

Integrarea tehnologiilor blockchain și IoT în clădirile din sectorul rezidențial și terțiar

Coordonator proiect: Prof. Univ. Paul Sterian

Autor: Dr.-Ing. Vladimir Tanasiev

Autor: Dr.-Ing. Grigore Stamatescu

The image shows two handwritten signatures in blue ink. The top signature is for Vladimir Tanasiev, written in a cursive style. The bottom signature is for Grigore Stamatescu, also in a cursive style.

Decembrie 2018

Cuprins

Relevanța științifică.....	3
Preocupări la nivelul UE privind tehnologia blockchain.....	4
Evoluția IoT.....	5
Tehnologia blockchain.....	9
Studii de caz.	12
Microgridul bazat pe blockchain.	12
Sistem de transport a energiei bazat pe soluții flexibile și transparente	12
Realizarea unui sistem inteligent de management al energiei (EMS) pentru controlul predictiv într-o micronețea rezidențială.....	12
Gateway Industrial Internet of Things (IIoT) pentru aplicații de management al energiei în clădirile inteligente – KUNBUS RevPiConnect.....	14
Implementarea comunicației dintre KUNBUS RevPi Connect și Controllerul Victron Color Control GX (CCGX)	16
Referințe bibliografice	20

Relevanța științifică.

Clădirile au devenit gradual actori critici pentru consumul de energie și provocările legate de calitatea vieții în societățile moderne, puternic urbanizate. Creșterea sectorului rezidențial, creșterea demografică și migrația populației spre zonele urbane reprezintă principalele provocări la nivelul UE pe termen mediu și lung. În acest context, consecințele directe vor fi creșterea anuală a emisiilor de CO₂ și a consumului de energie. În prezent, strategiile energetice ale UE ce vizează sectorul rezidențial și soluțiile comunității științifice sunt orientate spre eficiență energetică, implementarea soluțiilor inteligente și tehnologiilor digitale cu scopul de a reduce consumul de energie și de a crește confortului utilizatorilor.

În ultimii ani, inovarea digitală și numărul dispozitivelor Internet of Things (IoT) cu aplicații în sectorul rezidențial au cunoscut o creștere exponențială. IoT este un concept care integrează un număr mare de obiecte fizice identificate în mod unic, interconectate și accesibile prin Internet. IoT își propune să transforme orice obiect din lumea reală într-un dispozitiv de calcul care are capacități de detectare, comunicare și control. Se așteaptă ca până în 2020 numărul dispozitivele IoT să depășească 25 mld până în anul 2025 [1].

Economia digitală în UE are o rată de creștere de 7 ori mai mare decât restul economiei, 12% pe an. La nivel global, piața dispozitivelor IoT pentru uz casnic se va tripla la aproape 1.7 trilioane de usd până în 2020 [2]. Odată cu scăderea masivă în ceea ce privește costurile puterii de calcul, ajungând la valoarea de 0,06 \$ per milion de tranzistori în 2012, performanța costului lățimii de bandă atingând 23 \$ pe 1000 megabiți pe secundă (Mbps) în 2012 și performanța costurilor de stocare [3] domeniul de aplicabilitate s-a extins, inclusiv în sectorul rezidențial și terțiar.

Aceste date arată clar maturitatea tehnologiilor digitale și tendința mediului economic de a investi în sectorul rezidențial și terțiar, cu precădere în soluții care să reducă consumul de energie fără a compromite confortul locuitorilor. Aceste preocupări au fost, de asemenea, evidențiate în [4] unde s-a arătat un potențial de reducere a consumului de energie estimat la 35-55% [4].

Dpdv social, aplicațiile IoT pentru sectorul rezidențial promet să schimbe modul în care interacționăm cu clădirile, creând în același timp o nouă dimensiune a confortului.

O problemă de actualitate rămâne cea legată de securitatea datelor. Odată cu creșterea domeniului de aplicabilitate al IoT, cresc numărul și complexitatea atacurilor împotriva sistemelor IoT ce au ca scop furtul de date, întreruperea funcționării normale a rețelei sau serviciilor, introducerea de informații false [5-7]. Cele mai cunoscute soluții de securizare sunt cele dezvoltate de principalii

jucători: Lora, ZigBee, NFC Forum, Thread Group, precum și organismele de standardizare IEEE și IETF [7].

Soluțiile actuale propun doar securizarea transferului de date prin rețele fără fir, neexistând o metodă standardizată de securizare a datelor. În prezent, cea mai promițătoare soluție de securizare a datelor o reprezintă tehnologia blockchain. Implementarea acestei tehnologii în securizarea structurilor de date va accelera dezvoltarea soluțiilor IoT [8,9].

A doua problemă de mare actualitate o reprezintă necesitatea dezvoltării de algoritmi inteligenți, capabili să proceseze, analizeze cantități mari de date (big data analytics) și să genereze decizii adecvate pentru unitățile control-comandă. Un model mai adecvat este considerat a fi modelul ascuns Markov (HMM). În literatura științifică există numeroase aplicații bazate pe HMM, de la analiza structurii ADN, analiza pieței financiare până la modelarea consumului de energie la domiciliu și a profilului de ocupare [10-13].

Preocupări la nivelul UE privind tehnologia blockchain

În anul 2018, Comisia Europeană a lansat Observatorul și forumul UE privind tehnologia blockchain, cu sprijinul Parlamentului European. Observatorul și forumul UE privind tehnologia blockchain pune accentul pe principalele evoluții din domeniul tehnologiei blockchain, promovează actorii europeni din sector și consolidează cooperarea Uniunii Europene cu diversele părți interesate implicate în activități de tip blockchain.

Tehnologiile blockchain, care stochează blocuri de informații ce sunt distribuite la nivelul unei întregi rețele, sunt considerate a reprezenta un progres major în domeniu, întrucât asigură un nivel ridicat de trasabilitate și securitate a tranzacțiilor online. Se estimează că aceste tehnologii vor avea un impact semnificativ asupra serviciilor digitale și vor transforma modelele de afaceri dintr-o gamă largă de domenii, cum ar fi sănătatea, asigurările, finanțele, energia, logistica, gestionarea drepturilor de proprietate intelectuală și serviciile guvernamentale [14].

