Consiglio Nazionale delle Ricerche
Istituto di Calcolo e Reti ad Alte Prestazioni

Blockchain and IOT

Antonio Francesco Gentile, Davide Macrì, Emilio Greco

RT-ICAR-CS-22-05 **Maggio 2022**

Consiglio Nazionale delle Ricerche, Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR)
– Sede di Cosenza, Via P. Bucci 8-9C, 87036 Rende, Italy, URL: *www.icar.cnr.it*
– Sezione di Napoli, Via P. Castellino 111, 80131 Napoli, URL: *www.icar.cnr.it*
– Sezione di Palermo, Via Ugo La Malfa, 153, 90146 Palermo, URL: *www.icar.cnr.it*

Sommario

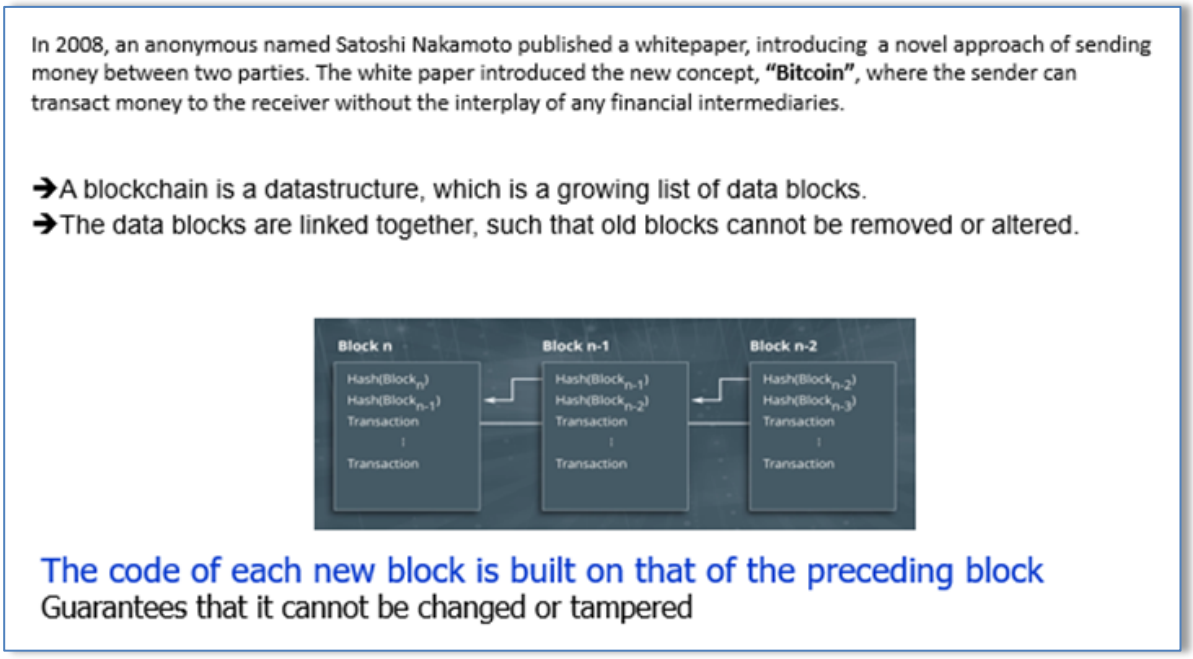
Introduzione

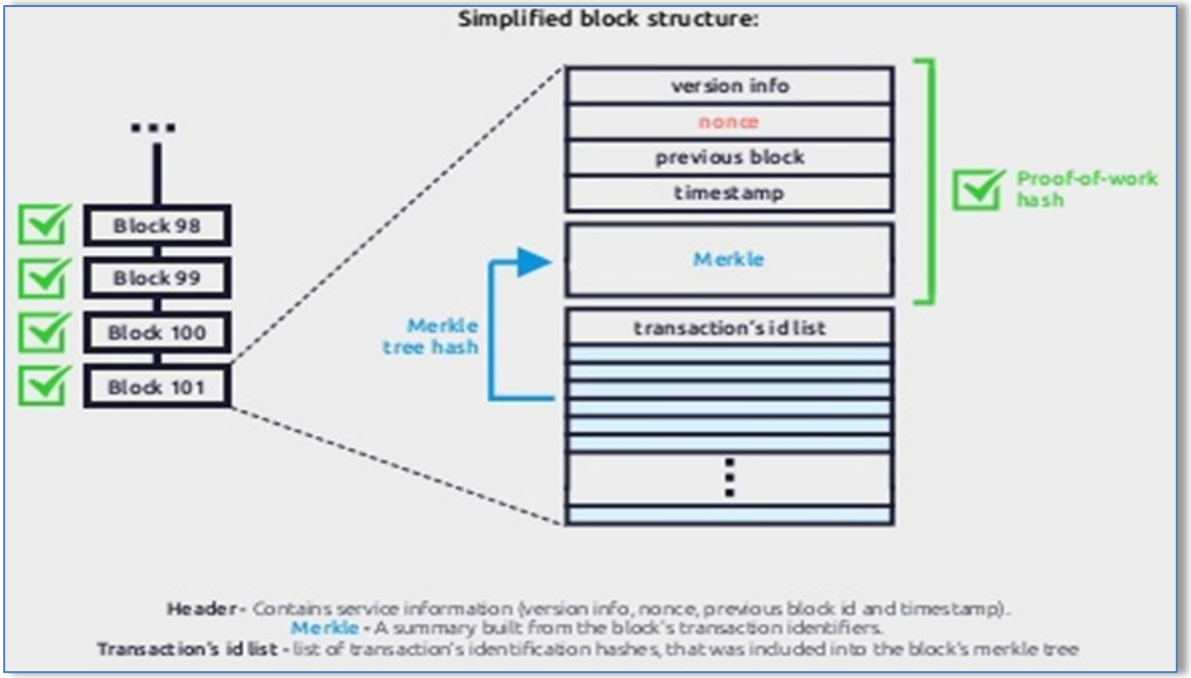
L'elaborato è strutturato nel seguente modo: nella prima parte parleremo ed introdurremo la tecnologia Blockchain e le caratteristiche che ne hanno determinato il suo successo. Dedicheremo una parte alla trattazione degli smart contracts ed al linguaggio Solidity che ha dato il via ad una nuova era per le applicazioni basate su Blockchain ed infine analizzeremo due diverse metodologie applicative mirate ad estendere la tecnologia in campo dell'Internet delle Cose (IOT).

- Overview of Blockchain technology
- Solidity and smart contracts
- IOT Platform and load balance with Smart Contract and Nfts
- Development ad hoc technologies for the realization of M2M
- Application specific blockchain (Ternedermint)
- PSO over blockchain

Overview of Blockchain technology

Introduciamo la nostra dissertazione spiegando cosa significa il termine blockchain, ovvero letteralmente ("catena di blocchi") contenenti solitamente "transazioni" ,una struttura dati condivisa e immutabile un registro digitale le cui voci sono raggruppate in "blocchi", concatenati in ordine cronologico, e la cui integrità è garantita dall'uso della crittografia.





Le problematiche che la questa tecnologia consente di superare come il problema dell'infinita riproducibilità di un bene digitale e della doppia spesa, senza l'utilizzo di un server centrale o di un'autorità. Spieghiamo più tecnicamente il problema della doppia spesa. Quando una transazione viene registrata nella blockchain, dopo aver aggiunto z blocchi, gli aggressori decidono di rigenerare un nuovo brach della blockchain. Se il nuovo branch della blockchain funziona più velocemente di quella esistente, gli aggressori recupereranno le monete che hanno speso in precedenza perché il protocollo Bitcoin selezionerà sempre la catena più lunga. In questo scenario più realistico, la probabilità che l'attaccante recuperi è

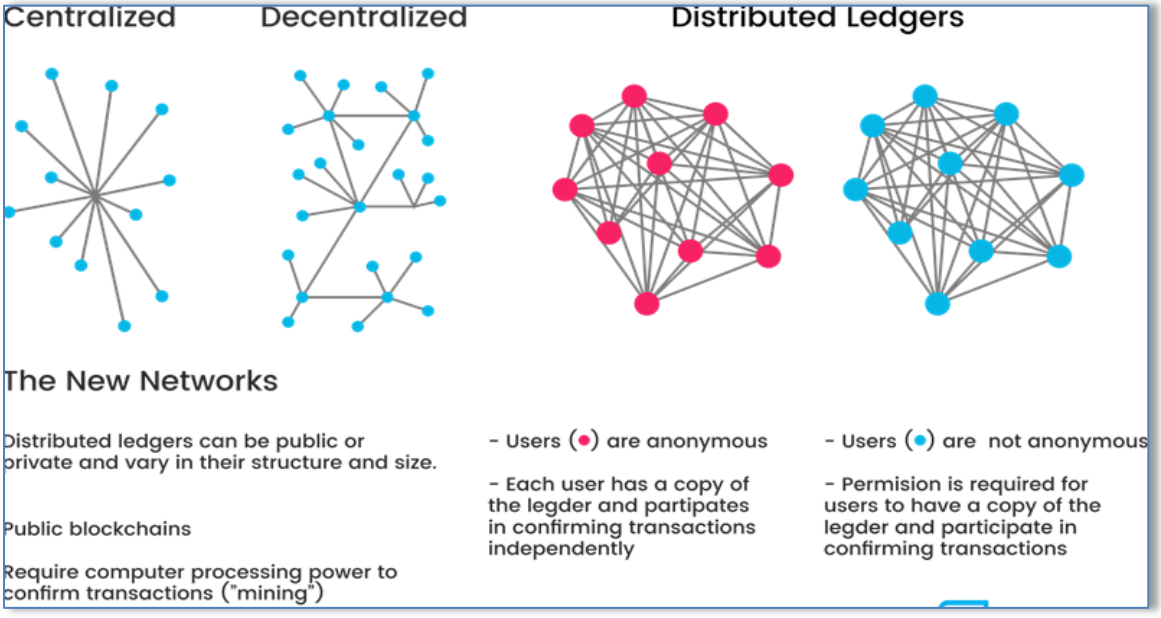
$$1-\sum_{k=0}^{z}\frac{\lambda^k e^{-\lambda}}{k!}\left(1-(q/p)^{(z-k)}\right)$$

dove p: è la probabilità che un nodo onesto trovi il blocco successivo,
q: è la probabilità che l'attaccante trovi il blocco successivo;

Quando q = 0,1, p = 0,9 e z = 6, la probabilità che l'attaccante raggiunga è 0,0002. Nella vera rete Bitcoin, p è molto più grande di q. In generale, dopo che un beneficiario ha atteso z=6 blocchi, è molto difficile per gli attaccanti spendere il doppio di quanto pagato in precedenza.

