LUISS Guido Carli

LIBERA UNIVERSITÀ INTERNAZIONALE DEGLI STUDI SOCIALI

Gli effetti sulla Corporate Governance e sull'Auditing della Disruptive Innovation della Blockchain

Dipartimento d'impresa e Management

Laurea Magistrale in Consulenza Professionale e Revisione Aziendale

Corporate Governance and Internal Auditing

Relatore

Giovanni

Fiori

Candidato

Mariano

Guzzetta

672721

Co - Relatore

Maria Federica

Izzo

Anno Accademico 2016/2017

Contents

1. Introduzione 5

2. Blockchain: a disruptive Technology 8

2.1. Osservazioni Iniziali 8

2.2. Cosa è la Blockchain? 11

2.3. Il mining Process e l'architettura di rete 14

2.4. La struttura dei Blocchi 21

2.5. La firma digitale ed il sistema delle chiavi 27

2.6. Design Principles 32

2.7. Blockchain Eras 37

2.7.1. Blockchain 1.0: Wallet & Payments 37

2.7.2. Blockchain 2.0: Smart Contracts 39

2.7.3. Blockchain 3.0 Cross-Industries Revolution 44

2.8. Limiti del modello delle Blockchain 56

2.9. Osservazioni Finali 60

3. Gli effetti della distruptive innovation sulla CG e sull'Auditing 62

3.1. Osservazioni Iniziali 62

3.2. Gli effetti sulla CG 65

3.2.1. Le ICO e i Colore Coins: l'emissione dei titoli di Capitale di Rischio e di Finanziamento tramite la Blockchain 65

3.2.2. La Blockchain e i miglioramenti apportati alla trasparenza nelle aziende 73

3.2.3. Il Corporate Voting e l'effetto apportato dalla Blockchain Technology 83

3.3. La Blockchain il game changer della Contabilità e della Revisione Aziendale 86

3.3.1. Gli improvement nel Firm Accounting 86

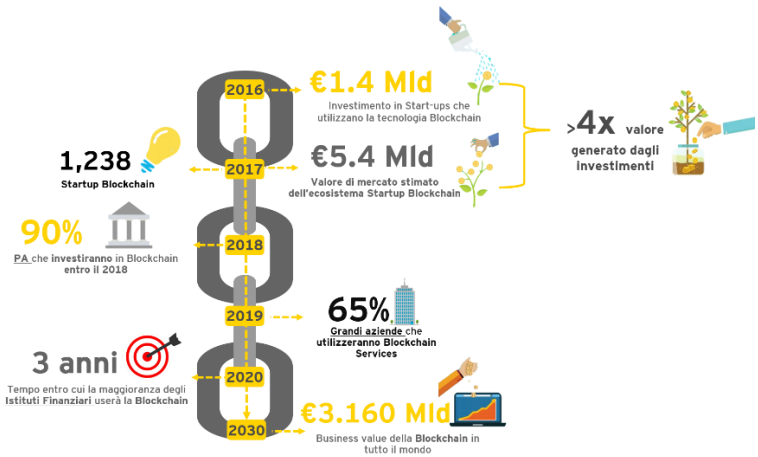
3.3.2. Il Blockchain Audit Model 92

3.4. Osservazioni Finali 96
4. Blockchkain CG & Audit Use Case 98
4.1. Osservazioni Iniziali 98
4.3. BTL, BP, ENI e Wien Energy 106
4.4. Tallystic 114
4.5. Osservazioni Finali 122
5. Conclusione 124
6. Bibliografia e Sitografia 131
7. Riassunto 142
7.1. Osservazioni Iniziali 142
7.2. Blockchain: a disruptive Technology 142
7.3. Gli effetti della distruptive innovation sulla CG e sull'Auditing 146
7.3.1. Le ICO e i Colore Coins: l'emissione dei titoli di Capitale di Rischio e di Finanziamento tramite la Blockchain 146
7.3.2. Il Corporate Voting e l'effetto apportato dalla Blockchain Technology 147
7.3.3. La Blockchain e i miglioramenti apportati alla trasparenza nelleaziende . 149
7.3.4. Gli improvement nel Firm Accounting 152
7.3.5. Il Blockchain Audit Model 153
7.4. Blockchkain CG & Audit Use Case 154
7.4.1. Otonomos 154
7.4.2. BTL, British Petroleum , Wien Energy, ENI e EY. 155
7.4.3. Tallystic 156
7.5. Osservazioni Finali 156

1. Introduzione

Le **grandi aziende leader**, se vogliono continuare a **guidare ed innovare**, non possono continuare ad ignorare la rivoluzione portata dalla Blockchain nei loro differenti ambiti, in quanto **la Blockchain nei prossimi 10 anni cambierà molti settori rispetto a come li conosciamo noi oggi.** Per le aziende che **non si saranno adattate** si potrà immaginare lo **stessa sorte** che hanno avuto le imprese che **nei primi anni duemila non si sono adattati alla rivoluzione digitale** del web, le quali sono rimaste sempre di più **fuori dal settore fino ad arrivare al fallimento.** La Blockchain[1] sarà nei prossimi anni per i **suoi *early adopters* un grande vantaggio competitivo**, il quale diventerà nei prossimi **5-10 anni** uno **standard cross industry** per diversi elementi quali ad esempio la **sicurezza** e la **trasparenza** delle **informazioni**, **l'efficienza** e **automazione** dei **processi** ed infine per **interoperabilità** delle soluzioni e delle piattaforme. La **Blockchain** entro i prossimi **3/5 anni** avrà un **tasso di adozione elevatissimo**, ad esempio **nel settore pubblico** si avrà un coinvolgimento di **quasi il 90% degli attori** (2018), per il **settore corporate** la partecipazione si attesterà a **circa il 65%** (2019). Rispetto allo stato attuale la Blockchain produrrà una enorme crescita nei **differenti settori economici** andando a **quadruplicare in pochi anni gli investimenti fatti.**

Figura 1Blockchain Developpement Pipeline



[1] Report EY, *Blockchain industry Outlook (2016),*
CoinDesk Quarterly update Q3 2016,
angel.co
Blockchainangel.eu,
Gartner
"Building trust in government", IBM

L'obiettivo di questo documento è quello di esplorare le innovative e variegate opportunità proposte dalla Blockchain al mondo aziendale e nello specifico attinenti all'area della Corporate Governance, Accounting a all'Auditing.

Per analizzare al meglio le applicazioni al settore specifico è necessario esplorare la componente tecnica e funzionale della Blockchain, ciò viene approfondito nel secondo capitolo, "Blockchain: a disruptive Technology", il quale conterrà gli approfondimenti relativi alle più importanti caratteristiche della tecnologia Blockchain, quali ad esempio la storia, i pillar cardine, il processo e gli attori che gestiscono la creazione dei blocchi, l'architettura, i modelli di criptazione, le chiavi, la firma digitale, i design principles, gli Stadi di evoluzione della Blockchain, l'approfondimento degli use case nelle diverse industry ed infine l'analisi dei limiti della Blockchain technology.

L'applicazione della Blockchain nelle realtà aziendali, verso la moltitudine di attori come manager, shareholder, governo e PA, clienti, fornitori, dipendenti, creditori, banche e investitori, può avere differenti effetti compositi sia di tipo positvo che negativo, per questa ragione nel terzo capitolo "Gli effetti della distruptive innovation sulla CG e sull'Auditing" verranno approfonditi gli use case relativi alla Corporate Governance, all'auditing e all'accounting. Verranno discussi differenti argomenti come le modalità di emissioni dei titoli aziendali, quali ad esempio i colored coins e le ICO (meccanismi di funzionamento, trend di alcune interessanti ICO, differenze tra le due modalità, la risposta dei governi nazionali a questo fenomeno, specificatamente le risposte di Cina e USA), l'influenza della trasparenza al mondo aziendale (L'automazione delle dichiarazione dei pacchetti azionari, l'effetto sui Corporate Raider, sui Azionisti di maggioranza e di minoranza sul governo, la Agency Theory I e II, Il check sull'ownership per l'acquisto di azioni di competitor diretti e non, Vendita e manipolazione delle Management Stock Option), il corporate voting (funzionamento, effetto su assenteismo nelle assemble e come sostituto del proxy Voting), Accounting (situazione attuale e il triple ledger accouting system,), ed auditing (nuove modalità di auditing, attestazione dell'integrità dei documenti contabili, cambiamenti nella figura dell'auditor e limitazioni dell'Accrual Managament)

Il quarto capitolo andrà a trattare la disamina di 3 differenti esperienze di applicazione reale delle soluzioni Blockchain in ambito Corporate Governance, Auditing e Accounting. Lo scopo di questo capitolo sarà quello di dimostrare, tramite lo studio di casi reali, che la tecnologia Blockchain è già applicabile allo stato attuale alle imprese ed ha su di esse ha effetti positivi. Le start up che saranno esaminate sono:

a. Otonomos, start up dell'ambito della Corporate Governance, la quale permette di utilizzare wallet e smart contract per abilitare la creazione istantanea di società e delle Capitalization Table, la gestione delle transazione dei titoli aziendali e l'automazione delle gestione, produzione e conservazione della documentazione aziendale.
b. BTL, BP, ENI e Wien Energy stanno sviluppando una piattaforma per la riconciliazione trade-by-trade near real-time ed ad altre attività di back office aziendale
c. Tallystic è una integrazione ai sistemi ERP che permette di contenere errori nella fatturazione, i costi per il controllo e l'attestazione (ad esempio i revisori) ed il fabbisogno finanziario.

2. Blockchain: a disruptive Technology[2]

2.1. Osservazioni Iniziali

La Blockchain è stata definita il quinto paradigma disruptive della computing,hera, essa, nei prossimi anni, porterà all'intera economia una grande rivoluzione su tutti i diversi settori, abilitando nuovi servizi e prodotti o migliorando quelli già esistenti. Essa è salita alla cronaca grazie ai Bitcoin, della quale è la tecnologia abilitante le sue transazioni e la quale è soltanto una delle prime e primitive applicazioni.

[2] EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

"Tech Trends 2017: The Kinetic Enterprise", Deloitte University, 2017

"Blockchain: back office block buster", Autonomos

"Blockchain: democratised trust", Eric Piscini, Joe Guastella, Alex Rozman, Tom Nassim, Deloitte 2016

"Embracing disruption tapping the potential of distributed ledgers to improve the post-trade landscape", dttc, 01/2016

"Distributed ledger technology: beyond block chain", uk government chief scientific adviser, Matthew Hancock, Ed Vaizey

"Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, 2008

"Technological Disruption of Capital Markets and Reporting? An introduction to Blockchain", Charted Professional Accountants of Canada, 2016

"Blockchain and its coming impact on Financial Services, Kurt Fanning, David P. Centers, ER The Journal of Corporate Accounting and Finance, 2016

"Blockchain Hitting the big Time, but is Ready?", Frontiers in Finance: for decision-maker in financial services, J. Cassidy, E. Maguire, D. Montes, 2016

"Mastering Bitcoin - Second Edition", Andreas M. Antonopoulos, In pubblicazione

"Blockchain Technology: Preparing for change",D. Treat, L. McGraw, C. Helbing, C. Brodersen , Accenture, 2016

"Bitcoin, Blockchain & Distribted Ledger: Caught between promise and reality, P. Evans-Greenwood, R. Hilard, I. Harper, P. Williams, Deloitte Australia

Un elemento essenziale per capire al meglio le applicazioni della Blockchain al mondo reale è la conoscenza "tecnica" delle sue modalità di funzionamento, per questo motivo il secondo capitolo intitolato **"Blockchain: a disruptive Technology"** sarà incentrato sulla definizione della tecnologia Blockchain su diversi elementi, quindi esso sarà propedeutico alla migliore spiegazione dei successivi capitoli. Esso tratterà argomenti eterogeni, quali ad esempio:

1. la sua storia dal sua nascita come tecnologia abilitante le transazioni dei Bitcoin fino alla sua applicazione cross industry
2. la declinazione e l'analisi dei suoi pillar caratterizzanti quali il consensus, distributed ledger, automazione ed immutabilità
3. i problemi da essa risolti come il *double spending* e il *Byzantine Generals' Computing*),
4. Lo studio relativo alle sue modalità di funzionamento con un focus sui miners e sulle modalità di mining
5. L'infrastruttura architetturale dei nodi e delle diffrenti tipologie di nodi, del network e dei aritcolati tipi di network ed il fork
6. La struttura dei Blocchi della catena e le sue modalità di creazione ed inserimento nella Chain.
7. Le modalità di criptazione delle transazione e dei dati in essa inserita ed il modello di funzionamento delle chiavi e della firma digitale delle transazioni
8. L'analisi dei design principles, quali ad esempio il distributed power, il valore degli incentivi all'interno del network, la sicurezza, l'integrità dei dati, l'interoperabilità, la velocità e la riduzione dei costi, l'interoperabilità, il trusted protocol e l'integrità del network
9. Gli Stadi di evoluzione della Blockchain (La Blochain 1.0, 2.0 e 3.0) e la trattazione per ogni stadio evolutivo di differenti use cross industry
10. I limiti della Blockchain technology come ad esempio la possibile influenza del sistema ecosistema governativo, la percezione pubblica ed i limiti tecnologici.

Ciò verrà fatto in modo tale da permettere una sua esplorazione e per permettere di capire al meglio le applicazioni reali e gli use case che saranno approfonditi, rispettivamente nei capitoli 3 e 4 di questo documento.

2.2. Cosa è la Blockchain?[3]

Considerando i nuovi trend in ambito digital e tecnologico, che negli ultimi anni stanno caratterizzando il mercato, si possono scorgere degli elementi caratterizzanti che accomunano le tecnologie emergenti: tutte loro sono ***enabler*** di nuovi servizi. Data la presenza di questi trend, la sicurezza delle informazioni e dei dati guadagnerà nel prossimo futuro un ruolo sempre più importante, per questa ragione, la Blockchain sarà al centro dell'interesse mondiale, essendo la tecnologia che più è affine alle problematiche relative alla sicurezza, alla trasparenza, all'interoperabilità e alla privacy. Essa occuperà un importante parte del panorama tecnologico mondiale, secondo le stime del *World Economic Forum,*[4] il protocollo Blockchain trasporterà entro il 2025 circa il 10% del PIL mondiale, grazie ai suoi elementi di ***distruption*** e di trasversalità lungo le ***industry*** e i mercati di applicazione.

L'incredibile innovazione portata dalla Blockchain al mondo è così grande da essere definita il quinto paradigma ***distructive*** *del* ***computing***, dopo i *mainframe* negli anni settanta, *i personal computers* negli ottanta, internet negli anni novanta e nei anni duemila i social network. La Blockchain si sta imponendo e si imporrà sempre di più nell'economi mondiale. La sua innovatività è paragonabile per grandezza solamente alla potenza innovativa apportata da internet. Il suo apporto non è solamente limitato ai sistemi di pagamento, ma il suo paradigma può essere esteso a qualunque situazione nella quale viene richiesto un soggetto terzo indipendente garante di un elevato livello di sicurezza.

La tecnologia Blockchain nasce come protocollo sottostante alla criptovaluta chiamata *Bitcoin*. Nel 2009 la parola *Bitcoin* viene utilizzata per la prima volta, da ***Satoshi***

---

[4] "Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world", Don Tapscott, Alex Tapscott

"Blockchain: blueprint for a new economy", Melanie Swan, 2015

"Deep Shift Technology Tipping Points and Societal Impact: Global Agenda Council on the Future of Software & Society" Survey Report, World Economic Forum, September 2015

Nakamoto[5] nel suo celeberrimo *paper* intitolato *"Bitcoin: a Peer-to-Peer Eletronic Cash System"*. Nakamoto introduce e descrive una valuta digitale, il cui scambio viene permesso **senza l'ausilio di un terzo fidato**, ma direttamente tra le due parti. La sua apparizione è da ricollegare molto probabilmente alla **crisi del 2008**, alla **minore fiducia** dei consumatori nelle classiche **istituzioni bancarie** e al modello centralizzato delle stesse. Il meccanismo attraverso cui avvengono le transazioni della criptovaluta, come già detto, è la Blockchain, essa è un **registro**, un libro contabile *(**ledgers***), il cui contenuto è diffuso sui **nodi** (*nodes*) di una **rete decentralizzata** (*distributed*) basata sul **protocollo *peer-to-peer***, essa viene aggiornata dai **minatori** (*"miners"*), i quali **aggiungono i blocchi** l'uno dopo l'altro, legandoli in maniera sequenziale in base ad un **ordine temporale**, inserendo indelebilmente e in maniera cifrata all'interno di questi blocchi le transazioni che ricevono dagli utilizzatori del Bitcoin.

In ogni modello di criptovaluta possiamo distinguere **3 differenti livelli**: la Blockchain, il protocollo e la valuta. La **valuta** è l'elemento che viene **scambiato** tramite il software che conduce la transazione con elevata sicurezza (**il Protocollo**), la quale transazione viene scritta all'interno di uno *spreed sheet* decentralizzato (**Blockchain**), ad esempio nel modello Bitcoin possiamo riscontrare la presenza di una valuta Bitcoin, il protocollo Bitcoin e la sua relativa Blockchain. Derivando dal mondo delle criptovalute la Blockchain vede il suo primo utilizzo in questo ambito, in quanto la sua applicazione ha permesso di risolvere diversi complessi problemi relativi al ***double spending*** e al ***Byzantine Generals' Computing***.

Il *double spending problem* è legato al problema della possibilità di **spendere due volte la stessa criptovaluta**, essendo i Bitcoin una stringa di codice, quindi come tutti gli elementi digitali **infinitamente copiabile.** Non si può avere la certezza che quel Bitcoin non sia già stata speso in una differente transazione **senza l'intermediazione di un terzo indipendente** o della Blockchain.

[5] **Pseudonimo** di uno o più informatici, ancora **rimasti anonimi**. Sulla sua identità, soprattutto negli ultimi anni, si sono sviluppate diverse ipotesi, nessuna delle quali è stata ancora acclamata per vera.

Il problema del *Byzantine Generals' Computing*[6] è relativo al fatto che le differenti parti (*Generals*) pur non fidandosi e non conoscendosi devono coordinarsi, comunicare e fare transazioni tra di loro. La tecnologia Blockchain risolve entrambi i problemi, in quanto grazie alla combinazione della tecnologia del *file-sharing,* basata sulla rete *Peer-to-peer di BitTorrent,* con una chiave pubblica crittografata, si può eliminare sia il problema del *double spending* e sia la necessità di avere una *trusted third party*. Ciò avviene poiché la proprietà del Bitcoin è registrata in un *public ledger record* e confermata dal protocollo di criptazione e dalla *community* dei minatori. Il problema del *Byzantine Generals' Computing* viene risolto dal fatto che la Blockchain è una tecnologia *trustless*, in quanto non richiede agli attori che operano al suo interno di fidarsi gli uni degli altri o di una entità centralizzata, che controlla i vari processi, ma bensì richiede la fiducia solamente verso il sistema Blockchain, il quale basandosi su una sequenza di transazioni rese pubbliche in maniera sequenziale su una *pubblic ledger* permanente e visibile a tutti risolve il problema della fiducia verso gli altri attori.

[6] "The Byzantine Generals Problem", Leslie Lamport, Robert Shostak, and Marshal Pease

2.3. Il mining Process e l'architettura di rete

La Blockchain può essere monitorata da tutti, ma al contempo non è di proprietà di alcun soggetto, in quanto essa è un database diffuso e distribuito su una rete di nodi indipendenti tra loro, quindi per modificarne o aggiungere i blocchi, servirebbe avere il controllo del 50%+1 (*Consensus*) per questa ragione non esiste un unico *single point of control*.

La modalità con cui vengono aggiunti i blocchi e con cui vengono immessi nel mercato dei nuovi Bitcoin viene chiamata ***mining***, essa viene assolta dai Minatori ("*miners"*). Inoltre esso rappresenta anche il processo attraverso con cui le transazioni sono verificate ed aggiunte alla *pubblic ledger*. L'azione dei *miners* è basata essenzialmente nel risolvere problemi matematici, in base alle informazioni contenute nel blocco. I *miners* sono incentivati a svolgere questa attività dal ricevere in cambio una ricompensa. La ricompensa non è data a tutti, ma è il premio per il vincitore di una "gara" tra tutti i minatori, che si avvia in media ogni 10 minuti, per la risoluzione di un algoritmo matematico col fine di verificare un determinato numero di transazioni e, allo stesso tempo, creare un *fingerprint*, un'impronta univoca nel registro. Esso è un processo iterativo, i miners per trovare l'effettivo Hash risolvente provano diverse volte con Hash diversi tra loro.

Per questa ragione, il primo *miners* che risolve il problema, condivide la soluzione con gli altri minatori come prova del lavoro (*Proof-of-work*), gli altri minatori accetteranno la prova del lavoro e cosi il blocco viene aggiunto alla Blockchain. Questo meccanismo ha un doppio effetto incentivante, il primo è quello relativo ai minatori, che vengono premiati per il lavoro svolto, il secondo è indirizzato all'incentivazione del network ad emettere nuove monete in modalità prefissata. Nel 2008 la ricompensa era fissata in 50 Bitcoin per ogni blocco minato, mentre ora è di 12,5 Bitcoin per ogni blocco. La netta diminuzione della quantità emessa è dovuta al fatto che il numero di Bitcoin emessi si dimezza ogni 4 anni, per arrivare ad una situazione in cui non saranno più emissioni di nuovi Bitcoin ed ad una quantità emessa totale di Bitcoin pari a circa 21 milioni, ciò si avrà nel 2140, quindi non potendo più emettere vi sarà un periodo di deflazione.

Figura 2 Il Processo di Mining

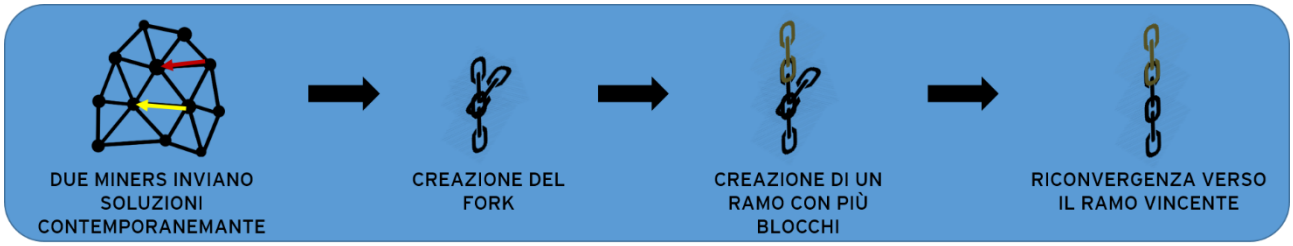
Nella Blockchain, essendo un registro decentralizzato, può accadere che vi siano **differenti copie** di essa, in quanto ogni nodo seleziona e cerca di aggiungere il blocco che ha **la più lunga catena** o che la **catena** che ha cumulato la **maggiore difficoltà** nel **minare**. Però può accadere che, in normali condizioni vi siano **due o più minatori**, che competano per formare la catena più lunga o la catena con il livello più alto di difficoltà, potrà accadere che due **minatori risolvano** gli **algoritmi** in un breve lasso di tempo tra l'uno e l'altro. Entrambi i blocchi generati dai minatori contendenti conterranno una **soluzione validata** dal suo *proof-of-work* ed entrambi sono **blocchi figli dello stesso blocco padre.**

Trovata la soluzione all'algoritmo, entrambi i minatori provvederanno a spedire i loro blocchi, con la relativa *proof-of-work,* al **nodo più vicino**, che lo **propagherà** agli altri nodi del network, quando i ognuno di essi lo riceverà, provvederà a **validarlo** e lo **incorporerà** alla sua **Blockchain** come nuovo blocco, estendendo la propria catena. Lo stesso **nodo** riceverà anche **l'altro blocco**, spedito dall'altro *miner* "vincente", il nodo lo validerà e lo aggiungerà ad una **catena secondaria**, non alla principale, in quanto ogni blocco dovrà essere collegato al suo *parent block*. Si verrà a creare una situazione in cui i nodi avranno due catene con blocchi differenti, ciò farà venire **meno l'unicità** dell'*Hash Height* dei blocchi.

Esso è uno **stato temporaneo**, chiamato ***Fork***, nonostante il quale, si continuerà a minare e quindi ad aggiungere i blocchi, finché uno delle due versioni non riuscirà a **creare un ramo con più blocchi** e con un **livello di difficoltà maggiore**. In questo caso, chi avrà scelto come **Blockchain principale** la catena **vincente**, **aggiungerà il blocco** ed **interromperà** la ***chain* secondaria**. I nodi che avevano scelto come ramo principale la chain **non vincente** vedranno due catene, aventi **differenti livelli di difficoltà** e **da numero differente di**

blocchi. Saranno costretti, dal criterio alla base della Blockchain, a scegliere la chain "vincente" come primaria e l'altra come secondaria, questo è chiamato riconvergenza della catene rispetto al *Fork*. Il network di nodi, in questo modo, avrà nuovamente una catena univoca. Ogni minatore che stia minando un blocco per la chain secondaria smetterà di minare in quanto essa non è la catena più lunga e quindi tutti i minatori nuovamente mineranno la stessa catena.

Figura 3 Il Fork di una Blockchain



La rete è basata su una architettura *peer-to-peer* costruita al di sopra del protocollo internet. I nodi della rete sono tutti sullo stesso piano in quanto non ci sono né server, ne servizi centralizzati e ne gerarchie tra i nodi stessi. Pur essendo sullo stesso piano i nodi hanno differenti ruoli e funzionalità, quali *routing*, *DB* di tutta la Blockchain, minare e le funzioni di *Wallet*. Tutti i nodi per partecipare al network devono avere almeno la funzione di *routing* e devono validare e inoltrare i blocchi.

Possiamo distinguere diverse categorie di nodi in base alle funzioni svolte da loro:

1. *Full Nodes*: svolge le funzioni di *Full DB, mining, wallet e routing*. Essi possono autonomamente verificare le transazioni senza bisogno di una referenza interna.
2. *Lightweight Node o SPV:* mantengono solo una parte dell'intera Blockchain e possono verificare tramite il metodo di *simplified payment verification (SPV).*
3. *Mining Nodes:* minano i blocchi per risolvere l'algoritmo matematico. I mining node possono essere a loro volta *full nodes o lightweight nodes*.
4. *Wallet Nodes:* sono quei nodi che incorporano la funzione di *wallet* per le cryptocurrencies.

Figura 4 Categorie di Nodi

	DB	MINING	WALLET	ROUTING
FULL NODE	✓ FULL	✓	✓	✓
LIGHTWEIGHT NODE	✓ PARZIALE	✓	✓	✓
MINING NODE		✓	✓	✓
WALLET NODE			✓	✓

Quando viene **creato un nuovo nodo,** esso deve cercare e **connettersi** con gli **altri nodi** del network. Per farlo è necessario che **scopra almeno un nodo**, esso può avvenire mediante **i *DNS Seed*** (liste di indirizzi di nodi) oppure tramite l'utilizzo di un ***bootstrapping nodes*.** Una volta trovato il primo nodo a cui connettersi, esso userà lo stesso per arrivare ad altri nodi per stabilire differenti connessione con il network. Completata la connessione, inizierà a **scaricare il database** della Blockchain per sincronizzarsi con essa e per poter **verificare le transazioni**. Oltre ai suddetti nodi ci sono altri nodi che fanno girare protocolli diversi dal *peer-to-peer*, essi abilitano ulteriori servizi per la rete.

La rete può essere strutturata in **diverse forme** in base ai **differenti permessi** per gli attori:

a) ***Permissionless***: il **network** ed il **registro** sono **accessibili a tutti** ed è **possibile** per ogni attore **diventare** un **nodo** della stessa rete. Il network è basato su **incentivi** per i ***miners*** in quanto il ***mining*** richiede dei **costi da sostenere.**

b) ***Permissioned***: in questa conformazione il **registro** è **accessibile** a tutti, ma per poter diventare un **nodo** è necessaria una **approvazione**. Questa è la forma prescelta dalle **banche** che si sono uniti in **consorzi** per lo sviluppo della tecnologia Blockchain. Per funzionare possono essere creati due sistemi basati su **due liste differenti di attori:**

   a. ***White List***: lista degli attori a cui è **permesso entrare** in contatto con il network di nodi. Questa modalità richiede una formazione della lista ex ante o tramite richiesta per i nuovi nodi.

   b. ***Black List:*** la lista dei soggetti che sono **stati bannati** della rete. La sua formazione è graduale ed iterativa in base al comportamento o alle caratteristiche degli attori presenti nella rete.

c) **Privata:** il registro **non è pubblico** e i **nodi** sono gli **enti dell'azienda** e della **filiera di imprese.** Questa modalità è usata dalla **aziende** per creare delle ***ledger*** per i propri **processi interni** e per **offrire servizi** proprietari legati ad essa.

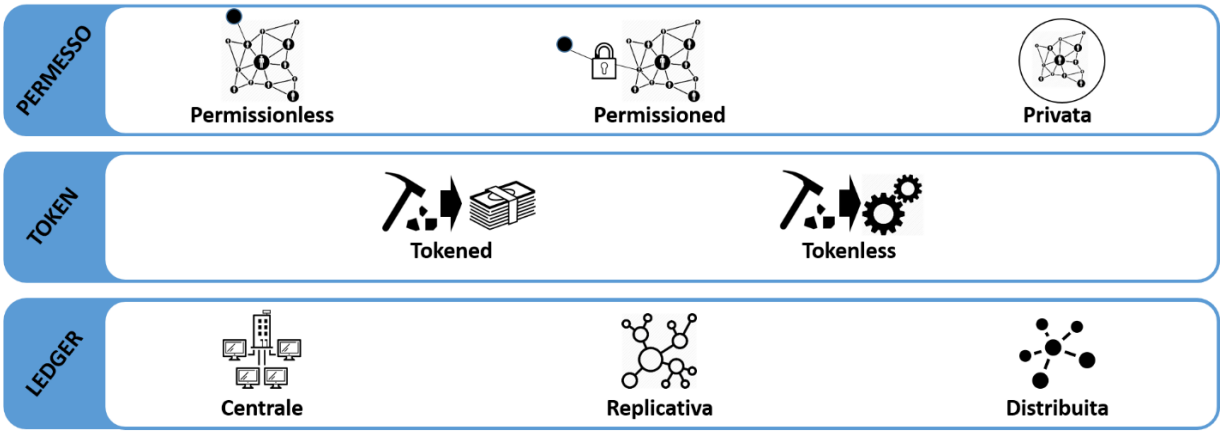
La **struttura** della rete può variare in base alle **modalità di funzionamento operativo** della stessa:

1. ***Tokened***: per operare necessitano di utilizzare sistemi basati su ***token***, riflettenti un valore in valuta. Il loro utilizzo è necessario per il **pagamento dei *miners***.
2. ***Tokenless***: le reti *tokenless* per funzionare **non hanno bisogno** di utilizzare dei ***token*** al fine di effettuare dei scambi. Sono implementate in Blockchain dove **non sono necessari incentivi esterni** per i *miners*, come ad esempio nelle Blockchain **private o permissioned,** dove i ***miners*** sono gli enti, BU della azienda o del consorzio. La loro volontà di fare *mining* non è data dall'eventuale incentivo in criptovaluta, fornito al *miners* vincente, ma dal **volere inserire le transazioni e le relative informazioni in Blockchain**.

La **ledger** può essere anche classificata anche in base al modo in cui **i dati sono replicati:**

1. **Centrale:** i file sono detenuti solamente da **una autorità centrale** e gli altri attori devono **richiedere l'accesso** all'autorità centrale per accedervi. L'autorità centrale limita l'accesso e **garantisce l'integrità dei dati e l'identità della rete.**
2. **Replicativa:** questa forma di rete è gestita da **una autorità centrale**, gli altri attori per avere **accesso** e per aggiungere un record **devono comunicare con l'autorità centrale**. Gli **attori** possono **avere** e mantenere una **copia** dei dati in locale, ma sono **loro** che devono adoperarsi per **aggiornarla**. **L'autorità centrale limita l'accesso** e garantisce **l'integrità** dei dati e **l'identità** della rete.
3. **Distribuita:** La responsabilità di mantenere la rete è divisa **tra un gruppo di pari (nodi).** Gli attori possono avere **una copia dei file** dagli altri attori, data la mancanza di una autorità centrale. **L'aggiunta di record** è basata sul meccanismo del consenso ed è gestita dall'intero network di **nodi** ed **approvata** dalla **maggioranza**.

Figura 5 Tipologie di Ledger



La ***ledger*** contiene due tipi di ***records***:

a. **Records Nativi:** essi rappresentano informazioni, nascono solo quando vengono inserti nella rete, come ad esempio le informazioni legate ai **beni virtuali** o come gli *Smart Contracts*.
b. **Record di Collegamento:** sono dei dati che permettono il **collegamento ad elementi esterni,** che già esistono **separatamente dalla rete, di elementi digitali**. È il caso dei certificati esterni, essi esistono al di fuori della Blockchain ma possono essere inseriti in Blockchain.

La rete è basata sul **sistema del consenso**, il suo emergere deriva da diversi **processi,** che avvengono **indipendentemente sui nodi lungo la rete:**

1. **Verifica Indipendente di ogni transazione:** quando il nodo riceve la transazione, esso provvederà a **verificarla** tramite il **matching** tra gli **elementi della transazione** ed alcuni **criteri**. Una volta completato il match, essa verrà **aggiunta** ad un ***memory pool*** in attesa di essere aggiunta ad un blocco ed essere propagata lungo tutto il **network**.
2. **Aggregazione indipendente delle transazioni in un nuovo blocco:** una volta inserite nel **memory pool,** esse rimarranno in **attesa** di essere **minate** in un **nuovo blocco** (*Candidate Block).*
3. **Indipendente verifica dei nuovi blocchi**

4. Assemblaggio dei blocchi nella Blockchain e selezione indipendente della catena con il più elevato impiego computazionale: Dopo essere stato verificato, il blocco viene propagato nel network, mentre quelli invalidi sono eliminati. I nodi possono contenere diversi tipi di blocchi, vi potranno essere blocchi connessi alla Blockchain principale, altri potranno formare un ramo secondario oppure vi saranno blocchi che non hanno il block parents (*Orphan Block),* essi verranno inseriti nella *orphan pool* per poi essere reindirizzati verso un *parents block*.