Evoluția IoT

Pe măsură ce numărul de dispozitive conectate crește de la miliarde la sute de miliarde principalii jucători, guvernele și corporațiile, se deplasează pentru a prelua controlul asupra dispozitivelor și a datelor printr-un model de business bazat pe centralizarea informațiilor. Soluția la acest model o reprezintă dezvoltarea unei economii digitale foarte eficiente creată prin produse îmbunătățite și experiențe noi ale utilizatorilor ce au la baza valoarea colaborativă.

Fundamentul ce stă la baza calculatoarelor moderne este procesarea tranzacțiilor. De la apelurile telefonice la contorizarea energiei electrice, acestea sunt cunoscute ca fiind tranzacții care trebuie procesate.

Procesarea tranzacțiilor nu este task nou. Fiecare interacțiune digitală poate fi considerată o tranzacție. În lumea de astăzi bazată pe web, amploarea și volumul tranzacțiilor au explodat. Peste 5 miliarde de tranzacții media socială sunt procesate în fiecare zi. O nouă direcție își face loc în lumea digitală, dispozitivele IoT. Aceasta explodează în continuare atât prin prisma volumului mare de dispozitive dezvoltate dar și prin prisma volumului tranzacțiilor care urmează să fie procesate.

Procesarea tranzacțiilor nu a putut fi redimensionată până la nivelul actual fără distribuirea efortului de calcul. Calculul computerizat a existat de ceva timp, așa cum au existat și sistemele peer-to-peer. Pe măsură ce tehnologiile digitale avansează va fi posibilă în curând valorificarea puterii de calcul, a terabyților de spațiu de stocare și a lățimii de bandă pentru miliarde de dispozitive, în milioane de locații, pentru procesarea tranzacțiilor. [15]

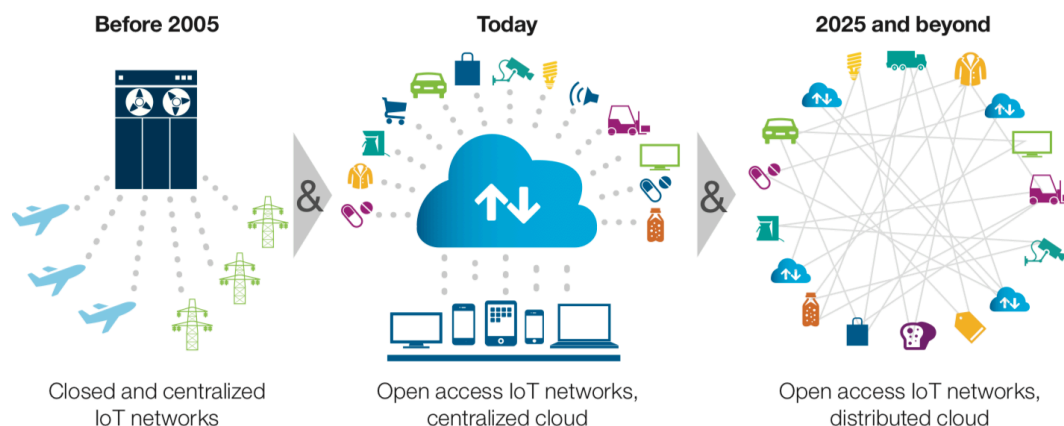


Fig 1. Progresul rețelelor și a tehnologiilor digitale [15].

În ultimii ani, dispozitivele inteligente pentru sectorul rezidențial au urmat o tendință exponențială în ceea ce privește creșterea și inovațiile. Internetul obiectelor (IoT), o tehnologie emergentă aflată în continuă creștere, promite să ne schimbe modul de a interacționa cu clădirile, creând în același timp o nouă dimensiune a confortului.

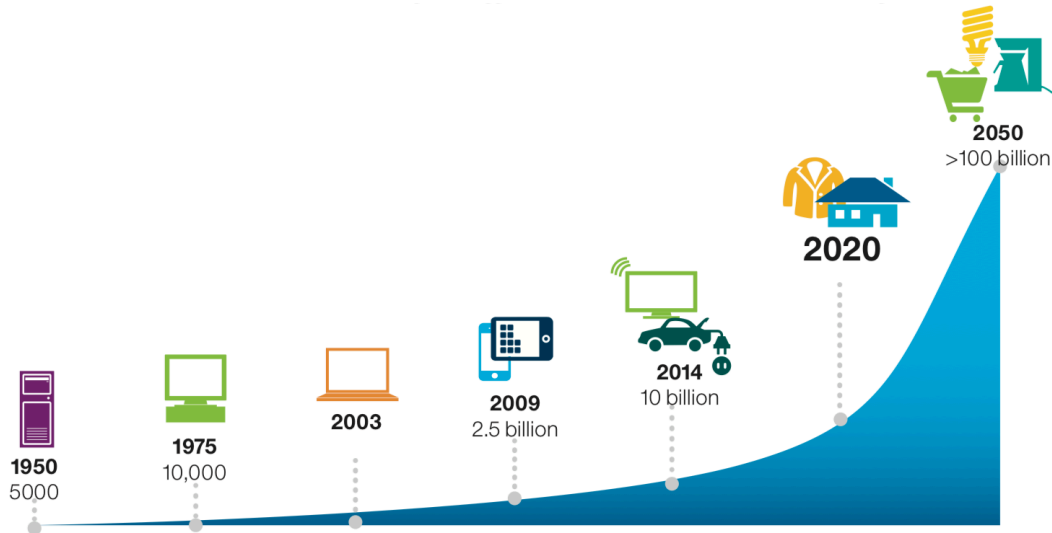


Fig.2. Avansul dispozitivelor IoT [15].

Internetul obiectelor nu are o definiție clară, totuși o definiție recomandată a fost propusă de grupul de studiu 13 al Uniunii Internaționale a Telecomunicațiilor ca o "O infrastructură globală pentru societatea informațională, care permite servicii avansate prin interconectarea (fizică și virtuală) tehnologiilor interoperabile de informare și comunicare existente și în evoluție " [16].

