NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY POLITEHNICA BUCHAREST

Doctoral School of Electronics, Telecommunications and Information Technology

Decision No. 2 **from** 29-01-2024

REZUMAT TEZA DE DOCTORAT

Ing. Răzvan MIHAI

TRANZACȚII ECONOMICE EFECTUATE CU AJUTORUL TEHNOLOGIE BLOCKCHAIN: ÎNREGISTRAREA DREPTURILOR ȘI OBLIGAȚIILOR ȘI EFECTUAREA PLAȚILOR FINANCIARE RECURENTE

BLOCKCHAIN-ENABLED ECONOMIC TRANSACTIONS: RECURRING FINANCIAL ACCRUAL AND PAYMENTS

THESIS COMMITTEE

Prof. Dr. Ing. Gheorghe BREZEANU National University of Science and Technology Politehnica Bucharest	President
Prof. Dr. Ing. Gheorghe M. Ștefan National University of Science and Technology Politehnica Bucharest	PhD Supervisor
Prof. Dr. Ing. Radu Vasiu Politehnica University of Timisoara	Referee
Conf. Dr. Ana Bobirca Academy of Economic Studies, Bucharest	Referee
Prof. Dr. Ing. Nicolae Goga National University of Science and Technology Politehnica Bucharest	Referee

BUCHAREST 2024

Acknowledgements

Detaliile tehnice din acest document au fost dezvoltate și pregătite pe baza discuțiilor și schimburilor tehnice între membrii Universității Politehnica din București, IEEE și Universitatea California Berkeley. Prin urmare, mulțumirile mele se îndreaptă către Nicu Goga și Viorel Marian de la Politehnica și Gora Datta de la Berkeley; de asemenea, lui Bill Bowman (billabowman@fastmail.fm), prieten și fost partener de afaceri la KPMG România, pentru că a pus întrebări provocatoare și a oferit supraveghere lingvistică. Contribuțiile lui Bogdan Mihai (bogdan.mihai@ieee.org) și Marius Pui (m.pui@kpmg.com), care au lucrat îndeaproape cu Grupul Blockchain al IEEE România (http://dils.pub.ro/blockchain-romania/) pentru suportul lor tehnic, feedback-ul constructiv și spiritul de echipă; și lui Ioana Rizea-Popp (ipopp@kpmg.com) pentru participarea la dezvoltarea inițială a conceptului, brainstorming și oferirea de comentarii financiare pe parcursul întregului proces. Recunoașterea specială se extinde către Omer Faruk (omer.faruk@ieee.org) pentru asistența sa inestimabilă în implementarea specificațiilor în cod, și astfel aducerea prototipului la viață. În final, profesorului meu coordonator, Gheorghe M. Stefan (gheorghe.stefan@upb.ro) de la Universitatea Politehnica din București, pentru contribuția sa la conturarea ideilor și conceptelor din acest document, oferind sprijin necondiționat pe tot parcursul procesului și având răbdare cu mine.

Table of contents

List of figures

Chapter 1

Introducere

1.1 Prezentarea domeniului tezei de doctorat

Tehnologia blockchain a apărut ca o forță transformatoare, cu potențialul de a revoluționa diverse sectoare începând cu introducerea sa în 2008. În ciuda scepticismului inițial, blockchain-ul și-a dovedit capacitatea de a aborda provocările fundamentale din finanțe, economie și contabilitate. Această teză de doctorat explorează potențialul tehnologiei blockchain de a îmbunătăți eficiența și fiabilitatea tranzacțiilor economice, concentrându-se în mod specific pe tranzacțiile recurente guvernate de contracte implicite sau explicite. Prin folosirea unui contract universal bazat pe blockchain, această lucrare investighează modul în care tranzacțiile economice pot fi executate mai eficient și cum rezultatele acestor tranzacții pot fi înregistrate și conciliate transparent între participanți.

Premiza centrală a acestei lucrări este că tranzacțiile economice se bazează pe acorduri contractuale care definesc drepturile și obligațiile părților implicate. Prin prototipul propus bazat pe blockchain, este capturat esențialul tranzacțiilor economice recurente, evidențiind eficacitatea, eficiența și urmărirea aproape în timp real a acestor tranzacții. Blockchain-ul Ethereum este utilizat ca platformă pentru contracte inteligente datorită maturității și adoptării sale răspândite. În mod remarcabil, această cercetare descoperă limitele tehnologiei blockchain actuale legate de plățile recurente automate, oferind înțelegeri valoroase în domenii care necesită îmbunătățiri.

Obiectivul principal al acestei lucrări interdisciplinare este de a investiga cum tehnologia blockchain poate îmbunătăți semnificativ practicile curente în economie, contabilitate și audit. Cercetarea vizează automatizarea și optimizarea tranzacțiilor universale de uz general, concentrându-se în același timp pe aplicația specifică a tranzacțiilor recurente. Prin dezvoltarea unui prototip care automatizează atât aspectele de acumulare, cât și de plată ale tranzacțiilor recurente, această lucrare urmărește îmbunătățirea procesului de înregistrare, consolidarea capacităților de auditare și facilitarea prognozelor de venituri.

Pentru a îndeplini aceste obiective, această lucrare pune accentul pe cercetarea empirică și dezvoltarea unui prototip realist care redă fidel comportamentul tranzacțiilor

economice. Folosind metodologii din domeniile economiei, finanțelor, informaticii și criptografiei, cercetarea utilizează date autogenerate pentru a construi o simulare robustă care surprinde dinamicile intricate ale tranzacțiilor economice recurente. Această abordare permite o înțelegere mai profundă și explorarea modului în care aceste tranzacții sunt înregistrate, depășind abordările tradiționale bazate pe date.

În cele din urmă, această lucrare contribuie la creșterea corpului de cunoștințe privind potențialul tehnologiei blockchain de a revoluționa tranzacțiile economice. Prin evidențierea capacității sale de a optimiza tranzacțiile recurente și de a îmbunătăți diverse aspecte ale ciclului de tranzacții, această lucrare deschide calea pentru progrese suplimentare în integrarea tehnologiei blockchain în practicile economice, contabile și de audit.

În plus, această lucrare își propune să contribuie la standardizarea gestionării tranzacțiilor recurente. Ca rezultat direct al concluziilor și insușirilor derivate din această cercetare, un nou organism de standardizare în cadrul IEEE a fost înființat în iunie 2023 - Grupul de lucru pentru Tranzacții Recurente pe Tehnologiile de Ledger Distribuit (DLTs) (P3228 WG). Corpul de standardizare va lucra pentru definirea celor mai bune practici și a liniilor directoare pentru implementarea soluțiilor bazate pe blockchain în contextul tranzacțiilor recurente, promovând o eficiență și o interoperabilitate mai mari în implementările viitoare.

1.2 Scopul tezei de doctorat

Scopul acestei cercetări este de a investiga cum practicile curente din domeniul economic, contabilitate și audit pot fi îmbunătățite semnificativ și să beneficieze de tehnologia blockchain. Scopul este de a explora provocările și oportunitățile asociate cu integrarea tehnologiei blockchain pentru a automatiza și optimiza tranzacțiile universale de uz general și apoi de a se concentra asupra aplicației mai specifice a tranzacțiilor recurente. Cercetarea își propune să dezvolte un prototip care automatizează tranzacțiile recurente, inclusiv atât partea de angajamente, cât și partea de plată, să îmbunătățească procesul de înregistrare, să consolideze capacitățile de auditare și să faciliteze prognozele de venituri.

1.2.1 Automatizarea contractelor universale folosind tehnologia blockchain.

Un obiectiv semnificativ al acestei cercetări este examinarea automatizării contractelor universale. În timp ce accentul principal este pus pe tranzacțiile recurente din cadrul sistemelor de contabilitate pe bază de acumulare, acest obiectiv își propune să investigheze conceptul mai amplu al automatizării tranzacțiilor economice generale prin aplicarea tehnologiei blockchain. Contractele universale cuprind o gamă largă de tranzacții economice în diverse industrii și contexte.

Prin explorarea automatizării acestor contracte, cercetarea își propune să identifice modele comune, provocări și soluții care pot fi aplicate pentru simplificarea și îmbunătățirea proceselor de gestionare a tranzacțiilor. Acest obiectiv va oferi o înțelegere cuprinzătoare a beneficiilor și limitărilor potențiale ale automatizării contractelor universale folosind tehnologia blockchain. Studiind domeniul mai larg înainte de a intra în detaliile cazului specific al tranzacțiilor recurente, cercetarea își propune să extragă înțelegeri valoroase și să dezvolte o metodologie care poate fi aplicată universal în practicile de gestionare a tranzacțiilor.

1.2.2 Dezvoltarea prototipului pentru tranzacții recurente automate

Principalul obiectiv al acestei cercetări este să dezvolte un prototip care automatizează tranzacțiile recurente pe blockchain. Prototipul va încorpora o metodologie care asigură recunoașterea precisă a drepturilor și obligațiilor pe întregul ciclu de viață al tranzacției. Nucleul prototipului va fi un contract inteligent, care va servi ca motor pentru automatizarea atât a aspectelor de acumulare, cât și a celor de plată ale tranzacțiilor recurente.

