UNIVERSITATEA BABEŞ-BOLYAI
FACULTATEA DE MATEMATICĂ ŞI INFORMATICĂ

Antrenarea rețelelor neuronale pe blockchain

Rezumatul tezei de doctorat

Student-doctorand: Gyulai-Nagy Zoltán Valentin
Coordonator științific: Prof. dr. Czibula Gabriela

2026

Conținut

Lista publicațiilor

Clasificarea publicațiilor a fost realizată conform standardelor CNATDCU (Consiliul Național de Atestare a Titlurilor, Diplomelor și Certificatelor Universitare), aplicabile doctoranzilor înmatriculați după data de 1 octombrie 2018. Toate clasificările sunt prezentate conform clasificării revistelor[1] și conferințelor[2] din domeniul Informaticii.

Publicații în reviste internaționale

[GN25a] **Gyulai-Nagy Zoltán-Valentin**, *Accelerated Neural Network Initialization via Training of Symmetrically Partitioned Models*, Acta Universitatis Sapientiae, Informatica (AUS 2025), Volume 17, Article no. 12 (**indexare Web of Science**, Q4)

Rang C - 2 puncte.

Publicații în volumele conferințelor

[GN23] **Gyulai-Nagy Zoltán-Valentin**, *Acceleration of Neural Network training algorithm via FPGA Devices*, The 29th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES), Procedia Computer Science, Volume 225, 2023, Pages 2674-2683 (**indexare Web of Science**)

Rang B, 4 puncte.

[GN24] **Gyulai-Nagy Zoltán-Valentin**. *Combining clustering algorithms to extract symmetric clusters from noisy data, applied to parking lots*. The 19th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2024), SciTePress, Volume 1: ENASE, 2024, Pages 362-369 (**indexare Web of Science**)

Rang B, 4 puncte.

[GN25c] **Gyulai-Nagy Zoltán-Valentin**, *Proof of Learning applied to Binary Neural Networks*, The 17th International Conference on Agents and Artificial Intelligence (ICAART), 2025, pp. 411-417 (**indexare Web of Science**)

Rang B, 4 puncte.

[1] https://uefiscdi.ro/premierea-rezultatelor-cercetarii-articole
[2] http://portal.core.edu.au/conf-ranks/

Publicații în volume internaționale

[GN25b] **Gyulai-Nagy Zoltán-Valentin**, *Exploring the Usability and Applicability of Proof of Learning in Binary Neural Networks*, Lecture Notes in Artificial Intelligence (LNAI), 2025, în curs de publicare (**indexare Web of Science**)

Rang C - 2 puncte.

Punctaj publicații: 16 puncte.

Introducere

Această teză investighează integrarea tehnologiei blockchain cu rețelele neuronale, având ca obiectiv optimizarea eficienței computaționale și redefinirea mecanismelor de validare în sistemele descentralizate. Rețelele blockchain, în special cele care utilizează algoritmi de consens de tip Proof-of-Work (PoW), se confruntă cu provocări cauzate de procesele de hashing intensive din punct de vedere computațional, care consumă cantități semnificative de energie [Sed20] fără a produce rezultate utile dincolo de securitatea rețelei. În același timp, antrenarea rețelelor neuronale este un proces costisitor din punct de vedere al resurselor și este adesea limitat de hardware-ul tradițional, precum procesoarele CPU și GPU [FL20]. Această teză propune abordarea acestor provocări prin utilizarea dispozitivelor Field-Programmable Gate Arrays (FPGA) pentru accelerarea antrenării rețelelor neuronale și prin reutilizarea funcțiilor de validare din blockchain pentru a genera rezultate computaționale utile prin intermediul BNN-urilor (Binary Neural Networks).

Problema centrală abordată este ineficiența mecanismelor PoW, care impun participanților să rezolve puzzle-uri criptografice complexe ce nu generează produse secundare tangibile [Pil16]. Această teză sugerează înlocuirea acestor sarcini de validare cu algoritmi care efectuează calcule utile, precum antrenarea rețelelor neuronale, transformând astfel rețelele blockchain în platforme distribuite pentru calcul de înaltă performanță. O contribuție esențială constă în dezvoltarea unei arhitecturi bazate pe FPGA pentru antrenarea rețelelor neuronale, demonstrând potențialul accelerării hardware de a depăși blocajele unităților de procesare convenționale. De asemenea, teza introduce o tehnică de inițializare a modelelor prin partiționare simetrică, menită să reducă timpul de antrenare și consumul de resurse, să susțină distribuirea modelelor într-un număr mare de computere și să permită utilizarea acestor resurse pentru evoluarea modelelor existente în rețea.

Cercetarea stabilește inițial fundamentele teoretice necesare pentru corelarea rețelelor neuronale cu sistemele blockchain. După ce aceste aspecte sunt demonstrate ca fiind viabile pentru o arhitectură de bază, atenția se mută către scalarea sistemului, ceea ce implică și valorificarea modelelor existente și partiționarea acestora pentru a îmbunătăți eficiența. Pentru a ilustra mai clar un scenariu real în care acest sistem oferă beneficii concrete, este prezentat un proiect simplu ce implică antrenarea continuă a rețelelor neuronale. Deși algoritmii pot avea o complexitate crescută, eficiența lor depinde în principal de acuratețea rețelelor neuronale, care poate fi îmbunătățită prin acumularea de date în timp și reantrenări frecvente. Acest lucru face ca proiectul propus să reprezinte un caz de utilizare adecvat.

Prin reducerea decalajului dintre optimizarea hardware și inovația blockchain, acest studiu contribuie la dialogul extins privind sistemele descentralizate sustenabile și orientate spre utilitate, oferind un cadru pentru utilizarea rețelelor neuronale ca instrument cu dublu scop, atât pentru învățare automată, cât și pentru consens distribuit.