2.4. La struttura dei Blocchi[7]

Ogni **blocco** è formato da diverse parti:

1. ***Hash:*** è l'elemento **identificativo** del blocco e delle transazioni, esso viene generato usando la tecnologia crittografica ***SHA256*** **sull'*header* del blocco** e restituirà una **stringa** di lunghezza predefinita. Per far sì che sia possibile fare l'*Hashing* delle informazioni contenute nel blocco sono necessarie alcune specifici elementi, quali **il *nounce*, una stringa di codice** (contenuta nell'Header del blocco) e **un contatore.**

2. ***Block Height*:** esso permette **un'identificazione univoca** del blocco, quindi anche delle relative transazioni. Esso è un elemento identificativo del blocco in quanto esprime la **posizione del blocco lungo catena** e quindi rispetto al blocco generatore di quella particolare Blockchain. Esso però **non è un identificatore universale**, in quanto il *block height* può perdere il suo carattere identificativo in caso di *fork.*

3. ***Block Header:*** esso ha una dimensione di circa 80 bytes e contiene **tre diversi metadata**:

    a. **Versione:** numero relativo agli aggiornamenti del software e del protocollo

    b. **Metadata del blocco precedente (*parent block*):** esso crea una catena di collegamenti tra i blocchi, i quali sono collegati con il primo blocco della catena (*Genesis Block*). Esso influenza l'*hash* del blocco, quindi l'*Hash* del

[7] https://en.Bitcoin.it/wiki/Block

https://github.com/tendermint/tendermint/wiki/Block-Structure

https://en.Bitcoin.it/wiki/Block_hashing_algorithm

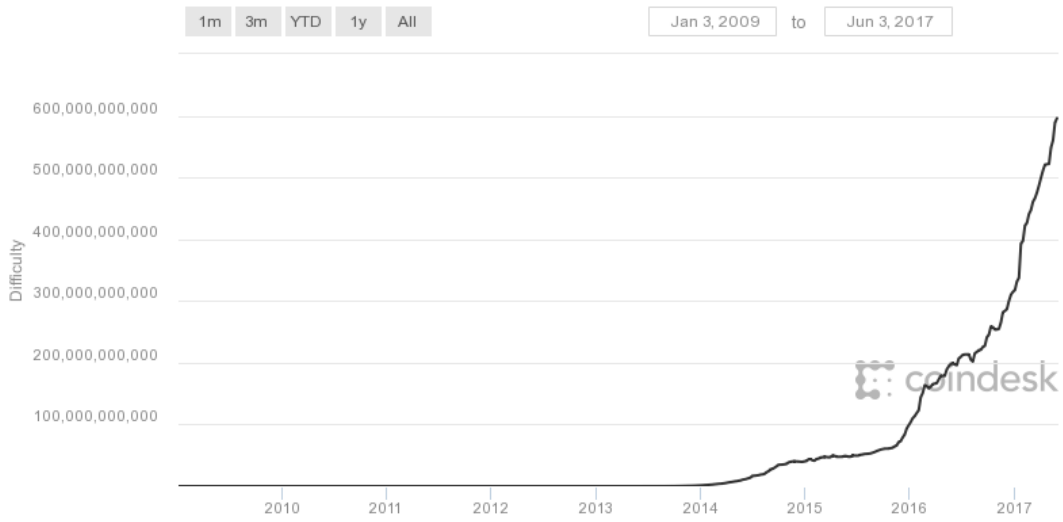
https://www.fjordnet.com/conversations/the-trust-trade-off-permissioned-vs-permissionless-Blockchains/

https://www.ibm.com/blogs/think/2016/07/checking-the-ledger-permissioned-vs-permissionless-Blockchains/

blocco figlio è influenzato dall'*Hash* del blocco padre. Una modifica di un blocco padre comporta la modificazione di tutti i successivi. Ciò è una garanzia per la sicurezza delle informazioni contenute nella Blockchain, in quanto la modifica di un blocco porta per effetto a cascata il ricalcolo di tutti i successivi *Hash,* richiedendo un enorme sforzo computazionale tale da rendere immutabile ed inconveniente modificare il blocco già inserito in Blockchain. Con questo modello è possibile cambiare solo i blocchi superficiali, statisticamente si considera come limite di immodificabilità il blocco numero sei.

c. Metadata relativi al *mining*: questa classe contiene la difficoltà nel minare, il *timestamp* e il *nounce* (un contatore utilizzato per assicurarsi che ogni transazione può essere elaborata una sola volta), queste sono tutte grandezze collegate alla competizione tra i minatori. La difficoltà nel minare è crescente e viene aggiornata ogni 2016 blocchi.

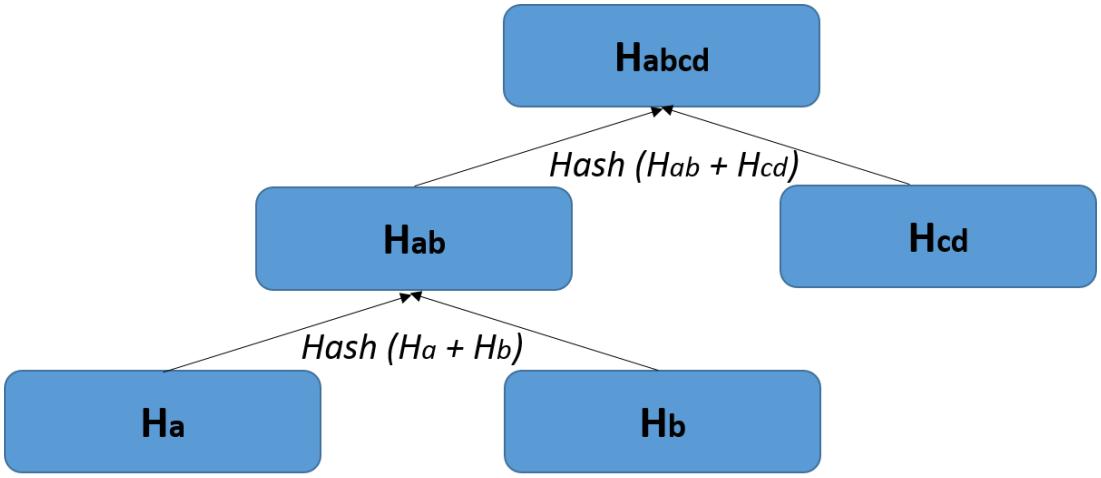
Figura 6 Difficoltà nel Mining



d. *Merkle tree root* del blocco: esso è il *summary* di tutte le transazioni contenute nel blocco. Il summary viene ottenuto tramite il sistema *Binary Hash Tree*, usato per riassumere e verificare un grande set di dati. Il *merkle tree* è costruito in maniera ricorsiva, prendendo i due *hash* in un nodo,

concatenandoli ed creando l'*Hash* congiunto. Ad esempio il nodo H_{ab} ha due hash figli H_a e H_b, i quali vengono concatenati ed Hashati a loro volta.

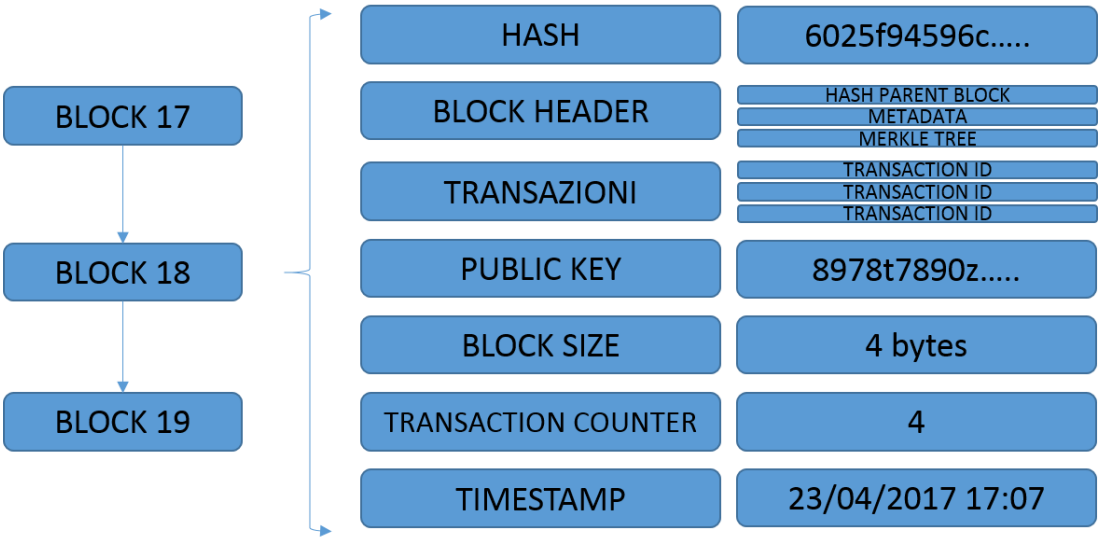
Figura 7 Merkle Tree Root



e. *Soluzione dell'algoritmo*

4. Transazioni: ogni blocco può contenere al suo interno una o più transazioni, ogni blocco contiene in media circa 500 transazioni.
5. *Public Key*: stringa di codice necessaria al ricevente e al mandante per identificare e verificare le informazioni della transazione.
6. *Blocksize:* esso è la grandezza del blocco ed è generalmente in media intorno ai 4 bytes
7. *Transaction counter:* esso è un contatore, che esprime il numero delle transazioni contenute nel Blocco e la sua dimensione è compresa tra 1 e 9 bytes

Figura 8 Struttura del Blocco



La **criptografia** su cui si basa il sistema della Blockchain ha una differente funzione rispetto ai classici sistemi criptografici. La differenza si basa nelle finalità dell'uso della criptografia stessa, in quanto nel sistema Blockchain essa viene usata **per provare la conoscenza di un segreto senza rivelare il segreto stesso** (Firma Digitale) o per **provare l'autenticità dei dati** (*Digital Fingerprint*), quindi la sarà finalizzata **per il *proof-of-work***.

Uno degli elementi fondamentali delle transazioni sono **i *transaction output*,** essi sono indivisibili **gruppi di Bitcoin** validati e riconosciuti dall'intero network. I *transaction outputs* sono composti da diversi elementi*:*

1. **Valore della transazione:** essa può avere **qualunque valore**, è denominato in Bitcoin ed è espresso in multipli di *sathoshi* (10^{-8} Bitcoin).
2. **Un *Cryptographic puzzle:*** che rappresenta le **condizioni** che determinano la **spendibilità** dell'output.
3. **Le *Fee* delle transazioni:** le quali andranno a **remunerare i minatori,** per mantenere sicuro il network, inoltre le fee sono loro stesse un **deterrente contro i soggetti** che vogliono **attaccare il network,** in quanto rendono **anti-economico** il raggiungimento del possesso di più della metà del network. Le *transaction fee* all'inizio **erano fisse e costanti**, ma gradualmente si sono **evolute** verso la **variabilità** guidata dalla capacità e dal volume delle transazioni. Esse sono calcolate **in base ai Kilobytes della transazione**, esse perciò influenzano il processo

di **prioritizzazione** delle transazioni. I minatori daranno la priorità alle transazioni con una *fee* più alta, ciò implica che le transazioni con una *fee* bassa verranno incluse in successivi blocchi minati o non verranno incluse. La struttura delle transazioni **non contiene esplicitamente il valore della fee** delle transazioni, essa viene desunta indirettamente tramite la **differenza** tra il valore degli **input** e il valore degli **output**.

4. ***Coin base Transaction***: esse rappresentano la **prima transazione di ogni blocco** e sono una eccezione al collegamento input-output, sono generate dal **minatore vincente** e **rappresentano i Bitcoin creati per la remunerazione del minatore**.

Gli **output** spendibili sono chiamati ***Unspent Transaction Outputs (UXTO),*** la somma di essi per ogni *wallet* è valore del wallet stesso. Quando nella transazione il *wallet* ricevente riceve l'output della transazione significa che il *wallet* ha trovato nella Blockchain **una transazione** che **non** è stata **spesa** e che può essere **spesa** con una delle **chiavi** depositate presso il ***wallet***. Quando il valore degli *Unspent Transaction Outputs* è più grande del valore della transazione da effettuare, essendo gli ***UXTO*** indivisibili, quindi dovranno essere **interamente spesi** e tal fine verranno **generati due output**: il primo servirà **a pagare l'oggetto** della transazione e l'altro effettuerà il ***charge back*** **al *wallet*** per un valore pari alla differenza tra il valore degli *UXTO* e il valore dell'oggetto della transazione.

La maggioranza degli output delle transazioni è reso **sicuro** dallo ***script Pay-to-Public-Key-Hash (P2PKH)*** che lega **l'output** ad uno specifico ***Bitcoin address***, esso può essere sbloccato solamente presentando la chiave pubblica e la firma digitale che corrisponde a quella specifica **chiave privata**.

Durante la trasmissione al network delle transazioni vengono **serializzate**. La serializzazione è un procedimento che converte la **rappresentazione interna** della struttura dei **dati** in un **formato** che ne permetta una migliore **trasmissione,** tramite uno stream di un byte alla volta. Una volta che il flusso ha raggiunto la **destinazione** viene **de-serializzato** e quindi trasformato nella **rappresentazione interna.**

Un altro elemento fondamentale della transazione sono i ***transaction input***, essi sono composti da:

1. Un'indicazione sugli *UXTO* formato da:
    a. *Hash* della transazione
    b. Numero sequenziale che rappresenta la posizione della transazione nella Blockchain (*Blockheight*)
    c. *ID* della transazione che contiene gli *UXTO* che verranno spesi
2. *Unlocking script*: è lo *script* che pone le condizioni necessarie affinché gli *UXTO* vengano spesi, esso contiene una firma digitale ed una chiave pubblica. Ogni nodo validerà la transazione eseguendo lo *script di locking*, seccessivamente eseguirà quello di *un-locking*, l'esecuzione avrà un esito positivo se lo *script di unlocking* soddisferà le condizioni dello *script di locking*, ciò produrrà il trasferimento della transazione per effettuare la spesa.

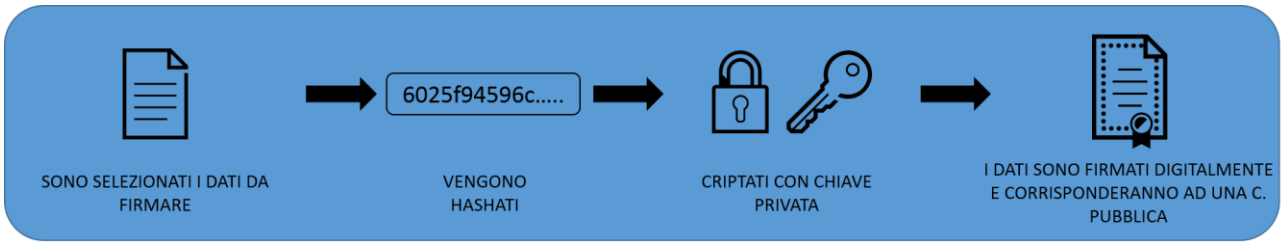
2.5. La firma digitale ed il sistema delle chiavi

Le **firme digitali,** con le quali vengono criptate le transazioni, sono degli **schemi matematici** che consistono in due parti, la prima è **l'algoritmo** per la **creazione della firma** che usa la **chiave privata** per **firmare il messaggio** e la seconda parte è l'**algoritmo** di **verifica** della **firma** che fornisce la **chiave pubblica.**

Le firme digitali ottemperano a **3 compiti:**

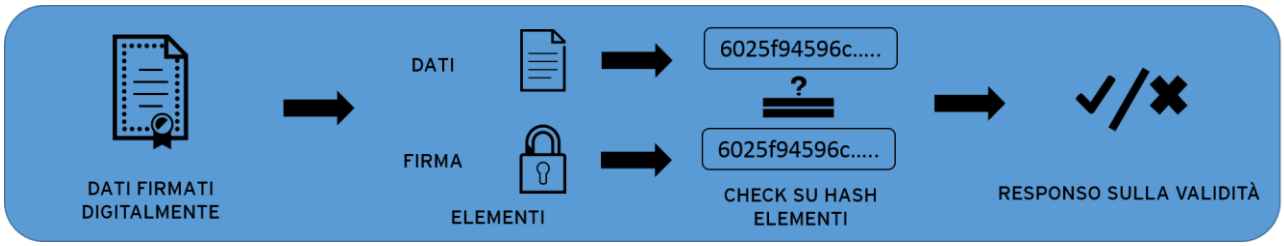
1. Forniscono la **prova** che il possessore della chiave privata è chi **possiede** i **fondi** ed è **autorizzato** a **spenderli**
2. Attestano che la **prova dell'autorizzazione** è **incontrovertibile**
3. La **firma** prova che la **transazione** non **po' essere modificata** dopo essere stata firmata

Figura 9 Processo di Firma



L'algoritmo di verifica legge il messaggio, la chiave pubblica che lo ha firmato, la firma e darà come output vero, se la **firma** è **valida** per quel determinato **messaggio** e per quella determinata **chiave pubblica**.

Figura 10 Verifica della Firma

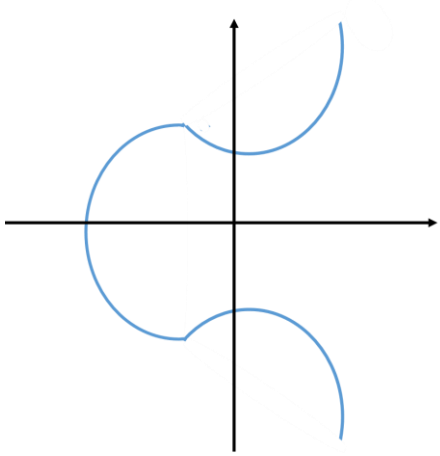


La **proprietà** del Bitcoin è stabilita tramite la ***digital keys*, l'indirizzo del Bitcoin e la firma digitale**. Le **chiavi digitali** non sono contenute dal network ma sono invece create e depositate dagli utenti un file in l**ocale o in un *wallet.***

Ogni **transazione,** per essere **inscritta** in **Blockchain,** richiede che sia **validata** tramite una **firma digitale**, essa è generata da una **chiave privata**, il cui possesso assegna il controllo e ne dimostra il possesso dei Bitcoin contenuti nella transazione.

Il sistema è basato su un **sistema asimmetrico avanzato** di chiavi, con due diversi tipi di chiavi chiamate **chiavi pubbliche e chiavi private,** a cui sono assegnati due diverse funzioni: **criptazione e decriptazione**.

Figura 11 Elliptic Curve



Esse sono collegate ad un sistema di criptografia su una **funzione matematica** (ad esempio l'*Elliptic Curve Moltiplication*[8]), essa è una funzione di **tipo *one-way*,** quindi **irreversibile**, poiché può essere calcolata facilmente solamente in un verso ed è difficilmente calcolabile nel verso opposto. La **chiave privata** è un **numero casuale,** al quale viene applicata la **funzione ellittica** per ottenere la **chiave pubblica**. Alla **chiave pubblica** vengono applicate due funzione di tipo ***hash one-way***, **prima secondo lo *SHA256*** e il suo risultato viene computato per una seconda volta **tramite il *RIPEMD160*** per ottenere **l'indirizzo Bitcoin**. Il Bitcoin address è una stringa formata da numeri e lettere

[8] È basata sulla **somma** e **moltiplicazione** dei punti su una **curva ellittica.**

ed iniziante per 1 (ad esempio: 1J7mdg5rbQyUHENYdx39WVWK7fsLpEoXZy), essa può essere condivisa con tutti per ricevere i pagamenti sul proprio *wallet,* di solito è presentata tramite un sistema basato su 58 caratteri *(Base58Check*[9]) per evitare ambiguità, proteggere dagli errori umani nell'inserimento e nella trascrizione dello stesso. Il meccanismo di creazione della chiave pubblica permette di creare firme digitali infalsificabili, in quanto la chiava privata può essere usata per firmare i messaggi e questa può essere validata per una *public key,* senza rilevare la chiave privata, essendo *one-way*. Quando vi è una transazione con i Bitcoin, il proprietario dei Bitcoin presenta la sua chiave pubblica e la firma (sempre diversa, generata tramite la chiave privata). Attraverso questi due elementi, tutti gli utenti nel network possono confermare che il soggetto trasferente possieda, al tempo del trasferimento, i Bitcoin ed accettarne il trasferimento.

La chiave privata può essere rappresentata in differenti basi, le differenti basi sono richieste dalle diverse circostanze d'uso. Ad esempio la rappresentazione esadecimale e la rappresentazione binaria sono usati all'interno nei software e la forma *WIF (Wallet Import Format)* è usata per importare ed esportare le chiavi tra i wallet.

La stringa rappresentate la chiave pubblica sarà formata da un prefisso (*WIF*) e da due serie, essendo la chiave pubblica un punto di una curva ellittica essa sarà composta da due serie rappresentanti i punti x e y.

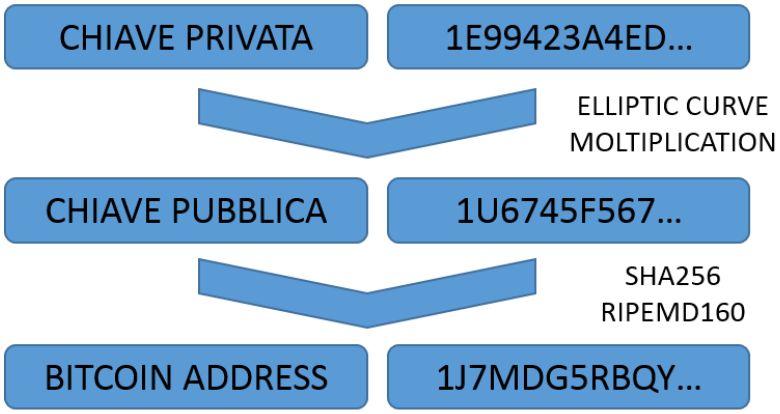
[9] Esso è un linguaggio che appartiene al gruppo dei **Base-64,** esso usa lettere maiuscole, minuscole, numeri e due simboli (" e /). I codici del tipo Base-64 forniscono una **versione compatta**, facilmente **leggibile** ma la Base 58 esclude alcuni caratteri che possono facilmente generare errori come o, 0, l e I. Per aggiungere un ulteriore **sicurezza** contro gli **errori** di battitura e di trascrizione viene usata la **versione encoded,** che comprende un **checksum**, che deriva dall'Hash dei dati codificati e che può essere **usato per prevenire ed individuare errori**. Quando viene presentato presso il software di decodifica **calcolerà il checksum** e lo **comparerà** al checksum contenuto **nel codice**, se il match avrà un responso negativo sarà indice di un dato invalido.

Per trasformare una **stringa** in una a **Base58Check** bisogna aggiungere al dato un **prefisso** (Version byte), che indica il tipo di **informazioni codificate all'interno**, la loro unione viene **computata per due volte** tramite lo SHA256. Il risultato sarà un **hash di 32 byte**, di questo verranno prese solo **4** per formare il **checksum**, che verrà **concatenato** alla **fine** della **stringa,** che dovrà essere controllata, essa sarà **composta** dai **dati**, dal **prefisso** e dal **checksum**. Il tutto sarà **codificato** secondo **l'algoritmo della base 58**.

Le **chiavi pubbliche** possono essere rappresentate in diversi formati, i principali sono due: **compresso e non compresso**. La versione **compressa** è stata introdotta per **ridurre** la **dimensione** della transazione e conservare lo spazio sul disco dei nodi. Essendo la chiave una funzione a due variabili x e y, avendo la una delle due variabili è possibile ottenere ricorsivamente la seconda variabile, ciò permette di depositare solo la coordinata x della chiave pubblica, così da avere una **riduzione del 50%** dello **spazio occupato.**

Possiamo avere due prefissi in quanto essendo **ellittica** ad una x corrisponderanno due y, con segno opposto, quindi questo **genererà due prefissi diversi.** Ciò **produrrà due differenti** Bitcoin address anche se generate dalla stessa chiave privata.

Figura 12 Processo di Creazione del Wallet Address



Per Indicare quali **parti** siano **incluse** nella **firma della chiave privata** vengono usati il *Sighash flag*, esso è formato da **un singolo *bite,*** che **viene aggiunto alla firma** ed è **univoco** per una singola firma. Il *Sighash* è applicato tramite l'imposizione di una lunghezza pari a 0 di alcuni campi, l'applicazione avviene al completamento della serializzazione e la somma delle due parti viene Hashato.

Vi sono **differenti tipi di *Sighash flag***:

1. ***All:*** la firma è applicata a **tutti** gli **input** ed a tutti gli **output**
2. ***None:*** la firma è applicata a **tutti** gli **input** e **non** agli **output**, può essere usata per creare una transazione sulla base degli assegni in bianco, dove l'input è fisso

invece lo script di output può essere cambiato permettendo così di poter cambiare il soggetto che riscatterà la somma pattuita.

3. *Single:* la firma è applicata a tutti gli input ma solo ad un output con lo stesso *index number* dell'input firmato.

Inoltre può essere aggiunto il *modifier Anyonecanpay,* che permette di firmare solo un input e lasciando il resto aperto a modifiche. Con *Sighash flag* del tipo *All* può essere applicato a transazioni sullo stile del *crowfunding,* dove le transazioni in input sono collegate ad un solo output e saranno sbloccate se la sommatoria degli input è pari alla somma target prevista. Può essere anche applicata alle transazioni di tipo *none* per creare delle transazioni che abbiano come obiettivo quello di unire gli *UXTO* di piccola dimensione.

2.6. Design Principles

La tecnologia Blockchain, per essere applicata, necessità di alcuni elementi chiave che vengono usati come ***Design Principles***[10] delle differenti soluzioni applicative. Possiamo racchiudere tra questi *design principles:*

a. ***Trust Protocol, Network Integrity and the trusted thirds party:*** La fiducia che i soggetti ripongono nel Sistema è intrinseca allo stesso, deriva dal network e dalla sua integrità. In quanto grazie all'integrità del sistema i soggetti partecipanti al network possono scambiarsi direttamente (disintermediazione) del valore senza aver bisogno di avere fiducia nel terzo e senza avere aspettative sul fatto che il soggetto stesso agisca con integrità (***Double spending Problem)***. L'integrità del network è garantita tramite l'utilizzo di un *network peer-to-peer*, del *timestamp* e della *criptografia* per creare il sistema del consenso. Il sistema impone un ***timestamp*** alla prima transazione effettuata dal soggetto con quei Bitcoin e respinge le successive transazioni effettuate dallo stesso soggetto con gli stessi Bitcoin. Grazie alla trasparenza, gli scambi sono visibili da tutti e nessuna transazione può essere nascosta, rendendo così la criptovaluta più tracciabile del denaro. Un ulteriore sicurezza è data dalla struttura del network, esso è distribuito su diversi nodi, nessun singolo membro può prenderne il controllo, in quanto non è economicamente vantaggioso, dato che l'onere per acquisirne il controllo è superiore ai possibili vantaggi scaturenti dall'acquisizione.

[10] EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

"Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world", Don Tapscott, Alex Tapscott

"Blockchain: blueprint for a new economy", Melanie Swan, 2015

b. *Distributed Power:* il potere del *consensus* è distribuito sui nodi, creando così un network senza *un single point of control*. Ciò è prodotto dal fatto che nessun singola parte può far cadere il sistema, ne l'eventuale presenza di una autorità centrale che tagli fuori uno più soggetti che possano minare l'esistenza e la sopravvivenza del network. La Blockchain è distribuita ed è mantenuta volontariamente dai nodi stessi, i quali utilizzano il loro potere computazionale per minare i diversi blocchi.
c. *Value as Incentive:* il funzionamento del Sistema si basa sull'allineamento degli interessi e sulla reputazione di tutti i stakeholder. Il sistema fornisce una ricompensa come incentivo per chi ha fornito del lavoro al network, come ad esempio i Bitcoin della *Fee* o di *reward* per il minatore che ha risolto per primo il puzzle relativo al blocco. Esso si bassa sul presupposto economico della teoria dei giochi nella quale gli attori agiscono egoisticamente rispetto ai propri interessi e sono influenzati dai incentivi esterni. Quindi corretti incentivi possono produrre modifiche del comportamento dell'agente verso le azioni volute dal sistema e ritenute opportune.
d. *Security:* il Sistema di sicurezza è integrato nel Sistema distribuito e si basa su diversi elementi:
    - Criptografia: il suo utilizzo è obbligatorio per tutti i soggetti del sistema e il suo mancato utilizzo porta all'isolamento e all'esclusione da network. All'interno del network viene utilizzata, come già detto, un sistema di chiavi che rende più sicure e protette le transazioni.
    - *No Single point of Failure, consensus e trasparenza:* la combinazione di questi elementi permette di eliminare il rischio che agenti agiscano in maniera opportunistica. Un eventuale comportamento opportunistico, grazie al sistema del consenso, sarebbe portato all'attenzione di tutto il network, data la trasparenza sulle transazioni, e non essendoci un solo singolo *point of Failure* il sistema non subirebbe danni.

- Reputazione: la trasparenza porta le azioni dei soggetti alla visibilità dell'intero network, associando gli stessi ad una identità. L'associazione di comportamenti considerati non meritevoli con una identità permette di identificare ed isolare i suddetti soggetti.

e. *Privacy and Rights Preservation:* Gli utenti hanno il diritto di proteggere le proprie informazioni e di decidere con chi, cosa e come esse siano condivise con gli altri. Il meccanismo alla base della Blockchain riconosce l'inalienabilità di questo diritto e ritiene che gli stessi debbano essere protetti, quindi grazie alla sua trasparenza, i diritti dei singoli sono individuabili, riconosciuti e rispettati. Questo diritto incontra dei bisogni prettamente di natura economica, relativi alla sicurezza negli scambi, questa necessità deriva dall'esigenza di capire se il soggetto con cui si sta effettuando la transazione sia affidabile e se ottempererà alla parte dei suoi obblighi. Grazie alla fiducia risposta nel network, le due parti non hanno il bisogno di sapere chi sia la controparte, in quanto è la rete dei nodi a garantire per loro, quindi la fiducia verso il terzo è sostituita dalla fiducia verso il network. Ulteriormente il network, non richiede elementi identificativi come nome, cognome, email o altri dati personali quindi il diritto alla privacy è rispettato. La Blockchain rende possibile effettuare le transazioni senza condividere i propri dati personali, senza perdere l'elemento di sicurezza sull'adempienza delle parti alle loro obbligazione, in quanto la prima viene sostituita da una identità digitale (Wallet a*ddress*) senza nessun elemento di collegamento con quella reale, la seconda viene supportata dalla fiducia nel network e nei suoi meccanismi.

f. *Inclusion:* il protocollo Blockchain permette di abbassare le barriere, permettendo così di aumentare la partecipazione e l'inclusione degli attori. Ad esempio allo stato attuale, ci sono circa due miliardi di persone che non possiedono un conto presso una banca e non effettuano pagamenti online. Ciò dovuto all'elevato costo dei micropagamanti dal mobile e alla mancanza della connessione internet. La Blockchain permetterebbe di effettuare i

pagamenti senza l'ausilio di internet, grazie a degli *simplified payment system (SPV)* ed a costi inferiori.

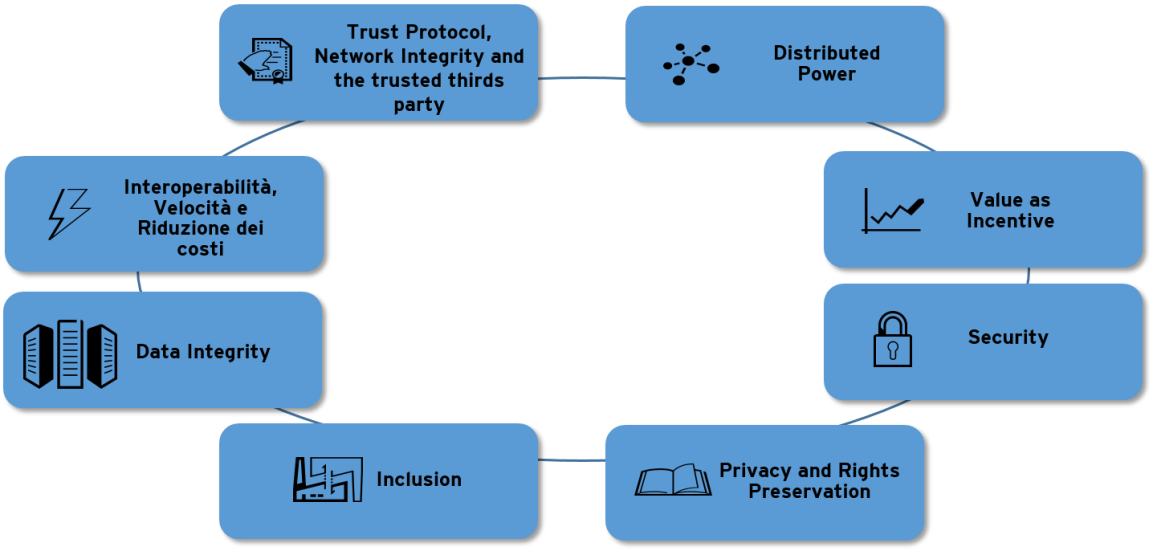
g. *Data Integrity*

- ***Honesty:*** per stabilire una relazione con i differenti stakeholder si devono fornire informazioni accurate, veritiere e complete. Non devono essere contemplate informazioni non veritiere, tramite l'omissione e né offuscamento attraverso la complessità.
- ***Consideration:*** è necessario tenere in considerazione il rispetto per gli interessi, desideri e sentimenti degli altri operando con la buona fede.
- Accountability: concerne il mostrare un chiaro commitment per gli stakeholder e per aver onorato la loro parto dell'accordo.
- Trasparency: dimostrare di aver operato senza nascondere informazioni ed azioni.
- Immutability: Un'informazione, quando è inserita nella Blockchain, non può essere modificata senza la modifica di tutti i blocchi successivi sulla maggioranza dei nodi. Per questa ragione è difficile ed antieconomico il cambiamento delle informazioni di un blocco già inserito in Blockchain, per questa ragione si possono considerare immutabili le informazioni inserite.

h. Interoperabilità, Velocità e Riduzione dei costi: il sistema Blockchain è strutturato affinché vi sia:

- Interoperabilità: l'architettura distribuita è adattabile sia ad organizzazioni e sia a sistemi disomogenei.
- Velocità: il protocollo Blockchain abilita le transazioni con un settlement e un audit prossimo al real-time.
- Riduzione dei Costi: molte volte la tecnologia Blockchain è preferibile ad una centralizzata in quanto la sua implementazione e la sua manutenzione sono più economiche.

Figura 13 Blockchain Design Principles



2.7. Blockchain Eras

Possiamo articolare l'evoluzione dell'applicazione della Blockchain in diverse ondate: Blockchain 1.0, Blockchain 2.0 e Blockchain 3.0.

