Универзитет у Новом Саду, Факултет техничких наука

ОАС Информациони инжењеринг

Вештачка Интелигенција у Оптимизацији Концензус Алгоритма у Blockchain Технологијама

Семинарски рад из предмета

ОСНОВИ РАЧУНАРСКЕ ИНТЕЛИГЕНЦИЈЕ

Аутори

Ђорђе Станковић, IN13/2018
Вукашин Лупуровић, IN30/2018

Нови Сад, 2021.

Садржај

Увод

Blockchain, иако се сматра као релативно нова технологија, заправо има своје корене још из осамдесетих, када су тадашњи криптографи желели да направе систем који бележи времена и детаље некаквих догађаја, који се не може касније изменити. Видели су велику примену оваквог система у будућности у пољима финансија и безбедности, где се, на пример, неки запис о количини пребаченог новца или евиденција приступа некој битној бази података, не може ни на какав начин модификовати у било чију корист. Већ се тада разматрало о свакаквим могућностима које овакав сигуран систем може да пружи, и то у другим сферама, од логистике и транспорта робе до бележења гласача на изборима.

Сматра се да је први *blockchain* систем направила група или појединац Сатоши Накамото 2008. године, у време једне од највећих светских економских криза [1]. Његов "бели папир" је изашао као одговор на тадашњи скептицизам у централизовани банкарски систем и светску економију, као корак ка слободним трансакцијама између људи било где на свету користећи нову дефлаторну криптовалуту, без икакве финансијске институције или регулативе између њих.

Сатоши је желео да направи сигурну, праведну и децентрализовану *peer-to-peer* мрежу, доступну свима на свету, која ће бележити све трансакције које су се икада десиле на њој, између било које две партије, од зачетка. Такав систем је успео да направи користећи јавне и енкриптоване "уланчане блокове" трансакција на мрежи, које ће сваки чвор у мрежи поседовати, и који ће свима бити исти и видљиви. Ово подразумева да треба да постоји некакав концензус између чворова на мрежи да би сви чворови у сваком тренутку били сигурни да имају правилну верзију *blockchain*-а код себе. За ово је креиран концензус алгоритам који је, у то време, радио по *Proof-of-Work* (PoW) принципу. Сатошијев *peer-to-peer blockchain* није престао са радом од свог зачетка, јер ће у било ком тренутку увек постојати неки чвор који одржава мрежу.

Концензус алгоритам *blockchain*-а може имати различите имплементације, односно "доказе" о верификацији, сваки од њих има своје предности и мане, али сви раде по таквом принципу да ланац остане непромењен, сигуран, транспарентан и брз. Он ради по таквом принципу да онемогућује дупло наплаћивање трансакције код оба чвора, и уједно решава проблем Византијских генерала, где се више дистрибуираних чланова морају у исто време договорити око једног поступка, да не би дошло до конфликта - овде се то примењује у контексту валидације правилног блока трансакција на тренутно најдужи ланац блокова на *blockchain* мрежи. Пошто је сам концензус алгоритам, односно његова ефикасност и тачност, управо и најбитнији део имплементације *blockchain* технологије, то је уједно и поље на којем можемо највише да порадимо, и он је савршен за експериментисање и оптимизацију користећи машинско учење и вештачку интелигенцију.

Очекујемо да овим истраживањем читаоца уведемо у свакакве могућности имплементације вештачке интелигенције, у један од најсавременијих аспеката технологије.

Тренутни Принципи Валидације Blockchain-а

Proof-of-Work Принцип

Proof-of-Work принцип у раду концензус алгоритма се заснива на идеји колективног рада чворова на мрежи, и "доказивање" валидности *blockchain*-а самим присуством дигиталног потписа сваког блока који је остварен тим радом.

Цела *blockchain* мрежа је у овом принципу подељена на више базена рудара (енгл. *mining pool*) по географским регионима. Свака трансакција која се деси на мрежи се првобитно пакује у енкриптовани блок, односно скуп трансакција, од стране базена, и насумично се прослеђује неком рудару (енгл. *miner*) тог базена за валидацију.

Задатак сваког рудара у базену је да дешифрује блок који је преузео, да за њега закачи дигитални потпис да је блок исправан, и да ажурира тренутно најдужи *blockchain* на мрежи новим потписаним блоком. Након тога ће се следећи блок, који буде био потписан било где на свету, на исти начин закачити за тај претходни блок на најдужем *blockchain*-у, и сви чворови у мрежи ће имати идентичан ланац трансакција.

Разлог зашто се блокови првенствено и енкриптују је због сигурности и непробојности *blockchain*-а. Списак трансакција свих чворова у неком тренутку времена не може увек бити конзистентан због великог кашњења мреже у *point-to-point* комуникацији, што креира прозор за хакерски напад. Након што се блокови енкриптују SHA-256 хеш функцијом, потребно је мало времена док рудар не дешифрује прослеђени хеш. Брзина дешифровања зависи од саме хеш функције, од тога како је она подешена, односно да ли се дешифровање отежава са већим бројем рудара на мрежи, али и од самог хардвера, односно процесорске снаге рудара. Предност ове енкрипције је то што је у будућности потпуно немогуће некоме да одређени блок на *blockchain*-у промени на време. Ако се промени било који детаљ неке трансакције, мора се дешифровати потпуно нова енкриптована порука и тај блок мора бити присутан код барем 50% чворова на мрежи, што је чак и са великим бројем суперкомпјутера немогуће остварити. За време за које би ти суперкомпјутери покушавали да преовладају *blockchain* мрежом, тренутни *blockchain* ће се сигурно проширити и даље валидирати од стране других чворова на мрежи, па ће тај покушај пропасти.

Овај принцип рада алгоритма је први заживео на *Bitcoin blockchain*-у, и и даље се користи на великој већини *blockchain*-а криптовалута, међутим временом се овај принцип показао као јако спор за трансакције и неефикасан што се тиче рачунарске снаге. Цена одржавања *blockchain* мреже се све више повећава са све већим бројем рудара на мрежи. Ово се догађа због награде коју рудари добијају након дешифровања блока трансакција, сама функција хеширања се отежава, потребне су јаче машине за дешифровање, популарност криптовалута утиче на огроман број трансакција и крајњи производ тога је огромна потрошња струје на светском нивоу. Ово наравно може да проузрукује озбиљне еколошке последице, поготово у регионима где обновљиви извори енергије нису редовно доступни, а број рудара је велик, као на пример у Кини. Такође, пошто је најбољи хардвер за рударење, односно дешифровање, процесор са што већим бројем језгара, настала је велика потражња за комерцијалним графичким процесорима, што је доста утицало на тренутну несташицу компјутерских чипова.