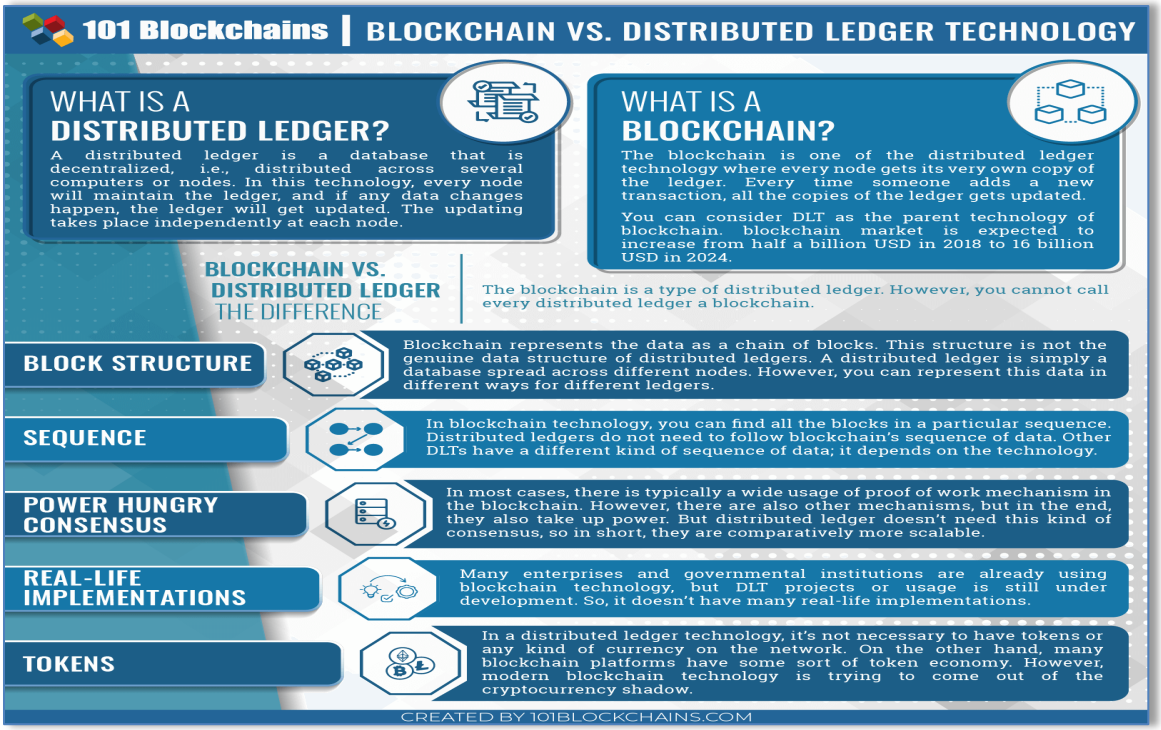
Nella immagine successiva riepiloghiamo quali sono le caratteristiche principali che deve avere una blockchain.

Strengths lie in transparency, immutability and security	▪ Core benefits include transparency, censorship resistance (immutability), security and orderly data structures which result in a high degree of auditability and reliability
	▪ Transparency enables identical visibility of ledger information across all users
	▪ It is designed to resist the alteration of data, eliminating asymmetric information ▪ Append-only,No update, no delete
	▪ Blockchains are also distributed, which means there is no single point of failure or attack vector for hackers or other malicious actors
Solving the "double spend" problem	▪ Blockchain characteristics allow for the creation of unique digital representations
	▪ This solves the "double spend problem," defined as the ability to maintain multiple digital copies or replicas of an asset already transferred to someone else
	▪ Blockchain permits certainty in digital transactions and reassures sellers and buyers that the item(s) in the transaction are unique and have not been duplicated or sold to others

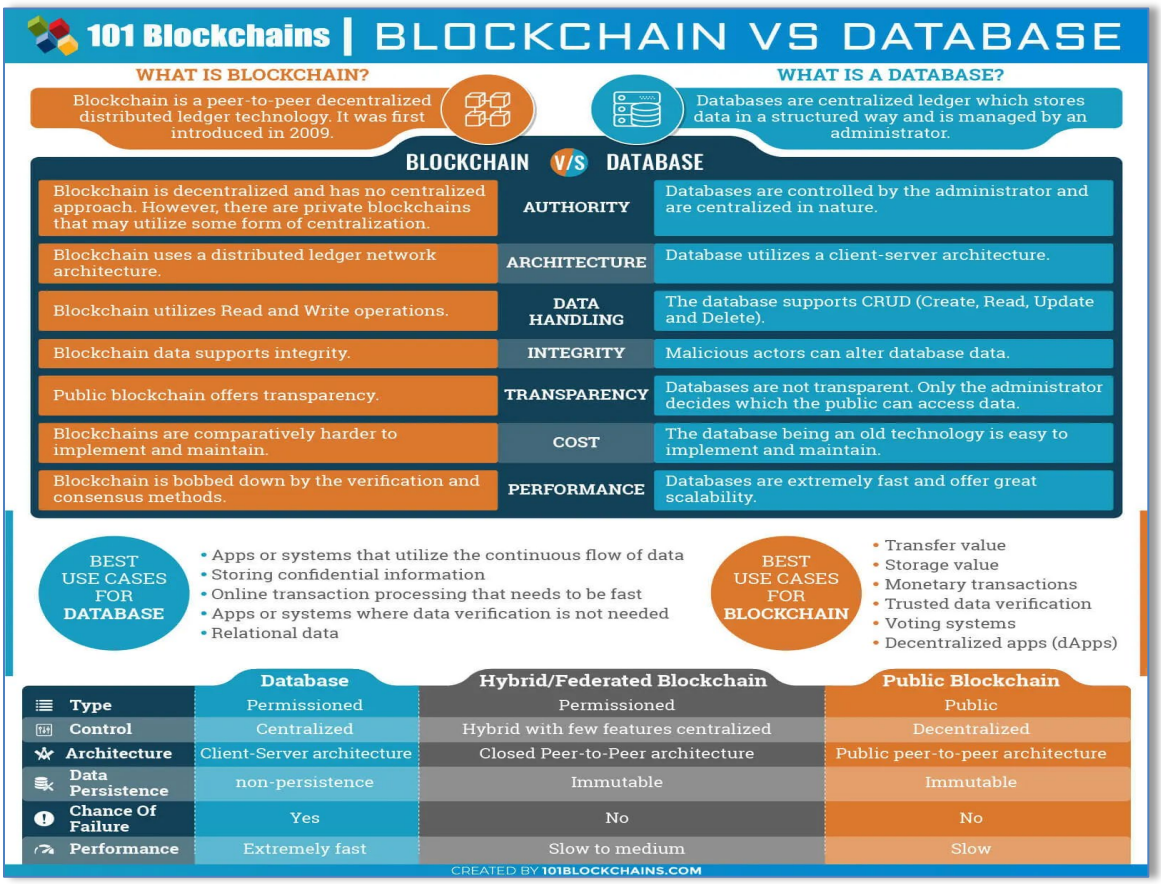


La tecnologia Blockchain è inclusa nella più ampia famiglia dei Distributed Ledger, ossia sistemi che si basano su un registro distribuito, che può essere letto e modificato da più nodi di una rete. Non è richiesto che i nodi coinvolti conoscano l'identità reciproca o si fidino l'uno dell'altro perché, per garantire la coerenza tra le varie copie, l'aggiunta di un nuovo blocco è globalmente regolata da un protocollo condiviso. Una volta autorizzata l'aggiunta del nuovo blocco, ogni nodo aggiorna la propria copia privata. La natura stessa della struttura dati garantisce l'assenza di una sua manipolazione futura.

Nelle seguenti immagini evidenzieremo le differenze che ci sono tra una blockchain e un distribuited ledger mentre la seconda evidenzia le differenze con un database.



Possiamo dire brevemente che una blockchain è una specializzazione di un distribuited ledger, dove le differenze sostanziali sono la tipologia di struttura dati usata della blockchain tipicamente il blocco e l'algoritmo per raggiungere il consenso.



La principale differenza tra una blockchain e un database invece è principalmente la centralizzazione. Mentre tutti i record protetti su un database sono centralizzati, ogni partecipante su una blockchain ha una copia protetta di tutti i record e tutte le modifiche in modo che ogni utente possa visualizzare la provenienza dei dati. L'importanza di questa caratteristica è tangibile quando c'è un'incoerenza: poiché ogni partecipante conserva una copia dei record, la tecnologia blockchain identificherà e correggerà immediatamente qualsiasi informazione inaffidabile. Inoltre blockchain pubblica è senza autorizzazione perché chiunque può accedervi. Per quanto riguarda la velocità il database è invece più performante. Un'altra differenza che merita una citazione è che sulla blockchain possono essere fatte solo operazioni di inserimento mentre nel databse le canoniche operazioni Il di creazione, lettura, aggiornamento ed eliminazione.

Abbiamo citato precedentemente le blockchain permissioned, ora vedremo la differenza che intercorre tra una permissioned e una permissioless.

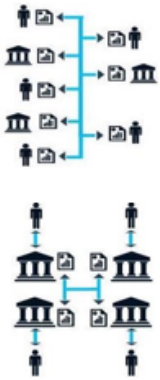
Blockchain pubblica o Permissionless

Le blockchain pubbliche sono reti aperte che consentono a chiunque di partecipare alla rete, ovvero la blockchain pubblica è senza autorizzazione. In questo tipo di blockchain chiunque può entrare in rete e leggere, scrivere o partecipare all'interno della blockchain. Una blockchain pubblica è decentralizzata e non ha un'unica entità che controlla la rete. I dati su una blockchain pubblica sono sicuri (soprattutto all'aumentare della chain) in quanto non è possibile modificare o alterare i dati, a una volta che sono stati convalidati sulla blockchain.

Permissioned or Private Blockchain

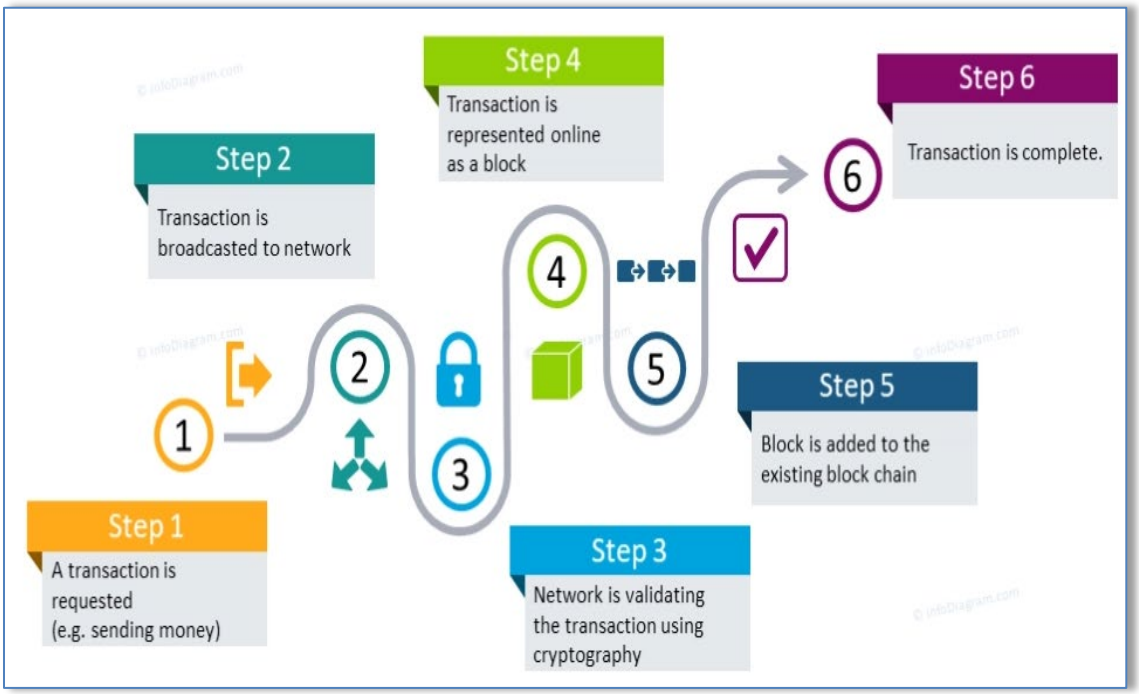
Una blockchain privata è gestita da un amministratore di rete e i partecipanti hanno bisogno del consenso per entrare nella rete, quindi una blockchain privata è una blockchain autorizzata. Esistono una o più entità che controllano la rete e questo porta a fare affidamento su terze parti per le transazioni. In questo tipo di blockchain solo le entità partecipanti alla transazione sono a conoscenza della transazione eseguita mentre altre non potranno accedervi, ovvero le transazioni sono private.
Le blockchain private sono solitamente sistemi che si basano su copie e/o emulazioni del codice delle blockchain pubbliche, ma che vengono limitate ad un numero di "nodi noti", ad una federazione di nodi ad esempio, ed arricchite di sistemi crittografici per mantenere i dati riservati e non pubblici. Sono tipicamente più veloci, ma maggiormente esposte ad attacchi informatici.

