SCHOOL OF MANAGEMENT

UNIVERSITÀ LUM JEAN MONNET

Master I Livello

MIGEM

"Master in Imprenditorialità e General Management dell'Industria Creativa e 4.0"

TESI IN

INDUSTRIA DIGITALE 4.0

BLOCKCHAIN, BITCOIN E ALGORITMI MATEMATICI: L'EVOLUZIONE DELL'INTERNET OF THINGS NEL MONDO DELL'INDUSTRIA 4.0

Relatore:
Prof. Michele RUBINO

Candidato:
Dott. Stefano FRANCO

ANNO ACCADEMICO 2017 / 2018

ECE0A06D3222DAA2A8B6A090794142797

F6C4FD55A47B96CFADD23509CF335CD

Sommario

Introduzione 6

1. La tecnologia Blockchain e il contesto Industry 4.0 9

1.1 Cos'è la Blockchain e come funziona 9

1.1.1 La basi della tecnologia 10

1.1.2 Architettura dei sistemi 11

1.1.3 Principi di funzionamento 13

1.2 Tecnologie esponenziali e algoritmi matematici 14

1.2.1 La definizione di Ray Kurzwail 14

1.2.2 La matematica come forma di democratizzazione 15

1.2.3 Teoria dei Giochi e Crittografia 17

1.3 Collegamenti con l'Industry 4.0 e scenari futuri 19

1.3.1 Industry 4.0 ed economia digitale 19

1.3.2 Internet of Things 21

1.3.3 Ipotesi di evoluzione 22

2. Mainstream e applicazioni della Blockchain 25

2.1 Bitcoin e cryptovalute 25

2.1.1 Satoshi Nakamoto e il primo Whitepaper 26

2.1.2 Le implicazioni della moneta digitale 28

2.1.3 Altre Crypto 29

2.2 Le Blockchain alla base delle Crypto 30

2.2.1 Il Proof of Work (PoW) 30
2.2.2 Il Proof of Stakes (PoS) 33
2.2.3 Altri modelli 35
2.3 Applicazioni 36
2.3.1 Fintech 36
2.3.2 Pubblica Amministrazione 39
2.3.3 Smart Contracts e dApps 40
3. Il gruppo Blocktech: casi di studio e sperimentazioni 42
3.1 Il gruppo Blocktech: introduzione 42
3.1.1 Alumni Mathematica è lo *#ImproveTheWorld* 43
3.1.2 Le origini del gruppo Blocktech 44
3.2 Le applicazioni nel settore finanziario 46
3.2.1 Il Sell Wall Detector Tool 46
3.2.2 BTC Notify – Bot Telegram 47
3.2.3 Consulenza e formazione 49
3.3 Altre applicazioni 50
3.3.1 Pubblica Amministrazione 50
3.3.2 Blockchain proprietaria 52
3.3.3 Esperimenti di mining 54
Conclusioni 55
Riferimenti 56
Bibliografia 56
Sitografia 56
Ringraziamenti 57

“I miei più calorosi ringraziamenti al governo

degli Stati Uniti, ai senatori McCain e Lieberman

per aver spinto Visa, MasterCard, Payal, AmEx,

Mooneybookers, e altri, nella costruzione di un blocco

bancario illegale contro WikiLeaks a partire dal 2010.

Questo ha causato il nostro investimento in Bitcoin,

con un guadagno maggiore del 50000%”

Julian Assange (Wikileaks) via Twitter il 14 ottobre 2017

Introduzione

Il 17 dicembre 2017 balzava agli onori di cronaca su quasi tutte le tv nazionali il Bitcoin, la cryptovaluta che superava la soglia dei 20.000$ e che nell'arco dell'anno aumentava il proprio valore con un tasso del +2.000%.

Per quanto mi riguarda la conoscenza del Bitcoin cominciava un po' prima, a luglio 2017. Diciamo che è stata una folgorazione. Qualcuno me ne ha parlato, abbiamo ragionato un po', ho fatto molte domande. E poi, boom! Non riuscivo a credere quanto potesse essere importante quello che avevo appena imparato. No, non si trattava del Bitcoin, ma della tecnologia alla base delle cryptovalute, la Blockchain! Non riuscivo a capire in quel momento tutti i passaggi, capivo solo che il paradigma tecnologico alla base della blockchain era un qualcosa che avrebbe sicuramente cambiato il mondo del prossimo futuro. Non ci è voluto molto affinché attivassimo in *Alumni Mathematica*, l'associazione di ricerca scientifica indipendente che ho costituito qualche anno fa e che ho l'onore di guidare come presidente, un gruppo di persone interessate al tema. Con la solita reattività che contraddistingue Alumni Mathematica abbiamo organizzato da lì a due mesi, il 14 novembre 2017, il primo evento a Bari aperto al pubblico su blockchain e bitcoin. Evento che ha riscosso un grandissimo interesse di pubblico e che ci ha spinto a continuare ad approfondire la tematica, in maniera scientifica e razionale. Decidemmo insieme all'amico e collega Ing. Vito Pesola di dar vita al gruppo *Blocktech*, spinoff di Alumni Mathematica, con l'obiettivo di esplorare la tecnologia blockchain, realizzare una nostra blockchain e lanciare una *ICO* (*Initial Coin Offering*). Da quel momento non ci siamo più fermati, e abbiamo collezionato esperienze molto importanti.

Fin dall'inizio di questa avventura, una delle mie personalissime battaglie è stata quella di scindere dall'immaginario collettivo cosa fosse Bitcoin e cosa fosse Blockchain. Si

tratta di tematiche sicuramente collegate tra loro, ma che appartengono a sfere di interesse completamente differenti. La Blockchain è la tecnologia alla base del progetto Bitcoin, e il Bitcoin ha il grande merito di aver portato la blockchain agli onori di cronaca e al pubblico di massa. Ma i collegamenti finiscono lì. È opportuno riuscire a separare le due sfere di interesse in modo che possa essere dato spazio alla tecnologia di sedimentare nella mente dei tecnologi e dei curiosi, scevra dalla sfera speculativa che avvolge inevitabilmente il Bitcoin e le altre cryptovalute.

Nella sequenza temporale degli avvenimenti di novembre 2017, ho avuto la grande opportunità di iniziare la frequenza del master MIGEM, e di ricevere tanti spunti dai docenti dei vari moduli che sono serviti alla mia maturazione professionale. In particolare, gli insegnamenti legati al mondo dell'Industry 4.0 sono stati particolarmente vicini alle mie corde.

Il presente *Project Work* nasce come connubio tra due temi apparentemente distaccati, come Blockchain e Industry 4.0, che in realtà hanno molto in comune e che bisogna trattare con la massima attenzione. Si tratta, infatti, di due tra i temi principali su cui si concentreranno i business dei prossimi anni, anche per le opportunità che deriveranno dagli investimenti pubblici e privati.

Nel primo capitolo verranno introdotti i due argomenti. Da un lato verrà introdotta la tecnologia Blockchain, con un approfondimento sull'architettura dei sistemi, i principi di funzionamento e i modelli matematici e algoritmici presenti. Poi verrà introdotto il contesto Industry 4.0 e, in particolare, si approfondirà l'*Internet of Things* (*IoT*), una delle sue tecnologie abilitanti. Si contestualizzerà a questo punto il legame che c'è tra la Blockchain e l'IoT: si vedrà perché la prima può a buon diritto essere considerata la massima evoluzione della seconda.

Nel secondo capitolo si procederà ad illustrare le principali applicazioni della Blockchain. Cominceremo con un'introduzione del Bitcoin, che resta comunque uno dei principali prodotti del sistema blockchain. A questo punto vedremo quali sono le differenze tra le varie Blockchain, il perché ne esistono più di una e come capire qual è la Blockchain migliore per sviluppare un dato prodotto. Infine, descriveremo quali sono i settori principali su cui attualmente si stanno concentrando i progetti blockchain.

Nel terzo ed ultimo capitolo, racconteremo meglio l'esperienza del gruppo Blocktech, illustrando i lavori realizzati, i progetti in corso e gli obiettivi futuri.
È venuto fuori un lavoro che sembra raccontare un viaggio, alla scoperta dapprima delle bellezze teoriche della tecnologia e poi delle reali applicazioni e dei casi di utilizzo.
E come tutti i viaggi che si rispettino, c'è un inizio e una fine.
E se questo viaggio è cominciato il 14 novembre 2017, per quelle strane circostanze – che però se uno sa leggere le storie capisce che non sono strane – è un percorso che finisce un anno dopo. Ma solo per fermarsi un attimo, guardare la strada fatta, e poi continuare di nuovo.

Bari, 14 novembre 2018

Stefano Franco

“Blockchain – not Bitcoin –
will prove revolutionary in banking”

1. La tecnologia Blockchain e il contesto Industry 4.0

1.1 Cos’è la Blockchain e come funziona

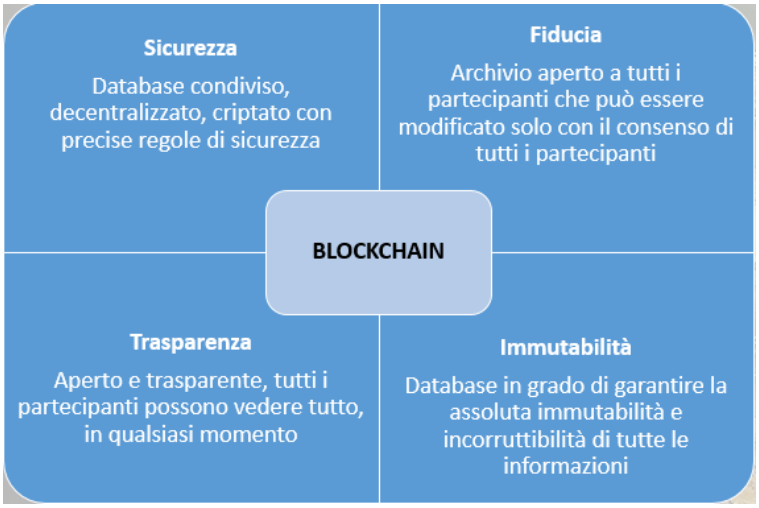
La Blockchain è una tecnologia che nasce per proteggere le informazioni contenute nei documenti digitali. È una tecnologia che porta avanti il paradigma del network *peer-to-peer*, dove non c’è un’entità centrale che garantisce l’integrità del sistema ma tutto si basa sul *trust* tra i nodi. È stata inventata per creare una moneta alternativa – il Bitcoin – ma poi è stata utilizzata per una serie di altre applicazioni, che vanno dalla sicurezza delle

firme digitali, alla garanzia dei sistemi di voto. In questo paragrafo spiegheremo come funziona e cosa la rende speciale.

1.1.1 La basi della tecnologia

La tecnologia della Blockchain si basa su quattro concetti:

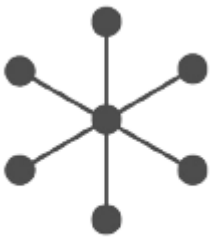
- *Sicurezza:* il sistema sviluppato è un database condiviso, all'interno del quale le informazioni vengono distribuite in maniera decentralizzata, senza che ci sia un'unità centrale che garantisca il controllo; tale sistema, attraverso sofisticate regole di crittografia, risulta criptato e assolutamente sicuro.
- *Fiducia*: le informazioni contenute all'interno della blockchain sono aperte per tutti coloro che intendono accedervi e le modifiche possono essere autorizzate solamente quando ricevono il consenso di tutti i partecipanti.
- *Trasparenza:* tutto l'archivio delle informazioni è consultabile nella sua interezza e ogni volta che viene effettuata una modifica essa viene immediatamente riportata all'interno del registro pubblico accessibile a chiunque.
- *Immutabilità:* attraverso regole legate alla crittografia, una volta che una modifica ha ricevuto un certo livello di convalida sufficiente, il sistema garantisce l'assoluta immutabilità e incorruttibilità di tutte le informazioni.



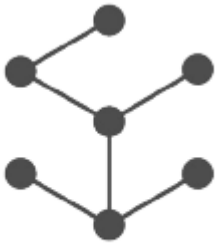
1.1.2 Architettura dei sistemi

A partire dagli anni ’50, e quindi da quando l’informatica ha cominciato a muovere i primi passi, i grossi calcolatori adibiti a svolgere calcoli e operazioni logiche sono stati organizzati e coordinati tra loro con l’obiettivo di rendere tutta l’infrastruttura il più efficiente e sicura possibile. I sistemi centralizzati, ossia quei sistemi che necessitano di un’unità centrale di controllo e gestione, si sono affermati per la loro semplicità di costruzione e coordinamento. Tra gli anni ’70 e ’80, tuttavia, tale modello è stato messo in discussione: le nuove innovazioni tecnologiche e, soprattutto, la maggiore economicità e qualità dei servizi, hanno favorito l’avvento di sistemi decentralizzati. I limiti che si sono riscontrati nel corso del tempo nell’utilizzo di sistemi centralizzati sono stati:

- accentramento del potere;
- assenza di neutralità del potere;
- costi di manutenzione di server elevati:
- scarsa sicurezza e resistenza ad attacchi informatici.



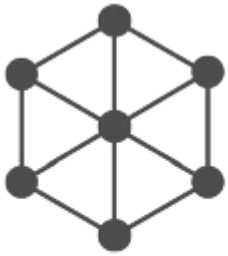
Esempio di Sistema Centralizzato



Esempio di Sistema Decentralizzato

La Blockchain altro non è che la realizzazione di un database distribuito chiamato *distribuited ledger*, in italiano libro mastro. Incarna il miglioramento di database tradizionali, centralizzati e decentralizzati, sfruttando la tecnologia *peer-to-peer* ed ha lo scopo di racchiudere al suo interno qualunque transazione eseguita nel contesto di una determinata rete. È basata su quello che prende il nome come sistema distribuito, ossia un’applicazione dove non esiste più un’unità cardine. Una rete peer-to-peer, abbreviata *P2P*, rappresenta un modello logico di rete in cui ogni nodo è equivalente a tutti gli altri.

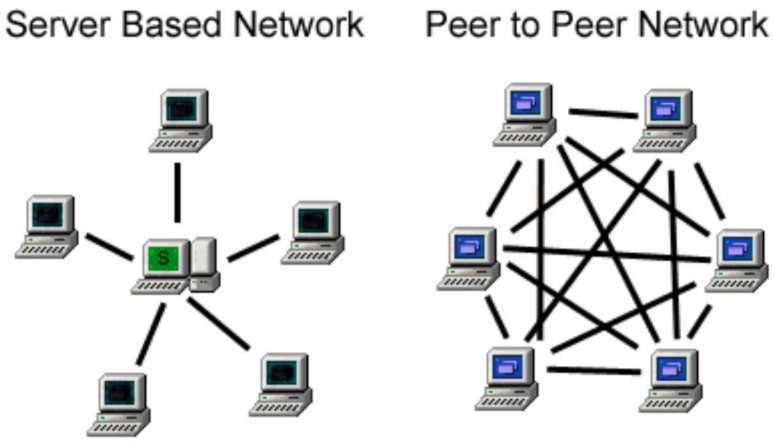
Queste reti hanno la grande caratteristica che non esiste un sistema server dedicato alla gestione delle informazioni, ma ogni nodo funge contemporaneamente da punto di gestione dell'informazione e trasmissione della stessa.



