Universitat de les Illes Balears

Escola Politècnica Superior

Memòria del Treball de Fi de Grau

Blockchain dins IoT

Antoni Rullan Pomar

Grau d'Enginyeria Informàtica

Any acadèmic 2017-18

DNI de l'alumne: 43208218G

Treball tutelat per Dr. Bartolomé Jaime Serra Cifre
Departament d'Informàtica i Matemàtiques

S'autoritza la Universitat a incloure aquest treball en el Repositori Institucional per a la seva consulta en accés obert i difusió en línia, amb finalitats exclusivament acadèmiques i d'investigació	Autor		Tutor	
	Sí	No	Sí	No
	X		X	

Paraules clau del treball:
blockchain, Internet of Things, smart homes, security, ethereum, smart contracts

Índex

1. Introducció 4
   1.1 Objectiu del treball 4
2. Internet of Things 5
   2.1 Origen 5
   2.2 Estructura 5
   2.3 Tecnologies de comunicacions 6
   2.4 Aplicacions 7
3. Smart Home 8
   3.1 Problemes de seguretat en smart home 10
4. Blockchain 12
   4.1 Fites 12
   4.2 Origen 12
   4.3 Concepte 13
   4.4 Algoritmes de consens 13
      4.4.1 PoW (Proof of Work) 14
      4.4.2 PoS (Proof of Stake) 14
      4.4.3 DPoS (Delegated Proof of Stake) 14
   4.5 Tipus de blockchain 15
   4.6 Problemes 15
5. Ethereum 17
6. Smart contract 18
   6.1 Definició 18
   6.2 Oracle 18
   6.3 Problemes 19
   6.4 Exemple d'aplicació 20
7. Cas pràctic 21
   7.1 Enunciat 21
   7.2 Metodologia 22
      7.2.1 Requisits 22
      7.2.3 Definició del prototip 22
   7.3 Contractes 23

7.4 Implementació 26
8. Visió de futur 27
8.1 Testeig de blockchain 27
8.2 Frenar la centralització 27
8.3 Analítica de big data 27
8.4 Aplicacions de blockchain 28
8.5 Millors algoritmes de consens (Algorand) 28
9. Conclusió 29
10. Bibliografia 30

1. Introducció

Internet de les Coses (IoT) és un concepte que es refereix a la interconnexió digital d'objectes quotidians amb Internet. El IoT ha experimentat un creixement molt gros aquest darrers anys, dels 6,3 bilions de dispositius connectats de 2016 s'ha passat a 8,3 i es calcula que pel 2020 ja haurà 20 bilions de dispositius connectats [1]. Aplicant IoT a un entorn com una ciutat o una casa s'aconsegueix transformar-la en "smart", on els dispositius recol·lecten i analitzen informació per automatitzar les seves funcions i facilitar la vida als usuaris.

El problema és que aquests dispositius, que estaran a les nostres cases en un futur, de moment no estan protegits contra atacs. En octubre de 2016, un proveïdor d'Internet americà va rebre múltiples atacs DoS. Es varen realitzar amb molts de dispositius del IoT infectats amb un virus informàtic, com impressores, càmeres de monitors d'infants, etc. Amb una càrrega de 1,2 Tbps és el major DDoS en la història [2]. Per realitzar un atac d'aquesta magnitud va ser necessari infectar desenes de milions de dispositius. Si varen poder aconseguir el control de tots aquests dispositius també poden robar la informació dels seus usuaris, i a una xarxa IoT pot haver-hi dispositius amb informació sensible. Imagineu tenir una casa intel·ligent, amb dispositius IoT com un càmera d'infants. Si algú aconseguís entrar en el dispositiu podria robar informació del vostre infant i veure el vídeo que transmet.

A part de aquest problema de seguretat, amb alguns dispositius del IoT hi ha un problema energètic. Tres quarts de les cases en Estats Units tenen aire condicionat i utilitzen un 6% de l'energia produïda del país. En total, cada any costa uns $29 bilions als usuaris i 117 milions de tones de carbó al medi ambient [3].

Els dos exemples anteriors serveixen per demostrar que fa falta una solució en l'entorn IoT que la protegeixi d'atacs externs i alhora permeti automatitzar les seves funcions per estalviar energia. En aquest document farem una reflexió sobre quina tecnologia seria l'adequada a utilitzar i farem un experiment d'implementació.

L'estructura que té aquest document és: en el capítol dos es veu l'estructura que té el IoT i un repàs d'algunes de les tecnologies de comunicacions que més utilitza. En el capítol tres es veu funcionalitats de les smart homes i alguns dels problemes de seguretat que tenen. En el capítol quatre s'explica que és i com funciona el blockchain, dues maneres de classificar-lo, segons el seu algoritme de consens o tipus de centralització, i alguns dels problemes que té la tecnologia. En el capítol 5 s'explica Ethereum i en capítol 6 els seus contractes intel·ligents. En el capítol 7 es veu un cas pràctic, un prototip de contracte per un climatitzador. En el capítol 8 es dóna una visió de futur de la tecnologia, reflexionant sobre alguns aspectes que s'haurien de millorar. En el capítol 9 s'expliquen les conclusions finals del treball.

1.1 Objectiu del treball

Aconseguir desenvolupar i implementar una sèrie de smart contracts damunt un blockchain que permetin automatitzar i protegir les funcions d'un climatitzador de una casa intel·ligent.

2. Internet of Things

El Internet de les Coses és la xarxa de dispositius físics equipats amb sensors que permeten recol·lectar dades, analitzar-les i intercanviar-les amb altres dispositius de la xarxa. Les "coses" refereixen dispositius com implants de monitorització, chips en animals, càmeres o cotxes amb sensors.

En aquest apartat veurem el origen del Internet de les Coses, una explicació de la seva estructura, exemples de tecnologies de comunicacions dins IoT i finalment un exemple d'aplicació.

2.1 Origen

El concepte d'una xarxa de dispositius smart va aparèixer per primera vegada l'any 1982 a la Carnegie Mellon University, on varen modificar un dispensador de Coca Cola per poder-se connectar a una xarxa i reportar el seu inventari i avisar de quan les begudes es refredaven [4]. Més tard, a l'any 1999 es va popularitzar el concepte amb la introducció de Radio-frequency identification (RFID) per Kevin Ashton gràcies a la seva aplicació per poder identificar objectes ràpidament i facilitar inventaris [5]. No va ser fins a l'any 2004 que va aparèixer el concepte que tenim avui en dia de IoT, on els dispositius són capaços de funcionar i intercanviar informació de forma automàtica [6]. En 2014 IoT era el primer en el "Gartner hype cycle" de tecnologies emergents [7].

Encara així, com a tecnologia emergent, IoT no té estandarditzada la seva estructura i hi ha moltes interpretacions de com hauria de ser l'arquitectura d'una xarxa IoT. A continuació veurem la estructura que ens pareix més adequada pels objectius d'aquest treball.

2.2 Estructura

En el IoT, cada capa està definida per les seves funcions i els dispositius que les utilitzen. Hi ha diferents opinions sobre el nombre de capes en el IoT, però segons molts investigadors, el IoT opera damunt 3 capes anomenades Percepció, xarxa i Aplicació [8]. En la figura 1 es pot veure l'arquitectura per capes. En el nostre cas, un sensor de temperatura, un bus de connexió i un dispositiu climatitzador representaria cada capa, respectivament.

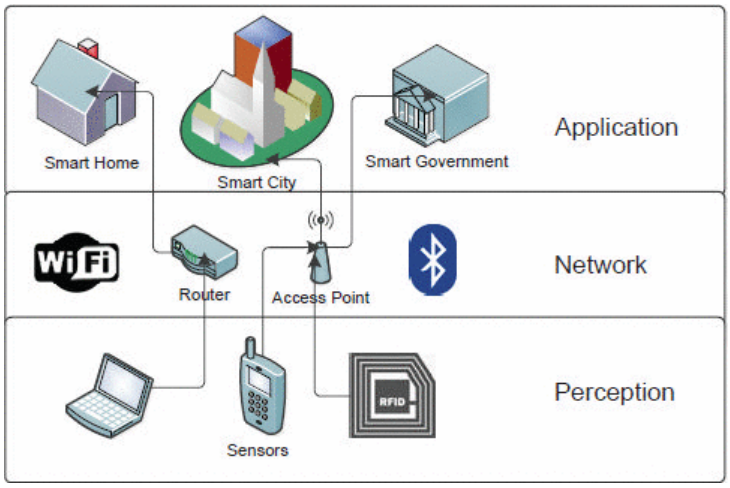

Fig 1. Capes de una xarxa IoT [9]

- Capa de percepció: la funció d'aquesta capa és adquirir dades de l'entorn amb l'ajuda de sensors. Així detecta, col·lecciona i processa informació i la transmet a la capa de xarxa [10].
- Capa de xarxa: la capa de xarxa del IoT fa la funció d'encaminar i transmetre les dades de diferents IoT hubs cap a la internet i viceversa. Els dispositius d'aquesta capa operen amb tecnologies recents com WiFi, LTE, Bluetooth, 3G, etc [11]. En aquesta capa
- Capa d'aplicació: aquesta capa garanteix l'autenticitat, integritat i confidencialitat de les dades. Així es compleix la creació d'un smart environament [12].

Ara que tenim definida l'estructura de la nostra xarxa IoT passarem a veure quina tecnologia de comunicacions podrem fer servir en la nostra capa de xarxa.