- Public blockchain
  - Open P2P network
    - Participants can join and leave without notification
  - Anonymous, untrusted participants
  - Large-scale distributed ledger
- Private blockchain
  - Closed permissioned network
  - Identified, trusted participants
  - Regulated control
  - Small to medium-scale distributed ledger



	Public	Permissioned
Throughput	Low	Medium
Latency	High	Medium
# Readers	High	High
# Writers	High	Low
Centrally Managed	No	Yes
Transaction Cost	High	Free

Nella immagine soprastante descriviamo in maniera compatta le differenze tra la due tipologie di blockchain, che ci aiutano a capire quale delle due tipologie sia più adatta ai nostri scopi. Es. Se abbiamo un sistema altamente responsivo che necessita scrivere molte transazioni con una latenza bassa la scelta più indicata è una blockchain privata.



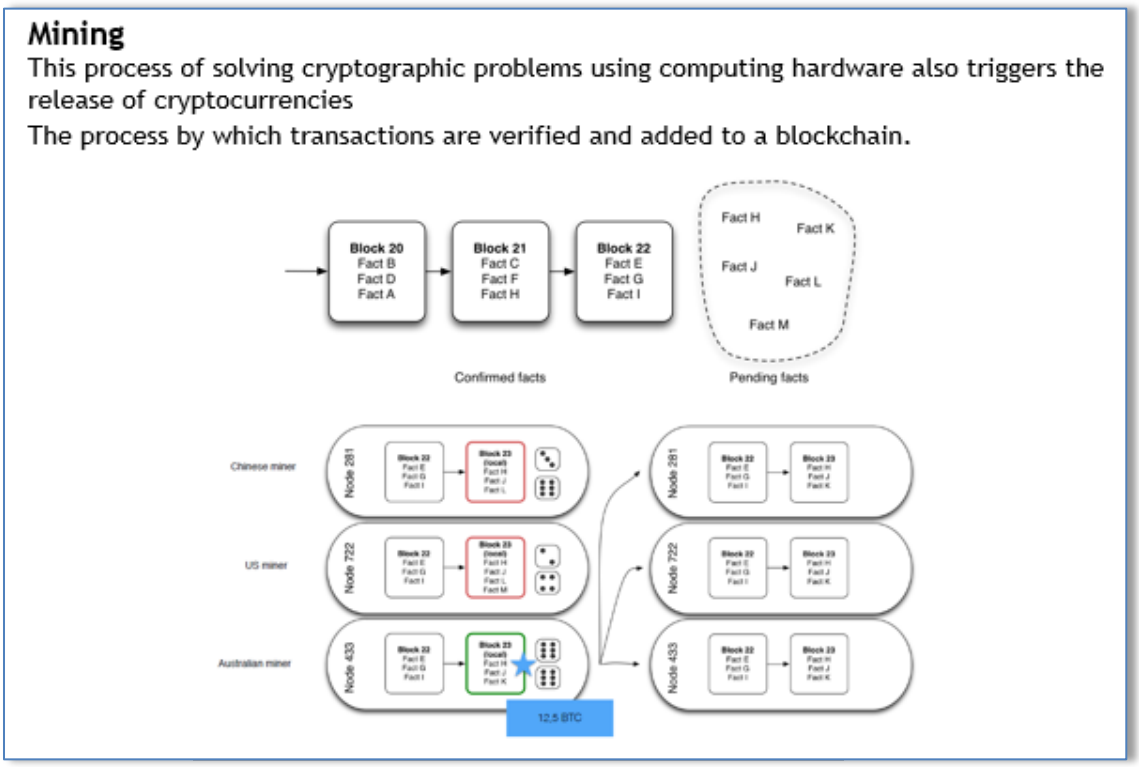
Nell'immagine soprastante descriviamo come avviene la scrittura di una transazione all'interno di un blocco della chain. In breve dopo la creazione della richiesta richiesta di transazione, viene propagata in broadcast sulla rete, viene validata e infine aggiunta alla catena.

Mining

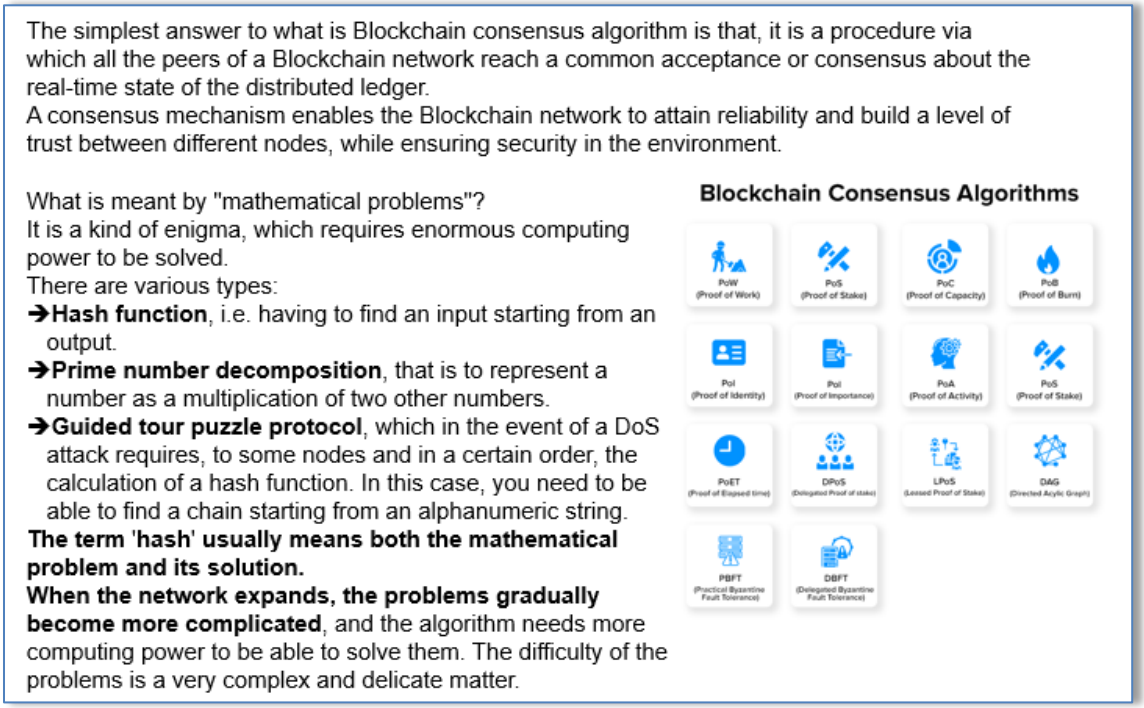
Il mining è il processo alla base del sistema di Consenso Decentralizzato e dunque senza il bisogno di un'autorità centrale. Le transazioni vengono convalidate ed inserite nella blockchain, mantenendo inoltre questo meccanismo e la rete sicuri. Il mining è dunque l'invenzione che rende Bitcoin il meccanismo di sicurezza che è alla base del contante digitale peer-to-peer.

I miners ricevono due tipi di ricompense per il loro lavoro: i bitcoin creati ad ogni nuovo blocco e le transaction fees in esso incluse. Per ottenere queste ricompense, i miners devono competere per risolvere un difficile problema (vedi immagine successiva) computazionale basato su un algoritmo di hashing; la soluzione al problema, chiamato proof-of-work (cap. successivo), è inclusa nel nuovo blocco ed agisce come prova che il miner ha impiegato uno sforzo computazionale per arrivare alla soluzione. Vincendo questa gara, si ottiene la ricompensa ed il diritto di registrare le transazioni nella blockchain.

Il processo viene detto" mining" perché la ricompensa è progettata per ottenere rendimenti man mano decrescenti con il tempo, proprio come l'estrazione di materiali preziosi: l'offerta di moneta di bitcoin viene creata attraverso il mining ad ogni transazione.



Quindi ne consegue che la quantità massima di Bitcoin che un minatore può ottenere come ricompensa diminuisce approssimativamente ogni 4 anni (precisamente ogni 210000 blocchi): si è iniziato con 50 bitcoin per blocco nel gennaio del 2009, si è dimezzato a 25 bitcoin nel novembre 2012 e si è arrivato a 12,5 bitcoin nel 2016. Sulla base di questo schema, i premi del mining di bitcoin diminuiranno esponenzialmente fino a circa l'anno 2140, quando tutti i 21 milioni di bitcoin saranno stati emessi.



Proof-of-Work

Proof-of-Work (PoW) indica l'algoritmo di consenso alla base di una rete blockchain. Questo algoritmo viene utilizzato per confermare le transazioni e produrre i nuovi blocchi della catena; L'obiettivo del PoW è incentivare i miner a competere tra loro

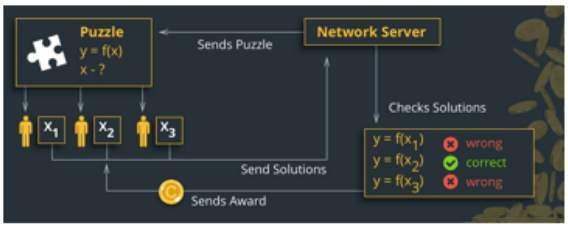
nell'elaborazione degli scambi, ricevendo in cambio una ricompensa.
I miner risolvono il problema, danno vita a un nuovo blocco e confermano tutte le transazioni al suo interno.Il nodo che per primo risolve il puzzle(problema matematico) ha diritto di inserire il blocco sulla blockchain e ottiene una ricompensa per incentivare la continuazione del lavoro. Solo in questo modo un utente può essere sicuro che tutte le proprie transazioni vengano incluse nella blockchain. Descriviamo brevemente come funziona il POW e come vengono validate le transazioni:

1. per ogni transazione inviata, la rete richiede circa 10 minuti per confermarla, e può gestire sino a circa sette transazioni al secondo. Nell'intervallo di tempo dei dieci minuti si forma un nuovo blocco;
2. ogni blocco contiene diverse transazioni, che devono essere validate in modo indipendente.
3. i miners, computazionalmente più performanti, prendono una transazione alla volta e risolvono un algoritmo crittografico, noto come proof of work;
4. la transazione, a questo punto viene validata e pubblicata sulla blockchain pubblica affinché tutti possano vederla;
5. i miners più veloci, i primi che risolvono l'algoritmo, vengono ricompensati in criptovalute, quella di utilizzo della blockchain su cui operano. Migliaia di computer gareggiano per diventare i primi a risolvere l'algoritmo crittografico, per cui uno dei maggiori problemi di proof of work è che non è un sistema corretto, nel senso che utenti con hardware più potenti e costosi avranno sempre le maggiori possibilità di vincere la ricompensa. Vediamo l'implicazione di questo lavoro concorrente in termine di energia nel prossimo capitolo.

Proof-of-Work is the foundation of several cryptocurrencies.

The most popular application of PoW is Bitcoin: it was this cryptocurrency that laid the foundation for this type of consensus. The problem is called Hashcash, and the algorithm changes its difficulty dynamically depending on the computing power available on the network. The block creation time is approximately 10 minutes. Other Bitcoin-based currencies, such as Litecoin, also use a similar system.

Another important PoW-based project is Ethereum: since in the world of cryptocurrencies around 75% of projects are based on Ethereum, it is possible to say that most of the Blockchain applications exploit the PoW consensus model.