Problemele abordate

Teza noastră abordează în primul rând provocarea realizării calculelor într-un mod mai eficient comparativ cu unitățile de calcul tradiționale, precum CPU-urile sau GPU-urile. În tehnologia blockchain, circuitele ASIC sunt utilizate pe scară largă datorită consumului redus de energie și vitezei superioare de calcul, fiind proiectate special pentru astfel de sarcini la nivel hardware [BT13]. Arhitecturile hardware de uz general, deși puternice și versatile, pot beneficia de îmbunătățiri de viteză prin optimizări la nivel hardware. Totuși, aceste dispozitive execută de regulă doar tipuri specifice de operații, ceea ce se aliniază cerințelor hardware-ului specializat utilizat în blockchain. Înainte de fabricarea cipurilor ASIC și implementarea lor în aplicații reale, dispozitivele FPGA sunt utilizate pentru prototipare. Astfel, această cercetare se concentrează pe dezvoltarea unor arhitecturi FPGA care să reprezinte soluții eficiente pentru această problemă.

A doua direcție a cercetării noastre vizează reutilizarea algoritmului de validare pentru a genera produse secundare utile. În contextul actual, multe produse bazate pe inteligență artificială necesită un consum energetic semnificativ [ZLL+24]. În același timp, blockchain-urile au un potențial neexploatat, oferind oricui posibilitatea de a contribui cu putere de calcul pentru a susține un ecosistem larg de algoritmi de antrenare. Acest aspect este deosebit de valoros, deoarece antrenarea modelelor reprezintă una dintre cele mai costisitoare operații în dezvoltarea de noi modele destinate pieței de consum. Acest lucru presupune înlocuirea procesului actual de validare cu unul nou, capabil să valideze blocurile prin munca efectuată de computere care antrenează modele de rețele neuronale. Ideea fundamentală a procesului de hashing, care presupune transformarea blocurilor într-o anumită formă pentru a demonstra efortul computațional, prezintă ineficiențe inerente [G+16], deoarece depinde de puterea de procesare a unităților aflate în competiție. Dorim să abordăm această problemă prin orientarea mecanismului de proof-of-work către evaluarea unor modele din lumea reală, pe care sugerăm să le reprezentăm prin rețele neuronale binare, în locul dependenței exclusive de hash-uri care trebuie să respecte o anumită formă. Aceasta include și posibilitatea de a distribui astfel de sarcini pe mai multe computere din rețeaua blockchain. Așa cum se observă în sistemele blockchain existente, participarea nu este limitată de o cantitate predefinită de putere de calcul pe care computerele trebuie să o dețină, deoarece acest lucru ar limita scalabilitatea rețelei și ar împiedica participanții mai mici să contribuie. În schimb, conceptul de pool-uri de minare este frecvent întâlnit în rândul participanților care dispun de unități de calcul de nivel consumer, dar doresc să contribuie. Ne propunem să explorăm scenarii în care putem permite acestor indivizi să extindă capacitatea blockchain-ului.

În continuare, ne propunem să integrăm și să prezentăm un proiect care poate fi implementat în scenarii din viața reală. Chiar dacă propunerea din această teză este solidă din punct de vedere științific și algoritmii rezolvă eficient problemele menționate anterior, dorim să demonstrăm un scenariu real în care utilizarea sa ar fi benefică. Considerăm că susținerea cercetării prin aplicații care oferă exemple concrete este utilă și menține contextul într-o zonă practică, spre deosebire de una pur empirică, în care cititorul este lăsat să presupună domeniile de aplicare ale sistemului.

Toate problemele menționate mai sus urmăresc crearea unui sistem blockchain mai eficient, care să optimizeze utilizarea puterii de calcul, păstrând în același timp principiile fundamentale ale tehnologiei blockchain.

Contribuții originale

Cercetarea noastră s-a concentrat pe utilizarea dispozitivelor FPGA și a BNN-urilor pentru dezvoltarea unui algoritm blockchain îmbunătățit. Integrarea strânsă a acestor tehnologii oferă o abor-

dare inovatoare cu aplicații practice în reutilizarea blockchain-ului și în antrenarea modelelor la scară largă, care sunt aplicate în final pentru rezolvarea problemei recunoașterii automobilelor într-o parcare. Metodele discutate în Capitolele 2, 3 și 4 sunt sintetizate mai jos:

Perspectiva hardware asupra blockchain-ului

Având în vedere natura problemei, primul aspect analizat este capacitatea de a transpune calculele necesare antrenării rețelelor neuronale la nivel hardware. Acest lucru facilitează integrarea întregului ecosistem în hardware specializat, asigurând un avantaj competitiv care face blockchain-urile mai eficiente pentru sarcini specifice. În acest context, am contribuit prin dezvoltarea unei soluții hardware complete pe dispozitive FPGA, care poate fi adaptată cu ușurință în procesoare ASIC complete. Contribuțiile noastre principale includ implementarea și cercetarea unor arhitecturi hardware capabile să accelereze calculele necesare blockchain-ului propus.

Operațiile de bază aflate la fundamentul rețelelor neuronale sunt operațiile de înmulțire și sumare. Provocarea apare atunci când numărul acestora este mare și există dependențe între ele, care trebuie respectate în timpul calculelor dintre straturi.