DISTRIBUTED

Esempio di Sistema Distribuito

All'interno di queste reti, ciascun nodo ha pari capacità e responsabilità, il ché differisce molto dal modello classico *client/server*[1]*:* in un sistema P2P ogni nodo è in grado di ricoprire sia il ruolo di *client* che di *server*, a seconda dell'esigenza del sistema in un dato momento.



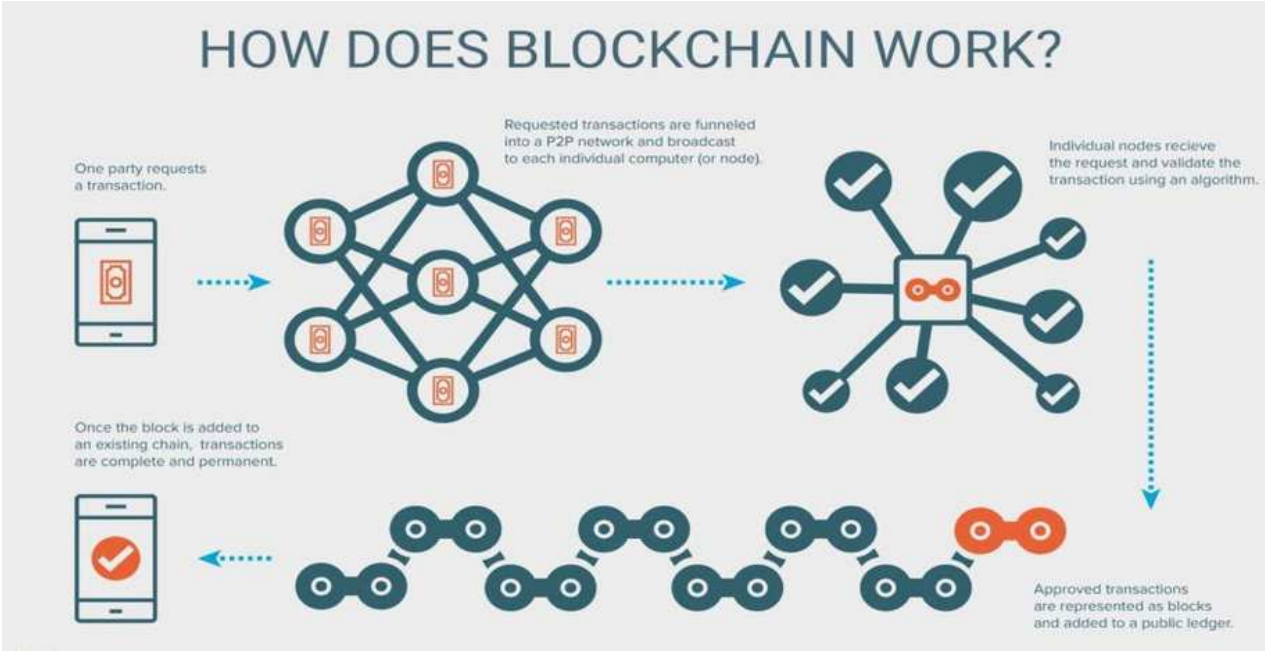
Architettura client/server vs P2P

[1] Si tratta di un'architettura di rete nella quale genericamente un computer *client* o terminale si connette ad un *server* per la fruizione di un certo servizio

1.1.3 Principi di funzionamento

La Blockchain è dunque un aperto e continuamente crescente database distribuito. I processi e le attività transitano tra i vari contributori senza il controllo di un amministratore centrale. Tutti i partecipanti all'interno del network della blockchain possiedono una copia di questo registro distribuito e possono caricare modifiche attraverso un meccanismo e un protocollo di consenso. La sicurezza delle transazioni è legata a precise regole di crittografia che rendono molto difficile le alterazioni indebite. Il registro della blockchain è replicato su tutti i nodi computazionali del network, in modo da evitare la presenza di un unico punti di fallimento.

Più in dettaglio il funzionamento è descritto dall'immagine sottostante:



Sintesi di funzionamento di un sistema Blockchain (fonte G2 Crowd)

Ogni volta che una unità richiede una transazione, tale richiesta entra all'interno del network P2P, ovvero all'interno dei computer degli individui che hanno autorizzato la presenza di nodi computazionali. Attraverso un *algoritmo di consenso*[2], i singoli nodi autorizzano e validano la richiesta ricevuta e, solo quando queste validazioni rispettano il

[2] Nel successivo paragrafo 2.2 maggiori dettagli

protocollo di consenso della blockchain, vengono inserite all'interno di *blocchi*[3] che poi vengono aggiunti al registro distribuito. Non appena il blocco viene aggiunto alla catena, le transazioni richieste vengono inserite nella blockchain, e sono da quel momento complete e permanenti.

1.2 Tecnologie esponenziali e algoritmi matematici

Durante il SingularityU Summit, l'evento globale promosso dalla *Singularity University*[4], la blockchain è stata inserita nella lista di quelle che vengono definite *tecnologie esponenziali*, ossia quelle tecnologie che hanno la caratteristica di crescere molto velocemente in termini di impatto nel mondo. Conoscere le funzionalità e le potenzialità di tale tecnologia diventa dunque fondamentale, in quanto consente di posizionarsi in maniera consapevole nel futuro. Tale conoscenza non può prescindere da quelli che sono i fondamenti teorici della blockchain – e, in generale, di ogni forma di tecnologia – che quasi sempre risiedono nei principi logici e negli algoritmi matematici.

1.2.1 La definizione di Ray Kurzwail

Ray Kurzwail è un inventore, informatico e saggista statunitense[5]. È autore di numerosi libri sulla salute, l'intelligenza artificiale, il transumanesimo e la singolarità tecnologica. In uno dei suoi libri Kurzwail, partendo da un'analisi storica dell'impatto delle tecnologie, dimostra che l'evoluzione del progresso tecnologico è un processo che cresce come un modello esponenziale, e non come un modello lineare. Egli, infatti, afferma:

<< Un processo evoluzionistico, e sia la biologia che la tecnologia sono processi evoluzionistici, nel tempo accelera. Il motivo è perché funzionano per interazione, cioè creano una funzionalità, e poi utilizzano quella funzione per fare il prossimo passo. >>

[3] Letteralmente *Blockchain* significa "catena di blocchi"
[4] La *Singularity University* è un'organizzazione a scopo di lucro cha eroga corsi con l'obiettivo di "educare, ispirare e aiutare i leader ad applicare le tecnologie esponenziali per affrontare le grandi sfide dell'umanità". Sito web: https://su.org
[5] Pagina di wikipedia: https://it.wikipedia.org/wiki/Raymond_Kurzweil

Kurzwail ha inserito all'interno di un grafico in scala logaritmica le 15 differenti liste di cambiamenti paradigmatici per la storia umana, preparata da filosofi, scienziati e accademie blasonate, mostrando per l'appunto una crescita esponenziale. Il grafico dimostra che c'è una precisa legge matematica che governa l'evoluzione del cambiamento e della complessità nell'Universo, e che quindi è possibile effettuare studi preliminari per prevedere l'impatto delle nuove tecnologie nel corso del tempo.

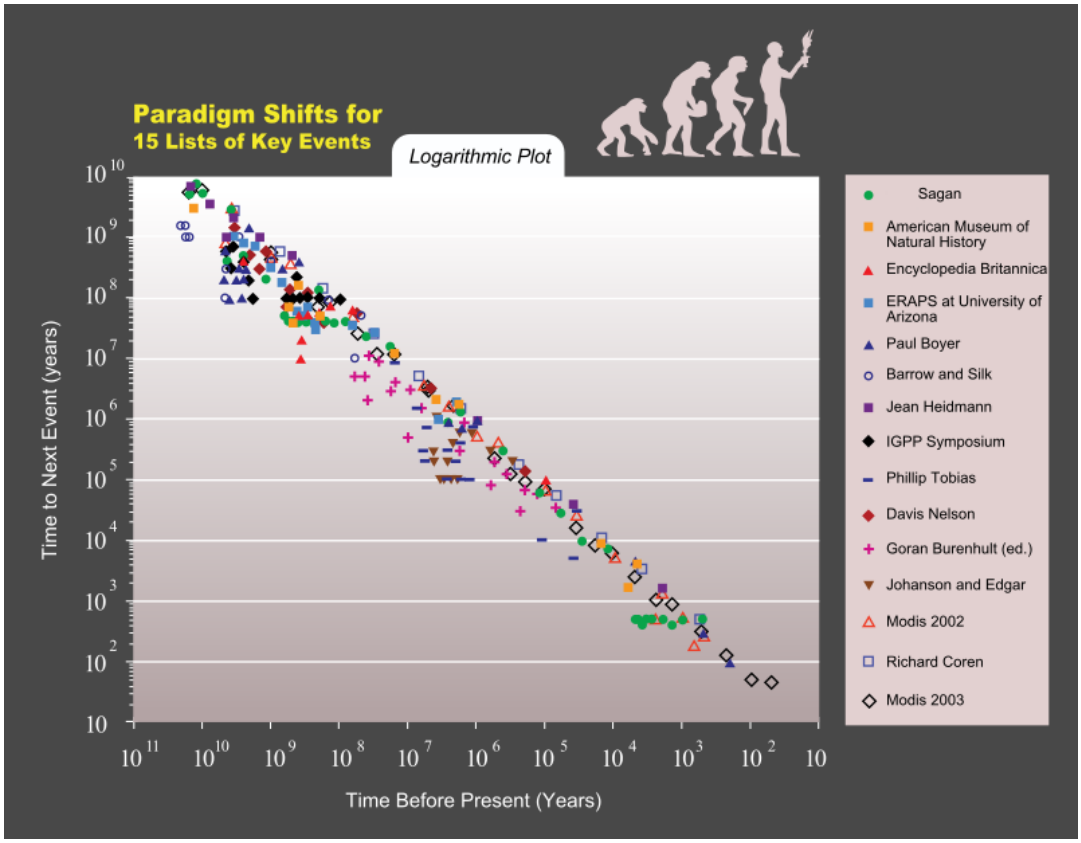


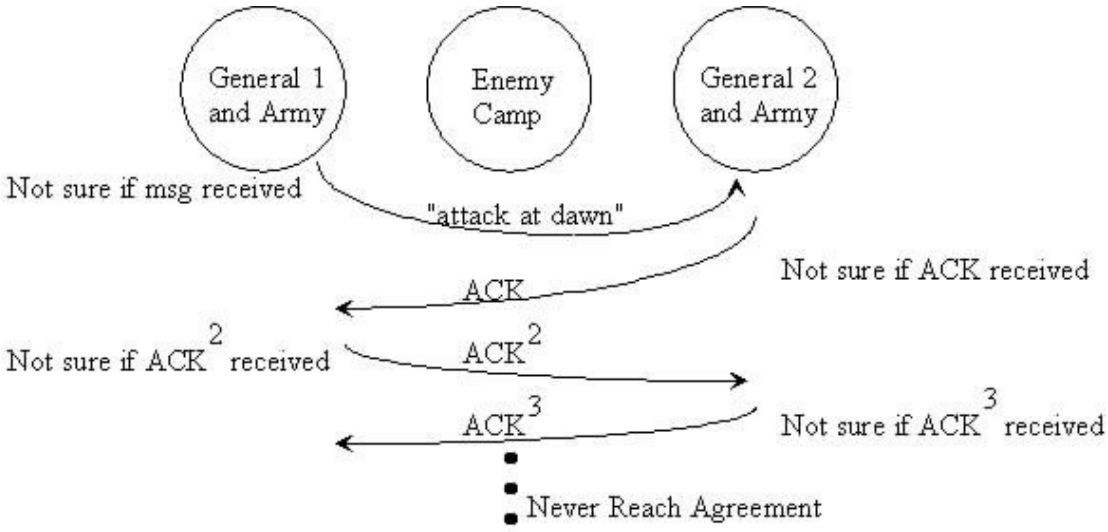
Grafico di Ray Kurzweil che dimostra la crescita esponenziale delle principali innovazioni

1.2.2 La matematica come forma di democratizzazione

Le leggi matematiche sono quindi fondamentali per riuscire a comprendere realmente l'evoluzione del mondo, cercare di prevedere il prossimo futuro e, in generale, vivere consapevolmente la vita di ogni giorno. Contrariamente a quanto si possa pensare in

primissima analisi, la matematica è presente in maniera davvero importante all'interno della blockchain, anzi senza matematica molto probabilmente non esisterebbe nessuna blockchain. I meccanismi che regolano la blockchain sono basati su algoritmi matematici, crittografia e teoria dei giochi. In particolare, il *Trust*[6]della blockchain è sviluppato attraverso un approccio del tutto nuovo e originale dato a quello che va sotto il nome di *Problema dei Generali Bizantini.*

Questo problema è un rompicapo basato sulla possibilità di un generale bizantino di inviare strategie di assalto al nemico a propri luogotenenti che sono localizzati in posti differenti. Come può il generale essere certo che queste strategie siano state ricevute correttamente, pur sapendo che tra le truppe si nascondono spie e traditori che farebbero di tutto per alterare il messaggio originale confondendo le truppe bizantine?



Schema di Problema dei Generali Bizantini

L'approccio classico di risoluzione del problema consiste nella individuazione di figure fiduciarie, con una affidabilità e autorevolezza riconosciuta da tutti, a cui tutti possono rivolgersi per verificare l'attendibilità del messaggio ricevuto. Si tratta, tuttavia, di una soluzione debole, in quanto non si può assicurare che tali figure possano essere

[6] Fiducia, guarda 1.1.1

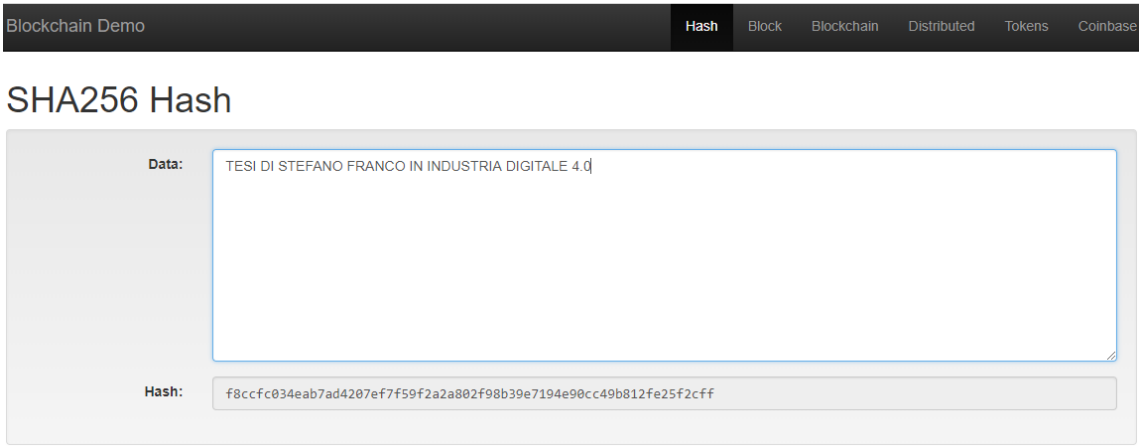
effettivamente raggiunte da tutti i luogotenenti in ogni istante di tempo. La Blokchain a riguardo propone una soluzione del tutto originale: non ci sono più generali o figure che comandano sugli altri, ma tutti possono proporre messaggi, vedere quelli proposti da altri e condividerli. Quando si raggiunge il *consenso*, ossia almeno una maggioranza approva l'istruzione, questa viene certificata nel sistema e da quel momento in poi sarà la strategia da utilizzare. Anche coloro che non sono riusciti a partecipare alla votazione (e che sono comunque in minoranza) possono vedere l'istruzione ricevuta. In questo modo tutti sanno tutto allo stesso modo, e non c'è modo per spie e traditori di corrompere il meccanismo.
Come può essere applicato tutto ciò all'interno di un sistema informativa? Semplice, attraverso algoritmi matematici.