Proof-of-Stake Принцип

Proof-of-Stake (PoS) принцип је основан као алтернатива за *Proof-of-Work* алгоритам. Када се иницира трансакција, подаци трансакције се смештају у блок максималног капацитета од 1 мегабајта, а затим се дуплирају на више рачунара или чворова у мрежи. Чворови су административно тело *blockchain*-а и верификују легитимност трансакција у сваком блоку.

За разлику од *Proof-of-Work* принципа, *Proof-of-Stake* принцип се сматра за мање ризичан алгоритам. Он покушава да реши проблем превелике употребе енергије тако што приписује рударску снагу (енгл. *mining power*) у пропорцији са бројем новчића које рудар поседује. На овај начин, уместо да се енергија користи за решавање *Proof-of-Work* загонетке, *Proof-of-Stake* рудар је ограничен на ископавање оноликог процента трансакција колико он поседује. На пример, рудар који поседује 3% доступних новчића теоретски може да ископа само 3% блока, што би значило да особа која поседује више новчића има већу снагу копања.

Главна предност *Proof-of-Stake* алгоритма је уштеда енергије и сигурност. Поступак насумичности чини мрежу децентрализованијом јер рударски базени нису више потребни за рударење. А пошто је мања потреба за пуштањем многих нових новчића за награду, ово помаже да цена одређеног новчића остане стабилнија.

Још једна разлика у односу на *Proof-of-Work* је то што за *Proof-of-Stake* није неопходно пуно улагања у хардвер да би чвор имао шансу за креирање нових блокова [2].

Иако је *Proof-of-Work* заступљен код *Bitcoin*-а и *Ethereum*-а, две тренутно највеће криптовалуте, *Ethereum* група разматра да ове године своју криптовалуту пребаци на *Proof-of-Stake* како би смањили потрошњу енергије мреже.

Две најчешће методе које се користе за валидацију *blockchain*-а су *Randomized Block Selection* и *Coin Age Selection*.

У *Randomized Block Selection* методи валидатори се бирају тражењем чворова са комбинацијом најниже хеш вредности и највећег улога, а с обзиром на то да је величина улога јавна, следећи чворови обично могу бити предвиђени од стране других чворова.

Coin Age Selection метода бира чворове на основу тога колико су стари њихови уложени новчићи. Старост новчића се израчунава множењем броја дана у којима се новчићи држе као улог са бројем уложених новчића. Једном када је чвор направио блок, старост његових новчића се враћа на нулу и мора да сачека одређени временски период да би могао да направи други блок - ово спречава чворове великих улога да доминирају у *blockchain*-у [3].

Овај принцип са собом доноси и одређен ризик. С обзиром да ради на принципу “што више уложиш већу снагу добијаш” то може довести до огромних проблема. Постоји велика шанса да се јави олигопол, односно да се појави неколико доминантних учесника који би пуно улагали, а самим тим и имали већи профит и већу снагу у односу на конкуренцију.

Вештачка Интелигенција и Blockchain

Имплементација неких метода вештачке интелигенције у свет *blockchain*-а, као и имплементација *blockchain*-а у неким апликацијама и системима заснованих на вештачкој интелигенцији, била је једна од главних тема треће IEEE конференције о *blockchain*-у 2020. године. Ове две технологије су се показале као револуционарне у претходној деценији и могу бити главни играчи у следећој индустријској револуцији. На панелима конференције су биле разне организације које су виделе велики значај у комбинацији ових технологија, као на пример у разним децентрализованим апликацијама (енгл. *decentralized applications, dApps*) у области транспорта, друштвених мрежа или трговине, затим у анализи паметних уговора (енгл. *smart contracts*) на *blockchain*-у, и у оптимизацији тренутних и креирању нових концензус механизама за *blockchain*, што је и фокус овог рада.

Једна од популарнијих комбинација ове две технологије су *AI DAO*-и, дистрибуиране аутономне организације, односно апликације, које живе на *blockchain*-у и користе вештачку интелигенцију у своје сврхе. Пример овакве апликације је *ArtDAO*, пројекат који користи дубоке мреже (енгл. *deep nets*) да изгенерише некакво јединствено уметничко дело, у овом случају апстрактну слику (слика 1), озваничи је на *blockchain*-у преко паметног уговора и лицитира је на некој интернет продавници. Овим начином сама апликација може да поседује свој новчаник и креира своје мало богатство у криптовалутама, једноставно креирајући медијуме које би људи, или чак неке друге *AI DAO* апликације, купиле, као на пример музику или поезију.

Слика 1. *ArtDAO* Уметничко Дело

Рекурентне неуронске мреже (енгл. *Recurrent Neural Network, RNN*) и мреже са продуженом краткорочном меморијом (енгл. *Long Short-Term Memory Network, LSTM*) омогућују нам предвиђања комплексних временских низова. Ово, као посебан сектор у машинском учењу, може бити јако добар алат у увиђању корисних параметара у будућности, референцирајући се на параметре из прошлости, на пример за естимацију кретања цена криптовалута, или увиђања некаквих трендова у разноликим сферама.

Вештачка интелигенција, и поготово неуронске мреже, представљају могуће решење за наведене негативне последице тренутних принципа рада концензус алгоритма у данашњим *blockchain* системима. Пример овога су превелика потрошња струје и загађење животне средине, споро време доласка до консензуса и монополизација чворова *blockchain*-а, што би даље могло креирати неки вид централизованог система. У даљем тексту ћемо објаснити принципе рада два механизма који су засновани на споменутој технологији и који ће избећи ове последице - *Proof-of-Artificial-Intelligence* (PoAI) и *Proof-of-Useful-Work* (PoUW).