2.7.1. Blockchain 1.0: Wallet & Payments

La Blockchain 1.0 è legata, nel suo primo utilizzo, ai Bitcoin ed i wallet, quindi come protocollo per effettuare e ricevere i pagamenti. Il Bitcoin è usato per contenere e trasferire valore tra i partecipanti nel network. Esso, come tutti le monete convenzionali, può essere usato per comprare e vendere beni, mandare denaro alle persone o alle organizzazioni, estendere il credito, inoltre può essere venduta, acquistata e scambiata con altre valute. A differenza della moneta normale, essa è completamente digitale, gli utenti hanno una propria chiave, che permette di provare il possesso dei Bitcoin contenuti nei wallet, che permette di firmare le transazioni, con il fine di sbloccare la criptomoneta e spendere la stessa nelle transazioni. Le chiavi sono, di solito, depositate in un portafoglio digitale (*Digital Wallet*), contenuto nel pc o nello smartphone del possessore. Vi sono differenti tipi di portafogli digitali, essi si differenziano per l'uso di specifiche piattaforme e per la difficoltà d'uso, essi possono essere divisi in:

1. *Desktop Wallet:* è stata la prima tipologia di wallet creato, esso può essere utilizzato su Pc windows e su sistemi basati MacOS. Viene scelto per l'autonomia e il controllo offerto ma ha carenze in termini di sicurezza e di configurazione.
2. *Mobile Wallet*: è il tipo di *wallet* con il maggiore utilizzo, esso può essere usato su smartphone con sistemi *Apple iOS and Android. È* caratterizzato da un design semplice e da una elevata facilità di utilizzo.
3. *Web Wallet:* sono depositati presso un server detenuto da terzi e accessibili tramite browser. Molti di loro sono basati su sistemi che operano facendo girare una parte del codice sul terminale dell'user, ciò permette di tenere il controllo delle chiavi Bitcoin.
4. *Hardware Wallet*: essi sono *wallet* contenuti in dispositive hardware, che interagiscono tramite la tecnologia *NFC e USB, con la Blockchain*. Considerando

queste caratteristiche essi sono valutati come molto sicuri ed adatti a contenere grandi somme di denaro.

5. *Paper Wallet:* in questo tipo di portafogli digitali le chiavi possono essere stampate (*cold storage*) per una conservazione di lungo termine.

Un secondo elemento caratterizzante i portafogli è il loro grado di autonomia e il loro modo di interagire con il network. Secondo questi elementi possiamo distinguere in:

1. *Full node client:* esso è un client che immagazzina l'intera storia delle transazioni di ogni utente. Inoltre esso gestisce tutti gli aspetti del protocollo ed è indipendente nel validare l'intera Blockchain e ogni transazione.
2. *Lightweight client o simple-payment-verification (SPV)*: sono dei client che devono essere connessi a dei *full node* client per accedere alle informazioni sulle transazioni, sono dei *client* ma immagazzinano il *wallet* localmente ed indipendentemente creano, validano e trasmettono le transazioni.
3. *Third-Party API client*: *third-party API* client sono dei client che interagiscono con la rete attraverso un Sistema di terze parti (API), i portafogli possono essere tenuti presso l'utente o presso la terza parte.

2.7.2. Blockchain 2.0: Smart Contracts

Un passo avanti nella tecnologia Blockchain è stato ottenuto grazie alla possibilità di inserire nella Blockchain dei contratti digitali (*Smart Contracts*) e di altri protocolli quali le *Smart property*, le applicazioni decentralizzate (***DAPP***), le organizzazioni e le società centralizzate. La Blockchain 1.0 si era caratterizzata per permettere la decentralizzazione del denaro e dei pagamenti, di contro la Blockchain 2.0, ha permesso di decentralizzare il mercato e il trasferimento di ogni tipo asset, in quanto il registro decentralizzato permette di registrare e confermare ogni tipo di contratto e di proprietà. Gli asset sottostanti possono essere di qualunque tipo, ad esempio come il registro del catasto, il registro dei veicoli, delle licenze, dei matrimoni, delle licenze, della motorizzazione, carte identità, passaporti, documenti notarili, diritti di proprietà intellettuale, contratti tra privati e assicurazioni. L'innovazione non si insinua solamente nei rapporti tra privati, ma coinvolge anche i rapporti e i documenti tra la pubblica amministrazione e il cittadino in una molteplicità di casistiche relativamente ai suoi diritti (voto, identità, possesso...) e ai documenti attestanti (patente, carta identità, certificati di nascita, di matrimonio, di proprietà immobiliare, brevetti, licenze…), sia per asset fisici e sia per asset intangibili.

La tecnologia è stata applicata proficuamente a diversi ambiti quali ad esempio:

- *Financial Services*: la Blockchain ha portato un forte miglioramento per le transazioni relative ad azioni, titoli obbligazionari, *crowfunding*, partecipazioni in fondi comuni, derivati, pensioni. Anche per i *financial services* esso funziona come ***enabler*** di funzioni e servizi come i trasferimenti P2P eliminando la necessaria intermediazioni delle *Clearing* e *settlement house.*
- *Crowfunding:* la BC ha permesso di creare una piattaforma per il ***funding peer-to-peer*** per la vendita presso una base di utenti diffusa delle *cryptographics* share delle start-up.
- *Smart Property:* una delle migliori applicazioni è da ritrovare nell'utilizzo della Blockchain come uno ***Smart register*** per le diverse tipologie di *asset*, fisici e non, ed nell'utilizzo di ***Smart Contracts*** per regolare il trasferimento e le transazioni ad essi abbiate. Ad ogni prodotto registrato è assegnata una chiave privata ed è

detenuta dal **proprietario** dell'oggetto, quindi per effettuare la **vendita** è necessario **trasferire** la suddetta **chiave** ed effettuare una **transazione** che affermi l'avvenuto **cambio di proprietà.** La coniugazione delle diverse ***Blockchain solution*** con altre tecnologie quali ad esempio ***l'Internet of Things (IoT)*** può **abilitare soluzioni** altamente **smart** quali *l'unlocking* sicuro solo a determinati soggetti verificati a cui è stato assegnato l'accesso a veicoli per il noleggio, abitazioni per l'affitto, stanze di hotel, consegna dei pacchi, storing nei locker…. Su questi elementi può essere fatto un controllo **in real time** e **paperless** ciò facilita le transazioni ed a questi possono essere collegati, tramite ***Smart Contract,*** ad ulteriori **servizi aggiuntivi** come la gestione contrattuale della garanzia in maniera automatica e dematerializzata.

Gli ***Smart Contract***[11] sono l'**oggetto informatico abilitante** l'ondata della **Blockchain 2.0**, in quanto essi **abilitano** ed **automatizzano diversi servizi.** Gli Smart Contract sono la **versione digitale**, in **linguaggio informatico** ed ad **esecuzione automatica** dei **contratti tradizionali**. I **contratti** tradizionali sono **accordi** tra una o più parti nel quale vengono **scambiate uno o più prestazioni** in cambio di denaro o di altre prestazioni. Questo schema implica la **necessità** che vi sia tra le parti la **fiducia** relativamente al fatto che l'altro soggetto **adempia** ad i suoi **obblighi contrattuali**. **Gli Smart Contract** sottendono lo **stesso schema contrattuale,** ma **non** necessitano della **fiducia,** in quanto eseguono **autonomamente** il contratto **evitando** la **discrezione** nell'interpretazione del contratto ed **auto eseguendo** le **clausole** legati ad **eventi specifici**. Il paradigma degli Smart Contract è basato su alcuni **elementi specifici:**

1. **Autonomia**: una volta scritto ed avviato, lo Smart Contract **non necessità** di **nessun'altra azione per garantire l'avvenimento delle prestazioni**, quindi **non** sarà **necessario** l'utilizzo di un **terzo** come broker, avvocati o qualunque altro intermediario.

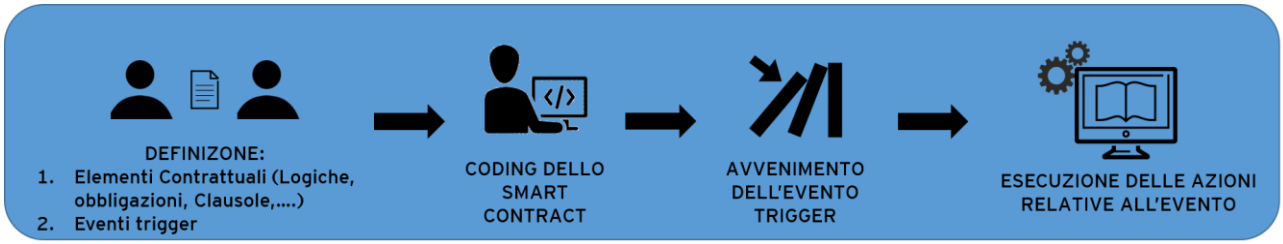
[11] First Monday, Vol 2 N 9, Nick Szabo, 1997
https://www.icbpi.it/smart-contracts-la-vera-rivoluzione-della-Blockchain/
https://blockgeeks.com/guides/smart-contracts/
http://www.Blockchaintechnologies.com/Blockchain-smart-contracts

2. **Self-sufficient:** gli Smart Contract hanno **l'abilità di reperire** le **informazioni autonomamente** per la loro **esecuzione** e la successiva **abilitazione** di determinate **azioni**.
3. **Decentralizzati:** essi **non** sono depositati presso un **server centralizzato** ma sono **distribuiti** sui nodi della **rete**.
4. **Fiducia Intrinseca:** I documenti sono **criptati**, **inseriti** nella **ledger** e **non** possono essere **persi o cancellati.**
5. **Backup**: essendo basato sulla Blockchain, i **documenti** saranno **replicati** su **ogni nodo,** quindi si avrà un copia disponibile.
6. **Sicurezza**: la **criptografia** della Blockchain rende sicuri tutti gli elementi dello Smart Contract.
7. **Velocità**: grazie all'utilizzo dei software, molti **processi sono resi automatici** e **paperless**, **riducendo** così i **tempi** di **esecuzione**.
8. **Risparmio**: gli *Smart Contract,* **sostituendo il terzo intermediario,** permettono di **risparmiare** sui **costi** ad esso legato come ad esempio i costi per la notarizzazione.
9. **Accuratezza**: grazie agli **automatismi,** è possibile **evitare errori** dovuti alla lavorazione manuale dei dati e all'errore umano.

Analizzando la **struttura** dello ***Smart Contract*** si possono individuare **tre parti principali:**

1. **Descrizione della logica contrattuale** in un linguaggio di programmazione compatibile con il sistema;
2. **Il mapping degli eventi** che funzionano da **trigger** per la logica contrattuale
3. Un **meccanismo** che **abiliti le conseguenze** previste dalla **logica contrattuale** in base ai differenti **eventi.**

Figura 14 Funzionamento di uno Smart Contract



Il protocollo Bitcoin non è adatto all'implementazione dei servizi della Blockchain 2.0, per questa ragione sono state sviluppate diverse piattaforme abilitanti tra queste vi è la piattaforma Ethereum.

Ethereum[12] è una piattaforma basata sulla Blockchain e su un protocollo aperto, sopra la quale è possibile costruire ed usare applicazioni decentralizzate (*DAPP*), basate sulla tecnologia Blockchain. *Ethereum* è il primo computer virtuale decentralizzato del mondo, dato che non risiede in alcun luogo fisico ma nella rete, essendo composto da diversi computer in diverse parti del mondo. A differenza del protocollo Bitcoin, *Ethereum* è stata disegnato come una piattaforma non rigida, adattabile e flessibile alle esigenze del suo sviluppatore, ciò porta ad una grande facilità nell'implementazione di nuove applicazioni che utilizzano la piattaforma. Per questa ragione essa è una piattaforma programmabile, non dà all'utente un set predefinito e finito di operazioni, ma permette ai sui utenti di creare applicazioni e software personalizzati. Il cuore della piattaforma è *l'Ethereum Virtual Machine (EVM).* Essa esegue i codici degli algoritmi e permette agli sviluppatori di creare e di far girare su di essa programmi in linguaggi compatibili come *JavaScript e Python*. Date queste sue caratteristiche, *Ethereum* è più adatta di altre piattaforme ad alcuni tipi di software, in quanto automatizza le interazioni dirette tra i loro pari, è di facile implementazione, permette la coordinazione delle azioni di gruppo all'interno di un network come la costituzione dei *Marketplace* ed automatizza complessi contratti finanziari. A differenza del Bitcoin, che è abilita lo scambio di denaro senza bisogno di un'intermediazione di un terzo fidato ed indipendente come banche, governo e istituiti finanziari, *Ethereum* ha un impatto maggiore, in quanto può eseguire interazioni o scambi di ogni complessità ed avente come sottostante qualunque tipo di elemento.

L'esistenza di un consenso decentralizzato dà ad *Ethereum* un alto livello di tolleranza degli errori, assicurando *zero down time* e fa sì che i dati contenuti nella Blockchain siano resistenti alla censura e a possibili modifiche. L'unità base di *Ethereum* è *l'Ether*, mentre il registro traccia lo stato di ogni account e tutti gli stati delle transazioni.

Ci sono due tipi di account:

[12] http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

1. *Externally Owned Accounts (EOAs)* che sono controllati da chiavi private, quindi richiedono un intervento umano che usi la chiave per averne il controllo.
2. Contract Accounts, che sono controllati dal protocollo degli *Smart Contract*

Come per i Bitcoin, le transazioni richiedono il pagamento di una *fee* per incentivare il network (oltre alla ricompensa ricevuta per il *mining* di un nuovo blocco), per far sì che il sistema sia sicuro. Essa viene pagata in ogni step dal soggetto che effettua la transazione tramite ether. Le *fee* sono raccolte dai nodi che validano le transazioni. Nel modello *Ethereum*, così come in quello Bitcoin, i minatori sono quei soggetti che ricevono, propagano, verificano ed eseguono le transazioni.

Anche *Ethereum* si basa oggi sul sistema del *Proof-of-Work*, ma sin dalla sua creazione si è stabilito che vi sarà una migrazione al *cosiddetto Proof-of-Stake*[13] per risolvere i problemi legati al consumo di energia del primo. Il *Proof-of-Stake* permette di *prevenire il double spending* creando un *nuovo* tipo di *consensus* basato non sulla potenza di calcolo, ma sull'ammontare di "*stake*", cioè di *Ether* detenuto (*Store Value*). In questo modo un attacker dovrebbe avere la maggioranza degli ether ed esso soffrirebbe più di tutti da una perdita di valore del sistema dovuta ad una perdita legata alla mancata sicurezza. Un'ulteriore differenza con la tecnologia Bitcoin-Blockchain è relativa alla grandezza del blocco, attualmente ha un limite pari ad un 1 mb nel sistema Bitcoin, mentre in *Ethereum* non vi è una dimensione limite fissa dei blocchi, ma questa si aggiusta dinamicamente. Il tempo tra un blocco e l'altro è di circa 16 secondi, contro i 10 minuti di *Bitcoin*.

[13] Nel mondo Blockchain sono **previste ulteriori modalità di consenso:**

1. **Proof-of-Activity**: essa **combina** il **proof-of-stake e il proof-of-work** tramite il **sorteggio** di un numero di **miners** che dovranno **firmare il blocco** con una criptokey per far diventare il blocco valido
2. **Proof-of-Capacity**: per **verificare** il blocco viene richiesto ai **minatori di riservare una definita** parte dei loro **hard drive.**
3. **Proof-of-Storage**: per la verifica è **richiesto** ai minatori di **riservare e condividere** in un **cloud distribuito** parte dei loro **hard disk.**

2.7.3. Blockchain 3.0[14]: Cross-Industries Revolution

Nella *Wave 3.0* la Blockchain si propaga dall'ambito dei *financial services* verso tutte le *industry* portando la possibilità di re-configurare servizi e gli standard negli stessi. La Blockchain si presenta come un nuovo paradigma organizzativo *cross-industry,* portatore di una maggiore efficienza e scalabilità, che vede le varie interazioni come transazioni, economiche e non, con un valore e diversi attributi, che possano essere iscritti nella *distributed ledger*.

Qui di seguito sono analizzate i più importanti *Use Case* della tecnologia Blockchain nelle diverse *industry*.

Nell'ambito della Pubblica Amministrazione sono riscontrabili differenti casi si applicazione: il catasto digitale in Svezia, la creazione di una *digital Identity* e della *e-residency* in Estonia.

La *Lantmäteriet* (Ente Pubblico che gestisce il catasto svedese) ha riscontrato diversi *pain point* nel suo attuale sistema di gestione, come ad esempio il grande lasso di tempo che intercorre tra la firma della vendita e il trasferimento della proprietà (tra i 3 e i 6 mesi), la mancanza, nella maggior parte del processo, di trasparenza. Inoltre questo sistema spinge i diversi attori del processo (venditore, acquirente, banche e agenti immobiliari),

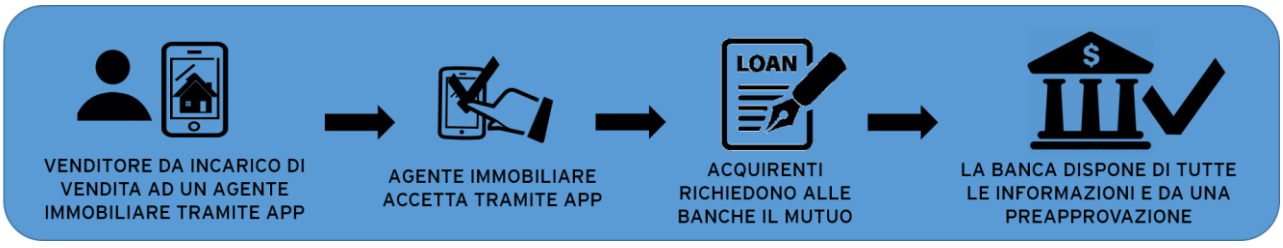
[14] Fonte:
http://www.coindesk.com/sweden-moves-next-stage-Blockchain-land-registry/
http://www.coindesk.com/sweden-taking-chance-Blockchain-land-registry/
https://qz.com/947064/sweden-is-turning-a-Blockchain-powered-land-registry-into-a-reality/
http://www.financemagnates.com/cryptocurrency/innovation/sweden-tests-property-transactions-Blockchain-chromaway/
https://chromaway.com/landregistry/
The Land Registry in the Blockchain – testbed :A development project, Lantmäteriet, Landshypotek Bank, SBAB, Telia company, ChromaWay and Kairos Future
https://e-estonia.com/component/electronic-id-card/
http://e-resident.gov.ee/become-an-e-resident/
http://www.wired.co.uk/article/estonia-e-resident
https://blogs.thomsonreuters.com/answerson/e-estonia-power-potential-digital-identity/

alla creazione di **complessi processi** per la stesura dei contratti per evitare che vi siano delle perdite, dato l'elevato valore dei beni (il valore delle proprietà in Svezia è circa il triplo del PIL della stessa e rappresenta per gli svedesi il più importante asset). Per queste ragioni il **governo Svedese,** insieme alla Startup ***ChromaWay,*** ha progettato una soluzione per la **digitalizzazione** in **Blockchain** di **tutto il processo** ***end-to-end*** per l'acquisto e la vendita delle abitazioni.

Figura 15 Use Case: Catasto Svedese - Pain Point e Attori

La soluzione permette al **venditore,** tramite una semplice **app,** di verificare la **proprietà**, i **diritti/ipoteche** sull'abitazione e dare il **mandato di vendita** ad un agente immobiliare. L'agente, se accetterà l'incarico **metterà** in **vendita** l'abitazione, potendo vedere e verificare tutte le informazioni sull'abitazione tramite app con aggiornamento in *real-time*.

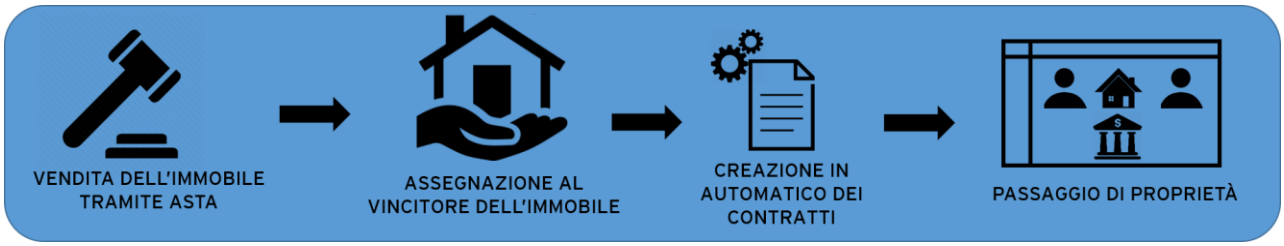
Figura 16 Use Case Catasto Svedese – Soluzione I



Una volta richiesta la vendita, la proprietà viene **messa all'asta** e viene **assegnata al soggetto** che ha offerto la **somma più alta**. L'acquirente può **richiedere digitalmente** un **mutuo** ad una banca che potrà accettare/rifiutare in base alle **informazioni contenute in Blockchain,** relativamente al ***rating*** del soggetto e allo **storico di informazioni** sullo stesso. Inoltre la Banca per erogare l'eventuale prestito, potrà **verificare il prezzo offerto** per la casa, grazie alle **informazioni condivise,** la cui **veridicità** è **garantita** dalla **Blockchain**. Il possibile **acquirente** potrà avere dalla banca una **approvazione preliminare,** che sarà una garanzia del pagamento per il venditore. Una volta decretato il vincitore, i **contratti di**

vendita, di mutuo e le relative firme e registrazione potranno essere fatte sempre tramite app, che permetterà di approvvigionare automaticamente tutte le informazioni necessarie e di scrivere in Blockchain le informazioni generate.

Figura 17 Use Case Catasto Svedese – Soluzione II



Il secondo use case analizzato è relativo alla *e-identity* e alla *e-residency* estone. L'Estonia ha creato il primo Sistema al mondo di Carta d'identità digitale smart a cui sono stati associati diversi servizi tra I quali:

1. Carta d'identità valida per viaggiare in Europa;
2. Tessera Sanitaria Nazionale;
3. Prova identificativa per l'accesso online ai conti bancari;
4. Tessera per il trasporto pubblico;
5. Firma digitale;
6. Abilità il riconoscimento per voto in formato digitale (*e-Voting*);
7. Accesso ai Database pubblici relativi a dati sanitari, fiscali, ….
8. Richiesta e produzione delle prescrizioni sanitarie (*e-Prescription*).

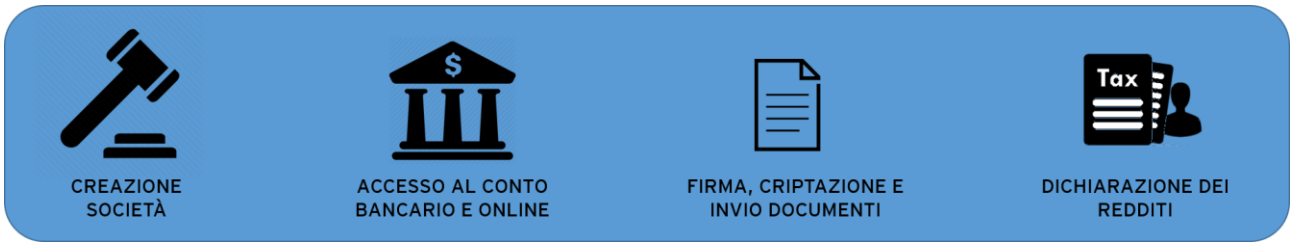
I servizi sono abilitati grazie alla Blockchain, che cripta, stora e rende accessibili i servizi e le informazioni solo ai soggetti abilitati.

Figura 18 Use Case e-Identity Estone

L'e-residency abilita differenti servizi ad imprenditori, estoni e non, che vogliono costituire o gestire un'azienda. I principali servizi abilitati sono:

1. **Creazione di una società** completamente **online,** da ogni parte del mondo, collegando la stessa ad un **conto bancario** per predisporre **online i pagamenti.**
2. **Gestione in remoto dell'azienda**, grazie alla **firma**, alla **autenticazione online**, alla **criptazione** e **all'invio** sicuro di **documenti nativi digitali** e alla **dichiarazione online dei redditi** per il calcolo delle tasse.

Figura 19 Use Case e - Residency Estone



Un ulteriore campo di applicazione della tecnologia Blockchain è relativo al ***tracking*** della ***supplychain*** e alla **notarizzazione** delle **informazioni** relative a **prodotti ad alto valore** come **opere d'arte**[15]**, gioielli**[16]**, titoli di studio** e **capi d'alta moda**[17] oppure per **prodotti** che necessitano di **verifiche** ed **attestazioni** relativamente a **tecniche di lavorazione**, **provenienza**, **stato e condizioni** di conservazione (temperatura, umidità, …) come **alimenti**[18] (carne, pesce, …) o **bevande** (Vino[19], liquori, …). Questi ambiti sono caratterizzati da **una elevata perdita** di **informazioni**, di **ricavi** e di **opportunità** lungo il processo che potrebbero **essere valorizzate** nella **proposal** verso il **cliente** (assicurazione

[15] http://www.coindesk.com/deloitte-creates-Blockchain-proof-of-concept-for-tracing-artworks/
http://www.the-Blockchain.com/2016/05/18/deloitte-rolls-Blockchain-proof-concept-art-world/

[16] http://www.wired.co.uk/article/Blockchain-conflict-diamonds-everledger

[17] http://www.Blockchain4innovation.it/iot/la-rivoluzione-nel-fashion-passa-per-la-Blockchain/
http://www.thefashionlaw.com/home/what-is-Blockchain-and-what-does-it-have-to-do-with-fashion
http://www.managingip.com/Article/3667444/Blockchain-IP-and-the-fashion-industry.html

[18] https://www.nytimes.com/2017/03/04/business/dealbook/Blockchain-ibm-Bitcoin.html?_r=0
https://www.provenance.org/whitepaper

[19] http://www.ansa.it/canale_terraegusto/notizie/vino/2017/04/13/vino-arriva-etichetta-intelligente-wine-Blockchain-ey_763092ee-10d6-4155-917d-4e4e06d5de87.html
http://www.lastampa.it/2017/04/17/tecnologia/idee/lidea-di-una-startup-italiana-usare-la-Blockchain-per-tracciare-la-filiera-del-vino-QIhzYu11J5A6kZlG6gUxTP/pagina.html

della qualità, dell'eticità e dell'originalità del prodotto) oppure per ottimizzare i processi interni (raccolta e analisi in maniera sicura e immodificabile dei dati di tutto il processo).

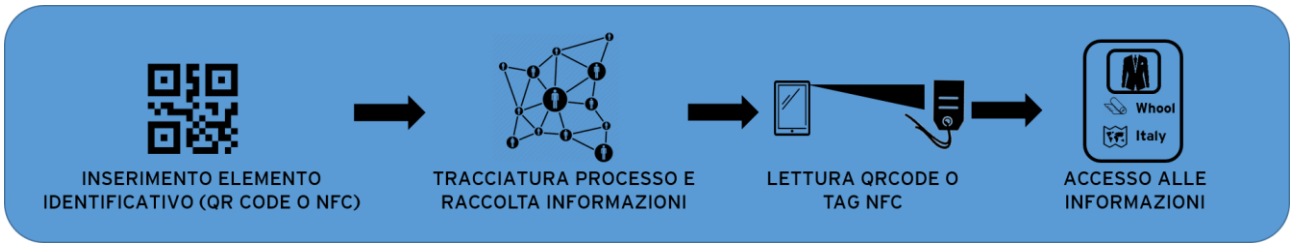
La Blockchain, nel caso del vino[20], permette di tracciare, passaggio per passaggio, l'intera filiera dalla coltivazione dell'uva, alla produzione e fino alla distribuzione del vino. La Blockchain opera come un registro immutabile, che permette di raccogliere i dati, di renderli disponibili al pubblico, in modo tale da azzerare il rischio di contraffazione sia per il produttore e sia per il consumatore. Grazie al *tracking* sarà possibile assicurare il reale possesso delle certificazioni di denominazione, quali DOC, DOP, DOCG e Bio. Le informazioni sono disponibili per ogni singola bottiglia e sono facilmente accessibili dal cliente, tramite un *QrCode* stampato sull'etichetta della bottiglia. Tramite lo scansionamento mediante smartphone della etichetta smart, sarà possibile accedere ad un carta d'identità del vino stesso, contenente informazioni sul produttore, sui vigneti, sulla provenienza, sui processi di coltivazione e trasformazione.

Nei prossimi anni nel settore della moda diverrà uno standard diffuso l'utilizzo della Blockchain essa permetterà al consumatore di poter verificare l'originalità del capo, dei materiali con cui è stato prodotto, del luogo di produzione ed eventuali certificazioni (ed esempio OEKO TEX), semplicemente scansionando il *QrCode* presente sul capo o sulla etichetta dello stesso oppure avvicinando il telefono al capo per poter accedere ad alla informazioni contenute nei *smart tag* basati su tecnologia *NFC*.

In questi ambiti la Blockchain potrà portare una ondata di trasparenza, permettendo così al consumatore di fare acquisti in maniera consapevole, attraverso azioni semplici quali lo scansionamento di *Qrcode* o la lettura di oggetti *NFC*, tutte effettuabili tramite comuni app per qualunque smartphone. Per i produttori porterà un vantaggio in termini di *Brand Protection*, di *Client Loyalty* e di lotta alla contraffazione del loro prodotto, esigenze molto sentita nel mondo della moda e dei prodotti ad origine controllata.

[20] EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

Figura 20 Use Case Tracking Supplychain



In un **mondo del lavoro** altamente **competitivo,** l'aver frequentato una **università di rilievo,** con eccellenti risultati sono diventati dei **elementi necessari** per poter **competere al meglio**. Per questa ragione si riscontrano sempre di più **informazioni non veritiere nei CV degli applicant**, circa il 56%[21] dei CV contiene informazioni false sul candidato e molte delle volte esse sono relative all'area **dell'education universitaria e alle prime esperienze lavorative**. Negli ultimi anni sono entrati nella cronaca **casi di rettori o CEO di grandi multinazionali** che si sono **dimessi** a seguito di **scandali legati a informazioni errate inserite nei CV**, come ad esempio il caso di Marilee Jones[22](Dean di MIT), di Valeria Fedeli[23] (attuale Ministro dell'istruzione) o di Scott Thompson[24](CEO di Yahoo). Ciò rende evidente la necessità di una **maggiore sicurezza, verificabilità e trasparenza** riguardo a queste **informazioni**. La **Blockchain** può soddisfare queste necessità, grazie alla sua **immodificabilità e trasparenza**. Diverse istituzioni scolastiche stanno proseguendo in questa direzione, come **l'MIT, l'Hoberton School e l'University of Nicosia** stanno testando soluzioni Blockchain che permettano la **certificazione e la notarizzazione delle informazioni**. La Blockchain può **hashare** ed inscrivere in **blocchi le informazioni** provenienti da **enti certificati**, quali **Università**, **entità Formative** (IELTS, TOEFL, …) ed **aziende** (posizione lavorativa, periodo,…). Tutte queste informazioni sono legate per creare **una identità certificata online**, una sorta di **"CV Sicuro"**[25]. L'inscrizione in

[21] http://www.statisticbrain.com/resume-falsification-statistics/

[22] http://www.nytimes.com/2007/04/27/us/27mit.html

[23] http://www.ilgiornale.it/news/politica/laurea-falsa-fedeli-si-auto-assolve-e-accusa-contro-me-1342771.html

[24] http://money.cnn.com/2012/05/13/technology/yahoo-ceo-out/index.htm

[25] EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

Blockchain genera un **codice univoco** per ogni **singola informazione o per la totalità**, il suo inserimento nel **front-end web** permette di **mostrare all'utilizzatore le informazioni volute** dal candidato in **maniera sicura** sia per il **candidato**, in quanto le informazioni **sono visibili solamente a chi è in possesso del codice**, sia per **l'utilizzatore**, che **accederà** solamente ad **informazioni veritiere**. L'applicazione a livello diffuso presso **aziende, università ed enti formatori** potrebbe portare ad una **maggiore sicurezza** ed ad una **migliore veicolabilità delle informazioni**.

Figura 21 Certificazione delle Esperienze Formative e Professionali

Nell'ambito dei **servizi bancari ed assicurativi**[26], già da qualche anno si sono **sviluppate diverse soluzioni** in ambito **Blockchain**. Il nascere di una moltitudine di soluzioni in questo ambito è dovuto al **proliferare degli investimenti dei *big player*** del **settore**. Uno dei maggiori player è il consorzio **R3**[27], formato dai **70 gruppi bancari tra i più grandi al mondo** tra cui ***Barclays, Credit Suisse, Goldman Sachs, J.P. Morgan, Royal Bank of Scotland, UBS,***

[26] European Banking Authority, "EBA Opinion on 'virtual currencies'", European Banking Authority Opinion, 4th July 2014.

Britto A. et al., "The Ripple Protocol Consensus Algorithm", whitepaper, Ripple Labs Inc, 2014.

Yoon S. Park, "The Inefficiencies of Cross-Border Payments: How Current Forces are Shaping the Future", VISA, 2008.

Barry C. et al, "Cross-Border Payments: Challenges and Trends", AITE Group report, January 2015

Knieff B., "Blockchain: What Is It Good for? Absolutely Something", Aite Group report, December 2015, p. 13.

Wright A., De Filippi P., "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," 2015

[27] https://en.wikipedia.org/wiki/R3_(company)

http://fortune.com/2016/11/21/goldman-sachs-r3-Blockchain-consortium/

Bank of America, Citi, Commerzbank, Deutsche Bank, Morgan Stanley e Unicredit. Il consorzio R3 ha investito diverse centinaia di milioni per sviluppare e testare la loro piattaforma *Blockchain,* con il fine di rendere possibile l'applicazione della stessa al mondo della finanza a livello mondiale. Possiamo evidenziare alcune motivazioni che mostrino i possibili profondi cambiamenti nel settore:

1. Attestazione: la Blockchain permette di effettuare transazioni tra due soggetti tra loro sconosciuti, senza il bisogno che vi sia fiducia nel soggetto con cui si effettuerà lo scambio. Inoltre la Blockchain può stabilire all'occorrenza la fiducia tramite l'analisi delle passate transazioni.
2. Costo: l'utilizzo della Blockchain permette di eliminare elevati costi di *back-office* senza dover cambiare il modello di business sottostante.
3. Velocità: attualmente le tempistiche per completare la transazione e la trasmissione richiedono differenti giorni (Rimesse da 3 a 7 giorni, trasferimento di azioni dai 2 e i 3 giorni ed i mutui circa 30 giorni) di contro ai circa 10 minuti della necessari alla Blockchain per effettuare la stessa operazione.
4. Value Innovation: la Blockchain è una piattaforma open source sulla quale è possibile implementare facilmente soluzioni personalizzate.