1.2.3 Teoria dei Giochi e Crittografia

La *Teoria dei Giochi* è la disciplina matematica che studia il *gioco*, ovvero un ambiente dove diversi soggetti (*giocatori*) in situazione di conflitto o interazione strategica devono creare strategie per massimizzare il loro guadagno (*pay-off*) in un contesto in cui le proprie azioni influenzano il comportamento di altri giocatori – e viceversa – tali da spingerli a soluzioni competitive o cooperative[7]. Il Problema dei Generali Bizantini rientra tra le situazioni descritte e analizzate all'interno delle Teoria dei Giochi. La Teoria dei Giochi è dunque la scienza matematica utilizzata per garantire una delle caratteristiche principali della blockchain, ossia la *fiducia*.
Per garantire, invece, la *sicurezza* del sistema blockchain si ricorre alla crittografia, ovvero la branca di scienza che studia i metodi per rendere i messaggi opportunamente offuscati in modo che possano essere comprensibili solo alle persone autorizzate alla lettura. In generale, il messaggio che deve essere protetto viene chiamato *testo in chiaro* e, una volta offuscato, viene definito *testo cifrato*. L'operazione che trasforma il primo messaggio nel secondo viene detta *cifratura*, mentre l'operazione inversa viene chiamata *decifratura*. All'interno delle blockchain la funzione di cifratura che viene utilizzata

[7] Per approfondimenti: https://www.slideshare.net/stefanofran1987/il-fantastico-mondo-della-teoria-dei-giochi-festival-della-scienza

prende il nome di *Hash Function*[8]. Si tratta di un'operazione che consente di trasformare un testo di qualsiasi lunghezza in una stringa alfanumerica di lunghezza prestabilita. Questo rende più semplice la gestione dell'informazione e contemporaneamente altamente sicura, in quanto solamente chi possiede la chiave di lettura, ovvero il codice di decodifica, ha la possibilità di risalire al testo originale.



Esempio di funzione di hash[9]

Nella blockchain l'hash function identifica in modo univoco e sicuro ciascun blocco. Tali funzioni sono utilizzate per verificare che le transazioni siano eseguite correttamente, in quanto sono progettate in modo tale che una minima differenza nell'input cambi di molto il risultato di output. Esempi di funzioni di hash utilizzate all'interno di sistemi blockchain sono la *SHA256*[10] e la *RIPEMD160*[11].

[8] In inglese hash vuol dire *pasticciare*
[9] Per fare delle prove: https://anders.com/blockchain/hash.html
[10] https://it.wikipedia.org/wiki/Secure_Hash_Algorithm#Pseudocodice_di_SHA-256_(una_variante_di_SHA-2)
[11] https://it.wikipedia.org/wiki/RIPEMD#Hash_del_RIPEMD-160

1.3 Collegamenti con l'Industry 4.0 e scenari futuri

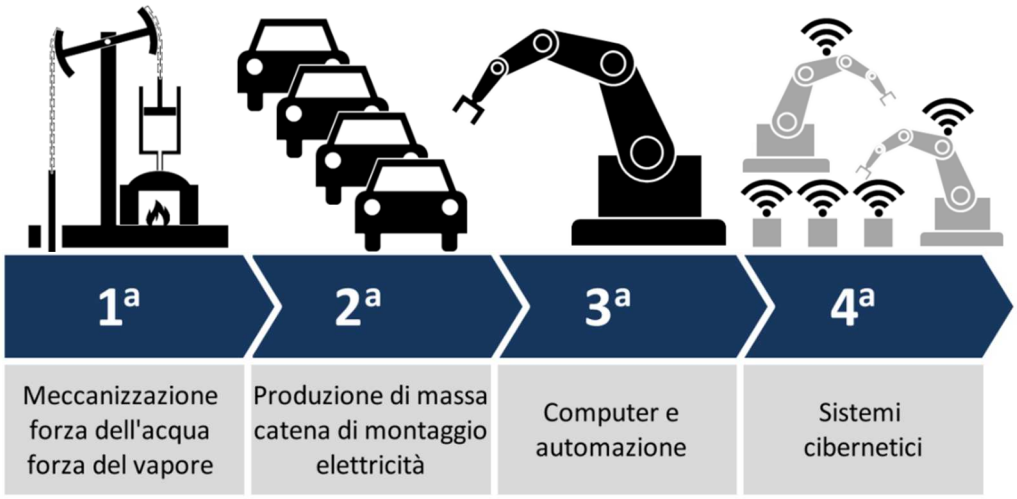
Il tema della blockchain è entrato di diritto tra le più promettenti strategie innovative per il miglioramento del mercato globale introdotte dai vari piani nazionali legate ai temi dell'*Industry 4.0*. Sicuramente ha giocato un ruolo chiave l'*hype* attorno a questa tecnologia per gli eventi di fine 2017, ma è anche vero che già un paio di anni prima grosse aziende leader dei mercati – su tutte IBM – avevano deciso di investire in ricerca e sviluppo su progetti blockchain, in quanto avevano intuito l'impatto importante che tale tecnologia avrebbe potuto dare ai propri business. In questo paragrafo, verrà illustrato in particolare quali sono le implicazioni di tale tecnologia nell'Industria 4.0 e quali potrebbero essere gli scenari futuri.

1.3.1 Industry 4.0 ed economia digitale

Il tema dell'*Industria 4.0* nasce nel 2011, quando durante una fiera di lavoro ad Hannover venne utilizzato il termine *Zukunftsprojekt Industrie 4.0*[12] per indicare le prassi e le nuove modalità di investimento da attuare per riportare la Germania ai vertici mondiali della produttività industriale. Il progetto prevedeva nuovi investimenti su infrastrutture, scuole, sistemi energetici, enti di ricerca e aziende per ammodernare il sistema produttivo tedesco e riportare la manifattura tedesca ai vertici mondiali rendendola competitiva a livello globale. La Germania è stata, infatti, la prima nazione al mondo che ha affrontato in maniera sistematica il problema legato all'aumento dei prezzi dei prodotti locali dovuti al costo del lavoro alto, completamente in opposizione a quanto avveniva nei paesi emergenti *BRICS* [13] dove il costo del lavoro basso consentiva di poter uscire con costi dei prodotti finali molto più bassi.

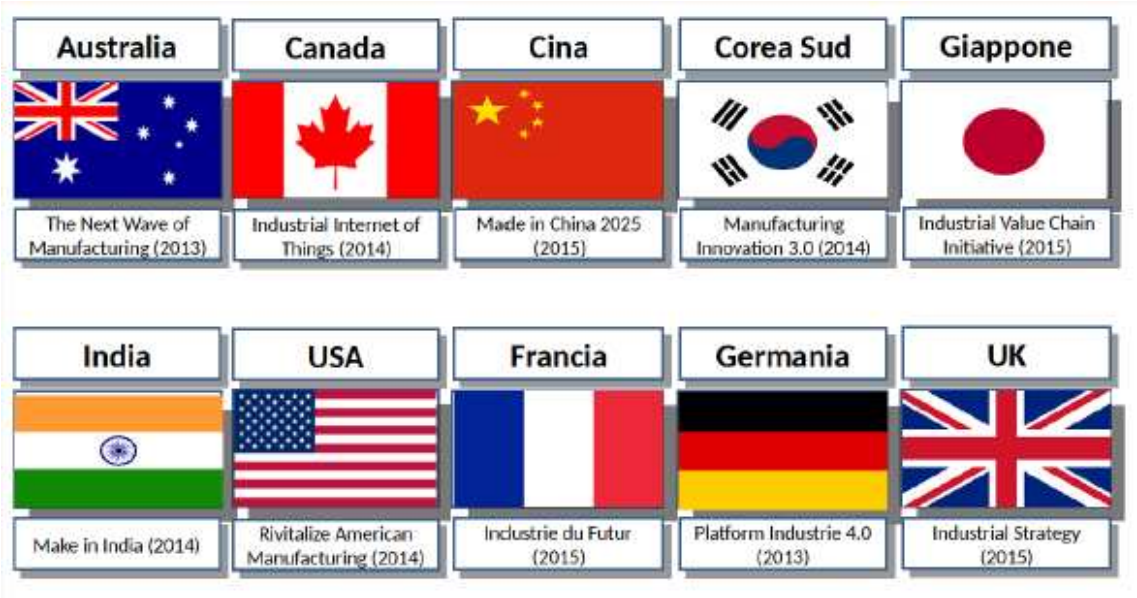
Il termine Industria 4.0 è stato utilizzato per evidenziare l'avvento di quella che possiamo definire *Quarta Rivoluzione Industriale*, basata su una *economia digitale* sempre più evidente, conseguenza inevitabile della maturità di internet, dei modelli di business legati al web e del miglioramento delle tecnologie informatiche.

[12] Letteralmente *Progetto Futuro Industria 4.0*
[13] Acronimo utilizzato in economia per indicare i paesi emergenti Brasile, Russia, India, Cina, Sud Africa



Rivoluzioni industriali e future tendenze[14]

Gli incoraggianti risultati raggiunti dall'economia tedesca hanno portato fin da subito i principali stati europei prima, e poi anche i principali paesi del mondo, ad adottare politiche simili, con particolari differenze a seconda della caratteristica produttiva interna di ogni paese.



I piani nazionali per la digital transformation dei principali paesi

[14] Fonte: Christoph Roser in www.allaboutlean.com

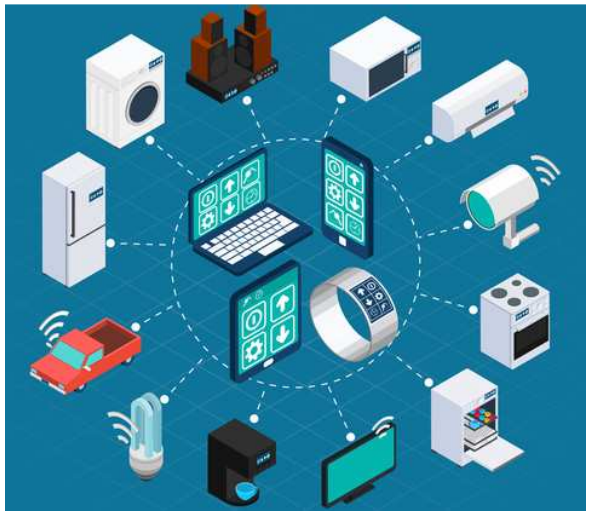
In Italia il *Ministero per lo Sviluppo Economico* ha introdotto il *Piano nazionale Impresa 4.0*[15] che prevede misure a supporto delle aziende basate su tre linee guida che sono:

- operare in una logica di neutralità tecnologica,
- intervenire con azioni orizzontali e non verticali o settoriali,
- agire su fattori abilitanti.

1.3.2 Internet of Things

L'*Internet of Things (IoT)*, o internet delle cose, è stato inserito da uno studio del *Boston Consulting Group*[16] intitolato *"Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries"* tra le tecnologie abilitanti, ossia quelle tecnologie fondamentali per poter raggiungere gli obiettivi dei progetti inseriti nei piani economici dei vari stati e che rientrano nei temi dell'Industria 4.0[17].

L'internet delle cose è la tecnologia che abilita il collegamento tra gli oggetti attraverso internet. Internet, che agli albori nasceva per collegare tra loro persone in luoghi differenti, evolve e si estende a tecnologia che collega persone con cose, cose con persone e cose con cose.



Schema di collegamenti IoT

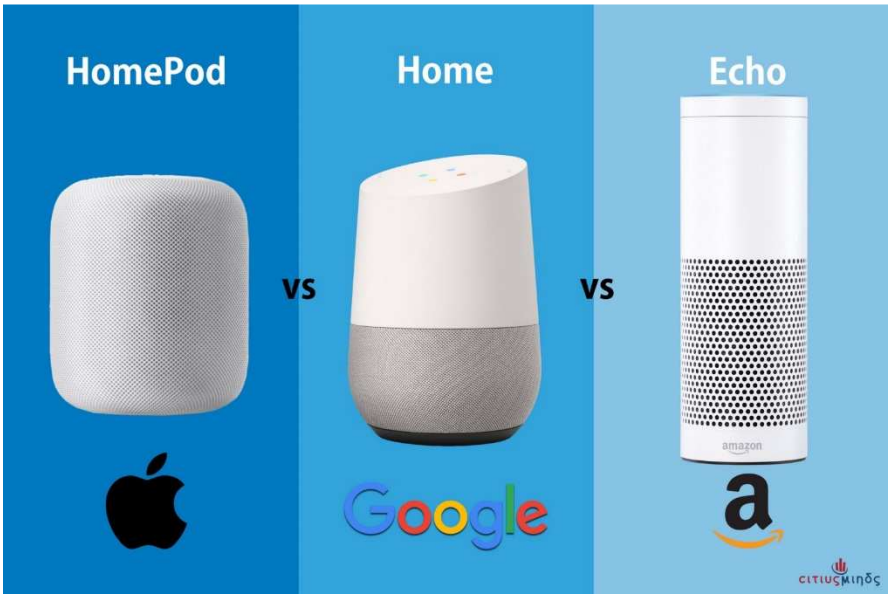
[15] Per maggiori approfondimenti: https://www.sviluppoeconomico.gov.it/index.php/it/industria40
[16] Società leader nella consulenza strategica ed economica delle aziende
[17] Altre tecnologie abilitanti sono: Advanced Manufactoring Solution, Additive Manufactoring, Augmented Reality, Simulation, Horizontal and Vertical Integration, Cloud, Cyber-sicurity, Big Data Analytics

Riuscire a concepire come due oggetti possano comunicare tra loro potrebbe in un primo momento sconcertare, ma è sufficiente osservare quanto lo smartphone sia ormai parte della vita di tutti e quanto spesso viene utilizzato in maniera integrata con le attività quotidiane delle persone, per capire che il mondo del futuro sia ormai attuale e che sempre di più gli oggetti che ci circondano riusciranno a interagire tra loro al fine di garantire servizi migliori per le persone.