2.3 Tecnologies de comunicacions

Amb diferents tecnologies disponibles, els dissenyadors de dispositius IoT poden seleccionar diferents mètodes de comunicació i arquitectures. Depenent del seu objectiu es pot utilitzar la tecnologia que més convé. Les tecnologies disponibles més utilitzades són:

- **RFID**: Radio Frequency Identification és una tecnologia on la informació guardada en un microxip es pot llegir de forma remota. En radio frequency s'utilitzen varius rangs de freqüència com per exemple Low Frequency (LF, 125 kHz), High Frequency (HF, 13.56 MHz), Ultra High Frequency (UHF, 433 MHz, 860-960 MHz) i microones (2,45 GHz, 5,8 GHz). Algunes bandes es poden usar globalment (HF) mentre que altres són especifiques d'una regió (UHF en USA, EU i el Japó).
- **NFC**: Near Field Communication és una modalitat de RFID de curta distancia i alta frequencia (13,56 MHz) que permet intercanviar informació entre dos dispositius amb NFC. Gràcies a la seva simplicitat per establir connexió i accessibilitat es creu que en el futur serà una de les tecnologies de comunicació més utilitzades [13].
- **Bluetooth**: es basa en el Standard IEEE 802.15.1. És una tecnologia de baix consum i de baix cost adequada per transmissions entre dispositius mòbils amb curta distancia (8-10 m). Opera en la banda 2,4 GHz.
- **Wi-Fi**: IEEE 802.11 és una col·lecció de WLAN estàndards. Per exemple, 802.11a opera en la banda 5 GHz, mentre que 802.11g opera en la banda 2,4 GHz. Wi-Fi dona un rang de comunicació de 20 metres a interiors i 100 metres a exteriors.
- **ZigBee**: La ZigBee Alliance va desenvolupar una solució amb cost baix, molt poc consum per comunicacions d'alt nivell de radis digitals, com cases autònomes i dispositius mèdics de recol·lecció de dades. La seva poca potència permet transmissions de 10-100 metres amb línia de visió, amb una velocitat de 250 kbit/s, ideal per transmissions intermitent de dades des de un sensor.

Per les seves característiques, creiem que la tecnologia ZigBee seria la ideal a utilitzar en la nostra capa de xarxa. La nostra aplicació estarà basada sobre el entorn d'una casa intel·ligent però hi ha moltíssimes aplicacions possibles amb el IoT. A continuació veurem un exemple.

2.4 Aplicacions

Les aplicacions pel IoT són extensives. La habilitat de poder utilitzar dispositius amb poca capacitat de CPU, memòria i consum vol dir que es pot aprofitar en quasi tots els sectors [14].

Es podria fer un treball sencer sobre possibles aplicacions damunt IoT, però en el nostre s'ha decidit donar dos exemples: l'ús de dispositius wearable per un sistema sanitari i les smarts homes o cases intel·ligents, on elaborarem més en el següents apartats.

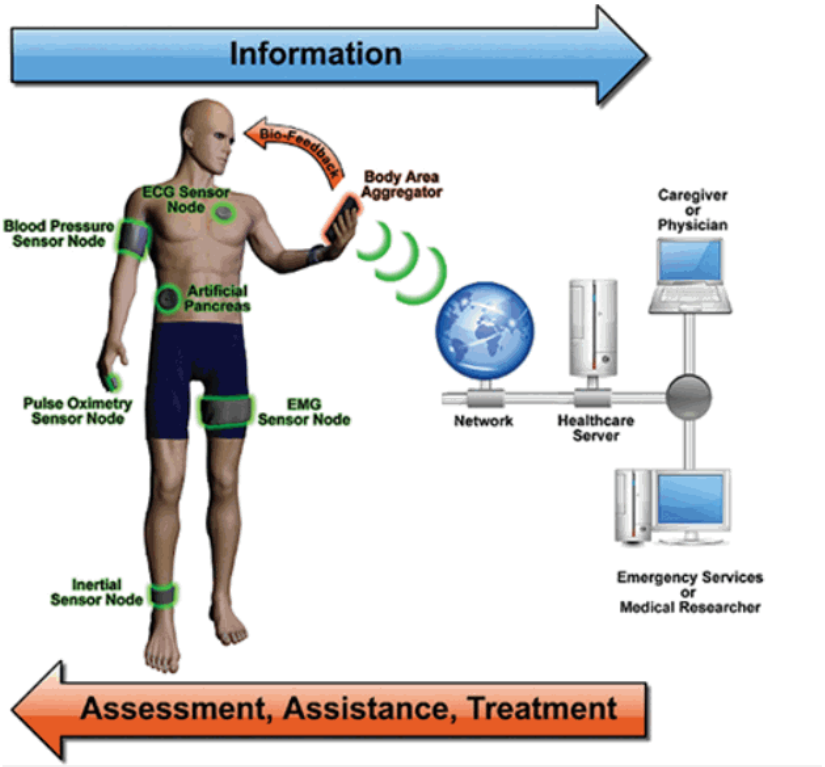

Fig 2. Sistema de recol·lecció de dades mèdiques amb IoT [15]

La figura 2 mostra un sistema que mesura les dades biològiques d'un usuari per ser enviades mitjançant internet als serveis sanitaris o serveis d'emergència. D'aquesta forma es pot tenir un flux automàtic de les dades del pacient i ell pot rebre feedback sobre el seu tractament.

Els sensors biològics representen la capa de percepció, la xarxa (composta per dispositius com encaminadors i punts d'accés) és la capa de xarxa i els serveis com el sanitaris o emergències representen la capa d'aplicació.

El nostre objectiu és implementar la solució dins l'altra exemple, on s'aprofita molt l'essència del IoT, que són les smarts homes o cases intel·ligents, on moltes funcions com el control de l'aire condicionat o geleres estan al càrrec de dispositius que formen part de la xarxa IoT.

3. Smart Home

En aquest apartat veurem el concepte de smart home i alguns dels problemes de seguretat que té.

El concepte de smart home es va originar per la dècada de 1970. En 1984, es va construir el primer edifici smart en Amèrica, marcant la realització del concepte de smart home. Avui en dia moltes cases de nova construcció ja es fan smart en Amèrica i altres països [16].

Una smart home representa l'essència del Internet de les coses, on les comunicacions entre xarxes, l'automatització i intel·ligència artificial estan integrades en la plataforma de les cases. Comparat amb les cases tradicionals, les smart homes, a més de tenir les funcions tradicionals per viure, també tenen interactivitat de la informació i l'avantatge d'estalviar energia amb la combinació de tecnologies. Tots els dispositius en les smart homes estan connectats al Internet de les Coses, permetent diverses funcions com el control de la llum, la calefacció, ventilació, seguretat; inclús electrodomèstics com rentadores, assecadors i geleres.

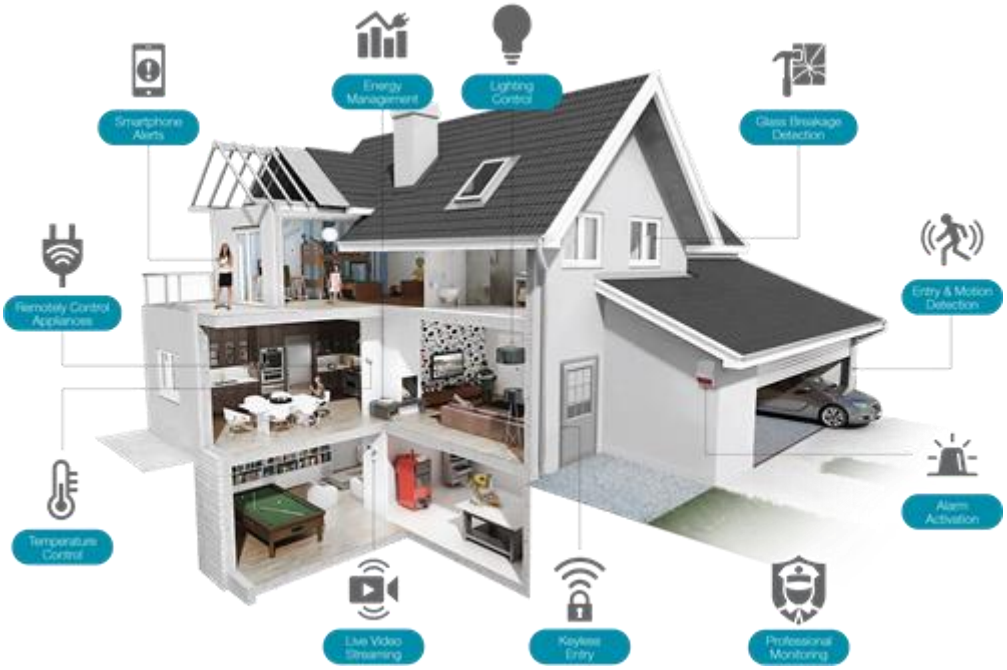

Fig 3. Funcionalitats de smart home [17]

En la figura 3 podem veure la majoria de funcions que pot fer una casa intel·ligent. A continuació descriurem algunes de les funcions:

1) La porta de la entrada se desbloquejarà amb l'empremta dactilar del propietari.
2) Les cortines de la casa se pujaran o baixaran segons la intensitat de la llum que mesuren els sensors.
3) Controlar la llum de la casa utilitzant un smart phone o un panell de control.
4) Climatització automàtica de les habitacions segons la temperatura i humitat que hi ha en aquell moment.

5) Detecció de fum i fugues de gas. El sensor de gas, en cas de fuga, automàticament tancaria la vàlvula. El sensor de fum podria avisar al serveis d'emergència en cas d'incendi.

Els sistemes de gestió generalment consisteixen de switches i sensors connectats a un hub central, anomenat "gateway" o unitat central, on es controla és sistema mitjançant una interfície d'usuari a través d'un dispositiu muntat a una paret, aplicació de mòbil o tablet, o interfície web a través de web services d'internet.