1.2.3 Limitari și provocări ale automatizării tranzacțiilor recurente

Principalul obiectiv al acestei cercetări este să dezvolte un prototip care automatizează tranzacțiile recurente pe blockchain. Prototipul va încorpora o metodologie care asigură recunoașterea precisă a drepturilor și obligațiilor pe întregul ciclu de viață al tranzacției. Inima prototipului va fi un contract inteligent, servind ca motor pentru automatizarea atât a aspectelor legate de inregistrarea angajamentelor (drepturi si obligatii), cât și de plată ale tranzacțiilor recurente.

1.2.4 Standardizarea tranzacțiilor și plăților recurente

Pentru a promova interoperabilitatea și fiabilitatea, un obiectiv al acestei cercetări este de a impulsiona standardizarea în domeniul tranzacțiilor și plăților recurente pe tehnologiile de tip ledger distribuit. Prin stabilirea unor linii directoare, protocoale și practici optime, această cercetare își propune să faciliteze gestionarea eficientă și automatizarea tranzacțiilor recurente în diverse industrii și contexte.

1.2.5 Explorarea domeniilor pentru dezvoltare viitoare - Integrarea prototipului cu Învățarea Automată pentru Prognoza Solidității Economice

Integrarea prototipului cu algoritmi de învățare automată reprezintă un alt obiectiv al acestei viitoare cercetări. Prin utilizarea datelor istorice de pe blockchain, cercetarea

își propune să dezvolte un cadru care poate prezice soliditatea economică a afacerilor. Această integrare își propune să permită gestionarea proactivă a riscurilor, luarea deciziilor informate și prevenirea dificultăților financiare neașteptate sau a falimentelor.

În concluzie, obiectivele acestei teze de doctorat gravitează în jurul explorării beneficiilor potențiale ale integrării tehnologiei blockchain cu sistemele de contabilitate pe bază de acumulare pentru tranzacțiile recurente. Prin dezvoltarea unui prototip, abordarea limitărilor, impulsionarea standardizării, această cercetare își propune să deschidă calea pentru automatizarea și eficiența gestionării tranzacțiilor recurente. Concluziile vor contribui la cunoștințele academice, practicile industriale și avansarea eforturilor de standardizare în acest domeniu.

1.3 Conținutul tezei de doctorat

1.3.1 Capitolul 2 - Starea Actuală a Tehnologiei

Acest capitol oferă o prezentare cuprinzătoare a stării actuale a tehnologiei în ceea ce privește gestionarea tranzacțiilor economice folosind tehnologia blockchain. Se examinează diverse soluții existente, cum ar fi Hyperledger, și se explorează cazuri de utilizare în domenii precum finanțe, sănătate, energie, lanțul de aprovizionare, votul și gestionarea identității digitale. Capitolul evidențiază provocările de interoperabilitate, scalabilitate și reglementare în adoptarea blockchain-ului. De asemenea, privește către viitor, imaginând integrarea blockchain-ului cu IA și IoT. Acest capitol pregătește terenul pentru înțelegerea problemelor cu care se confruntă mediul economic actual și modul în care acestea pot fi abordate la nivel general și în cazuri de utilizare specifice.

1.3.2 Capitolul 3 - Contractul Universal pe Blockchain

Acest capitol explorează conceptul de contract universal pe blockchain și potențialul său transformativ. Se discută limitările Bitcoin și apariția contractelor inteligente pe alte blockchains, cum ar fi Ethereum. Tranzacțiile sunt evidențiate ca blocuri de construcție fundamentale ale ecosistemului blockchain. Se explică diferența dintre contabilitatea bazată pe numerar și cea bazată pe acumulare și se subliniază necesitatea de a le lua în considerare ambele în soluțiile blockchain. Sunt discutate cerințele de proiectare, straturile de permisiuni și confidențialitatea tranzacțiilor. Capitolul discută diferite soluții arhitecturale pentru gestionarea contractelor universale și a tranzacțiilor economice folosind blockchain-ul. Se conturează beneficiile blockchain-ului pentru accesul la informații financiare și audituri și se introduc funcțiile de hash pentru autenticitatea contractelor.

1.3.3 Capitolul 4 - Tranzacții Economice Recurente pe Blockchain: Studiu de Caz al Închirierii de Active

Acest capitol se bazează pe conceptele teoretice discutate în Capitolul 3 și explorează un caz mai specific și mai practic al tranzacțiilor economice recurente în cadrul ecosistemului blockchain, concentrându-se explicit asupra închirierii de active ca studiu de caz. Capitolul intră în aspectele teoretice ale tranzacțiilor recurente și a implementării lor practice prin dezvoltarea unui prototip. Acest prototip este o reprezentare tangibilă, demonstrând cum tranzacțiile recurente pot fi înregistrate și gestionate eficient pe blockchain. Oferă o demonstrație cuprinzătoare a întregului ciclu de viață al unei tranzacții de tip contract recurent, includând drepturile și obligațiile tuturor părților implicate în tranzacție. În plus, aspectul plăților al tranzacției este, de asemenea, înregistrat și gestionat folosind tehnologia blockchain.

Capitolul intră în detaliile implementării plăților recurente în cadrul ecosistemului blockchain. Subliniază provocările întâlnite în realizarea plăților recurente automate pe blockchain-ul Ethereum, dezvăluind că protocoalele blockchain existente nu susțin nativ această funcționalitate într-un mod non-custodial. Cu toate acestea, prin investigații și analize riguroase, capitolul propune o soluție sub forma unui standard complet nou de blockchain, proiectat explicit pentru Ethereum. La momentul redactării acestei teze, un astfel de standard a fost generat sub IEEE SA ca rezultat direct al lucrărilor efectuate.

1.3.4 Capitolul 5 - Concluzii

În cele din urmă, Capitolul 5 completează cercetarea privind tranzacțiile economice activabile prin blockchain, concentrându-se explicit pe acumularea financiară recurentă și plățile. Capitolul evidențiază, de asemenea, contribuțiile originale realizate pe parcursul cercetării și conturează perspectivele pentru dezvoltări ulterioare în domeniu.

Cercetarea empirică efectuată în această teză a condus la dezvoltarea unui prototip care automatizează tranzacțiile recurente, îmbunătățește procesul de înregistrare, consolidează capacitățile de auditare și facilitează prognozele de venituri. Acest prototip demonstrează modul în care tehnologia blockchain poate gestiona și înregistra eficient tranzacțiile recurente. Acesta evidențiază potențialul blockchain-ului în asigurarea unei recunoașteri precise a drepturilor și obligațiilor pe întregul ciclu de viață al unei tranzacții.

Cercetarea relevă, de asemenea, o limitare semnificativă privind plățile recurente pe blockchain. Protocoalele blockchain existente nu susțin nativ plățile recurente automate într-un mod non-custodial. Această limitare subliniază necesitatea unei dezvoltări și inovații ulterioare. Pentru a aborda această problemă, un nou grup de lucru, "Recurring Transactions on the Distributed Ledger Technologies (DLTs) Working Group" (P3228 WG), a fost înființat în cadrul Institute of Electrical and Electronics Engineers (IEEE)

ca rezultat direct al acestei cercetări. Acest grup de lucru își propune să dezvolte un standard axat pe tranzacțiile și plățile recurente folosind tehnologia blockchain.

Contribuțiile cercetării sunt categorisite și listate. Metodologia de gestionare a tranzacțiilor economice generale, derivată dintr-un contract universal, este dezvoltată, oferind o acoperire largă și aplicabilitate în diferite industrii.

În concluzie, cercetarea privind tranzacțiile economice activabile prin blockchain a adus contribuții semnificative în domeniu. Prototipul dezvoltat evidențiază potențialul tehnologiei blockchain în automatizarea tranzacțiilor recurente, iar înființarea grupului de lucru P3228 WG subliniază importanța standardizării în acest domeniu. Dezvoltările viitoare vor continua să avanseze integrarea învățării automate, să îmbunătățească stabilitatea și integrarea fiat, să îmbunătățească activarea și controlul contractelor și să abordeze preocupările legate de confidențialitate. Aceste progrese vor continua să transforme și să rafineze gestionarea tranzacțiilor recurente folosind tehnologia blockchain.

Chapter 2

Starea actuala a tehnologiei

ChatGPT

2.1 Analiza Literaturii

O abordare holistică asupra modului în care să includem atât partea de acumulare, cât și partea de plată a tranzacțiilor economice a fost adoptată de R. Mihai în articolul "Contract Universal pe Blockchain" [1]. Autorul susține că practic orice tranzacție economică poate, cu o configurare adecvată, fi plasată pe blockchain. Articolul oferă cadrul general al implementării, lăsând detaliile specifice pentru lucrările viitoare. În acest document, ne construim pe această idee generală și implementăm un caz particular pentru tranzacțiile recurente într-un contract de închiriere.

Un număr de inițiative de cercetare abordează beneficiile potențiale pe care tehnologia blockchain le aduce în lumea financiară. Privind inițiativa MIT zkledger, Auditarea cu păstrarea confidențialității pe ledger distribuit [2], explorează auditarea tranzacțiilor folosind blockchain privat și o dovadă de cunoștințe zero în contextul unei bănci. Această lucrare recunoaște beneficiile blockchain-ului în contextul transferului de fonduri (adică plăților). Astfel, articolul face o pledoarie doar pentru o parte a tranzacției, adică stabilirea în numerar. Alte inițiative s-au axat în mod specific pe modul în care să abordăm plățile recurente; totuși, aceste soluții propuse sunt de natură custodială, ceea ce le face dependente de o parte centrală și nu abordează partea de recunoasterea drepturilor si obligatiilor in cadrul unui tranzactii [3], [4].