- Abordarea de accelerare hardware prezentată în articolul original [GN23], introdusă în Capitolul 2, urmărește să abordeze aceste provocări. Cercetarea noastră se concentrează pe dezvoltarea unor nuclee de înmulțire și adunare capabile să satisfacă aceste cerințe. Aceste nuclee sunt modulare și configurabile, permițând scalarea în funcție de hardware-ul FPGA utilizat. Ele pot fi dispuse pe hardware astfel încât să reflecte structura și straturile rețelelor neuronale, permițând un flux de date eficient între nuclee pentru a crește viteza de procesare. Conectate prin blocuri de memorie special proiectate, un nucleu scrie întotdeauna într-un bloc, în timp ce un singur nucleu citește din acesta. Această configurație elimină necesitatea unei logici personalizate de prioritizare pentru planificarea calculelor. Lățimea magistralei sistemului este ajustabilă, suportând diferite tipuri de date, de la valori pe 2 biți până la 64 de biți. Această flexibilitate permite antrenarea modelelor cu cuantizări adaptate cerințelor aplicației. Calculele sunt efectuate în paralel ori de câte ori este posibil. Practic, toate valorile de pe magistrală pot fi înmulțite sau însumate într-o singură operație, crescând semnificativ viteza. Nucleele sunt proiectate pentru a fi ușor scalabile, fiind limitate în principal de spațiul disponibil pe hardware-ul FPGA sau ASIC pentru extinderea magistralei. Utilizarea hardware-ului specializat reduce, de asemenea, consumul energetic, deoarece focalizarea pe un set limitat de operații elimină funcțiile periferice inutile întâlnite în procesoarele de uz general, conducând la o utilizare mai eficientă a energiei.

În ansamblu, contribuția noastră prin intermediul nucleelor de calcul urmărește să ofere o soluție pentru extinderea blockchain-ului pe hardware personalizat, proiectat să accelereze operațiile. Acestea evidențiază posibilitățile extinse de specializare și optimizare suplimentară în domeniul hardware.

Încredere algoritmică prin validare reutilizată

Scopul blockchain-urilor este de a stabili o bază solidă care să susțină multiple funcții critice, asigurând în același timp disponibilitatea și consistența. Acestea posedă proprietăți inerente care le susțin principiile fundamentale. Un element esențial este algoritmul de validare, care verifică dacă un bloc face parte din blockchain și dacă îndeplinește criteriile necesare pentru a fi adăugat, asigurând respectarea tuturor cerințelor. Aceste cerințe sunt concepute pentru a garanta că, în cadrul unor sisteme de calcul distribuite de mari dimensiuni, participanții respectă regulile stabilite. Cercetarea noastră explorează posibilitatea menținerii unui astfel de cadru, modificând în același timp modul de funcționare

al blockchain-urilor PoW. Scopul este valorificarea mai eficientă a capacității de calcul și oferirea unui nou scop acesteia, generând beneficii suplimentare pentru utilizatorii blockchain-ului prin crearea de produse secundare utile în aplicații reale.

- În articolul nostru original [GN25c], introdus în capitolul 3, prezentăm un algoritm de validare modificat care leagă blocurile prin verificarea faptului că participanții care le-au trimis au antrenat efectiv un model de rețea neurală. Dovada trimisă de contributori constă într-un bloc ce conține câmpurile standard, precum tranzacții și informații încorporate, plus o rețea neuronală binară. Sunt luate în considerare scenarii în care seturi de date limitate pot determina convergența modelelor către stări similare. Pentru a preveni acest lucru, algoritmi evolutivi ajustează modelele pentru a menține diversitatea și performanța optimă. Procesul implică testarea modelelor cu date pentru identificarea indicatorilor de performanță, consumând putere de calcul. Cercetarea noastră arată că metodele alternative de validare, comparativ cu PoW tradițional, pot urmări eficient efortul contributorilor în antrenarea și validarea rețelelor neuronale.

- Pentru a completa algoritmul, articolul original [GN25a], prezentat în Capitolul 3, explorează modalități de a permite distribuirea volumului de lucru între toți contributorii rețelei, reducând astfel nevoia de hardware de înaltă performanță. În mod obișnuit, mining pool-urile din blockchain colaborează pentru a rezolva provocările computaționale impuse de blockchain. În cazul nostru, pentru a permite același mecanism, ne propunem să împărțim iterațiile de antrenare între noduri, pentru a obține rezultate mai rapide. Totuși, trebuie să avem în vedere faptul că modelele trebuie să se încadreze în limitele hardware, ceea ce nu este întotdeauna posibil. Prin urmare, antrenarea aceluiași model mare de rețea neuronală în batch-uri ar putea să nu fie potrivită. Ideal ar fi ca modelul să poată fi împărțit fie pe straturi, fie prin tăiere în interiorul straturilor, porțiunile mai mici fiind distribuite contributorilor, care apoi combină aceste părți pentru a forma un model antrenat. Astfel de metode de antrenare necesită sincronizare frecventă între noduri, motiv pentru care am propus o abordare diferită: pre-antrenarea sub-secțiunilor de ponderi ale modelului pe o rețea neuronală, cu scopul de a le antrena în continuare după concatenare. Cercetarea noastră demonstrează cu succes că această metodă poate inițializa ponderile modelului într-un mod distribuit, reducând astfel timpul total de antrenare pentru modelul complet. Această contribuție deschide calea pentru mining pool-uri care distribuie recompensele între participanți să devină mai incluzive, în special pentru cei care nu dispun de puterea de procesare necesară antrenării rețelelor neuronale de dimensiuni mari.

- Dezvoltând rezultatele articolului anterior, ne-am extins cercetarea în [GN25b], prezentat în Capitolul 3, prin includerea unor cazuri de utilizare suplimentare și prin efectuarea de teste suplimentare pentru a-i verifica fezabilitatea. Aceasta a implicat explorarea beneficiilor utilizării modelelor generate prin blockchain, cu scopul de a îmbunătăți securitatea și de a ne asigura că acestea respectă constrângerile arhitecturii blockchain. Printre aspectele cheie analizate se numără capacitatea de a ajusta dificultatea rețelei, care influențează modul în care recompensele sunt scalate și reglementate. De asemenea, am evaluat diversitatea modelelor, care contribuie la întărirea securității împotriva spoofing-ului și a potențialelor atacuri ce ar putea compromite blockchain-ul. Rezultatele arată viabilitatea acestei abordări, demonstrând că poate fi eficientă nu doar în medii controlate, ci și în sisteme distribuite la scară largă, în care actori externi ar putea încerca să manipuleze rezultatele și să submineze mecanismul de validare.