La figura 4 mostra l'estructura d'una casa intel·ligent. La unitat de control central s'encarrega de gestionar les funcions de la casa. És el nucli del sistema, i es comunica mitjançant Zigbee amb els nodes, switches i sensors de la casa. Així, amb Zigbee, coordina la temperatura, humitat, intensitat de la llum, alarmes i cortines. El sistema d'entrada i el panell de control es connecten amb la unitat central mitjançant Wi-Fi [18].

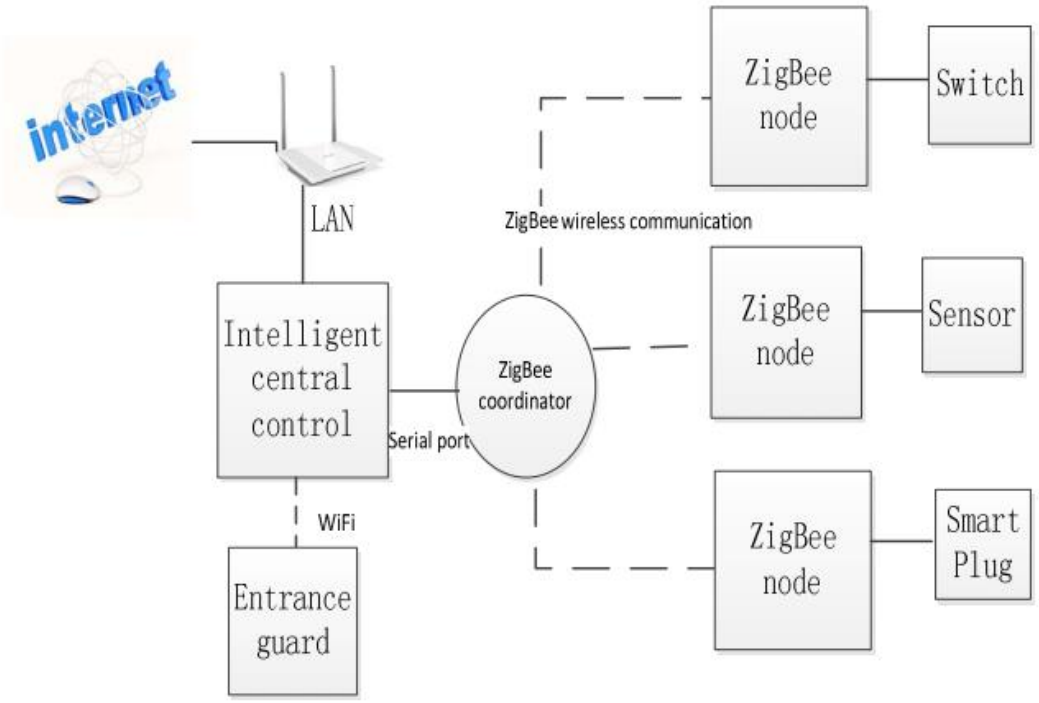

Fig 4. Estructura d'una smart home [19]

A pesar d'haver molts de venedors que ja ofereixen dispositius IoT, hi ha molt pocs estàndards acceptats en la indústria i el sector està molt fragmentat [20].

L'any 2014 el mercat de les smart homes estava valorat en $20.38 bilions, es prediu que en 2020 tindrà un valor de $58.68 bilions [21]. Un mercat amb una expansió tan gran de dispositius atrau l'atenció de persones amb males intencions que volen explotar les possibles vulnerabilitats del sistema, per tant en el següent apartat veurem alguns dels problemes de seguretat que pot haver-hi en una casa intel·ligent.

3.1 Problemes de seguretat en smart home

En un entorn smart home es pot controlar i monitorar aspectes de la casa com la llum, temperatura, finestres i portes. Aquests aspectes són possibles de controlar amb un smartphone. Per culpa de la connexió a Internet dels dispositius IoT que formen la smart home hi ha problemes de seguretat que s'han de considerar. Les smart homes contenen informació de caràcter privat de l'usuari, per tant és necessari implementar un sistema de seguretat.

Els 5 objectius més importants per assegurar la protecció d'una smart home [22] són:

- Autenticació: verificació de la identitat entre entitats que es comuniquen entre si.
- Autorització: assegurar-se que cada acció que pot fer un usuari tingui les limitacions que li correspon.
- Confidencialitat: només els usuaris autoritzats poden accedir a les dades privades del sistema.
- Integritat: assegurar-se que la informació es mantén consistent i precisa.
- Disponibilitat: assegurar-se que per qualsevol usuari amb autorització tots els serveis estaran disponibles i els recursos protegits davant atacs.

Complir els objectius és molt important per la seguretat de la casa, per encara així mai s'està 100% protegit davant alguns atacs. Hi ha molts de tipus de ciberatacs, s'ha decidit explicar les dues classificacions d'atacs amb un exemple de cada un. A una smart home pots rebre dos tipus d'atacs, passius i actius [23].

En els atacs passius l'atacant intenta aconseguir informació del sistema fora afectar els recursos. Així pot obtenir informació de la monitorització, dels missatges client/servidor fora que ningú es doni compte. Un exemple d'atac passiu és "eavesdropping", on l'atacant únicament monitoritza el tràfic de les dades que circula entre dos nodes d'una xarxa smart home. Aquí l'objectiu de l'atacant és saber quin tipus de transferència de dades hi ha a la xarxa i quin patró segueixen, sense ser detectat. Les dades que l'atacant captura poden contenir informació delicada. Per tant, accés a la informació delicada de l'atacant pot causar un gran perill a la xarxa [24].

En els atacs actius l'atacant utilitza la informació recol·lectada en l'atac passiu per i l'utilitza per poder canviar els recursos del sistema, modificar informació o alterar les seves operacions. Un exemple és el "Sybil attack". Aquest tipus d'atac és molt comú en l'escenari de les xarxes. Aquí l'atacant obté moltes adreces IP i MAC d'usuaris legals i suplanta la seva identitat. Després realitza activitat maliciosa damunt tota la xarxa i es mostra com un node que conté múltiples identitats als altres nodes [25].

Un exemple d'atac a gran escala és l'atac a Dyn, que va utilitzar el malware Mirai [26]. Va infectar dispositius del IoT que tenia les credencials d'administrador per defecte de forma silenciosa (atac passiu) per després controlar aquests dispositius per poder fer DDoS de forma sincronitzada (atac actiu). Gràcies a Mirai, que el codi està penjat a Internet, es va crear una entrada per accedir a molts de dispositius de IoT. Una vegada han aconseguit entrar, els atacants poden robar tota la nostra informació guardada en els dispositius de la nostra smart home i alguns contenen informació de caràcter sensible, com sensors biològics.

Com els dispositius del Internet de les Coses tenen poca potència de computació no podem usar solucions convencionals de seguretat, com una encriptació de les comunicacions entre dispositius. Hi ha solucions com la lightweight cryptography que tenen en compte aquest problema. Lightweight cryptography són uns algoritmes d'encriptació fet a mida pels dispositius amb restriccions com etiquetes RFID, smart cards, dispositius de seguretat social, etc. Són algoritmes amb menor eficiència d'encriptació i consum d'energia. Les propietats de LWC estan especificades en ISO/IEC 29192.

La LWC, a pesar d'oferir una bona protecció als dispositius IoT, no compleix l'objectiu d'automatització que volem aconseguir. Per aquesta raó, ara veurem la tecnologia que està darrera les criptomonedes, el blockchain. Presentarem les funcionalitats que la fan molt bona opció per protegir les smart homes, especialment la possibilitat de fer contractes intel·ligents per automatitzar les tasques d'un dispositiu IoT.

4. Blockchain

Hem vist l'arquitectura per capes del Internet of Things, les tecnologies de comunicacions disponibles, com funcionen les cases intel·ligents i alguns dels seus problemes de seguretat. Com a solució a aquests problemes proposem la tecnologia darrera les emergents criptomonedes, el blockchain.

En aquest apartat explicarem fites de la tecnologia blockchain, el seu origen amb la moneda bitcoin, el concepte de com funciona amb els nodes i blocs, els diferents tipus de blockchain que hi ha, com funciona i els diferents tipus d'algoritmes de consens que utilitza i els problemes actuals que té la tecnologia.

4.1 Fites

La tecnologia blockchain és una base de dades distribuïda que manté una llista de transaccions en constant creixement, anomenats blocs. Des de la seva aparició en 2008 s'ha viscut una sèrie d'innovacions en els darrers 10 anys. A continuació veurem 3 de les més importants:

- La primera innovació va ser el Bitcoin, un experiment de moneda digital. En el moment d'escriure això el market cap de bitcoin és de 145 bilions de dòlars i és usat per milions de gent per fer pagaments.
- La segona innovació va ser l'abstracció del blockchain. La tecnologia darrera el bitcoin es podia separar de la moneda i ser usada per diferents tipus d'aplicacions. Quasi cada institució financera del món està fent recerca sobre el blockchain i el 15% dels bancs ja usen blockchain al 2017 [27].
- La tercera innovació varen ser els "smarts contracts" o contractes intel·ligents. Integrats en un blockchain de segona generació anomenat Ethereum, que pot compilar petits programes directament en el blockchain que permeten per exemple a instruments financers com préstecs ser representats i no només monedes simples com bitcoin.

4.2 Origen

La primera aparició d'una cadena de blocs encriptada va aparèixer en 1991 en un document escrit per Stuart Haber i W. Scott Stornetta [28]. En 1992 varen incorporar arbres Merkle [29] al disseny, millorant la seva eficiència al permetre varius documents ser recol·lectats en un sol bloc [30]. En 2002, David Mazières i Dennis Shasha varen proposar un sistema de fitxers basat en xarxa descentralitzada similar a un proto-blockchain on els clients autoritzats poden sempre escriure, en els blockchains moderns nomes els clients que resolen un problema criptogràfic poden escriure un bloc. En 2005 Nick Szabo va proposar una espècie de blockchain per propietats descentralitzades i el seu sistema de pagament anomenat bit gold tenia implementat timestamping i proof-of-work, però era vulnerable al double-spending [31].