Le aree che hanno subito e subiranno il maggiore impatto innovativo sono quelle legate al *retail banking* ed ai pagamenti, specialmente nelle rimesse internazionali e nei pagamenti *P2P* dove negli anni precedenti sono già stati offerti servizi similari, ma a costi elevati, grazie alla tecnologia Blockchain, invece è e sarà possibile offrirli a costi contenuti o talvolta anche con formule che permettano l'uso gratuito degli stessi (ad esempio in bundle con servizi a pagamento), anche ad un pubblico non bancarizzato. Le principali funzioni svolte dalla Blockchain in questo ambito sono:

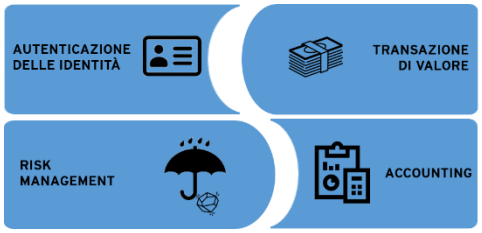
1. Autenticazione delle identità: la Blockchain permette di gestire ed autenticare in modo univoco, con un elevato livello di sicurezza le identità dei soggetti grazie ai protocolli criptografici, elemento base per l'accesso al *mobile e all'home banking*, quindi di vitale importanza per il mondo bancario.
2. Transitare, depositare e prestare del valore: la Blockchain permette di transitare e storare valore, asset e denaro, in modo sicuro, in breve periodi ed a costi

contenuti. Inoltre grazie alla **trasparenza** del sistema e **all'identificazione** sicura dell'account la Blockchain funziona da ***rating system*** per le transazioni *ed i lending.*

3. **Risk Management:** permette di mitigare **diverse forme di rischio**, quali il *settlement risk, la counterparty risk ed il systemic risk.*

4. **Contabilizzare il valore**: l'*accounting* attuale **non** sostiene l'attuale **velocità** richiesta delle **transazioni** e della finanza, ma grazie **a nuovi metodi di contabilità**, revisione e *financial reporting* mediante **Blockchain** si potranno ottenere un accounting in ***real-time*** permettendo di ottimizzare gli *screening dei regulators*.

Figura 22 Principali Funzioni in Ambito Finanziario



Le solution in Blockchain permettono di **effettuare *settlement* in *real time* per tutte le fasi** (Conferma della disponibilità dei fondi, Assicurazione che il pagamento verrà effettuato e pagamento), in maniera **automatica** e a **costi ridotti**. I **principali use case** riscontrabili sono:

1. **Rimesse e pagamenti internazionale**
2. Pagamenti ***P2P***
3. **Micropagamenti**
4. ***IoT* Payments**
5. **Firma** dei **documenti** bancari

Allo stato attuale, **non vi è un Sistema di pagamento globale interbancario**, ma solo a livello **nazionale**, quindi per la maggioranza dei pagamenti internazionali sono utilizzate le reti bancarie estere della banca stessa, le quali sono basate su accordi multilaterali tra le differenti istituzioni finanziarie. Quindi in realtà **non vi è** effettivamente un **trasferimento di denaro** tra le **diverse nazioni** ma solamente **tra le differenti banche** nella nazione di provenienza del denaro e poi un settlement contabile al loro interno. Questo

modello di pagamento è stato creato quasi quarant'anni fa, in quel periodo la transazioni internazionali erano molto meno frequenti e tra pochi player. Inoltre questo modello è caratterizzato da ulteriori problemi come:

1. Tempistiche: questo modello indiretto richiede almeno due giorni ed inoltre possono emergere problemi che ritardino ulteriormente le tempistiche.
2. Costi: si possono considerare due ordini di costi, quelli diretti che sono di competenza del cliente come ad esempio le *transaction fee* della banca che manda i fondi e di quella che li riceve ed invece costi indiretti derivanti dal mancato uso dei fondi che devono essere depositati presso la banca ricevente a garanzia del pagamento che sono a carico della banca che effettuerà il pagamento.
3. *Tracking* dei progressi del pagamento
4. *Standardizzazione* a livello internazionale del processo di pagamento per rendere compatibili i differenti schemi bancari.
5. Automazione delle attività interne alla banca per permettere di erogare un servizio più efficiente.

La regolamentazione Bancaria, specialmente quella relativa al *Know Your Customer (KYC)* e quella relativa all'antiriciclaggio (*AML*), spingono ad evolvere l'attuale modello, in quanto richiedono ulteriori costose *due diligence*.

In questo campo, si stanno affacciando dei *player* dai settori non bancari, i quali stanno offrendo dei servizi ad *alto livello di disruptive, come* ad esempio pagamenti basati su una struttura diffusa come la Blockchain specialmente nell'ambito dei pagamenti *P2P*. Un esempio è la piattaforma distribuita di pagamento *Ripple,* che permette, attraverso un sistema decentralizzato, di effettuare pagamenti diretti tra le banche, in *real time,* in ogni valuta ed ottimizzando la fee al valore minimo grazie al loro algoritmo che sceglie "la via" migliore.

Un ulteriore caso applicativo, può essere legato ai prodotti finanziari utilizzati in ambito commerciale, come ad esempio prestiti, emissioni di lettere di credito e factoring. La Blockchain può mitigare i rischi legati al commercio, anche con una moltitudine di attori. Ad esempio, considerando un wallet detenuto diversi attori, il cui contenuto si sbloccherà in automatico solo quando tutte le condizioni poste da tutti gli attori saranno state

soddisfatte, ciò limiterà molti i rischi delle parti come ad esempio il rischio di controparte o di liquidità. Ciò permetterà, in caso di mancato soddisfacimento dell'obbligazione del terzo nostro cliente, di non dover soddisfare la nostra obbligazione nei confronti del fornitore. Sarà possibile in quanto la prestazione del nostro eventuale creditore avverrà solo se la seconda obbligazione verrà soddisfatta. Ciò è possibile fornendo diversi accessi e diverse chiavi ai differenti attori, legate da uno Smart Contract, nel quale ad esempio, vi è il Soggetto 1 (Banca) che transiterà una somma X al soggetto 2 (Produttore Manifatturiero), solo se il soggetto 3 (Cliente) soddisferà le condizioni del soggetto 2 (Effettuazione di un ordine a fronte del quale il produttore necessiterà della somma X per acquistare macchinari e materie prime). Il soggetto 1 transiterà la somma X nel wallet ed essa non verrà trasferita finché le chiavi dei soggetti 2 e 3 non sbloccheranno la transazione al verificarsi delle condizioni.

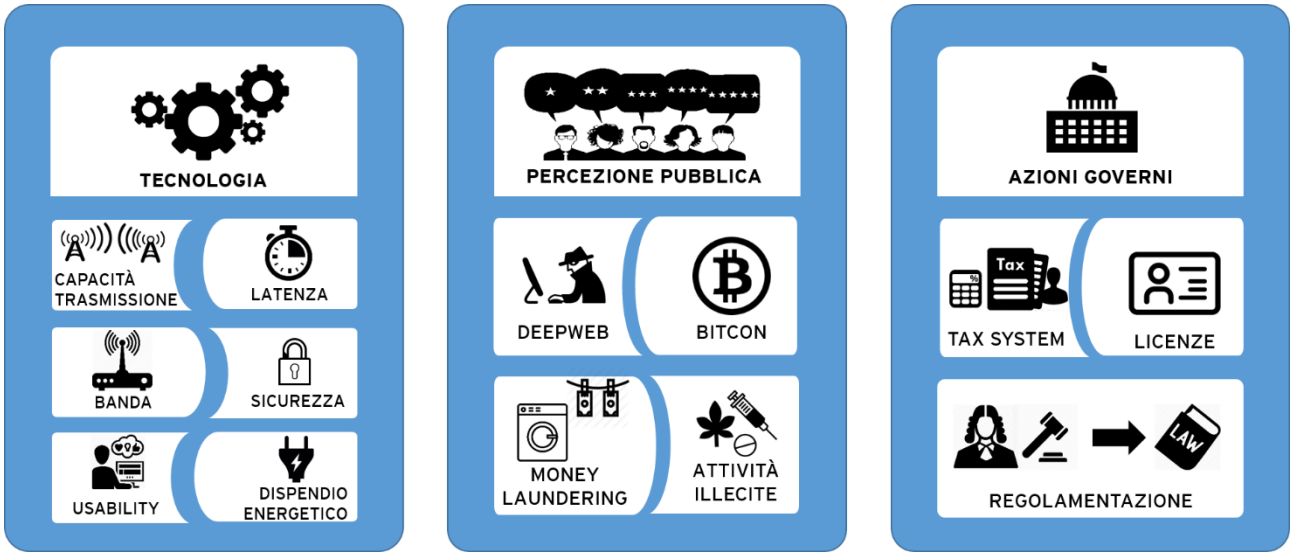
Un esempio applicativo è dato dal NASDAQ, che sta utilizzando la Blockchain per migliorare gli scambi *Over The Counter (OTC).* La situazione attuale è caratterizzata da una moltitudine di soggetti che intermediano la transazione, aumentandone così il costo ed il tempo necessario affinché venga completata, in quanto ogni intermediario vorrà un suo compenso e dovrà aggiornare i propri sistemi e registri affinché la transazione venga processata. Secondo un report della società di consulenza *Oliver Wyman* questo procedimento richiede a livello globale un *effort* pari a circa 65 – 80 Miliardi ogni anno. La tecnologia Blockchain può ridurre il lasso di tempo da qualche giorno a qualche minuto, potrebbe ridurre i costi, i rischi di controparte e di frode. Il trasferimento dell'asset potrebbe essere associato ad una transazione, visibile da tutti sulla Blockchain, ma allo stesso tempo criptata per proteggere le informazioni sensibili, disponibile e replicata su ogni nodo, richiedendo così circa solamente 10 minuti contro ai 2/3 giorni canonici per essere transata.

La Blockchain potrebbe essere usata per creare una piattaforma abilitante il voto degli azionisti. Spesso il corporate voting è caratterizzato da liste inesatte, una incompleta distribuzione dei voti e da un caotica tabulazione dei voti stessi. Grazie alla Blockchain, le elezioni avverrebbero tramite l'assegnazione dei diritti di voto mediante Token in Blockchain, grazie ai quali verrà espressa la preferenza. Ciò porterebbe ad sistema di

voting più trasparente, accurato, veloce e sicuro, variabili che possono spingere la partecipazione dei shareholder alla governance aziendale e la possibilità di poter proporre un voting più frequente.

2.8. Limiti del modello delle Blockchain

Figura 23 Limiti del Modello Blockchain



Il **protocollo Blockchain** allo stato attuale mostra alcuni **limiti tecnologici, legislativi e culturali** che potrebbero **rallentare o negare** la sua **applicazione a livello diffuso** e **globale**.

1. **Sfide tecnologiche:** l'implementazione e l'applicazione della tecnologia Blockchain porta con se diverse **problematiche tecnologiche** quali:
    i. **Capacità di trasmissione:** le infrastrutture attuali permettono di processare in media **una transazione al secondo,** con un massimo teorico di sette al secondo, ma questo limite può essere **aumentato modulando la grandezza del blocco**. Comparando la capacità di trasmissione della Blockchain con gli altri sistemi di pagamento, ad esempio **Visa,** che può **transare** in media circa **2.000 transazioni al secondo,** con picchi di circa 10.000 al secondo, si può notare **l'elevata differenza tra le due capacità di trasmissione.**
    ii. **Latenza:** il tempo di **conferma/*mining*** del blocco è di circa **10 minuti,** elevato rispetto ai comuni sistemi di pagamento come **Visa, che richiede solo qualche secondo per confermare la transazione.**

iii. **Dimensione e larghezza della banda:** attualmente la Blockchain ha una **dimensione** pari **a 25 GB,** nell'ultimo anno è aumentata di circa 14 GB, le sue considerevoli dimensioni **rendono complesso** il suo **download**.

iv. **Sicurezza**: ci sono due **possibili problemi legati alla sicurezza**:

    1. La **possibilità**, seppur remota dato dalla sua anti-economicità, che un **soggetto acquisisca** il **50%+1** dei nodi.
    2. ***L'elliptic curve Cryptography system*** potrebbe essere ***de-criptata*** nei prossimi anni, ma ciò è facilmente risolvibile **scegliendo un diverso sistema di criptazione.**

v. **Dispendio energetico relativo al *mining***: il processo di *mining* di un blocco richiede un **elevato dispendio di energie**, ciò produce anche un **costo** per il **sistema**, che **accentua** delle **distorsioni**, in quanto entrando in una logica di **massimizzazione del profitto,** i miners daranno **priorità** alle **transazioni** con la **fee maggiore**, così facendo, transazioni con **fee inferiore,** verranno inserite **successivamente** nella rete o **non verranno mai inserite,** se il **costo** del *mining* è **inferiore alla fee**. **Sostituendo** il ***proof-of-work*** con un **diverso sistema di verifica,** ad esempio come il ***proof-of-stake,*** è possibile **tagliare i costi** per la verifica e per la creazione del blocco. Questa criticità è tipica delle **reti pubbliche,** dove sono necessari degli **incentivi** per i ***miners,*** affinché minino il blocco, ciò **non** è presente invece nelle **altre tipologie di rete,** in quanto i miners (l'azienda o le aziende che hanno creato la *ledger*) si ***auto-incentivano*** a minare.

vi. ***Usability***: l'attuale versione delle ***API*** utilizzate con la Blockchain, **non** sono totalmente ottimizzate per una ***esperienza userfriendly***, ciò **limita l'applicazione** delle stessa tecnologia ad un contesto di massa, caratterizzato da un variegato panorama con soggetti a differente tasso di alfabetizzazione tecnologica e informatica. L'utilizzo delle ***REST API***, basata sul protocollo *REST (REpresentational State Transfer*), che necessita per il suo funzionamento di una **minore larghezza della banda**

di trasmissione/ricezione, rendendo così le *API* più agevoli nell'utilizzo, potrebbe portare ad un forte miglioramento.

2. Percezione Pubblica: l'immaginario pubblico lega l'idea della Blockchain ai Bitcoin, quindi agli scambi sul ***deepweb,*** al relativo al riciclaggio di denaro, a scandali, virus, allo scambio di droga ed ad altre attività illecite. Una piena informazione sull'argomento e una educazione sulle diverse tematiche legata alla Blockchain, potrebbe cambiare la visione delle stessa presso i possibili utenti, eliminando così la diffidenza verso essa e facilitando così una apertura dalla posizione di nicchia verso il grande pubblico.
3. Azioni dei Governi: i modi e le aree in cui i governi decideranno di intervenire o non intervenire relativamente alla Blockchain, alla sue applicazione a livello di business influenzeranno fortemente i futuri sviluppi ed ambiti di applicazione. Un possibile scenario comprende la possibilità che i governi tutelino gli attuali servizi, quali ad esempio quelli delle banche tradizionali, per garantire l'occupazione e i livelli economici, a discapito dei nascenti *Blockchain Financial services,* basati sulla disintermediazione, quali i lending P2P oppure i trasferimenti P2P diretti tra i soggetti senza dover passare tramite un soggetto terzo. Se da una parte, una regolamentazione stringente potrebbe creare un danno all'ecosistema, d'altra parte si potrebbe pensare ad una regolamentazione in formato light. Questa modalità potrebbe permettere uno sviluppo migliore dando al consumer una maggiore sicurezza, potrebbe allontanare alcune paure dettate dall'errata percezione pubblica, come hanno fatto ad esempio le normative bancarie del *Know Your Customer (KYC*) o i requisiti richiesti dalla normative legate a Basilea, dopo gli scandali legati all'ambito dei *financial services* e della raccolta diffusa del risparmio. Una soluzione potrebbe essere ad esempio, la creazione di una licenza, come già avviene a *New York (**The New York Bitlicense**),* per chi gestisce o produce *wallet*. Un ulteriore ***pain point*** potrebbe essere l'inapplicabilità dell'attuale sistema di tassazione delle attività alle attività decentralizzate, per risolvere

questo problema potrebbe essere pensato un sistemata fiscale a livello globale basato sui consumi e non sul reddito come gli attuali.

2.9. Osservazioni Finali

Questo capitolo è stato incentrato sull'analisi tecnica della Tecnologia Blockchain, elemento necessario per lo studio delle applicazioni nell'ambito della Corporate Governance, dell'Accounting e dell'Auditing. Analizzando le differenti componenti si è potuto capire la motivazione per cui il World Economic Forum ritiene che entro il 2025 il 10% dell'economia mondiale girerà sulla Blockchain, ciò è ampliamente giustificato dal fatto che essa è una tecnologia flessibile, interoperabile, automatizzante, data safer, crittografata.

Dal punto di vista tecnico sono state analizzate la storia (dai suoi albori fino alle ultime applicazioni), i pillar cardine (consensus, distributed ledger, automazione ed immutabilità), il funzionamento (miners mining), il funzionamento dell'architettura (nodil e network), la struttura e le modalità di creazione dei Blocchi, i modelli di criptazione, delle chiavi e della firma digitale ad essi connessi, lo studio dei design principles (distributed power, il valore degli incentivi all'interno del network, la sicurezza, l'integrità dei dati, l'interoperabilità, la velocità e la riduzione dei costi, l'interoperabilità, il trusted protocol e l'integrità del network), gli Stadi di evoluzione della Blockchain (La Blochain 1.0, 2.0 e 3.0), approfondimento di use case cross industry (Smart Property, Estonia – eResidency, Lantmateriet, Nasdaq – OTC Trading & Corporate Voting, Anticounterfeiting & Supplychain Tracking, Digital CV e Financial Applications) ed infine dei limiti della Blockchain technology (l'influenza del sistema ecosistema governativo, la percezione pubblica ed i limiti tecnologici).

Un caso particolarmente interessante è quello dell'applicazione portata avanti dal NASDAQ. Essa sta utilizzando la Blockchain per supportare le transazioni Over The Counter, in quanto essa può portare una diminuzione di costi e di tempo grazie all'automazione e alle disintermediazione grazie alla creazione di un network trusted. Il sistema non supporterebbe solamente le transazioni ma permetterebbe di portare un miglioramento anche in ambiti affini come il corporate voting,

Un altro caso di rilievo è quello implementato dal governo estone, il quale ha creato la prima identità digitale del cittadino sul network blockchian. La e-identity può fornire al

cittadino, tramite una ottimizzata user experience, differenti funzionalità, come quella di carta d'identità valida in tutta l'unione europea, di identificativo per l'accesso ai conti bancari legati a quel singolo cittadino, di tessera per il trasporto pubblico, di documento per l'accesso alle prestazioni sanitarie nazionali e la relativa richiesta di prescrizioni sanitarie, di Firma digitale per la validazione dei documenti e dei atti, di piattaforma per abilitare il voto digitale nelle elezioni nazionali.

Dall'analisi dell'applicazione della tecnologia è stata proposta una visione interessante in quanto da questa è scaturito la possibilità di applicare in modo proficuo la Blockchain in tutte le industry come ad esempio al settore pubblico, al finanziario, al trasportation, al real estate, energy food, ….

3. Gli effetti della distruptive innovation sulla CG e sull'Auditing[28]

3.1. Osservazioni Iniziali

Diversi studi, ad esempio come quelli redatti da *Gartner*[29], classificano la tecnologia Blockchain come una tecnologia emergente, che tra circa 5 – 10 anni raggiungerà una enorme diffusione e presenza di mercato, ad esempio nel 2030, il suo valore di mercato sarà di circa di 3,1 trilioni di dollari.

La Blockchain sta già rivoluzionando e rivoluzionerà sempre di più, il mondo aziendale, sostituendo o supportando l'intervento umano nei task, specialmente nelle aree in cui è richiesto un lavoro ripetitivo, time consuming e guidato dal dover seguire delle regole ben definite e non derogabili. [30]

Per questa ragione, tutte le aree legate alla *Corporate Governance* e al Controllo Aziendale (in senso lato), come ad esempio l'amministrazione, la finanza, il controllo di gestione, la gestione aziendale, l'audit interno ed esterno, il controllo del collegio sindacale, le relazione con gli stakeholder e la materia legale, sono tutte aree in cui la Blockchain sta e potrà innovare sempre di più sia nel breve che nel medio termine. La Blockchain diventerà cosi, nel breve periodo, soprattutto per i suoi *early adopters*, un enorme vantaggio competitivo ed invece nel medio-lungo termine, sarà considerata uno standard per sicurezza, trasparenza, efficienza, automazione ed interoperabilità.

28 Corporate Governance and Blockchain, David Yermack, 2015

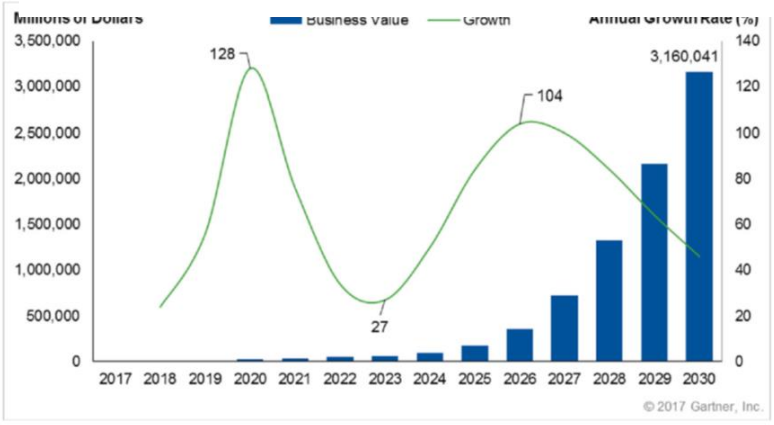
EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

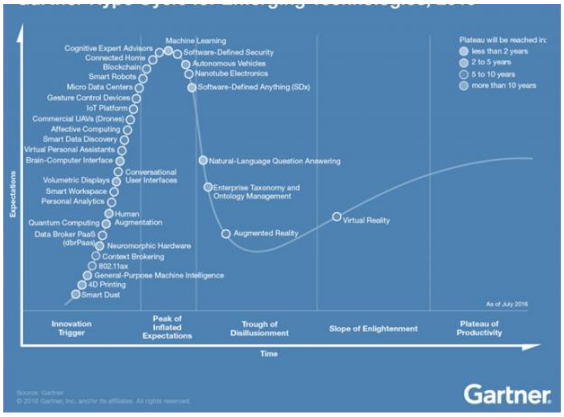
29 Gartner Hype Cycle for Emerging Technology, 2016, Gartner

Pratical Blockchain: A Gartner Trend Insight Report, David Furlonger, Ray Valdes, Gartner, 2017

30 EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

Figura 24 Gartner:The Blockchain Hype





Creare o inserire un azienda in Blockchain può avere molti **effetti positvi o negativi**, ma a **somma positiva**, sui **diversi stakeholder** come manager, shareholder, governo e PA, clienti, fornitori, dipendenti, creditori, banche e investitori.

Per queste ragioni in questo capitolo verranno esaminate le più importanti tematiche attinenti all'unione **della Corporate Governance e dell'auditing con la tecnologia basata sul distributed ledger.**

Il primo argomento che verrà trattatati sarà quello relativo agli **effetti delle tecnologia sulla corporate governance,** in particolare verranno approfondite tematiche attinenti alle modalità di **emissioni dei titoli aziendali**, specificatamente saranno trattate le modalità di emissione relativi **ai colored coins e alle ICO**. Di quest'ultimo verranno analizzati sia i **meccanismi** per poterne comprendere il funzionamento, sia verrà analizzato il **trend** di alcune interessanti **ICO**, per concludere con l'approfondimento sulla **risposta dei governi nazionali a questo fenomeno**, andandoci a focalizzare sulle risposte di **Cina e USA.** Successivamente saranno analizzate le modalità di funzionamento dell'emissione tramite **colored coin per andare ad individuare le differenze con le ICO.**

Il secondo tema che verrà trattato sarà relativo all'analisi dell'influenza della trasparenza portata dall Blockchain technology al mondo aziendale. La tematica della trasparenza nella corporate Governance abbraccia diverse sottotematiche come ad esempio:

a. L'automazione delle dichiarazione dei pacchetti azionari superiori ad una certa soglia considerata rilevante
b. Le strategie ed i problemi legati alla trasparenza per i Corporate Raider
c. Gli Azionisti di maggioranza e la Agency Theory I
d. I Piccoli Azionisti e la Agency Theory II
e. Il check sull'ownership relativamente a diversi ambiti quali: l'acquisto di azioni di competitor diretti e non, Vendita e manipolazione delle Management Stock Option
f. Il governo e la trasparenza nelle aziende

La successiva tematica che sarà trattata sarà inerente agli effetti sul corporate voting e della sua possibile influenza nel diminuire l'assenteismo ed nel proporsi come sostituto del proxy Voting.

La seconda parte del capitolo è focalizzata dall'interazione della tecnologia con le tematiche di Accounting e di auditing. La prima tematica che sarà affrontata sarà quella relativa all'accounting, ai suoi problemi odierni e di come la Blockchain potrà risolverli tramite l'introduzione della triple ledger accouting system, sistema basato su un ledger unico e decentralizzato che permetterà di andare incontro alle esigenze aziendali odierne. Successivamente sarà approfondito la sua struttura architetturale per poter capire al meglio la sua capacità d'implementazione nell'attuale sistema.

Relativamente all'auditing saranno trattati diversi argomenti come:

a. Le nuove modalità di auditing delle imprese
b. L'attestazione dell'integrità dei documenti contabili
c. I cambiamenti relativi alla figura dell'auditor e alle sue attestazioni e Giudizio
d. Le limitazioni dell'Accrual Managament

3.2. Gli effetti sulla CG

3.2.1. Le ICO e i Colore Coins: l'emissione dei titoli di Capitale di Rischio e di Finanziamento tramite la Blockchain

Emettendo le azioni della società sulla Blockchain, usando il sistema delle ***ICO***[31] (*Initial Coin Offer*) o dei ***Colored Coins*** sarà possibile dare **una maggiore trasparenza sulla ownership dei titoli**, sia quelli di capitale e sia quelli di finanziamento. La dematerializzazione e l'inserimento delle stesso in Blockchain permetterà di osservare chi **sia realmente il proprietario**, quasi **in tempo reale**, in media solo con un piccolo delay di pochi **minuti**, contro i **3 giorni** richiesti dalla struttura attuale, creando così una diminuzione del *settlement time* pari al **– 99%.**[32]

L'emissione attraverso ***ICO*** ***tokenizza*** i diritti derivanti dal quella **partecipazione** e permette di **venderli facilmente** come **una semplice criptovaluta**. Una volta effettuato l'acquisto, la **chiave** relativa a quella moneta **viene assegnata al wallet** dell'acquirente, per poter dimostrarne il **possesso**. Gli ***smart contract***, tramite *un Blockchain explorer* leggeranno il **registro pubblico** distribuito e daranno **informazioni** in tempo reale riguardanti il **possesso** dei diversi titoli da parte dei diversi attori.

Figura 25 Meccanismo ICO

Le **ICO** sono un composto tra il ***crowfunding***, le classiche ***IPO*** societarie e la **piattaforma Blockchain**, in quanto hanno come scopo **la raccolta di capitale** di rischio per *l'issuer* (***IPO***),

[31] https://medium.com/@TweetFromHilary/from-ipo-to-ico-blockchains-finance-revolution-b34c46ef281b
http://investingnews.com/daily/tech-investing/fintech-investing/blockchain-technology-stocks/
https://etherevolution.eu/cose-un-blockchain-ico-perche-importante/

[32] EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

la raccolta avviene in **forma diffusa** tramite la rete (***Crowfunding***) e il tutto avviene tramite **transazioni in Blockchain**. *L'issuer* ***dell'ICO*** emette **una propria criptomoneta**, avente **valore unitario** ed incorpora i **diritti** connessi al possesso del titolo di credito sottostante alla parte di capitale di rischio acquisito. L'emissione di capitale avviene **attraverso un asta**, alla fine della quale verranno **emesse le monete** *ICO*, le quali andranno a formare il **capitale di rischio della società *issuer***.

L'utilizzo delle ***ICO*** come modalità di **emissione dei titoli** porta diversi **vantaggi** ai vari stakeholder, ad esempio è possibile per la società ***issuer*** far acquistare agli investitori, da qualunque parte del mondo, partecipazioni **senza dover pagare fee** delle **piattaforme** di vendita, **degli intermediari** effettuanti la **vendita e dell'ente tributario**. Questa modalità d'investimento, già attualmente, permette anche all'investitore medio di poter **investire in tecnologie emergenti**, cosa di solito **riservata ad investitori professionisti**. La moneta emessa, porta un ulteriore vantaggio all'investitore, essa può essere **scambiata liberamente** con altra **criptovaluta**, monete **ICO** o moneta, ciò rende le monete ICO **altamente liquide**. Sarà possibile per l'investitore **monetizzare** il proprio **investimento senza** dover aspettare di effettuare un **exit**, ma solamente è **necessario** convertire la moneta ICO in altre valute. Analizzando i casi[33] di alcune recenti ***ICO***: *NXT, Ethereum, Lisk, DAO, Waves, Stratis*, possiamo notare un **trend positivo** nel profitto degli investitori, escludendo *Waves* con *PP* negativo e *DAO* con un *PP* pari a 0. Calcolando il **valore medio ponderato** per il valore di **Fondi raccolti** (Valuta USA Dollar) dei **profitti** delle **ICO** possiamo evincere un valore pari al ***364,84%.***[34]

[33] https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/

[34] Rielaborazione (Fonte: https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/)

EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

Figura 26 ICO Analysis

ICO	Anno	Funds Gathered (BTC)	Funds Gathered (USA dollar)	Token Distribuiti	Profit Percentage	Profit WAVG
NXT	2013	21,00	$4.201,47[35]	1.000.000.000,00	1.999.00%	4,17%
Ethereum	2014	31.529,49	$18.439.086,00	60.000.000,00	3.900%	357,46%
Lisk	2016	15.480,53	$5.700.000,00	85.000.000,00	138%	3,91%
DAO	2016	12.700.000,00	$160.000.000,00	1.153.816.598,70	0%	0,00%
Waves	2016	30.096,70	$16.436.095,00	85.000.000,00	-25%	-2,04%
Stratis	2016	915,00	$598.684,50	84.000.000,00	450%	1,34%
		12.778.042,72	**$201.178.066,97**	**2.467.816.598,70**		**364,84%**

Le ICO stanno suscitando un sempre maggiore **interesse** ed in molte nazioni si stanno **adoperando per regolamentarne il fenomeno** e renderlo **alternativo alle attuali fonti di raccolta di capitale** delle aziende. Le **diverse nazioni** stanno avendo **differenti approcci** all'emissione di **token nelle ICO** come **forme di finanziamento per le esperienze blockchain**, i due più importanti esempi sono gli **USA** e la **Cina**. La Cina[36] ha mostrato un approccio **molto restrittivo verso le ICO**, nel settembre 2017 diversi istituti cinesi (Peoplès Bank, la China Banking Regulatory Commision, la China Insurance Regulatory

[35] Stima del valore in base al Cambio BTC/US Dollar del 10/2013, pari a circa 200,07 dollari per ogni Bitcoin
[36] http://www.ilsole24ore.com/art/finanza-e-mercati/2017-09-04/la-cina-mette-freno-ico-bitcoin-caduta-160613.shtml?uuid=AEyvsMNC
http://www.repubblica.it/economia/finanza/2017/09/06/news/il_bitcoin_non_teme_la_cina_e_torna_a_correre-174782399/
https://www.economyup.it/fintech/la-vera-strategia-della-cina-dietro-il-bando-delle-ico-ed-il-crollo-del-bitcoin/
https://www.money.it/Divieto-ICO-in-Cina-non-uccidera-criptovalute

Commission, e la Cina Securities Regulatory Commission e la China National Internet Finance Association), hanno considerato il crowfunding attraverso le ICO una forma di finanziamento illegale e non approvato. La motivazione alla base del provvedimento è quella di voler evitare una eventuale bolla speculativa, dovuta all'uso fraudolento dello strumento. Vietando le ICO, quindi l'emissione delle criptovalute, si privilegerà il Bitcoin, il quale non viene emesso ma esso può soltanto essere minato e del quale la Cina è il più grande minatore, producendo così prima un deprezzamento in seguito alla notizia del blocco, al quale seguirà un rialzo dovuto alla maggiore richiesta dovuta alla mancanza di altre criptomonete concorrenti.

Negli Stati Uniti vi è stato un intervento della SEC che nel medio lungo termine mira a creare un corpus di regolamentazioni. Questo approccio può essere visto come premiante della riconosciuta qualità innovativa della tecnologia Blockchain, in quanto la regolamentazione non va a limitare fortemente l'attività ma va solo ad imporre degli obblighi d'informazione per tutelare l'investitore. La SEC, come primo passo ha prodotto un report[37] nel quale analizzano le ICO e affermano l'equivalenza dei token delle ICO alle securities regolate dal *Security Act del 1933* e al *Security Exchange Act 1934*, ciò impone agli enti emittenti di seguire le regole previste dalla SEC per le emissioni delle azioni sul listino nazionale. Le ragioni tecniche che hanno portato la SEC ha disporre la equipollenza dei processi di emissione dei titoli stessi è basata sui seguenti elementi:

1. Principio alla base della regolamentazione applicata alle organizzazioni virtuali e alle entità che raccolgono capitale facendo uso della distributed ledger:

[37] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: DAO, release n.81207, 25/07/2017

Trendon T. Shavers and Bitcoin Savings and Trust, SEC, Civil Action No. 4:13-CV-416 (E.D. Tex., complaint filed July 23, 2013)

Erik T. Voorhees,SEC, Rel. No. 33-9592, 03/06/2014

BTC Trading, Corp. and Ethan Burnside, SEC, Rel. No. 33-9685, 08/122014

Bitcoin Investment Trust and SecondMarket, Inc., SEC, Rel. No. 34-78282 (July 11, 2016)

SEC, Sunshine Capital, Inc., File No. 500-1, 11/04/ 2017)

Bitcoin and Other Virtual Currency-Related Investments, SEC, 07/05/2014

nell'analizzare cosa possa essere definito una azione si deve guardare la sostanza economica dello strumento e non la nomenclatura. Analizzando la sostanza si possono riscontrare diversi motivi per cui l'emissione di token attraverso ICO può essere paragonata ai contratti d'investimento, ad esempio è prevista la presenza di ragionevoli aspettative di generare un profitto per i differenti investitori derivante da un lavoro manageriale o imprenditoriale.

a. La presenza di un investimento: uno degli elementi caratterizzanti il contratto di investimento è la presenza di una fuoriuscita per il soggetto investitore, esso può essere effettuata in varie forme oltre in denaro, come ad esempio le criptovalute. Essa è presente nelle ICO, in quanto in cambio dei token - coin dell'emittente vi è un esborso in criptovaluta, a sua volta generato da uno scambio con le monete nazionali in degli exchange.
b. Aspettative di profitto: gli investitori che acquistano i token della DAO stanno investendo in una impresa e da questa si aspettano un profitto. I fondi raccolti verranno investiti in progetti ritenuti meritevoli in base alla votazione di tutti gli owner dei coin, da questi si aspetterà un ritorno maggiore dell'investimento (Return > Investement).
c. Deriva da un impegno di tipo Manageriale: i profitti sono derivati dall'attività imprenditoriale dai fondatori e dal curatore della DAO e dalle loro capacità manageriali a supporto degli stessi. Il loro *effort* è determinante nel raggiungimento del risultato ottenuto dalle attività finanziate, per questa ragione gli investitori hanno delle aspettative di profitto dalle loro azioni. Un esempio di questa attività sono i compiti svolti dal curatore, ad esempio esso si occupa di vagliare i soggetti terzi, determinare cosa e quando è possibile votare in assemblea, determinare l'ordine e la frequenza degli stessi. Un ulteriore esempio è dato dal fatto che il potere dei token holders è limitato dalla presenza dei founders e del curatore, in quanto ad esempio il voto dei token holders è limitato alle proposte approvate dal curatore.