IoT nu este o soluție tehnică, dar poate fi considerată ca un model de concept care utilizează tehnologii digitale pentru o integrare mai largă.

Nu există un numitor comun pentru descrierea arhitecturii IoT. Alte abordări pot fi luate în considerare pentru a descrie numai arhitectura hardware, software sau arhitectura rețelei.

Indiferent de aplicație, Höller și colab. [17] a propus un model cu următoarele capacități funcționale:

Tabelul 1. Cele mai comune blocuri IoT

IoT Data and Service	Management	Security	Business layer
			Application layer
			Data and information layer
			Service support layer
			Communication layer
			Resource layer
			Asset layer

1. Asset layer

Reprezintă obiectele din lumea reală supuse monitorizării și controlului având reprezentări și identități digitale. Acest nivel este considerat a fi la granița dintre lumea reală compusă din semnale analogice și lumea digitală

2. Resource layer

Asigură capabilitățile funcționale ale identității de detectare, de acționare și de integrare. Acest nivel oferă posibilitatea de a obține semnalul și de a-l transforma într-un semnal digital. Senzorii și dispozitivele de acționare pot furniza date prin intermediul rețelelor cu sau fără fir utilizând protocolul IP.

3. Communication layer

Este utilizat pentru a asigura mijloacele de conectivitate între resurse și entitățile de calcul. Conform recomandărilor făcute de Sectorul de Standardizare a Telecomunicațiilor al Uniunii Internaționale a Telecomunicațiilor (ITU-T), nivelul de comunicare trebuie să ofere: capabilitatea rețelei - funcțiile de control și conectivitate a rețelei (funcții de acces, transport, autentificare, autorizare); capabilități de transport - conectivitate pentru transportul informațiilor de control și de gestionare și transferul informațiilor. În funcție de specificitatea dispozitivului, se pot stabili protocoale de comunicare și stive de rețea, care pot varia de IEEE 802.15.4 (6LoWPAN, ZigBee, Thread), IEEE 802.11 (WiFi) la Z-Wave, Bluetooth, Message Queue Telemetry Transport (MQTT), Constrained Application

Protocol (CoAP), IPSec, eXtensible Messaging and Presence Protocol (XMPP), Radio-Frequency Identification (RFID) și alți facilitatori de comunicare.

4. Service support layer

Poate oferi diagnosticare la distanță, gestionare, manipulare a dispozitivelor, actualizarea software-ului, reconfigurarea dinamică a instrumentelor de aplicație. Aceste capacități sunt de obicei specifice mediului de tip cloud.

5. Data and information layer

Are un scop mai abstract și se axează pe organizarea și reprezentarea cunoștințelor. Acest nivel se sprijină pe logica de control avansată denumită KMF (Knowledge Management Framework). Prin urmare, KMF include modele de date și informații, reprezentare și stocare. KMF este foarte diferită de la o aplicație la alta și poate fi prezentată într-o varietate de moduri și pot fi utilizate diverse tehnici pentru a consuma cunoștințele sau a lua decizii pe baza cunoștințelor anterioare și actuale.

6. Application Layer

Stratul aplicației conține aplicații IoT. Există o gamă largă de aplicații diferite pentru controlarea inteligentă, automatizarea clădirilor, aplicații web etc.

7. Business layer

Acest nivel se concentrează pe integrarea aplicațiilor IoT, gestionează întregul sistem sau alte activități de bază ale oricărei întreprinderi. Mai mult decât atât, poate oferi și mijloacele de comunicare pentru accesul la date și informații către alte aplicații

Pe lângă modelul funcțional compus din 6 niveluri, sistemele IoT integrează transversal 3 niveluri: Management, Securitate și Date și servicii.

Nivelul de management se ocupă de operarea, conectivitatea, întreținerea și administrarea diferitelor părți ale soluției.

Nivelul de securitate protejează sistemul, serviciile și informațiile generate de entitățile neautorizate. Măsurile de securitate sunt implementate în toate nivelurile. Securitatea rețelei, gestionarea identității, confidențialitatea și reziliența reprezintă componentele cheie. Despre nivelul de securitate se va discuta separat, în continuare.

Nivelul de date și servicii se concentrează asupra etapelor de procesare a datelor la diferite niveluri, de granularitate și complexitate, precum și de data mining și analiza datelor.

Într-o rețea de amploare a internetului, atingerea unui nivel de securitate dorit poate fi greu de obținut, dacă nu chiar imposibilă. Cu toate acestea, pentru adoptarea pe scară largă a internetului în continuă expansiune, confidențialitatea și anonimatul trebuie integrate în proiectarea sa, oferind utilizatorilor controlul asupra vieții private.

Modelele actuale de securitate sunt depășite și trebuie înlocuite cu o abordare mai nouă - securitate prin transparență. Pentru aceasta, este necesară o trecere la o soluție software de tip open source. Și în timp ce sistemele open source pot fi în continuare vulnerabile la accidente și slăbiciuni exploatabile, ele sunt mai puțin susceptibile de a fi afectate de intruziunile guvernamentale și de altă natură, pentru care automatizarea acasă, mașinile conectate și multitudinea de alte dispozitive conectate prezintă o mulțime de oportunități.

Însă, cea mai mare provocare nu este aceea de a construi pur și simplu un sistem IoT descentralizat, ci unul general valabil, menținând în același timp tranzacții private, sigure și fără încredere (ce pot fi realizate fără intermediari).

IoT reprezintă un loc unde miliarde de participanți ce realizează tranzacții, dintre acestea nu toate pot fi de încredere, unele chiar dăunătoare, cu o nevoie de o anumită formă de validare și consens. Pentru acest model Blockchain-ul oferă o soluție promițătoare.

În absența unui server care centralizează mesajele și comunică cu celelalte dispozitive, o soluție IoT descentralizată ar trebui să susțină trei tipuri de tranzacții: comunicarea peer-to-peer fără intermediari, partajarea datelor într-un mediu securizat, o modalitate scalabilă de coordonare a dispozitivelor. Noutatea comunicațiilor peer-to-peer este dată de criptarea datelor între dispozitivele IoT.