Proof of Artificial Intelligence

Основни Појмови

Proof-of-Artificial-Intelligence је принцип валидације уведен 2018. године од стране Jianwen Chen-а и тима из AICHAIN фондације. Њиховим експериментисањем су установили да је овај принцип на истом нивоу што се тиче брзине прихватања трансакција и безбедности самог *blockchain* система као и наведени *Proof-of-Work* и *Proof-of-Stake*, и то без потребе за спорим и захтевним хеш операцијама и валидацијама, као и без могућности превладавања *blockchain*-а од стране неког чвора.

Начин на који се ово може постићи је да се имплементира алгоритам селекције чворова заснован на вештачкој интелигенцији [4]. Алгоритам би првобитно узео у обзир просечан број трансакција сваког чвора и затим упоређивао те просеке по неком критеријуму да би поделио све чворове, односно рударе, у три категорије - супер чворови (енгл. *super nodes*), насумични чворови (енгл. *random nodes*) и непознати чворови (енгл. *unknown nodes*). Уз ово је креиран и механизам способности чворова, који ће бити коришћен у конволуционој неуронској мрежи за потребе селекције, што ће даље скратити време неопходно за валидацију.

Рацио рачунарске снаге (енгл. *computing power ratio*) може се дефинисати као однос рачунарске снаге посматраног чвора и рачунарске снаге целе мреже. У *Proof-of-Work* сценариу се рачунарска снага једног чвора мери као број покушаја насумичног погађања решења хеш загонетке по секунди, тачније као *hashrate*, MH/s (*MegaHash per second*, број милиона погађања у секунди). Одатле би *blockchain* мрежа која ради по том принципу била најефикаснија ако користи хардвер који има огроман број језгара, па би, на пример, у случају *Bitcoin* алгоритма централни процесор био најмање ефикасан јер је спор при прикључивању између процеса и зато што нема пуно језгара, иако је највештији у обављању компликованијих задатака, док би нешто попут графичког процесора или специфичне ASIC машине (*Application Specific Integrated Circuit*) било идеално.

Просечан број трансакција чвора (енгл. *Average Transaction Number*, ATN) се користи као главни фактор селекције чворова и он може да се моделира као евалуациона функција која прима следеће независне параметре :
- Особине чвора (ознака CRT), овде се убрајају рацио рачунарске снаге (енгл. *computing power ratio*), укупно време чвора на мрежи (енгл. *online time*) и исплата (енгл. *payoff*), односно награда чвору за валидацију;
- Природа мреже (ознака HCL), ово представља хоп посматраног чвора на мрежи (енгл. *hop*), број чворова на мрежи (енгл. *connection number*) и латенција чвора (енгл. *latency*);
- Сигурносни елементи (ознака DAA), овде спадају вероватноћа одбацивања чвора (енгл. *discarded probability*), вероватноћа напада (енгл. *attacked probability*) и вероватноћа привлачења (енгл. *attract probability*).

$$ATN = f(CRT, HCL, DAA)$$

Супер чворови (енгл. *super nodes*) су чворови са високом рачунарском снагом, одатле бољим хардвером и малом латенцијом на мрежи. Супер чворови се бирају од стране имплементираног механизма вештачке интелигенције.

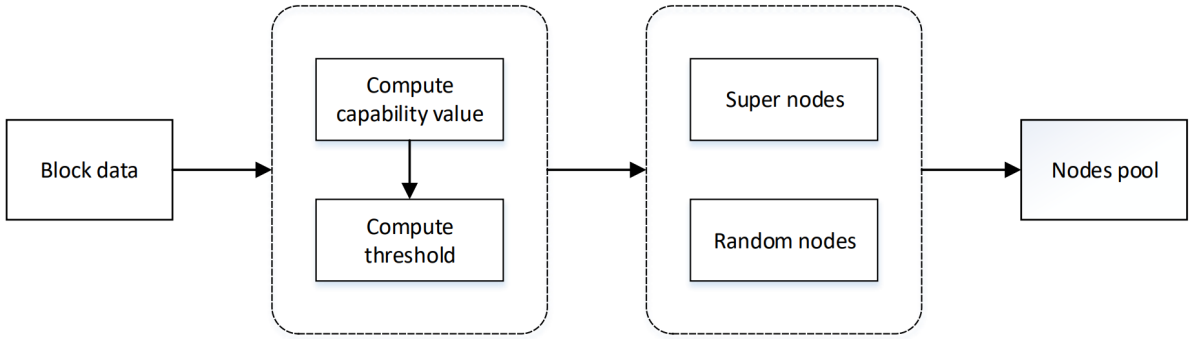
Насумични чворови (енгл. random nodes) су чворови са мањим просечним бројем трансакција (ATN) у односу на супер чворове, али они гарантују праведност мреже и спадају у базен чворова.

Параметар који раздваја супер чворове од насумичних је праг способности (енгл. *capability threshold*, ознака Thres) који је динамичан и мења се у односу на перформансе *blockchain* мреже.

Алгоритам

Први корак алгоритма је рачунање просечног броја трансакција за сваки чвор у мрежи користећи конволуциону неуронску мрежу (енгл. *Convolutional Neural Network*, CNN). Други корак је селекција супер чворова и насумичних чворова по одређеном критеријуму. Подаци о сваком чвору се узимају као улазни параметри у *Proof-of-Artificial-Intelligence* алгоритам, док би излаз представљао диференцијацију базена чворова од чворова рудара.

Оваквим приступом превазилазимо конфликте око рударења, што утиче на то да побољшавамо праведност у распоређивању посла, децентрализацију и сигурност, а и смањујемо потрошњу струје тиме што избегавамо решавање хеш задатака. Насумична расподела посла чворовима ће помоћи и око хакерских напада на *blockchain* мрежу, јер је хакеру непредвидиво који ће чвор бити следећи за валидацију трансакције. Такође, процес генерисања базена чворова, односно процес селекције чворова, не захтева људски труд.