Aceste direcții demonstrează că stabilirea unei încrederi algoritmice care să reflecte natura distribuită a blockchain-urilor este realizabilă, chiar și modificând mecanismul fundamental de vali-

dare. Modificările păstrează principiile de bază ale blockchain-urilor și funcționalitatea existentă, permițând utilizarea puterii de calcul pentru dezvoltarea ulterioară a rețelelor existente și viitoare.

Un caz de utilizare practic

Cercetarea empirică se încheie adesea cu o metodologie care pare potrivită pentru aplicații reale, dar care uneori se deconectează de realitatea practică. Din acest motiv, dorim să demonstrăm cu o aplicație concretă care poate valorifica mecanismul nostru de validare adaptat, pentru a-i demonstra fezabilitatea.

- Am dezvoltat o aplicație complexă care implică mai mulți algoritmi ce urmăresc să identifice în mod determinist disponibilitatea locurilor de parcare. Așa cum este prezentat în articolul noastru [GN24], introdus în Capitolul 4, contribuția noastră constă într-un algoritm bine definit, care nu depinde de variabile externe pentru a specifica locurile de parcare și pentru a detecta automat disponibilitatea lor. Am folosit tehnici de clusterizare și segmentare pentru a estima probabilitatea ca o mașină să fie parcată într-un anumit loc. În ciuda naturii deterministe a algoritmului și a performanței sale bune, am constatat că este esențială reantrenarea continuă, pe baza detecțiilor pozitive, pentru a-i îmbunătăți acuratețea până la un nivel mai fiabil. Mașinile sunt identificate în imaginile provenite de la camere folosind rețele neuronale convoluționale, care, deși au evoluat și mai mult de la momentul redactării, rămân o metodă standard pentru detecția de obiecte. Condițiile de mediu, iluminare și vreme influențează semnificativ modul în care mașinile apar în imagini. Reantrenarea regulată, folosind date relevante colectate de camerele de la fața locului despre mașini, îmbunătățește acuratețea sistemului. Această abordare ilustrează modul în care validarea prin blockchain poate fi folosită pentru a asigura că sistemul rămâne precis, în ciuda factorilor externi în continuă schimbare, precum reflexiile, iluminarea și multe altele. Cercetarea noastră evidențiază importanța reantrenării continue a modelului pentru a se adapta la numeroșii factori externi care evoluează și afectează capacitatea de detecție a locurilor de parcare.

Acest exemplu clarifică tipurile de aplicații care pot beneficia de sistemul propus. Cererea pentru antrenarea modelelor specializate va continua să existe, iar un depozit centralizat, accesibil public, permite verificarea și reutilizarea eficientă a modelelor.

Structura tezei

Restul tezei este structurat după cum urmează. Capitolul 1 oferă o introducere generală în problema propusă, explicând mecanica și scopul blockchain-urilor, împreună cu ineficiențele acestora. De asemenea, stabilește cunoștințele fundamentale necesare pentru a înțelege funcționalitatea tehnologiilor precum rețelele neuronale si blockchain, oferind o perspectivă asupra modului în care aceste tehnologii se pot completa reciproc. Capitolul evidențiază domeniile în care acestea au suprapunere și își pot extinde funcționalitățile. În plus, oferă o revizuire cuprinzătoare a literaturii existente, concentrându-se asupra stadiului actual al cercetărilor în aceste domenii.

Capitolul 2 se concentrează pe aspectele hardware implicate în implementarea unor componente de accelerare pentru blockchain. Se subliniază importanța accelerării hardware și avantajele acesteia în ceea ce privește viteza și eficiența energetică. Capitolul evidențiază blocurile de bază care oferă fundamentul pentru proiectarea unor arhitecturi hardware personalizabile, adaptate unui blockchain complet. Sunt discutate mai multe arhitecturi ca posibile soluții pentru efectuarea operațiilor matematice pe dispozitive FPGA, denumite nuclee de procesare (processing cores). Aceste nuclee reprezintă

componentele de bază pentru dezvoltarea dispozitivelor accelerate hardware destinate aplicațiilor blockchain. Deși capitolul nu se concentrează în mod special pe ASIC-uri, el descrie beneficiile utilizării dispozitivelor FPGA, care pot depăși unitățile de calcul tradiționale. Transformarea arhitecturilor FPGA în cipuri ASIC îmbunătățește performanța prin eliminarea limitărilor inerente dispozitivelor FPGA, rezultând cipuri cu o putere de procesare mai mare. Aceasta este, de altfel, o practică răspândită în domeniul blockchain. Capitolul subliniază, de asemenea, importanța scalării și integrării acestor nuclee în arhitecturi hardware configurabile, care să corespundă nevoilor în continuă evoluție ale sistemelor blockchain.

Capitolul 3 abordează perspectiva software a aplicației. Discută modul în care reutilizarea algoritmului de validare ridică provocări esențiale ce trebuie soluționate pentru a construi un blockchain funcțional. Capitolul descrie funcționalitățile de bază și ajustările algoritmice necesare pentru integrarea noului mecanism de validare. Oferă detalii despre logica algoritmului și subliniază importanța naturii distribuite a blockchain-ului, esențială pentru funcționarea acestuia. O posibilă implementare presupune distribuirea volumului de lucru prin antrenarea unor partiții simetrice ale modelelor de rețele neuronale. Per ansamblu, acest capitol prezintă propunerea principală a tezei, permițând un algoritm de validare funcțional care poate fi integrat în blockchains și care face posibilă utilizarea puterii de procesare intr-o manieră mai semnificativă.