2.2 Introducere în Tehnologia Blockchain

2.2.1 Blockchain ca o Tehnologie de uz General

Blockchain a devenit faimos datorită Bitcoin - prima sa aplicație [5]. Tehnologia a atras multă atenție în ultimii ani, demonstrându-și un potențial uriaș pentru o gamă largă de

aplicații care se întind mult dincolo de criptomonede. Blockchain îmbină componente din multe discipline; concepte din economie, criptografie, informatică - atât hardware, cât și software; de asemenea, din matematică (de exemplu, teoria grafurilor și teoria probabilităților); astfel, înțelegerea modului în care funcționează tehnologia blockchain și implicațiile sale actuale și viitoare este departe de a fi o sarcină ușoară. Pe lângă furnizarea unei imagini de ultimă generație a Blockchain-ului așa cum este acum, acest raport creează un pod între spațiile economic și tehnic pentru a facilita înțelegerea mai bună a tehnologiei Blockchain și a aplicațiilor sale viitoare.

Tehnologia blockchain a fost definită ca o tehnologie de uz general [6]. Tehnologiile de uz general generează cea mai mare creștere economică pe termen lung. Exemplele includ motorul cu abur, utilizarea electricității, internetul. Ori de câte ori apare o astfel de invenție, nu este neobișnuit ca mulți ani să treacă înainte ca beneficiile complete să fie realizate. Ceea ce le face "generale" este că pot fi aplicate în mai mult de un segment industrial; de aceea poate dura ceva timp până să se difuzeze în economie.

Practica contabilității tradiționale este o abordare de dublă înregistrare în care o tranzacție financiară este înregistrată în cărțile contabile ale ambelor părți implicate în tranzacție. Tehnologia blockchain a fost tot mai recunoscută ca o oportunitate de a permite contabilitatea cu triplă înregistrare, adică înregistrarea unei tranzacții financiare pe un sistem separat de sistemele individuale ale părților participante [7].

Proof of Work

Proof of Work("PoW"), the most notorious algorithm, is the consensus algorithm used by Bitcoin and Ethereum blockchain. Under the PoW consensus, miners (i.e. nodes) are required to solve a complex mathematical problem that will allow them to attach the block to the blockchain. It is essential to understand that solving this complex mathematical problem does not bring knowledge by itself, such as finding a solution to a complex known mathematical problem. It is simply similar to solving a puzzle which allows the miners to participate in the blockchain lottery. Solving the puzzle requires computing power, which in turns translates into energy consumption. This is they price of the “lottery ticket” to participate in the “blockchain game”. The concept of proof of work was first introduced by Dwork et al. in 2005 when it was called also called "proof of computational effort" [8]. The concept had several applications, such as avoiding e-mail spamming, before being made notorious in the bitcoin context.

Proof of Stake

Protocolul de consens prin dovada de participare rezolvă problema ambiguității prin alegerea următorului câștigător al blocului folosind un sistem de loterie. PoS funcționează cu o formă de protocol de consens bizantin în care mai multe noduri (adică validatori) verifică și sunt de acord cu blocul propus. PoS a fost dezvoltat parțial ca o necesitate

pentru a rezolva consumul de energie necesar pentru menținerea și securizarea unui blockchain.

Validatorii plasează o parte din tokenurile lor într-un cont de garanție ca și colateral - "Dovada de Participare". Dacă un validator ar adăuga un bloc invalid la blockchain, ar risca să piardă acel colateral. Protocoalele PoS diferă în modul în care sunt aleși validatorii pentru fiecare rundă. În unele cazuri, grupul de validatori este static, în timp ce în altele, validatorii se rotesc între runde de loterie.

În mod obișnuit, șansa de a câștiga o rundă de loterie depinde de participația unui validator în sistem. Astfel, de exemplu, un validator cu o participație de 10% va putea confirma aproximativ 10% din blocuri. Acest sistem asemănător cu o loterie are alte caracteristici, cum ar fi de exemplu, de cât timp sunt plasate participațiile. Aceste caracteristici specifice sunt menite să rezolve problema ambiguității și să securizeze în același timp blockchain-ul.

Contracte Inteligente

Banii digitali există de ceva vreme acum. Astăzi, majoritatea interacțiunilor cu băncile sunt digitale. Care este, deci, inovația introdusă de criptomonedele precum Bitcoin sau Ether? Provocarea este că banii nu erau programabili. Toate activele digitale create pe rețeaua blockchain sunt programabile încă de la început. Aici intervin contractele inteligente.

Un contract inteligent este, în esență, un contract care acționează în anumite moduri definite de termenii contractului. Contractele inteligente încep cu o criptomonedă, iar apoi pot fi adăugate straturi suplimentare. De exemplu, se poate construi un contract simplu de închiriere în care chiriașul plătește chirie automat proprietarului la sfârșitul perioadei specificate, cu condiția să fie îndeplinite anumite condiții. Aceste condiții sunt în esență instrucțiuni programabile care reacționează la situații din mediu sau la evenimente noi care apar.

2.3 Business Applications of Blockchain

2.3.1 Platforme Blockchain pentru Întreprinderi

Tehnologia blockchain a atras atenția lumii întreprinderilor, iar ca urmare, o serie de platforme blockchain, în general private și cu permisiuni, au fost dezvoltate. Această secțiune își propune să acopere cele mai cunoscute și promițătoare platforme blockchain la nivel de întreprindere până la data redactării. În timp ce blockchain-ul privat permite doar anumitor participanți să intre în rețea, blockchain-urile cu permisiuni se situează undeva între blockchain-ul public și cel privat. Într-un blockchain cu permisiuni, participanții sunt autorizați să se alăture rețelei după verificarea identității lor; participanții într-un blockchain cu permisiune au voie să efectueze doar anumite activități

în blockchain [9]. De exemplu, un participant poate fi autorizat să citească, dar nu și să adauge în blockchain.

2.3.2 Use Cases and Industries

Sectorul financiar

Ripple este un exemplu care ilustrează cum un concept de blockchain s-a dezvoltat dintr-o aplicație de criptomonedă, inițial numită OpenCoin, într-un protocol blockchain adoptat de un număr semnificativ de instituții financiare, în special bănci. Puternic influențat de nevoile specifice ale băncilor și instituțiilor financiare, punctul principal de vânzare al Ripple este viteza executării tranzacțiilor în comparație cu alte soluții blockchain existente, făcându-l astfel o alternativă la remiterile bancare folosind protocolul tradițional SWIFT. Legat de, dar distinct de protocolul său blockchain, Ripple are propria criptomonedă (adică XRP), care tinde să fluctueze între poziția a treia și a patra după Bitcoin și Ethereum în ceea ce privește capitalizarea de piață (adică 8,7 miliarde de dolari, la data acestui raport).

Sectorul sănătății

Asigurarea integrității și accesibilității înregistrărilor medicale este crucială pentru buna funcționare a unui sistem de sănătate. O provocare critică cu înregistrările medicale este confidențialitatea datelor. Este important de remarcat că nu există o opoziție între confidențialitate și blockchain. Confidențialitatea datelor este o opțiune în blockchain; nu este o restricție. Medicalchain stochează înregistrările medicale pe blockchain, dar permite accesul cu autorizare din partea utilizatorului prin intermediul telefonului mobil. Alte organizații remarcabile care exploatează potențialul blockchainului în spațiul sănătății includ MedRec al MIT și Spitalul Universitar de Medicină Taipei.

Energie

Sectorul energetic oferă un potențial considerabil pentru aplicațiile bazate pe blockchain. Cu toate acestea, companiile din acest sector s-au dovedit a fi adoptatori lenti ai tehnologiei blockchain în comparație cu alte industrii. Domeniile semnificative care ar putea beneficia de soluțiile blockchain includ tranzacționarea energiei, generarea descentralizată, gestionarea rețelei și măsurarea inteligentă. Una dintre primele implementări ale unei soluții experimentale de blockchain a avut loc în 2018 când Transactive Grid, în parteneriat cu LO3 Energy, Consensus, Siemens și Centrica, au creat o platformă de tranzacționare a energiei peer-to-peer bazată pe blockchain. În esență, consumatorii pot vinde energia lor excedentară direct vecinilor lor folosind un contract inteligent bazat pe Ethereum.

Votul

Blockchain-ul are potențialul de a îmbunătăți semnificativ procesul de vot prin adăugarea nivelului necesar de securitate la votul online. Caracteristicile intrinseci ale blockchain-ului ajută la eliminarea fraudelor și pot crește participarea votanților la alegeri. Un astfel de experiment a fost deja efectuat în noiembrie 2018, în Virginia de Vest, SUA, unde cetățenilor aflați în afara SUA li s-a oferit opțiunea de a vota online folosind o aplicație bazată pe blockchain numită Voatz. Protocolul blockchain, argumentat, asigură transparența în procesul electoral, reducând personalul necesar pentru desfășurarea unei alegeri. Un studiu MIT [10], publicat în februarie 2020, a identificat vulnerabilități în aplicație, ceea ce a determinat cercetătorii să-și îndrume descoperirile către Departamentul pentru Securitate Internă. Principalele vulnerabilități găsite s-au axat pe posibilitatea unui adversar de a deduce opțiunea de vot a utilizatorului sau coruperea pistei de auditare. Blockchain-ul, completat cu Inteligența Artificială, are potențialul de a schimba dramatic modul în care este guvernată societatea noastră, începând cu votul, dar extinzându-se la o serie de aspecte complexe și dinamice cu care se confruntă lumea astăzi [11].