Слика 2. Блок дијаграм PoAI принципа

Поступак којим би категоризовали све чворове мреже у супер чворове, насумичне чворове и непознате чворове је описан у следећем алгоритму (слика 2) :

1. Генерише се *ATN_sorted*, листа рангирања чворова у опадајућем редоследу на основу просечног броја трансакција ATN, добијеног од стране конволуционе неуронске мреже;
2. Одређује се максималан капацитет једног базена чворова, *Whole_max*;
3. Генерише се насумичан природан број *i* као број чворова у базену чворова *Node_pool_num*, тако да је $\frac{1}{2}$ **Whole_max* < *i* < *Whole_max*;
4. Генерише се праг способности *Thres* у односу на перформансе *blockchain* мреже, *Thres* < *Nodes_pool_num* - њиме одређујемо број супер чворова *Sup_num*;
5. Бира се првих *Sup_num* чворова у листи за супер чворове;
6. Бира се *Rad_num* насумичних чворова од преосталих чворова.

Чвор ће бити супер чвор ако му је ранг виши него *Sup_num*, односно првих *Sup_num* чворова у опадајућој листи ће бити супер чворови. *Sup_num* је параметар који представља праг који одваја супер чворове од насумичних чворова. Сви чворови у *ATN_sorted* листи испод чвора са индексом *Sup_num* могу бити или насумични чворови или непознати чворови. На стохастичан начин се бира *Rad_num* чворова да буду насумични, остали су непознати чворови. Због таквог рада механизма за бирање насумичних чворова мрежа постаје отпорна на екстерне нападе. Пошто се у записима трансакција налазе и доминантни супер чворови и уобичајени насумични чворови, *blockchain* мрежа такође остварује и праведно распоређивање посла. Овакав концензус механизам подстиче чворове мреже да појачају своје особине (CRT), односно да појачају рацио рачунарске снаге и укупно време на мрежи, а и да смање сигурносни ризик (DAA) колико год је могуће.

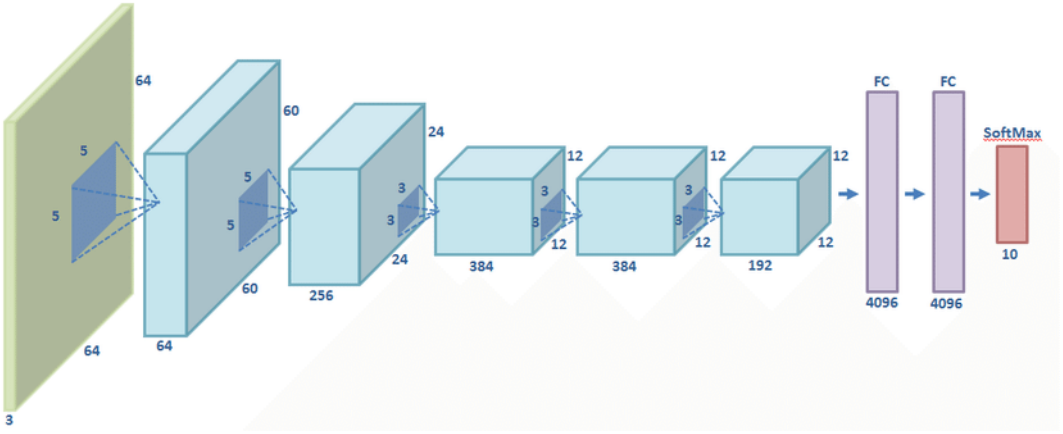
Како се број чворова на мрежи повећава, максималан капацитет једног базена чворова (*Whole_max*) остаје исти, они су фиксне величине.

Рудар чвор, односно валидатор, се бира из базена чворова, којег формирају супер чворови и насумични чворови, на основу стохастичног ротационог механизма - чворови у базену рударе редом, један по један, у насумичном редоследу.

Тренирање Конволуционе Неуронске Мреже

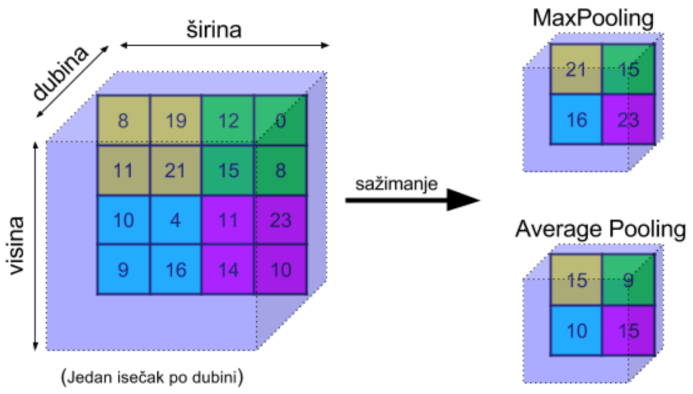
Конволуциона неуронска мрежа нам служи да добијемо просечан број трансакција ATN за сваки чвор. Као што је већ наведено, ATN се добија као резултат евалуационе функције која за параметре прима особине чвора CRT, природу мреже HCL и сигурносне елементе DAA. Ове параметре чвора можемо да поставимо у матрицу способности чвора M (енгл. *aptitude test questionnaire matrix*), па би главни циљ неуронске мреже био да фитује ATN у односу на улазну матрицу M, за сваки чвор понаособ.

За систем процене способности чвора (енгл. *capability assessment system*) предложена је модификована верзија AlexNet-а, модела конволуционе неуронске мрежне структуре направљеног од стране Alex Krizhevsky-а за такмичење на ImageNet 2012 Visual Recognition Challenge-у, који је користио графичке процесоре за имплементацију [5].



Слика 3. Блок дијаграм оригиналног AlexNet модела конволуционе неуронске мреже.