Capitolul 4 adoptă o abordare diferită, ilustrând un caz de utilizare pentru tehnologia blockchain. Se îndepărtează de stilul capitolelor anterioare pentru a explora și descrie o problemă complexă, care necesită o integrare algoritmică extinsă pentru a funcționa eficient. Problema tratată în acest capitol este detectarea locurilor de parcare libere și ocupate. Deși descrie o abordare construită special, cu o acuratețe bună, capitolul concluzionează că o acuratețe mai ridicată depinde de sesiuni frecvente de reantrenare cu date noi, colectate din sistem. Prin scalarea acestei aplicații la un nivel de integrare mai mare, cu multiple parcări, devine evident că blockchain-ul poate genera continuu noi modele pe baza datelor în timp real, permițând îmbunătățirea continuă a rețelelor neuronale fără hardware specializat, menținând în același timp securitatea.

În final, ultimul capitol prezintă concluziile acestei teze și conturează direcțiile viitoare de explorare a avantajelor abordării propuse.

Capitolul 1

Fundamente teoretice

În acest capitol vom oferi o perspectivă asupra stadiului actual al principalelor tehnologii utilizate în cadrul proiectului. Soluția propusă reprezintă o îmbunătățire, iar pentru a înțelege problema pe care ne propunem să o rezolvăm, vom prezenta funcționalitatea și arhitectura blockchain-urilor și a rețelelor neuronale. Comunitățile care utilizează aceste tehnologii au identificat deja mai multe domenii în care pot fi aduse îmbunătățiri; prin urmare, pentru a înțelege comportamentul specific al proiectului nostru, vom prezenta și o parte din cercetările existente care încearcă să ofere soluții acestor probleme.

Capitolul 2

Perspectiva hardware asupra blockchain-ului

Acest capitol explorează potențialul dispozitivelor FPGA de a revoluționa ecosistemele hardware utilizate în blockchain. Sunt evaluate avantajele acestora față de unitățile de procesare tradiționale (CPU/GPU) și sunt cuantificate câștigurile de productivitate pentru dezvoltatori, în special în scenarii care necesită prototipare rapidă sau procesare paralelă.

Blockchain-urile, cu natură descentralizată, se bazează în mare măsură pe circuite integrate specifice aplicațiilor (ASIC) pentru executarea sarcinilor intensive din punct de vedere computațional, precum minarea și validarea contractelor inteligente. Deși ASIC-urile oferă o eficiență neegalată pentru operații predefinite, rigiditatea acestora și consumul energetic ridicat ridică provocări semnificative. Pe măsură ce cererea pentru soluții blockchain sustenabile și adaptabile crește, limitările ASIC-urilor, în special lipsa de flexibilitate în fața algoritmilor în continuă evoluție și costurile aferente, impun necesitatea unor alternative inovatoare.

Dispozitivele Field-Programmable Gate Arrays (FPGA) apar ca o punte promițătoare între procesoarele de uz general și ASIC-uri. Spre deosebire de ASIC-uri, care sunt cablate static pentru sarcini specifice, FPGA-urile oferă arhitecturi hardware reconfigurabile, permițând optimizarea dinamică pentru diverse sarcini blockchain. Această adaptabilitate este în concordanță cu natura evolutivă a protocoalelor blockchain, precum algoritmii de tip proof-of-work (PoW) sau mecanismele de consens bazate pe învățare automată, menținând în același timp eficiența energetică. Prin echilibrarea flexibilității cu performanța, FPGA-urile abordează compromisul critic dintre puterea de calcul și consumul energetic, poziționându-se ca un pas intermediar viabil către viitoare proiectări ASIC.

Rezultatele prezentate în acest capitol sunt incluse într-unul dintre articolele originale [GN23]. Contribuția noastră este următoarea:

- Au fost proiectate două nuclee de calcul personalizate pentru a efectua operațiile esențiale necesare antrenării rețelelor neuronale. Acestea gestionează operații de adunare și multiplicare pe magistrale cu lățimi de biți variabile. Fiecare magistrală codifică valorile folosind un număr configurabil de biți, permițând operații pe diferite niveluri de cuantizare ale modelelor. Nucleele sunt configurate pentru a procesa simultan toate valorile de pe magistrale, sporind paralelismul. Aceste nuclee pot fi integrate în proiecte hardware care reflectă structura operațiilor de antrenare ale rețelelor neuronale, permițând calcule eficiente, realizate în flux, între ele. Ele constituie baza dezvoltării de hardware optimizat pentru modele specifice de rețele neuronale.

Prin demonstrarea capacității FPGA-urilor de a reduce costurile energetice și de a îmbunătăți eficiența computațională, acest capitol contribuie la discuția privind infrastructura blockchain susten-

abilă. El evidențiază potențialul hardware-ului reconfigurabil de a depăși limitările actuale și de a deschide calea către soluții scalabile și eficiente energetic în sistemele descentralizate.

Restul acestui capitol este organizat în șase secțiuni principale, fiecare abordând aspecte specifice ale soluțiilor hardware bazate pe FPGA pentru aplicații blockchain. Structura este concepută pentru a explora sistematic fezabilitatea, performanța și beneficiile de productivitate oferite de FPGA-uri și pentru a răspunde întrebărilor de cercetare. Secțiunea 2.1 introduce o abordare de accelerare a antrenării rețelelor neuronale utilizând dispozitive FPGA. Enunțul problemei este prezentat în Secțiunea 2.2, iar analiza stadiului actual al literaturii științifice este prezentată în Secțiunea 2.3. Metodologia utilizată în cercetarea noastră este detaliată în Secțiunea 2.4, în timp ce Secțiunea 2.5 discută rezultatele și testele efectuate pentru a reafirma viabilitatea abordării propuse. În final, Secțiunea 2.6 concluzionează cercetarea și identifică direcții viitoare de explorare.