1.3.3 Ipotesi di evoluzione

Sebbene i miglioramenti alla vita delle persone saranno sempre maggiori grazie all'Internet of Things, una delle cose che più di tutte preoccupa gli analisti e i tecnologi è la questione sicurezza del trasferimento delle informazioni e, soprattutto, dei dati personali. Secondo le stime dell'analista indiano MarketsandMarkets[18] il mercato IoT, in termini di valore, è destinato a crescere a un tasso medio annuo del 32,4%, passando dagli attuali 130 miliardi di dollari a 883,5 nel 2020. Per quella data saranno circa 34 miliardi i device smart connessi ad internet (24 miliardi di oggetti IoT, la restante parte saranno i device standard come smartphone, smartwatch, smartring…) contro gli attuali 10 miliardi. Grosse compagnie come Amazon, Apple e Google hanno già immesso sul mercato dispositivi domotici che, interfacciandosi con i device personali degli utenti e tramite tecniche di *intelligenza artificiale*[19], consigliano gli utenti a svolgere determinate azioni all'interno della propria abitazione.

[18] Sito web: https://www.marketsandmarkets.com/
[19] L'Intelligenza Artificiale è la branca della scienza che approfondisce le tecniche informatiche che simulano il comportamento umano



Immagini dello HomePod di Apple, Google Home e Echo di Amazon

Con il progressivo ampliamento dei business connessi all'IoT si moltiplicano le sfide tecnologiche e le implicazioni legate alla sicurezza di architetture IoT sempre più capillari. La tecnologia del trust distribuito della blockchain sembra essere l'unica in grado di assicurare scalabilità, rispetto della privacy e affidabilità degli ambienti IoT in crescita. Infatti, la natura decentralizzata e sicura della blockchain ne fanno la tecnologia ideale per gestire la rete di ragnatela generata dalle connessioni tra tutti i vari device. Giù grossi leader di mercato come IBM e Samsung hanno lanciato nuovi servizi integrati, come la piattaforma basata su blockchain chiamata *ADEPT*[20] .

Senza blockchain, i problemi legati all'eccessivo congestionamento del carico di rete dovuto all'aumentare dei dispositivi connessi tra di loro e controllati da un unico sistema centrale, sembrerebbero poter creare pericolosi colli di bottiglia senza possibilità di risoluzione. Le reti su cui saranno connessi tra loro lavatrici, tostapani e frullatori potrebbero interferire con le reti su cui viaggeranno informazioni sensibili, oppure legate alla salute dell'uomo, potendo causare danni irreparabili. La tecnologia blockchain

[20] Per approfondimenti: https://www.youtube.com/watch?v=U1XOPIqyP7A

sembra suggerire in maniera molto naturale una via di fuga a questa situazione limite a cui potremmo arrivare, anche in tempi molto brevi.

“Bitcoub’s low of $1.800+ yesterday
simply could not be manteined. In the long term
Bitcoin moves above $500.000 whitin three years. Bets?”

2. Mainstream e applicazioni della Blockchain

2.1 Bitcoin e cryptovalute

Il Bitcoin è una moneta virtuale e digitale che può essere scambiata via internet tra due soggetti. È la prima applicazione di un progetto blockchain, in quanto tutto il paradigma dell’acquisto, della vendita e della generazione di nuovi Bitcoin è basato sulla tecnologia argomento di questo lavoro. Nel presente paragrafo verrà illustrato il contesto nel quale

il Bitcoin si inserisce, si parlerà della genesi della valuta e si illustrerà l'impatto che attualmente essa e le altre cryptovalute hanno nell'economia mondiale.

2.1.1 Satoshi Nakamoto e il primo Whitepaper

Il primo novembre 2008 apparve sul sito Metzdowd.com[21] un documento che avrebbe cambiato profondamente gli anni successivi e tutto ciò che gravita attorno ai sistemi di pagamento elettronici. Si tratta del *Whitepaper*[22] del *Bitcoin*, il documento in cui per la prima volta si parla di moneta digitale attraverso tecnologia blockchain.

Il documento si intitolava *"Bitcoin: A Peer-to-Peer Electronic Cash System"*e racconta dell'idea di utilizzare un nuovo sistema di pagamenti elettronici basato su tecnologia Peer-To-Peer[23], ossia una tecnologia priva di un controllo centrale ma basata su un concetto di fiducia e decentralizzazione. Il documento[24], originariamente in lingua inglese, si presenta molto chiaro nell'esposizione e questo appare incredibile, soprattutto per il fatto che si accenna a problematiche quali signoraggio[25] bancario, fiducia degli interlocutori finanziari, double spending[26] , crittografia e si propone una soluzione apparentemente semplice, nell'enunciazione e nell'attuazione.

Autore del documento è un certo *Satoshi Nakamoto*, che in seguito si è scoperto essere uno pseudonimo utilizzato per non lasciare traccia sull'identità reale del proponente del progetto. Ancora oggi non si sa chi sia realmente Satoshi Nakamoto, ci sono molte congetture a riguardo, ma pare che attualmente Satoshi non lavori più sul progetto Bitcoin, abbia delegato altre persone per l'evoluzione, e oggi stia lavorando su altri

[21] http://www.metzdowd.com/ è un sito in cui è possibile inviare email a una lista di persone appassionate ed esperte nel settore della crittografia

[22] Il Whitepaper (o libro bianco) è un documento pubblico rilasciato da un'azienda dove vengono evidenziate in maniera trasparente le strategie da attuare da parte della società per risolvere un dato problema. Nell'ambito della blockchain è il documento pubblico in cui vengono spiegate le funzionalità e le specificità della blockchain e del progetto associato

[23] *Peer* in inglesa vuol dire "Pari", quindi il Peer-To-Peer (o P2P) è un modello "tra pari"

[24] A questo link è possibile visualizzare l'intero documento: https://bitcoin.org/bitcoin.pdf

[25] Per *signoraggio* si intende l'insieme dei redditi ottenuti dalla stampa delle monete

[26] Il *double spending* riguarda il problema di garantire che un certo pagamento elettronico non possa essere effettuato due volte presso rivenditori differenti

progetti. È ancora online il suo Blog[27], dove sono descritti tutti gli step che si sono susseguiti nel corso del tempo, a partire dal 2008.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In

Prima pagina del Whitepaper del Bitcoin

[27] Indirizzo del blog: http://satoshinakamoto.me

2.1.2 Le implicazioni della moneta digitale

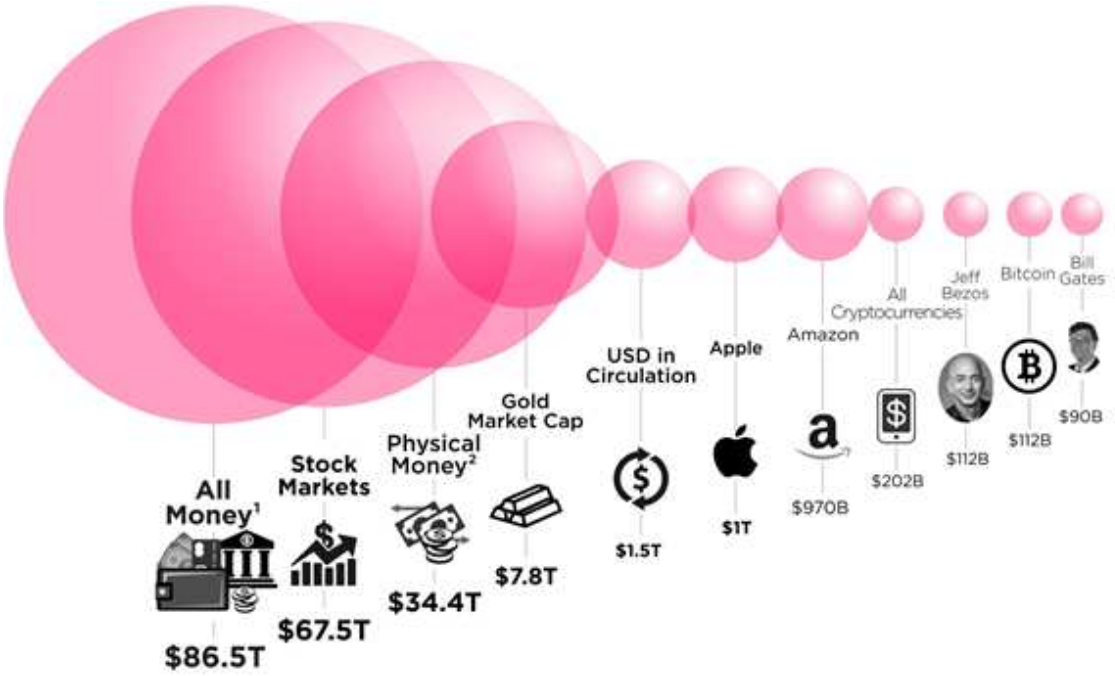
Il *Bitcoin* ha raggiunto il pubblico di massa alla fine del 2017, quando nel mese di Dicembre ha superato la soglia di 20.000$ di valore unitario[28]. Da quel momento in poi la tematica *Crypto Currencies*, ovvero delle Crypto Valute, è balzata agli onori di cronaca, generando un *hype*[29] notevole: giornali, web, tv, radio ne hanno parlato quotidianamente, contagiando gli ascoltatori e i lettori che in molti casi hanno pensato di poter avere guadagni facili in maniera semplice.

Screenshot del momento in cui il Bitcoin ha raggiunto il suo massimo valore[30]

La febbre del Bitcoin è anche in un certo senso giustificata, perché non è per nulla scontato trovare un modello finanziario[31] che cresce di +2.000% in un solo anno (2017). Tuttavia, un'analisi più approfondita dimostra come l'impatto che attualmente le

[28] Il 17 dicembre alle ore 13:41 il valore del Bitcoin ha toccato la soglia massima di 20.001,4$
[29] Letteralmente *battage pubblicitario*, ossia una promozione smisurata e chiassosa della tematica
[30] Fonte: www.coinmarketcap.com
[31] Sul fatto che il Bitcoin, e in generale le cryptovalute, possano essere considerati modelli finanziari c'è un'aperta discussione. Si rimanda al seguente link per un approfondimento a riguardo: https://www.ilsole24ore.com/art/norme-e-tributi/2018-04-22/per-fisco-bitcoin-vale-come-valuta-estera-102458.shtml?uuid=AE7d0kcE&refresh_ce=1

cryptovalute hanno nel mercato finanziario deve essere molto ridimensionato, soprattutto se si effettua un confronto con altri asset, come i contratti derivati e il mercato azionario.



Confronto tra le ricchezze del mondo[32]

2.1.3 Altre Crypto

Il Bitcoin non è l'unica cryptovaluta, anzi attualmente esistono più di duemila valute elttroniche che possono essere acquistate e scambiate. Molte di queste sono progetti embrionali, senza ancora un piano chiaro di crescita e di espansione. Molte altre, invece, esistono ormai da anni e vengono utilizzate per scambi o acquisti online. In ogni caso, la valuta principale resta il Bitcoin che da sola detiene oltre i 2/3 di capitalizzazione di tutto il mercato delle cryptovalute.

[32] Fonte: https://howmuch.net/articles/worlds-money-in-perspective-2018

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | USD ▾ | ← Back to Top 100

#	Name	Symbol	Market Cap	Price	Circulating Supply	Volume (24h)	% 1h	% 24h	% 7d
1	Bitcoin	BTC	$111.244.374.036	$6.404,25	17.370.387	$3.756.182.696	0,15%	0,03%	0,63%
2	Ethereum	ETH	$21.886.559.524	$212,22	103.132.234	$1.413.217.081	0,11%	0,52%	5,82%
3	XRP	XRP	$20.275.575.388	$0,504298	40.205.508.733 *	$308.661.955	-0,19%	0,20%	10,84%
4	Bitcoin Cash	BCH	$9.496.758.572	$544,16	17.451.988	$656.031.225	-0,59%	0,64%	1,61%
5	Stellar	XLM	$5.089.112.263	$0,268735	18.937.256.481 *	$76.737.878	-0,45%	4,82%	11,89%
6	EOS	EOS	$4.894.532.093	$5,40	906.245.118 *	$621.788.073	0,31%	0,20%	-0,01%
7	Litecoin	LTC	$3.063.792.085	$51,83	59.109.188	$357.423.912	-0,04%	-0,42%	-1,19%
8	Cardano	ADA	$1.979.954.135	$0,076366	25.927.070.538 *	$18.873.281	-0,45%	2,35%	3,22%
9	Tether	USDT	$1.774.259.570	$0,998783	1.776.421.736 *	$2.505.477.751	0,63%	0,42%	1,01%
10	Monero	XMR	$1.724.978.298	$104,16	16.560.746	$14.074.730	0,44%	-1,90%	-2,51%

Lista delle prime 10 cryptovalute per capitalizzazione[33]

2.2 Le Blockchain alla base delle Crypto

La Blockchain alla base del Bitcoin è probabilmente il database più sicuro al mondo. Le transazioni sono immutabili, potenzialmente eterne ed impossibili da imitare o modificare. Ciò che rende possibile ciò è quello che prende il nome di *Algoritmo di Consenso*, ed è alla base del concetto di trust di ogni blockchain. La logica alla base di tale algoritmo è che ogni transazione, e dunque ogni modifica da importare nella blockchain, deve essere prima autorizzata e validata dai nodi. Il modo con cui questo consenso avviene determina la differenza sostanziale tra una blockchain e un'altra. Nel paragrafo che segue verranno illustrate le tecniche di consenso delle principali blockchain.

2.2.1 Il Proof of Work (PoW)

Il *Proof of Work* (*PoW*) è un modello secondo il quale il consenso viene raggiunto dopo aver garantito una certa dimostrazione di lavoro al sistema blockchain. In pratica

[33] Fonte: www.coinmarketcap.com

all'interno della blockchain ci sono alcuni utenti speciali che prendono il nome di *miners*[34]. Tutte le nuove transazioni vengono inserite all'interno di un blocco che dovrà essere collegato ai blocchi precedenti e che costituirà parte integrante della blockchain da quel momento in poi. Il modo con cui questo avviene è affidato ai miners e alla loro capacità di risolvere un problema di crittografia: dovranno riuscire a trovare la funzione corretta (chiamata *hash*[35]) che corrisponde al modo migliore con cui il nuovo blocco potrà collegarsi al precedente. La difficoltà di questa operazione dipende dal grado di difficoltà della blockchain che aumenta nel tempo, secondo regole precise quasi sempre riportate all'interno dei white paper.