Tehnologia blockchain

Blockchain este o bază de date distribuită implementată într-o rețea de tip peer-to-peer unde nodurile din sistem creează și difuzează tranzacții continue [18]. Ideea de sistem distribuit pentru tranzacții și verificarea acestora nu este nouă, ea a fost analizată și descrisă în detaliu în lucrarea de referință „Bitcoin: A Peer-to-Peer Electronic Cash System”. Odată ce acest concept a fost

investigat din punct de vedere teoretic, în prezent sunt puține aplicații practice și în continuare sunt necesare mai multe demonstrații de implementare ale conceptului (proof of concept).

Printre principalii jucători care investighează oportunitatea de implementare a blockchain se numără și companiile IBM și Samsung. Tehnologia blockchain va avea un impact deosebit asupra internetului și că există eforturi continue pentru a crea diferite produse și servicii noi destinate, printre altele, și sectorului rezidențial [19].

Blockchain-ul deține o înregistrare a fiecărei tranzacții efectuate de fiecare participant. Criptografia este utilizată pentru verificarea tranzacțiilor și păstrarea informațiilor despre blocul privat. Mulți participanți verifică fiecare tranzacție, oferind o verificare extrem de redundantă și sunt recompensați pentru munca de calcul cerută. Prin confirmarea tranzacțiilor utilizând consensul descentralizat, blocul elimină nevoia de încredere.

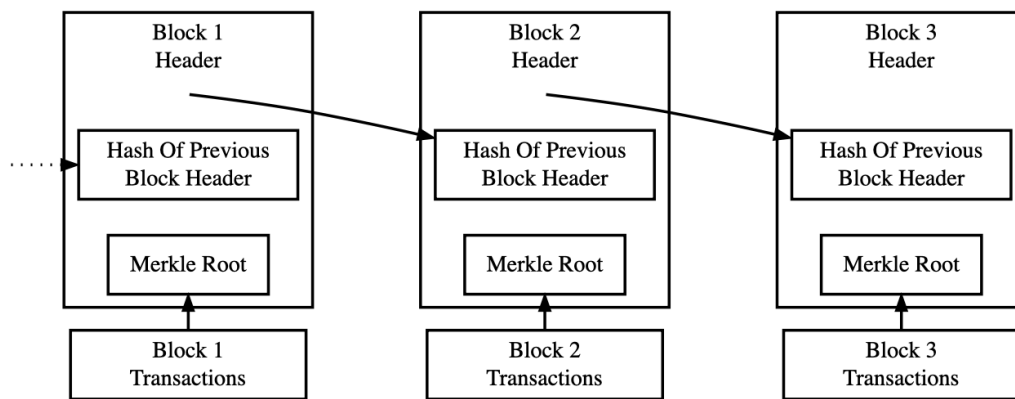


Fig. 3. Model simplificat de blockchain [20]

În figura 3 este prezentată informația înmagazinată într-un bloc. Un nou bloc este rezultatul unei noi tranzacții. După realizarea tranzacției, copiile generate au asociate un hash (produs secundar criptografic al algoritmului hash), care la rândul lor sunt asociate din nou sub forma unui arbore de hash-uri. De asemenea, fiecare bloc nou are înmagazinat în header, hash-ul blocului anterior. O tranzacție poate fi descrisă ca fiind o entitate mică, ca rezultat al unui task, stocată în înregistrările publice (public ledger). Aceste blocuri sunt executate, implementate și stocate în blockchain numai după validarea de către toate persoanele implicate în rețeaua de blocuri pentru evitarea manipulării datelor. Fiecare tranzacție anterioară poate fi revizuită oricând, dar nu poate fi actualizată.

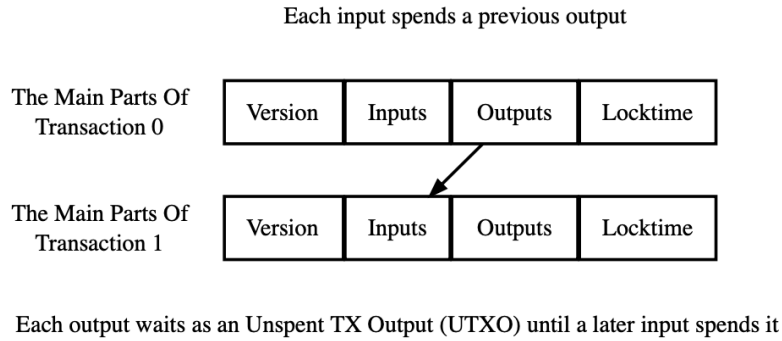


Fig. 4. Componenta principală a unei tranzacții [20].

Orice tranzacție are asociată cel puțin o intrare și cel puțin o ieșire. Tranzacțiile sunt transmise fiecărui nod care își creează propria versiune actualizată a evenimentelor. Modalitatea de structurare a datelor după modelul distribuit face ca tehnologia blockchain să fie extrem de utilă. Această inovație în domeniul înregistrării și distribuției informațiilor elimină intermediarul care facilitează transferul informațiilor digitale.

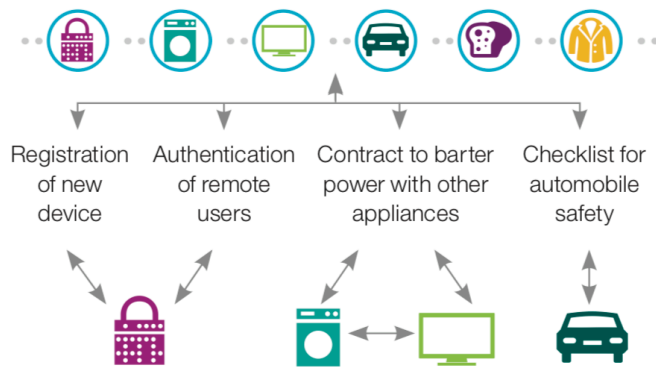


Fig. 5. Regstru universal [15].

Un IoT descentralizat având la bază conceptul blockchain este framework-ul care facilitează procesarea tranzacțiilor și coordonarea între dispozitivele care interacționează. În acest ecosistem nou, utilizatorii leagă dispozitivele folosind identificarea și autentificarea securizată.