Capitolul 3

Încredere algoritmică prin validare reutilizată

Validarea în blockchain reprezintă un pilon fundamental al sistemelor descentralizate, asigurând consensul și încrederea prin mecanisme precum Proof of Work (PoW) sau Proof of Stake (PoS). În blockchain-urile tradiționale, tranzacțiile sunt verificate de noduri prin intermediul hashing-ului criptografic, iar algoritmii de consens garantează imutabilitatea și securitatea rețelei. Cu toate acestea, aceste metode se confruntă adesea cu provocări precum costuri computaționale ridicate, limitări de scalabilitate și ineficiență energetică. Acest capitol explorează o abordare inovatoare a validării prin reutilizarea tehnicilor algoritmice din domeniul învățării automate (Machine Learning – ML) pentru a aborda aceste limitări, permițând cadre de validare eficiente, distribuite și scalabile.

Metoda propusă mută accentul de la validarea centrată exclusiv pe blockchain către conceptul de încredere algoritmică, printr-un model alternativ de validare a modelelor, partiționare și segmentare a seturilor de date. Sunt abordate, de asemenea, aspecte esențiale legate de menținerea caracterului distribuit al blockchain-ului, astfel încât participanții care dispun de resurse de calcul diferite să poată contribui în mod echitabil. Rezultatele prezentate în acest capitol sunt incluse în trei articole originale [GN25c], [GN25b], [GN25a], după cum urmează:

- Aplicarea conceptului de Proof of Learning asupra rețelelor neuronale binare este introdusă în articolul [GN25c]. Contribuția noastră principală constă în definirea unui algoritm care permite crearea și validarea blocurilor pe baza dovezii că rețele neuronale au fost antrenate. Ideea centrală este stocarea rețelelor neuronale binare în fiecare bloc, lucru fezabil datorită dimensiunii lor reduse. Participanții, la acceptarea noilor blocuri, verifică îndeplinirea unor metrici-cheie de performanță. Abordarea gestionează și scenarii complexe, precum utilizarea algoritmilor evolutivi pentru a preveni convergența modelelor de rețele neuronale către rezultate similare. Forma și ponderile modelelor sunt evoluate pentru a menține un nivel suficient de diversitate, permițând astfel adaptarea la cererea potențial constantă de noi blocuri. Abordarea studiată stabilește o bază pentru reutilizarea puterii de procesare a blockchain-ului prin stocarea BNN-urilor — produsele secundare ale procesului de validare — direct pe blockchain. Aceste modele sunt accesibile publicului sub forma unui depozit centralizat de modele, păstrând în același timp funcționalitățile tranzacționale ale blockchain-ului.

- Următoarea contribuție este prezentată în articolul [GN25b], care extinde direcțiile de cercetare ale lucrării anterioare. Pe baza rezultatelor obținute anterior, cercetarea a fost extinsă prin includerea unor cazuri de utilizare suplimentare și prin testări riguroase menite să valideze fezabilitatea integrării modelelor generate de blockchain în sisteme descentralizate. Studiul s-

a concentrat pe valorificarea blockchain-ului pentru creșterea securității, respectând în același timp constrângerile sale arhitecturale. Principalele direcții investigate includ: analiza modului în care setările de dificultate ale rețelei influențează scalarea recompenselor și stabilitatea sistemului, precum și evaluarea rolului variației arhitecturale a modelelor în atenuarea atacurilor adversariale și a tentativelor de spoofing. Aceste aspecte evidențiază capacitatea sistemului de a respecta și susține principiile consacrate ale tehnologiei blockchain. Rezultatele obținute confirmă viabilitatea acestei abordări atât în medii controlate, cât și în sisteme distribuite de mari dimensiuni, unde tentativele de manipulare externă sunt frecvente.

- O altă contribuție, prezentată în articolul [GN25a], introduce o abordare inovatoare pentru inițializarea distribuită a rețelelor neuronale, permițând nodurilor cu resurse limitate să participe la antrenarea modelelor de mari dimensiuni. Cadrul propus abordează atât provocările legate de inițializare, cât și pe cele ale antrenării distribuite, oferind beneficii precum reducerea timpilor de calcul, îmbunătățirea scalabilității și creșterea acurateții pentru rețele neuronale mari și complexe. Prin valorificarea colaborării inspirate de blockchain, metoda permite participanților cu resurse reduse să contribuie în mod semnificativ la procesele de antrenare. Abordarea include un algoritm de partiționare a modelelor, care împarte rețelele neuronale în segmente mai mici pentru antrenare paralelă, inițializarea distribuită a ponderilor pentru accelerarea convergenței și tehnici de completare (padding) pentru gestionarea datelor cu dimensiuni impare. Validarea experimentală pe seturi de date precum MNIST, CIFAR-10 și ImageNet demonstrează îmbunătățiri semnificative în eficiența antrenării și acuratețea modelelor.

Restul capitolului este organizat după cum urmează. Secțiunea 3.1 detaliază aplicarea mecanismului de proof of learning asupra algoritmului de rețele neuronale binare. Analiza literaturii de specialitate care susține cercetarea curentă este prezentată în Subsecțiunea 3.1.1, în timp ce enunțul problemei și întrebările de cercetare sunt descrise în Subsecțiunea 3.1.2. Subsecțiunea 3.1.3 oferă o descriere detaliată a algoritmului și a rezultatelor obținute, incluzând testele prezentate în Subsecțiunea 3.1.4. Concluziile referitoare la acest algoritm sunt formulate în Subsecțiunea 3.1.5. Secțiunea 3.2 introduce apoi algoritmul de inițializare accelerată a rețelelor neuronale, analiza literaturii fiind prezentată în Subsecțiunea 3.2.1. Detaliile metodologice sunt explicate în Subsecțiunea 3.2.2, rezultatele testelor fiind prezentate în Subsecțiunea 3.2.3. În final, concluziile privind algoritmul de inițializare sunt formulate în Subsecțiunea 3.2.4.