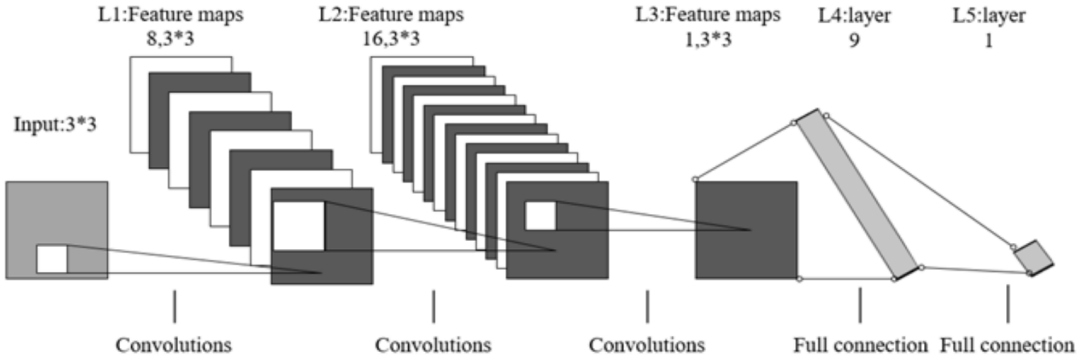
AlexNet користи 5 конволуционих слојева (енгл. *convolution layers*), 3 потпуно повезана слоја (енгл. *full connection layers*), од којих прва два користе технику напуштања (енгл. *dropout technique*), 60 000 параметара и 650 000 неурона да би остварио 1 000 различитих врста класификације слика (слика 3). Пре конволуционог слоја се налази улазни слој којим се подаци уводе у неуронску мрежу. Конволуциони слој је главни елемент конволуционе неуронске мреже јер обавља врло захтевна израчунавања у циљу обучавања неурона мреже. Конволуциони слој користи филтер функцију у свом раду и као излаз прави мапу карактеристика. Након неких изабраних конволуционих слојева налазе се слојеви сажимања (енгл. *pooling layer*), слој активационе функције *ReLU* (енгл. *Rectified Linear Unit*) и слој нормализације (енгл. *batch normalization layer*). Слој сажимања дели улазни параметар, односно матрицу, на секције специфичних димензија, по којима ће активациона функција радити сажимање. *ReLU* активациона функција се користи за побољшање перформанси мреже поступком сажимања по максимуму, и има формулу $f(x) = max(0, x)$. Разлог за ово сажимање јесте смањивање димензија улазног параметара за лакшу даљу обраду. Поред сажимања максимумом (енгл. *max pooling*) постоји и принцип сажимања по средњој вредности (енгл. *average pooling*) (слика 4) [6].



Слика 4. Различите врсте сажимања улазног параметра, односно матрице.

Модификовани AlexNet модел (слика 5) користи 3 слоја конволуције и 2 потпуно повезана слоја. Да би избегли проблем прекомерног фитовања и побољшали предвиђање користи се L2, односно Еуклидска нормализација тежина сваког конволуционог слоја.

Оваквим моделом неуралне мреже можемо предвидети просечан број трансакција сваког чвора у *blockchain* мрежи. За скуп података над којим конволуциона неуронска мрежа ради узима се матрица способности чвора M, односно она се користи као улазни параметар у конволуциони слој.



Слика 5. Блок дијаграм модификованог AlexNet модела конволуционе неуронске мреже.

Експерименти

На основу алгоритма из претходног поглавља осмишљен је AICHAIN, *blockchain* систем контролисан од стране вештачке интелигенције, који тестира *Proof-of-Artificial-Intelligence* принцип рада концензус алгоритма. На овај начин AICHAIN може да одабере супер чворове у својој архитектури и да послужи као софистицираније платформа за дигиталну трговину. Првенствено ће ниво задужен за вештачку интелигенцију одрадити анализу трансакција у свим блоковима, након тога ће утврдити резултат сваког чвора који може да креира блокове, да их рангира, и да, по представљеном алгоритму, изабере супер чворове за креирање и ажурирање блокова на *blockchain* мрежи.

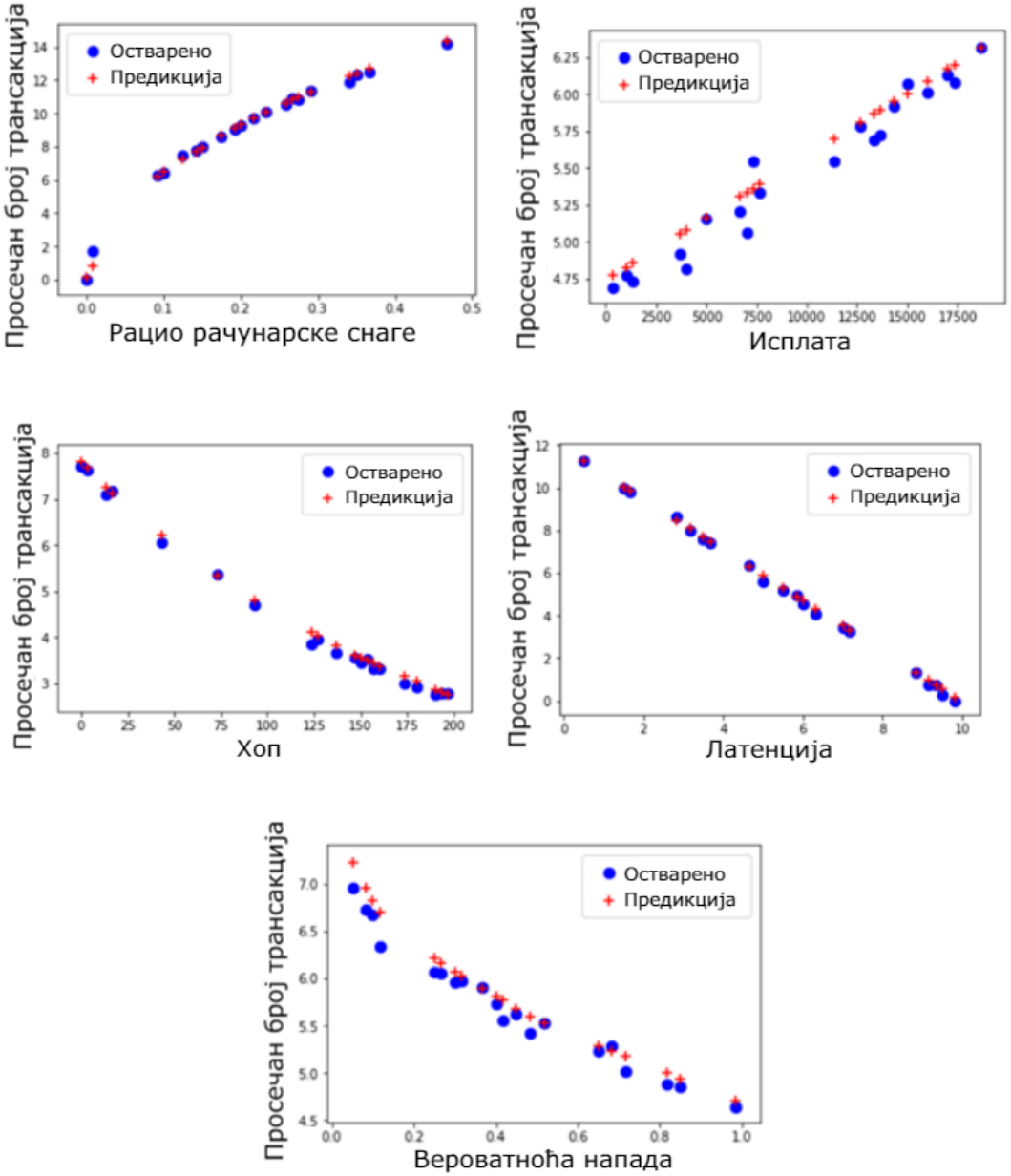
Скуп података *blockchain*-а над којим се ради истраживање би сачињавао матрице способности сваког чвора, односно имао би за сваки чвор његов скуп особина (табела 1). Тестирање је рађено на *Keras framework*-у, на четворојезгарном процесору са 8 гигабајта радне меморије.