O vulnerabilitate teoretică este considerată a fi controlul a 51% a puterii de calcul din rețea. Prin controlul majorității puterii de calcul din rețea, un atacator sau un grup de atacatori poate interfera cu procesul de înregistrare a blocurilor noi.

Crearea și executarea de către utilizatori a listelor de verificare digitale bazate pe un set de reguli predefinite poate să asigure funcționarea optimă a dispozitivele.

Studii de caz.

Microgridul bazat pe blockchain.

În 2016 compania LO3 Energy a colaborat cu Siemens pentru a crea un microgrid pilot, în orașul New York, utilizând tehnologia blockchain. Locuitorii cu panouri solare pot vinde astfel, surplusul de energie către vecinii lor, prin intermediul tranzacțiilor peer-to-peer, ce au la bază conceptul de blockchain. Rețelele microgrid minimizează cantitatea de energie pierdută prin tranzit, reducând pierderile cu 5% și oferind astfel o alternativă eficientă. Aceste companii au prezentat soluții pentru comercializarea surplusului de energie produs de orice consumator, indiferent dacă este vorba despre o reședință, un condominiu, o fabrică sau o fermă. Soluțiile curente permit, în general, ca fiecare unitate de energie electrică să fie urmărită de la punctul de producție până la punctul de consum, utilizând rețeaua locală de distribuție a energiei electrice. Blockchain combină o tranzacție de energie cu o tranzacție financiară, făcând procesul mai simplu și mai sigur [21].

Sistem de transport a energiei bazat pe soluții flexibile și transparente

În Europa, TenneT, este un important operator de transport de energie electrică, preocupat de limitările surselor convenționale de energie ce a decis să investească în noi modalități de producere și furnizare a energiei pentru a fi pregătită pentru creșterea viitoare a cererii. TenneT împreună cu companiile Sonnen Group și Vandebron investighează în prezent potențialul utilizării tehnologiei open source Hyperledger Fabric dezvoltat de Linux Foundation pentru a integra unitățile de producție a energiei electrice furnizată de mașinile electrice și bateriile de uz casnic în rețeaua electrică [21].

Realizarea unui sistem inteligent de management al energiei (EMS) pentru controlul predictiv într-o microrețea rezidențială

Conceptul unui sistem EMS pentru controlul predictiv al fluxurilor de energie este prezentat în [22,23]. Integrarea pasivă a surselor de energie regenerabilă conduce la incertitudini în creștere și costuri operaționale mai mari pentru rețeaua electrică. Deoarece obținerea unor răspunsuri rapide din partea centralelor electrice convenționale a devenit o provocare ținând cont de scăderea proporției acestora în totalul producției, conceptul de operare al sistemului energetic

se deplasează către sarcini/consumatori flexibili. O abordare modernă presupune deplasarea curbelor de sarcină prin sarcini controlabile e.g. la nivelul sistemelor de încălzire, ventilație și aer condiționat (HVAC) în clădirile inteligente. Dispozitivele de stocare a energiei e.g. baterii sunt de asemenea folosite ca rezervă suplimentară pentru echilibrarea rețelei. Această abordare necesită o interacțiune robustă între rețea și sistemul de management al energiei clădirii. Controlul predictiv pentru un microgrid rezidențial include și participarea optimă din punctul de vedere al costurilor clădirii la piața de energiei volatilă. Clădirea oferă propriul profil de consum planificat și primește prețurile energiei pentru ziua următoare, calculate în funcție de condițiile de piață curente. Scenariul simplificat de interacțiune grid-microgrid presupune adaptarea profilului de consum anticipat pe baza prețurilor primite și a unor cereri de flexibilitate din partea rețelei care reprezintă deviații impuse de la acest profil. Algoritmul MPC optimizează operarea microrețelei și generează ieșiri sub forma unor profile de schimb de energie impuse pentru elementele controlabile la nivelul microrețelei.

Arhitectura de implementare a conducerii predictive pentru un microgrid rezidențial este ilustrată mai jos.