El primer blockchain modern va ser dissenyar per Satoshi Nakamoto en 2008. Va publicar un paper [32] al seu blog personal on explicava el seu funcionament i a l'any següent va treure una implementació com nucli de la moneda bitcoin.

4.3 Concepte

En el paper Nakamoto introdueix un sistema per validar les transaccions i ho defineix com una cadena de blocs. Cada bloc, com es pot veure en la figura 5, té les transaccions dels darrers 10 minuts, la seva representació hash SHA256, un contrapès pel hash anomenat nonce i el valor hash del bloc anterior, per poder formar la cadena.

Per un bloc ser vàlid ha de tenir un hash que comenci amb un nombre concret de zeros, determinat per la dificultat actual de la xarxa. És aquí on entra en joc el nonce, és un integer de 32 bits que fa la funció de contrapès per poder arribar a un hash vàlid. A aquest càlcul per poder trobar un nonce vàlid es coneix popularment com mining.

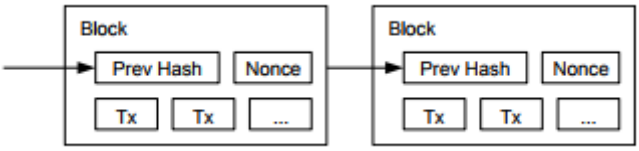

Fig 5. Encadenament de nodes [33]

El blockchain que proposa Nakamoto és de tipus distribuït. Cada node de la xarxa té una còpia del blockchain i quan un node aconsegueix trobar un hash vàlid per un bloc nou el retransmet a tota la xarxa [34].

En el cas que algú volgués modificar l'historial de transaccions té dos obstacles:

- Haver de recalcular el *nonce* del bloc a modificar i de tots els blocs més recents.
- Obtenir la majoria de la xarxa.

Per decidir quina còpia del blockchain serà la valida s'utilitza un mecanisme basat en els algoritmes de consens.

4.4 Algoritmes de consens

A les implementacions de blockchain, s'ha de resoldre dos problemes: el doble pagament i el problema dels generals bizantins.

El doble pagament significa reutilitzar la moneda en dues transaccions. Amb les monedes tradicionals no existeix el problema al fer una transacció. A les transaccions d'Internet el problema és resolt amb una institució intermèdia centralitzada. Blockchain resol aquest problema amb el mètode de verificar les transaccions amb els nodes distribuïts [35].

El problema dels generals bizantins és un dels principals problemes en el sistema distribuït. Les dades es poden rebre entre diferents nodes a través de comunicacions peer-to-peer. Malgrat això, alguns nodes poden ser atacats maliciosament, i duria canvis al contingut de les comunicacions. Els nodes normals necessiten poder distingir la informació que ha estat manipulada i obtenir resultats consistents amb els altres nodes normals.

L'algoritme de consens s'ha estudiat durant molts d'anys en el sistema distribuït [36]. A continuació s'explicarà els principis de diferents tipus d'algoritmes de consens.

4.4.1 PoW (Proof of Work)

PoW és l'algoritme de consens utilitzat en bitcoin. La idea principal és assignar els privilegis i recompenses a través de la competició de poder de hashing entre els nodes. Basat en la informació del bloc previ, cada node diferent calcula la solució especifica d'un problema matemàtic. És difícil resoldre el problema. El primer node que el resolgui pot crear el següent bloc i obtenir certa quantitat de bitcoin com recompensa [37].

Tots els nodes confien amb la cadena de blocs més llarga. Si algú modifica el blockchain, necessitaria controlar més del 50% del poder de hashing del món per assegurar-se ser el primer node a generar el nou bloc i controlar la cadena més llarga. Així el PoW garanteix efectivament la seguretat del blockchain [38].

4.4.2 PoS (Proof of Stake)

En PoS, la moneda digital té un concepte anomenat edat. L'edat de la moneda és el seu valor multiplicat pel període de temps després de ser creada. Com més temps passa, més privilegis tens en la xarxa. Propietaris de la moneda també obtenen certa recompensa segons l'edat. PoS limita el poder de hashing de cada node. La dificultat del mining és inversament proporcional a l'edat de la moneda [39].

PoS anima als propietaris de les monedes a augmentar l'edat. Amb el concepte de l'edat de la moneda, el blockchain no depèn només en el proof of work. La seguretat del blockchain utilitzant PoS millora quan augmenta el seu valor. Els atacants necessitarien acumular una gran quantitat de monedes i mantenir-les el suficient per atacar el blockchain. Això dificulta bastant fer un atac [40].

4.4.3 DPoS (Delegated Proof of Stake)

En la fase inicial de disseny de bitcoin, Satoshi Nakamoto esperava que tots els participants poguessin utilitzar la CPU per minar. Així el poder de hashing de tots els nodes era similar i tots tindrien l'oportunitat de participar en les decisions del blockchain. Amb el desenvolupament de la tecnologia i l'apreciació del bitcoin, s'han inventat màquines específiques per fer mining. El poder de hashing està agrupat en els participants que tenen moltes d'aquestes maquines. Els miners ordinaris rarament tenen l'oportunitat de crear un bloc. El blockchain que utilitza DPoS és més eficient amb l'energia que PoW i PoS [41].

A part de poder ser classificats pel seu algoritme de consens, un blockchain pot ser classificat pel tipus de centralització que utilitzen, que veurem a continuació.

4.5 Tipus de blockchain

Els tres tipus més coneguts de blockchain són blockchain públic, blockchain de consens i blockchain completament privat.

En el cas del blockchain públic, no hi ha cap autoritat central que tingui més poder que la resta. Aquí tothom es lliure d'entrar i sortir quan vulguin. La blockchain és oberta públicament i tothom té el dret de poder validar una transacció. En el cas de bitcoins són els miners qui validen les transaccions. Obtenen bitcoins amb tasses de transaccions i amb l'esforç que fan per resoldre el proof of work [42].

En el cas del blockchain de consens, no tothom té els mateixos drets per validar transaccions. Només a certes persones se lis dona el privilegi de validar-les. Aquestes han d'arribar al consens.

Una versió diferent del tipus de consens són els blockchains privats. Tenen una estructura centralitzada. Una sola entitat té el poder sobre les decisions i el procés de validació. Aquesta figura s'assegura que el consens que se segueix és el mateix que es proposa.

El blockchain públic també se'l coneix com blockchain sense permisos mentre que els altres dos entren dins la categoria de blockchain amb permisos. Els blockchain amb permisos són més ràpids, més eficients amb energia i més fàcil d'implementar comparats amb els que no tenen permisos. Els algoritmes basats amb blockchain amb permisos són els més usats i més aplicacions estan sent desenvolupades per ells [43].

4.6 Problemes

Blockchain té un potencial enorme. No obstant això, alguns experts asseguren que la tecnologia està sobrevalorada, no és suficient madura encara, o s'aplica a casos on es podria utilitzar una tecnologia ja dominada [44].

Els que desitgin implementar aquesta tecnologia haurien de saber sobre els problemes no resolts i les noves necessitats, i tenir present que blockchain podria no ser la solució optima, ja que els seus avantatges varien de sector a sector i d'un ús a un altre. Blockchain també té present alguns inconvenients, els quals haurien de ser avaluats minuciosament abans de decidir adoptar-lo.

A continuació s'explicarà els principals problemes de blockchain, des de problemes energètics a problemes legals:

1) Té un gran consum energètic. Per exemple, una transacció bitcoin podria costar $6 en considerar l'energia consumida pels nodes de la xarxa. Cada segon, hi ha una mitja de 2100 transaccions en la xarxa. Si el cost energètic puja, també puja les emissions de carbó al medi ambient. El minat de bitcoin consumeix, com a mínim, tanta energia en un any com Irlanda (24 TWh) [45].
2) El mining s'ha especialitzat molt. Ja estam molt enfora de la visió d'en Sakamoto de que cada node serien entitats independents. Avui en dia, per poder minar i treure un profit, necessites hardware poc accessible.

3) Mining requereix hardware costós, i la majoria del poder computacional és malgastat. El mining de blocs és una competició entre els nodes on el més ràpid guanya (els altres només malgasten recursos). Per augmentar la probabilitat de guanyar, els nodes poden unir-se a grups col·lectius, anomenats pools, i col·laborar amb altres nodes, repartint-se el benefici. Una solució per reduir la quantitat necessària de poder computacional seria canviar de PoW a PoS [46].
4) La mida en constant creixement d'un blockchain s'està convertint en un problema. Bitcoin, per exemple, ha crescut fins als 167GB a maig de 2018. Aquest creixement descontrolat del blockchain serà un problema en el futur, ja que alguns discs durs podrien ser massa petits per guardar tot l'historial del blockchain i fer un recorregut a través de les transaccions podria tornar-se molt lent.
   Ja hi ha alguns clients en vàries plataformes blockchain (bitcoin inclòs), que no guarden tota la cadena localment si no depèn en una tercera entitat per enviar-li els blocs que necessiten. Hi ha molts de problemes amb aquests clients, principalment problemes de seguretat, ja que tornen a confiar en una autoritat central. Els coneixements d'aquests clients sobre el blockchain és basat en la confiança d'una tercera entitat, mentre que la base conceptual de blockchain és confiança distribuïda [47].
5) Afegir informació no és ràpid. Crear i consolidar un bloc bitcoin tarda entre 10 a 60 minuts. Ethereum requereix 15 segons, una quantitat més petita però encara significant [48].
6) La immutabilitat i transparència podria fer mal a la privacitat dels usuaris i la seva reputació. Cada node de la xarxa podria guardar una còpia del blockchain i possiblement accedir al seu contingut. Per altra banda, la nova regulació GDPR de dades de la Unió Europea, que entra en vigor en maig de 2018, obliga a les companyies a respondre positivament a les sol·licituds dels usuaris per eliminar les seves dades de les bases de dades de la companyia. Per culpa de la immutabilitat del blockchain aquesta tasca és impossible, és a dir, el blockchain estaria incomplint la llei [49].