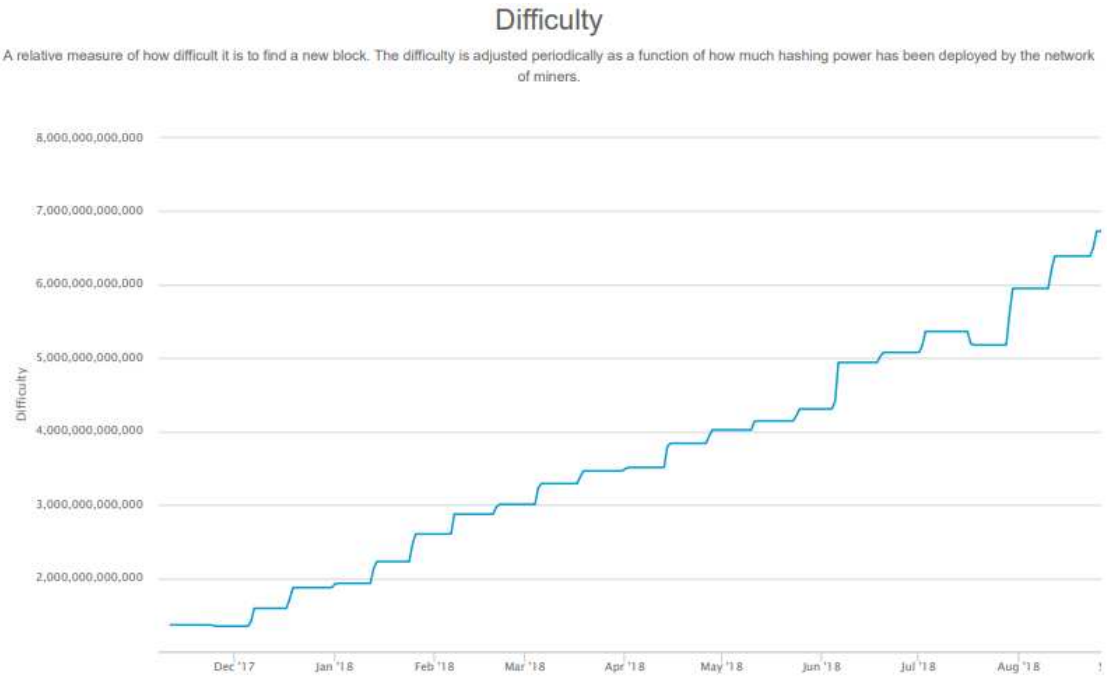


Grafico dell'algoritmo di difficoltà della blockchain Bticoin[36]

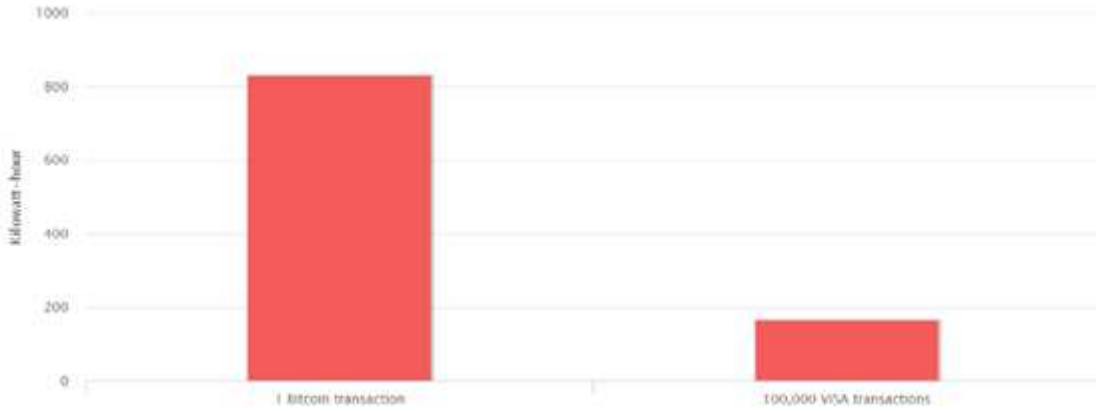
Tutti i miners contemporaneamente cercano di risolvere questo problema mettendo a disposizione le loro risorse di calcolo, ossia i loro server e i loro computer, e chi riesce

[34] Letteralmente *minatori*
[35] Leggi paragrafo 1.2.3
[36] Fonte: https://www.blockchain.com/charts/difficulty

per prima a risolvere il problema riceve una ricompensa in denaro corrispondente a circa 50.000$ più tutte le commissioni delle transazioni contenute nel blocco. Questo meccanismo incoraggia i miners a cercare di risolvere il problema per aggiudicarsi la ricompensa e, contemporaneamente, scoraggia coloro che vorrebbero compromettere l'integrità del sistema in quanto, per effettuare modifiche fraudolente, dovrebbero riuscire ad autenticare un blocco risolvendo il problema e, per farlo, dovrebbero mettere a disposizione le loro risorse di calcolo senza nessuna garanzia che possano essere effettivamente loro i *vincitori* della gara.

È importante osservare che questo meccanismo virtuoso del PoW è, al contempo, il suo limite principale. Mettere a disposizione le proprie risorse di calcolo vuol dire mettere a disposizione molta energia per tenere accesi server e computer e questo rende tutto il processo energivoro. In territori dove i controlli ambientali non sono elevati e il costo dell'energia è basso, tipo in Cina o nel Sud America, intere città sono state adibite a fabbriche per il *mining*[37] con conseguenze preoccupanti per quanto riguarda l'inquinamento.

Per capire la portata negativa di questo fenomeno, nell'immagine sottostante si confronta il costo energetico di una transazione in Bitcoin e una di un classico circuito Visa.



Consumo medio del network Bitcoin e quello Visa[38]

[37] Il *mining* è l'attività di risoluzione del problema crittografico eseguita dai *miners*

[38] Fonte: www.bitcoinenergyconsumption.com

Nonostante questo limite, le principali cryptovalute, come Bitcoin, Litecoin, Bitcoin Cash, Ethereum, Vertcoin girano su blockchain basate sul PoW.

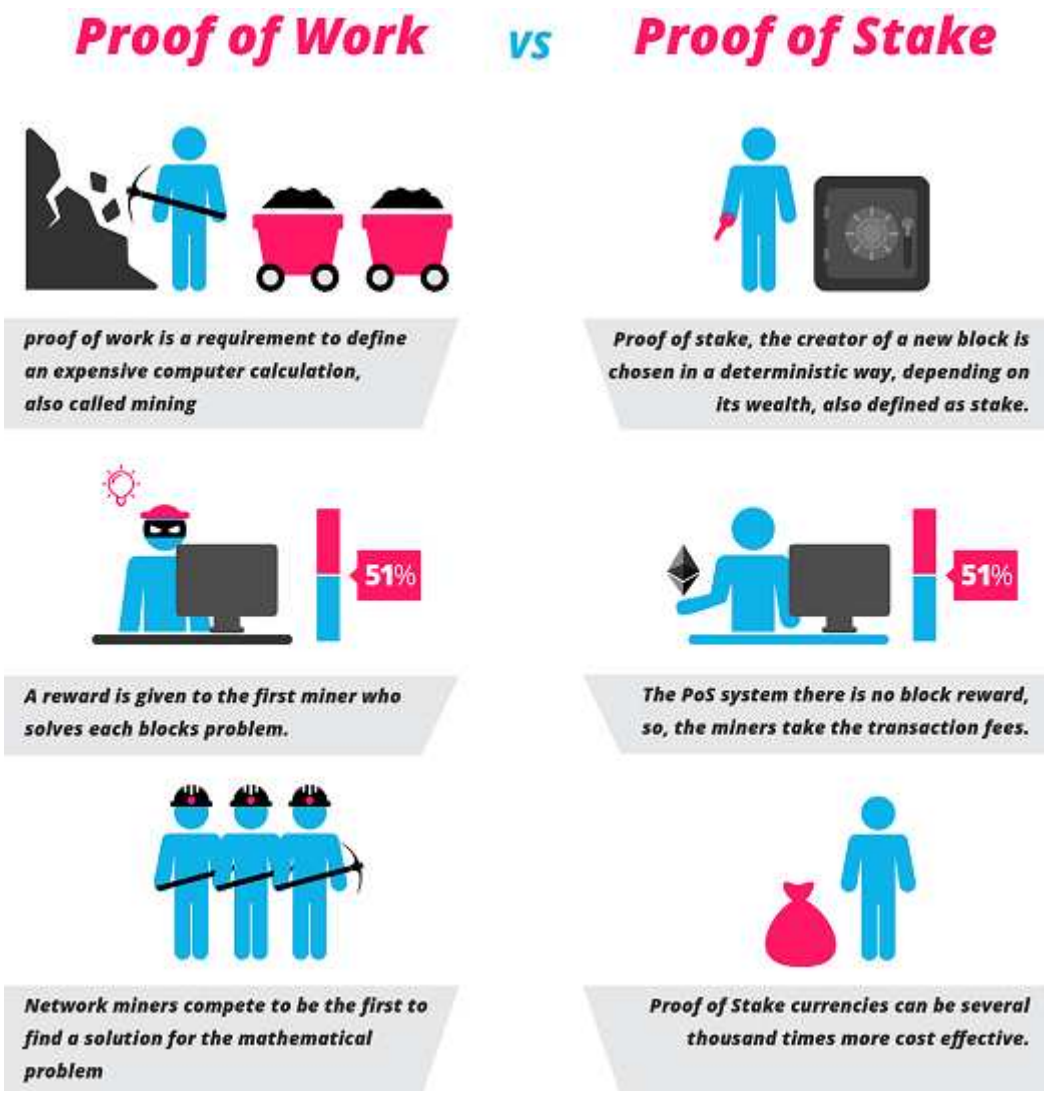
2.2.2 Il Proof of Stakes (PoS)

A differenza del PoW nel *Proof of Stakes* (*PoS*) a garantire il sistema blockchain, e dunque il consenso e la fiducia nel sistema, non sono figure più o meno neutre, come possono essere i miners, bensì sono coloro che detengono più ricchezza nel network. Si tratta di una differenza sostanziale. Mentre nel PoW tutti possono svolgere attività di mining, perché hanno il legittimo interesse a ricevere la ricompensa, nel PoS il creatore nel nuovo blocco che contiene tutte le transazioni viene scelto in maniera deterministica tra coloro che detengono un maggior numero di *stakes*, ovvero di posta in gioco nella blockchain. Secondo questo schema, infatti, la garanzia e l'affidabilità della blockchain viene affidata a coloro che più di tutti gli altri hanno l'interesse che non ci siano modifiche fraudolente al sistema.

Alla figura dei miners si sostituisce quella dei *validators*: solo i validators possono occuparsi della creazione del nuovo blocco e il loro impegno è al più proporzionale rispetto a quelle che sono le loro quote all'interno di tutto il network. In pratica, i validators vengono individuati attraverso un algoritmo di selezione: una volta individuati, tutti insieme contribuiscono alla creazione del nuovo blocco, mentre tutti gli altri possessori della moneta non possono effettuare attività di mining. Inoltre, i validators hanno tutto l'interesse che la creazione del blocco non sia fraudolenta, in quanto loro mettono a garanzia la propria quota posseduta e, in caso di corruzioni del sistema in fase di creazione del loro blocco, tali quote verrebbero definitivamente perdute.

Questo modello, adottato da alcune cryptovalute come Peercoin, Shadowcash, Nxt, Blackcoin, NuShares, Qora e Nav Coin, annulla in un colpo solo quelli che sono i principali limiti del PoW, in quanto il sistema non è energivoro, poiché solo una selezionata fetta di utenti partecipa all'attività di mining e per compromettere il network occorrerebbe che i proprietari che detengono il 51% delle quote si organizzino ma, pur

dovendo riuscire a fare ciò, porterebbero a un crollo della valuta con conseguente perdita delle proprie ricchezze.



Schema riassuntivo di confronto tra PoW e PoS[39]

Sebbene i suoi vantaggi da un punto di vista ambientale, il PoS non è attualmente un modello molto diffuso, in quanto sono presenti importanti limiti tecnologici, legati soprattutto alla velocità di trasferimento delle transazioni. Tuttavia è abbastanza probabile

[39] Fonte: www.blockgeeks.com

che alcune barriere tecnologiche nel prossimo futuro possano cadere e già cryptovalute importanti come *Ethereum*[40] hanno annunciato di voler passare al PoS nelle versioni successive[41].

2.2.3 Altri modelli

Oltre al PoW e al PoS, che sono sicuramente i principali modelli che reggono il mondo blockchain, molti sviluppatori stanno lavorando per proporre valide alternative, con l'obiettivo soprattutto di ridurre l'impatto ambientale dovuto alle attività di mining. Tra queste possiamo introdurre:

- *Delegated Proof of Stakes* (*DPoS*): partendo dal classico modello PoS, il DPoS introduce il concetto di delegato/testimone. In pratica il network affida a una cerchia ristretta di persone la possibilità di effettuare scelte strategiche, come l'impostazione delle tariffe di transazione, l'individuazione di coloro che effettueranno il mining e la conferma dei blocchi da inserire nella blockchain. Si tratta di persone che hanno una grande responsabilità e che ovviamente hanno tutto l'interesse a effettuare scelte ponderate e non compromettenti per il network, perché potrebbero immediatamente perdere il consenso e l'affidamento dell'incarico e i compensi previsti per tale attività. Si tratta di un modello maggiormente democratico, che consente a tutti di poter entrare senza costi particolarmente elevati, e che è già stato applicato da cryptovalute importanti come *Steem*[42].
- *delegated Byzantine Fault Tolerance (dBFT)*: il dBFT applica alla blockchain la soluzione del problema dei generali bizantini che abbiamo affrontato in 1.2.2. Innanzitutto la base utenti viene suddivisa tra gli utilizzatori e i nodi professionali (*bookkeeping nodes*), a seconda che si punti o meno al guadagno economico

[40] Ethereum è la seconda valuta per capitalizzazione di mercato, dopo il Bitcoin
[41] Per approfondimenti: https://www.cryptominando.it/2018/09/09/ethereum-2-0-pos-sharding-ewasm-ecco-la-roadmap/
[42] Steem (www.steem.io) è una piattaforma di microblogging in cui è possibile ricevere compensi proporzionali all'interesse della rete sui propri contenuti pubblicati

derivante dalla validazione della blockchain. Con un sistema molto simile al DPoS, gli utilizzatori votano i propri delegati tra i nodi professionali. Questi delegati hanno l'onere di validare i nuovi blocchi e, ad ogni verifica, viene scelto in maniera casuale un delegato tra quelli già votati dagli utilizzatori, che deve dare la sua versione di blockchain e solamente quando sarà confermata da almeno il 66% dei delegati il nuovo blocco verrà confermato e agganciato alla blockchain. Si tratta di un sistema articolato, ma che riesce a garantire sicurezza e affidabilità. Tale blockchain è stata utilizzata prima di tutti dalla cryptovaluta *NEO*[43].