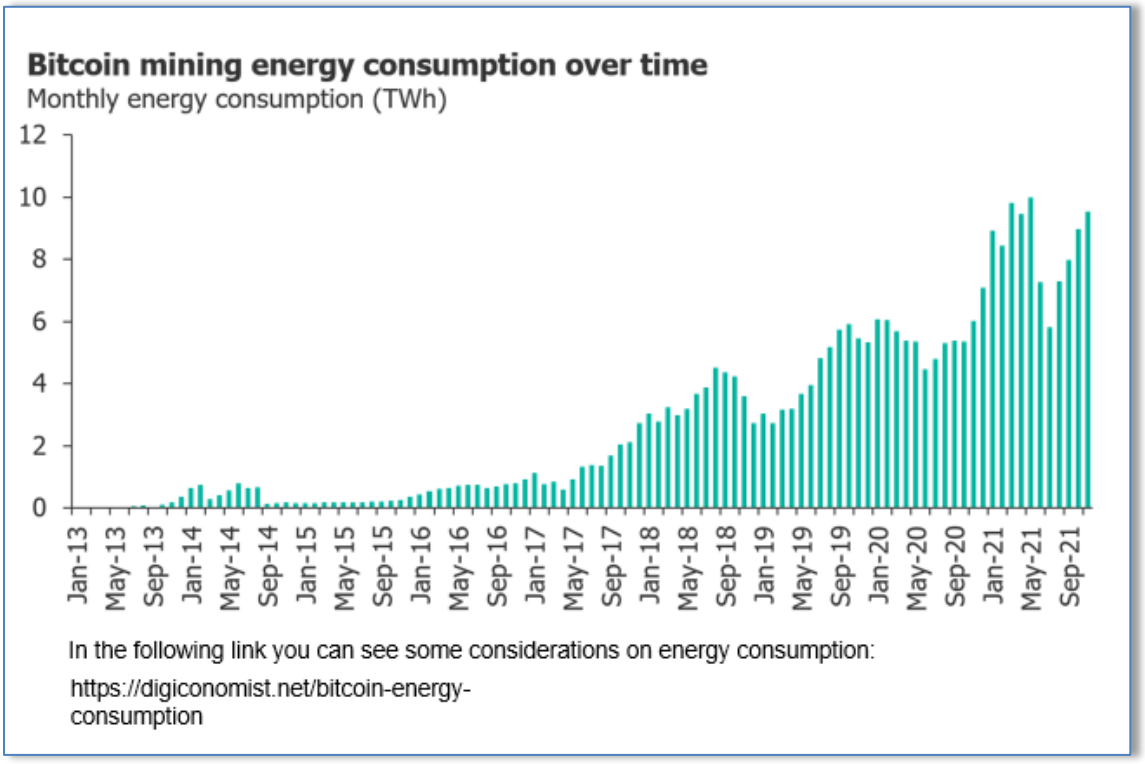
Why use a PoW consensus algorithm?

1. an excellent defense against DoS attacks

2.the marginal impact of quotas in mining.(Those with large amounts of money, therefore, have no more control over the network).

POW energy problem

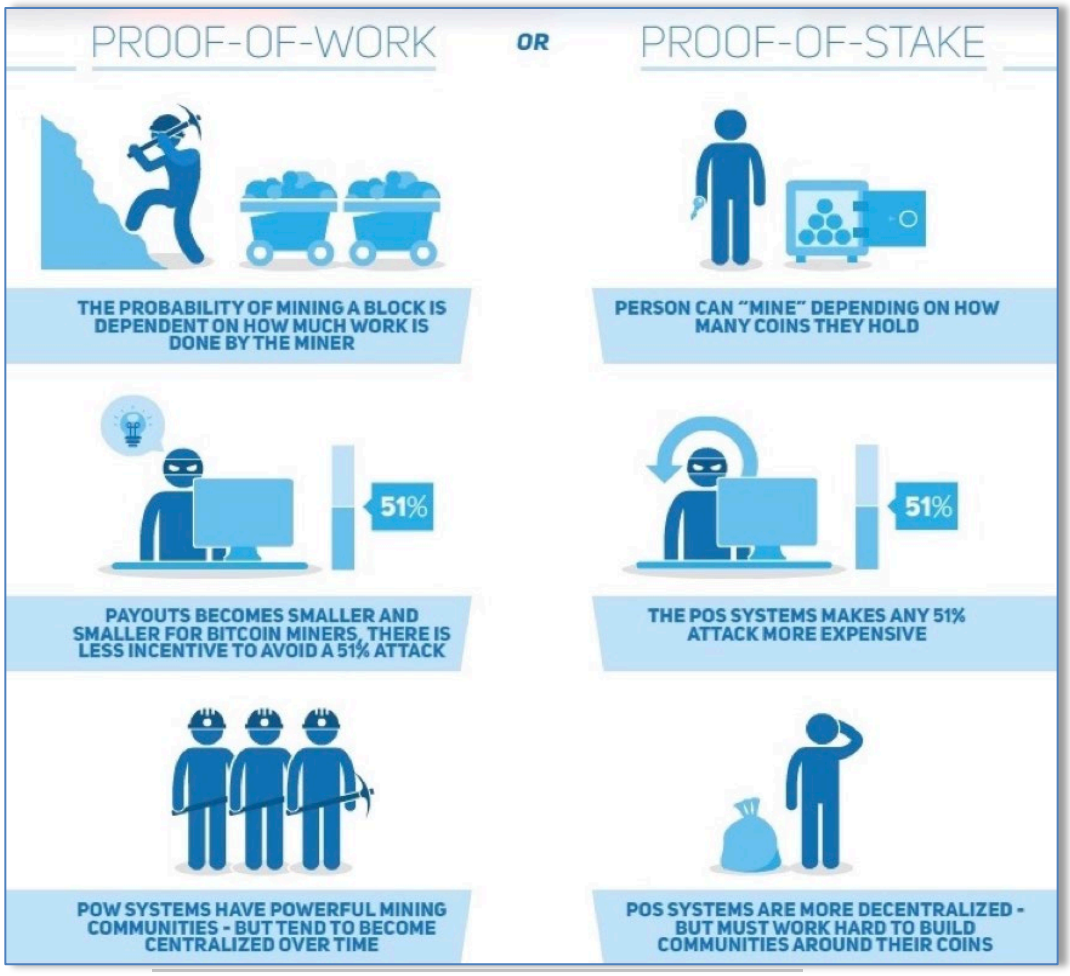
Nel capitolo precedente abbiamo discusso del POW e dell'elevata potenza di calcolo richiesta
dai vari nodi per risolvere concorrentemente i puzzle, adesso vediamo gli impatti che ne derivano, analizzando l'articolo di Alex De Vries del 2018 parla del problema dello spreco di energia e ha stimato che la rete Bitcoin consumava, fino a quel momento, almeno 2,55 gigawatt di elettricità e potenzialmente 7,67 gigawatt in futuro, rendendola paragonabile a paesi come l'Irlanda (3,1 gigawatt) e l'Austria (8,2 gigawatt). Inoltre, secondo i modelli economici il consumo di elettricità di Bitcoin si sarebbe aggirato verso quest'ultimo numero. Con la rete Bitcoin che elabora solo 200.000 transazioni al giorno, ha fatto anche una stima sull'elettricità media consumata per transazione, con la conclusione che era pari ad almeno 300 KWh e avrebbe potuto superare i 900 KWh per transazione entro la fine dell'anno. L' immagine successiva mostra come il consumo di energia sia stato negli anni sempre crescente. Vediamo nel prossimo capitolo come si è cercato di trovare uan soluzione al problema energetico



Da POW a POS

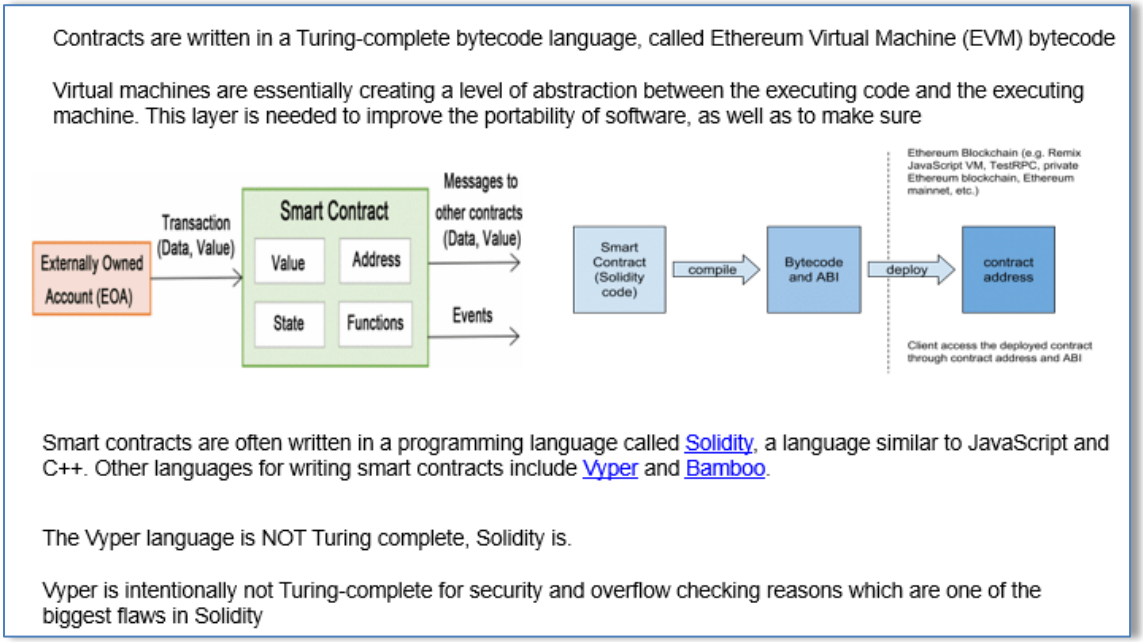
Per cercare di ovviare il problema energetico le varie blockchain esistenti hanno rivisto gli algoritmi del consenso, ad esempio, Ethereum, la seconda criptovaluta più grande utilizzata, sta attualmente spostando i suoi meccanismi di consenso da PoW a Proof-of-

Stake (PoS). In PoS, i validatori di rete, che svolgono una funzione simile ai miner in Bitcoin, supportano la rete mettendo in palio un token per determinare quali transazioni vengono aggiunte come blocchi alla blockchain. Nell'ambito del proof-of-stake, la risoluzione dei puzzle arbitrario non è necessaria. Rimuovendo la risoluzione dei puzzle si riduce drasticamente il dispendio energetico necessario per mettere in sicurezza la rete.
Poiché i validatori PoS non sono in competizione attraverso la potenza di calcolo, che consuma energia, l'esecuzione di questi nodi di validazione richiede solo risorse economiche come i token di rete. Fatta eccezione per le quantità relativamente minime di energia per far funzionare i nodi della rete distribuita, nessuna energia aggiuntiva. Secondo la Ethereum Foundation, il passaggio da PoW a PoS riduce il consumo energetico totale della rete di Ethereum di almeno il 99,95% , ovvero 2,62 megawatt equivalenti a una piccola città di circa 2.100 case americane.