Managementul identității digitale

Managementul identității este un concept care se pretează ușor la aplicații bazate pe blockchain. Oferă un excelent exemplu în care confidențialitatea datelor devine o opțiune într-o aplicație blockchain, spre deosebire de o restricție. Există numeroase situații în care este necesar un ID pentru a permite accesul într-o clădire, de exemplu. Într-o situație ca aceasta, informațiile de permisiune ar fi suficiente pentru a permite accesul, spre deosebire de detaliile complete de identitate cum ar fi numele, adresa sau data nașterii. Aplicații cunoscute bazate pe blockchain includ uPort, care se concentrează pe crearea unei identități digitale care în cele din urmă reprezintă o persoană sau o organizație, permițându-le să facă declarații despre cine sunt. Aplicația încarcă informațiile într-un depozit de date decentralizat independent, menținându-și adresa pe blockchain-ul Ethereum. Este necesară o distincție importantă între locul în care datele sunt stocate (adică stocarea decentralizată a datelor) și adresa blockchain-ului, care oferă validitatea datelor stocate. Sovrin este încă o altă aplicație bazată pe blockchain pentru managementul identității digitale. Spre deosebire de uPort, proiectul Sovrin a construit un blockchain personalizat special proiectat pentru acest scop, care are potențialul de a escalada mai eficient la nivel global decât aplicațiile bazate pe Ethereum.

2.4 Provocări în Adoptarea Tehnologiei Blockchain

Există mai multe provocări în calea adoptării și implementării tehnologiei blockchain. Cele mai multe dintre aceste obstacole sunt înerente în orice tranziție către o nouă etapă

tehnologică, în timp ce altele sunt specifice tehnologiei în sine. Principalele obstacole sunt:

2.4.1 Interoperabilitatea

Există o lipsă de standarde pentru a asigura interoperabilitatea între diversele platforme blockchain, dat fiind stadiul incipient al dezvoltării. Unul dintre cele mai critice aspecte care necesită atenție specială sunt protocoalele privind pierderea și furtul cheilor [12]. Această provocare este, totuși, pe cale de a fi abordată odată cu înființarea în 2016 a Organizației Internaționale pentru Standardizare a Tehnologiilor Blockchain și a Ledgerelor Distribuite. Mai mult, există o provocare la fel de mare dată de interoperabilitatea între platformele blockchain și sistemele de informații moștenite.

2.4.2 Scalability

Scalability has been recognized from the very beginning as one of the biggest concerns of blockchain implementations. In the Ethereum Yellow Paper [13], Woods, makes a clear reference that given the generalized state transition function of the blockchain, it is difficult to partition and parallelize to apply the divide-and-conquer strategy. On the other hand, Croman et. al, proposed in 2016 an approach to dividing blockchains into various abstract layers called planes, with each plane being responsible for performing specific functions: network plane, consensus plane, storage plane, view plane, and side plane [14]. According to their position paper – On scaling decentralized blockchains – the authors propose that this abstraction allows tackling the inherent limitations of blockchains at each such plane individually in a structured manner.

2.4.3 Provocări legislative

Astăzi, mediul legislativ nu este la fel de prietenos cu criptomonedele cum era cu Internetul. Trebuie să avem în vedere însă că criptomonedele sunt doar o aplicație a tehnologiei blockchain. Este esențial să facem această separare și să nu generalizăm atunci când abordăm subiectul reglementării. Regulatorii privesc criptomonedele cu precauție din două motive fundamentale. În primul rând, au existat o serie de înșelăciuni în domeniul criptomonedelor [15], dintre care Mt. Gox este cel mai notoriu exemplu în spațiul Bitcoin; prin urmare, reglementatorii sunt preocupati în mod justificat. În al doilea rând, există percepția că aspectul decentralizării tehnologiei blockchain pune sub semnul întrebării chiar puterea statului de a crea monedă sau puterea reglementatorilor de a reglementa.

2.5 Viitorul Tehnologiei Blockchain

Una dintre cele mai interesante dezvoltări de urmărit este modul în care tehnologia blockchain va interacționa cu alte tehnologii disruptive cum ar fi inteligența artificială (AI) și Internetul Lucrurilor (IoT). Blockchain-ul a fost tot mai recunoscut ca o tehnologie de uz general. Așa cum s-a discutat anterior în acest raport, una dintre caracteristicile cheie ale GPT este că catalizează inovația în tehnologiile complementare. În același timp, inteligența artificială și învățarea automată au avut o redescoperire impresionantă în ultimii ani, de când cercetarea în acest domeniu a început în anii 1950. Combinarea blockchain-ului și a inteligenței artificiale are potențialul de a schimba radical o serie de verticalizări industriale importante, inclusiv profesia contabilă și de audit [16].

Au apărut mai multe soluții care propun să rezolve, de exemplu, confirmarea tranzacțiilor financiare cu ajutorul blockchain-ului și să analizeze acele tranzacții și să vină cu un mecanism de diagnostic potrivit care va ajuta la luarea unei decizii financiare mai eficiente cu suportul Inteligenței Artificiale [17].

Comisia Europeană a creat Observatorul și Forumul Blockchain al UE pentru a încuraja angajamentul transfrontalier al regiunii cu tehnologia și diferiții săi stakeholderi. UE prevede că blockchain-ul și AI-ul ar putea ajuta, de asemenea, la securizarea platformelor de servicii financiare bazate pe blockchain în procesul de combatere a spălării de bani (AML) prin urmărirea tranzacțiilor și detectarea riscurilor de fraudă [18].

Amazon merge înainte pe această linie de a combina blockchain-ul, inteligența artificială și IoT-ul. În plus față de Serviciile lor Blockchain AWS, compania a dezvoltat platforma AWS IoT, o platformă bazată pe cloud care permite crearea și implementarea de modele în cloud, care rulează, argumentat, de două ori mai rapid decât alternativele lor convenționale [19].

Chapter 3

Contract Universal pe Blockchain

În ciuda faptului că este numită de sceptici o soluție în căutare de problemă, tehnologia are potențialul de a aborda provocări financiare, economice și contabile fundamentale. La baza fiecărei tranzacții economice există un contract implicit sau explicit care stipulează drepturile și obligațiile părților implicate în tranzacție. Plecând de la această înțelegere fundamentală, acest capitol examinează cum pot fi efectuate tranzacțiile economice mai eficient și mai eficace, bazate pe un contract universal pe blockchain; și examinează cum pot fi înregistrate și conciliate mai fiabil și mai transparent tranzacțiile rezultate între participanții economici.

3.1 Introducere

Blockchains-ul propuse recent a dat naștere la dezvoltarea unei game mai largi de aplicații și a adus mai multe algoritme de consens care sunt diferite de Proof of Work-ul inițial cunoscut pentru a fi intens din punct de vedere energetic. Cel mai cunoscut blockchain care permite implementarea de contracte inteligente este Ethereum, care în data acestei lucrări trece de la un consens Proof of Work la un Proof of Stake [20].

În ciuda hype-ului inițial în aplicațiile contractelor inteligente, "contractele inteligente" s-au dovedit a nu fi atât de inteligente în realitate [21]. Dimpotrivă, contractele inteligente permit simpla executare automată dacă un set dat de condiții sunt îndeplinite, și prin urmare pot fi considerate "contracte proaste".

3.2 Baza Contabilității: Principiul Contabilitatii de Angajamente vs. Principiul Contabilitatii pe baza de Numerar

Diferența principală între contabilitatea bazată pe cash și cea bazată pe principiul de acreștere este momentul înregistrării veniturilor și cheltuielilor în înregistrările contabile.

În contabilitatea bazată pe cash, veniturile și cheltuielile sunt înregistrate atunci când are loc schimbul de bani între cele două părți ale unei tranzacții. În contrast, într-o contabilitate bazată pe principiul de acreștere, veniturile sunt înregistrate atunci când sunt câștigate, indiferent dacă au fost colectate, adică încasate; iar cheltuielile sunt înregistrate atunci când există o presupusă obligație de a plăti cheltuiala respectivă, dar nu neapărat atunci când cheltuiala este plătită.

Lucrarea MIT zkledger - Auditarea cu păstrarea confidențialității pe un registru distribuit [2] investighează auditarea tranzacțiilor folosind blockchain-ul privat și dovada zero de cunoștințe în contextul bancar. Această lucrare recunoaște importanța auditului în timp real, dar se concentrează strict pe un context bancar în care fondurile sunt transferate de la expeditor la destinatar. În esență, lucrarea propune o soluție doar pentru prima parte a ecuației, adică tranzacțiile cu numerar, și nu reușește să abordeze partea de acreștere a unei tranzacții economice.

3.3 Specificatii de design

Ne așteptăm la crearea unui contract universal care poate încapsula și parametriza toate detaliile unui contract comercial tipic dincolo de sfera unui simplu contract de împrumut. Toate detaliile unui astfel de contract universal vor putea fi stocate într-un format care poate fi citit de oameni, dar și citit, interpretat și executat de o mașină. Formatul JSON (JavaScript Object Notation) este un candidat potrivit pentru a reprezenta și transmite date generice deoarece implică un număr limitat de tipuri de date: șiruri de caractere, numere, valori Boolean, liste, obiecte și nul. Aceste tipuri de date sunt reprezentate în toate limbajele de programare principale și pot fi utilizate de API-uri și baze de date.