2.3 Applicazioni

A partire dalla seconda metà del 2018, a seguito anche della stabilizzazione del prezzo del Bitcoin nell'intorno dei 6.000$, l'immaginario collettivo sul tema blockchain ha cominciato ad assumere maggiore consapevolezza sulla sua importanza e sull'impatto che la stessa avrà nel prossimo futuro. La tecnologia ha cominciato ad essere analizzata in maniera sistemica anche da coloro che in un primo momento cercavano di allontanarsi, probabilmente perché pensavano che si trattasse solamente di un mero strumento per speculazioni finanziarie, o solo perché annoiati del fatto che se ne parlasse troppo senza troppa consapevolezza. Fatto sta che ormai non ci sono dubbi sul fatto che la blockchain possa essere utile in tantissimi settori e che più passerà il tempo più cresceranno gli ambiti in cui essa sarà applicata. Nel paragrafo illustreremmo alcune tra quelle che sono le maggiori applicazioni della blockchain.

2.3.1 Fintech

Una delle prime aree di business per le società che investono in progetti su tecnologia blockchain è sicuramente quella legata ai servizi finanziari. Attirati in un primo momento dall'interesse mediatico dovuto alla nascita delle cryptovalute, i principali gruppi

[43] NEO (www.neo.org) è la cryptovaluta n.15 per capitalizzazione di mercato

finanziari e le *Big Four*[44] hanno fin da subito annunciato il loro interesse ad investire in tecnologie blockchain. In particolare, l'AD di EY, Marcel Stalder, ha dichiarato:

<< *Non vogliamo solo parlare di digitalizzazione, ma vogliamo anche guidare attivamente questo processo insieme ai nostri dipendenti e ai nostri clienti. Per noi è importante che tutti siano a bordo, e si facciano trovare pronti alla rivoluzione nel settore finanziario che avverrà attraverso la blockchain, dovuta all'avvento degli smart contract e delle cryptovalute.* >>[45]

L'interesse principale è quello di riuscire a trovare soluzioni innovative che interfaccino il mondo crypto con i tradizionali sistemi bancari e finanziari, creando un nuovo modello più potente e sicuro grazie alla blockchain. Diverse imprese hanno già cominciato a correlare sistemi blockchain alle tradizionali soluzioni finanziarie e di pagamento e innumerevoli banche centrali sparse nel mondo stanno considerando l'uso di valute digitali interne. La banca centrale di Russia, ad esempio, ha costituito un gruppo di lavoro, mentre quella Popolare della Cina sembrerebbe essere già attrezzata in questo senso[46].

Molti sarebbero i benefit ottenuti a seguito dell'adozione della blockchain e delle cryptovalute nel mondo finanziario per banche e clienti:

- l'uso di un sistema blockchain permetterebbe un abbassamento dei costi, un aumento della velocità e maggiore trasparenza nelle transazioni bancarie;
- le informazioni sarebbero registrate e monitorate automaticamente durante il processo di transazione;
- la digitalizzazione ridurrebbe le procedure necessarie per la convalida di una transazione ed eliminerebbe del tutto la carta;

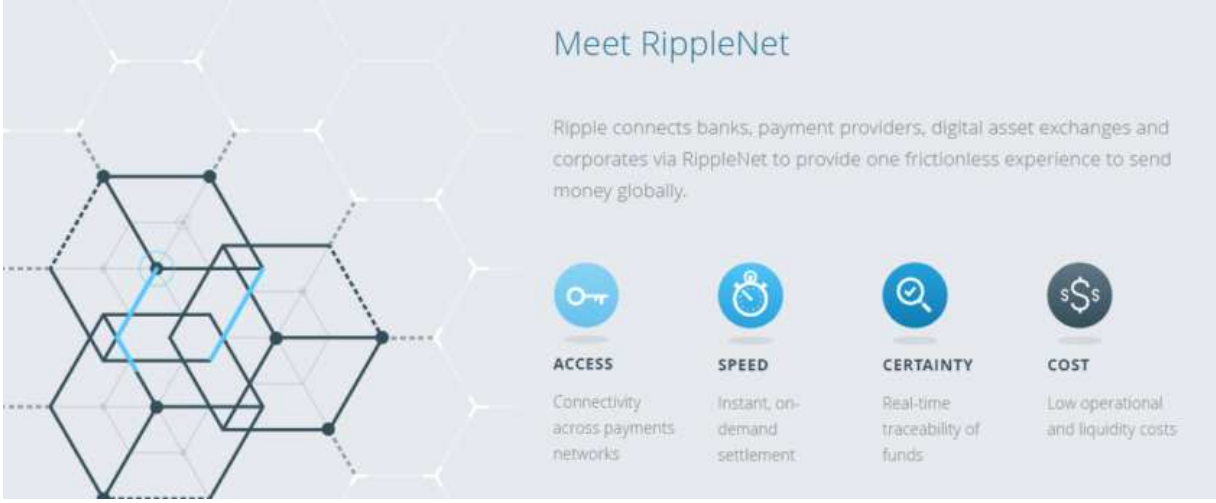
[44] Termine con cui si definiscono le quattro principali società di revisione dei servizi finanziari, ossia KPMG, Deloitte, EY e PWC

[45] Report completo: https://www.ey.com/Publication/vwLUAssets/ey-news-release-switzerland-accepts-bitcoins-for-payment-of-its-services/%24FILE/ey-news-release-switzerland-accepts-bitcoins-for-payment-of-its-services.pdf

[46] Per approfondimenti: https://www.startmag.it/fintech/cripto-valuta-cina/

- ci sarebbe una maggiore protezione delle transazioni e si potrebbe tenere traccia dei clienti e dei movimenti più facilmente, riducendo il riciclaggio di denaro e l'evasione fiscale;
- non ci sarebbero problemi legati alla falsificazione delle valute.

Oltre ai tentativi più o meno di successo dei grossi player finanziari di creare progetti innovativi attraverso blockchain, molti sono anche i tentativi di aziende private di lanciare nuovi modelli di business attraverso blockchain che possano stravolgere il sistema finanziario. Tra tutti, il progetto che più si sta distinguendo nel settore è sicuramente *Ripple*[47], sistema che consente alle banche di inviare in tempo reale dei pagamenti attraverso una rete finanziaria. Se può sembrare strano che delle banche possano scegliere un sistema terzo per l'invio di denaro, per di più attraverso tecnologia blockchain, bisogna considerare che attualmente Ripple ha 42 clienti, e tra questi ci sono le 15 più grandi banche al mondo.



Proposta di valore del modello di business di Ripple

[47] Ripple (www.ripple.com) è la terza cryptovaluta per capitalizzazione di mercato

2.3.2 Pubblica Amministrazione

I quattro concetti cardine di un sistema blockchain – sicurezza, fiducia, trasparenza, immutabilità – inevitabilmente si incontrano con quelli che sono i principali ostacoli da superare dei progetti digitali della Pubblica Amministrazione. L'avvento di internet ha radicalmente modificato il modo in cui si conservano le informazioni, soprattutto quando queste afferiscono alla sfera personale e privata dei cittadini. Il dibattito sulla blockchain e l'*e-governament*[48] ha messo in luce vantaggi di grande rilievo che si potrebbero avere in riferimento a identità digitali, pagamenti e riscossione delle imposte.

Marcella Atzori, esperta in blockchain e in sistemi di e-goverment dell'Unione Europea, ha individuato diversi ambiti di immediata applicazione delle tecnologie blockchain nel settore pubblico, per esempio:

- decentralizzazione e automatizzazione di tutti gli archivi pubblici e digitali;
- *timestamping*[49] e prova di esistenza, compresa la creazione, l'origine, il contenuto, la sicurezza e l'integrità, di qualsiasi documento, come gli atti pubblici, i contratti di locazione, la richiesta di documenti personali…
- protezione dei dati, privacy e trasparenza;
- gestione di identità digitali decentralizzate, attraverso un sistema che colleghi privati e imprese attraverso il modello del *privacy-by-design*, mediante il quale le autorizzazioni a certi dati sensibili possono essere concesse solo a chi ne detiene i diritti;
- riscossione delle imposte, gestione dei piani finanziari dei fondi pubblici e pagamenti.

A questi ambiti di applicazione se ne possono aggiungere tanti altri, tutti con l'obiettivo di prevenire l'uso illecito e improprio dei beni pubblici e garantire un servizio di maggiore efficienza per il cittadino. Quello che attualmente sembra il limite più importante per un'applicazione immediata del sistema blockchain nel settore pubblico riguarda

[48] L'e-governament è il sistema di gestione digitalizzata della Pubblica Amministrazione
[49] Il *timestamping* è la pratica dell'applicazione di una sequenza di caratteri nei documenti che rappresenta la data di creazione e l'orario in cui è avvenuto un certo evento

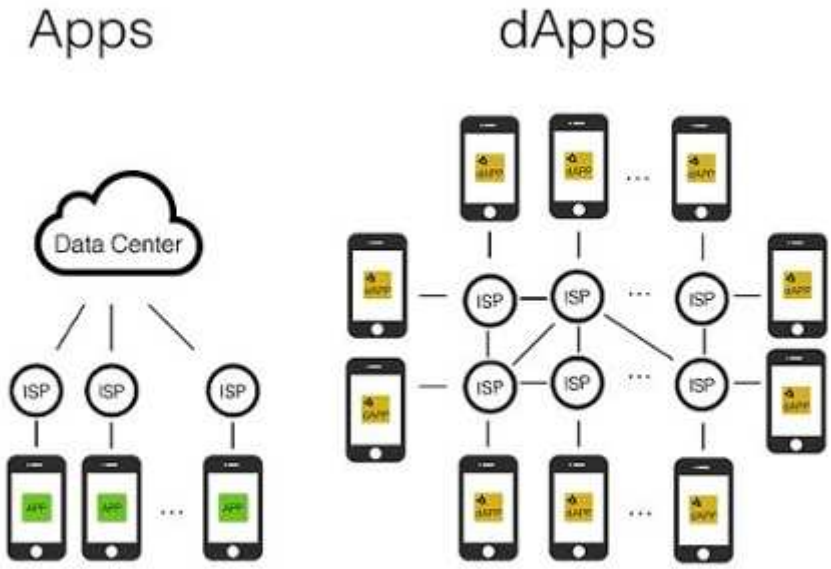
l'individuazione dei requisiti tecnici e di governance per un'implementazione sicura dei registri distribuiti. Il mondo blockchain è, infatti, fortemente radicato in principi di autogestione del network, decentralizzazione del trust e libero mercato, e questo contrasta con l'esigenza legittima dei servizi pubblici di proteggere gli interessi generali dei cittadini e il bene pubblico. Il problema è, dunque, la questione della legittimità dei servizi, e al contempo della loro qualità tecnica e giuridica. Con molta probabilità gli attori che giocheranno un ruolo fondamentale in questo scenario saranno i *Trust Service Providers* (*TSP*) europei, ovvero i fornitori già accreditati dai sistemi di vigilanza governativi europei che operano nel settore digitale.
Tra i principali TSP c'è già *TrustedChain*[50], ecosistema blockchain in grado di decentralizzare e rendere più efficienti e sicuri i flussi di dati, documenti e identità digitali.

2.3.3 Smart Contracts e dApps

Gli ambiti di applicazione della tecnologia blockchain sono davvero svariati e, senza correre il rischio di sembrare eccessivi, si può dire che sono pressoché infiniti. Ciò è dovuto soprattutto al fatto che la blockchain di Ethereum dà la possibilità di creare quelli che prendono il nome di *Smart Contracts*. Prima di introdurre gli Smart Contracts, c'è da dire che mentre il Bitcoin sta scuotendo il settore finanziario, Ethereum utilizza la tecnologia blockchain per eliminare gli intermediari su internet.
Gli Smart Contracts, come suggerisce il nome, sono contratti intelligenti, ossia software installati sulla blockchain Ethereum che consentono l'attivazione di determinate transazione a seconda delle condizioni al contorno che ci sono. Mentre un contratto tradizionale viene scritto da due o più parti che si impegnano a rispettare le condizioni al verificarsi o meno di determinate clausole, e può essere firmato da un notaio come certificato di garanzia, uno Smart Contract è caratterizzato dal fatto che il contratto è costruito attraverso un algoritmo matematico che automaticamente attiva il contenuto del contratto, una volta che vengono verificate le condizioni. Senza nessun intermediario che garantisca o meno il rispetto delle condizioni. Questo concetto rivoluzionario permette di

[50] Per approfondimenti: https://trustedchain.it/pubblica-amministrazione/

creare contratti per scambiare denaro, acquistare proprietà e altre cose di valore in maniera del tutto trasparente e senza conflitti evitando i servizi di un intermediario.
Questi contratti intelligenti consentono lo sviluppo di quelle che vengono definite *decentralized apps* (*dApps*), vere e proprie applicazioni digitali, come quelle classiche che si trovano sui tradizionali cellulari, con un'unica ma sostanziale differenza, ossia che sono decentralizzate e quindi non c'è un server centrale, ma il codice gira in back-end su una rete Peer-To-Peer basata su blockchain.



Schema sulla modalità di funzionamento di un'app classica e di una dApps

Tramite gli Smart Contracts si stanno creando dApps per svolgere praticamente qualsiasi cosa. È doveroso osservare che molto spesso c'è un abuso di dApps, nel senso che molti progetti che vengono implementati tramite blockchain in realtà potrebbero tranquillamente essere sviluppati attraverso tecnologie classiche. La sensazione è, tuttavia, che nel medio-lungo periodo la maggiore flessibilità delle dApps, integrata con i miglioramenti a livello tecnologico della blockchain, potrà essere uno degli elementi principali che porteranno alla diffusione ed effettiva fruizione di nuove funzionalità e nuovi prodotti nel mercato degli utenti digitali.

"Use the hashtag #ImproveTheWorld
and steps by steps the world will really improve!"

3. Il gruppo Blocktech: casi di studio e sperimentazioni

3.1 Il gruppo Blocktech: introduzione

Il gruppo Blocktech è uno spinoff dell'associazione *Alumni Mathematica*[51] impegnato nella sperimentazione delle innovazioni nell'ambito della blockchain, del mining e della speculazione finanziaria legata alle cryptovalute. Alumni Mathematica ha creato questo

[51] Per approfondimenti: www.alumnimathematica.org

spinoff con l'obiettivo di esplorare la tecnologia blockchain, realizzare una propria blockchain e lanciare una propria *ICO* (*initial coin offer*[52]).

Logo dello spinoff Blocktech

3.1.1 Alumni Mathematica è lo *#ImproveTheWorld*

Alumni Mathematica è una organizzazione non profit impegnata nella ricerca scientifica indipendente e nella diffusione delle discipline matematiche. È stata fondata a Bari nel Marzo del 2013 da due persone e attualmente è un network di più di 100 professionisti, laureati, ricercatori, professori in matematica, fisica, informatica, economia ed ingegneria. La sede operativa è situata nel Dipartimento di Matematica dell'Università degli Studi di Bari Aldo Moro.