Smart Contract

Nel lavoro del 1995 Nick Szabo definisce gli smart contract come “Un insieme di promesse, compresi i protocolli all'interno dei quali le parti rispettano le altre promesse. I protocolli sono solitamente implementati con programmi su una rete di computer o in altre forme di elettronica digitale, quindi questi contratti sono (più intelligenti) dei loro antenati cartacei”.
In sostanza possiamo definire uno smart contract come un programma eseguito su una blockchain in grado di supportarli. Sono una raccolta di codice (le funzioni) e dati (lo stato) che risiede a un indirizzo specifico sulla blockchain ad esempio su Ethereum.Analizziamo nello specifico uno smart contract, possiamo dire che in effetti sono un account di Ethereum.Avere un account significa avere un saldo e poter inviare transazioni in rete. La differenza tra un (EOA) Externally Owned Account, e un account di uno smart contract è che questi ultimi non sono controllati da un utente, ma distribuiti in rete ed eseguiti come programmato. Gli account degli utenti possono quindi interagire con uno smart contract inviando transazioni che eseguono una funzione definita sul contratto. Gli smart contract possono definire regole, come un normale contratto, e imporle automaticamente tramite codice,inoltre non sono eliminabili di default e le interazioni con essi sono irreversibili.Per quanto riguarda la creazione di uno smart contract,possono essere scritti mediante l’utilizzo ti linguaggi Turing-completi come Solidity



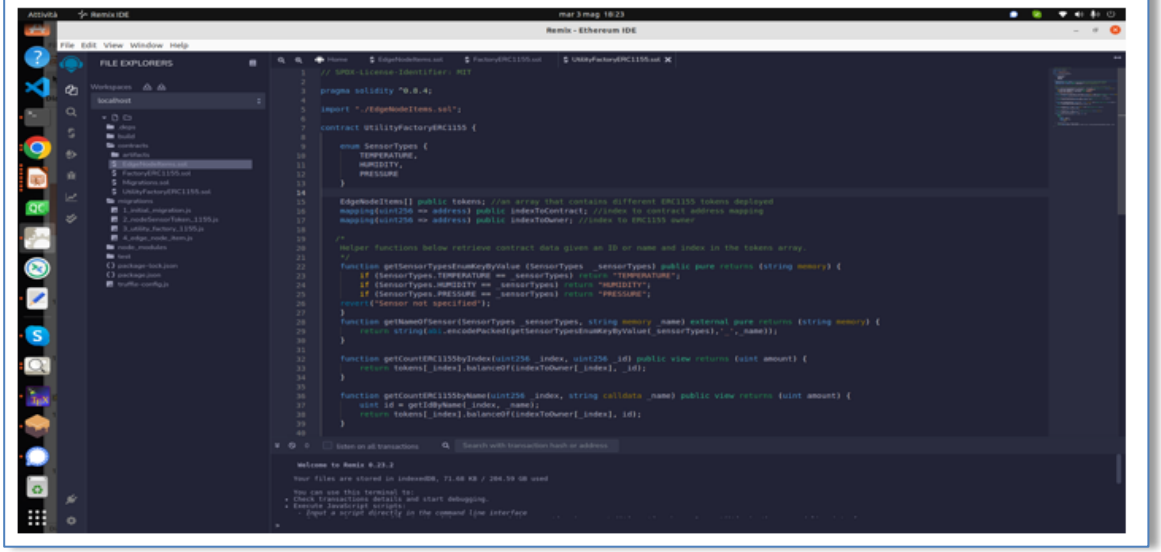
Solidity and smart contracts

NFT sta per Non-Fungible Token, ovvero un gettone digitale non fungibile. Si tratta di token unici, non fungibili, cioè non intercambiabili né sostituibili ed indivisibili, con cui rappresentare un asset in formato digitale, come opere d'arte digitali, oggetti collezionabili su blockchain, quindi certificati come un bene digitale unico e con provenienza garantita. Con un NFT è possibile rappresentare qualsiasi oggetto digitale come foto, video, audio. È proprio la sua peculiare caratteristica di infungibilità che lo contraddistingue da altri asset, come le criptovalute; ad esempio, un bitcoin è fungibile in quanto può essere sostituito con un altro.
Gli NFT possono essere utilizzati in molteplici i settori cosi come gli ambiti di applicazione di questa tecnologia sono molteplici:

- Proprietà intellettuale: gli NFT rappresentano un quadro, un brevetto, una canzone o altri diritti di proprietà intellettuale:
- Gaming: gli NFT diventano oggetti da collezione digitale o gadget utilizzabili nei giochi virtuali;
- Certificati: gli NFT possono essere utilizzati per verificare l'autenticità dell'identità di una persona o di certificati di nascita, di credenziali accademiche, di licenze o di altro;
- Documenti finanziari: fatture, bollette, ordini possono essere trasformati in NFT;
- Real estate: immobili e altre proprietà di valore possono essere tokenizzate per migliorare la liquidità della proprietà o per rendere più veloce il finanziamento;

Un aspetto che ha catturato il nostro interesse sugli NFT è la possibilità di utilizzarli come identity management; Poterli utilizzare in ottica di Edge Computing come elemento per poter identificare un sensore/dispositivo in maniera univoca, specifica un eventuale processo di autenticazione e autorizzazione.

Smart contract is not self-executable.
It requires an external call to be executed. Otherwise, it is pending till one calls one of its implemented functions.
Once it is executed, transactions resulting from the execution are transcribed on the blockchain and eventually smart contract's meta data are updated.



IOT Platform and load balance with Smart Contract and Nfts

Per coniare token NFT utilizziamo vengono creati smart contract specifici, ognuno caratterizzato dalle proprie specifiche. Nell'immagine successiva viene definito tramite il linguaggio Solidity un tipo di token ibrido chiamato ERC-1155.
Nell'immagine successiva vengono o riportati alcuni tipi di token NFT, come ERC-20 che viene utilizzato come criptovaluta mentre ERC-721 viene utilizzato per rappresentare oggetti univoci come un'opera d'arte.

Non-fungible tokens or NFTs are the digital assets on a blockchain. NFTs are unique and they cannot be divided like cryptocurrencies. NFTs could store digital ownership of artwork or collections or can be fan tokens or tickets for clubs.

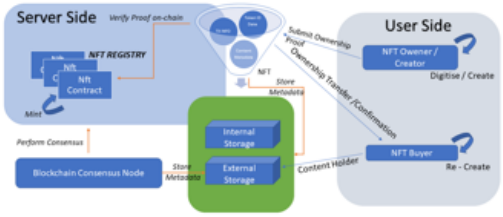
NFTs are based on a smart contract on a blockchain network which supports them such as Ethereum, Cardano, or Polkadot.

ERC-20: A general standard for tokens which is mostly used on the Ethereum blockchain with basic functionality to transfer tokens through a smart contract.

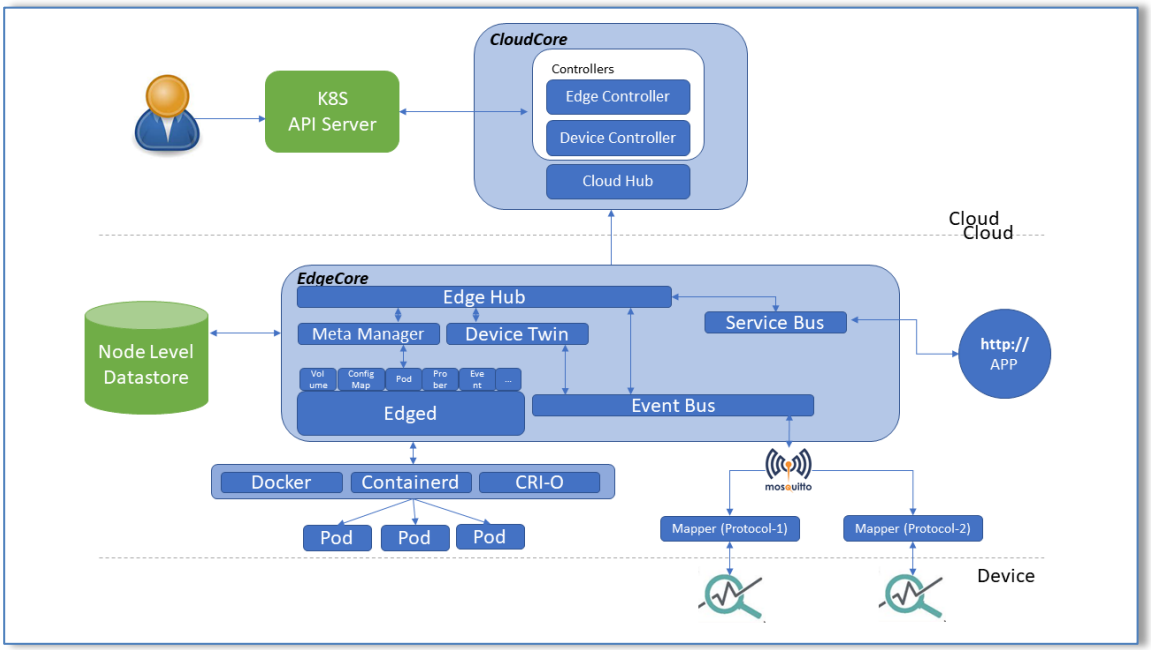
ERC-721: A common non-fungible standard that each token is a unique distinguishable asset. With this standard, each NFT has its ownership in a smart contract.

ERC-821: Through this standard, anyone can check the address of the contract and find which features are supported. There are also other standards for NFTs on blockchains such as NEO and EOS

ERC-1155: A new standard that supports the features of fungible (ERC-20) and non-fungible tokens (ERC-721). It also supports converting and minting new tokens



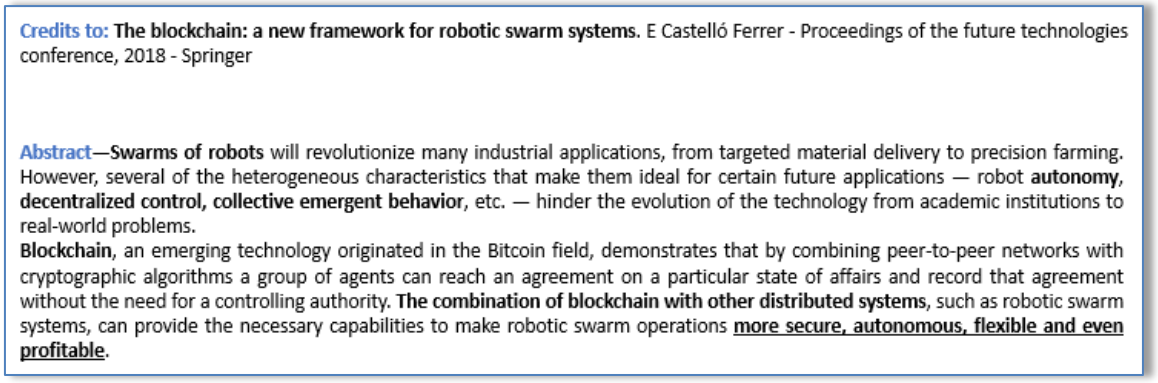
Piattaforma IOT tramite kubeEdge smart Contract e NFT:



Development ad hoc technologies for the realization of M2M

Nei paragrafi precedenti abbiamo visto come realizzare una infrastruttura di sistema per la gestione di servizi IoT utilizzando gli strumenti messi a disposizione dalle principali blockchain presenti oggi sul mercato delle criptovalute. Tra questi ricordiamo due elementi fondamentali che ci consentono di utilizzare questi sistemi anche come infrastrutture per realizzare servizi differenti al tradizionale scambio di criptovalute : gli smart contracts e i Token Indivisibili. Di seguito, prendendo a riferimento il lavoro “Proceedings of the future technologies conference, 2018 - Springer”, possiamo connotare le applicazione descritte, all’interno due aree di intervento : L’allocazione dinamica di risorse ed nuovi modelli di business. Dato il particolare contesto applicativo ed i requisiti stringenti in termini di tempo di risposta, le soluzioni finora proposte devono essere supportate ed integrate con sistemi di comunicazione dette “off-chain” al fine di rispondere ai requisiti di progetto. Tuttavia, dati i recenti sviluppi tecnologici nel settore, oggi è possibile adoperare una sola infrastruttura per supportare tutte le fasi di comunicazione tra dispositivi IoT senza necessariamente dover ricorrere a doppio canale di comunicazione (on-chain ed off-chain).