Табела 1. Приказ особина чворова, односно елемената улазне матрице.

Рбр. секвенце	Рацио рачунарске снаге	Укупно време на мрежи (секунде)	Исплата (0.00000001 BTC)	Хоп чвора	Латенција чвора (секунде)
1	0.12	1000	5000	50	0.01
2	0.22	650	10000	125	0.001
3	0.05	1200	2500	90	0.001

Рбр. секвенце	Број чворова на мрежи	Вероватноћа одбацивања	Вероватноћа напада	Вероватноћа привлачења	Просечан број трансакција (ATN)
1	200	0.04	0.002	0	65.2
2	1000	0.03	0.001	0	125
3	900000	0.12	0.001	0.001	7.5

За тестирање модела су изабрана 5 фактора, и у следећим графицима је приказана варијација просечног броја трансакција како су се изабрани фактори мењали, црвени крстићи представљају нашу предикцију моделом, док су плаве тачкице остварени резултати (слика 6).

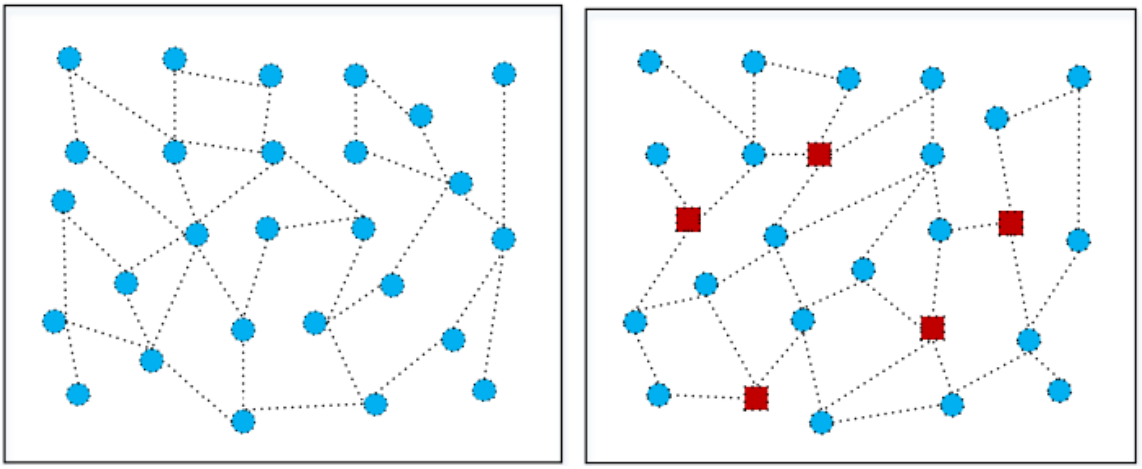


Слика 6. Просечан број трансакција по различитим факторима.

На првом графику можемо видети логаритамски тренд раста просечног броја трансакција за чвор како му се рацио рачунарске снаге повећава - ово је важило и код *Proof-of-Work* принципа, што јачи хардвер, то ће и чвор више трансакција валидирати. Исто тако, ако повећавамо награду чвору, тако ће му се и просечан број трансакција повећавати, линеарно. У преосталим графицима видимо да је просечан број трансакција у негативној корелацији са погоршавањем његове конекције са мрежом и са фактором сигурности, па се ATN скоро линеарно смањује у свим случајевима, дакле, што боља конекција и што сигурнији чвор, то ће и ATN бити већи.

У свим случајевима се показало да је предложен модел константно предвиђао тачне резултате, односно да се варијације тренда поклапају са предикцијом, па можемо рећи да је овај модел успешан.

У поређењу са другим принципима имплементације концензус алгоритма, у *Proof-of-Artificial-Inteligence* приступу често се дешава да неки насумични чворови буду изабрани за рударе, док се код осталих сви чворови бирају за рударе, односно валидаторе (слика 7). Тиме што поред супер чворова бирамо и неке насумичне чворове за рударе ми повећавамо сигурност од хакерског напада, осигуравамо децентрализованост и одржавамо праведно распоређивање посла у *blockchain* мрежи. Што се више чворова придружи мрежи, то ће она бити сигурнија. Као што је случај и код *Proof-of-Work* приступа, рацио рачунарске снаге је и овде присутан као битан фактор, али у знатно мањој мери, јер се поред њега убрајају и остале битне особине чвора, као и саме мреже.



Слика 7. Конвенцијални приступ рада концензус алгоритма, и PoAI приступ. На левој слици су сви чворови рудари, док су на десној црвеном бојом означени насумично изабрани рудари.

Proof-of-Artificial-Inteligence се у тестирању показао као јако успешан принцип валидације, па се може у блиској будућности развити у комплетан концензус протокол.

Proof of Useful Work

Принципи Рада

Proof-of-Useful-Work (PoUW) механизам ради тако што сваки рудар прво мора да обави неки користан посао, као на пример класификацију података, а затим се такмичи за вођу према броју извршених процесорских инструкција. У поређењу са конвенционалним факторима као што је кашњење мреже, време обављања корисног посла је нови и истакнути фактор који доводи до рачвања *blockchain*-а заснованог на *Proof-of-Useful-Work* принципу.