Per poder fer aplicacions en un blockchain, necessitem una plataforma que ofereixi un entorn per programar. Hi ha moltes criptomonedes [50] que han implementat la possibilitat d'escriure contractes intel·ligents en el seu blockchain. En el nostre cas hem decidit per utilitzar la plataforma més popular, Ethereum.

5. Ethereum

Proposat per Vatalik Buterin en el 2013, Ethereum és una plataforma basada en blockchain distribuït [51]. Gràcies a que té diversos llenguatges propis de programació, com Solidty [52], permet als developers escriure i compilar programes que poden córrer damunt una Ethereum Virtual Machine (EVM). Una vegada compilat el codi es tradueix a opcode i després a binari, permetent ser executat en l'entorn. Així Ethereum aconsegueix combinar un sistema de computació amb blockchain. Gràcies a la naturalesa del blockchain, els usuaris que escriguin el codi tenen la garantia que no serà manipulat i es comportarà com s'espera.

La EVM representa el cor de Ethereum, on s'executa el codi de les aplicacions. Cada node de la xarxa executa la EVM i les mateixes instruccions. Per aquesta rao Ethereum es descriu moltes vegades com un "ordinador mundial" [53]. Aquesta massiva paral·lelització de la xarxa Ethereum no es fa per fer-la més eficient en termes de velocitat de computació. De fet, la fa més lenta i més costosa que un "ordinador tradicional". A canvi, tenim una xarxa a prova d'errors, amb zero temps de caiguda i fa que les dades dins el blockchain no es puguin canviar mai.

El codi no pot ser modificat dins el blockchain però si es pot consultar, això permet consultar contractes, fer serveis d'apostes o de votacions. Les votacions poden ser fàcilment implementades amb la seguretat que no es podrien falsificar o manipular. Gràcies a això, moltes companyies estan intentant trobar usos a Ethereum [54].

Ether és la moneda que representa Ethereum. S'utilitza per pagar "gas", una unitat de computació que s'utilitza en les transaccions. Aquesta moneda es confon amb Ethereum, que és la plataforma. Com les altres criptomonedes la validesa de cada ether es proporciona per un blockchain. Ether és diferent de Bitcoin en diversos aspectes:

- El temps per generar un bloc són 14 o 15 segons, comparat amb els 10 minuts de bitcoin.
- El mining de ether genera noves monedes a una ràtio consistent, mentre que bitcoin la ràtio baixa un 50% cada 4 anys.
- Les taxes de transacció es calculen per complexitat computacional i ús de l'amplada de banda, en bitcoin es calculen per la mida de transacció en bytes. Per aquesta raó les taxes per ether són considerablement més petites que les de bitcoin. En desembre de 2017, la taxa de transacció mitjana de ether eren $0,33, mentre que amb bitcoin eren $23.
- Ethereum té planejat passar-se a Proof-of-stake. És un algoritme on el creador del següent bloc del blockchain és triat per una combinació de selecció aleatòria i riquesa o antiguitat. En contrast, l'algoritme de Proof-of-work de bitcoin utilitza puzles d'alta intensitat computacional per validar les transaccions i crear nou blocs.

Ethereum és una plataforma de computació distribuïda, el que significa que totes les entitats que participen contenen parts del blockchain de Ethereum. Així sabem que les transaccions són executades i guardades amb un algoritme consensual. Aprofitant aquesta característica podem construir un sistema IoT que és suficientment robust per aguantar atacs de denegació de servei i falsificació d'informació. Amb aquest sistema experts creuen que es poden sincronitzar centenars de dispositius [55].

El codi que permet fer Ethereum són els contractes intel·ligents o smart contracts. Un contracte intel·ligent és anàleg a una classe de programació orientada a objectes. A continuació veurem més en detall com funcionen.

6. Smart contract

En aquest apartat explicarem que són els smarts contracts, definició de oracle, problemes dels smarts contracts i un exemple d'ús.

6.1 Definició

Un smart contract és un mecanisme d'intercanvi controlat digitalment i autònomament que pot fer operacions amb entitats que no confien entre si. Un exemple serien dues entitats que realitzen una aposta per un partit de futbol, posen els diners en un compte neutral controlat pel smart contract i quan acaba el partit el contracte seria capaç de verificar qui ha guanyat i pagar automàticament al guanyador. Aquest intercanvi quedaria enregistrat dins el blockchain, així és assegura la seva autenticitat i la seva protecció.

Una possible aplicació dels smarts contracts és l'automatització dels dispositius de les smart homes. Un sensor de temperatura podria formar un contracte amb l'aire condicionat, de tal forma que quan hi ha un canvi de temperatura s'aplica el canvi de forma automàtica i la transacció queda protegida dins el blockchain.

Gràcies a això es poden crear polítiques d'ús. Per exemple es pot programar que un dispositiu canviï a mode estalvi d'energia quan supera un consum de 150 KW. Quan l'usuari envia la configuració a través d'un smartphone, les dades s'envien a la xarxa Ethereum. De mentre, dispositius com làmpades o aire condicionats obtenen periòdicament valors de la política des de Ethereum. Un mesurador obté el consum d'energia del dispositiu i ho envia a Ethereum.

6.2 Oracle

A un sensor en el contexte de smart contract se li diu oracle. És un agent que troba i verifica ocurrències en la vida real i envia la informació al blockchain. Els smart contracts contenen valors i només els desbloquegen quan certes condicions són complides. Quan s'arriba a un determinat valor, el smart contract canvia el seu estat i executa els algoritmes definits, activant de forma automàtica un event al blockchain. La tasca dels oracles és proveir els valors al smart contract de forma segura. Alguns exemples de valors són temperatures, pagaments exitosos, fluctuacions de preus, etc. [56]

6.3 Problemes

La Ethereum Virtual Machine està basada amb piles amb una mida de paraules de 256 bits, i cada instrucció opera amb operadors de 256-bit. La raó va ser per facilitar l'esquema hash Keccak-256 i computacions de corba el·líptica [57].

La majoria de dispositius IoT utilitzen arquitectures de 8, 16 o 32 bits. El típic és que el codi d'una aplicació IoT consisteixi d'operacions de 16 o 32 bits. Per conseqüència, les operacions de 256-bit de Ethereum crearien un sobrecost gran amb l'execució dins els dispositius IoT. Suportar operacions de 256 bits implicaria un cost computacional extensiu, que es pot veure a la figura 6 que dóna el nombre de cicles de rellotge requerits per executar vàries operacions de 8, 16, 32 i 64 bits, i operacions que suportin el tipus "big number"(incloent-hi 256 bits) [58].

Operation	Clock Cycles				
	8bit	16bit	32bit	64bit	Big Number[2]
Add	9	16	28	72	1159
Compare	12	21	37	90	298
Multiply	12	24	103	368	2666
Assignment	3	6	12	17	1077

Fig 6. Cicles requerits per executar varies operacions [59]

Els smarts contracts no poden dependre de APIs externes. Cada node hauria de ser capaç de processar les transaccions prèvies i acabar amb el mateix resultat que els altres nodes. La informació hauria de ser immutable. En conseqüència, les dades requerides per un smart contract haurien de ser primer injectades dins el smart contract. Els oracles podrien permetre aquesta injecció, però requeriria un sistema de reputació sòlid o un mecanisme de govern tan robust com el mateix blockchain, per no tornar-se la part més dèbil del procés [60].

Els smart contracts poden tenir errors del programador. Ja que el seu codi és públicament disponible i es tornen entitats autònomes una vegada són creats, poden ser "caramels" per hackers. Quan es guarda dins el blockchain, un smart contract ja no es pot modificar. Per eliminar errades en el codi, els programadors han de crear nous smart contracts i transferir totes les dades i punters dels antics als nous. L'atac basat amb smart contracts més impactant va passar dins Ethereum en juny de 2016, quan es varen robar $60 milions [61].

6.4 Exemple d'aplicació

Experts ja teoritzen sobre l'aplicació de smart contracts per automatitzar l'entorn de IoT. Un exemple és la màquina virtual AlkylVM, que permet als dispositius amb recursos limitats interactuar amb sistemes blockchain [62].

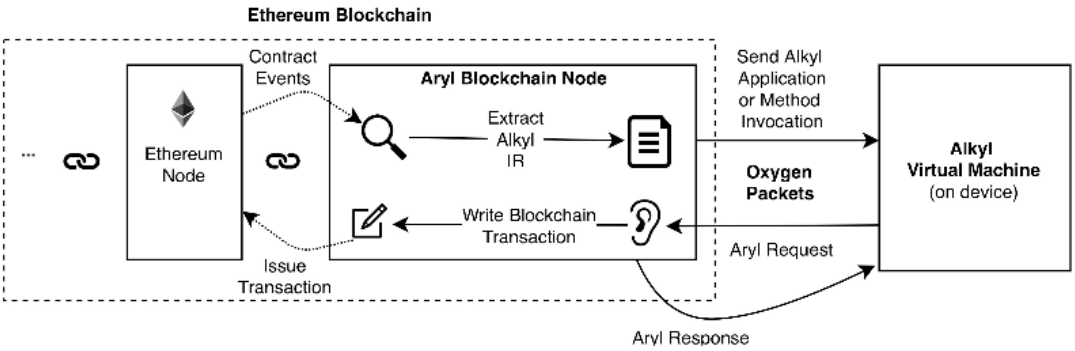

Fig 7. Arquitectura de AlkylVM [63]

La figura 7 mostra l'arquitectura del exemple. El Aryl Blockchain Node actua com porta d'enllaç entre el blockchain i els dispositius IoT connectats. Cada dispositiu connectat executaria una instancia de la Alkyl Virtual Machine, que permet programabilitat de cada dispositiu al comunicar-se amb el seu node. El canal de comunicació entre el node i la màquina virtual és necessari que sigui de confiança.