3.4 Hashingul contractelor comerciale

"Hashingul" oferă o modalitate fiabilă de a dovedi că un anumit contract comercial a fost semnat în mod unic de părțile implicate în acea tranzacție. Un contract comercial, fie sub forma unui contract inteligent sau a unui contract tradițional în formă digitală, poate fi salvat într-o bază de date distribuită sau într-o resursă cloud, în timp ce hash-ul contractului este pus pe blockchain. În acest fel, autenticitatea contractului este verificată fără dubii de către orice parte interesată.

3.5 Tranzacții

Tranzacțiile sunt componentele de bază cele mai fundamentale ale blockchain-ului. Faptul că blockchain-ul a găsit "utilitatea" sa în spațiul financiar poate crea confuzii în ceea ce privește ce este o tranzacție, în contextul blockchain-ului. Termenul de tranzacție

în contextul blockchain-ului include definiția unei tranzacții din punct de vedere financiar. Într-un sens mai holistic, însă, înseamnă a face tranzacții, adică transmiterea unui set de informații de la punctul A (expeditor) la punctul

Chapter 4

Recurring Economic Transactions on Blockchain: Asset Rental Case Study

Notă: Conținutul acestui capitol se bazează fundamental pe lucrarea intitulată "Tranzacții Economice pe Baza Blockchain-ului: Acumulări Financiare și Plăți Recurente," care a fost publicată în cadrul conferinței IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond din 2022 [22].

Tranzacțiile economice se bazează pe contracte implicite sau explicite care stabilesc drepturile și obligațiile părților implicate în tranzacții. Tehnologia blockchain poate aborda provocări financiare, economice și contabile fundamentale. Propunem un prototip bazat pe blockchain capabil să surprindă esența tranzacțiilor economice recurente. În acest scop, am elaborat un contract de închiriere de active pentru a arăta cum sunt înregistrate și urmărite tranzacțiile economice mai eficient, mai eficace și în timp aproape real. Folosim blockchain-ul Ethereum ca platformă de smart contract-uri cea mai evoluată și utilizată pe scară largă. Prezentăm o descoperire semnificativă legată de limitele actuale ale tehnologiei blockchain pentru a efectua plăți recurente automate. Arătăm cum prototipul poate fi extins pentru o serie de tranzacții recurente.

4.1 Introducere

Potențialul tehnologiei blockchain depășește cu mult aplicațiile legate de criptomonede. Unii susțin că blockchain-ul este o tehnologie contabilă, având potențialul de a optimiza atât executarea tranzacțiilor economice, cât și modul în care aceste tranzacții sunt înregistrate și verificate [23].

Tranzacțiile sunt elementele de bază ale blockchain-ului. Termenul de "tranzacție" în contextul blockchain-ului include definiția sa din punct de vedere financiar; totuși, într-un sens mai abstract, a efectua o tranzacție înseamnă transmiterea unui set de informații de la punctul A (expeditor) la punctul B (destinatar). Astfel, o tranzacție este similară cu

transmiterea și primirea unui înregistrări, care poate include, dar nu se limitează la, o reglementare financiară [1].

Diferența dintre Accrual și Plăți. Contabilitatea pe bază de acumulare este cea mai utilizată metodă de contabilitate, care necesită înregistrarea veniturilor atunci când sunt câștigate și a cheltuielilor atunci când sunt înregistrate, indiferent de momentul încasării sau plății. În contrast, contabilitatea pe bază de numerar înregistrează veniturile și cheltuielile atunci când sunt achitate în numerar. Diferența fundamentală dintre aceste două metode adesea generează confuzie pentru cei care nu sunt familiarizați cu principiile și practicile contabile.

Rolul verificatorului independent, adică al auditorului, este probabil să se schimbe semnificativ de la munca manuală efectuată în prezent pentru verificarea detaliilor din documente, la auditarea smart contractelor care stau la baza tranzacțiilor economice pe blockchain [17]. Acest articol documentează o implementare specifică a unui prototip privind modul în care acest lucru poate fi realizat în practică. În acest sens, folosim un exemplu de închiriere a activelor în care clientul (adică chiriașul) recunoaște obligația de plată și efectuează plăți lunare către furnizor (adică locator).

4.2 Arhitectura Prototipului

4.2.1 Specificații

Un contract între doi jucători economici conține mai multe termeni și condiții răspândite uneori pe un număr intimidant de pagini de text. Cu toate acestea, în cele mai multe cazuri, numărul critic de parametri este destul de limitat. Arhitectura prototipului blockchain este prezentată în Fig. 4.1. Documentația în curs de desfășurare, codul și rezultatele testelor pot fi găsite la: https://github.com/UniversalContractOnBlockchain/Recurring-Economic-Transactions. Parametrii fundamentali fără de care un contract nu poate exista sunt următorii:

Furnizor. ID-ul unic al unui furnizor este utilizat în mod tipic aici, de exemplu, *numele* companiei, *numărul* de înregistrare comercială/fiscală și *adresa* sediului înregistrat. Cu toate acestea, elementul esențial într-un mediu blockchain este *adresa publică* - numărul unic folosit pentru a înregistra și a soluționa tranzacțiile.

Client. Informațiile vor reflecta parametrii descriși mai sus în cazul furnizorului. În ambele cazuri (furnizor și client), dacă este vorba de o persoană fizică în loc de o companie, informațiile necesare sunt: *numele complet* al persoanei fizice, *numărul* de identificare și *adresa* conform documentelor de identitate, precum și *adresa publică*.

Durată. Durata pentru care contractul este valabil de la și până la. Trebuie să știm cât timp contractul își va menține valabilitatea și să efectuăm plățile corespunzător. Acest lucru înseamnă blocarea unor plăți dacă nu sunt datorate sau adoptarea unei alte abordări dacă sunt întârziate.

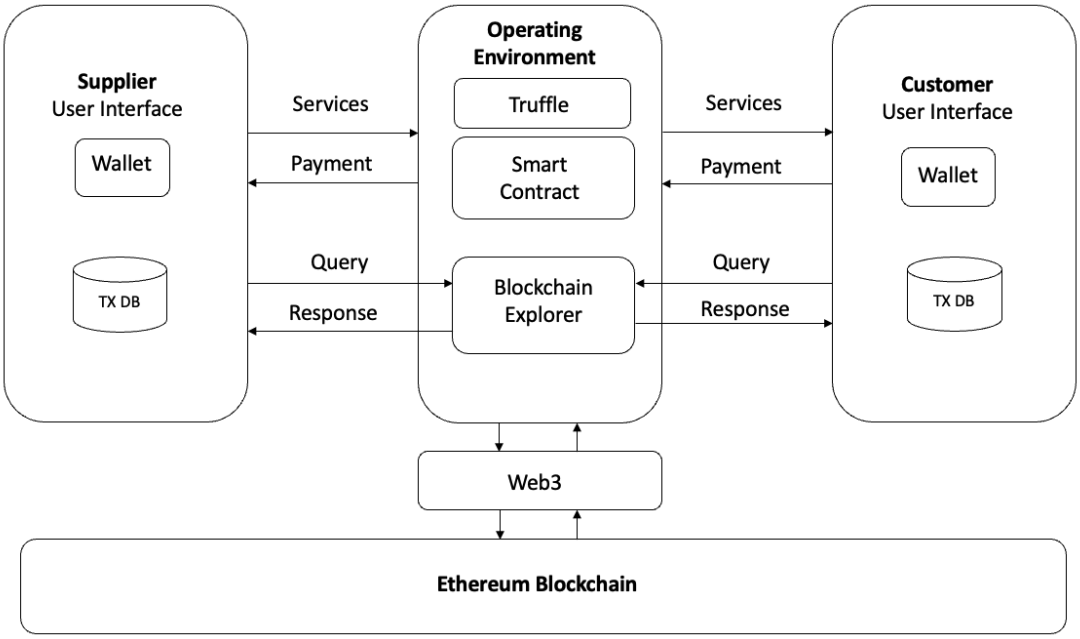

Fig. 4.1 Prezentare generală a arhitecturii prototipului

Sumă. Acest parametru este crucial pentru ca contractul inteligent să calculeze plata totală, precum și pentru a ști cât de mult sau mai degrabă câte tokenuri să perceapă în fiecare lună recurentă. În loc să facem ca furnizorul să introducă întreaga sumă pe durata contractului (durata contractului x plata lunară), permitem introducerea plății lunare și calcularea restului când prezentăm acea informație utilizatorului final.