Fin dall'inizio l'obiettivo dell'Associazione è stato quello di migliorare il mondo a partire dalla conoscenza e dal sapere scientifico. Il sito web dell'organizzazione recita:

<< In un periodo di trasformazione tecnologica come quello che è in atto nella società moderna, TUTTI devono essere protagonisti della tecnologia e non spettatori passivi. Per tale motivo le iniziative che organizziamo hanno l'obiettivo di eliminare l'analfabetismo tecnologico (nelle aziende e nelle persone) per fornire a tutti gli uomini, grandi e piccini, le basi per essere partecipi del fantastico mondo nuovo del domani.>>

[52] La *Initial Coin Offering* (*ICO*) è la fase iniziale del lancio di un nuovo progetto nell'ambito del mercato delle cryptovalute, equivalente alla *Initial Public Offering* (*IPO*) per la quotazione delle aziende in borsa

Gli obiettivi associativi vengono realizzati attraverso tre attività:

- ricerca scientifica indipendente, svolta in collaborazione con partner industriali e accademici. I settori di interesse dell'Associazione sono l'innovazione tecnologica**,** il deep learning, l'industry 4.0, l'intelligenza artificiale, la blockchain, l'open data e la data science;
- didattica innovativa nelle scuole, attraverso la metodologia dell'*apprendimento consapevole*, che capovolge il paradigma didattico dalla teoria alla pratica, alla teoria dalla pratica. Attualmente sono state svolte attività in più di 20 scuole a livello regionale;
- divulgazione scientifica, attraverso partecipazioni ad eventi di svariata natura, dagli eventi istituzionali nelle università alle fiere del fumetto. Finora sono stati organizzati più di 300 eventi.

Foto di gruppo in una riunione associativa

3.1.2 Le origini del gruppo Blocktech

Il gruppo Blocktech nasce ufficialmente il 14 novembre 2017 quando nell'Ex Palazzo delle Poste a Bari è stato organizzato il primo convegno aperto al pubblico sulle

tecnologie blockchain dal titolo "*Bitcoin: cos'è e come si usa la valuta virtuale*"[53]. All'evento parteciparono oltre 250 persone e diverse testate giornalistiche e televisioni ne hanno parlato. L'entusiasmo attorno all'evento ha spinto l'Associazione a pensare seriamente di creare un nucleo operativo che potesse approfondire i tecnicismi della blockchain, diffondere nel territorio la conoscenza maturata attraverso ulteriori eventi e intercettare esigenze del mercato proponendo soluzioni innovative.

Il gruppo Blocktech è stato fondato dal Dott. Stefano Franco e dall'Ing. Vito Pesola e attualmente vede impegnate cinque persone che lavorano sui vari progetti. Dalla sua fondazione, il gruppo Blocktech ha lavorato su dieci progetti blockchain e ha organizzato cinque eventi di divulgazione sul tema blockchain.

Foto scattata in occasione dell'evento del 14 novembre 2017

[53] Maggiori dettagli sull'evento: http://alumnimathematica.org/evento-bitcoin-bari/

3.2 Le applicazioni nel settore finanziario

In questo paragrafo verranno illustrati i principali progetti realizzati dal gruppo Blocktech che rientrano nella sfera di interesse del settore finanziario.

3.2.1 Il Sell Wall Detector Tool

Il *Sell Wall Detector Tool* è uno strumento per la determinazione automatica di una particolare manipolazione di mercato detta *Sell Wall* (o anche *Fake Sell Wall*). Questa manipolazione consiste nel posizionamento di grandissime quantità di ordini di vendita (*ASK*) all'interno dell'*Order Book* di un singolo mercato di cryptovaluta al fine di mantenerne basso il prezzo di contrattazione.

Esempio di Sell Wall nel mercato delle cryptovalute

Generalmente accade che il prezzo venga manipolato da un grosso player di mercato che, tenendo fisso un ordine di vendita di size molto ampia, incomincia ad acquistare le posizioni di vendita che vengono inserite nel book da altri trader a prezzo ribassato. Quando il grosso player rimuove il suo ordine di vendita accade nella maggior parte dei casi che il prezzo cominci a salire in modo abbastanza rapido, offrendo una opportunità di trading a chi avesse seguito la manipolazione dall'esterno.

Il Sell Wall Detector Tool individua la presenza di Sell Wall, senza indagare su quali possono essere i motivi per cui un certo grosso ordine di vendita sia stato inserito.

Il tool utilizza le API[54] di *BITTREX*, uno dei principali exchange del mercato delle cryptovalute, e, una volta individuata la presenza di un sell wall, invia una notifica all'utente. In questo modo l'utente può valutare la situazione ed eventualmente effettuare acquisti o vendite a seconda delle proprie strategie a seguito dei suggerimenti ricevuti dal tool.

Il tool è attualmente in versione beta e viene attualmente ceduto in test agli interessati in maniera gratuita.

3.2.2 BTC Notify – Bot Telegram

BTC Notify è un Bot Telegram[55] che invia agli utenti registrati al canale Telegram degli alert quando determinate cryptovalute aumentano il proprio valore oltre certe soglie limite.

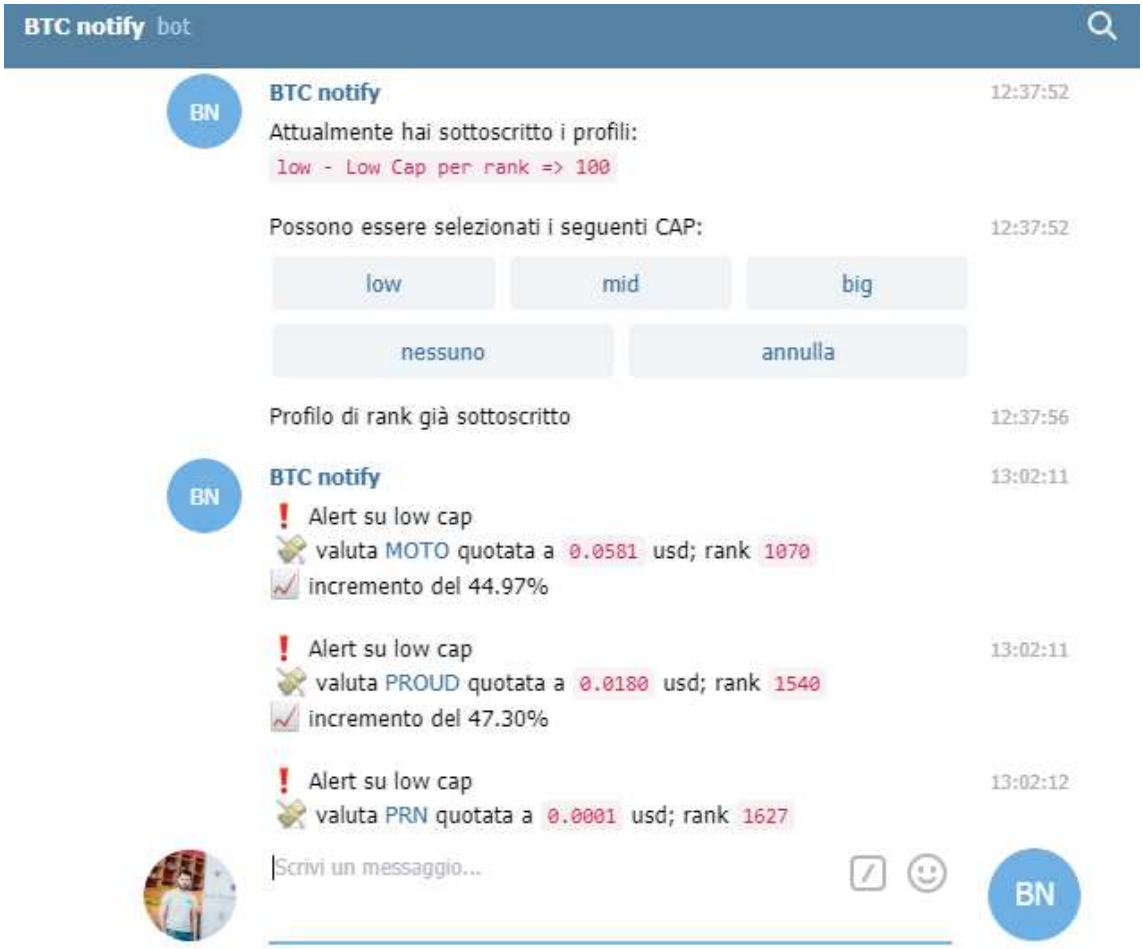
BTC Notify nasce dalla constatazione che ad oggi ci sono oltre 2.000 cryptovalute in circolazione e risulta sempre più difficile comprendere quali siano i progetti più promettenti e identificare quelli con maggior potenziale di crescita nel breve-medio periodo. Inoltre, molte rimangono invariate per lunghi periodi prima di subire improvvisi e repentini apprezzamenti seguiti da veloci correzioni, spesso in prossimità di miglioramenti tecnici o annunci di nuove partnership o semplicemente di notizie rilevanti. Esistono sul mercato diversi sistemi, più o meno sofisticati, per individuare i trend di un asset finanziario, ma uno studio più approfondito del settore mostra come la crescita di valore delle cryptovalute sia molto legata al sentimento di mercato, e quindi risulta difficilmente prevedibile.

BTC Notify è basato su un algoritmo che monitora l'andamento delle cryptovalute, analizzando le variazioni assolute e percentuali della capitalizzazione rispetto a una media data in un istante temporale precedente. Al verificarsi di alcune condizioni predefinite il

[54] Le *Application Programming Interface* (API) sono interfacce che consentono il collegamento tra due software differenti

[55] I Bot Telegram sono automatismi, configurati nella famosa chat di messaggistica istantanea, che inviano notifiche quando succedono particolari avvenimenti

bot genera istantaneamente dei segnali di acquisto o vendita, in modo che l'utente abbia un po' di tempo di anticipo per investire o ritornare dall'investimento.



Screenshot che mostra il funzionamento del Bot Telegram

La versione attuale del bot monitora tre tipi di segnali:

- variazioni del 10% nelle ultime 6h rispetto alla media del giorno precedente;
- variazioni del 20% nelle ultime 12h rispetto alla media dei 3 giorni precedenti;
- variazioni del 30% nell'ultimo giorno rispetto alla media degli ultimi 7 giorni.

Il tool è stato implementato per un cliente privato ed è in fase di rilascio.

3.2.3 Consulenza e formazione

Oltre alla prototipazione di output elettronici, il gruppo Blocktech è periodicamente impegnato in consulenze presso istituzioni e privati che hanno l'interesse di creare nuovi progetti legati all'economia delle cryptovalute, oppure che vogliono meglio capire il mondo del business delle crypovalute in modo da affacciarsi al trading online in maniera consapevole.

Sempre al fine di diffondere il know-how sul tema blockchain e cryptovalute, il gruppo Blocktech partecipa gratuitamente ad eventi nel territorio, come tavole rotonde o lezioni universitarie. Finora, oltre all'evento di lancio del 14 novembre 2017, altri eventi organizzati sono stati:

- *Bitcoin e il futuro dell'economia*, presso Facoltà di Economia di Bari, 22 novembre 2017
- *Bitcon & Blockchain, tutto quello che c'è da sapere*, presso Impact Hub Bari, 6 dicembre 2017
- *Bitcoin e Blockchain, perché il nostro futuro sta cambiando*, presso Università LUM Jean Monnet, 15 marzo 2018
- *Blockchain, Bitcoin e Algoritmi Matematici*, presso Dipartimento di Matematica di Bari, 24 maggio 2018
- *Startup Weekend Blockchain and Artificial Intelligence*, presso Aulab, 26-28 ottobre 2018.

Per quanto riguarda la formazione, il gruppo Blocktech ha realizzato un videocorso che è stato inserito online su *Udemy*, una tra le più grandi piattaforme online di apprendimento a distanza. Il videocorso, dal titolo *"Blockchain, Bitcoin e Cryptovalute: corso pratico completo!"*, è attualmente il più venduto in Italia sul tema blockchain.

Copertina del videocorso su Udemy

3.3 Altre applicazioni

Oltre al settore finanziario, il gruppo Blocktech ha sviluppato progetti blockchain anche in altri settori, in collaborazione con aziende del territorio e enti pubblici. Nel presente paragrafo verranno presentati alcuni tra i principali lavori svolti e quelli in fase di esecuzione.

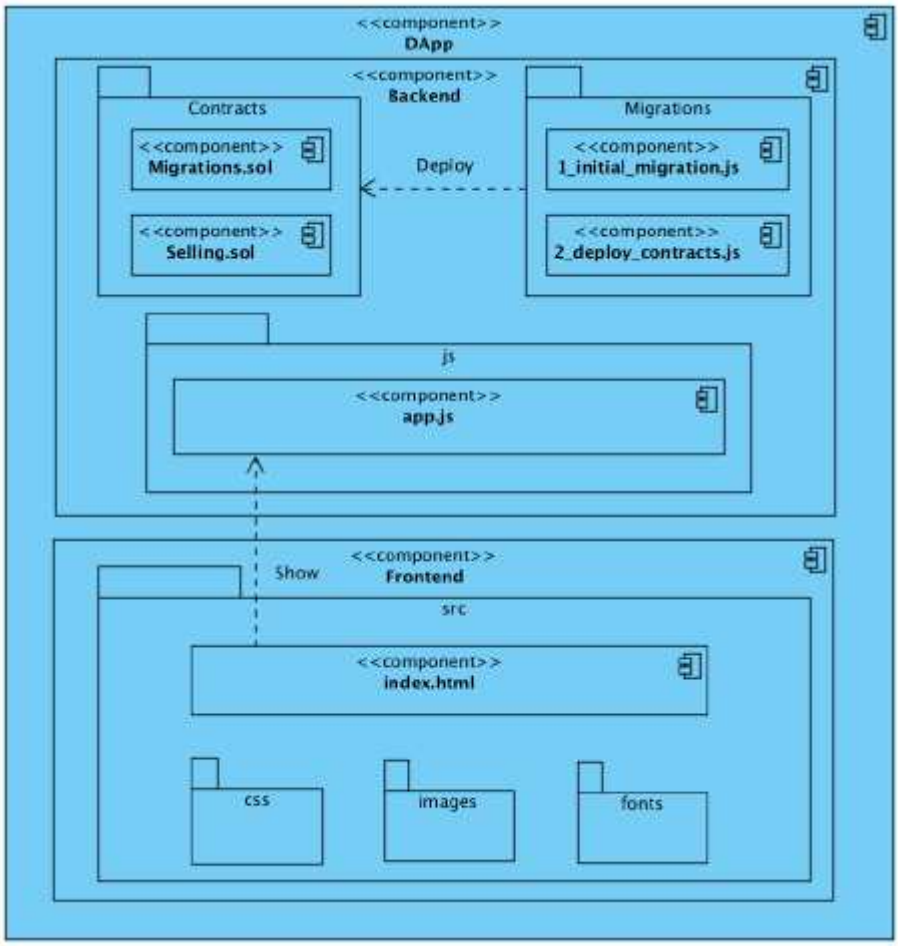
3.3.1 Pubblica Amministrazione

Come già ampiamente discusso nella sezione 2.3.2, uno degli ambiti di maggiore interesse nell'applicazione delle tecnologie blockchain è senza dubbio la Pubblica Amministrazione. Proprio per tale ragione, il gruppo Blocktech ha sempre avuto un occhio attento alle evoluzioni della blockchain in tale settore, e in più casi ha cercato soluzioni innovative che potessero migliorare il settore pubblico.

