast se konfirmohet që hash-i i transaksionit është nënshkruar vërtet nga variabli signature dhe FALSE në qoftë së jo.

Deri tani është shpjeguar krijimi i blloqeve dhe i përmbajtjes së tyre (transaksionet) por nuk është ndërtuar akoma zinxhiri apo struktura që do të lidhë blloqet me njëra-tjetrën. Për këtë krijohet klasa Blockchain si më poshtë:

```
class Blockchain{
  constructor(){
      this.chain=[this.createGenesisBlock()];
  this.niveli=2;
  this.pendingTransactions=[];  }
```

Atributi chain do të jetë vektori që do të përmbajë blloqet e zinxhirit, niveli përfaqëson nivelin e vështirësisë për algoritmin e Proof-of-Work (numri i zerove në fillim to kodit hash të bllokut) dhe është lënë 2 por mund të ndryshohet në një moment të dytë, pendingTransactions është një vektor që do të përmbajë transaksionet që janë në pritje përpara krijimit të një blloku dhe do të shpjegohet në vijim. Elementi i parë i zinxhirit të blockchain është blloku gjenez i cili do të ndërtohet në mënyrë manuale nëpërmjet funksionit createGenesisBlock():

```
createGenesisBlock(){
        return new Block(Date.parse('2021-05-28'),[],"0");  }
```

Një bllok mund të përmbajë një numër të madh transaksionesh. Për të bërë më efektive shtimin e tyre në blloqe transaksionet pasi krijohen shtohen në vektorin pendingTransactions dhe më pas kur krijohet një bllok të dhënat e këtij vektori i jepen atij. Përpara se transaksioni ti shtohet bllokut duhet të kontrollohet nëse ai ka adresa të përcaktuara dhe nëse është e vlefshme (valide).

```
addTransaction(transaction){
        if(!transaction.fromAddress||!transaction.toAddress){
          throw new Error('Transaksioni duhet të ketë adresë');  }
        if(!transaction.isValid()){
                throw new Error('Transaksion jo valid'); }
        this.pendingTransactions.push(transaction);}
```

Pasi transaksionet i shtohen vektorit të quajtur pendingTransactions duhet ndërtuar një funksion i cili krijon një objekt të tipit **Block** që merr atributet e duhura.

```
getLatestBlock(){ return this.chain[this.chain.length-1];}
minePendingTransactions(){
        let block = new Block(Date.now(), this.pendingTransactions,
                this.getLatestBlock().hash);
        block.mineBlock(this.niveli);
        console.log('Blloku u minua me sukses');
        this.chain.push(block);
        this.pendingTransactions=[]; }
```

Kujtojmë që një objekt **Block** ka për atribute kohën që kthehet në mënyrë automatike nga funksioni Date.now(), transaksionet që i jepen nga vektori pendingTransactions dhe hash e bllokut paraardhës që merret nga funksioni getLatestBlock(). Pasi krijohet blloku ai i shtohet zinxhirit (this.chain.push(block)) dhe në fund vektori pendingTransactions boshatiset për tu ripërdorur në thirrje të tjera të funksionit. Kodi burim gjithashtu përmban funksione të tjera që kontrollojë vlefshmërinë e transaksioneve të një blloku, vlefshmërinë e zinxhirit të blloqeve por dhe kontrollin e balancës së një llogarie.

Përfundime dhe rekomandime

Në përfundim të këtij punimi do të jepen disa konkluzione dhe rekomandime duke u ri-theksuar dhe njëherë rëndësia dhe potenciali që blockchain ka. Kjo teknologji ofron një formë të re të organizimit të ruajtjes së të dhënave e cila përforcon karakteristika të tilla si siguria, transparenca, decentralizimi dhe pandryshueshmëria. Pikërisht fokusi në këto element e bëjnë blockchain një mekanizëm të përshtatshëm, efektiv dhe mjaft interesant për studime të mëtejshme. Implementimi i blockchain për krijimin dhe funksionimin e kriptomonedhave shënon një hap shumë të rëndësishëm në zhvillimin e kësaj teknologjie. Ky aplikim rriti popullaritetin dhe bëri që të njihet gjerësisht potenciali i saj. Gjithashtu nga një perspektivë ekonomike kriptomonedhat kanë ndryshuar tregjet financiare duke ofruar një mënyrë të re pagesash e cila nuk ka nevojë për palë ndërmjetëse si bankat. Gjithsesi horizonti i kësaj teknologjie shkon përtej këtij implementimi financiar.