Capitolul 4

Caz de utilizare practic

Cercetarea științifică se dezvoltă prin conectarea cadrelor teoretice cu aplicații din lumea reală. Un caz de utilizare practic este esențial pentru a valida necesitatea metodologiilor propuse și pentru a demonstra capacitatea acestora de adaptare în medii dinamice. Acest capitol prezintă un caz de utilizare practic: dezvoltarea unei abordări robuste, fără parametri prestabiliți, pentru detectarea locurilor de parcare în parcări monitorizate video. Algoritmii tradiționali de partiționare (eng. *clustering*), precum OPTICS sau DBSCAN, se bazează pe parametri fixați, care se confruntă cu dificultăți în cazul distribuțiilor neuniforme ale datelor și necesită ajustări manuale. Această limitare este deosebit de pronunțată în parcări, unde modelele de ocupare a vehiculelor variază atât spațial, cât și temporal. Pentru a depăși aceste limitări, propunem un cadru de antrenare iterativă care elimină dependența de praguri predefinite, asigurând rezultate consistente indiferent de rezoluție sau unghiul camerei.

Cel mai potrivit caz de utilizare pentru antrenarea iterativă este detectarea locurilor de parcare, unde imaginile detectate ale vehiculelor au forme variabile, iar valorile aberante sunt eliminate progresiv. În acest context, rafinarea iterativă este indispensabilă: parcările prezintă modele de utilizare neregulate (de exemplu, zone subutilizate sau distorsiuni ale imaginii) și necesită adaptare dinamică la schimbările de mediu. Prin iterarea pragurilor de dimensiune ale clusterelor și prin utilizarea unor metrici derivate din date (de exemplu, lățimea mediană a clusterelor), abordarea noastră se adaptează automat la variațiile de densitate, eliminând necesitatea intervenției umane. Deși această abordare, utilizată independent, poate detecta cu o acuratețe ridicată locurile de parcare, în anumite situații vehiculele nu sunt identificate corect din cauza factorilor de mediu. Pentru a remedia acest aspect, pot fi utilizate mostrele vehiculelor detectate pentru reantrenarea modelului și îmbunătățirea detecției în timp real. Această metodă nu doar că îmbunătățește acuratețea pentru utilizatorii în timp real, ci evidențiază și necesitatea unui sistem precum cel prezentat în această teză, în care modelele pot fi reantrenate continuu pe baza datelor noi, adaptând și scalând aplicația în mod constant.

- Articolul original [GN24] contribuie cu o metodologie nouă și flexibilă pentru detectarea locurilor de parcare, care combină clusterizarea ierarhică (HDBSCAN), hărțile auto-organizatoare (Self-Organizing Maps – SOM) și algoritmul K-means. Contribuțiile principale includ următoarele aspecte: un proces iterativ de eliminare a zgomotului care reduce sistematic zgomotul și clusterele neregulate prin ajustarea dimensiunii minime a clusterelor și evaluarea simetriei folosind praguri generalizate de lățime; adaptarea topologică prin utilizarea hărților auto-organizatoare (SOM), care mențin relațiile spațiale și folosesc memorie pe termen scurt pentru a identifica schimbări de topologie, precum modificările perspectivei camerei; creșterea acurateții în timp real prin reantrenarea modelelor YOLOv8 care utilizează bounding box-urile detectate, sporind precizia detecției și reducând numărul de rezultate fals negative; metrici dinamice care generează scoruri de încredere și analizează suprapunerile spațiale pentru a furniza informații

privind gradul de ocupare, susținând astfel gestionarea eficientă a parcărilor.

Aplicația poate funcționa autonom, însă nu dispune de informații explicite despre mediul parcărilor. Deși modelele se îmbunătățesc în timp, acestea generalizează întotdeauna pe baza datelor de antrenare și sunt, într-o anumită măsură, limitate de acestea. Factori precum condițiile de mediu sau iluminarea variabilă pot reduce performanța sistemului, care este centrat pe analiză de imagine. Deși aplicația include și alți algoritmi menite să atenueze aceste constrângeri, performanța generală rămâne dependentă de calitatea detecțiilor vizuale. Reantrenarea rețelelor neuronale convoluționale cu date noi, specifice cazului de utilizare, este esențială și poate fi realizată prin intermediul unui blockchain modificat care furnizează modele ca produs secundar al procesului de validare. Prin urmare, această aplicație reprezintă un exemplu relevant al modului în care algoritmul blockchain modificat propus în această teză își poate demonstra avantajele.

Restul acestui capitol este organizat după cum urmează. Secțiunea 4.1 descrie aplicația și scopul acesteia, în timp ce Secțiunea 4.2 prezintă o analiză a abordărilor existente din literatura de specialitate. În Secțiunea 4.3 este formulat enunțul problemei, însoțit de întrebările de cercetare care delimitează aria de studiu. Secțiunea 4.4 detaliază metodologia și algoritmii utilizați în cadrul aplicației. Secțiunea 4.5 prezintă cazurile de testare și rezultatele obținute. În final, Secțiunea 4.6 sintetizează concluziile și discută posibilitățile de extindere a aplicației.

Concluzii

Teza prezentată oferă un studiu cuprinzător care integrează tehnologia blockchain cu rețelele neuronale în vederea îmbunătățirii mecanismelor de validare pentru aplicații din lumea reală, având ca studiu de caz principal detectarea disponibilității locurilor de parcare. Cercetarea își propune să demonstreze modul în care mecanismele de validare reutilizate pot fi aplicate eficient prin intermediul tehnologiei blockchain, cu accent pe aplicații la scară largă.