Per rendere realizzabile questa infrastruttura è necessario fare ricorso a blockchain realizzate ad hoc per la particolare applicazione, ottimizzando le risorse ed abbattendo così i tempi di risposta.



Credits to: **The blockchain: a new framework for robotic swarm systems.** E Castelló Ferrer - Proceedings of the future technologies conference, 2018 - Springer

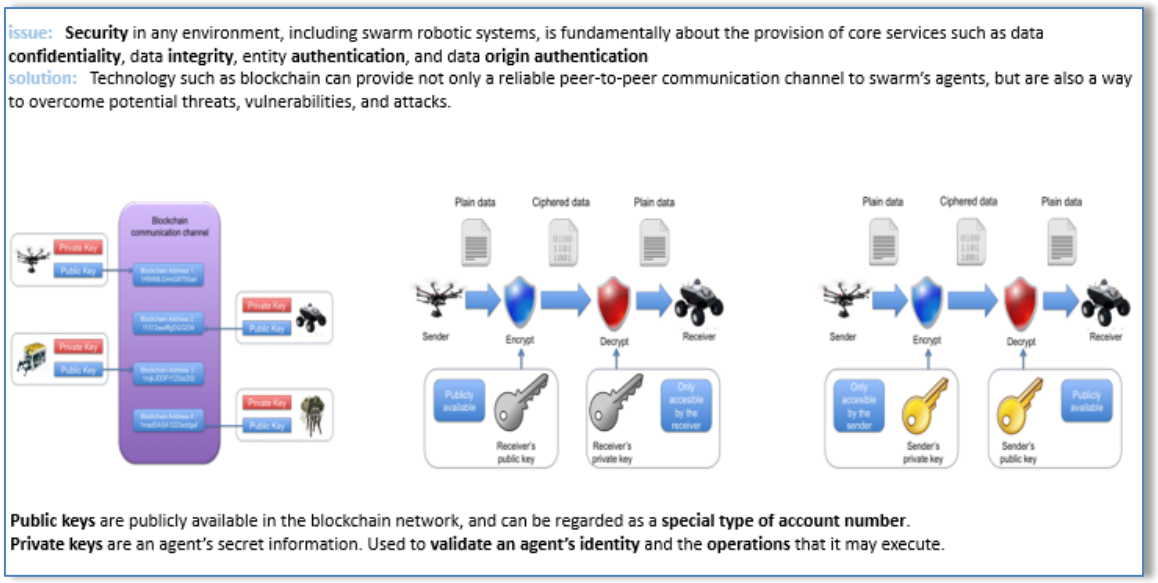
Abstract—**Swarms of robots** will revolutionize many industrial applications, from targeted material delivery to precision farming. However, several of the heterogeneous characteristics that make them ideal for certain future applications — robot **autonomy, decentralized control, collective emergent behavior**, etc. — hinder the evolution of the technology from academic institutions to real-world problems.
Blockchain, an emerging technology originated in the Bitcoin field, demonstrates that by combining peer-to-peer networks with cryptographic algorithms a group of agents can reach an agreement on a particular state of affairs and record that agreement without the need for a controlling authority. **The combination of blockchain with other distributed systems**, such as robotic swarm systems, can provide the necessary capabilities to make robotic swarm operations **more secure, autonomous, flexible and even profitable**.

Le ricerche effettuate negli ultimi anni hanno prodotto diverse soluzioni per l'integrazione di servizi e sistemi IoT, ma questi non hanno avuto un grande successo nel campo industriale

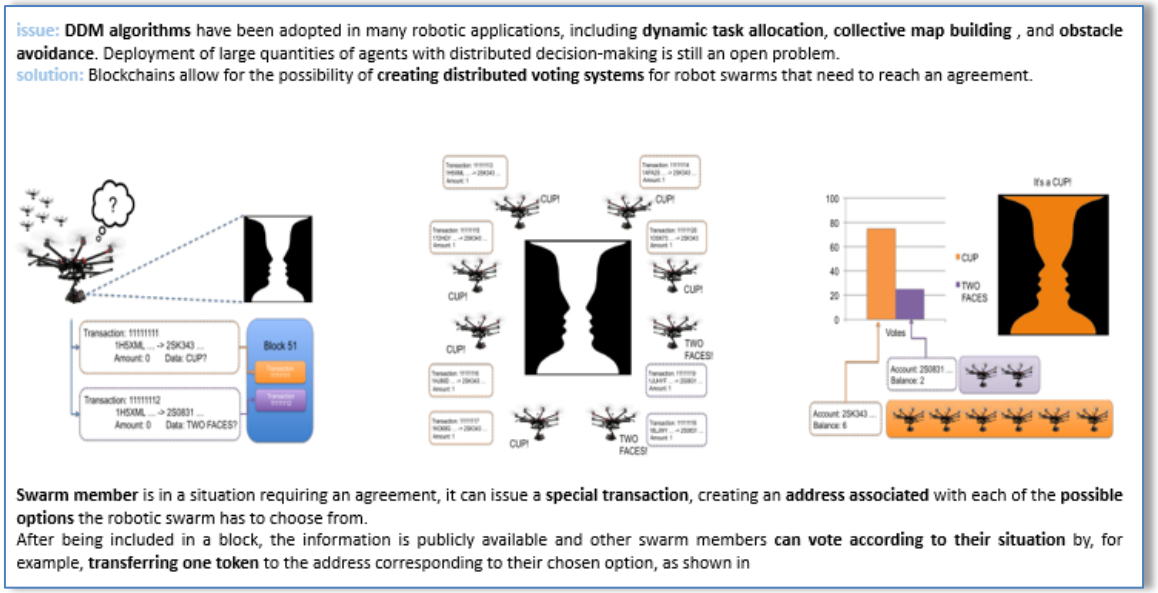
a seguito di diversi problemi, risolvibili tutti o in parte attraverso l'uso di una infrastruttura blockchain.
Di seguito analizzeremo alcune soluzioni a problemi noti e ne proporremo una possibile soluzione in ambito blockchain.
Il principale problema dei sistemi multi agente è senza dubbio la sicurezza. In ambito IoT ancora più sentita, data la particolare vulnerabilità dei dispositivi. In questo ambito l'uso di infrastrutture blockchain, nate per lo scambio di criptovalute, ha già ampliamente dimostrato la sua robustezza agli attacchi informatici ed alla capacità di isolamento di nodi malevoli. Di fatto la tecnologia adoperata riesce a combinare la crittografia su archivi praticamente immodificabile ed allo stesso tempo consentire la trasparenza e la verificabilità di ogni transizione da parte degli utenti del chain.
Un esempio di questo processo è descritto di seguito:

- Ogni dispositivo IoT presente nel chain dispone di fatto di due chiavi, una chiave pubblica che espone nella blockchain e ne rappresenta anche il suo account, ed una privata.
- Un dispositivo che vuole comunicare con un altro, genera un messaggio che codifica con la chiave pubblica del destinatario. Una volta pubblicato, il messaggio verrà ricevuto da tutti, ma soltanto il destinatario riuscirà a decifrarlo con la corrispondente chiave privata.

- Inoltre ogni ricevente può conoscere l'identità del mittente se quest'ultimo firma digitalmente il messaggio con la propria chiave privata. Di fatti, a partire da un messaggio cifrato con chiave privata è possibile risalire alla chiave pubblica associata.

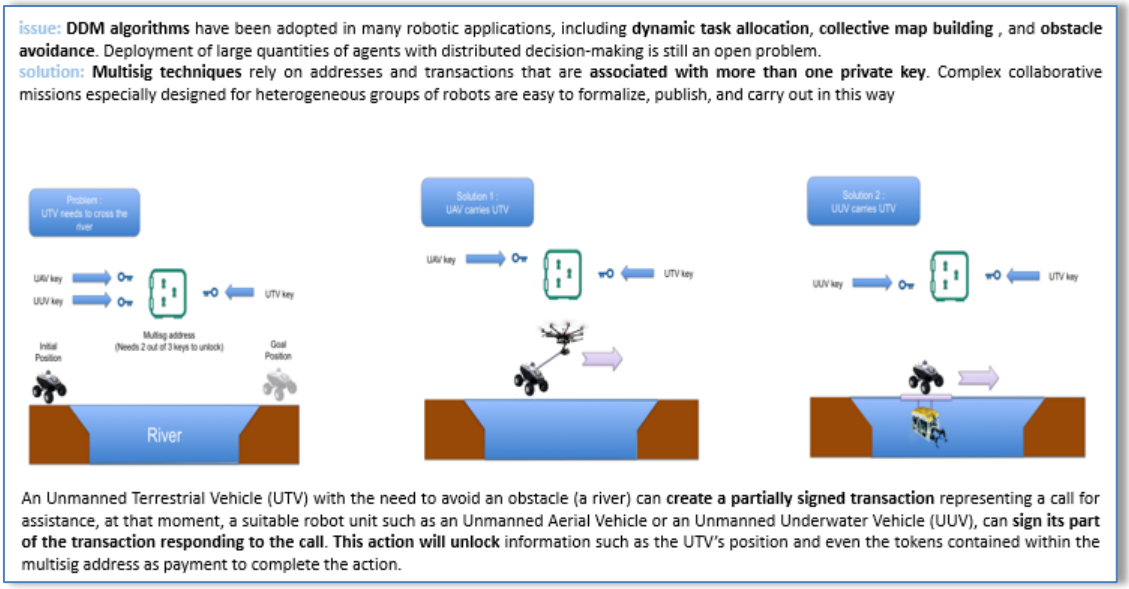


Gli algoritmi decisionali distribuiti sono stati adottati in molte applicazioni robotiche, tra cui l'allocazione dinamica delle attività, la costruzione di mappe collettive e l'elusione degli ostacoli. In questo contesto la blockchain è una tecnologia eccezionale per garantire che tutti i partecipanti di una rete decentralizzata possano condividere una visione identica del mondo. Ad esempio, attraverso l'uso di una blockchain si dà la possibilità di creare sistemi di voto distribuito in cui si può raggiungere un accordo in tempi molto rapidi.
Ogni volta che un membro di un gruppo di robot si trova in una situazione che richiede un accordo, può emettere una transazione speciale, creando un indirizzo associato a ciascuno delle possibili opzioni che lo sciame robotico deve votare. Dopo essere state incluse in un blocco, le informazioni sono disponibili pubblicamente, quindi gli altri membri dello sciame, possono votare in base alla loro situazione, ad esempio, trasferendo un token a l'indirizzo corrispondente all'opzione scelta. Il raggiungimento di un accordo come ad esempio attraverso la regola della maggioranza, può essere ottenuta rapidamente e in un modo sicuro e verificabile poiché tutti i robot possono monitorare gli indirizzi coinvolti nel processo di voto.