Кључна разлика између *Proof-of-Work* и *Proof-of-Useful-Work* принципа је *task processing* време, што је нови фактор који доводи до *Proof-of-Useful-Work* рачвања (енгл. *fork*). Стога се постојећи теоријски модели не могу директно користити за анализу вероватноће рачвања *Proof-of-Useful-Work*-а.

За разлику од *Proof-of-Work* принципа, ток обраде у *Proof-of-Useful-Work* се може сажети у пет корака:

Корак 1 - Рудар синхронизује *blockchain* статус са *peer-to-peer* мреже: У *blockchain peer-to-peer* мрежи сви генерисани блокови се дистрибуирају међу свим рударима. Када је рудар спреман да ископа нови блок, он прво синхронизује најновији статус блока са мреже и добија последњи блок у ланцу. Након тога, рудар обавезује и проверава садржај забележен у новом блоку.

Корак 2 - Рудар преузима задатак од корисног радног клијента: Рудар прима задатак од корисних радних клијената и дели задатак у неколико подзадатака, јер сваки задатак може имати различите величине.

Корак 3 - Рудар обрађује задатак и копа нови блок користећи *Proof-of-Useful-Work* механизам: У *Proof-of-Useful-Work* механизму напор ископавања мери се у смислу извршених хеширања, док се у *Proof-of-Useful-Work* механизму мери бројем извршених корисних упутстава за рад, односно за задатак. *Proof-of-Useful-Work* сваку инструкцију третира као Берноуллијево суђење. Стога се време експлоатације у *Proof-of-Useful-Work*-у дистрибуира на приближно исти начин као у *Proof-of-Work*-у.

Корак 4 - Рудар преноси резултат обраде корисном радном клијенту: Једном када се задатак *Proof-of-Useful-Work*-а заустави, рудар враћа израчунате резултате корисном радном клијенту. У таквој ситуацији, иако рудар не копа нови блок, његов процесорски напор се и даље користи за користан рад, уместо да се троши.

Корак 5 - Рудар емитује ископани блок на *peer-to-peer* мрежу: Након што рудар ископа нови блок, рецимо да пронађе одговарајући тренутак, он емитује тај нови блок на мрежу. Једном када прими овај блок, сваки рудар га додаје последњем блоку и ажурира статус ланца блокова. На тај начин, *blockchain* статус свих рудара може бити синхронизован.

У *Proof-of-Useful-Work* консензус механизму рудари користе приступ који се назива *batch lottery* да би се надметали за вођу, а затим генеришу нове блокове, уместо да користе приступ *one-by-one lottery* као што то ради *Proof-of-Work*. Конкретно, у *Proof-of-Work* принципу рудари непрестано покушавају да користе случај *task processing* времена за извлачење лутрије, док у *Proof-of-Useful-Work* принципу рудари покушавају без лутрије након неког времена (тј. *task processing* време). Што је кориснији посао урађен током *task processing* времена, то је већа вероватноћа победе. Стога је *batch lottery* у *Proof-of-Useful-Work* механизму еквивалентна вишеструком извлачењу спојеног *Proof-of-Useful-Work*-а.

У *Proof-of-Useful-Work-y* сваки рудар повремено ради две ствари да би генерисао нови блок:
1) Обавља користан посао у *task processing* времену;
2) Извршава серијску лутрију.

Coin AI

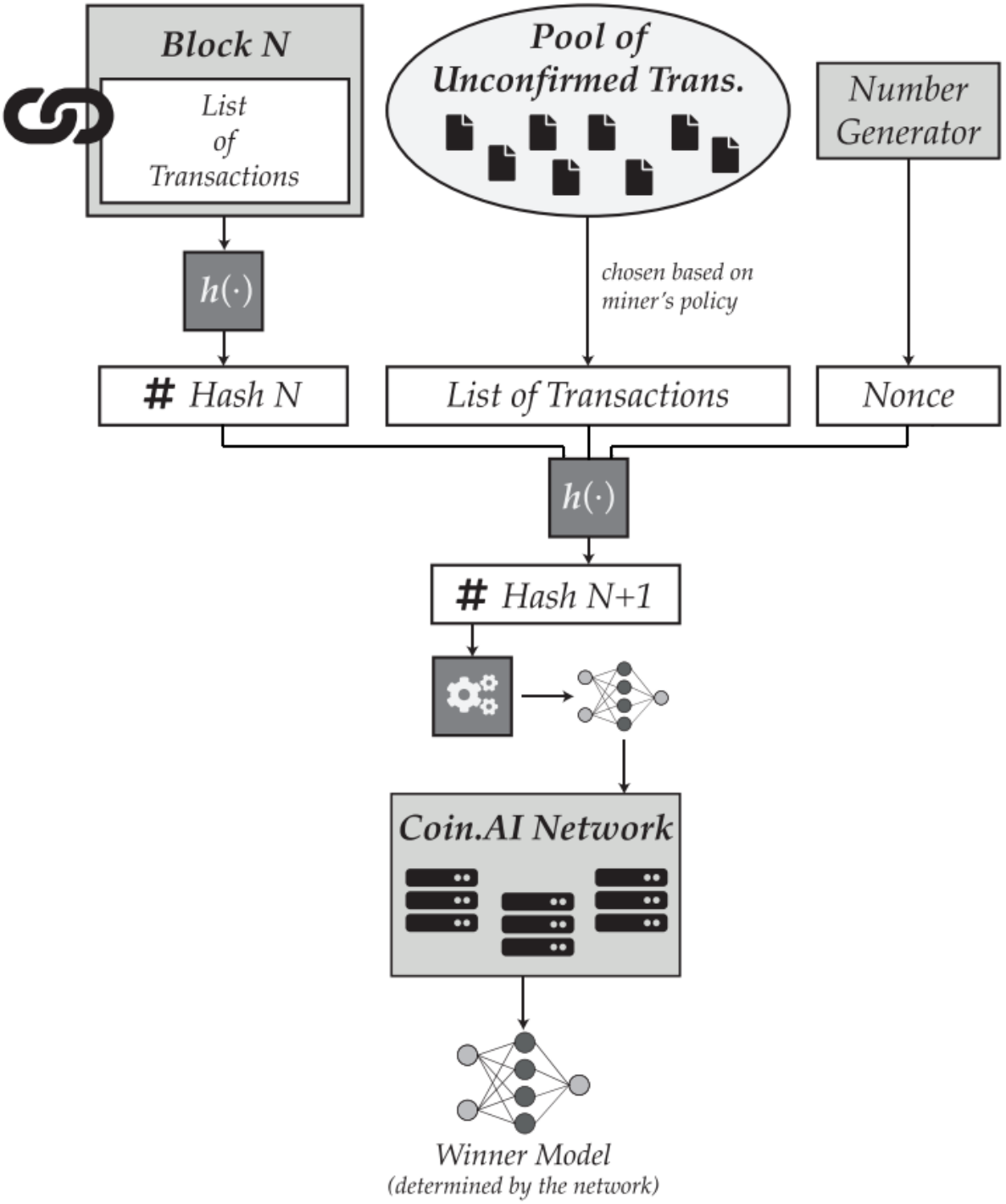
Примена *Proof-of-Useful-Work* алгоритма се може наћи у *blockchain* мрежи која садржи алтернативни новчић, познатија као *Coin AI*.