7. Cas pràctic

Ara que hem com funcionen els contractes intel·ligents es farà un exemple d'implementació per poder complir l'objectiu del projecte, protegir i automatitzar el climatitzador d'una casa intel·ligent.

7.1 Enunciat

L'objectiu d'aquesta demostració és crear una solució IoT composta de sensor, dispositiu i bus intermediari que funcioni damunt un blockchain. La idea és fer una sèrie de smart contracts per poder protegir i automatitzar un aire condicionat d'una casa intel·ligent, com per exemple l'edifici Ca ses Llúcies de la UIB, que es mostra en la figura 8.

Fig 8. Edifici Ca ses Llúcies en construcció

Com encara no podem implantar la solució dins la casa farem un exemple amb la màquina virtual de Ethereum (EVM) i després veurem diferents formes de desplegar i utilitzar els contractes dins un blockchain.

Hi ha diverses formes de escriure codi Solidity, el llenguatge d'ethereum que utilitzarem per la pràctica. Per aquest cas pràctic utilitzarem un entorn de desenvolupament basat en web anomenat Remix. Permet fàcilment escriure smart contracts i arrancar-los des de la web. Per desplegar els contractes provarem diferents eines, com la plataforma Pragma i l'aplicació Geth.

A continuació veurem la metodologia que utilitzarem per realitzar aquest cas pràctic, el model de prototips.

7.2 Metodologia

Per realitzar l'experiment ens hem decantat per la metodologia de model de prototips [64]. És mètode de desenvolupament de sistemes on es construeix, es fa proves i es remodela tantes vegades com faci falta fins que s'aconsegueix un prototip acceptable que permetrà completar el desenvolupament del producte final. Aquest model funciona en escenaris on no es coneixen tots els requeriments del projecte en detall. És un procés iteratiu, de prova i error. En la figura 9 es poden veure les etapes de la metodologia.

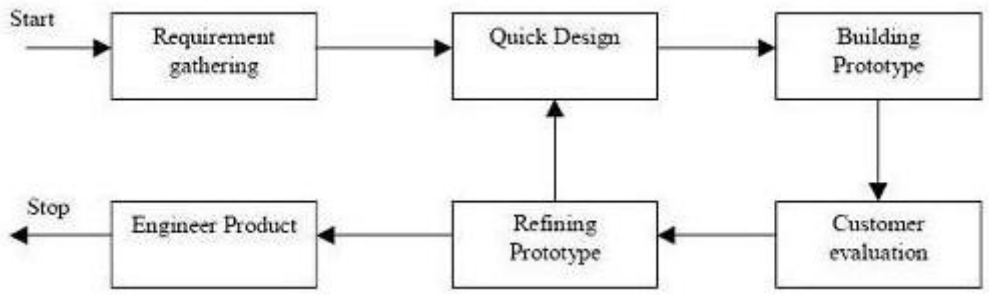

Fig 9. Model de prototip [65]

En el nostre cas, com fem feina en un entorn molt punter com les cases intel·ligents i blockchain, i només volem realitzar un prototip per demostrar com podria ser una solució final, aquest mètode pensem que és el més adequat.

7.2.1 Requisits

L'objectiu és desenvolupar i implementar una sèrie de smart contracts damunt un blockchain que permetin automatitzar i protegir les funcions d'un climatitzador de una casa intel·ligent. Per això, el prototip ha de:

- R1: Un contracte ha de controlar la temperatura del climatitzador. Ha de poder posar-lo més calent o més fred.
- R2: Un contracte ha de simular la funció d'un sensor de temperatura.
- R3: per R1 i R2, ha de haver un canal de comunicacions entre els dos.
- R4: El contracte del climatitzador ha de canviar de forma automàtica la temperatura segons la lectura del sensor.
- R5: Els contractes han de estar desplegats en un blockchain.
- R6: El blockchain ha de tenir un algoritme de consens que protegeixi la xarxa, que permeti crear una confiança entre els dispositius.

7.2.3 Definició del prototip

El prototip comptarà amb tres mòduls: un sensor, el dispositiu climatitzador i un canal de comunicacions entre els dos. La simulació del dispositiu i el sensor es farà amb unes Raspberry Pi. Utilitzaran una aplicació per poder accedir a un blockchain de proves i poder desplegar i consumir contractes intel·ligents.

7.3 Contractes

El exemple té 3 mòduls:

- Un **sensor** que agafa la temperatura d'una habitació. Per efectes pràctics la temperatura és introduïda per l'usuari, simulant una lectura automàtica d'una habitació.

```
contract Sensor {

    uint public temp;

    function set(uint _temp) public returns(bool success) {
        temp = _temp;
        return true;
    }

}
```

Fig 10. Contracte del sensor

- Un **bus** per accedir al sensor des del dispositiu.

```
contract Bus {
    uint public temp;
    function set(uint _temp) returns(bool success) {}
}
```

Fig 11. Contracte del bus

- Un **dispositiu** que segons la temperatura que llegeix el sensor pot augmentar o disminuir la temperatura que emet.

```
contract Device {

    uint private deviceTemp = 25;
    uint private roomTemp;
    address addressSensor;

    event Instruction(string instruction);

    function Device(address SAddress) {
        addressSensor = SAddress;
    }

    function getRoomTemp() public constant returns(uint Sensor) {
        Bus b = Bus(addressSensor);

        roomTemp = b.temp();

        if (roomTemp < deviceTemp){
            Instruction("HOTTER");
        }
        if (roomTemp > deviceTemp){
            Instruction("COLDER");
        }

        return roomTemp;
    }

    function getDeviceTemp() public constant returns(uint Device) {
        return deviceTemp;
    }

}
```

Fig 12. Contracte del dispositu

Per provar la solució s'han de desplegar els tres contractes al blockchain. A l'hora de desplegar el dispositiu s'ha d'introduir l'adreça del sensor perquè puguin estar lligats entre si. Una adreça en Ethereum és un identificador d'un smart contract, per poder-se enviar informació entre si.

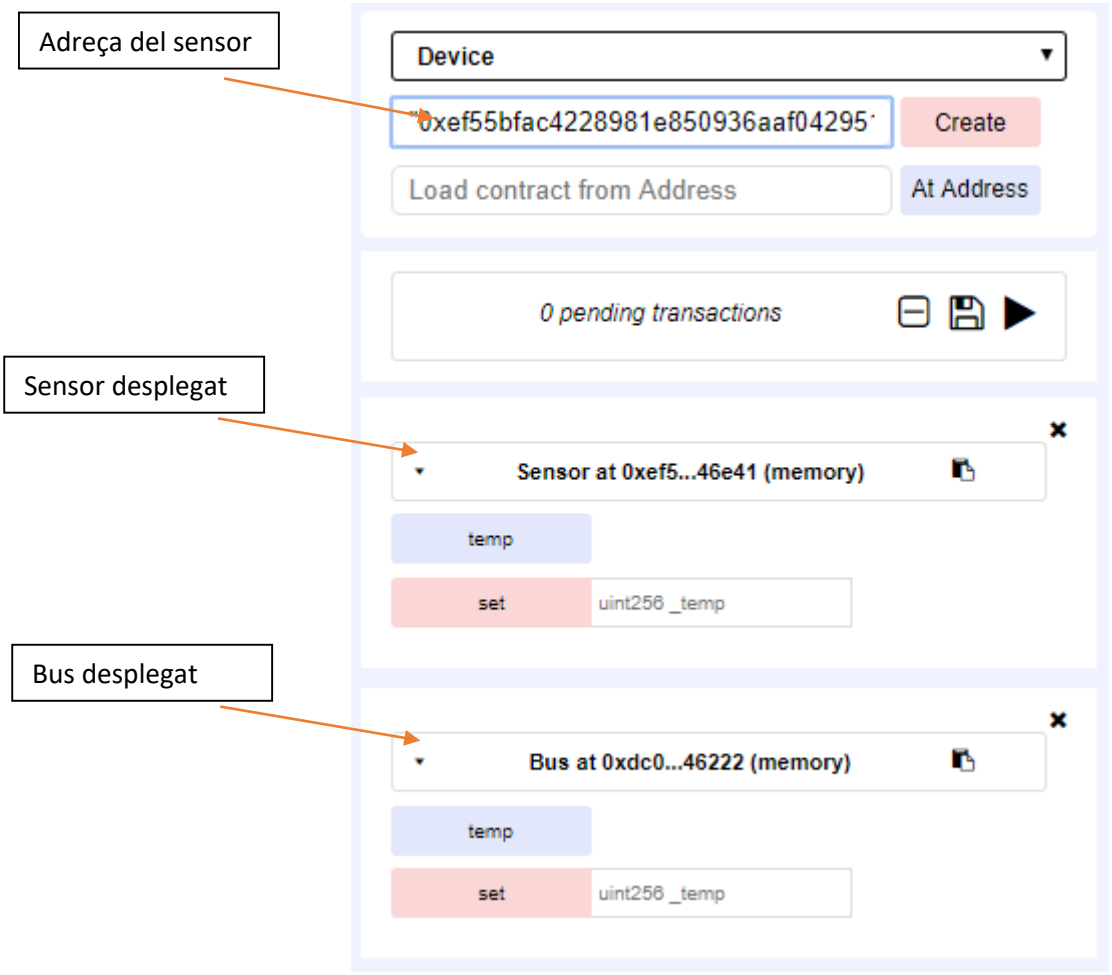

Fig 13. Desplegament dels contractes

Per demostrar el seu funcionament introduirem una lectura de 23 graus al sensor.