Structura tezei este organizată metodic de-a lungul mai multor capitole:

Capitolul 1 a introdus problema de cercetare, mecanismele blockchain-urilor, ineficiențele acestora și elementele de bază ale rețelelor neuronale. A trecut în revistă literatura existentă pentru a stabili modul în care aceste tehnologii se pot completa reciproc în atingerea rezultatelor dorite.

În Capitolul 2, accentul se mută pe aspectele hardware, discutând componente de accelerare pentru blockchain și subliniind importanța accelerării hardware pentru viteză și eficiență energetică. Capitolul a explorat dispozitivele FPGA și ASIC ca posibile soluții pentru executarea operațiilor matematice în blockchain, evidențiind capacitățile lor de scalare și integrare.

Capitolul 3 a oferit o perspectivă software, abordând provocările reutilizării algoritmilor de validare pentru aplicații blockchain. A descris ajustările algoritmice necesare pentru integrarea unor noi mecanisme de validare în sisteme distribuite.

Explorarea a continuat în Capitolul 4, printr-un caz de utilizare ce implică detectarea locurilor de parcare libere și ocupate. Acest capitol subliniază necesitatea reantrenării frecvente cu date noi și propune scalarea aplicației pentru a genera continuu modele, îmbunătățind astfel acuratețea rețelelor neuronale fără hardware specializat.

Utilizarea unei aplicații precum cea descrisă în Capitolul 4 la scară mai mare necesită antrenarea și centralizarea unui număr mare de modele și seturi de date. Fluxul constant de date și nevoia de reantrenare frecventă cer resurse de calcul semnificative. În plus, securitatea și trasabilitatea sunt esențiale; atunci când datele sunt centralizate, ele trebuie protejate împotriva modificărilor neautorizate și a accesului la informații personale sensibile. Publicarea acestor seturi de date și actualizarea lor regulată oferă comunității open source șansa de a valorifica datele și de a dezvolta aplicații noi și inovatoare.

Teza noastră a explorat atât dimensiunile empirice, cât și pe cele practice ale abordării propuse. Lucrarea de bază susține blockchain-uri complete care încorporează algoritmul nostru de validare adaptat. Partea de testare examinează diverși factori relevanți pentru implementări la scară largă ale lanțului. Capitolele au prezentat blocurile de construcție esențiale, acoperind aspecte hardware importante pentru calculele moderne de mare capacitate și detaliind algoritmi software capabili să implementeze un blockchain care aduce valoare suplimentară unui registru tranzacțional foarte sigur. Prin contribuțiile noastre în multiple domenii conexe acestui subiect, am analizat științific abordarea și i-am demonstrat viabilitatea.

În concluzie, teza și-a sintetizat rezultatele și a propus direcții viitoare pentru valorificarea avantajelor abordării prezentate. A oferit o modalitate inovatoare prin combinarea tehnologiei blockchain cu rețele neuronale pentru a aborda probleme din lumea reală, precum detecția disponibilității locurilor

de parcare, sugerând un model sustenabil care ar putea reduce sarcinile de calcul asupra centrelor de date. Accentul pus pe reantrenare continuă și scalabilitate evidențiază potențialul unor sisteme adaptive, capabile să evolueze odată cu schimbarea condițiilor.

Explorările viitoare s-ar putea concentra pe îmbunătățirea eficienței și scalabilității rețelelor neuronale integrate în blockchain, pe extinderea aplicațiilor dincolo de detecția locurilor de parcare și pe abordarea limitărilor sau provocărilor identificate în abordarea actuală.

Bibliografie

[BT13] Michael Bedford Taylor. Bitcoin and the age of bespoke silicon. In *2013 International Conference on Compilers, Architecture and Synthesis for Embedded Systems (CASES)*, pages 1–10, 2013.

[FL20] Zonghao Feng and Qiong Luo. Evaluating memory-hard proof-of-work algorithms on three processors. *Proc. VLDB Endow.*, 13(6):898–911, February 2020.

[G+16] Arthur Gervais et al. On the Security and Performance of Proof of Work Blockchains. In *CCS 2016*, page 3–16, 2016.

[GN23] Zoltán-Valentin Gyulai-Nagy. Acceleration of Neural Network training algorithm acceleration via FPGA Devices. In *The 27th International Conference on Knowledge-Based and Intelligent Information & Engineering Systems (KES 2023)*, pages 2674–2683, 2023. Procedia Computer Science, Volume 225.

[GN24] Zoltán-Valentin Gyulai-Nagy. Combining clustering algorithms to extract symmetric clusters from noisy data, applied to parking lots. In *Proceedings of the 19th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2024)*, pages 1–8, 2024.

[GN25a] Zoltán-Valentin Gyulai-Nagy. Accelerated Neural Network Initialization via Training of Symmetrically Partitioned Models. *Acta Universitatis Sapientiae, Informatica*, 17:Article no. 12, 2025.

[GN25b] Zoltán-Valentin Gyulai-Nagy. Exploring the Usability and Applicability of Proof of Learning in Binary Neural Networks. *Lecture Notes in Artificial Intelligence (LNAI)*, page to be published, 2025.

[GN25c] Zoltán-Valentin Gyulai-Nagy. Proof of Learning applied to Binary Neural Networks. In *Proceedings of the 17th International Conference on Agents and Artificial Intelligence (ICAART 2025)*, pages 1–8, 2025.

[Pil16] Marc Pilkington. Blockchain technology: principles and applications. In *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

[Sed20] Buhl-H.U. Fridgen G. et al. Sedlmeir, J. The energy consumption of blockchain. *Business Information Systems Engineering*, 2020.

[ZLL+24] Haiyun Zhu, Jiaqi Liu, Xianxu Li, Zhiqin Huang, and Yong Zhang. A power consumption measurement method for large ai-based intelligent computing servers. In *Proceedings of the 2023 5th International Conference on Internet of Things, Automation and Artificial Intelligence*, IoTAAI '23, page 150–155, New York, NY, USA, 2024. Association for Computing Machinery.