2. **Considerare la DAO un *Issuer* soggetto a registrazione:** secondo la normativa USA è considerato un ***issuer*** qualunque persona che **emette o propone di emettere securities.** L'appellativo persona è da **considerare in latu sensu** in quanto in esso sono considerati qualunque **tipo di società o entità che è responsabile del successo o del fallimento dell'attività per cui si sta investendo.**
3. **La piattaforma di emissione e di trading dei DAO's token è considerata equivalente al National Securities Exchange:** secondo **l'act 3a** viene definito **come *exchange* l'entità** (persona, gruppo di persone, società, associazioni, ..) che gestiscono e organizzano un **marketplace** o facilitano **la vendita e l'acquisto di titoli** o che svolgono qualunque **altra attività svolta** solitamente dagli ***exchange registrati***. Inoltre secondo ***l'act rule 3b – 16,*** vengono riscontrati come elementi essenziali il fatto che la piattaforma favorisca **l'incontro tra le offerte di acquisto e di vendita** ed l'aver **predisposto un metodo non discrezionale** che gestisca il modo di **interazione tra gli ordini stessi.** La piattaforma utilizzata per gestire l'emissione e la negoziazione dei token delle DAO **rispecchia appieno le regole previste secondo la rules 3a** e non sembra essere contrario ai dettami **presti dalla 3B.**

La posizione Cinese e sia quella Statunitense, sono **parte** del **naturale** e **necessario** percorso **dell'incorporamento** di una innovazione nell'economia, il quale dovendosi **integrare** in un sistema già esistente dovrà subire degli **aggiustamenti** che saranno recepiti in modo differente in base alla situazione corrente, vi saranno **nazioni** più **conservatrici** che mireranno a **salvaguardare l'ecosistema**, altre invece come la **Svizzera, Hong Kong e Singapore** che saranno più **aperte all'innovazione**[38]. Un ulteriore elemento da considerare è il fatto che le ICO si basano su una **tecnologia** molto **giovane**, la Blockchain, che proprio per questa ragione può **generare preoccupazione** nei governi e quindi **indurre comportamenti fortemente restrittivi,** come quello Cinese.

Un ulteriore modalità per traferire la **proprietà dei titoli**, pagare i **dividendi** ed abilitare **i diritti di voto** derivanti dal loro possesso è basata sui ***Colored Coins***[39]**.** E' una modalità per

[38] "State of Blockchain Q2 2017" Coindesk, 08/2017
[39] http://yoniassia.com/coloredbitcoin/

inserire dei ***metadata*** sulle ***crytpovalute***, come ad esempio i ***Bitcoin***, per le quali viene scelta **una quantità predefinita** (ad esempio un satoshi per i Bitcoin il quale equivale e 0.00000001 Bitcoin) a cui **associare** il valore **il titolo da trasferire**. In questa fase tutte le **informazioni** riguardanti il **titolo**, mediante ***metadati*** sono associati ed inseriti ad una determinata ***Cryptovaluta***, essendo questa associazione forte sarà possibile **tracciare le ownership** e le **transazioni** di quel determinato asset e di eventuali diritti ad esso associate, come esempio il diritto di voto incorporato dalle azioni I ***colored coins*** possono essere compresi nell'ondata della **Blockchain 2.0**, possiamo immaginarli come **un *layer* di metadati** sopra la **Blockchain** alla quale è pure è collegato. Una volta raggiunto una **accordo** tra le **parti** su quale **moneta** rappresenterà **il titolo**, la **quantità** della stessa che lo **rappresenterà** e una volta inscritte sullo stesso le informazioni sull'asset, vi sarà la **transazioni tra le part**i ed avvenendo mediante ***Blockchain e Colored Coins***, essa verrà registrata in maniera indelebile nella stessa. Per dimostrarne l'ownership basterà **leggere i metadata** contenuti nella ***criptovaluta*** oppure seguire nel **distributed ledger il transito della moneta** fino ad arrivare **all'attuale owner.**

I Colored coins possono essere usati per differenti utilizzi quali ad esempio: **asset tracking, loyalty point issueing, digital collectibles, Local Money, per la gestione di Subscription a servizi e diritto di accesso.** I ***Colored Coins*** a differenza delle **ICO non** richiedono di emettere **una nuova moneta** ma usa le ***cryptocurrencies*** già **esistenti** e per questa ragione hanno una **maggiore liquidità** ma al tempo stesso sono legati in maniera **indelebile alle**

---

https://bitcointalk.org/index.php?topic=101197.0

https://coloredcoins.org

http://www.bitcoinx.org

http://szabo.best.vwh.net/idea.html

https://www.usenix.org/legacy/publications/library/proceedings/ec98/fujimura.html

https://en.bitcoin.it/wiki/Colored_Coins

https://www.draglet.com/blockchain-applications/digital-tokens/colored-coins

Colored Coins White Papere, Yoni Assia, Vitalik Buterin, Meni Rosenfeld e Rotem Lev

problematica delle criptomoneta sottostante come limitazioni tecnologiche, volatilità del suo valore, ….

Figura 27 Colored Coins System

3.2.2. La Blockchain e i miglioramenti apportati alla trasparenza nelle aziende

Grazie alla Blockchain si avrebbe **un'automazione per le dichiarazioni** riguardanti il **possesso di pacchetti azionari** al di sopra della soglia per le **partecipazioni rilevanti**[40], attualmente la dichiarazione avviene attraverso **autodichiarazione** e con un **arco temporale ampio**, ad esempio, per le società SEC[41] il limite è pari a 10 giorni ed in Italia[42] è circa 90 giorni. Invece grazie alla **Blockchain**, l'accertamento di una posizione sopra alle soglie potrà avvenire in un **lasso di tempo breve**, in quanto grazie ad uno ***smart contract,*** verrà **scansionata** la Blockchain, per trovare tutte i **titoli**, in quella **determinata azienda**, legate allo stesso **soggetto** e verrà verificato il **valore aggregato** totale rispetto alle **soglie limite**, in caso di **superamento** delle soglia, verrà effettuata una **transazione** in **Blockchain** ,contenente il valore della posizione da esso detenuto , verso le **autorità** di **vigilanza** adibite al controllo e verso la società.

[40] https://nexchange.com/article/8637
http://fortune.com/2017/03/31/initial-coin-offering/
http://www.coindesk.com/overstock-first-day-blockchain-stock-trading/
http://www.nasdaq.com/article/how-stock-exchanges-are-experimenting-with-blockchain-technology-cm801802
http://business.nasdaq.com/marketinsite/2016/Building-on-the-Blockchain.html
http://www.reuters.com/article/us-usa-sec-settlement-idUSKBN16T1SW
http://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html
https://www.lhv.ee/en/
http://www.cuber.ee/en_US/
http://www.reuters.com/article/nasdaq-blockchain-idUSL1N1FA1XK
EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, Giuseppe Diego Mulè, 2017

[41] Schedule 13 D

[42] Art. 120 A (Partecipazioni rilevanti ex 117), 120B (strumenti finanziari e/o delle partecipazioni aggregate) e 120 C (strumenti finanziari) del TUF

Figura 28 Processo di Autodichiarazione del raggiungimento della soglia rilevante

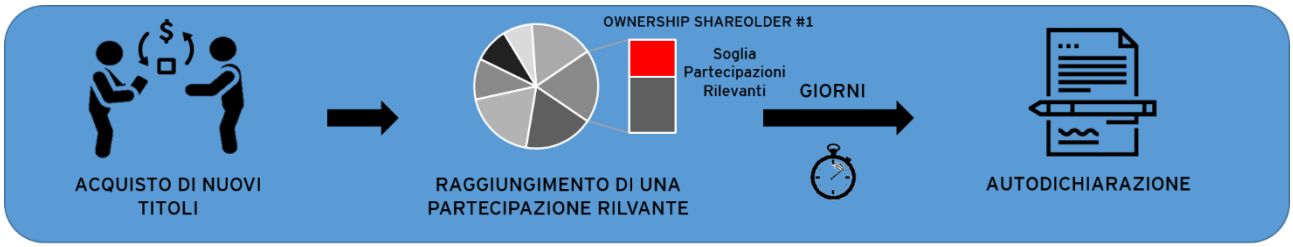
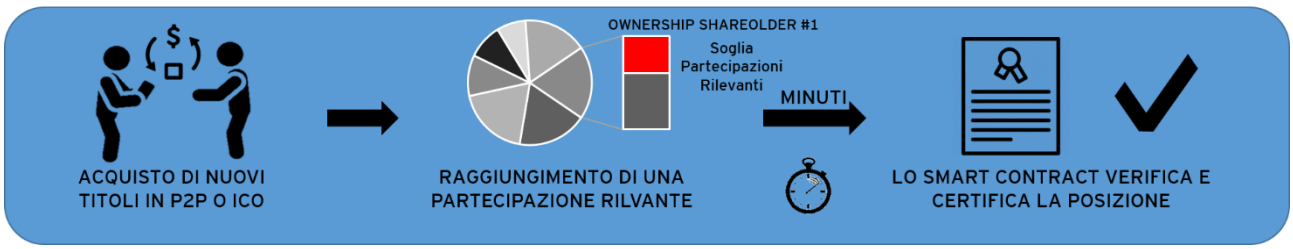


Figura 29 Certificazione delle soglie rilevanti tramite Blockchain



Una **maggiore trasparenza** riguardante le **ownership** ha una **moltitudine** di **effetti** altamente diversificati sui **differenti attori**[43].

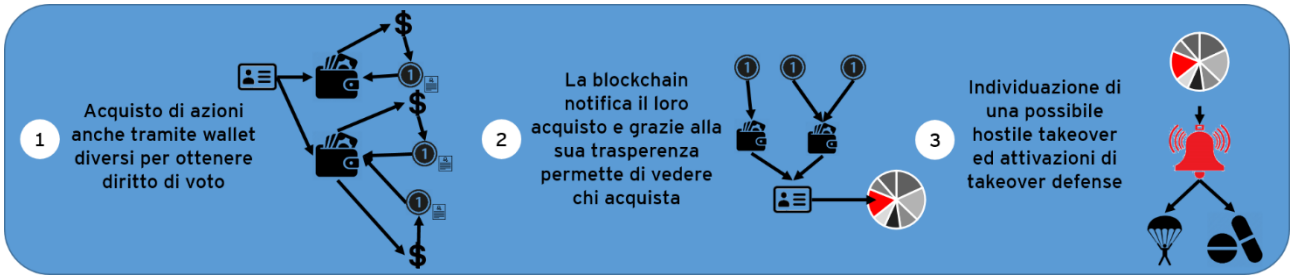
I **Corporate Raider**[44], basano la propria strategia **sull'acquisto di società** considerate **sottovalutate** dal mercato, in quanto il prezzo assegnato loro dallo stesso mercato è inferiore al valore che si otterrebbe vendendo in maniera atomistica i diversi asset della stessa azienda. Questa situazione può scaturire da una cattiva considerazione dell'azienda data dal mercato, da *insight* interni alla stessa, quindi da un mismatch tra le informazioni pubbliche e quelle private. Soprattutto nell'ultimo caso la Blockchain potrebbe essere una forte limitazione per loro in quanto se gli **elementi dell'azienda sono resi pubblici** e alla portata di tutti, il *mismatch* tra informazioni private e pubbliche si

[43] EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

[44] http://www.investopedia.com/terms/c/corporate-raider.asp
https://www.forbes.com/sites/steveschaefer/2011/02/15/private-equity-calling-plays-out-of-corporate-raider-playbook/#6100d12941df
https://www.strategy-business.com/blog/Corporate-Raiders-and-Their-Minions-A-History?gko=2ec7f
https://www.entrepreneur.com/article/78422
https://hbr.org/1987/05/from-competitive-advantage-to-corporate-strategy

potrebbe affievolire e quindi loro si vedrebbero **ridurre il loro vantaggio competitivo.** Inoltre una prassi tipica dei corporate raider è quella di acquisire la maggioranza della società target **mediante una acquisizione ostile.** Per tale ragione, essi cercheranno di tenere, nella fase embrionale del processo, **la strategia nascosta**, in modo da **non allertare** né il **mercato**, il quale produrrebbe un **impennata** dei **prezzi** dei titoli dell'azienda **target**, né l'attuale **management** e **proprietà**, che potrebbero attivare delle **difese all'hostile takeover,** ad esempio delle *poison pills, golden parachute*, *super-majority voting, green mail*, … La Blockchain potrebbe far **emergere e rendere evidenti** i loro **schemi** di acquisizione della società target, permettendo così ai differenti attori di mettere **attivare in tempi consoni le *antitakeover defense***.

Figura 30 Tracking delle Hostile Takeover dei Corporate Raider in Blockchain



Gli **azionisti di maggioranza**,[45] detenendo la **maggioranza del capitale sociale** e quindi eleggendo la maggioranza del Board stesso, saranno in possesso di una **completa informazione** o almeno maggiore rispetto a quella detenuta dagli altri soci o dal resto del mercato. Perciò la **trasparenza** può essere ritenuta come un **elemento sfavorevole** ai soci di maggioranza, in quanto detenendo una maggiore livello informativo, che rappresenta un **vantaggio competitivo**, una maggiore trasparenza potrà portare solamente un

[45] EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

http://www.investopedia.com/ask/answers/031815/what-role-agency-theory-corporate-governance.asp

Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns, Lex Donaldson, James H. Davis

Theory of the firm: Managerial behavior, agency costs and ownership structure, Michael C.Jensen .William H.Meckling

diminuzione dello stesso. Considerando anche gli effetti **dell'Agency Theory di primo tipo**, la Blockchain potrebbe essere un elemento fortemente positivo nel **ridurre** la stessa, in quanto porterebbe alla luce i **comportamenti negativi del Management** come ad esempio *l'earning management, backdating* delle azioni dei *manager*, l'acquisto da **parte degli stessi delle azioni dei competitor….**

Considerando la posizione dei **azionisti di maggioranza**, la Blockchain, essa è da ritenere a **somme positive** in quanto, anche se una **maggiore trasparenza** potrebbe portare uno spostamento di conoscenze verso l'esterno, producendo così una **perdita di valore della loro posizione** di *major shareholder*, essa porta con se un una **efficace soluzione** ad un complesso problema che spesso affligge le maggiori società, ***l'Agency Theory I.***

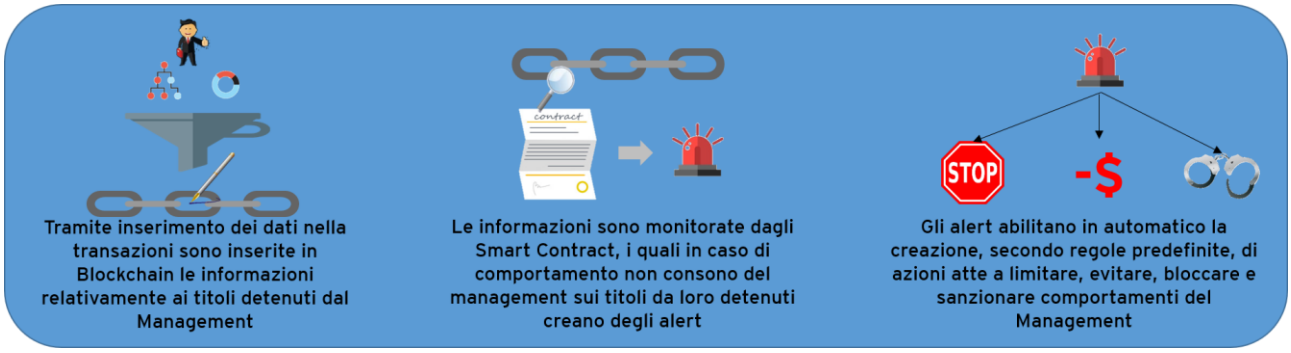
Figura 31 Agency Theory I e Blockchain

Una **maggiore trasparenza** ha un effetto positivo **sui piccoli azionisti** e sui **fondi con gestione passiva**, in quanto loro hanno un **livello informativo fortemente inferiore** agli azionisti di maggioranza. La carenza informativa è dovuta al fatto che il loro livello di informazione si attesta alle **comunicazioni obbligatorie per legge,** in quanto non avendo fondi o non essendo nella loro strategia non raccolgono ulteriori informazioni o se raccolte sono minimali e derivano dal mercato o da altri operatori. Ciò è il risultato della così detta ***Agency Theory*** **di secondo tipo**, dove vi è un contrasto ed una disuguaglianza tra i soci di maggioranza e quelli di minoranza. La **maggiore trasparenza** portata dalla **Blockchain** potrebbe affievolire **questa differenza informativa**, rendendo **accessibili le informazioni** che prima **non erano nella loro portata.**

Figura 32 La Blockchain per i piccoli azionisti

Un ulteriore elemento innovativo che potrebbe apportare al ***Check sulla ownership,*** è dato dalla **possibilità di tracciare i titoli detenuti da Manager** come parte variabile e bonus della loro remunerazione. Grazie alla **Blockchain** e alla **trasparenza** portata da essa, potranno essere **monitorate tutte le azioni** fatte dai **manager** sulla stesse e legare ad essi degli ***Smart Contract*** che, al compimento di **azioni non ritenute opportune**, attivino delle azioni che **limitino, blocchino o sanzionino l'azione fraudolenta.**

Figura 33 Blockchain per le Management Restriction



Numerose possono essere le **azioni** in questione[46]:

1. **Vendita delle *Management Stock Option***[47]: in molte grandi aziende si è sviluppata, come prassi, il pagamento della **parte variabile della retribuzione al top**

[46] EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, , Giuseppe Diego Mulè, 2017

[47] https://www.morganstanley.com/spc/knowledge/managing-equity/understanding-your-awards/restricted-stock.html
https://www.nceo.org/articles/stock-options-restricted-phantom-sars-espps

management dell'azienda tramite l'utilizzo di un **piano di stock option**. E' comune l'utilizzo delle cosiddette ***Restricted Stock Option***, le quali sono date ***al top management*** aziendale dopo fusioni, acquisizioni, IPO ,… Esse sono **soggette a restrizioni** nella loro **circolazione** per evitare vendite premature e in periodi specifici precedenti a possibili cadute di valore del titolo. La loro possibile vendita molte volte è in **parte postergata alla fine del contratto del manager** e talvolta anche per **diversi anni dopo questa.**

La **Blockchain** potrebbe **notificare** tutti i **passaggi degli stessi titoli** e vagliare la loro **aderenza** alle **regole specificate** alla loro emissione, mediante l'uso di ***smart contract***, in modo tale da **evitare** che esse vengano **vendute** impropriamente. La **vendita diretta** dei titoli, molte volte **non è l'unico modo** in cui manager effettuano la **vendita dei titoli** stessi, ad esempio essi possono essere **utilizzati come dei collateral** in **finanziamenti**. Utilizzandoli come collateral essi sono **una garanzia per l'eventuale inadempimento**, ma **se l'inadempimento è volontario**, l'istituto finanziario **venderà il titolo**, con la quale salderà il **debito del manager**. Invece il manager verrà **espropriato del titolo** ma in cambio avrà **ricevuto il valore economico** equivalente. Utilizzando questa modalità di vendita il manager avrà una **tassazione agevolata** e non configurando come vendita essa potrà essere usata come **modalità di vendita dei titoli.** La Blockchain mediante l'utilizzo ***di Smart Contrat*** traccerà tutti i ***passaggi ownership*** e sarà visibile a tutti l'utilizzo del titolo ***come collateral*** in un finanziamento, perciò sarà più semplice ed immediato il **riconoscimento di suddette azioni.**

Figura 34 Schema di Vendita indiretta dello Management Shares

http://www.investopedia.com/terms/r/restrictedstock.asp

http://www.menke.com/blog/how-to-structure-stock-ownership-plans-for-management-employees/

2. Manipolazione delle Stock Option[48]: oltre alla vendita delle *Stock Option* i manager potrebbero effettuare ulteriori azioni che mirano ad aumentare le loro revenues derivanti dai titoli come il ***backdating*** della data di emissione e/o di esercizio della option relativa al Manager oppure la manipolazione del ***vesting period*** dello stesso. Ciò che accomuna le differenti azioni è il fatto che tutte portino un incremento non dovuto del guadagno del Manager. La Blockchain essendo immodificabile non permette cha avvengano delle manipolazioni da parte degli attori degli elementi registrati al suo interno rendendola così ***tamper-proof by design***. Su ogni informazione registrata in Blockchain viene apposto un timestamp indelebile, una volta che è stato apposto esso non può essere rimosso e quindi le informazioni registrate sono salve da manomissioni. Questo sistema viene applicato con il fine di dotare di una maggiore sicurezza le informazioni contenute nelle diverse transazioni e renderle ***trusted*** dalla parti senza la necessità di avere una ***third trusted parts***. Per questa ragione una volta definite le date e i differenti periodi non potranno essere alterati per effettuare dei *gimmick* contabili con il fine di ottenere un maggior guadagno indebito. Ad esempio secondo la normativa della SEC le emissioni delle ***stock option*** devono essere dichiarate entro i due mesi dalla data di emissione, ma in questo modo viene reso possibile la manipolazione della data di emissione con il fine di sfruttare il ribasso del valore della stock ed avere un margine più elevato. La Blockchain, oltre a rendere tamper-proof le informazioni, rende immediata la registrazione delle informazioni e quindi la relativa dichiarazione agli enti preposti, rendendo così difficile le eventuali sofisticazioni dovute alla finestra temporale di dichiarazione agli stessi.

[48] Corporate Governance and Blockchain, David Yermack, 2015
https://blog.neufund.org/tokenizing-startup-equity-part-1-employee-incentive-options-plan-esop-on-ethereum-blockchain-dce2416f4505
https://neufund.org/esop/

Figura 35 Monipolaizone delle Stock Option

3. **Acquisto di azioni di competitor diretti e non**[49]**:** i manager, avendo informazioni sensibili e privilegiate rispetto al resto del mercato, potrebbero avvantaggiarsi usando questa asimmetria informativa par fare **dell'arbitraggio** ed avere **ulteriori guadagnati** collaterali in caso di **riduzione** del **valore** della **compagnia** stessa in rapporto con il valore dei competitor. Sapendo con **anticipo** che probabilmente **il titolo dell'azienda** di cui sono manager cadrà, essi potrebbero **investire in titoli di competitor** come tecnica di ***hedging***, aumentando così sempre di più la **divergenza di interesse** con l'azienda (***Agency Theory I***). Inscrivendo i titoli in Blockchain**, gli smart contract** potrebbero **monitorare gli acquisti** dei manager così da poter bloccare e impedire l'acquisto per gli stessi di azioni ed altri titoli relativi ai competitor e altre azioni **in contrasto con quanto predefinito da policy e contratti aziendali ed etiche a cui loro stessi hanno aderito**. Ad esempio usando la tecnica delle ***colored coin*** si potrebbero **definire delle classi di azioni** verticali **per industry e competitor**. Ad essi potrebbe essere possibile applicare delle **restrizioni**, ***tramite smart contract***, che sia controllino in automatico i wallet dei manager e al momento in cui ravvisano che il **soggetto possieda due stock non** della **stessa società** ma con lo **stesso "colore",** si potrebbe far **partire un alert** e in tal caso si potrebbero **bloccare** per il soggetto alcune **azioni** come il diritto di voto, l'escussione del dividendo, l'acquisto di altre azioni, ...

[49] Corporate Governance and Blockchain, David Yermack, 2015
EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, Giuseppe Diego Mulè, 2017

Essendo la Blockchain *tamperproof* e **trasparente** permetterà di **registrare** tutte le **transazioni** nel distribuited ledger e di rendere le **informazioni registrate** una **prova incontrovertibile** del comportamento del soggetto.

Questo tipo di **controllo** permette di **migliorare l'allineamento** tra il manager e gli obiettivi aziendali un migliore allineamento porta dei migliori rendimenti aziendali.

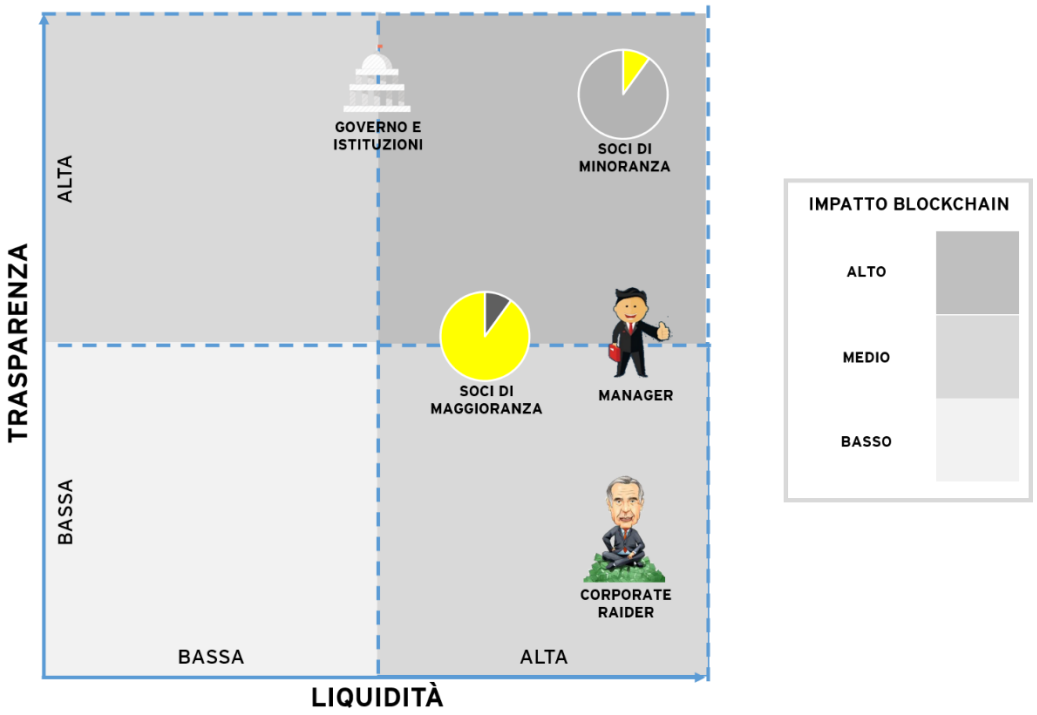
Figura 36 Acquisto delle azioni dei competitor

Il **governo e le istituzioni** hanno un elevato interesse nella Blockchain relativamente ai suoi effetti nella **Corporate Governance, nell'Accounting e nell'auditing,** soprattutto relativamente alla tematiche relativamente alla **trasparenza delle informazioni e della facilità di condivisione delle stesse**. La trasparenza può portare una più **efficiente offerta di servizi**, ad esempio per le **dichiarazioni previste ex legge** per le soglie di possesso del capitale di una società, **per il monitoring delle azioni dei soggetti**, ad esempio l'acquisto da parte del manager delle azioni di una società competitor, i controlli previsti ex legge per **le società soggette a revisione** e per le **dichiarazione dei dati** della contabilità aziendale contenuti nei bilanci **per finalità attinenti alla fiscalità.** Relativamente alla **liquidita**, il governo e gli enti pubblici sono quasi indifferenti anche se leggermente **propensi verso una maggiore liquidità** per ragioni di **ordine macroeconomico legate alla salute del mercato.**

Dopo aver analizzato gli effetti sui diversi soggetti si può notare che **tutti gli attori** hanno una **preferenza verso l'applicazione** della Blockchain con un effetto previsto nei quadranti con influenza della Blockchain **Medio-Alto.** Per tale ragione possiamo **prevedere nei prossimi 5 – 10 una adozione di massa** da parte dei differenti attori del network, ciò viene **supportato anche da diverse altre stime**, ad esempio secondo stime entro il **2018**, circa il

90% degli enti pubblici pianificherà di investire in progetti legati alla Blockchain[50], entro il 2019 almeno il 65% delle maggiori aziende al mondo avrà servizi che incorporeranno la tecnologia Blockchain ed entro i prossimi 3 anni la quasi totalità dei maggiori istituti bancari implementeranno soluzioni legate alla Blockchain.

Figura 37 La propennsione degli attori verso la Blockchain



[50] *Building trust in government", IBM*

Report EY, Blockchain industry Outlook (2016),

CoinDesk Quarterly update Q3 2016,

angel.co,

Blockchainangel.eu

3.2.3. Il Corporate Voting e l'effetto apportato dalla Blockchain Technology

La **Blockchain** può abilitare il voting per ogni tipo di votazione, principalmente potrà essere un **valido sostituto per il *corporate proxy voting*[51]**, permeato da molti **problemi ed inefficienze**, quali ad esempio la **lista dei votanti inesatta**, **l'incompleta distribuzione dei diritti di voto e la caotica tabulazione dei voti.** In un sistema di **voting in Blockchain,** i soggetti legittimati al voto, ad ogni votazione **riceveranno un *token* (*votecoins*),** che al momento del voto sarà trasmesso con una transazione. L'associazione del voto al token può avvenire **tramite l'utilizzo dei metadati** (come ad esempio utilizzando la tecnica dei ***colored coins***) oppure inserendo il **voto nella transazione** della critpovaluta. La transazione viene registrata nella Blockchain e sarà **immutabile e trasparente** verso tutti gli attori del network, in questo modo vi sarà più **fiducia** e maggiori possibilità che lo **shareholder voti la mozione**. Questa nuova modalità faciliterebbe gli shareholder, in quanto porterebbe **vantaggi in termini di tempo, trasparenza e accuratezza del voto**, **incentivandone la partecipazione** degli stessi, in modo particolare quella dei piccoli azionisti. Grazie alla sua **maggiore velocità** può essere un deterrente per le **pressioni effettuate dal management** durante le votazioni nei confronti dei soggetti dissidenti che votano contro la loro mozione. Un ulteriore problema risolvibile ***è l'empty voting***, ciò quella classe di schemi e strategie che permette tramite il prestito o utilizzando una combinazione di derivati su azioni per **ottenere i diritti di voto temporaneamente senza** avere una **esposizione economica** al flusso di cassa connesso alla sottostante azione. ***I giudizi sull'empty voting*** sono controversi in quanto da una parte della dottrina viene riscontrato che essi possono produrre degli **effetti negativi** sulle votazione come **la votazione in senso contrario** rispetto agli interessi del soggetto proprietario effettuata dal detentore temporaneo. L'altra parte della dottrina sottolinea **invece gli effetti positivi** generati dall'empty voting sia sul **mercato dei diritti di voto** e sia **sulla corretta valutazione del**

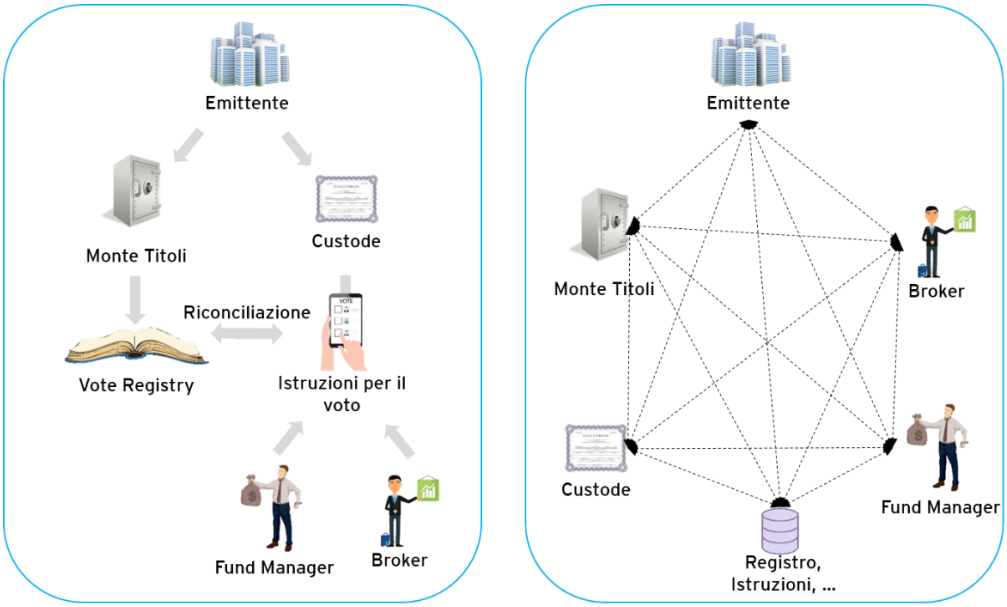
[51] Bitcoin and the Blockchain as Possible Corporate Governance Tools: Strengths and Weaknesses, Penn State Journale of Law & International Affairs, Fiametta S. Piazza, 07/2017
http://revfin.org/corporate-governance-and-blockchains-by-david-yermack/

pricing degli stessi. Grazie all'empty voting, gli azionisti detenenti una piccola partecipazione nel capitale sociale dell'azienda **possono vendere o noleggiare temporaneamente il proprio diritto di voto**, ricavando da questo un margine. Ulteriormente permette una **corretta valutazione**, in quanto il pricing potrà essere fatto utilizzando un modello di valutazione basato sul **benefit marginale dato da qual diritto di voto all'highest valued voter**. La Blockchain potrebbe **facilitare gli scambi** dei diritti di voto, mediante la creazione di un **marktplace p2p**, rendendo **trasparente** le transazioni e gestendo i **rapporti tra i due soggetti utilizzando gli smart contract**. Lo **smart contract**, potrebbe **gestire** in maniera ottimale **il lending temporaneo del diritto di voto**, in quanto **potendo imporre dei limiti alla sua utilizzazione** e potendone **monitorare** in automatico l'eventuale **inadempimento** ed **attivare,** in base alle necessità, **azioni esecutive e/o correttive** dell'azione sottostante. Ciò **limiterebbe** fortemente **l'uso fraudolento** ottemperato da alcune delle parti nei confronti del lender, in quanto in caso di utilizzo del diritto di voto contrario, a quanto pattuito dalle parti in fase di dealing, si attiveranno automaticamente in capo alla parte fraudolente azioni sanzionatorie. Inoltre la **maggiore trasparenza garantita dalla Blockchain** potrebbe portare ad ottenere **una migliore valutazione del pricing** in quanto, grazie alla trasparenza, si potrà basare la **valutazione su dati aggiornati** in real time e su un **data set completo** di transazioni. La trasparenza, **rendendo evidente la transazione** tra le parti, potrà fornire agli altri shareholder, al management e ai regulator le informazioni relative ad essa, permettendo così eventualmente di **effettuare azioni per contrattaccare o fermare l'azione d'acquisto**.