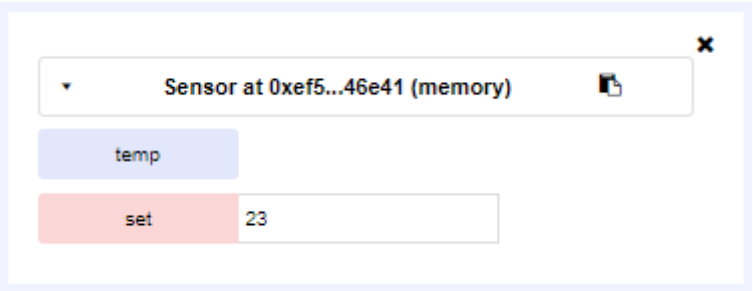

Fig 14. Simulació de lectura del sensor

Aquí podem veure que la transacció s'ha dut a terme dins el blockchain.

status	0x1 Transaction mined and execution succeed
from	0xca35b7d915458ef540ade6068dfe2f44e8fa733c
to	Sensor.set(uint256) 0xef55bfac4228981e850936aaf042951f7b146e41
gas	3000000 gas
transaction cost	41723 gas
execution cost	20259 gas
hash	0x3848e237d0382648d6e101234596041fa8199d42d40f60dda3da618a0d18f686
input	0x60fe47b1000000000000000000000000000000000000000000000000000000000000000017
decoded input	{ "uint256 _temp": "23" }
decoded output	{ "0": "bool: success true" }
logs	[]
value	0 wei

Fig 15. Transacció per escriure la nova temperatura al blockchain

I ara obtindrem la temperatura des del dispositiu.

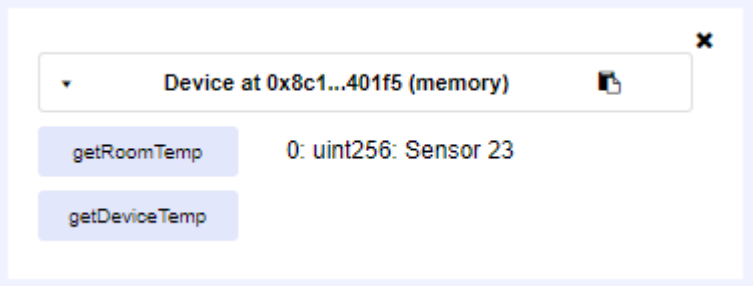

Fig 16. El dispositiu obté la temperatura

En aquest cas com que la temperatura és més petita que la desitjada el dispositiu hauria d'emetre aire més calent.

Per poder simplificar l'exemple s'ha utilitzat una lògica molt senzilla, però es podria complicar tant com es desitges. L'objectiu de l'exemple era demostrar com es podria automatitzar dispositius d'una xarxa IOT amb la protecció "by design" que té el blockchain. A continuació veurem com podem desplegar els contractes al blockchain.

7.4 Implementació

A l'hora d'implantar el exemple del apartat anterior primer es va optar utilitzar una Raspberry Pi per interactuar amb el blockchain.

Existeix una versió del blockchain de Ethereum per proves anomenat Rinkeby [66]. Hem triat aquesta ja que per desplegar dins el blockchain fa falta pagar "gas", que vindria a ser com cèntims de ether. En Rinkeby pots aconseguir 3 ETH per fer proves amb la següent referència [67].

Per interactuar amb qualsevol variant de Ethereum hi ha un programa de línia de comandes anomenat Geth. Provant l'aplicació ens vàrem adonar compte del problema que hi ha utilitzant una blockchain destinat al sector monetari. Amb Geth, per poder desplegar o utilitzar contractes en el blockchain abans se l'ha de descarregar tot. Una sincronització des de 0 pot arribar a tardar mes de 3 dies sencers, i això amb un ordinador decent. Si es fes amb una Raspberry estaria molt més. Per poder desplegar els contractes vàrem cercar alternatives i vàrem arribar a Pragma [68].

Pragma és una plataforma online que et permet escriure smart contracts, desplegar-los al blockchain i interactuar amb ells. Gràcies a Pragma vàrem penjar els contractes al blockchain i es poden consultar amb un explorador com Etherscan, per exemple en el següent enllaç es pot accedir al contracte del sensor i veure el seu codi. Per poder interactuar amb ells s'introdueix l'adreça del contracte i automàticament apareixen les funcions disponibles, en la figura 17 es poden veure les funcions del dispositiu.

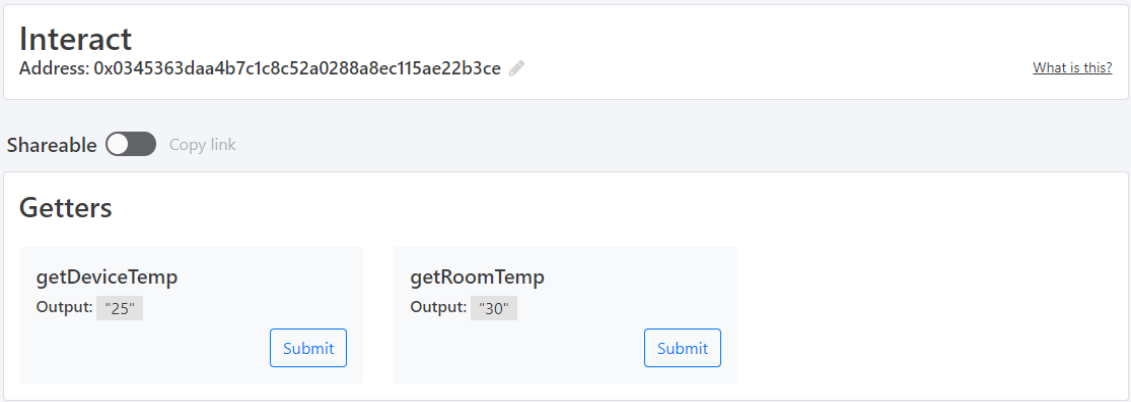

Fig 17. Funcions del contracte Device

A l'hora de voler utilitzar aquesta solució en una smart home, tindríem el problema de què cada vegada ens hauríem de sincronitzar amb una blockchain que té nodes que no ens interessa i duria molt de temps. Per tant lo ideal seria utilitzar una implementació feta a mida d'un blockchain privat que funcioni amb Proof of Stake, per poder validar a mà els nodes inicials i així crear una confiança en la xarxa. La nostra implementació només hauria de complir dos requisits: automatització dels nodes amb smarts contracts i ser una xarxa de confiança on no puguin incorporar-se nodes maliciosos.

8. Visió de futur

Blockchain ha mostrat el seu potencial a la indústria i acadèmia. En aquest apartat veurem possibles direccions de futur en cinc àrees diferents.

8.1 Testeig de blockchain

Recentment diferent tipus de blockchain han aparegut i hi ha més de 700 criptomonedes llistades [69]. No obstant això, alguns developers poden falsificar el rendiment del seu blockchain per atraure inversors motivats per gran èxit que té. Addicionalment, quan els usuaris volen combinar blockchain amb negocis, han de saber quin blockchain s'adapta als seus requeriments. Per tant, es necessita un mecanisme de testeig per provar diferent blockchains.

El testeig de blockchain es podria separar en dues fases: fase d'estandardització i fase de testeig. En la fase d'estandardització, s'han de fer i acordar tots els criteris. Quan neix un blockchain, es podria testejar amb els criteris acordats per validar si el blockchain funciona com els developers diuen. Per la fase de testeig, les proves s'han de fer amb criteris diferents.

8.2 Frenar la centralització

Blockchain està dissenyat com un sistema descentralitzat. No obstant això, hi ha una tendència on els miners se centralitzen en un mining pool. Els top 5 mining pools junts controlen més del 51% del poder de hashing en la xarxa Bitcoin [70]. A part d'això, les estratègies egoistes de mining demostren que els pools amb més de 25% de poder computacional reben més recompenses que la resta. Així els miners racionals són atrets a la pool egoista i així pot sobrepassar fàcilment el 51% del poder total. Com el blockchain no ha estat dissenyat per donar serveis a un parell d'organitzacions, s'haurien de proposar mètodes per resoldre aquest problema.

8.3 Analítica de big data

Blockchain combina bé amb big data. La combinació es pot separar en dos tipus: gestió de dades i analítica de dades. Per la gestió de dades, blockchain es podria utilitzar per emmagatzemar dades importants a la vegada que es distribueix i protegeix. Blockchain també podria assegurar-se que les dades son originals. Amb l'analítica de dades, les transaccions amb blockchain es podrien utilitzar per analítica de big data. Per exemple, els patrons dels intercanvis entre usuaris poder ser extrets. Es podria predir el comportament potencial amb l'anàlisi.

8.4 Aplicacions de blockchain

En aquest moment la majoria de blockchains són utilitzats en el sector financer, però més i més aplicacions per diferents àmbits estan apareixent. Les indústries tradicionals podrien considerar i aplicar blockchain dins els seus entorns per millorar els seus sistemes. Per exemple, la reputació dels usuaris. La indústria moderna també pot aprofitar el blockchain per millorar el seu rendiment. Per exemple, Arcade City, una start-up que ofereix un servei per compartir cotxe, ofereix un marketplace on els conductors connecten directament amb els acompanyants feta amb la tecnologia blockchain [71].