Blockchain ka potencialin të përmirësoj një sërë fushash në të cilat mund të gjejë përdorim. Të qenit e sigurt, e pandryshueshme dhe transparente bën që teknologjia të ketë mundësinë të revolucionarizoj aspekte të ndryshme të industrive të ndryshme ndër të cilat ajo farmaceutike, e modës, financiare që përmenden në këtë punim. Një aplikim me shumë perspektiv i blockchain i cili ka filluar të gjejë përdorim në praktikë sot është integrimi i kësaj teknologjie në zinxhirët e furnizimit. Veçanërisht kompanitë e mëdha që operojnë në mënyrë internacionale e kanë të vështirë të organizojnë dhe gjurmojnë të dhënat përgjatë zinxhirëve të furnizimit për shkak të madhësisë dhe kompleksitetit të tyre. Për këtë arsye një teknologji si blockchain e cila garanton që informacioni që ruhet nuk mund të manipulohet dhe është valid, është mjaft e përshtatshme për tu përdorur në to. Mënyra së si një blockchain mund të integrohet në një zinxhirë furnizimi ndryshon në varësi të industrisë dhe kërkesave specifike të procesit. Në këtë punim blockchain është përdorur për regjistrimin e shkëmbimeve të produkteve ndërmjet aktorëve të ndryshëm përgjatë zinxhirit dhe ky demonstrim ilustrues tregoj se një aplikim i tillë ka baza të qëndrueshme për të qenë i suksesshëm.

Në anën tjetër, teknologjia blockchain nuk mund të jetë perfekte. Ka disa aspekte rreth saj të cilat mund të gjejnë përmirësim. Së pari, duhet theksuar se shqetësimi më i madh kur flitet për përdorimin masiv të blockchain sot është shpërdorimi i energjisë. Ndonëse mekanizma si Proof-of-Stake shpenzojnë më pak energji elektrike se Proof-of-Work, përsëri ngelet një problematik e qenësishme. Për këtë është e nevojshme të kryhen studime të mëtejshme në këtë dimension të blockchain për të arritur rezultate më të kënaqshme. Për sa i përket implementimit të teknologjisë në zinxhirët e furnizimit apo dhe implementime të tjera rekomandimi i këtij punimi është që të përshtaten mekanizmat e blockchain me karakteristikat e fushës përkatëse. Zhvillimi i elementëve të funksionimit dhe

sigurisë së blockchain si për shembull "kontratat e zgjuara" (**smart contracts**) ofrojnë mundësinë për një nivel të lartë automatizimi të shumë proceseve përgjatë zinxhirëve të furnizimit por sigurisht duhet që të modelohet dhe kodohet blockchain sipas kërkesave të fushës, industrisë apo dhe vetë kompanisë.

Literatura

Abeyratne S. A., and Monfared R. P. (2016). Blockchain ready manufacturing supply chain. Ijret: international journal of research in engineering and technology, 05(09). https://ijret.org/volumes/2016v05/i09/IJRET20160509001.pdf

Casado-Vara, R., Prieto, J., De la Prieta, F., & Corchado, J. M. (2018). How blockchain improves the supply chain: case study alimentary supply chain. Procedia Computer Science, 134, 393-398. doi:https://doi.org/10.1016/j.procs.2018.07.193

Coindesk. (2021). Coindesk. Gjetur në Coindesk:

https://www.coindesk.com/price/bitcoin

Dougherty, C., & Huang, G. (2014). Mt. Gox Seeks Bankruptcy After $480 Million Bitcoin Loss. Bloomberg. Gjetur 09 22, 2022, nga: https://www.bloomberg.com/news/articles/2014-02-28/mt-gox-exchange-files-for-bankruptcy