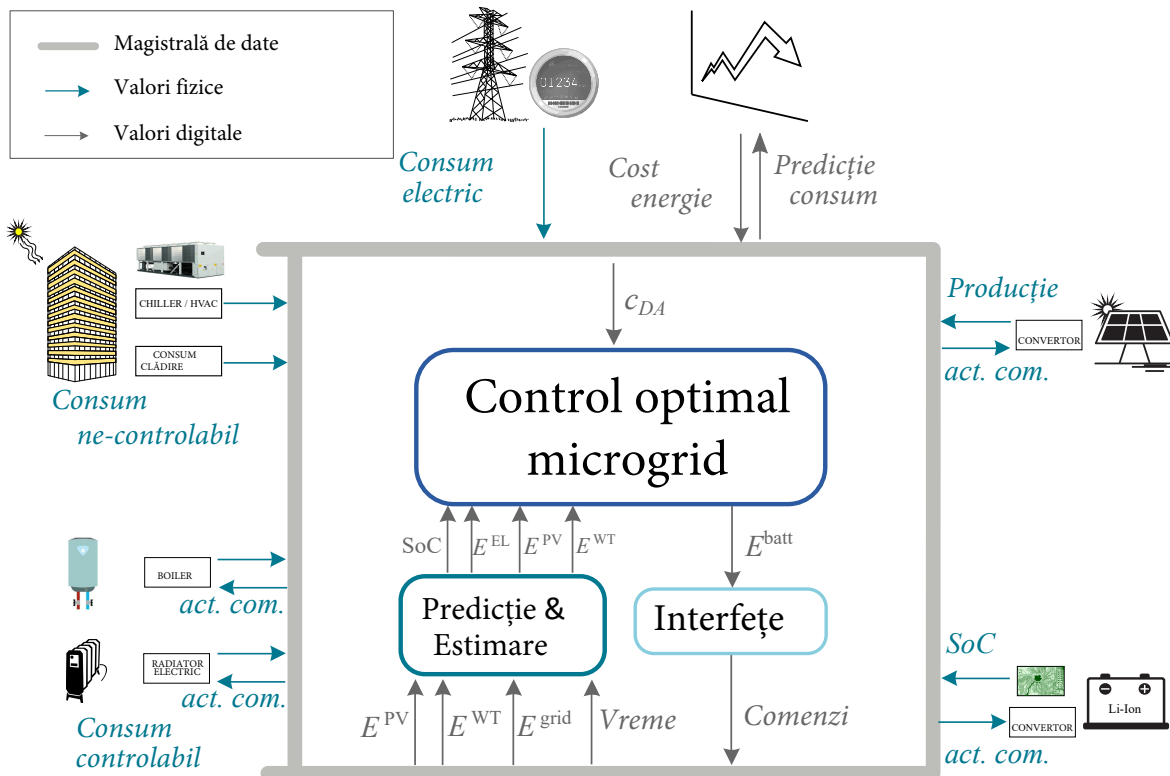


Fig. 6. Arhitectura de implementare a conducerii predictive pentru un microgrid rezidențial

Gateway Industrial Internet of Things (IIoT) pentru aplicații de management al energiei în clădirile inteligente – KUNBUS RevPiConnect

Sistemul deschis KUNBUS RevPi Connect funcționează ca un gateway IIoT pentru aplicații industriale și pentru monitorizarea și conducerea clădirilor inteligente. Componenta software este reprezentată de un sistem de operare Raspbian Linux cu un modul dedicat de timp real. Sunt suportate protocoale IIoT uzuale standardizate precum MQTT și OPC UA. Dezvoltarea locală de aplicații se poate realiza printre altele cu Node-RED, Python sau direct în limbajul de programare C. Un avantaj al acestui sistem este posibilitatea de extensie la nivel logic pentru suportul protocoalelor industriale PROFINET, Ethernet/IP, EtherCAT, Modbus TCP și RTU fără utilizarea unor module de comunicație hardware dedicate. În funcție de protocolul ales pot exista atât biblioteci software open-source gratuite sau variante comerciale ce necesită licențiere. Cele două interfețe Ethernet disponibile permit conectarea sistemului simultană la rețeaua industrială – de echipamente de măsurare și conducere pentru subsistemele energetice ale clădirii, cât și la rețeaua convențională IT, ce permite transmiterea datelor și comenzilor de la nivel de câmp către un sistem cloud/sistem IT ierarhic superior sau viceversa. Un semnal watchdog hardware liber configurabil monitorizează starea gateway-ului IIoT, în timp ce o ieșire de tip releu permite monitorizarea sau resetarea dispozitivelor conectate sau a modulelor de extensie. Dispozitivul oferă suplimentar o intrare de 24V pentru primirea de semnale de oprire de la un UPS, pentru operare robustă [24].

Construcția modulară a sistemului RevPi Connect permite conectarea facilă a unor module de extensie cum sunt cele de intrări/ieșiri analogice și digitale, module de comunicații și module radio, ca de exemplu un modul Bluetooth. Modulele de extensie se conectează printr-un conector amplasat în partea superioară a echipamentului și configurația logică este realizată intuitiv printr-o interfață grafică cu utilizatorul.



Fig. 7. KUNBUS RevPI Connect

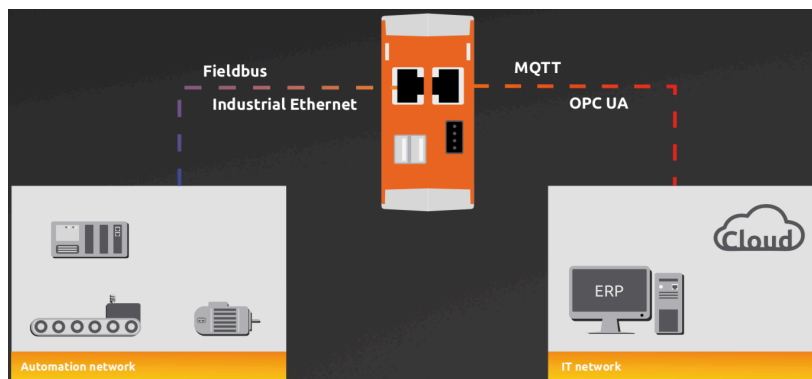


Fig. 8. Integreare rețea KUNBUS RevPI Connect

Tabelul 2. Specificații tehnice

Procesor	1.2 GHz Quad-Core
RAM	1 GB
Memorie Flash eMMC	4 GB
Tensiune de alimentare	12 – 24 V
Dimensiuni (L x l x h)	111 x 45 x 96 mm
Temperatură operare	-40 +55 C
Temperatură stocare	-40 +85 C
Umiditate	93%
Clasă de protecție	IP20
Protecție ESD	4 kV/8 kV
Teste EMI	Da – conform EN61131-2 și IEC 61000-6-2
Teste supratensiune	Da – conform EN61131-2 și IEC 61000-6-2

Tabelul 3. Interfețe de comunicare disponibile.

2 x RJ45 Ethernet
2 x USB 2.0
1 x Micro HDMI
1 x Micro USB 2.0 (doar pentru încărcare firmware)
1 x RS485 cu șuruburi (4 poli)
1 x PiBridge (pentru module de extensie RevPi)
1 x ConBridge (pentru module de extensie RevPi Con)
1 x 24 V pentru semnale de oprire de la un UPS
1 x Contact releu liber programabil

Implementarea comunicației dintre KUNBUS RevPi Connect și Controllerul Victron Color Control GX (CCGX)

Pentru realizarea aplicației de control predictiv al energiei într-o microrețea rezidențială este necesară integrarea gateway-ului IIoT cu echipamentul de control CCGX. Aceasta permite citirea valorilor măsurate și transmiterea comenzilor generate în urma rulării rutinelor de optimizare aferente MPC. Sunt identificate două modalități de integrare pentru care au fost identificate soluții software adecvate: în rețeaua locală prin protocolul ModBus TCP, la distanță prin internet folosind un API REST și cereri JSON sau prin protocolul MQTT.