8.5 Millors algoritmes de consens (Algorand)

Com s'ha vist en l'apartat 5.6, els algoritmes de consens més estandarditzats, com PoW, té el problema de què malgasta molta energia amb el càlcul dels seus problemes criptogràfics, ja que només qui acaba trobant la solució es du el premi i el càlcul que ha fet la resta no ha servit per res. Un nou algoritme que té potencial és Algorand.

Algorand confirma les transaccions amb ordre de latència d'un minut mentre escala amb molts d'usuaris. Algorand utilitza un nou protocol d'acord bizantí (BA) per arribar al consens entre els usuaris per fer la següent tanda de transaccions. Per escalar el consens a tants d'usuaris, Algorand utilitza un mecanisme punter basat en funcions aleatòries que permet als usuaris comprovar de forma privada si són seleccionats per participar en el BA per decidir la següent tanda de transaccions. En el protocol BA, els usuaris seleccionats són reemplaçats immediatament després d'enviar un missatge. Així es mitiguen atacs als usuaris després que la seva identitat sigui revelada. [72]

L'avaluació de l'algoritme Algorand damunt 500,000 usuaris mostra que pot fer transaccions en menys d'un minut, aconsegueix un rendiment 125 vegades superior a bitcoin i l'escalabilitat d'usuaris no fa cap penalització. [73]

9. Conclusió

S'ha aconseguit l'objectiu del projecte, implementant una sèrie de contractes intel·ligents per protegir i automatitzar les funcions d'una simulació de climatitzador d'una casa intel·ligent.

Gràcies a l'experiment realitzat, hem arribat a la conclusió de què per implementar un blockchain dins un entorn d'una casa intel·ligent no podem utilitzar qualsevol tipus de blockchain. Si utilitzéssim un blockchain destinat al sector financer, com bitcoin o ethereum, tindríem el problema de què els nodes s'haurien de sincronitzar i és un procés llarg per dispositius amb baixa potència, com els del IoT.

La solució seria implementar un blockchain de tipus privat, amb un algoritme de consens Proof of Stake. D'aquesta forma, assignant uns tokens als dispositius per gastar en transaccions, tenim un control sobre qui pot fer canvis en el nostre blockchain.

Amb aquests criteris, es podria tenir una xarxa IoT a una casa intel·ligent on les tasques dels dispositius estan automatitzades, fora intervenció humana, i amb un sistema robust davant atacs maliciosos.

10. Bibliografia

[1] – Rob van der Meulen, Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016, Gartner.com, Febrer del 2017
http://www.gartner.com/newsroom/id/3598917

[2]- Wikipedia, 2016 Dyn cyberattack
https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

[3] – Department of Energy, EEUU Goverment
https://www.energy.gov/energysaver/home-cooling-systems/air-conditioning

[4] - The "Only" Coke Machine on the Internet, The Carnegie Mellon University
https://link.springer.com/article/10.1007/BF00196791

[5]- Paolo Magrassi, Why a Universal RFID Infrastructure Would Be a Good Thing, 02 May 2002
https://www.gartner.com/doc/356347/universal-rfid-infrastructure-good-thing

[6]- Hai Zhuge, Future Interconnection Environment – Dream, Principle, Challenge and Practice, 2004
https://link.springer.com/chapter/10.1007/978-3-540-27772-9_2

[7]- Rob van der Meulen, Janessa Rivera, Gartner's 2014 Hype Cycle for Emerging Technologies Maps the Journey to Digital Business, August 11, 2014
https://www.gartner.com/newsroom/id/2819918

[8, 9, 10, 11, 12]- Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, Internet of Things (IoT) Security: Current Status, Challenges and Prospective Measures , ICITST, 2015
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=7412116

[13] - Mangal Sain, Young Jin Kang, Hoon Jae Lee, Survey on Security in Internet of things: state of the art and challenges, ICACT2017, February 19 ~ 22, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?arnumber=7890183&tag=1

[14]- Suwimon Vongsingthong and Sucha Smanchat, INTERNET OF THINGS: A REVIEW OF APPLICATIONS & TECHNOLOGIES
http://ird.sut.ac.th/e-journal/Journal/suwimonv/1403739/1403739.pdf

[15] – Sukanya Mandal, Internet of Things Healthcare Applications, 2015
http://medgizmo.info/news/internet-of-things-iot-healthcare-applications

[16, 18, 19] - Yujun Han i Baobin Liu, Interactive Smart Home Design Based on Internet of Things, ICCSE, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=8085534

[17] – Elizabeth Corvello, The ABC's of Smart Home Technology, 2017
http://realtorcorvello.com/2017/02/01/abcs-smart-home-technology

[20] – Luke Dormehl, 5 Open Source Home Automation Projects We Love, 2014
https://www.fastcompany.com/3038442/5-open-source-home-automation-projects-we-love

[21] – MarketsandMarkets, Smart Homes Market Worth $58.68 Billion by 2020, 2015
https://www.prnewswire.com/news-releases/smart-homes-market-worth-5868-billion-by-2020-292386861.html

[22, 23] - Waqar Ali, Ghulam Dustgeer, Muhammad Awais, Munam Ali Shah, IoT based smart home: Security challenges, security requirements and solutions, 23rd International Conference on Automation & Computing, University of Huddersfield, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=8082057

[24, 25] - Utkarsh Saxena, Dr. J.S Sodhi, Dr.Yaduveer Singh, Analysis of security attacks in a smart home networks, 7th International Conference on Cloud Computing, Data Science & Engineering, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=7943189

[26] – Wikipedia, Mirai (malware)
https://en.wikipedia.org/wiki/Mirai_(malware)

[27] – Lucinda Shen, Blockchain Will Be Used By 15% of Big Banks By 2017, 2016
http://fortune.com/2016/09/28/blockchain-banks-2017/

[28] - Stuart Haber, W. Scott Stornetta, How to time-stamp a digital document, 1991
https://link.springer.com/article/10.1007/BF00196791

[29] – Wikipedia, Merkle tree
https://en.wikipedia.org/wiki/Merkle_tree

[30] - Dave Bayer, Stuart Haber, W. Scott Stornetta, Improving the Efficiency and Reliability of Digital Time-Stamping
https://link.springer.com/chapter/10.1007/978-1-4613-9323-8_24

[31] - Florian Tschorsch, Björn Scheuermann, Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies, 2015
https://eprint.iacr.org/2015/464.pdf

[32, 33, 34] – Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008
https://bitcoin.org/bitcoin.pdf

[35, 36, 37, 38 ,39, 40, 41] - Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, Chen Qijun, A Review on Consensus Algorithm of Blockchain, IEEE International Conference on Systems, Man, and Cybernetics, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=8123011

[42, 43] - Lakshmi Siva Sankar, Sindhu M., M. Sethumadhavan, Survey of Consensus Protocols on Blockchain Applications, International Conference on Advanced Computing and Communication Systems, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=8014672

[44, 46, 48, 60, 61] - Valentina Gatteschi, Fabrizio Lamberti, Claudio Demartini, Chiara Pranteda, Víctor Santamaría, To Blockchain or Not to Blockchain: That Is the Question, 2018
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=8338007

[45] – Alex de Vries, Bitcoin's Growing Energy Problem, 2018
https://www.cell.com/joule/fulltext/S2542-4351(18)30177-6

[47] - Maxim Amelchenko, Shlomi Dolev, BLOCKCHAIN ABBREVIATION Implemented by Message Passing and Shared Memory, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=8171382

[49] - Thomas Delahunty, What Does the EU's GDPR Mean for Blockchain?, 2018
https://www.newsbtc.com/2018/04/06/what-does-the-eus-gdpr-mean-for-blockchain/

[50] – Michiel Mulders, Comparison of Smart Contract Platforms, 2018
https://hackernoon.com/comparison-of-smart-contract-platforms-2796e34673b7

[51, 55] - Seyoung Huh, Sangrae Cho, Soohyung Kim, Managing IoT Devices using Blockchain Platform, ICACT2017, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?arnumber=7890132&tag=1

[52] – Solidity documentation
https://solidity.readthedocs.io/en/develop/

[53] – Ethereum Virtual Machine, What is Ethereum?
http://ethdocs.org/en/latest/introduction/what-is-ethereum.html - ethereum-virtual-machine

[54] – Pete Rizzo, Thomson Reuters Demos New Ethereum Blockchain Use Cases, 2016
https://www.coindesk.com/thomson-reuters-blockchain-ethereum-devcon2/

[56] – Blockchain oracles, Blockchainhub
https://blockchainhub.net/blockchain-oracles/

[57, 58, 59, 62, 63] - Joshua Ellul, Gordon J. Pace, AlkylVM: A Virtual Machine for Smart Contract Blockchain Connected Internet of Things, 2018
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=8328732

[64] – Margaret Rouse, What is Prototyping model?, 2005
https://searchcio.techtarget.com/definition/Prototyping-Model

[65] – ISTQB, What is Prototype model- advantages, disadvantages and when to use it?
http://istqbexamcertification.com/what-is-prototype-model-advantages-disadvantages-and-when-to-use-it/

[66] – Rinkeby: Ethereum Testnet
https://www.rinkeby.io

[67] – Rinkeby: Authenticated Faucet
https://faucet.rinkeby.io/

[68] – Pragma – A platform for creating smart contracts
https://www.withpragma.com/

[69, 70, 71] - Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang, An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, 6th International Congress on Big Data, 2017
https://0-ieeexplore.ieee.org.llull.uib.es/stamp/stamp.jsp?tp=&arnumber=8029379

[72, 73] - Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, Nickolai Zeldovich, Algorand: Scaling Byzantine Agreements for Cryptocurrencies, 2017
https://dl.acm.org/citation.cfm?id=3132757

*Dia 29 de juny de 2018 s'ha entrat amb èxit a totes les referències.