Figura 38 Il processo di Blockchain Corporate Voting: Empty voting

La Blockchain può influire su **altri aspetti del corporate Voting**[52] come ad esempio nel facilitare il **rapporto tra i differenti attori** nel processo di riconciliazione tra i **registri aziendali,** quelli del Deposito Centrale Titoli **(Monte Titoli**) e della **società di asset managment** richiede circa **25 – 30 giorni** dall'annuncio fino alla chiusura del voto. Grazie alla **Blockchain** si possono **ridurre fortemente i tempi** richiesti dalla procedura utilizzando le potenzialità **del registro distribuito della Blockchain**, in modo da **condividere le informazioni** con il network di attori **senza doverle inviare,** in quanto già distribuito presso la rete, quindi accessibile a tutti. Grazie alla Blockchain potrà essere creato e disegnato un **workflow automatico per la comunicazione delle informazioni** ai differenti attori, le istruzioni per il voto, le notifiche ed i voti espressi.

Figura 39 Lo Scambio delle Informazioni per il Corporate Voting



[52] Streamlining Corporate Actions Processing with Blockchain, White Paper, R. Samudrala, G. R. admnabhan Tata Consultancy Services

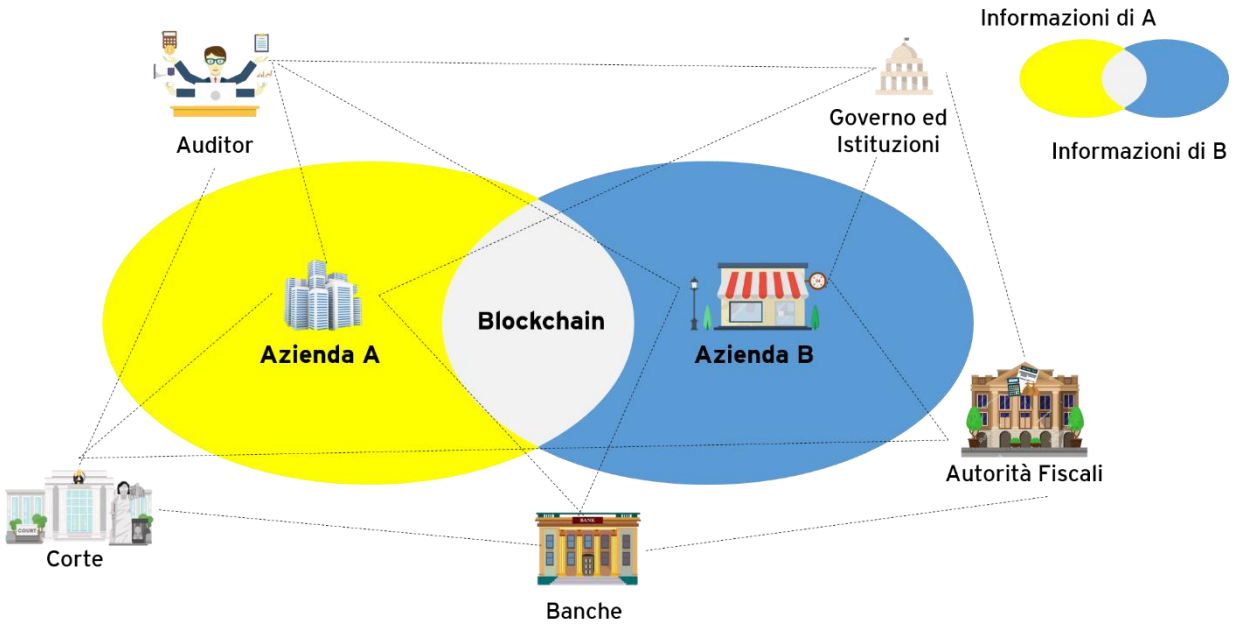
3.3. La Blockchain il game changer della Contabilità e della Revisione Aziendale

3.3.1. Gli improvement nel Firm Accounting

La **Blockchain** può abilitare la **raccolta** e la **notarizzazione sicura** e **certificata** dei **dati** aziendali, rilevati al fine di redigere le **scritture contabili** necessarie alla determinazione del risultato della gestione annuale, ciò può essere fatto in modo tale da **rendere immutabili le registrazioni contabili**, quindi renderle impassibili ad essere soggette ***all'Accruals Earning Management***, da eliminare **l'intermediazione dei revisori** e da controllare le **transazioni tra parti correlate**. Con questa modalità di contabilizzazione i dati sono **registrati in modo permanente**, in quanto su di essi vi è impresso un ***time stamp tamperproof***, che permette di **evitare l'alterazione ex post del dato** stesso.

La **Blockchain** può essere un ***game changer*** anche nelle **comunicazioni** richieste tra le aziende e con **attori esterni** all'azienda come revisori, banche, autorità fiscali, tribunali, governo ed altre istituzioni della PA. Permettendo **la registrazione nel ledger** distribuito delle **informazioni è possibile facilitare la loro condivisione** in maniera **sicura** e potendo **tracciare** chi ne ha **accesso** ed eventualmente revocare lo **stesso** in caso di comportamenti **non ritenuti consoni** dal data owner.

Figura 40 L'interazione ai fini dello scambio dei documento con i differenti Attori



La **Blockchain** abilita[53] la **raccolta in real-time dei dati contabili** della società, nel **sistema attuale** la raccolta in real-time è una **operazione proibitiva**, in quanto richiederebbe **elevati costi** dovuti dal dover fare **numerose operazioni altamente *time consuming***, che includono la raccolta dei dati stessi (anche automatizzata in parte) e il successivo audit interno della procedura stessa per la verifica del funzionamento della piattaforma.

Utilizzando la Blockchain per la gestione degli accounting record aziendali si effettuerà il passaggio **da un *double entry system*** per arrivare ad sistema contabile basato ***sul triple entry system***. Il sistema attuale basato sul ***double entry system***, richiede una **doppia scrittura contabile** in capo alle due parti della transazione per la stessa operazione. Quindi ogni parte dovrà effettuare **la propria scrittura** contabile **in maniera indipendente dall'altro**, ciò, oltre a portare una duplicazione delle scritture, può portare all'effettuazione di diversi **errori**, alla creazione delle **inconsistenze** tra i diversi i due differenti **registri contabili** delle *firm* nella transazione, a delle **inaccuratezze** ed inoltre **richiede** che vi siano tra le parti una diametrale corrispondenza tra i due registri a seguito delle **riconciliazioni** tra gli stessi. Considerando una transazione di acquisto prodotti dove **l'azienda A** (acquirente) compra un **prodotto X dall'azienda B** (Venditore), il quale al momento dell'acquisto **produrrà una fattura** relativamente al rapporto sottostante, ciò,

---

How Blockchain Tech Will Change Auditing for Good", Coindesk http://www.coindesk.com/blockchains-and-the-future-of-audit/ Matthew Spoke.

"Double Entry System Bookkeeping and Accounting Explained", Business Case Analysis, https://www.business-case-analysis.com/double-entry-system.html , Marty Schmidt.

"Cost? Trust? Something else? What's the killer-app for block chain technology?", Gendal Brown blog, http://gendal.me/2015/01/15/cost-trust-something-else-whats-the-killer-app-for- block-chain-technology/ , Richard Gendal Brown

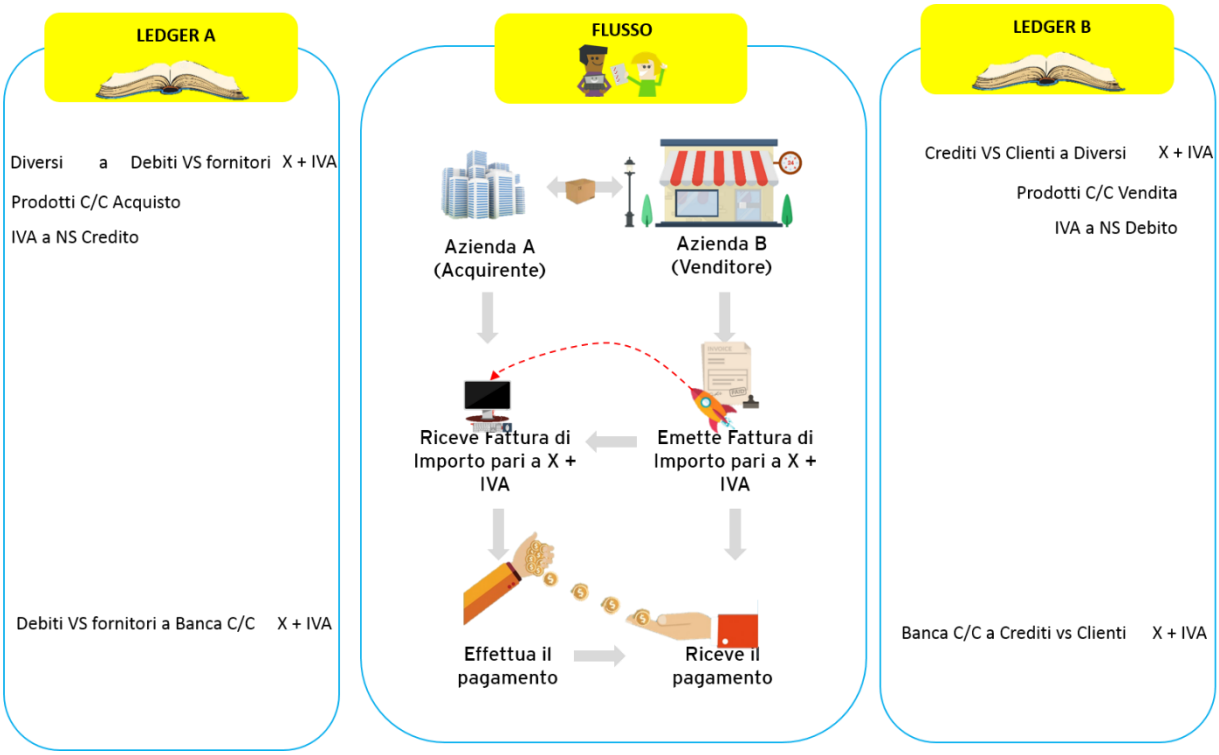
The term "Triple Entry Accounting," was first used by Ian Grigg in 2005, three years before Bitcoin. http://blockchainabc.blogspot.it/p/blog-page.html

"Triple Entry Bookkeeping With Bitcoin", Bitcoin Magazine, https://bitcoinmagazine.com/articles/triple-entry-bookkeeping-bitcoin-1392069656 , Jason M. Tyra., "If you call it a blockchain, it's not a single-entry system", Financial Timeshttp://ftalphaville.ft.com/2015/10/30/2143506/if-you-call-it-a-blockchain-its-not-a-single-entry-system/, Izabella Kaminska.

Knieff B., "Blockchain: What Is It Good for? Absolutely Something", Aite Group report, December 2015, p. 13.

in un **sistema double entry**, genera la necessita di effettuare **due serie di scritture contabili gemelle ed opposte**. La parte **acquirente** effettuerà dapprima le scritture per **l'acquisto del prodotto** e la **creazione del debito** da esso derivante, successivamente al momento del **pagamento** verranno redatte le scritture relative allo stesso, che prevedono una movimentazione finanziaria che eliminerà il debito e produrrà una fuoriuscita di liquidità verso il fornitore. Invece il **venditore** a sua volta dovrà effettuare le proprie scritture, prima relativamente alla **fuoriuscita** del **bene** oggetto della vendita dall'azienda a **fronte di una creazione di un credito** nei confronti **dell'acquirente** e successivamente una **movimentazione finanziaria** con l'eliminazione della posta relativa al credito e l'emergere di una entrata di cassa.

Figura 41 Double Entry System



Utilizzando la **Blockchian** e quindi **un sistema basato su un** Triple entry system, si porterà una maggiore **efficienza ed efficacia nel sistema**. Il **Triple entry system** porterà alla **creazione di un solo registro unico ma diffuso** presso **i diversi attori della rete**, al suo interno **verranno registrate tutte le informazioni relative alle transazioni**. L'avere un registro unico **distribuito abiliterà l'aggiornamento automatico** dello stesso tramite **una**

sola scrittura contabile e permetterà di informare ed avere accesso alle stesse a tutte le controparti. Considerando la stessa transazione di acquisto tra le due parti, questa volta vi saranno due scritture uniche per entrambi gli attori, la prima relativa all'acquisto/vendita del bene e la seconda, di tipo finanziario relativa al pagamento. L'azienda A al momento dell'acquisto dall'azienda B, genererà e firmerà una transazione contenente i dati dell'acquisto, che verrà inviata al venditore, il quale a sua volta firmerà la transazione, che una volta firmata da entrambe le parti, verrà iscritta nel registro distribuito, dove potrà essere eventualmente controllata dal revisore. La registrazione nel ledger distribuito farà nascere in capo al soggetto acquirente un obbligo di pagare al venditore una somma in corrispettivo al prodotto X. Uno smart contract regolerà i rapporti tra le due parti, in quanto renderà inutilizzabili temporaneamente le somme indicate dall'acquirente per adempiere all'obbligazione come garanzia per il debitore. Al momento della consegna del bene, lo smart contract libererà e transerà le somme verso il venditore, ciò farà venire meno l'obbligo di adempiere al debito. In questo sistema le informazioni sono crittografate e da queste sono rese immutabili, quindi è impossibile falsificare o cancellare le informazioni registrate.

Figura 42 Il Triple Entry System

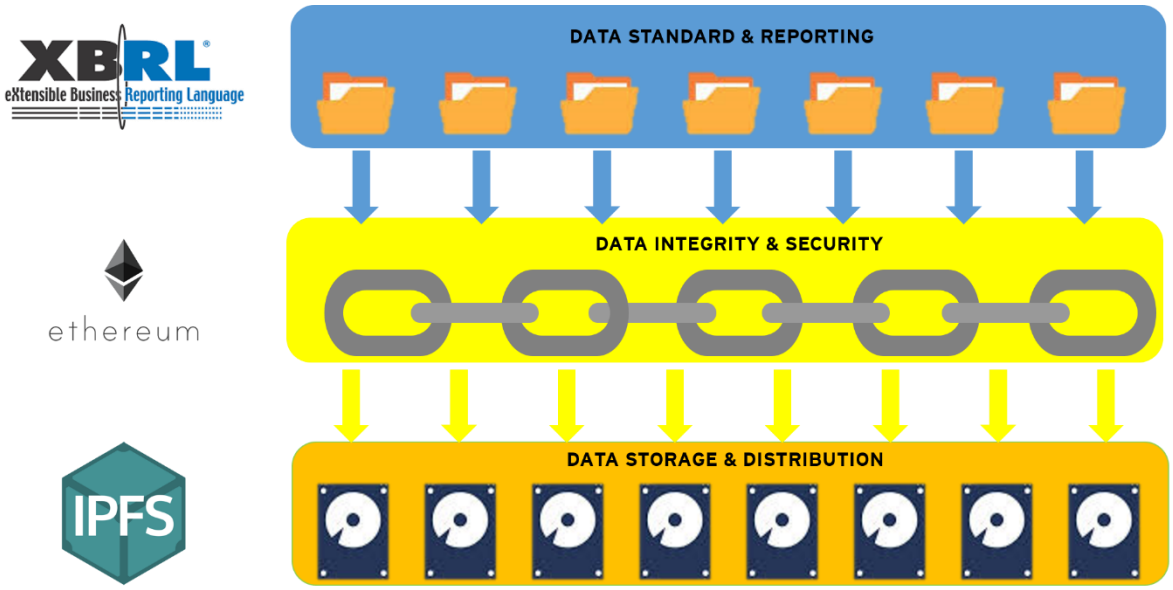
La soluzione può essere implementata sia al di sopra di network Blockchain pubblico sia al di sopra di uno ***permissioned.*** Nell'utilizzare la prima modalità, si permette l'accesso a tutti gli attori indistintamente, i quali potranno aggregare le transazioni e formare il conto

economico e lo stato patrimoniale dell'azienda in Real-time, senza dover sottostare alle suddivisioni periodiche. La soluzione potrà anche essere formata su un network *permissioned*, dove gli attori che visualizzeranno le informazioni registrate sono soggetti accettati dal network come azionisti, clienti, finanziatori, creditori, enti pubblici, regolatori di settore ed altre parti interessate alle informazioni registrate. Questa seconda soluzione è la soluzione più adatta quando vi è un elevato numero di attori che necessitano e possono verificare le informazioni registrate, invece la prima soluzione è la più adatta quando vi è la presenza di un numero contenuto di attori, in quanto essendoci solamente un numero ridotto di parti non viene permessa una sicura verifica delle informazioni al suo interno in una rete *permissioned* e quindi dovrà farsi sostenere dalla sicurezza e trasparenza di una rete pubblica, nella quale vi sono i ***miners*** che incentivati dalla ricompensa relativa al *mining* e *alla transaction fee* verificano in modo autonomo ed indipendente la transazione prima di registrarla nel *distributed ledger.*

Il sistema per funzionare adeguatamente richiede di 3 differenti *layer* con compiti diversi ma complementari per il funzionamento del sistema:

1. *Data Standard & Reporting*: esso è basato sul sistema universale XBRL, utilizzando lo stesso linguaggio permette l'estrazione dei dati in maniera semplice e facilmente utilizzabile da revisori e commercialisti. Essa impone il linguaggio ai dati in entrata ed in uscita.
2. *Data Integrity & Security*: può essere implementato su diverse blockchain sia pubbliche che private, come ad esempio Ethreum, Hyperledger, Bitcoin,… Essa assicura l'integrità dei dati ed certifica la loro sicurezza sia nello storing e sia nelle transazioni.
3. *Data Storage & Distribution*: i dati dopo essere stati conformati a dei standard universali e dopo essere stati resi sicuri ed integri vengono storati in dei sistemi decentralizzati di storage come per esempio IPFS, che permettono di salvare file in maniera criptata e sicura.

Figura 43 I 3 System Layer



3.3.2. Il Blockchain Audit Model[54]

La **Blockchain** apporterà sostanziali **innovazioni** che **modificheranno** totalmente il **settore della revisione aziendale** rispetto all'attuale conformazione, il ruolo del revisore andrà sempre di più a comprendere **l'attestazione dell'efficienza e dell'efficacia delle piattaforme abilitanti** le procedure e sempre **meno attinenti alla valutazione dei singoli elementi**. Possiamo pensare che il cambiamento non sia immediato e radicale, quindi possiamo immaginare che **in una prima fase preliminare** il sistema Blockchain **vada ad efficientare tramite il supporto all'attuale operatività** del revisore per poi andare sempre di più **a sostituire processi di verifica e controllo**. Quindi nella fase preliminare si potrebbe applicare **la tecnologia per verificare l'integrità dei documenti contabili**. La Blockchain potrebbe rendere possibile provare l'integrità dei documenti, in quanto una volta emesso il documento dall'ente emittente, esso **verrà *Hashato* per produrre *l'hash string***. ***L'Hash string*** relativa a quel documento sarà **inserita nella Blockchain** per permetterne la successiva verifica. Successivamente l'auditor che deve verificare l'integrità del documento ricevuto, **hasherà** il documento **per permettere la comparazione dello stesso** con quello del documento precedentemente inserito nella Blockchain. Se la Blockchain

[54] "Blockchain Technology, A Game changer in Accounting"Nicolai Andersen, Deloitte, 03/2016

"Blockchain & Audit", Christine Stark

"The Trust Machine", The Economist (h t t p : / / w w w. e c o n o m i s t . c o m / n e w s /leaders/21677198-technology-behind-bitcoin-couldtransform-how-economy-works-trust-machine/)

"The great chain of being sure about things", TheEconomist

(h t t p : / / w w w. e c o n o m i s t . c o m / n e w s /briefing/21677228-technology-behind-bitcoin-letspeople-who-do-not-know-or-trust-each-other-builddependable(

"How Blockchain Tech Will Change Auditing for Good", M. Spoke, (https://www.coindesk.com/blockchains-and-thefuture-of-audit/)

(Deloitte Explores Blockchain Tech for Client Auditing", P. Rizzo (https://www.coindesk.com/deloitte-blockchainauditing-consulting)

R3 (http://r3cev.com)

Rubix, Deloitte, (http://rubixbydeloitte.com)

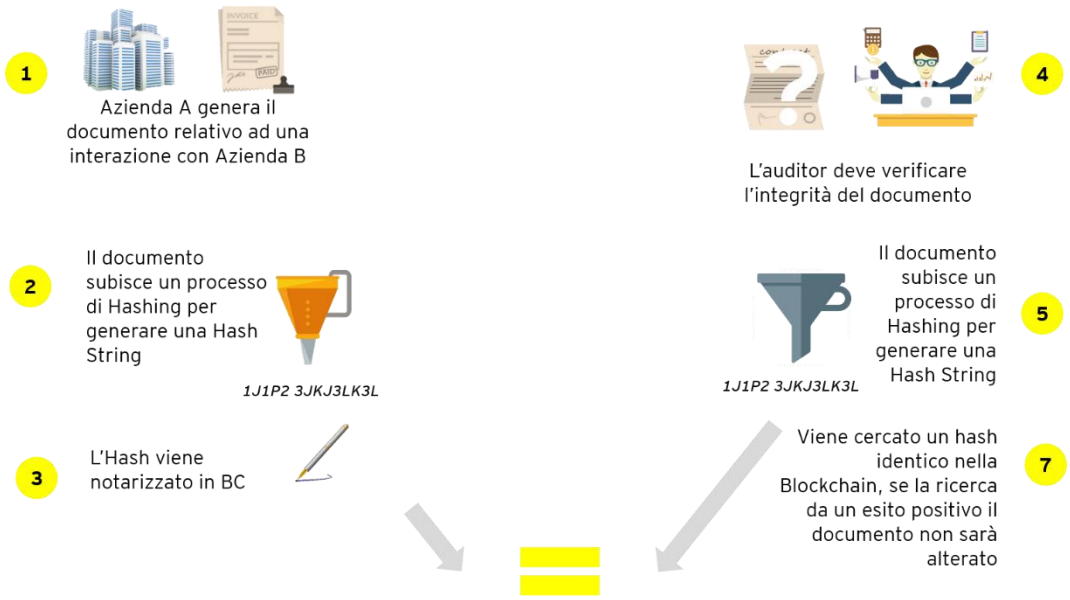
Triple Entry Accounting (http://blockchainabc.blogspot.fr/p/blog-page.html)

Trusting records: is Blockchain technology the answer? ", Records

Management Journal, Vol. 26 Iss 2 pp. 110 – 139, Victoria Louise Lemieux , (2016),"

troverà un hash identico a quello inserito in Blockchain si **avrà la conferma che il documento è integro** e che non ha subito modifiche da parte di altri attori.

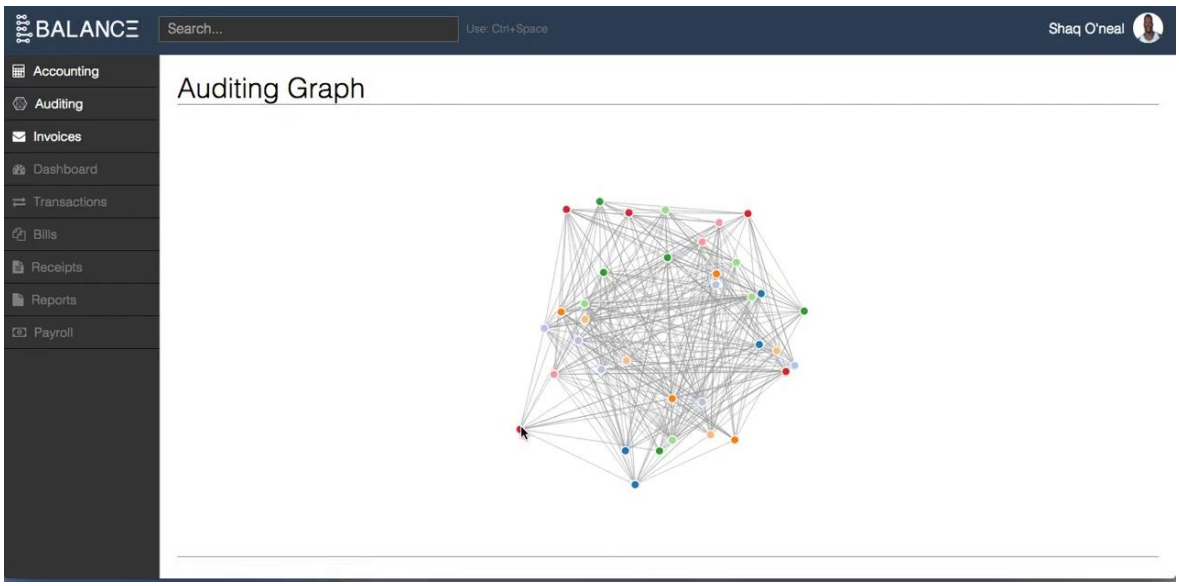
Figura 44 La Verifica dell'integrità dei Dati Tramite la Blockchain



In un seconda fase di sviluppo essendo possibile ***un real-time accounting***, **non** sarà più **necessario** il giudizio sulle informazioni **derivato dal lavoro di un soggetto terzo indipendente**, come il **revisore**, in quanto i diversi stakeholder riporranno la **fiducia** nei dati immutabili e certificati presenti **all'interno del network distribuito.** Grazie alla trasparenza introdotta dal ***real-time Accounting*** sarà possibile **monitorare** efficacemente ed efficientemente le transazioni tra le **parti correlate** ed individuare quelle **eventualmente sospette** di un possibile conflitto d'interessi tra gli stessi. La normativa attuale si base generalmente sulla **disclosure volontaria fornita**, in merito a quelle transazioni, dal Management del soggetto stesso, su quelle transazioni che lui stesso ritiene che siano state fatte con soggetti che possano **essere considerati delle parti correlate,** questa modalità è da considerare come una **via fortemente lacunosa**, quindi mediante l'utilizzo della tecnologia **Blockchain** si porterà a **limitare** sempre di gli **errori** dovuti ad una **mancata individuazione** di operazioni sospette e che potrebbero arrecare un ingente danno alla società ad esempio portando a conclusione **un negozio a prestazioni con non proporzionate.** Ad esempio utilizzando per la registrazione dei dati

contabili piattaforme come Balanc3[55] sarà possibile ai revisori controllare in real time le transazioni effettuate dalle differenti parti del negozio tramite semplici schermate, come quella qui di seguito.

Figura 45 Auditor View

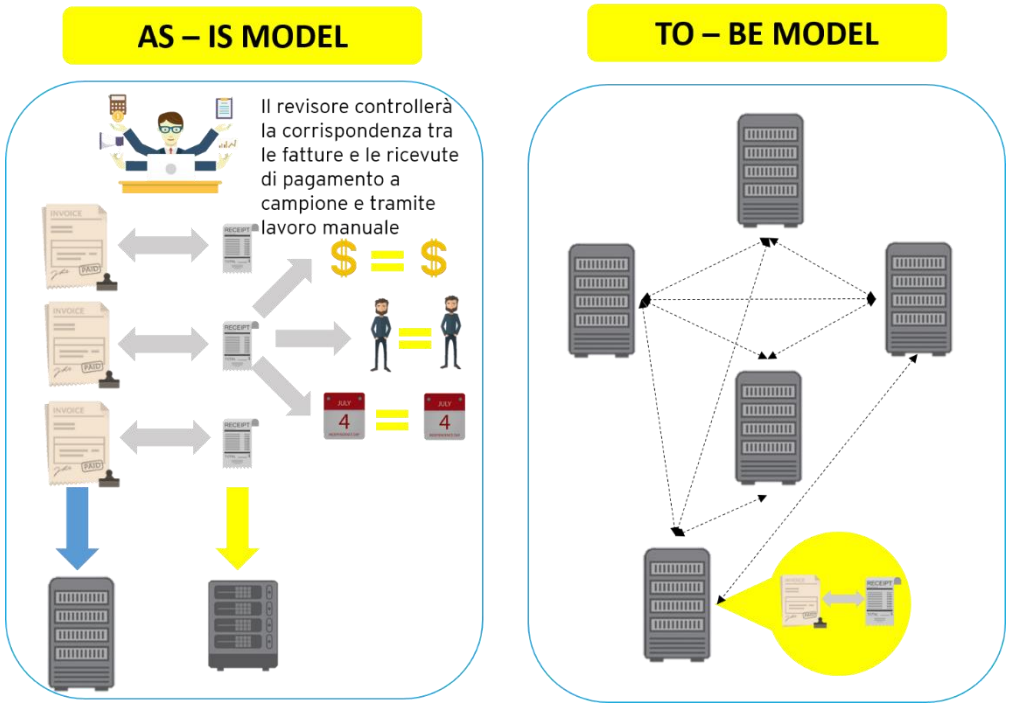


La Blockchain potrà portare innovazione ed un miglioramento anche nella **limitazione *dell'Accruals Earning Management.*** Grazie **all'irreversibile *timestamp*** apposto sopra alle transazioni, ai manager è reso impossibile applicare strategie mirate *all'accruals earning management* come il **backdating** dei contratti di vendita ad un periodo relativo ad un **precedente report periodico** oppure la pratica di **capitalizzare delle spese** agli anni successivi ed ammortizzarle in diversi anni, che invece secondo la prassi dovrebbero rientrare nella gestione dei costi del corrente anno e quindi spesate in una sola volta nel conto economico dello stesso periodo. *L'Accruals Earning Management* comporta per l'azienda **diverse distorsioni** come ad esempio quelle relative alla scelta dei manager per gli investimenti societari. Le loro decisioni andranno a beneficio di quei investimenti **che producono una crescita del profitto nel breve termine** anche a discapito di investimenti con un maggiore net present value nel medio-lungo termine.

55

Considerando ad esempio il **processo di revisione e riconciliazione delle fatture** con le relative **fuori uscita** di **cassa** al giorno d'oggi viene fatto su un **campione** di elementi e richiede una mole ingente di **lavoro time-spending** e **manuale** da parte del **revisore** con il rischio di **incorrere in errori umani**. Esso dovrà **matchare** il **pagamento** con la **fattura** che lo ha generato, molte volte si hanno **conti diversi, pagamenti differiti e frazionati**, ciò genera per il revisore una difficoltà. La riconciliazione è necessaria in quanto i differenti **elementi hanno provenienze diverse**. In un sistema basato sulla **tecnologia Blockchain** essendoci la registrazione delle **transazione in un unico registro** distribuito sui diversi nodi del network ed essendo possibile **effettuare un real time accounting** tramite un **triple ledger system non** vi sarà bisogno di effettuare nessuna **riconciliazione** manuale in quanto tramite gli **smart contract** è possibile effettuare su **tutte le transazioni in real-time ed in automatico le riconciliazioni** dei documenti in oggetto.

Figura 46 Esempio delle differenze tra un modello centralizzato ed un modello decentralizzato di Riconciliazione



3.4. Osservazioni Finali

In questo capitolo sono state analizzate differenti tematiche relative alla Corporate Governance, all'accounting e all'auditing con il fine di capire se le soluzioni proposte dal mercato nel ambito del settore siano efficaci ed pronte all'uso nelle realtà aziendali.

La prima macrotematica trattata è quella del connubio tra la tecnologia Blockchain e la corporate Governance aziendale. Dalla sua analisi è emersa una complementarietà tra le due materie in quanto sono stati riscontrati molti use case che possono dare un valore aggiunto alla situazione attuale. Il primo case esplorato è quello dell'emissione di nuovi titoli mediante gli schemi delle ICO e delle Colored Coins, entrambe le modalità permettono di emettere titoli con diritto di voto, di abilitare le transazioni in near real time, di diminuire i costi e di tracciare in maniera immutabile tutti i passaggi dei titoli. È emerso che al giorno d'oggi vi sono diversi approcci da parte degli enti governativi, ad esempio in Cina vi è stato un blocco totale dell'emissione di moneta tramite le ICO, invece un approccio totalmente differente è stato intrapreso dagli Stati Uniti d'America, i quali sono molto più propensi verso una regolamentazione del fenomeno alla stessa stregua di come oggi avviene per le IPO.

Il secondo macro tema trattato è quello della trasparenza e della sua influenza nel mondo aziendale. Da queste tematiche è emersa la piena capacità da parte della Blockchain a diminuire sia L'agency Theory I e sia l'agency theory II, in quanto essa permette ad esempio sia di rendere accessibili ulteriori informazioni che non sono alla portata di tutti i stakeholder, sia di rendere evidenti taluni schemi di partecipazione che permettono ad alcuni soci di avere la maggioranza.

La terza tematica che è stata affrontata è lo studio della moltitudine di applicazioni della blockchain al controllo dell'ownership del titolo. La Blockchain, oltre a permettere la tracciatura del titolo stesso, abilita il controllo dei titoli detenuti in portafoglio in ordine alla compatibilità dei dettami in capo al management relativamente all'acquisto dei titoli dei concorrenti, alla vendita e alla manipolazione delle stock option. Questi controlli, abilitati dai smart contract, oltre a permettere l'individuazione del casus permettono di

abilitare in automatico il compimento delle azioni con l'intenzione di bloccare, sanare o punire l'azione fraudolenta.

Analizzando l'interesse dei differenti shareholder intorno alle tematiche di trasparenza e liquidita forniti dalla Blockchain si può evincere che tutti gli attori sono indirizzati verso delle applicazioni Blockchain con un impatto medio-alto.

Dallo studio sull'utilizzo della Blockchain per effettuare il corporate voting è emerso che la Blockchain può essere uno degli strumenti per risolvere i problemi relativi all'empty voting, permetterebbe un pricing corretto del diritto di voto ed inoltre abiliterebbe la condivisione in modo più efficiente dei documenti per i soci obbligatori per legge derivante del diritto ad essere informati sulla situazione aziendale.

Analizzando le applicazioni all'accounting è evidente che la Blockchain possa senza dubbio migliorare il sistema attuale introducendo il triple ledger system, il quale permette di avere un real time accounting e la relativa registrazione in un unico luogo di archiviazione distribuito sui nodi della rete ed in maniera automatica. Questo sistema è particolarmente indicato per la tenuta della contabilità in quanto, oltre a vantaggi già detti, la Blockchain rende immodificabili i dati registrati e perciò essi sono considerati tamper proof alle modifiche, cancellazioni e falsificazioni.