1. ModBus TCP

Protocolul ModBus TCP este un protocol de comunicație industrială standardizat prin care se poate realiza integrarea echipamentului Victron CCGX cu alte echipamentele de automatizare (gateway IIoT, PLC, BMS, DCS) și dezvoltarea de aplicații complexe de control și optimizare [25].

Codurile de funcții ModBus suportate sunt:

- ReadHoldingRegisters = 3
- ReadInputRegisters = 4
- WriteSingleRegister = 6
- WriteMultipleRegisters = 16

Producătorul pune la dispoziție un fișier ce conține lista regiștrilor ModBus disponibili pentru fiecare familie de produse [26].

Codurile de eroare definite sunt:

Cod	Nume	Descriere
0x01	IllegalFunction	Funcția solicitată nu este disponibilă
0x02	IllegalDataAddress	Unit-id disponibil dar unul sau mai mulți regiștri nu există
0x03	IllegalDataValue	Cantitatea solicitată de regiștri este invalidă
0x0A	GatewayPathUnavailable	Unit-id definit în lista de mapare dar dispozitivul nu este găsit pe portul mapat.
0x0B	GatewayTargetDeviceFailedToRespond	Unit-id solicitat nu este găsit în lista de mapare.

Funcționalitatea ModBus este standard dezactivată pe sistemul CCGX. Serviciul Modbus TCP trebuie activat din meniul de configurare al echipamentului. Portul standard utilizat pentru comunicația ModBus TCP este 502. Unit-id-ul denumit și adresa slave specifică produsul conectat la CCGX ce se dorește a fi accesat. Tipurile de date utilizate sunt uint16 și int16, după primirea valorii solicitate, aceasta trebuie împărțită la factorul de scalare pentru obținerea valorii finale în unitățile specificate în tabel. Modalitatea de conectare prin ModBus TCP a echipamentului CCGX cu un alt echipament industrial de conducere este ilustrată în Figura 9.

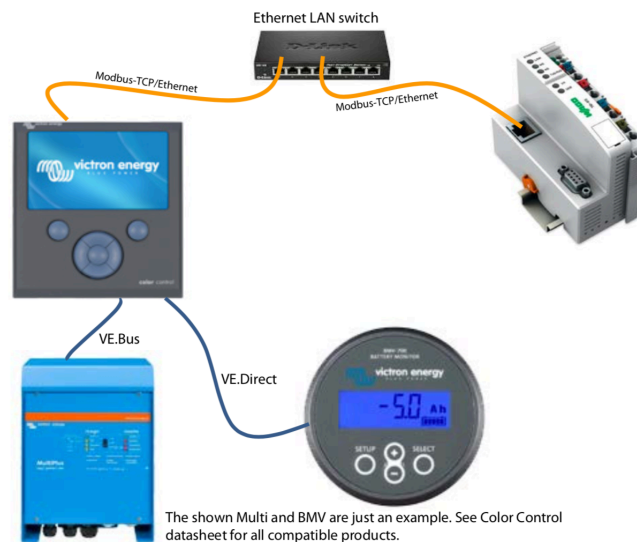


Fig. 9. Integrare CCGX - RevPI Connect prin ModBus TCP

2. VRMAPI

O alternativă la monitorizarea locală poate fi reprezentată de serviciul de monitorizare la distanță oferit de firma Victron Energy pentru echipamentele CCGX – Victron Remote Management (VRM). Acesta oferă o interfață de acces programatic la aceste sisteme printr-un API REST [26]. Pentru autentificarea prin VRM API este necesar un cont de client activ, se poate folosi același cont ca cel din platforma web VRM. Pentru autentificare este necesară o adresă de e-mail validă și o parolă. Odată ce validitatea credențialelor este verificată se generează un token web ce va fi utilizat ulterior pentru apelurile de date. Dacă acest token expiră un mesaj de eroare este returnat ceea ce conduce la solicitarea unui nou token cu datele de acces inițiale.

Cele două cazuri de utilizare pentru VRMAPI pot fi dezvoltarea unei aplicații front-end personalizate care folosește baza de date existentă a sistemului VRM sau colectarea/replicarea

datelor din baza de date VRM într-un sistem propriu complet. Adresa de bază a API-ului este:
<https://vrmapi.victronenergy.com>

Eroarea HTTP 429 este generată în cazul în care sunt depășite limitele prestabilite de rată de acces la date.

Autentificarea se realizează după cum urmează:

POST /v2/auth/login

```
{  
  "username": "john@example.com",  
  "password": "secret-passw0rd"  
}
```

Deconectarea se realizează prin comanda:

POST /v2/auth/logout

3. MQTT

DBUS-MQTT reprezintă un script python disponibil public pentru publicarea valorilor de pe magistrala D-Bus către un broker MQTT [6]. Scriptul suportă de asemenea cereri de la brokerul MQTT pentru modificarea valorilor de pe D-Bus. În varianta standard dbus-mqtt se va conecta la un broker MQTT Mosquito ce rulează pe echipamentul CCGX. Brokerul este disponibil în rețeaua locală la portul TCP 1883. Mai mult, brokerul este configurat să redirecționeze toate comunicațiile către brokerul Victron MQTT central (mqtt.victronenergy.com) care permite monitorizarea și controlul echipamentului CCGX prin internet [27].

Începând cu CCGX versiunea 1.70, dbus-mqtt este instalat standard dar nu este activat. Activarea se realizează prin Setări > Servicii.

Notificări

Atunci când se modifică o valoare pe D-Bus, scriptul va trimite un mesaj către broker. Subiectul MQTT are următoarea formă:

N/<portal ID>/<service_type>/<device instance>/<D-Bus path>

- Portal ID este identificatorul din portalul VRM asociat CCGX
- Service type reprezintă partea din numele serviciului D-Bus care descrie serviciul

- Device instance este un număr utilizat pentru a face serviciile de același tip unice (această valoare este publicată pe D-Bus ca /DeviceInstance)

Informația utilă din valoarea D-Bus este împachetată într-un dicționar și transformată în json. Mesajele sunt reținute de broker astfel încât va fi primit întotdeauna ultimul mesaj pentru fiecare subiect abonat.