4.2.2 Interfața Utilizatorului

Interacțiunea utilizatorului cu sistemul este descrisă în Fig. 4.2, care surprinde funcționalitățile fundamentale ale prototipului propus. Pentru a reduce încărcătura sistemului și a simplifica inițierea contractului, prototipul este proiectat în așa fel încât doar furnizorul poate iniția contractul. Utilizatorii sistemului pot fi fie furnizori, fie clienți în orice moment. Configurația implicită a prototipului este că utilizatorii pot vedea informațiile contractuale ale altora în măsura în care fac parte din acel contract specific, cu excepția cazului în care cheia publică a unui anumit furnizor sau client este deja cunoscută. Cu toate acestea, așa cum este descris în Secțiunea **??**, confidențialitatea este o opțiune și nu o constrângere, și prin urmare aceste caracteristici pot fi ajustate ulterior pentru a ține cont de nevoile particulare ale părților implicate în tranzacții. Funcționalitățile de bază ale prototipului sunt enumerate aici:

- Realizarea unui contract nou (Doar ca Furnizor)
  - Adresa publică a clientului
  - Durata contractului

  - Suma de plată lunară

- Vizualizarea contractelor (Furnizor și Client)
- Acceptarea termenilor contractului (Doar ca Client)
- Efectuarea plății pe contract (Doar ca Client)
- Inspectarea istoricului tranzacțiilor pe Explorerul Blockchain (Furnizor și Client)

Este important de remarcat că atunci când utilizatorul semnează o tranzacție, semnătura digitală este aplicată pe hash-ul tranzacției. În mod specific, pe Ethereum, utilizatorul semnează hash-ul Keccak-256 al datelor tranzacției serializate RLP [24].

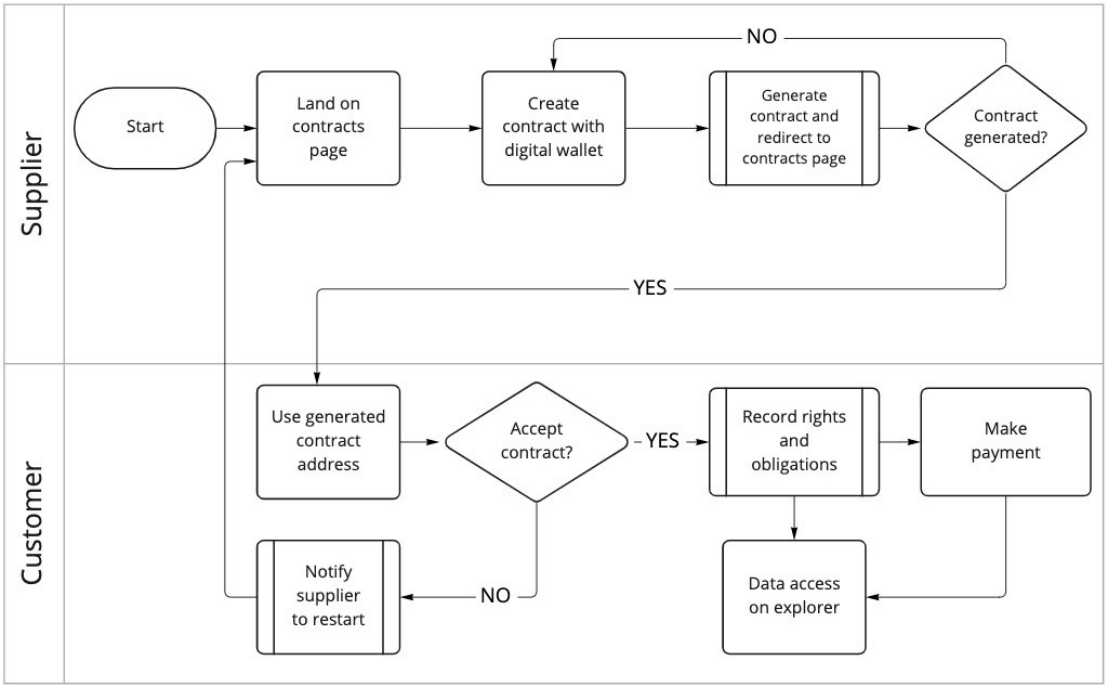

Fig. 4.2 Fluxul Interfeței Utilizator

4.2.3 Logica Smart Contractului

Metodele existente de creare a unui smart contract nu sunt optime pentru cerințele specifice ale tipului de tranzacții prevăzute. Este necesară informație suplimentară, cum ar fi suma plătită către contract. Chiar dacă este posibil să folosim modalitatea convențională de a accesa instanța unei tranzacții specifice și de a recupera detaliile sumei, aceasta este o sarcină dificilă. Prin urmare, am construit o structură de tip date personalizată ("struct History") care salvează eficient datele necesare.

4.2.4 Interacțiuni ale Modulelor

O reprezentare vizuală a modulelor software ale sistemului și interacțiunile lor este prezentată în Fig. 4.3, unde modulele sunt ilustrate sub formă de cutii și interconexiunile lor sunt reprezentate ca săgeți. Diagrama oferă o perspectivă asupra arhitecturii sistemului din perspectiva modulelor software implicate, comportamentul acestora și interacțiunile lor.

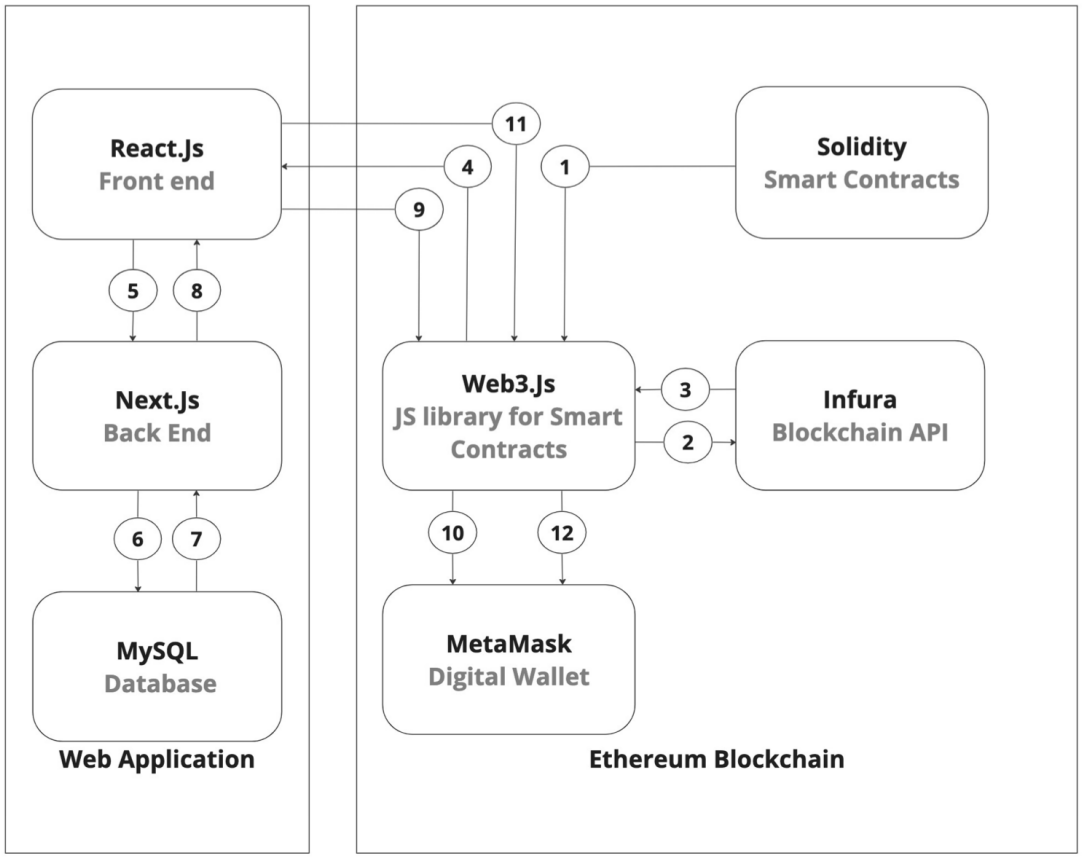

Fig. 4.3 Interacțiuni ale Modulelor

4.2.5 Interacțiuni ale Utilizatorilor

Această subsecțiune servește ca un ghid comprehensiv pentru utilizatori, detaliind pașii esențiali necesari pentru a interacționa cu un prototip de blockchain proiectat pentru a simplifica tranzacțiile și plățile recurente. Creșterea popularității tehnologiei blockchain a deschis noi căi pentru îmbunătățirea eficienței, transparenței și securității în sistemele financiare. Prin valorificarea naturii decentralizate a blockchain-ului, acest prototip își propune să simplifice procesul de tranzacții recurente, eliminând necesitatea intermediarilor și minimizând frecarea tranzacțională. Este prezentat un contur al pașilor secvențiali implicați pentru a ilustra accesarea, configurarea unui cont, gestionarea tranzacțiilor recurente și asigurarea înregistrării și plăților securizate și fără probleme prin intermediul

prototipului blockchain. Pentru o demonstrație vizuală a modului în care funcționează prototipul de blockchain pentru tranzacții și plăți recurente, o demonstrație video este disponibilă la *www.recurringtransactions.xyz*.

4.3 Automatizarea Plăților Recurente

Descoperire Semnificativă. Am descoperit că plățile recurente automate nu sunt acceptate nativ într-un mod ne-custodial de către blockchain-ul Ethereum. De fapt, fiecare tranzacție cu tokenuri trebuie semnată manual în momentul transferului. În mod crucial, incapacitatea de a efectua plăți recurente nu este o problemă specifică Ethereum-ului. Cele mai populare protocoale blockchain [25] nu susțin plățile recurente automate la date prestabilite, deoarece participanții la tranzacție trebuie să aibă control asupra cheii private în orice moment.