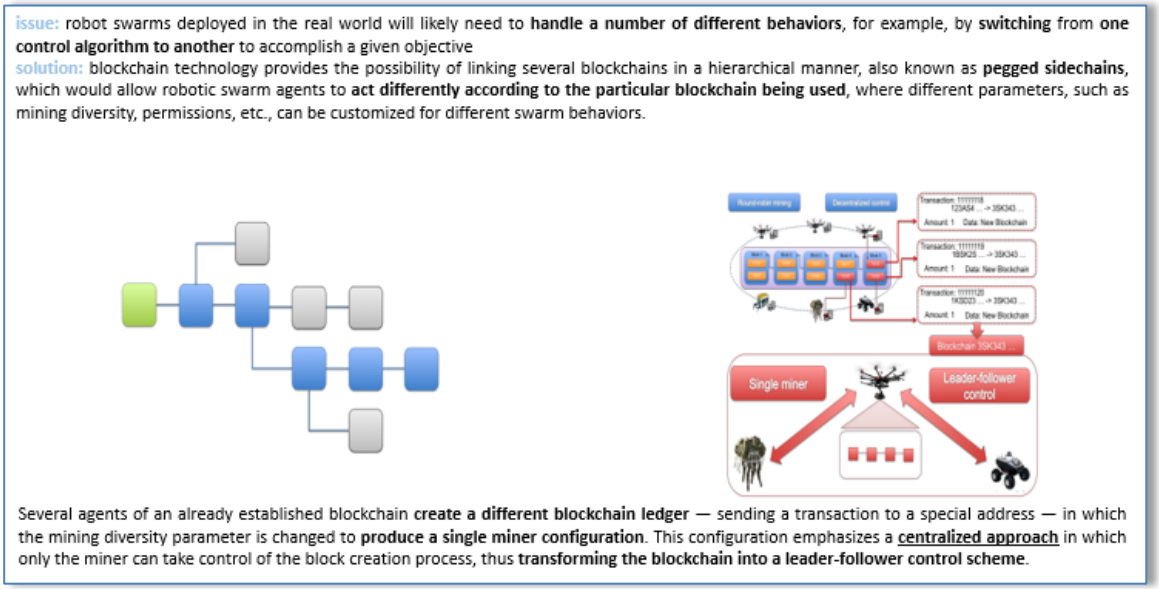
La differenziazione del comportamento è un altro dei problemi che può essere affrontato e risolto con l'ausilio delle blockchain**.** Si possono verificare ad esempio alcuni scenari dove uno sciame di robot dovrà gestire un numero di comportamenti diversi, ad esempio, commutando da un algoritmo di controllo all'altro per raggiungere un determinato obiettivo. In questo caso, la tecnologia blockchain offre la possibilità di collegare diverse blockchain in modo gerarchico, note anche come catene laterali ancorate, che consentirebbero agli agenti di agire in modo diverso a seconda della particolare blockchain in uso, con diversi parametri, con diversità dei miners, permessi, ecc., personalizzando per l'appunto i diversi comportamenti dello sciame.

Le blockchain risolvono allo stesso modo problemi di cooperazione che coinvolgano due o più dispositivi. Si pensi ad esempio ad un sistema di soccorso. Nell'immagine sottostante un veicolo di terra in difficoltà può emettere una transizione Multisig che per essere attivata necessita della sottoscrizione di due o più dispositivi. Nell'esempio, un drone o un veicolo subacqueo possono rispondere alla richiesta di soccorso del veicolo terrestre, sottoscrivendo la transizione ed acquisendo così un corrispettivo per il servizio svolto.



Oltre a presentarsi come una valida base per consentire lo sviluppo di algoritmi per gestire comportamenti collettivi è possibile allo stesso tempo prevedere e gestire la differenziazione del comportamento garantendo autonomia a flessibilità.

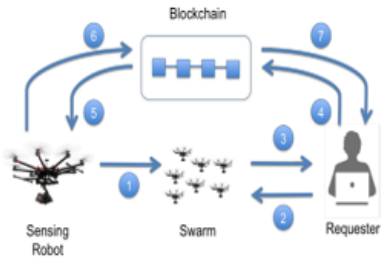
Nello scenario che presentiamo nella slide sottostante, un dispositivo che si troverà difronte ad un problema da gestire diverso dalla mission del gruppo, può creare una catena laterale ancorata ed arruolare un certo numero di dispositivi per poterlo risolvere. Una volta risolto il sotto problema i dispositivi coinvolti possono tornare a svolgere la normale attività.



Infine, le blockchain danno l'impulso a diversi sistemi o modelli di business basato su i dispositivi IoT.

Tra questi vediamo di seguito il modello Sensing-as-a-Services, in cui in questo scenario si evidenziano i due diversi approcci di comunicazione: on-chain ed off-chain. Esiste cioè una fase di preaccordo in cui un utente chiede un servizio utilizzando un tradizionale canale di comunicazione off-chain. Una volta finalizzato l'accordo, la comunicazione può essere veicolata sulla blockchain.

issue: The **lack of business models** hinder the progress to more broader commercial applications
solution: **Sensing-as-a-Service** is an emerging business model pattern, which is rising in the Internet of Things (IoT) field. SaaS helps to create multi-sided **markets for sensor data in which one or more customers** (the markets' buying side) subscribe to and pay for data that is provided by one or more sensors (selling side).



Individual robots register into a swarm where they can be found by a requester. Robotic swarms in this case can be regarded as a list of addresses where additional information, including the location of each agent, price of data provided, etc., can be found. The requester can ask for a complete list of these robots and their sensing services and send its corresponding payment directly to the robot's public address.

Come già anticipato nell'introduzione, la tecnologia blockchain anche se mostra innumerevoli vantaggi nel suo utilizzo, presenta ancora alcune limitazioni che ne impediscono l'applicabilità in più contesti.
La principale è naturalmente la latenza nell'approvazione delle transizioni.

Latency: The latency issue becomes **highly relevant** when robots are used in formation control or cooperative tasks. Currently, with the most widely used version of the blockchain — Bitcoin — a block takes **around 10 minutes** to be processed. **Collisions** or **other inconveniences** might arise in situations when **there is a mismatch** between the current state of affairs and the one in which the transaction was originated.

Size, throughput and bandwidth: If **large quantities of robots** are deployed for long periods of time, they might **expand the blockchain** to a point where they cannot keep a copy of the full ledger of transactions anymore. Even though important parameters such as the **block size** (how many transactions are included in each block). This limitation severely compromises the **throughput** of the system in busy networks with a large number of agents. Solution would be to create parallel blockchains where block size and frequency parameters are optimized for different types of information.

Application specific blockchain (Ternedermint)

Oggi sono molti gli studi che cercano di combinare l'uso della tecnologia blockchain con i sistemi di calcolo distribuiti ed i sistemi IoT. Di seguito ne riportiamo solo alcuni.

Related Works:

- ✓ **An Energy Blockchain, a use case on Tendermint**. M.L. Di Silvestre at all. DEIM University of Palermo, Italy 2018.
  Focused on the procedures for generating blocks and defining data structures for storing energy transactions in microgrids.
- ✓ **From Agents to Blockchain: Stairway to Integration**. Giovanni Ciatto at all. Appl. Sci. 2020.
  A custom blockchain integrating concepts borrowed from agent-oriented programming (e.g., programming agents through smart contracts)
- ✓ **Towards Trustless Prediction-as-a-Service**. Gautham Santhosh at all. 2019 IEEE International Conference on Smart Computing.
  They presented the Trustless Prediction-as-a-Service (TPaaS) framework: a blockchain-based system for secure deployment and provisioning of prediction APIs in Cloud environments
- ✓ **Threshold Cryptography with Tendermint Core**. Christian Cachin, Cryptology and Data Security Group Insitute of Computer Science University of Bern, Switzerland.
  Threshold cryptography provides protocols and techniques for building secure distributed systems and services that perform cryptographic operations while tolerating multiple faults and security breaches occurring at the same time.
- ✓ **DeepChain: Auditable and Privacy-Preserving Deep Learning with Blockchain-based Incentive**. Jiasi Weng at all. IEEE Transactions on Dependable and Secure Computing, 2021
  However, there are many security problems neglected in federated learning, for example, the participants may behave incorrectly in gradient collecting or parameter updating, and the server may be malicious as well. this work present a distributed, secure, and fair deep learning framework named DeepChain to solve these problems

Alcuni di questi studi hanno evidenziato una spiccata versatilità ed una elevata velocità di risposta della piattaforma di sviluppo per blockchain Tendermint.

Tendermint is a blockchain that allows the **secure and consistent replication of an application** on different machines.
Safe because it works even if 1/3 of the machines fail arbitrarily (capacity known as **Byzantine-BTF fault tolerance**) and consistent because each machine sees the same transactions and are in the same state.

The advantage of using Tendermint, as compared to the other blockchains, is the **possibility of using any programming language** to write the code of the **App** to **process the transactions** to be included in the blockchain blocks.

Speed. Once a transaction is included in a block, it is immediately finalized. There is no need to wait for confirmations. Tendermint Core can have a block time on the order of **1 second** and can handle thousands of transactions per second.

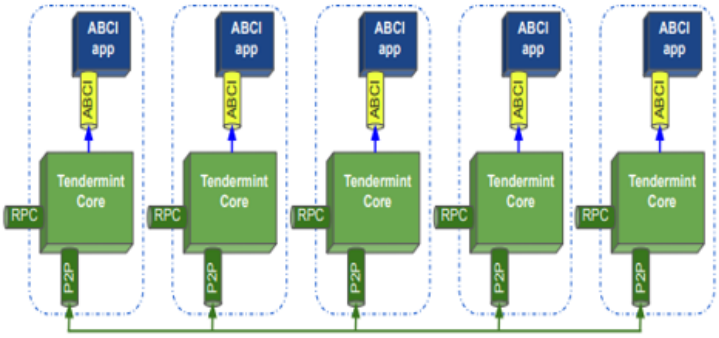
Modularity. Tendermint consists of **two main technical components**: a consent engine (Tendermint Core) and an interface application (Application BlockChain Interface - ABCI)

Developers can allow the application to have an electoral system that elects validators based on their native tokens by creating the one that it is called **Proof-of-stake for a public blockchain**. In addition, developers can create an application that defines a narrow set of pre-approved validators that deal with the consensus for new nodes entering the ecosystem. This is called **proof-of-authority** and is the distinctive consent mechanism of an **authorized or private blockchain**.

La piattaforma fornisce un algoritmo di consenso denominato Byzantine-BTF fault tolerance ed una serie di librerie che ne consentono l'uso con diversi linguaggi di programmazione. L'infrastruttura di sistema si compone da un nodo client che comunica con gli altri pari attraverso un canale Peer to Peer (P2P) nella realizzazione dell'algoritmo di consenso BTF. Inoltre ogni nodo espone un servizio di remote procedure call (RCP) a cui l'applicazione distribuita può accedere per richiedere i servizi del chain.

In ascolto ad ogni richiesta RPC o ad ogni richiesta proveniente dal canale P2P troviamo un middleware denominato ABCI che realizza la logica applicativa dell'infrastruttura.

In order to receive transactions from Tendermint Core via the ABCI, a client application has to implement a wrapper, called ABCI application. Except for Tendermint Core, nothing else should communicate with the ABCI application, to guarantee deterministic results. Tendermint Core and the ABCI application together form a node, and multiple nodes form a Tendermint peer-to-peer-network. A client can send transactions to be processed by Tendermint Core to any node in the network over a Remote Procedure Call (RPC) protocol. This REST interface can also be used for stating queries.



Una applicazione ABCI per funzionare deve implementare almeno tre dei diversi metodi di gestione delle transizioni. Il metodo CheckTx che viene richiamato ogni qualvolta il nodo è chiamato a validare una singola transizione; il metodo DeliverTx che viene richiamato ogni volta che si innesca un meccanismo di voto per l'approvazione di un nuovo blocco nella chain ed il metodo Commit che rende persistente lo stato di ogni nodo al termine di una fase di approvazione di un bocco.