Exemplu: Un invertor PC ce raportează o putere AC totală de 936W. Subiectul mesajului MQTT va fi:

Topic: N/e0ff50a097c0/pvinverter/20/Ac/Power
Payload: {"value": 936}

Cereri de scriere:

Sunt trimise pentru modificarea valorilor de pe D-Bus. Formatul este similar cu al unei notificări. Subiectul va începe cu W.

Exemplu: Pentru un sistem Hub-4 se poate schimba valoarea de referință AC-In cu mesajul:

Topic: W/e0ff50a097c0/vebus/257/Hub4/L1/AcPowerSetpoint
Payload: {"value": -200}

Cereri de citire:

O astfel de cerere va forța programul să trimită o notificare a unei valori D-Bus specifice. Formatul mesajului începe cu litera R.

Exemplu: Citirea puterii AC a unui inverotr PV prin publicarea:

Topic: R/e0ff50a097c0/pvinverter/20/Ac/Power
Payload: empty

Programul va răspunde prin mesajul:

Topic: N/e0ff50a097c0/pvinverter/20/Ac/Power
Payload: {"value": 926}

Referințe bibliografice

- [1] A. Spadafora, "IoT market to top \$1tn by 2025", 2018. Sursa online: <https://www.itproportal.com/news/iot-market-to-top-dollar1tn-by-2025/>
- [2] „Internet of Things market to triple to \$1.7 trillion by 2020: IDC”, 2016. Sursa online: <https://www.reuters.com/article/us-idc-research-idUSKBN0OI1NO20150602>
- [3] J. Hagel, J. Seely Brown, T. Samoylova, M. Lui, Raport 2 “From exponential technologies to exponential innovation”, 2013. Sursa online.
- [4] Strategia energetică a României pentru perioada 2007-2020.
- [5] M. Abomhara and G. M. Koiem, “Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,” *Journal of Cyber Security and Mobility*, vol. 4, no. 1, pp. 65–88, 2015.
- [6] M.Farooq,M.Waseem,A.Khairi,andS.Mazhar,“ACritical Analysis on the Security Concerns of Internet of Things (IoT),” *International Journal of Computer Applications*, vol. 111, no. 7, pp. 1–6, 2015.
- [7] D. Dragomir, L. Gheorghe, S. Costea, A. Radovici. “A Survey on Secure Communication Protocols for IoT Systems.” In *Proceedings - 2016 International Workshop on Secure Internet of Things, SIoT 2016*, 47–62.
- [8] T. Yanget al., "Applying blockchain technology to decentralized operation in future energy internet," 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), Beijing, 2017, pp. 1-5. doi: 10.1109/EI2.2017.8244418;
- [9] A. Goranović, M. Meisel, L. Fotiadis, S. Wilker, A. Treytl and T. Sauter, "Blockchain applications in microgrids an overview of current projects and concepts," *IECON 2017 - 43rd Annual Conference of the IEEE Industrial Electronics Society*, Beijing, 2017, pp. 6153-6158;
- [10] L. R. Rabiner. A tutorial on hidden markov models and selected applications in speech recognition. In *Proceedings of the IEEE*, pages 257–286, 1989.
- [11] V. S. Barbu, N. Limnios, *Semi-Markov Chains and Hidden Semi-Markov Models Toward Applications. Their Use in Reliability and DNA Analysis*. Springer, ISBN 78-0-387-73173-5, 2008.

- [12] Dodier RH, Henze GP, Tiller DK, Guo X. Building occupancy detection through sensor belief networks. *Energy and Buildings*. Vol 38, Issue 9, Pag. 1033-1043, 2006.
- [13] O. Ardakanian, S. Keshav. D. R. Cheriton, C. Rosenberg, Markovian Models for Home Electricity Consumption, SIGCOMM, 2011.
- [14] Comisia Europeană - Comunicat de presă, Comisia Europeană lansează Observatorul și forumul UE privind tehnologia blockchain, 2018.
- [15] Veena Pureswaran and Paul Brody. 2015. Device democracy: Saving the future of the Internet of Things. IBM Corporation (2015).
- [16] ITU-T Study Group 13, Next Generation Networks – Frameworks and Functional Models: Overview of the Internet of Things, International Telecommunication Union, Geneva, 2012.
- [17] J. Höller, et al., "From Machine-to-Machine to the Internet of Things." Academic Press, 2014.
- [18] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008). <https://bitcoin.org/bitcoin.pdf>
- [19] K. R. Özyılmaz, A Yurdakul, Work-in-progress: integrating low-power IoT devices to a blockchain-based infrastructure, 2017 International Conference on Embedded Software (EMSOFT), Seoul, 2017.
- [20] Bitcoin developer guide, <https://bitcoin.org/en/developer-guide#block-chain>
- [21] How technology is shaping the renewable energy sector, <https://www.ibm.com/blogs/blockchain/2017/12/how-technology-is-shaping-the-renewable-energy-sector/>, 2017.
- [22] D. Marušić, V. Lešić, T. Capuder and M. Vasak, "Price-Optimal Energy Flow Control of a Building Microgrid Connected to a Smart Grid," 2018 26th Mediterranean Conference on Control and Automation (MED), Zadar, 2018, pp. 1-9.
- [23] C. Galatsopoulos, S. Papadopoulou, C. Ziogou and S. Voutetakis, "Energy Management Strategy in a Residential Battery Energy Storage System," 2018 26th Mediterranean Conference on Control and Automation (MED), Zadar, 2018, pp. 831-836.
- [24] KUNBUS RevPI Connect Open Source IIoT Gateway, Disponibil on-line: <https://revolution.kunbus.com/revpi-connect/>

[25] Victron Energy, Data communication with Victron Energy Products, Disponibil on-line: https://www.victronenergy.com/upload/documents/Whitepaper-Data-communication-with-Victron-Energy-products_EN.pdf

[26] Victron Energy, VRM API v2 Documentation, Disponibil on-line: <https://vrmapi.victronenergy.com/v2/docs>

[27] DBUS-MQTT Script Readme, Disponibil on-line: <https://github.com/victronenergy/dbus-mqtt/blob/master/README.md>