Am investigat scenariul în care clientul furnizează cheia privată într-o bază de date criptată, similar modului în care sunt stocate parolele. Am ajuns la concluzia că aceasta este o opțiune inadecvată deoarece este vulnerabilă la hacking. Există diverse soluții în curs de dezvoltare; totuși, acestea sunt fie de natură custodială (adică centralizată), fie nu sunt legate de partea de acumulare a tranzacției [3, 4].

Nou Standard Blockchain. Am ajuns în cele din urmă la concluzia că cea mai bună soluție pentru a rezolva problema identificată, asigurând în același timp un mediu ne-custodial și conectând plata recurentă la partea de acumulare a tranzacției asociate, este să dezvoltăm un standard complet nou specific blockchain-ului Ethereum.

Chapter 5

Concluzii

Am propus un design de prototip bazat pe blockchain pentru a captura esența economică a tranzacțiilor recurente între două părți. Pentru implementare, am ales blockchain-ul Ethereum ca platformă de contracte inteligente cea mai matură și larg utilizată. Cazul specific al implementării noastre de prototip se învârte în jurul unui contract de închiriere cu plăți fixe și regulate.

Cu toate acestea, soluția poate fi extinsă virtual la orice tip de tranzacție recurentă, deoarece tranzacțiile recurente se întind mult dincolo de cazul de utilizare specific prezentat în acest articol, adică un acord privind un activ închiriat. Alte tipuri de tranzacții recurente, cum ar fi rambursările de împrumut cu rate lunare egale sau serviciile bazate pe abonament, de exemplu, abonamentele medicale, sunt bune candidați pentru a fi automate și urmărite folosind soluția propusă. Salariile și impozitele și sarcinile lor asociate sunt în general fixe și recurente, făcându-le încă un alt caz de utilizare potrivit pentru aplicația prototipului propus.

5.1 Rezultate obținute

Am demonstrat potențialul tehnologiei blockchain de a completa și în cele din urmă înlocui modul tradițional de păstrare a contabilității. În Secțiunea 4.3, prezentăm o ***descoperire semnificativă*** referitoare la ***limitarea*** soluțiilor blockchain actuale în ceea ce privește realizarea ***plăților automate recurente***. Această descoperire semnificativă solicită elaborarea unui nou standard blockchain pentru a permite realizarea plăților recurente într-un mod non-custodial și pentru a conecta aceste plăți la partea subiacentă de acumulare a tranzacției economice.

Ca rezultat direct al acestei constatări, înființarea "Grupului de lucru pentru Tranzacții Recurente pe Tehnologiile Ledgerului Distribuit (DLTs)" (P3228 WG) în cadrul Institutului de Inginerie Electrică și Electronică (IEEE) evidențiază importanța cercetării în îmbunătățirea și orientarea managementului tranzacțiilor recurente folosind tehnologia blockchain.

În concluzie, cercetarea empirică, concentrându-se pe conceptele de contabilitate a angajamentelor și tehnologia blockchain, a condus la crearea unui prototip care automatizează eficient tranzacțiile recurente, îmbunătățește procesul de înregistrare, sporește capacitățile de auditare și facilitează prognozele de venituri. Prototipul a evidențiat potențialul blockchain-ului în asigurarea recunoașterii exacte a drepturilor și obligațiilor pe tot parcursul întregului ciclu de viață al tranzacției. Cu toate acestea, limitarea referitoare la plățile recurente evidențiază necesitatea unor dezvoltări ulterioare. Înființarea "Grupului de lucru pentru Tranzacții Recurente pe Tehnologiile Ledgerului Distribuit (DLTs)" (P3228 WG) (https://opensource.ieee.org/oscom/official-project-requests/-/issues/15) subliniază importanța crucială a cercetării în avansarea managementului tranzacțiilor recurente folosind tehnologia blockchain.

5.2 Contribuții originale

5.2.1 Avansarea Managementului Tranzacțiilor Economice: O Metodologie pentru Contracte Universale

În această parte a cercetării, accentul se pune pe dezvoltarea unei metodologii pentru gestionarea tranzacțiilor economice generale, cu accent pe modul în care tranzacțiile economice izvorăsc dintr-un contract universal. Lucrarea s-a concentrat pe dezvoltarea metodologiei, care poate fi aplicată în diferite industrii și contexte. Implică un domeniu de aplicare mai larg, cuprinzând tranzacțiile economice în ansamblul lor.

5.2.2 Explorarea Dinamicii Tranzacțiilor Economice Recurente: Metodologie, Provocări și Soluții

Această lucrare evidențiază în mod specific contribuția legată de tranzacțiile economice rec

urente. Accentuează explorarea în profunzime a complexităților și provocărilor asociate cu gestionarea tranzacțiilor recurente în cadrul sistemului de contabilitate a angajamentelor. Această lucrare își îndreaptă atenția către tranzacțiile recurente și indică scopul cercetării de a identifica soluții și perspective adaptate acestei subseturi specifice de tranzacții.

5.2.3 Dezvoltarea unui Prototip pentru Tranzacții Recurente Automate pe Blockchain-ul Ethereum

În plus față de contribuțiile menționate anterior, o a treia contribuție semnificativă este dezvoltarea unui prototip care automatizează tranzacțiile recurente pe blockchain-

ul Ethereum. Acest prototip integrează metodologia dezvoltată anterior, oferind o implementare practică a constatărilor cercetării.

Dezvoltarea prototipului a implicat crearea unor specificații detaliate. La baza acestor specificații se află contractul inteligent, care servește ca motor pentru automatizarea atât a aspectelor de acumulare, cât și de plată ale tranzacțiilor recurente. Prin valorificarea capacităților blockchain-ului Ethereum, prototipul asigură acuratețea și fiabilitatea înregistrării tranzacțiilor, cuprinzând întregul ciclu de viață al tranzacției.

5.2.4 Revelarea Limitărilor și Îmbunătățirilor în Automatizarea Tranzacțiilor Recurente pe Blockchain

Ca parte a implementării și testării prototipului, apare o a patra contribuție semnificativă, evidențiind descoperirea unei limitări în tehnologia blockchain legată de automatizarea plăților recurente. Procesul de cercetare și testare a arătat o provocare specifică asociată tranzacțiilor recurente: necesitatea de a deține cheia privată în orice moment.

5.2.5 Promovarea Standardizării pentru Tranzacțiile și Plățile Recurente: Un Nou Grup de Lucru IEEE pentru Dezvoltarea Standardelor

În plus față de contribuțiile menționate anterior, apare o a cincea contribuție semnificativă ca rezultat al descoperirii limitării privind automatizarea plăților recurente pe blockchain. Această descoperire a condus la înființarea unui nou grup de lucru în cadrul Institutului de Inginerie Electrică și Electronică (IEEE) cu scopul de a dezvolta un standard care să abordeze în mod specific tranzacțiile și plățile recurente.

Recunoașterea importanței abordării acestei limitări și avansarea domeniului au dus la înființarea grupului de lucru, cunoscut oficial sub numele de "Recurring Transactions on the Distributed Ledger Technologies (DLTs) Working Group" (P3228 WG), care a fost fondat și este operațional începând cu iunie 2023. Fondarea și servirea în calitate de membru al bordului acestui grup prestigios este Razvan Mihai, cercetătorul responsabil pentru munca revoluționară în automatizarea tranzacțiilor recurente pe blockchain.

5.2.6 Integrarea Prototipului și a Învățării Automate pentru Prognozarea Solidității Economice

Dezvoltarea unui cadru care integrează prototipul, proiectat pentru automatizarea tranzacțiilor recurente pe blockchain, cu o soluție de învățare automată reprezintă o contribuție semnificativă. Această integrare își propune să valorifice datele blockchain pentru a prezice soliditatea economică a afacerilor, facilitând identificarea riscurilor și promovând stabilitatea financiară.

În concluzie, integrarea prototipului și a învățării automate reprezintă o contribuție semnificativă în domeniu. Prin valorificarea datelor blockchain și a analizei predictive, cadrul permite prognozarea solidității economice, identificarea riscurilor și prevenirea falimentelor neașteptate. Această integrare îmbunătățește practicile de gestionare a riscurilor, susține luarea deciziilor informate și promovează stabilitatea

5.3 Lista publicatiilor originale

1. R. Mihai, O. F. Ozkul, G. Datta, N. Goga, S. Grybniak, and C. V. Marian, "Blockchain-enabled economic transactions: Recurring financial accruals and payments," in 2022 IEEE Is Global Emerging Technology Blockchain Forum: Blockchain & Beyond. Irvine, CA, USA: IEEE, 2022, pp. 1-5. https://ieeexplore.ieee.org/document/10087074 [22]

2. R. Mihai, T. E. Nyberg, E. Michaelsen, I. Rizea-Popp, M. Dascalu, and G. M. Stefan, “IT-based financial confirmation and diagnosis mechanisms,” ROMANIAN JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY, vol. 22, pp. 284–299, 2019 [17].

3. R. Mihai, "Universal contract on blockchain," Economics of Financial Technology Conference, Edinburgh, 2022-05-13. https://www.eftconference.business-school.ed.ac.uk/past-papers?title=&page=4 [1].

4. R. Mihai, M. Malita, G.M. Stefan: "Nano-Structural Requirements for Artificial Intelligence and Blockchain Applications" Proceedings of the 42nd International Semiconductor Conference CAS 2019, 9—11 October 2019, Sinaia, Romania, pp 115-118. DOI: 10.1109/SMICND.2019.8923787 At: https://ieeexplore.ieee.org/document/8923787 [26].