Anche l'auditing sarà impattato in maniera decisiva dalla Blockchain, essa influirà fortemente su questa, in quanto in un primo momento sarà di supporto al auditor, permettendo la verifica in maniera istantanea e sicura dei documenti ricevuti dal cliente, fino a sostituire lo stesso sempre di più, obbligando lo stesso a cambiare il suo compito, ad esempio esso inizialmente controllerà il flusso di condivisione tra le controparti fino a testare e certificando le funzionalità della piattaforma stessa. La Blockchain, grazie alla sua notarizzazione immutabile dei suoi dati, potrà dare un supporto alla gestione dell'Accrual Managament.

4. Blockchkain CG & Audit Use Case

4.1. Osservazioni Iniziali

In questo Capitolo saranno esaminate 3 esperienze di applicazione reale delle soluzioni Blockchain esaminate nel terzo Capitolo, con il fine di dimostrare che la tecnologia Blockchain è già applicabile allo stato attuale alle imprese ed su di esse ha effetti positivi.

La prima start up che sarà esaminata è Otonomos, interessante start up nell'ambito della Corporate Governance, che permette tramite l'utilizzo e la combinazione di un wallet e con smart contract di:

d. Creazione istantaneamente una società
e. Creazione e gestione della Capitalization Table
f. Gestione delle transazione dei titoli
g. Automazione delle documentazione aziendale

La seconda esperienza che sarà esaminata è BTL, BP, ENI e Wien Energy. Essi hanno testato la tecnologia Blockchain per esaminare la possibilità di potere costruire su di essa un sistema di riconciliazione trade-by-trade (near real-time) ed ad una differenziata gamma di attività relative al back office aziendale, le quali supportano le attività core delle aziende.

La terza esperienza che verrà esplorata è quella di Tallystic, essa è una soluzione di tipo plug in che permette ai sistemi ERP, su cui è installata, di diminuire al massimo gli errori effettuati durante la fase di fatturazione verso il cliente, ridurre drasticamente i costi dipendenti dal controllo aziendale esterno come ad esempio i revisori, ridurre il cashflow necessario ad compire il fabbisogno finanziario scaturito dalle variazione del working capital ed inoltre stabilire un sistema dove vi sia maggiore fiducia e sicurezza nelle transazioni.

4.2. Otonomos[56]

Otonomos sarà una delle start up che innoverà il mondo delle **imprese medio-piccole e grandi pre-IPO**, in quanto **permetterà di gestire interamente l'impresa in Blockchain**.

Figura 47 Overview delle funzioni di Otonomos

Otonomos assegna un **wallet** basato sul sistema delle **cryptocurrencies**, a quale corrispondono dei **titoli** (come azioni, opzioni, bonds, note, …). Su questi è **implementato** un sistema ***di smart contract*** che abilitano **diverse funzioni**[57]:

a. Creazione in maniera **telematica** ed **istantanea** delle **aziende**[58]
b. **Creazione** ed **aggiornamento** in **real time** di un **registro** dei possessori dei **detentori dei titoli** (Capitalization Table), anche in situazioni di **alta complessità** e **frammentazione** della **compagine sociale**.
c. **Gestire** con **estrema facilità** il **trasferimento** delle azioni e degli altri titoli aziendali
d. **Codifica ed automazione delle documentazione aziendale** come lo shareholder agreements e di altri documenti governativi. Essi sono resi ***self executing*** tramite dei ***decentralized computers,*** il quale li abilita ad effettuare automaticamente delle **azioni in corrispondenza di avvenimenti ritenuti rilevanti**, che sono scelte in fase di stesura degli stessi secondo la logica ***IF <<Something Happen>> Then <<do something>>.***

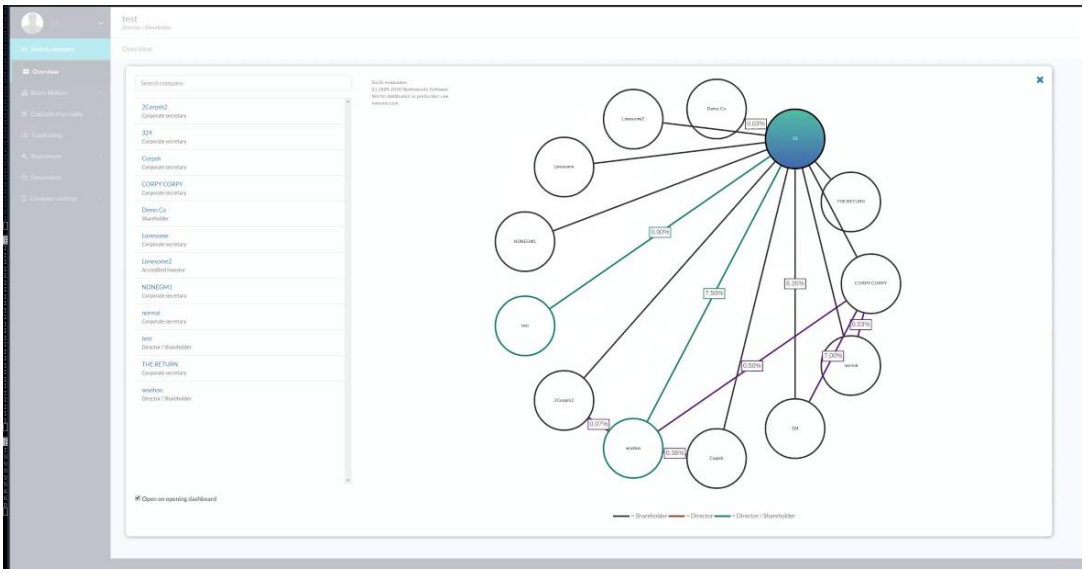
[56] www.otonomos.com
[57] https://www.youtube.com/watch?v=LAwCCi7lLcY
[58] Ciò attualmente è reso possible solo in alcune Nazioni

e. **Abilitare l'automazione di alcune azioni aziendali**, come ad esempio la **ripartizione e l'accredito dei dividendi** nei wallet degli differenti shareholder.

La **soluzione non** abilita l'azienda a fare maggiori ***revenues*** ma consente di **efficientare** i **processi amministrativi aziendale** permettendo così di **salvare tempo e denaro**.

Il ***wallet***[59] creato potrà contenere dei titoli, ad esempio come azioni ed obbligazioni, alle quali sarà apposto un "***watermark***" legata **all'identità del possessore**, elemento **necessario** affinché sia *compliant* alla normative del settore sulla tematica del ***Know Your Customer (KYC).*** I titoli creati in questo modo potranno avere le stesse **caratteristiche** dei **titoli normali**, come ad esempio per le azioni potranno essere create azioni con diritto o senza diritto di voto oppure con particolarità relativamente ai dividendi, ad esempio predisporre la correlazione del dividendo stesso a particolari indici aziendali o fornire altri tipi di **privilegi**, ulteriormente si potrebbe **postergarli** in maniera residuale agli altri ***shareholder***. Il wallet dell'utente potrà **contenere i titoli di differenti aziende,** di seguito l'immagine della piattaforma per la gestione dei titoli delle differenti aziende.

Figura 48 Schermata per la gestione del portafoglio dei Titoli



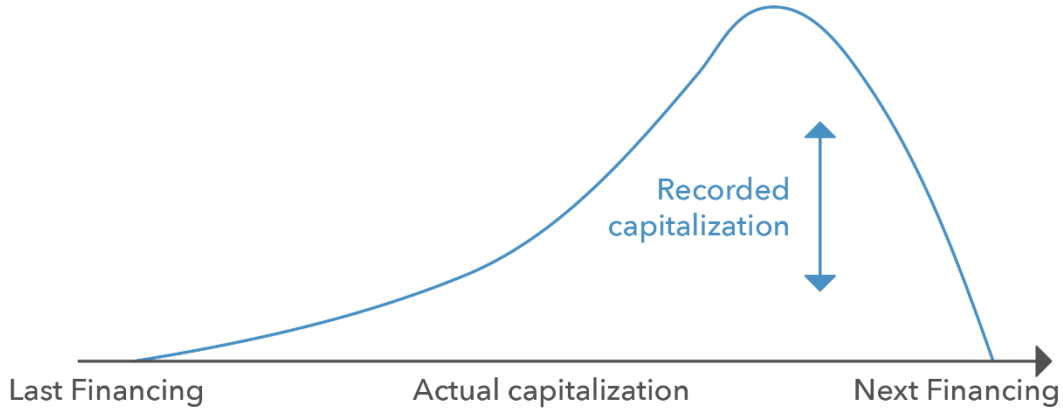
Il ***capitalization table*** è una tabella che mostra la **composizione della compagine sociale** dell'azienda, il breakdown **dei titoli di capitale, di debito ed altre tipologie di titoli emessi** come gli strumenti finanziari partecipativi, opzioni, warrant. Per ogni titolo sono

[59] https://www.youtube.com/watch?v=X7n6XVSKOxc

registrate le generalità del **soggetto**, il **prezzo** pagato, la **quantità** e la **percentuale** detenuta. Questo documento è necessario per un **efficiente registrazione e tracking** della **compagine sociale**, molte volte propedeutico **all'accesso a nuovi fondi**. Nella gestione attuale possiamo riscontrare **differenti problemi:**

1. **Errori nelle Capitalization Table:** molte **cap table** sono **errate** in quanto **non** sono **aggiornate** frequentemente, **l'eventuale** update avviene **manualmente**, il tracking viene registrato, se effettuato, in fogli excel o alcune volte le azioni emesse non vengono registrate nella cap table. **L'entropia nelle capitalization table** segue un andamento **periodico**, in quanto **cresce** finché non giunge, l'eventuale **successivo round di finanziamento**, momento nel quale vi è un **riordino** della stessa per effettuare il successivo financing round. L'entropia è **accentuata dai elevati costi** per mantenere aggiornata una cap table, quindi il suo aggiornamento **è differito fino al momento in cui essa diventa necessaria** e per il quale sarà necessario **pagare uno studio legale affinché rilasci un opinion** in merito, la quale costerà all'azienda tra i 5.000 e i 15.000 euro. [60]

Figura 49 Entropia nel recording della Cap Table



2. **Mancanza della tracciatura delle azioni:** durante delle **OPA** o durante le **acquisizioni** l'investitore, prima di pagare il prezzo per i titoli, **richiede di rilasciare i certificati** dei titoli al fine di determinare la **composizione attuale dell'azionariato,**

[60] https://www.youtube.com/watch?v=XgdRuSW0b50

ma molte volte essi non vengono consegnati, ma sono tenuti come **garanzia dall'avvocato della società emittente**, ma questo si può configurare come **conflitto d'interessi**. Inoltre i certificati non indicano la percentuale di capitale detenuta dai soggetti, ciò potrebbe portare l'investitore a **fare scelte errate** come ad esempio acquistare un pacchetto azionario di una società credendo di ottenere una maggioranza pur in realtà non avendola.

Figura 50 Mancata Tracciatura dei Titoli

3. **Titoli detenuti dai dipendenti:** i dipendenti hanno **differenti problemi nella gestione delle proprie stock option**, ad esempio hanno un numero esiguo delle stesse, hanno un tax rate elevato ed hanno una scarsa conoscenza in materia di azioni e opzioni

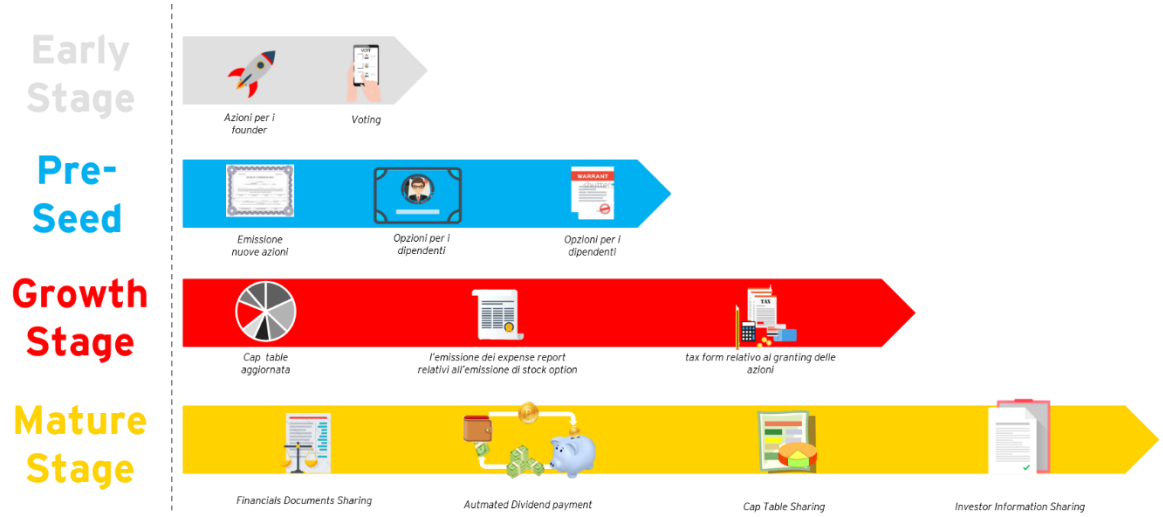
Otonomos può dare un grande supporto dalla creazione dell'azienda fino alla sua eventuale quotazione, in tutte **le fasi della vita dell'azienda**:[61]

a. **Early stage Firm:** fornisce il supporto per **l'emissione** delle azioni dei founder, assegnare i **diritti di voto** ed a tracciare fin dall'inizio il cap table
b. **Seed Lvl Start up: emissione** di altre azioni, warrant, obbligazioni convertibili ed ad emettere opzioni per i dipendenti
c. **Growth Stage:** facilita l'emissione dei expense report relativi all'emissione di stock option ed alla compilazione del tax form relativo al granting delle azioni

[61] http://fintank.net/2016/01/18/otonomos/
http://www.finanzprodukt.ch/fintech/otonomos-disrupting-business-incorporation-funding-and-governance-by-using-the-blockchain/

d. **Mature Stage:** abilita la condivisione con gli investitori dei cap table e dei dati finanziari.

Figura 51 Analisi della Funzioni per le diverse fasi del life cycle dell'azienda



La **creazione dell'azienda** sulla Blockchain avviene **in circa 72 ore**, ad oggi la sua valenza legale è relegate solamente ad alcune **nazioni virtuose** come ad esempio lo stato del **Dalaware**[62], il quale permette di tenere i **record degli shareholder e tutti gli altri registri obbligatori aziendali in Blockchain. Altre realtà** che permettono l'utilizzo della Blockchain per le tematiche di governance aziendale **sono** ad esempio **Singapore, Hong Kong , UK e le Isole Cayman.**

Esso può essere fatto in un modo molto semplice, pochi semplici step:

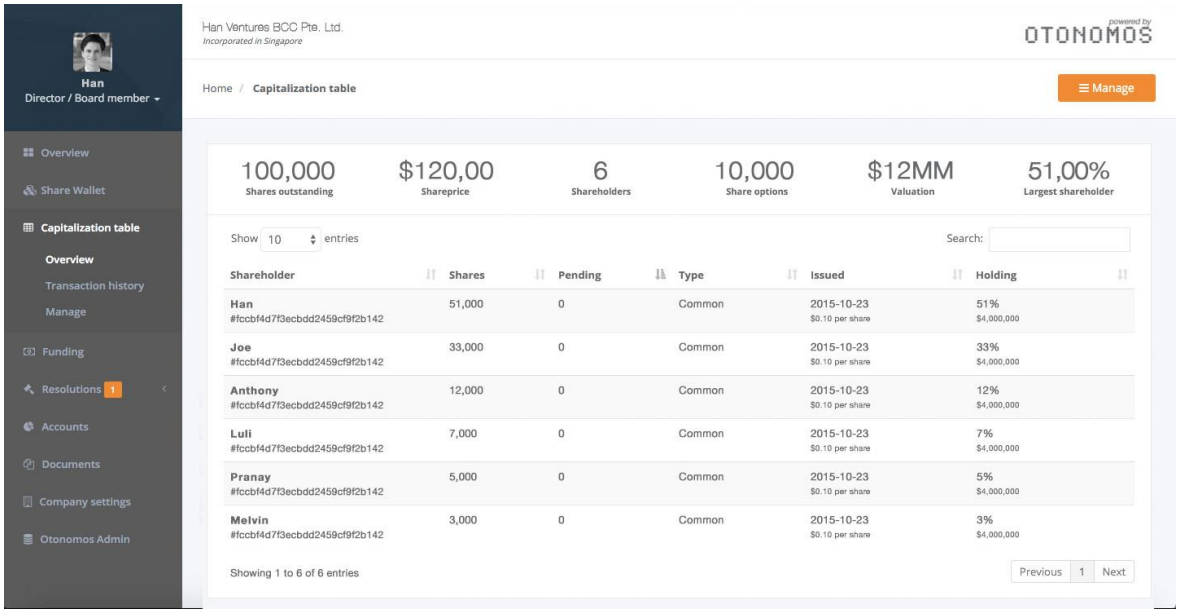
g. **Creazione del wallet della società:** in questa fase viene **notarizzata** nella rete la creazione dello **società**, allo stessa verrà **assegnato un indirizzo (wallet address)**, elemento necessario affinché **avvengano le transazioni sul network** Blockchain. La registrazione tramite **Otonomos in Blockchain** hanno lo stesso **valore legale e status di quelle create nel mondo reale**.
h. **Generazione della moneta a cui verrà assegnata il titolo:** viene creata una **criptovaluta**, la quale è utilizzata **come unità per il titolo da emettere** ed ad ognuna di essa verrà associata un titolo e le sue caratteristiche come il diritto di voto o di partecipare agli utili.

[62] http://fortune.com/2017/08/01/blockchain-shareholders-law/

i. **Assegnazione delle azioni ai wallet dei azionisti:** con una semplice **transazione** registrata in **Blockchain** vengono trasferite le azioni dal **wallet dell'azienda a quello dell'investitore.**

j. **Aggiornamento automatico della Cap Table dashboard:** la capitalization table si aggiornerà **automaticamente ad ogni transazione avvenuta**, anche tra gli investitori stessi.

Figura 52 Otonomos Cap Table Demo[63]



La piattaforma di **Otonomos** permette di fornire **livelli differenziati di permessi di accesso** in base alle **funzioni** svolte dall'utente, in base a questo possiamo definire **differenti tipologie di account** rispetto ad una singola società:

Figura 53 Tipologia di Account divisi per funzione[64]

	Esterno	Shareholder	Management

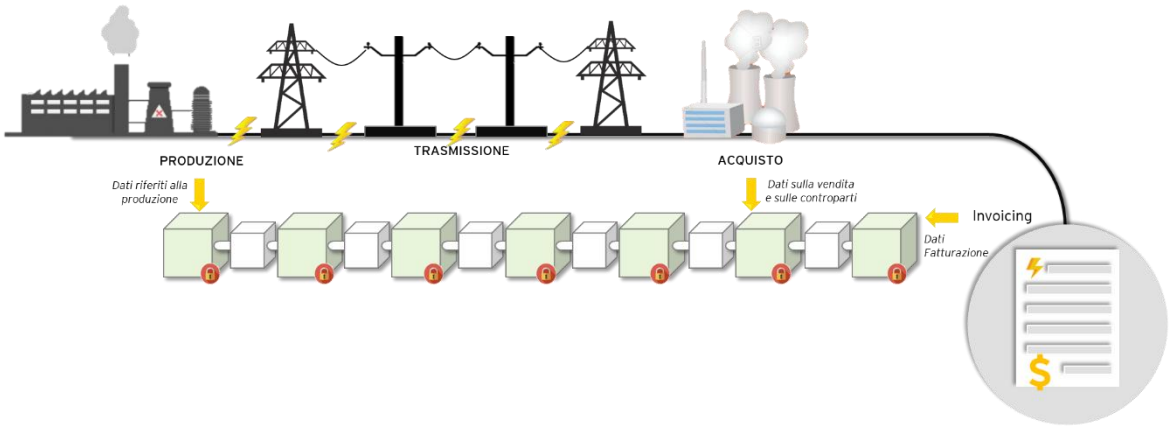
[63] https://angel.co/projects/209838-otonomos-launches-blockchain-powered-company-dashboard
[64] Elaborazione dei dati Otonomos

Società	Non è presente nella sua rete	La società appare nel suo network	Essi in aggiunta potranno modificare la pagina della società, le informazioni di fatturazione ed invitare gli utenti ad accedere all'azienda
Titoli	Non visibili nel suo portafoglio	Presenti nel suo portafoglio	Inoltre potranno modificare, trasferire ed attivare altre azioni sui titoli
Cap Table	Non ha accesso	Visibili e scaricabili dalla sua utenza ma non potrà visionare il livelli di dettaglio relativo al singolo utente	Visibili e scaricabili dalla sua utenza ma sarà possibile visionare il livelli di dettaglio per singolo utente e potrà visionare lo storico degli stessi
Report	Non ha accesso	Visibili e scaricabili dalla sua utenza	Visibili e scaricabili dalla sua utenza ed inoltre esso potrà attivare nuovi servizi in merito
Documenti di Bilancio	Non ha accesso	Visibili e scaricabili dalla sua utenza	Visibili e scaricabili dalla sua utenza ed inoltre esso potrà attivare nuovi servizi in merito

4.3. BTL, BP, ENI e Wien Energy[65]

La startup canadese **BTL** ha creato una piattaforma chiamata **Interbit**, per la quale ha ricevuto diversi **finanziamenti**. Questa Piattaforma ha visto la sua **prima applicazione** con delle società del settore **finanziario** ed **energetico**.

Figura 54 Esempio di applicazione della Soluzione in una transazione tra un produttore ed un buyer



Nella sua fase di **testing** la società ha creato **un progetto pilota di dodici settimane** incentrato sulle **riconciliazioni per mezzo della tecnologia *Blockchain***. Il pilota, gestito sulla piattaforma ***Blockchain*** di **BTL**, Interbit, ha dimostrato con successo che questa tecnologia **può abilitare un sistema di riconciliazione *trade-by-trade*** (***near real-time***). Questo risultato fornisce la prova per il potenziale più ampio e trasformativo che la tecnologia Blockchain promette di fornire in tutta la **gamma di attività back office** che **supportano le attività di trading nelle aziende energetiche**. Il testing è stato fatto con diversi **attori** quali:

i. **British Petroleum[66]:** è una società del **Regno Unito** del settore **dell'energia con un focus su petrolio e gas naturale**, settori nel quale primeggia livello mondiale insime a **Royal Dutch Shell, ExxonMobil e Total**. Essa si è originata dalla **Fusione tra British Petroleum e Amoco.**

[65] European Enerfy Pilot Exit Report, Hugh Halford Thmpson, BTL, 05/2017
http://btl.co/
http://uk.reuters.com/article/us-bp-eni-blockchain/bp-eni-deepen-blockchain-trading-in-european-gas-idUKKBN18W1N2
[66] https://it.wikipedia.org/wiki/BP_(azienda)

ii. **Wien Energy:**[67] è il fornitore leader in **Austria** di energia **elettrica, gas e termoriscaldamento.**

iii. **ENI[68]:** è una compagnia italiana presente in tutto il mondo, essa opera in **73 Paesi tramite circa 33.000 dipendenti**. Con una capitalizzazione di mercato pari a **55 miliardi** si attesta tra le più grandi aziende le settore Oil & Gas, inoltre essa è inclusa nella lista della **Fortune Global 500 Firm,** ad esempio nel **2016** ha occupato il **65° posto**. Tra le sue operazioni principali possiamo riscontrare la produzione, la raffinazione e la commercializzazione di olio e gas.

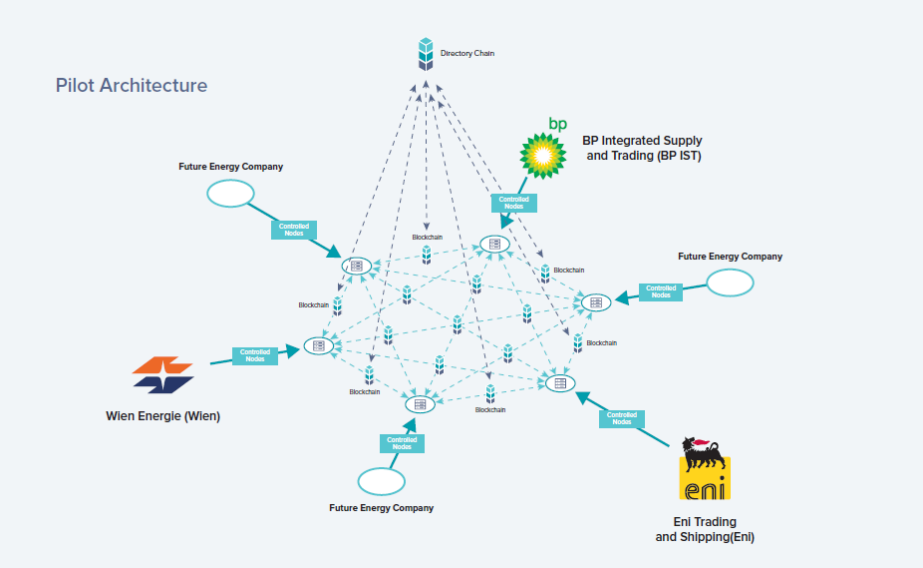
iv. **EY:** società **multinazionale** di **consulenza e revisione aziendale**, la quale negli ultimi anni ha **sviluppato dei team** con delle competenze **tecnologiche** dedite alla **design, alla creazione e all'implementazione di soluzioni in ambito Blockchain** .

Il pilota si è concentrato **sul processo di conferma** delle **transazioni** all'interno del network di aziende. Il team di progetto ha **confermato** che **l'applicabilità della tecnologia** Blockchain può essere estesa ad una serie di processi legati alle procedure di back office aziendali. Il Pilota del progetto è da considerarlo come **una prima pietra per l'applicazione della tecnologia Blockchain** ai processi in tutto il back office.

[67] https://de.wikipedia.org/wiki/Wien_Energie

[68] https://www.eni.com/it_IT/azienda/profilo-compagnia.page

Figura 55 Overview della soluzione BTL[69]



Nel pilota **l'ecosistema Blockchain** era formato **da diversi nodi** di sui **3 erano controllati** da **Wien Energie**, **British Petroleum** ed **Eni**, attraverso i quali **inserivano e verificavano** le **transazioni** all'interno del distributed ledger.

Il **design interoperabile** e **flessibile** della Blockchain offre notevoli **vantaggi** rispetto alla tecnologia del **database tradizionale** ad esempio essi possono essere considerati in termini di **tracciabilità, auditabilità, sicurezza** delle **transazioni** e **automazione** ed **efficienza** tra più **controparti**. Ad esempio, in aree come la regolamentazione e la conformità, logiche complesse **possono essere integrati in contratti intelligenti** che **eseguono automaticamente** direttamente sulla rete Blockchain anziché richiedere l'esecuzione individuale da parte di ciascuna società coinvolta in una transazione.

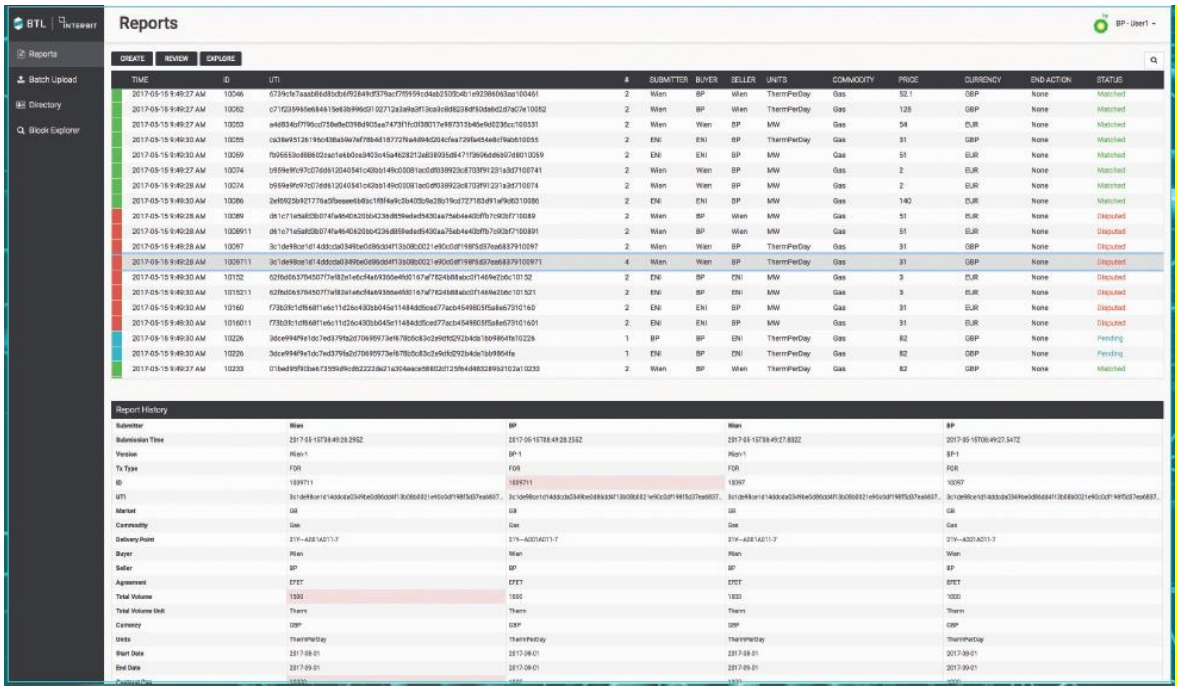
Interbit sfrutta una serie di Blockchain interconnesse per creare una **piattaforma altamente scalabil**e (risolvendo una delle principali sfide per le piattaforme Blockchain pubbliche di oggi), consentendo anche un **elevato livello di controllo della privacy** per garantire che i **membri che non fanno parte di una transazione non vedano** mai informazioni sulla **transazione**. Interbit **è un network blockchain privato** che opera all'interno di una rete limitata di nodi noti (**network permissioned**). Il meccanismo di

[69] Brochure Otonomos

consenso semplificato di Interbit è in grado di rilevare immediatamente eventuali manomissioni e in grado di scalare le esigenze di una rete regionale o globale.

Nelle transazioni registrate nel network Blockchain è possibile registrare tutte le informazioni inerenti alla transazione economica tra le parti.

Figura 56 Interbit Demo - Transazioni[70]



La maggior parte **dell'efficienza** resa possibile **dalle tradizionali tecnologie di rete** sono ormai state realizzate negli uffici di back office delle aziende energetiche globali e sono divenuti **uno standard di settore.** Tuttavia, le limitazioni inerenti alla tecnologia e alle procedure attuali comportano **numerosi post-trade processes, insieme** ai relativi costi di lavoro e di tempo necessari. A causa di queste limitazioni, il back office resta carico di **attività volte alla riconciliazione, convalida, controllo e cybersecurity.**

Il design di Interbit, basandosi sulla Blockchain permetta la c**reazione di record immutabili,** di favorire **l'automazione** e di **garantire la validità dei dati** inseriti nelle transazioni, di ridurre o eliminare gli **oneri attuali** previsti. Interbit grazie al fatto che essa **unisce** le fasi della **conferma di una transazione** con il momento **dell'inserimento** e della **registrazione**

[70] Materiale Marketing Otonomos

della stessa in un record, si elimina totalmente la necessità di una riconciliazione post-trade e si protegge dall'errore umano e dalle intercettazioni della corrispondenza. Ciò consente di aumentare notevolmente i volumi di negoziazione, ridurre il rischio di credito, ridurre i costi e di aggiungere preziose funzionalità quale l'aggiunta di nodi di controllo o di regolamentazione.

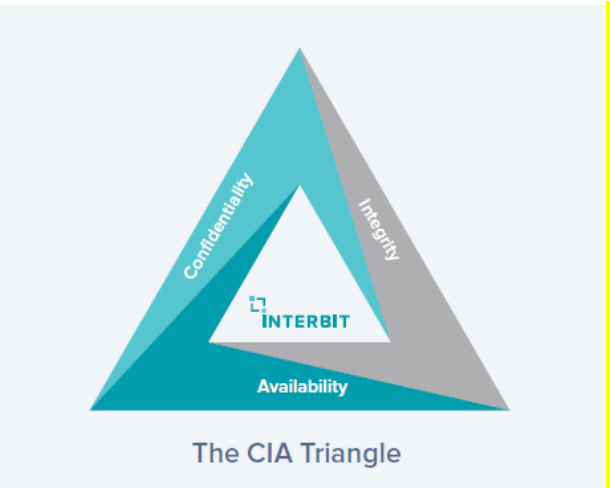
L' obiettivo del pilota è stato dimostrare che la Blockchain possa abilitare un processo di conferma di processi di back office automatico catturando le informazioni e restituendole così come i sistemi di Energy Trade e Risk Management delle singole società fanno oggi, aggiungendo le feature Blockchain già elencate. Dal pilota sono emersi interessanti risultati come ad esempio:

1. Il raggiungimento dell'80% del livello di automazione raggiungibile rispetto agli attuali sistemi.
2. Abilitazione di un Trading Matching istantaneo
3. Fornitura di un Real time reconciliation delle dedashboard dei dati
4. Elevata Sicurezza

Per poter elaborare un framework necessario alla base dello sviluppo e dello scaling della soluzione con il fine di garantire la sicurezza e la privacy dei dati senza intaccare l'operatività, la velocità e l'interoperabilità è stato utilizzato il cosiddetto CIA Triangle basato su tre driver:

a. Data Confidenzialità: la sicurezza che i dati sono salvati nel sistema blockchain ai quali non possono accedere utenti o sistemi non autorizzati
b. Data Integrity: esso si basa su due parametri, quali l'accuratezza e la consistenza dei dati, i dati saranno più integri quanto più sarà alta la loro accuratezza e la loro consistenza. I dati non potranno essere modificati da soggetti o sistemi non autorizzati.
c. Data Availability: la disponibilità dei sati del sistema, anche in situazioni critiche come Malware ed altre circostanze straordinarie.