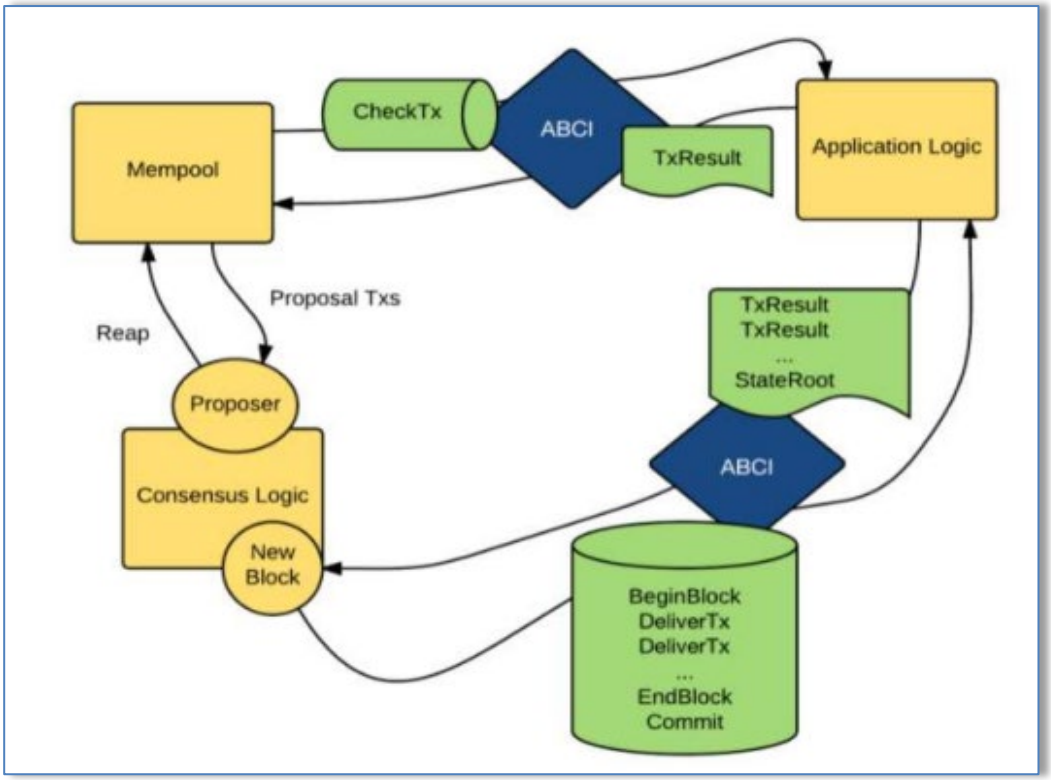
The ABCI consists of three primary messages types, that get delivered from Tendermint Core to the ABCI application, which replies with a corresponding response message.

CheckTx. Before a transaction is relayed to the other peers, Tendermint Core **checks the validity of a transaction.** More precisely, Tendermint Core checks the validity by calling the ABCI application, which replies with an approval or an error.

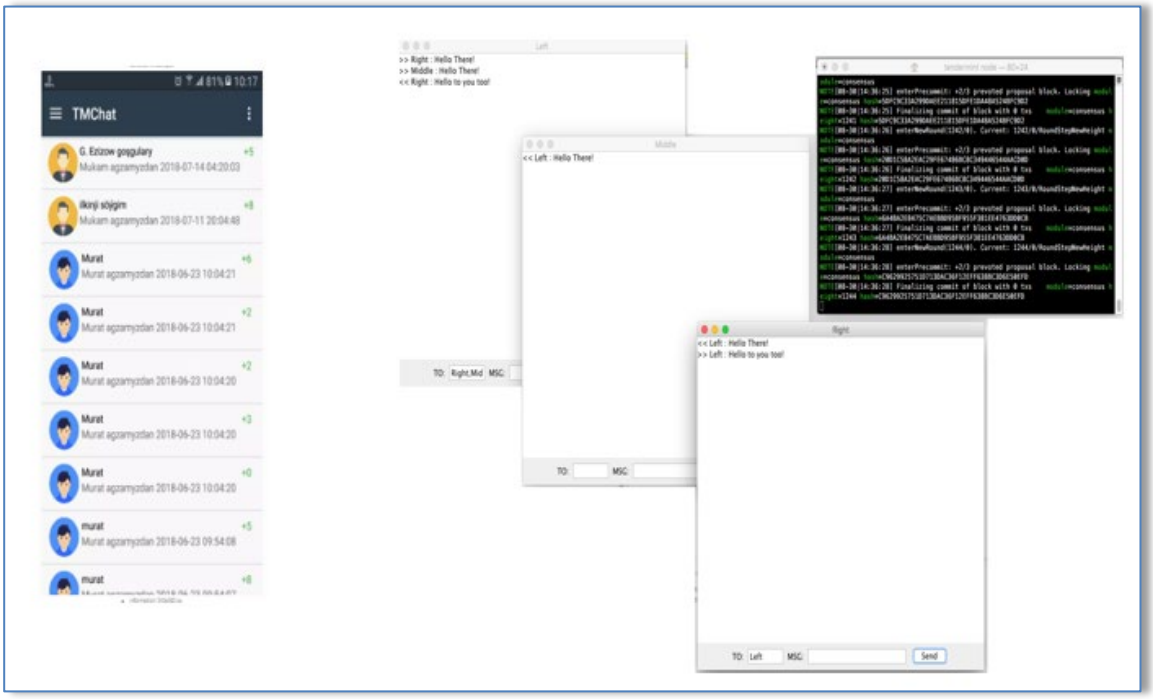
DeliverTx. Each transaction in the blockchain is delivered to the ABCI application with a DeliverTx message. When a transaction with this message is received, the ABCI application has to validate it against the current state of the application, the application protocol, and the cryptographic credentials of the transaction. A validated transaction will **update the application state.**

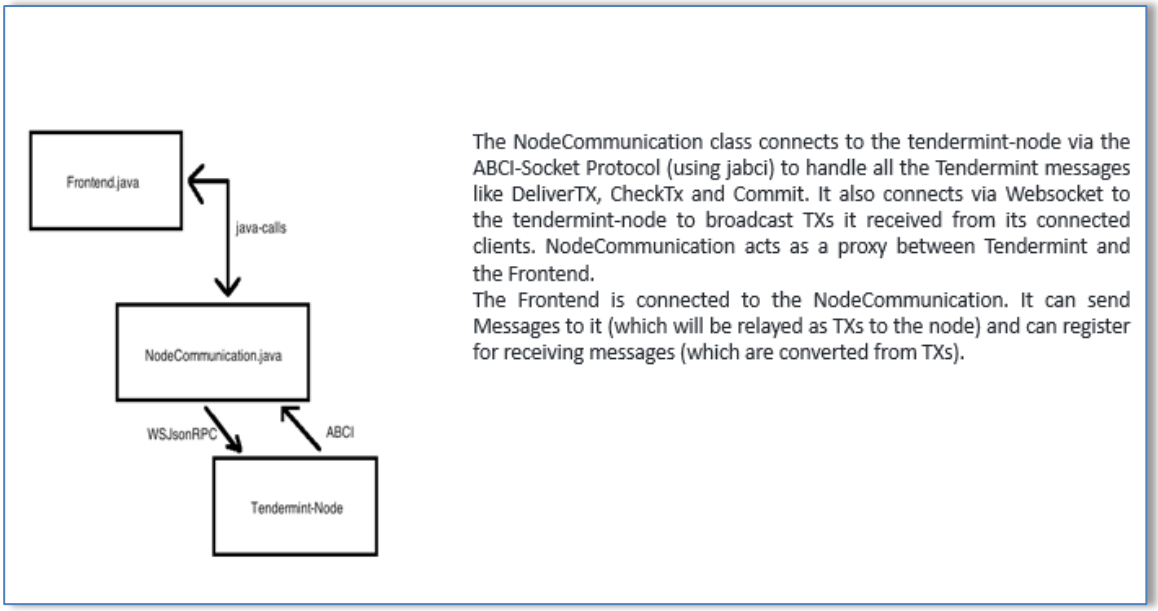
Commit. This message is used to **compute a cryptographic commitment to the current application state,** to be placed in the next block.

Le transizioni approvate dal metodo checkTx vengono momentaneamente inserite in una memoria locale denominata "Mempool" che viene svuotata dopo un'operazione di approvazione di un nuovo blocco.

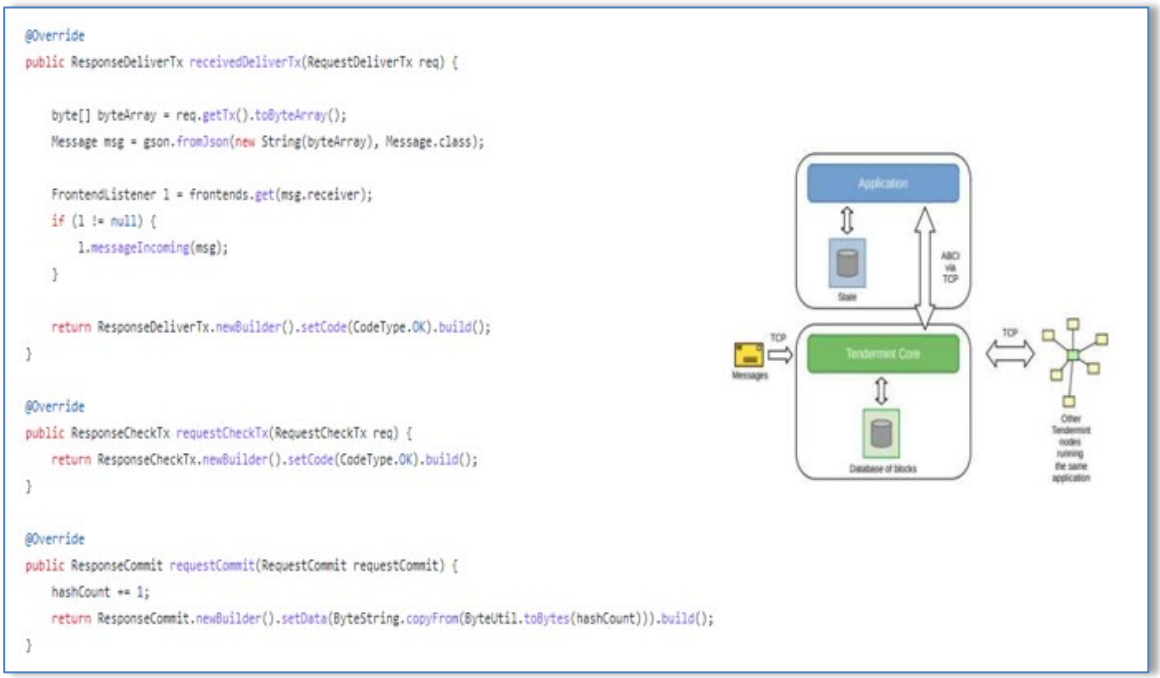


A titolo esemplificativo di seguito viene mostrata una applicazione distribuita (DAPP) che realizza una chat attraverso una blockchain Tendermint. La chat è disponibile sia in versione App Android che per in applicazione Java per laptop.





I metodi usati per realizzare l'infrastruttura blockchain sono molto semplici, non richiedono l'uso di criptovalute pertanto non sono necessari meccanismi di verifica all'interno delle singole funzioni del blocco ABCI.



```
@Override
public ResponseDeliverTx receivedDeliverTx(RequestDeliverTx req) {

    byte[] byteArray = req.getTx().toByteArray();
    Message msg = gson.fromJson(new String(byteArray), Message.class);

    FrontendListener l = frontends.get(msg.receiver);
    if (l != null) {
        l.messageIncoming(msg);
    }

    return ResponseDeliverTx.newBuilder().setCode(CodeType.OK).build();
}

@Override
public ResponseCheckTx requestCheckTx(RequestCheckTx req) {
    return ResponseCheckTx.newBuilder().setCode(CodeType.OK).build();
}

@Override
public ResponseCommit requestCommit(RequestCommit requestCommit) {
    hashCount += 1;
    return ResponseCommit.newBuilder().setData(ByteString.copyFrom(ByteUtil.toBytes(hashCount))).build();
}
```