Feld, S., Schonfeld, M., & Werner, M. (2014). Analyzing the deployment of Bitcoin's P2P network. The 5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014), the 4th International Conference on Sustainable Energy Information Technology (SEIT-2014). 32, fv. 1121-1126. Elsevier

Garcia, D. J., & You, F. (2015). Supply chain design and optimization: Challenges and opportunities. 8th International Symposium on the Foundations of Computer-Aided Process Design (FOCAPD 2014), July 13-17, 2014, Cle Elum, Washington, USA, 81, 153-170

Gervais, A., Karame, G. O., Wust, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016). On the Security and Performance of Proof of Work. CCS '16: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. (fv. 3-16). New York, NY, United States: Association for Computing Machinery. doi:https://doi.org/10.1145/2976749.2978341

Haber, S., & Stornetta, W. (1991). How to time-stamp a digital document. Journal of Cryptology , 3, 99–111. doi:https://doi.org/10.1007/BF00196791

Hugos, M. (2018). Essentials of Supply Chain Management, Fourth Edition. John Wiley & Sons, Inc

Thomsen, S. S., & Knudsen, L. R. (2009). Cryptographic Hash Functions. DTU Library

Hackius, N., & Petersen, M. (2017). Blockchain in logistics and supply chain: Trick or. Chapters from the Proceedings of the Hamburg International Conference of Logistics (HICL), Institut für Logistik und Unternehmensführung, Technische Universität Hamburg. 23, fv. 3-18. Hamburg: epubli GmbH, Berlin. doi:doi:10.15480/882.1444

Hassani, H., Huang, X., & Silva, E. (2018). Big-Crypto: Big Data, Blockchain and Cryptocurrency. Big Data and Cognitive Computing. 2. MDPI

Kroll, J. A., I. C., Davey., & E. W., Felten. (2013). The Economics of Bitcoin Mining,or Bitcoin in the Presence of Adversaries. Computer Science, Mathematics, Economics. CiteSeerX

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020, June). A Survey on the Security of Blockchain Systems. Future Generation Computer Systems, 107, 841-853

Liu, Y., & Tsyvinski, A. (2021). Risks and Returns of Cryptocurrency. The Review of Financial Studies, 34(6), 2689-2727. doi:10.3386/w24877

Mentzer, J. T., DeWitt, W., Keebler, J. S., Min, S., Nix, N. W., & Smith, C. D. (2001). The Review of Financial Studies. Journal of Business Logistics, 22(2), 1-25

Miraz, M. H., & Ali, M. (2018). Applications of Blockchain Technology beyond Cryptocurrency. Annals of Emerging Technologies in Computing (AETiC), 1-6.

N., C. (2021, May 05). How Much Energy Does Bitcoin Actually Consume? Gjetur në Harvard Business Review: https://hbr.org/2021/05/how-much-energy-does-bitcoin-actually-consume

Nakatomo, S. (2008, 09 26). Bitcoin: A Peer-to-Peer Electronic Cash System. WhitePaper. Gjetur në Bitcoin White Paper: https://bitcoinwhitepaper.co/

Pilkington, M. (2016). Blockchain technology: principles and applications. In Research Handbook on Digital Transformation

Rosati, P., & Cuk, T. (2019). Blockchain Beyond Cryptocurrencies. Në M. J. T. Lynn, Disrupting Finance. palgrave

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'REILL

Wood D. D. (2014). Ethereum: A Secure Decentralised Generalised Transaction Ledger. Ethereum Project Yellow Paper, 1-32

Yaga D., et al. (2018, October). Blockchain Technology Overview. National Institute of Standards and Technology. Gjetur në https://arxiv.org/abs/1906.11078

Yli-Huumo, J., Ko D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE. doi:https://doi.org/10.1371/journal.pone.0163477