Uno tra i principali progetti del gruppo in tale settore è stata la *realizzazione di una biblioteca digitale distribuita su piattaforma Ethereum*. Il motivo per cui il gruppo Blocktech ha deciso di implementare una soluzione per il sistema bibliotecario è stata perché si sono unite le passioni di diversi elementi del gruppo, rispetto a pregresse esperienze nel settore bibliotecario da parte di qualcuno, e alla realizzazione di ontologie per la descrizione dei libri da parte di qualcun altro.

Nello specifico, l'applicazione sviluppata si occupa della realizzazione e gestione di una *libreria 3.0*. Le principali peculiarità che differenziano tale libreria da quelle tradizionali sono:

- mappatura del proprietario e del libro su un database distribuito;
- pagamento dei libri mediante cryptovaluta;
- rappresentazione dei libri attraverso un'ontologia.



Schema di diagramma delle componenti della dApp

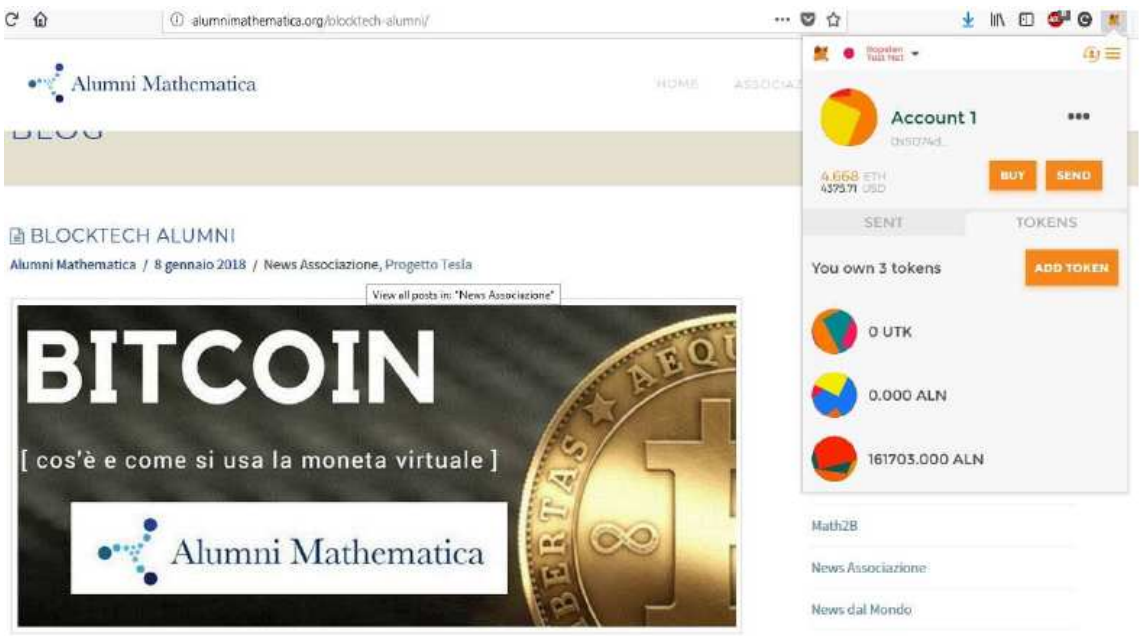
L'obbiettivo di questo progetto è stato quello di realizzare un'applicazione che coadiuvasse ed integrasse due tecnologie avanzate come quella ontologica e quella blockchain all'interno dello stesso sistema. Suddette tecniche, una volta affiancate, hanno

permesso di generare un nuovo sistema innovativo che potrebbe essere preso a riferimento per tutte le biblioteche innovative del futuro.

3.3.2 Blockchain proprietaria

Uno degli obiettivi a lungo termine del gruppo Blocktech è quello della realizzazione di una blockchain proprietaria di Alumni Mathematica che interpreti al meglio lo spirito associativo dell'organizzazione e che possa essere anche uno strumento utile per perseguire il fine associativo che è quello di migliorare il mondo attraverso la diffusione delle discipline scientifiche.

Si tratta di un progetto che necessita di risorse, soprattutto economiche, attualmente non alla portata dell'Associazione. Tuttavia si stanno già sviluppando implementazioni tecniche per tale fine. Il gruppo Blocktech ha, infatti, creato l'*Alumnus (ALN)*, il coin a disposizione di tutti i soci di Alumni Mathematica.



Schermata di visualizzazione per lo scambio degli Alumnus coins

L’Alumnus coin è stato implementato sul network Ethereum e per il momento è scambiato tra i soci di Alumni Mathematica per gestire l’impegno e il lavoro dei soci su alcune attività di interesse associativo.

Per gestire le transazioni si è scelto di implementare un plugin *Metamask*[56]. Attraverso un browser web standard, è possibile individuare lo ALN tra i network presenti, in modo che la dApp possa leggere e scrivere sulla blockchain. In questo modo è possibile per ogni utente gestire il proprio profilo ed effettuare transazioni, trasferendo o ricevendo ALN dal network.

La prima movimentazione di un Alumnus Coin è stata effettuata il 5 febbraio 2018, in occasione dell’Assemblea Annuale dei Soci di Alumni Mathematica.

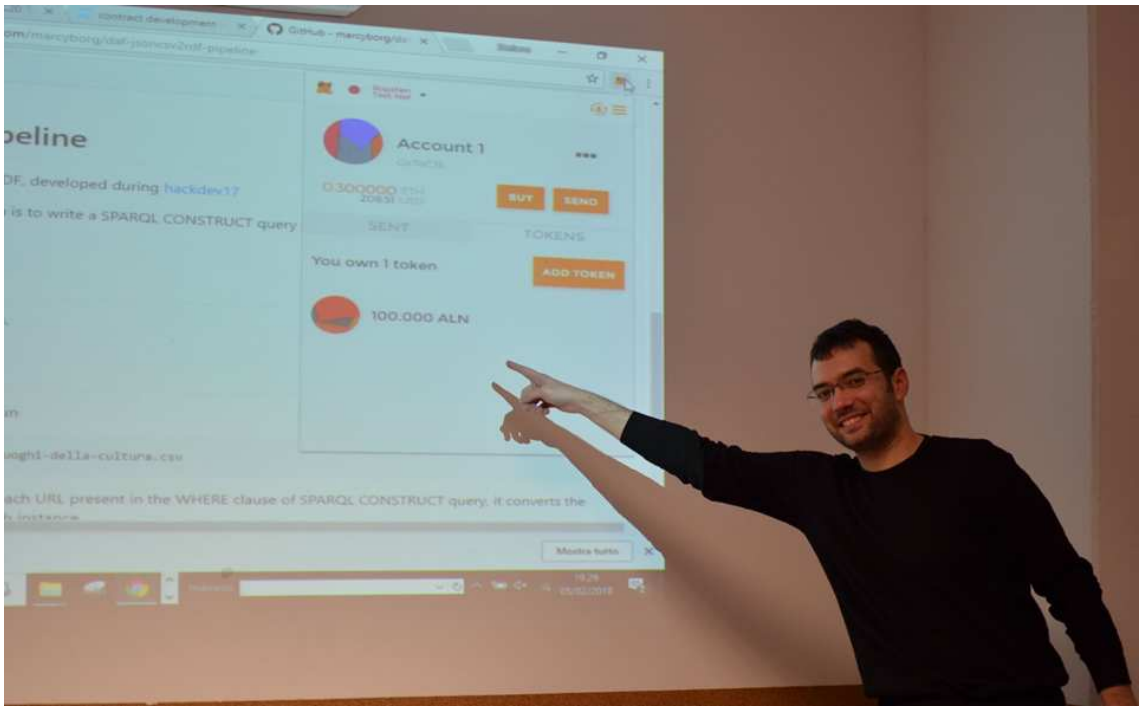


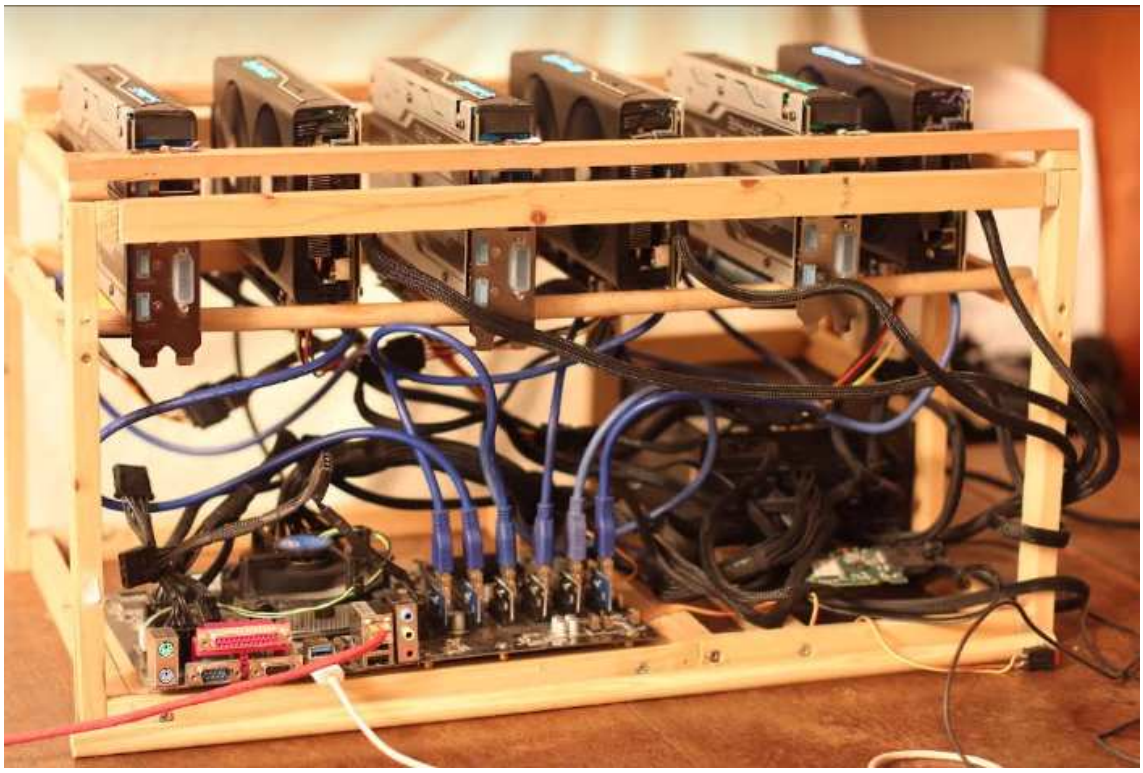
Foto scattata in occasione dell’Assemblea Annuale dei Soci di Alumni Mathematica che testimonia il primo trasferimento di un Alumnus Coin tra due utenti

[56] Metamask (www.metamask.io) è un’estensione Chrome, Firefox e Opera che funge da ponte tra il web classico e il web delle tecnologie distribuite

3.3.3 Esperimenti di mining

Nel paragrafo 2.2 si è già parlato di *mining*, ovvero quell'importante attività svolta da alcuni operatori speciali dei sistemi blockchain che ha l'obiettivo di garantire l'algoritmo di consenso e quindi il trust tra tutti gli utenti. È stato già illustrato il modo in cui questo mining può avvenire, e quali sono i limiti e i vantaggi per chi lo pratica (i limiti sono l'elevato consumo energetico per effettuare l'operazione, i vantaggi sono la possibilità di ottenere ricompense in denaro in caso di approvazione del proprio blocco).

Il gruppo Blocktech di Alumni Mathematica effettua periodicamente esperimenti di mining. Si tratta sempre di attività prototipali, in quanto l'elevato costo energetico non consente di ottenere profitti. Sono comunque attività che hanno il loro valore, in quanto consentono una conoscenza sempre più profonda della tecnologia e l'ottimizzazione costante delle architetture hardware destinate all'attività.



Una delle strutture utilizzate per il mining costituita da schede video poste in serie

Conclusioni

In questo *Project Work* sono stati illustrati casi concreti di utilizzo della Blockchain e il loro legame con i temi di interesse dell'Industry 4.0.
Solitamente c'è molta apertura da parte degli enti pubblici e delle aziende sui temi dell'Industry 4.0, mentre quando si parla di Blockchain sembra si parli di qualcosa di molto lontano, di qualcosa che afferisce a una sfera di sentimento negativo, di qualcosa che non può interessare nell'immediato nessuno, soprattutto se questo interesse riguarda la costruzione di nuovi modelli di business nei settori classici.
Come ampiamente discusso in questo documento, è bene cominciare a documentarsi sulla tecnologia Blockchain, a studiarla e ad approfondirla. Inevitabilmente il mondo del domani sarà basato su paradigmi legati ai registri distribuiti, e piano piano i vari settori si integreranno sempre più a sistemi blockchain. Non appena i limiti tecnologici saranno superati, la maggior parte dei servizi che oggi funzionano con i sistemi classici di centralizzazione della rete verranno erogati attraverso sistemi decentralizzati, semplicemente per il fatto che sarà il modo più sicuro – e con il tempo anche il più veloce – di trasferire e conservare informazioni.
Noi come Alumni Mathematica ci crediamo, e per questo fin da ora stiamo lavorando e investendo tempo e denaro in questa tecnologia. Non più e non meno rispetto a quello che stiamo facendo con tutte le altre tecnologie. Perché una cosa nel business vale sempre: non è importante ciò che è stato, è importante ciò che sarà e il futuro sarà caratterizzato da quanto si sarà stati abili a cogliere le nuove opportunità offerte dal mercato.
La Blockchain è una nuova opportunità.

#ImproveTheWorld

Riferimenti

Bibliografia

- *Blockchain* – Francesco Sacco
- *Cos'è Industry 4.0* – Francesco Sacco
- *Realizzazione di una biblioteca digitale distribuita su piattaforma Ethereum* – Zizzi Walter e Pierpaolo Basile
- *Bitcoin: cos'è e come si usa la valuta elettronica* – Vito Pesola

Sitografia

- http://blockchain.mit.edu/
- http://startegy.it/kurzweil-la-tecnologia-e-un-processo-esponenziale/
- www.blockchain4innovation.it
- https://medium.com/cryptoitalia/famosi-algoritmi-di-consenso-pow-vs-pos-vs-dbft-acbad9c6c11f
- https://blockgeeks.com/guides/proof-of-work-vs-proof-of-stake/
- https://steemit.com/bitcoin/@mooncryption/guide-proof-of-work-pow-vs-proof-of-stake-pos-vs-delegated-proof-of-stake-dpos
- https://www.agendadigitale.eu/cittadinanza-digitale/blockchain-quali-applicazioni-la-pubblica-amministrazione/
- https://www.fxempire.it/education/article/ethereum-e-smart-contract-come-funziona-137221
- https://www.criptomonete-italia.com/ethereum/

Ringraziamenti

Grazie a tutti.