Творци *Coin AI* сматрају да проблем који треба да реше рудари јесте обука модела вештачке интелигенције, а нарочито архитектура дубоког учења (вероватно конволуциона неуронска мрежа). Обука модела дубоког учења из података укључује учење његових параметара коришћењем неке врсте алгоритма градијентног спуштања. Ово је итеративни поступак који се генерално сматра за скуп рачунски задатак.

Пример *Proof-of-Useful-Work* шеме која је довела до развоја критповалута је *PrimeCoin*, чији се алгоритам копања састоји у тражењу *Cunningham* ланаца и ланаца двоструких близанаца простих бројева. Валута је доступна на многим берзама а цена једног *PrimeCoin*-а износи 0.1902$.

Процес Proof-of-Useful-Work алгоритма се састоји од 6 корака приказаних на слици 8:

(1) Сваки рудар узима хеш последњег блока у *blockchain*-у, бира трансакције из базена непотврђених трансакција и *nonce*.
(2) Три податка ће се конкатенирати и хеш ће се израчунати. Ово је хеш кандидата блока N+1.
(3) *Hash-to-Architecture* мапирање се користи за добављање архитектуре из хеша. Оно ће се тренирати у модел вештачке интелигенције користећи добављене податке.
(4) Ако модел премаши праг квалитета, он се емитује мрежи за процену.
(4а) Ако модел победи, блок N+1 се копа и ажурира на *blockchain*. Рудар добија награду.
(5) Ако модел не премаши праг квалитета, процес се враћа на почетак (1), са новим *nonce*-ом или различитим трансакцијама.
(6) Када се блок N+1 ископа од стране овог или другог рудара, процес се враћа на почетак (1), приморан да користи нови хеш N+1 уместо N, и нову листу трансакција, јер се базен непотврђених трансакција променио.



Слика 8. Алгоритам Proof-of-Useful-Work принципа.

Закључак

Иако је релативно нова технологија, *blockchain* има перспективу у најразличитијим сферама како индустрије, тако и свакодневног живота. Са растећом популарношћу криптовалута, интересовање у *blockchain* технологију, па и њеним побољшањем и оптимизацијама, је веће него икад. Концепти које смо предложили су само једни примери приступа рада *blockchain* концензус алгоритма - *Proof-of-Work* се користио од настанка прве *blockchain* мреже, међутим остали приступи, а поготово *Proof-of-Stake*, се полако уводе и у алгоритме највећих *blockchain* мрежа, наиме на Ether-у.

Вештачка интелигенција у овој причи може имати огромну улогу, не само у оптимизацији концензус алгоритама, већ и у корист самог случаја коришћења *blockchain*-а. *OpenMined* је један овакав пример, децентрализована платформа за размену података у корист научницима која пружа могућност сигурне размене скупова података ради тренирања модела вештачке интелигенције, користећи *blockchain*. *Blockchain*, као и у овом примеру, представља савршено решење за апликације које захтевају слободну и заштићену комуникацију између неке две партије, без умешања неког посредника, што би могло бити врло ризично.

Литература

[1] Bitcoin: A Peer-to-Peer Electronic Cash System: Satoshi Nakamoto.
[Интернет] Садржај доступан на: https://bitcoin.org/bitcoin.pdf

[2] Proof-of-Stake, Investopedia - https://www.investopedia.com/terms/p/proof-stake-pos.asp

[3] Proof-of-Stake Explained, Academy Binance -
https://academy.binance.com/en/articles/proof-of-stake-explained

[4] An AI Based Super Nodes Selection Algorithm in BlockChain Networks:
Jianwen Chen, Kai Duan, Rumin Zhang, Liaoyuan Zeng, Wenyi Wang.
[Интернет] Садржај доступан на: https://arxiv.org/abs/1808.00216

[5] ImageNet Classification with Deep Convolutional Neural Networks:
Alex Krizhevsky, Ilya Sutskever, Geoffrey E. Hinton. [Интернет] Садржај доступан на:
https://papers.nips.cc/paper/2012/file/c399862d3b9d6b76c8436e924a68c45b-Paper.pdf

[6] Duboke Konvolucijske Neuronske Mreže - Koncepti i Aktuelna Istraživanja:
Marko M. Dabović, Igor I. Tartalja. [Интернет] Садржај доступан на:
https://www.etran.rs/common/pages/proceedings/ETRAN2017/VI/IcETRAN2017_paper_VI1_1.pdf

[7] A Proof of Useful Work for Artificial Intelligence on the Blockchain:
Andrei Lihu, Jincheng Du, Igor Barjaktarević, Patrick Gerzanics, Mark Harvilla.
[Интернет] Садржај доступан на: https://arxiv.org/abs/2001.092

[8] Fork Probability Analysis of PoUW Consensus Mechanism: Zhijie Ma, Qinglin Zhao, Jianwen Yuan, Xiaobo Zhou, Li Feng.
[Интернет] Садржај доспутан на: https://ieeexplore.ieee.org/document/9192002

[9] Coin.AI: A Proof-of-Useful-Work Scheme for Blockchain - based Distributed Deep Learning: Alejandro Baldominos, Yago Saez
[Интернет] Садржај доступан на: https://arxiv.org/abs/1903.09800