5. M. Malița, G. M. Ștefan, and R. Mihai, “Architectural features for artificial inteligence and blockchain in the nano-era,” Romanian Journal of Information Science and Technology, vol. 23, no. 2, pp. 115–126, 2020 [27].

6. G. M. Ștefan and R. Mihai, “IT driven distributed consensus for an integrated globalized world,” Romanian Journal of Information Science and Technology, vol. 21, no. 2, pp. 114–128, 2018 [11].

7. S. Grybniak et al., “Recurring payments on EVM-based platforms,” in 2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain). Irvine, CA, USA: IEEE, 2022, pp. 1–6. [28].

5.4 Perspective pentru dezvoltări ulterioare

5.4.1 Avansarea Prototipului: Integrarea unei Soluții de Învățare Automată cu Cadru Există Bazat pe Blockchain

Ca parte a dezvoltării viitoare a lucrării noastre, accentul se mută acum către implementarea cadrului definit care integrează prototipul cu o soluție de învățare automată. În timp ce cadrul a fost conceptualizat și proiectat pentru a valorifica datele blockchain pentru a prezice soliditatea economică și pentru a promova stabilitatea financiară [17], următoarea fază implică implementarea efectivă a modelului de învățare automată.

5.4.2 Navigarea Provocării Blockchain: Pursuitarea Plăților Automate Decentralizate

Secțiunea 4.3 Automatizarea Plăților Recurente a dezvăluit o provocare cheie în tehnologia blockchain: automatizarea plăților recurente fără intervenție manuală. Accentul nostru se mută către abordarea acestei limitări. Un efort preliminar [28], scris în colaborare cu autorul tezei, marchează începutul acestei urmăriri. Munca viitoare implică proiectarea unei soluții pentru plățile automate decentralizate. Acest efort academic îmbină cunoștințele teoretice cu aplicarea practică, împingându-ne către un viitor promițător în care potențialul blockchain-ului este valorificat pentru a armoniza autonomia decentralizată cu automatizarea fără probleme. Această muncă viitoare completează efortul de contribuție la elaborarea standardului IEEE privind plățile recurente așa cum este conturat în Secțiunea **????**.

5.4.3 Îmbunătățirea Confidențialității în Tranzacțiile Economice Bazate pe Blockchain: Integrarea Zere-Knowledge Proof pentru o Confidentialitate Imbunatatita.

Pentru a îmbunătăți prototipul, se va acorda o atenție deosebită abordării conceptului de confidențialitate a datelor în tehnologia blockchain. Este crucial să eliminăm orice neînțelegeri privind utilizarea algoritmilor criptografici de hash în blockchain, care sunt folosiți în principal pentru a asigura validitatea blocurilor și securitatea tranzacțiilor, mai degrabă decât pentru a ascunde transferurile de fonduri.

Pentru a răspunde cerințelor de confidențialitate ale participanților în contextul economic, îmbunătățiri vor fi făcute prin incorporarea tehnologiilor emergente de strat 2, cum ar fi dovezi zero-cunoștințe, în prototip. Dovezile zero-cunoștințe oferă soluții promițătoare pentru îmbunătățirea confidențialității în timp ce mențin integritatea și transparența blockchain-ului.

References

[1] R. Mihai, "Universal contract on blockchain," Economics of Financial Technology Conference, Edinburgh, 2022-05-13. [Online]. Available: https://www.eftconference.business-school.ed.ac.uk/past-papers?title=&page=4,Accessed:May2022

[2] N. Narula, W. Vasquez, and M. Virza, "zkledger: Privacy-preserving auditing for distributed ledgers," MIT Media Lab, https://dci.mit.edu/zkledger, Accessed: Oct. 2021.

[3] P. Merriam, "Ethereum alarm clock," https://github.com/ethereum-alarm-clock/ethereum-alarm-clock, Accessed: Nov. 2021.

[4] Whitepaper, "Chainlink 2.0 and the future of decentralized oracle networks," https://chain.link/whitepaper, Accessed: Jan. 2022.

[5] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://org/bitcoin.pdf

[6] C. Catalini and J. S. Gans, "Some simple economics of the blockchain," April 2019, Rotman School of Management Working Paper No. 2874598, MIT Sloan Research Paper No. 5191-16. [Online]. Available: https://ssrn.com/abstract=2874598

[7] E. Mantelaers, M. Zoet, and K. Smit, "The Impact of Blockchain on the Auditor's Audit Approach," in *Proceedings of the 2019 3rd International Conference on Software and e-Business*. Tokyo Japan: ACM, Dec. 2019, pp. 183–187. [Online]. Available: http://dl.acm.org/doi/10.1145/3374549.3374551

[8] C. Dwork, M. Naor, and H. Wee, "Pebbling and proofs of work," in *Advances in Cryptology – CRYPTO 2005*, V. Shoup, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005, pp. 37–54.

[9] S. Seth, "Public, private, permissioned blockchains compared," *Investopedia*. [Online]. Available: https://www.investopedia.com/news/public-private-permissioned-blockchains-compared/

[10] M. A. Specter, J. Koppel, and D. Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US Federal Elections," in *29th USENIX Security Symposium (USENIX Security 20)*, 2020, pp. 1535–1553.

[11] G. M. Ştefan and R. Mihai, "IT driven distributed consensus for an integrated globalized world," *Romanian Journal of Information Science and Technology*, vol. 21, no. 2, pp. 114–128, 2018. [Online]. Available: https://www.romjist.ro/full-texts/paper585.pdf

[12] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards," *Overview report The British Standards Institution (BSI)*, vol. 40, p. 40, 2017. [Online]. Available: https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf

[13] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, 2014.

[14] K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. Gün Sirer *et al.*, "On scaling decentralized blockchains," in *International conference on financial cryptography and data security*. Springer, 2016, pp. 106–125.

[15] W. Chen, Y. Xu, Z. Zheng, Y. Zhou, J. E. Yang, and J. Bian, "Detecting" pump & dump schemes" on cryptocurrency market using an improved apriori algorithm," in *2019 IEEE International Conference on Service-Oriented System Engineering (SOSE)*. IEEE, 2019, pp. 293–2935.

[16] A. Vetter, "Blockchain, machine learning, and a future accounting," *Journal of Accountancy*, vol. 28, 2018. [Online]. Available: https://www.journalofaccountancy.com/newsletters/2018/aug/blockchain-machine-learning-future-accounting.html

[17] R. Mihai, T. E. Nyberg, E. Michaelsen, I. Rizea-Popp, M. Dascalu, and G. M. Stefan, "IT-based financial confirmation and diagnosis mechanisms," *ROMANIAN JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY*, vol. 22, no. 3-4, pp. 284–299, 2019.

[18] T. Lyons and L. Courcelas, "Convergence of blockchain, ai and iot," *The European Union Blockchain Observatory and Forum*, 2020. [Online]. Available: https://www.eublockchainforum.eu/sites/default/files/report_convergence_v1.0.pdf

[19] Amazon, "AWS IoT – Amazon Web Services," Accessed: Jun.8, 2020. [Online]. Available: https://aws.amazon.com/iot/

[20] M. S. Ferdous, M. J. M. Chowdhury, M. A. Hoque, and A. Colman, "Blockchain Consensus Algorithms: A Survey," 2020. [Online]. Available: https://arxiv.org/abs/2001.07091

[21] A. J. Kolber, "Not-So-Smart Blockchain Contracts and Artificial Responsibility," *Stanford Technology Law Review*, vol. 21, no. 18-44, p. 198, May 2018. [Online]. Available: https://ssrn.com/abstract=3186254

[22] R. Mihai, O. F. Ozkul, G. Datta, N. Goga, S. Grybniak, and C. V. Marian, "Blockchain-enabled economic transactions: Recurring financial accruals and payments," in *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond*. Irvine, CA, USA: IEEE, 2022, pp. 1–5. [Online]. Available: https://ieeexplore.ieee.org/document/10087074

[23] ICAEW, "Blockchain and the future of accountancy," ICAEW Thought Leadership, ISBN 978-1-78363-933-5, 2018, https://www.icaew.com/technical/technology/blockchain-and-cryptoassets/blockchain-articles/blockchain-and-the-accounting-perspective, Accessed: Oct. 2021.

[24] A. M. Antonopoulos and G. Wood, *Mastering Ethereum: Building Smart Contracts and DApps*. O'Reilly Media, 2018.

[25] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117 134–117 151, 2019.

[26] R. Mihai, M. Malita, and G. M. Stefan, "Nano-Structural Requirements for Artificial Intelligence & Blockchain Applications," in *2019 International Semiconductor Conference (CAS)*. Sinaia, Romania: IEEE, Oct. 2019, pp. 115–118. [Online]. Available: https://ieeexplore.ieee.org/document/8923787/

[27] M. Maliţa, G. M. Ştefan, and R. Mihai, "Architectural features for artificial inteligence and blockchain in the nano-era," *Romanian Journal of Information Science and Technology*, vol. 23, no. 2, pp. 115–126, 2020. [Online]. Available: https://www.romjist.ro/full-texts/paper642.pdf

[28] S. Grybniak *et al.*, "Recurring payments on EVM-based platforms," in *2022 IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain)*. Irvine, CA, USA: IEEE, 2022, pp. 1–6. [Online]. Available: https://doi.org/10.1109/iGETblockchain56591.2022.10087077