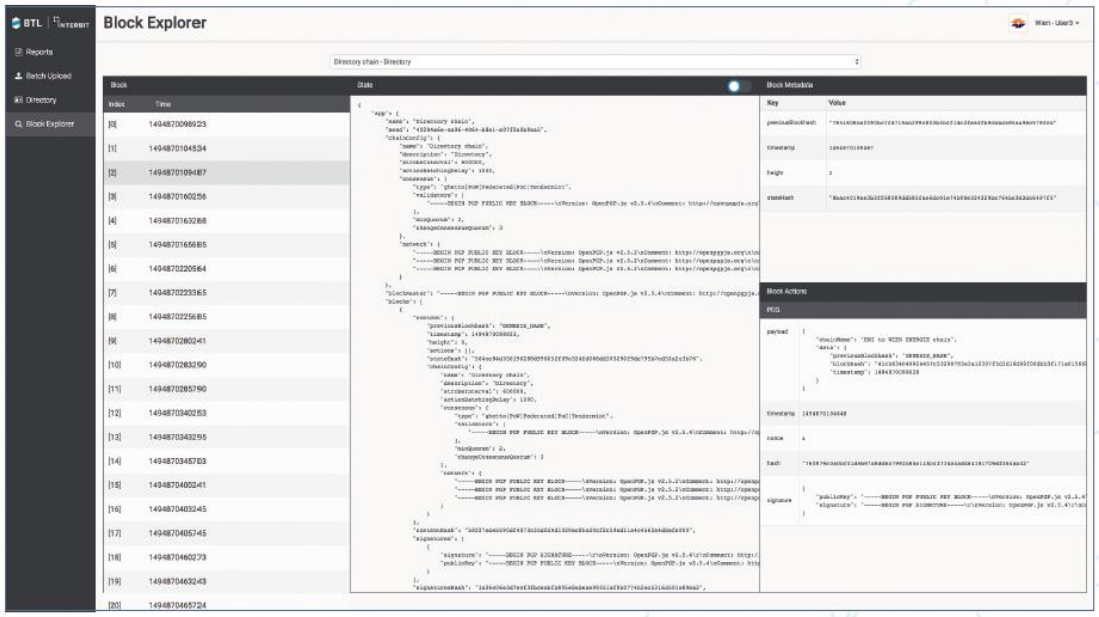
Figura 57 CIA Triangl[71]e



La soluzione creata da BTL si basa sulla gestione dei **nodi** partecipanti alla rete tramite dei server all'interno **di un ambiente cloud.**

La soluzione finale **verrà integrerà all'interno dei sistemi di Energy Trade e Risk Management** (ETRM) per **l'update automatico delle transazioni** con una transazione smooth al nuovo sistema senza cambi invasivi nell'operatività **attuale**.

Figura 58 Demo - Overview Platform Automation[72]



[71] Materiale Marketing Otonomos
[72] Ibidem

La soluzione può portare ulteriori vantaggi ai suoi attori, come ad esempio:

- Eliminazione costi di intermediazione di terze parti: riduzione dell'utilizzo di applicativi di terze parti grazie alla possibilità di sviluppare smart contract collaborativi sulle proprie Blockchain
- Riduzione significativa di costi di sviluppo e delivery di software: sviluppando su Interbit, i developer di applicazioni aziendali non devono preoccuparsi di audit, ridondanze, backup, sicurezza o reti nel codice applicativo. Lo sviluppo su Interbit è limitato allo sforzo necessario per sviluppare la logica di business per l'applicazione e l'interfaccia utente.
- Riduzione della duplicazione dei task: la conferma delle transazioni di brokeraggio energia può essere ottenuta su Interbit, grazie ad un meccanismo di consenso tra controparti e broker, eliminando la necessità di riconciliazioni separate e frequenti
- Fatturazione tempestiva e accurata: i dettagli di fatturazione possono essere inseriti dentro Interbit e notarizzati all'interno della Blockchain, eliminando la necessità di traffico email. Il processo può essere automatizzato mediante l'utilizzo dii smart contract per effettuare la creazione di fatture in automatico a seguito di un rapporto di tipo commerciale tra le parti della transazione.
- Netting di fatturazione efficiente: non sarà più necessario eseguire conferme e accordi per il settlement di fatture tramite email ma La Blockchain in automatico provvederà ad effettuare il netting tra fatture.
- Fatturazione sicura: vista la possibilità di confermare le fatture ricevute direttamente sulla Blockchain, si elimina il cyber-rischio di intercettazione e alterazione di queste informazioni tramite lo scambio di corrispondenza email o fisico
- Riduzione costi di audit: gli auditor possono avere un nodo sulla Blockchain per l'accesso ai dati di cui hanno bisogno invece che procedere con attività time-consuming come richiedere documenti
- Riduzione dei costi di reportistica: la produzione di materiale certificativo dalla Blockchain è garantita by-design tramite anche la condivisione di hash registrati

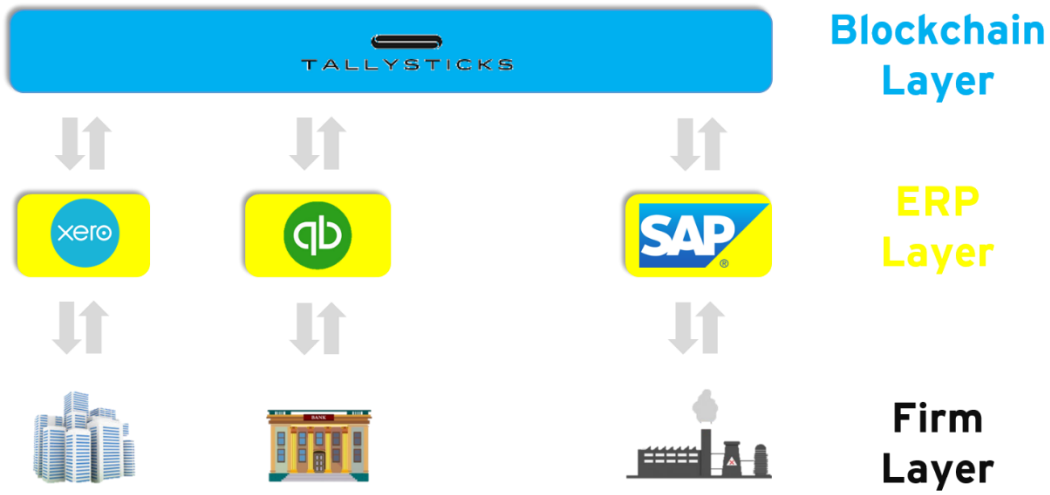
in Blockchain e sempre verificabili. È possibile affidare un nodo ai regolatori per un controllo immediato come per l'audit

- AML reporting automatico: report sulle attività sospette relativamente alla provenienza del denaro che possono essere generati direttamente dagli smart contract in automatico in base a dei trigger predefiniti o periodicamente
- Privacy: la privacy è garantita by design dalla tecnologia Blockchain nonostante la conferma delle transazioni avvenga da parte di tutto il network
- Immutable audit trail

4.4. Tallystic[73]

Tallystic è un plug in add-on per i sistemi **ERP**, grazie al quale è possibile minimizzare gli errori durante il **processo di fatturazione**, ridurre i costi relativi alla revisione, diminuire il **fabbisogno finanziario e del capitale circolante** ed infine induce una maggiore sicurezza nelle transazioni.

Figura 59 Tallystic Layers System[74]



Essa è una piattaforma che fa da **tramite tra le diverse soluzioni dei vendor**, anche tra piattaforme di vendor differenti, in modo tale da permettere di **effettuare delle interfirm operations** in modo **automatico, real-time e senza intermediari.**

[73] https://tallysticks.io/
http://treasurytoday.com/2017/01/invoice-financing-reimagined-ttff
https://www.youtube.com/watch?v=X7NZGk3V6js&pbjreload=10
Blockchain Technology and Applications from a Financial Perspective, Unicredit, Technical Report Version 1.0 Data & Analytics February 26, 2016

[74] Rielaborazioni Materiale Tallystic

Figura 60 Firm Transaction - Tallystic Demo[75]

Tallystic propone **due diverse soluzioni in Blockchain** implementabili presso le aziende.

a. **Tallystic Invocie Automation:** è una soluzione che permette di **efficientare tutto il ciclo dell'invoicing**, partendo dalla sua generazione, al suo invio, passando dalla ricezione e pagamento fino alla sua riconciliazione.
b. **Tallystic Invoicing Finanncing and exchange**: essa è una **soluzione nell'ambito del Invoice Financing.**

Possiamo riscontrare **diversi vantaggi nell'applicazione della soluzione** di Tallystic alle imprese in quanto **permette la connessione dei loro database** e alle loro informazioni al **network** al fine di **gestire la condivisione** delle stesse in base agli accordi tra le parti. Tra questi **possiamo riscontrare:**

a. **Immutàbilità dei records**
    a. **Registro dei dati storici** relativo alle transazioni effettuate con valenza legale
    b. Overview in **real-time dei dati finanziari** della società
b. **Distributed application**
    a. Invio automatico delle **fatture e dei aggiustamenti** ai network partners

[75] https://www.youtube.com/watch?v=o_t7F9VoXow

b. Riduzione di costi, errori e frodi mediante l'utilizzo di informazioni legate al processo di **invoicing codificate e quindi non leggibili**

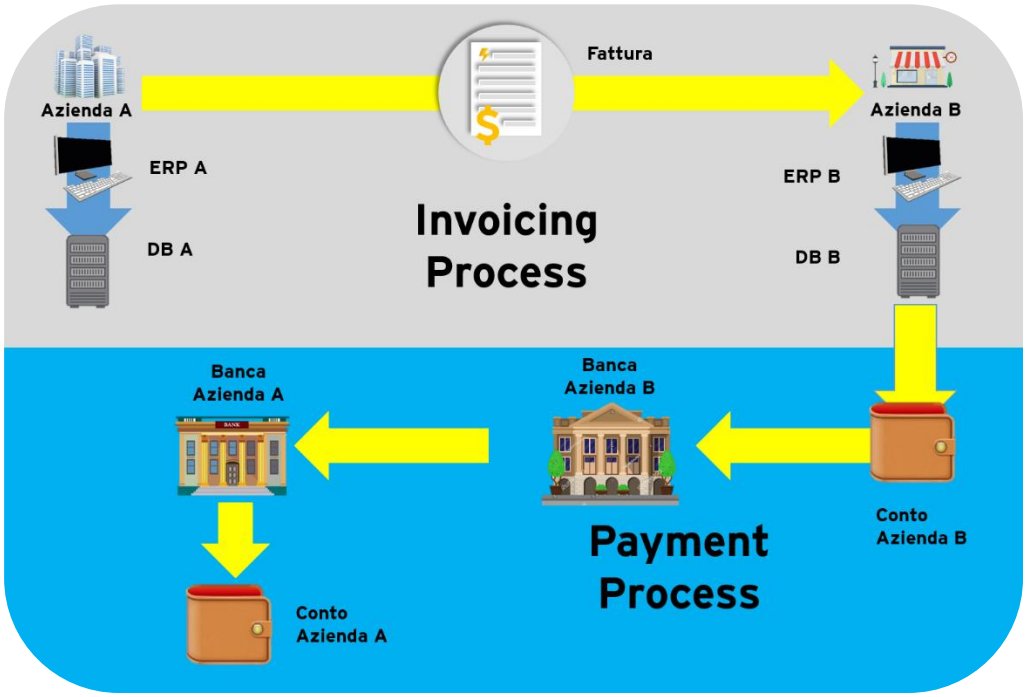
c. **Sicurezza**
   a. Condivisione sicura della visualizzazione ed accesso dei dati a soggetti terzi come **revisori, entità regolatori ed investitori**
   b. **Trasmissione e conservazione** in modo sicuro dei **dati sensibili**

d. **Compliance**: essa è una piattaforma che supporta le aziende e gli enti istituzionali a **migliorare la propria corporate governance, le** loro prassi di **internal Auditing e la loro adeguatezza alle norme vigenti**.

The Invoice Automation[76]

La maggior parte delle aziende **gestisce il loro processo di invoicing** tramite **l'emissione e l'invio delle fatture in pdf** o in formato **cartaceo**, la quale verrà registrata nei propri **ERP**, in attesa che la **controparte liquidi** il compenso e **provveda al pagamento.**

Figura 61 Invoice Process AS- IS [77]



[76] https://www.youtube.com/watch?v=lisL_5d4fSU

[77] Rielaborazione Materiale Marketing

Nel sistema attuale possiamo riscontrare diversi punti che **possono essere migliorati tramite l'utilizzo di Tallystic,** ad esempio si potrebbe:

a. Introdurre un **formato standard ed unico per le fatture** in modo da diminuire il rischio di rigetto o il delay nel working capital
b. **Prevenire le frodi sui pagamenti** verso società detenute da soggetti decisori dell'azienda
c. Processo che produca un **sistema di invoicing immutabile** al fine di migliorare l'efficienza operativa dell'azienda
d. Eliminare **l'accidentale doppia accettazione e pagamento** doppio delle fatture tramite il tracking e le riconciliazioni delle fatture e dei pagamenti
e. Abilitazione della **ricezione di pagamenti multipli** in maniera **simultanea**
f. **Eliminare gli errori effettuati durante l'introduzione dei dati** relativamente alle fatture ed al loro pagamento.
g. Eliminazione delle **riconciliazioni manuali o semi manuali**

Secondo le stime effettuate le imprese che applicano la soluzione di Invoice Automation hanno una **diminuzione dei costi tra il 2% e il 9%.**

Figura 62 As -Is Vs Tallystic To- Be[78]

	As- Is	Tallystic
Doppio Pagamento e Fatturazione	0,30%	0,06[79]
Sicurezza	0,80%	0,80%
Auditing	0,05%-0,09%	0,03%-0,05%[80]
Frodi interne	1% - 2%	0,2% - 0,4%[81]
Compliance	0,25	0,05[82]
Debiti	0,3	0,06
Totale	4,5% - 11,75%	2,56% - 3,03%

[78] Rielborazione dati da fonti Multiple: Grant Thornton, Gartner Group, TallysticksDeutsche Bank, Center for Strategic and International Studies, Association of Certified Fraud Examiners, , E&Y, Audit Analytics, Institute of International Auditors
[79] Riduzione secondo la legge paretiana dell'80/20
[80] Riduzione Approssimata al 50%
[81] Riduzione secondo la legge paretiana dell'80/20
[82] Riduzione secondo la legge paretiana dell'80/20

La soluzione abilita[83]

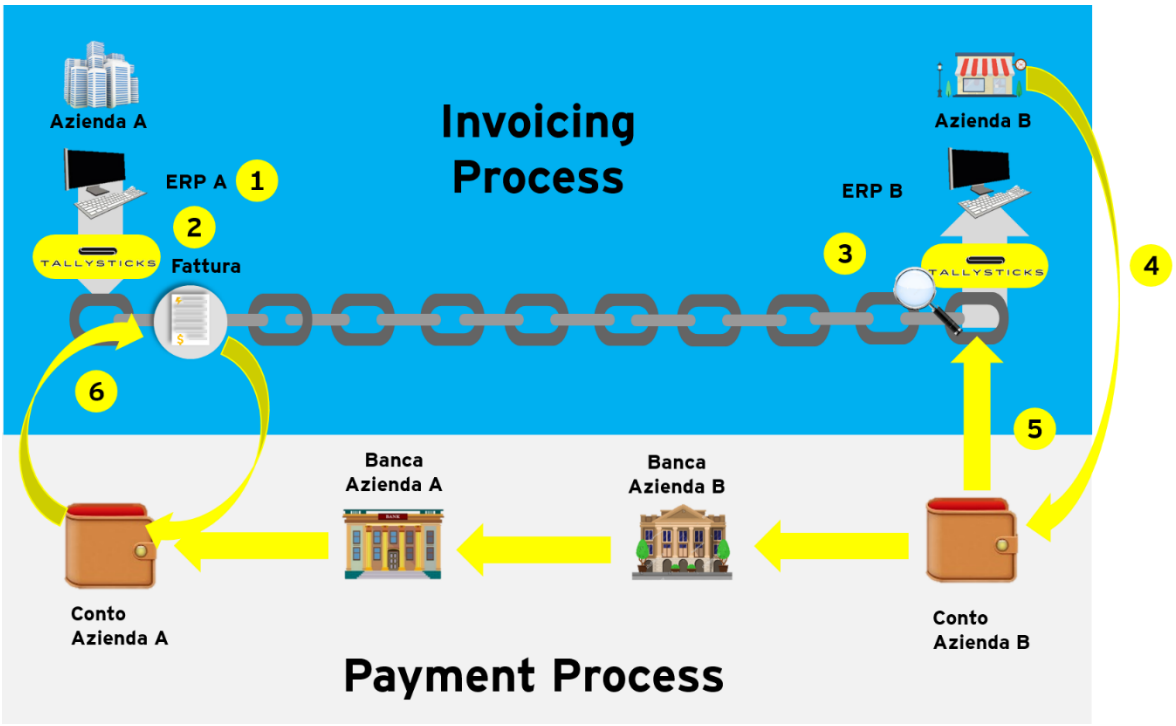
a. La registrazione di record immutabili che permettano di stabilire la fiducia tra gli attori del network e anche verso soggetti terzi
b. Una visione di overview e di dettaglio sulla situazione finanziaria
c. Riduzione del fabbisogno finanziario necessario a coprire le variazioni di working capital
d. Limitazione della possibilità del dipendente di effettuare frodi relativamente ai pagamenti

Il processo disegnato da Tallystic per l'invoicing process si articola in differenti fasi:

1. Il fornitore registra la fattura nel suo sistema ERP relativa alla vendita effettuata con la società
2. Il sistema ERP è collegato alla Blockchain ed in automatico le fatture vengono caricate su di essa
3. La fattura appare nella Blockchain ed essa è visibile all'acquirente
4. L'acquirente definisce le modalità di pagamento ed effettua lo stesso
5. Il pagamento viene registrato nella Blockchain
6. Vi è una riconciliazione automatica del pagamento con la fattura

[83] https://www.youtube.com/watch?v=YIH4MJf6kH8
https://www.youtube.com/watch?v=X7NZGk3V6js

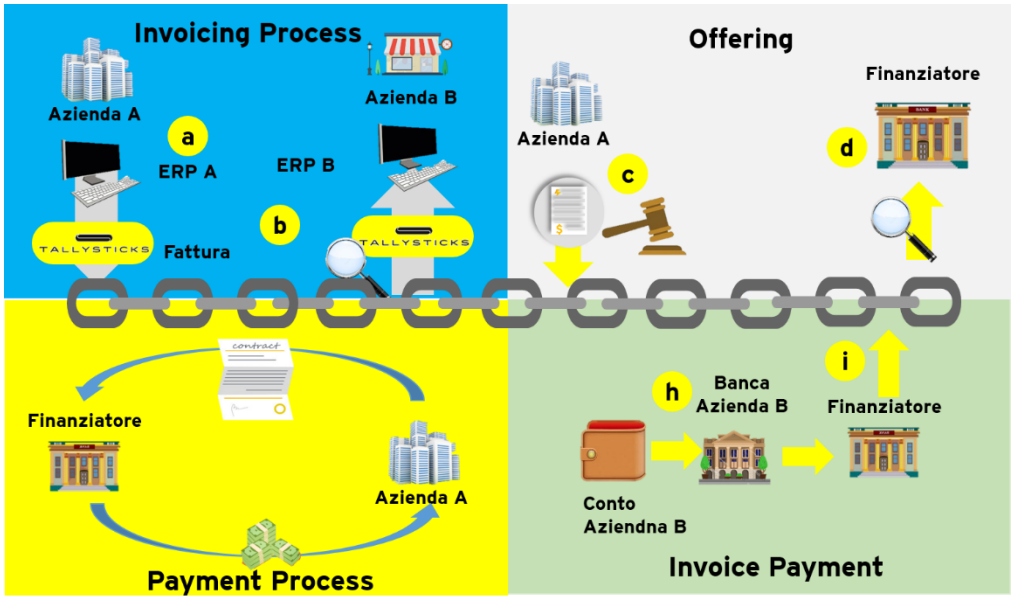
Figura 63 Tallystic System for Invoice Process



Tallysticks Invoice Financing and Exchange

Un grande problema delle aziende è quello legato **alla gestione del fabbisogno** generato dalla **gestione del capitale**, le imprese aderenti al network possono tramite la piattaforma **farsi finanziare e scambiare le fatture**.

Figura 64 Tallystic Invoice Financeing & Exchange Solution



Per analizzare l'uso della piattaforma possiamo analizzare il case di un fornitore che vende la sua fattura ad una istituzione finanziaria per avere dei fondi. Il processo sarà articolato in questo modo:

a. Il fornitore vende il prodotto o il servizio al suo cliente, per questo rapporto viene emessa una fattura che viene registrata nella Blockchain in automatico
b. Il Cliente può vedere sulla Blockchain la fattura e se contiene tutte le informazioni secondo la loro pattuizione approva la fattura e viene notarizzata
c. Il fornitore può vendere la sua fattura proponendola sulla piattaforma ad un prezzo scontato ad un Istituzione Finanziaria
d. L'istituzione finanziaria vedrà l'offerta e per ognuna di esse sarà presente un prezzo scontato, una data di inizio e una di fine[84]
e. Al momento d'acquisto il fornitore avrà una notifica per l'avvenuto acquisto. Il rapporto tra le due parti sarà regolato in automatico da uno smart contract che conterrà tutte le informazioni e le clausole previste, le quali saranno rese dallo stesso auto eseguibili.
f. Al momento della data di inizio lo smart contract abiliterà il pagamento del finanziatore verso il fornitore. A seguito della quale il fornitore riceverà il pagamento e l'istituto finanziatore una conferma di pagamento.
g. A fronte del pagamento vi sarà un passaggio di proprietà della fattura che passerà al finanziatore. Il passaggio verrà notarizzato nel registro distribuito e porterà la registrazione automatica della fattura in capo al finanziatore
h. Quando il cliente sarà pronto a pagare verrà mandato un pagamento alla banca del finanziatore.
i. Il cliente, il fornitore e il finanziatore riceveranno una conferma automatica
j. Quando lo smart contract troverà la registrazione dell'avvenuto pagamento risolverà le obbligazioni relative alle parti

Da questa soluzione possiamo evidenziare diversi vantaggi, come ad esempio:

a. Nel interest rate è compreso una quota che va a coprire la Credit protection

[84] Data nella quale se il cliente non ha pagato il fornitore dovrà dare indietro al finanziatore la somma data

b. Il **merito creditizio** può essere **attribuito automaticamente** con algoritmi basati su I **dati immutabili raccolti nelle scorse transazioni.**

c. Permette **l'automazione di diversi processi** a carattere amministrativo come **l'organizzazione del finanziamento, i pagamenti ed i settlement.**

Figura 65 Costi Associati all'invoicing financing[85]

	Media del Settore	Tallystic
Costo dei Legali	100 - 500	0
Credit Protection Fee	0,5% - 2%	0,00%
Financing Cost	1,5%-4%	1,5%-4%[86]
Costo del Servizio	0,5% - 2,5%[87]	0,5%[88]
Invoice Discounting	0,2% - 1%[89]	0,25%[90]
Totale	3,2% - 10%	2,5% - 5%

Secondo le stime effettuate, le imprese che applicano la soluzione di **invoice Financing** avranno una **diminuzione dei costi tra il 0,7% e il 7,5%.**

[85] RBS, www.http://moneyfacts.co.uk, www.nibusinessinfo.co.uk, Tallysticks.io
[86] Include Protection Fee
[87] Della Fattura
[88] della fattura
[89] della fattura
[90] della fattura

4.5. Osservazioni Finali

In questo Capitolo sono stati esaminati differenti esperienze in ambito Blockchain. Dalla disamina dei loro test o dalle loro applicazioni in contesti di on going è emerso che la tecnologia Blockchain può essere applicata alle aziende per migliorare la corporate governance, l'auditing e l'accounting, grazie alla trasparenza delle sue informazioni, alla immutabilità dei dati ed alla sicurezza delle sua infrastruttura.

La prima start up che è stata studiata è Otonomos, essa permette creare e gestire in Blockchain una società. Essa è stata già applicata da differenti società di piccola e media dimensione con ottimi risultati nell'efficientamento dei processi e nell'organizzazione aziendale. I risultati migliori sono stati ottenuti con l'applicazione alle imprese che sono nate interamente in Blockchain, in quanto sin dall'anno zero hanno potuto godere dei benefici apportati dalla soluzione. Il problema principale relativo alla sua applicazione è che la nascita dell'imprese non è sempre equiparata a quella "analogica", in quanto solo in poche nazioni vi è stata l'equiparazione totale. Relativamente alle altre funzioni vi può essere una piene applicabilità, in quanto vanno influire funzioni interne e quindi non si incontrano con vincoli di tipo normativo.

La successiva esperienza esaminata è quella nata dalla collaborazione tra BTL, British Petroleum, ENI e Wien Energy. Essi hanno testato la tecnologia Blockchain per esaminare la possibilità di potere costruire su di essa un sistema di riconciliazione trade-by-trade (near real-time) ed l'applicazione della stessa piattaforma al back office aziendale. I risultati ottenuti da questa applicazione sono fortemente positivi in quanto si è riscontrato:

a. Implementazione di una riconciliazione in real time
b. Raggiungimento di una elevate Sicurezza nei dati scambiati
c. Creazione di P2P Trading Matching in real time
d. Il livello di automazione che possono raggiungere le imprese che applicano il Sistema è pari a circa l'80%

Il terzo caso approfondito è quello di Tallystic, su di essa ancora non vi sono notizie riguardanti il risultato di test su aziende. Analizzando le sue funzioni possiamo evidenziare differenti vantaggi di una sua applicazione, come ad esempio:

a. Diminuzione degli errori durante l'articolato ciclo di fatturazione
b. Riduzione dei costi legati all'auditing
c. Ridurre del cashflow per soddisfare fabbisogno finanziario per il capitale circolante
d. Creazione di un ambiente trusted in una situazione con diversi attori con interessi contrapposti

Di seguito la tabella riepilogativa delle funzioni esaminate nei singoli use case:

	Pagamenti e Riconciliazioni	Smart Contracts	Contabilità	Capital Market Service	Trade Finance
Otonomos		x	x	x	
BTL	x	x	x		
Tallystic	x		x		x

5. Conclusione

L'obiettivo che ci siamo posti all'inizio di questo documento era quello di **esplorare** le **innovative e variegate opportunità** proposte dalla **Blockchain** al mondo **aziendale** e nello **specifico** quelle attinenti all'area della **Corporate Governance, dell'Accounting a dell'Auditing.** Alla luce dell'analisi condotta possiamo affermare che la tecnologia Blockchain **è altamente adatta all'implementazione nel mondo aziendale**, il quale essendo molto **variegato** e con particolari necessità verticali necessita di una tecnologia che sia flessibile, interoperabile, trasparente, automatizzata e tamperproof: **La Blockchain.**

La Blockchain avrà un **impatto notevole non solo nelle aree Corporate Governance, dell'Accounting a dell'Auditing** ma sarà una **rivoluzione cross industry.**

Figura 66 Industry Interessate dall'innovazione della Blockchain

Analizzando **le esperienze della Blockchain** in ambito **corporate governance, accounting ed auditing**, possiamo **ravvisare 5 aree di prossimo sviluppo della Blockchain** in ambito aziendale:

a. **Pagamenti e Riconciliazioni:** tutte le aziende **necessitano** di effettuare i **pagamenti** ai loro **fornitori** per approvvigionarsi delle materie prime, ma molto spesso i **sistemi attuali necessitano di molti task manuali** o semi manuali, **spese amministrative**, incertezze sull'adempimento della controparte. Per queste

ragioni l'impatto della Blockchain sarà elevato ed inoltre visto la maturità tecnologica della soluzione sarà possibile applicare la Blockchain agli stessi già adesso, raggiungendo in circa 3 anni la posizione di standard per i pagamenti nel settore finanziario e bancario, per poi entro 5 anni diventare uno standard di settore orizzontalmente per tutte le industry.

b. Smart Contracts: gli smart contract permetteranno di automatizzare delle azioni da attuare a seguito dei trigger selezionati ed in base a delle regole precedentemente definite tra le parti Lo stato attuale della tecnologia permette l'applicazione dello smart contract, ma il problema al momento attuale alla sua applicazione è la modalità del riconoscimento del trigger stesso, in quanto al momento attuale gli elementi che potrebbero essere trigger non sono completamente digitalizzati e quindi difficilmente connettibili alla Blockchain ed ai suoi smart contracts. Quindi al momento è applicabile su grande scala solamente ad trigger digitalizzati oppure su casi singoli anche su trigger più o meno digital native. La sua maturità può essere raggiunta in 3 – 5 anni, momento in cui vi sarà una applicazione su vasta scala in diversi ambiti grazie alla digitalizzazione delle fonti informative necessarie ad attivare i trigger, in quel momenti visto le multiple possibilità d'applicazione si avrà un grande impatto.

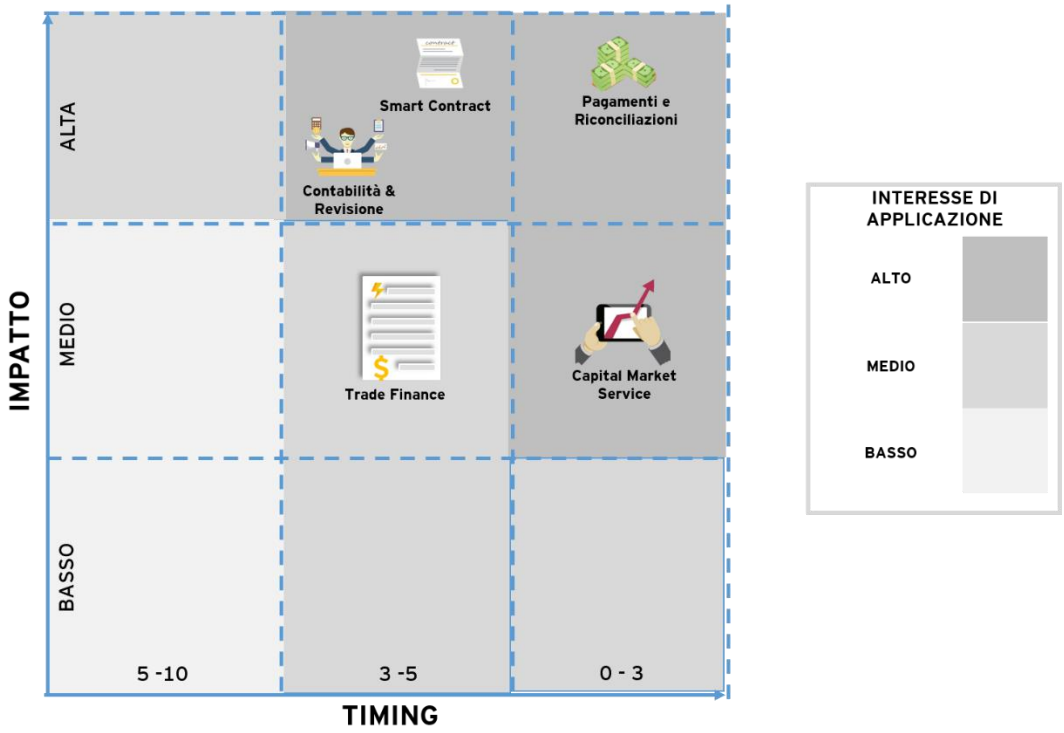
c. Contabilità e Revisione: l'attuale sistema contabile produce un duplicato per ogni scrittura creata, di conseguenza **duplica anche la possibilità di produrre errori ed imprecisioni, la probabilità di manomissioni o alterazioni**. Questi elementi sono ineliminabili in un sistema basato sul double ledger ma sono eliminabili in un sistema fondato sul triple ledger system. L'introduzione di quest'ultimo modello porterebbe un grande efficientamento nel sistema permettendo scritture e riconciliazioni tra le stesse in maniera unitaria e per tutte le parti nella transazioni, in near real-time, sicure e tamper proof. La sua struttura si baserà sui sistemi attualmente esistenti come i sistemi ERP, comprenderà il linguaggio XBRL (standard informatico del linguaggio contabile), le informazioni e i documenti verranno notarizzati nella Blockchain

e verranno in sistemi di storage distribuiti come IPFS. Questa applicazione avrà un forte impatto sull'economia, in quanto la tenuta delle scritture contabili è obbligatoria per legge ed necessaria per la definizione della tassazione per le società ed è una delle fonti della contabilità interna. Li elementi alla base della soluzione hanno una maturità tecnologia abbastanza consolidata e quindi potrebbero essere applicati nel breve periodo. L'audit invece avrà un timing d'applicazione più lungo in quanto necessita per poter essere implementata che la Blockchain sia prima applicata all'Accounting per utilizzarla come fonte sicura dei propri dati. L'applicazione della Blockchain all'audit potrebbe cambiare totalmente il processo rispetto a come è fornito attualmente. In un primo momento la Blockchain andrà a supportare il revisore permettendo la verificare l'originalità dei documenti, successivamente gli permetterà di vedere in real time le transazioni che avverranno tra i soggetti fino ad arrivare alla sua sostituzione nella verifica degli elementi contabili.

d. Capital Market Service: I servizi migliorati o creati in questo ambito dalla blockchain hanno un elevato potere disruptive ma probabilmente avranno solamente una influenza media sull'economia, in quanto alcune constrain legislative mitigheranno l'effetto positivo da loro offerto, il corpus legislativo di molti paesi non è pronto a recepire grandi sforzi innovativi, pur essendo già lo stato dell'arte della tecnologia pronto a supportare in maniera piena l'evoluzione degli stessi. Per queste ragioni è possibile classificarla con impatto medio e nel timing di 0-3 anni.
e. Trade Finance: l'innovazione del trade finance porterà un grande valore aggiunto all'aziende permettendo così di diminuire il delay finanziario dovuto ai pagamenti e inoltre permette di eliminare il rischio di effettuare una prestazione e di non essere pagato per essa, in quanto la somma predisposta per il pagamento della suddetta prestazione sarà congelata finché entrambe le parti non assolveranno alle loro obbligazioni. Essa avrà un impatto medio in quanto andrà a coprire i spazi lasciati liberi dalla protezione contrattuale fornita dagli accordi tra le parti. La sua implementazione sarà possibile nel breve

periodo e in circa 5 anni sarà uno standard per tutte le industry nelle transazioni per le diverse aziende. Un ulteriore elemento abilitato dalla blockchain è la possibilità di vendere oppure di usare come garanzia le fatture emesse verso i clienti, in una piattaforma decentralizata e disintermediante, ciò permette di fornire un mercato più fluido alle fatture e quindi di permettere un accesso agevolato al credito alle imprese con fatture non ancora pagate. L'impatto sull'economia sarà di tipo medio e la sua possibile implementazione richiederà circa 3-5 anni, in quanto per il suo utilizzo è necessario che sia sin da subito una soluzione di sistema insieme alle altre imprese del settore.

Figura 67 Impatto e Timing dell'applicazione della Blockchain in ambito CG, Accounting e Audit



Confrontando il risultato delle ricerca sui differenti ambiti di applicazione nel settore della Corporate Governance, dell'Auditing e dell'Accounting si può notare che tutti gli ambiti di applicazioni sono indirizzati nei quadranti con impatto medio ed alto e con timing 0-3 anni e 3-5 anni, queste combinazioni denotano un interesse medio ed alto all'applicazione della Blockchain in questi ambiti aziendali.

Avendo avuto la possibilità di esaminare il **sentiment del top management della più grandi imprese italiane**, grazie a **questionari**, agli **incontri e call conference** effettuate nella mia veste di **consulente in ambito Blockchain Technology** e membro del **Blockchain Hub per l'area MED per Ernst & Young**, posso sottolineare diversi elementi quali ad esempio:

a. **Più della metà** del top management italiano **conosce tematiche** attinenti alla blockchain e **sono interessati a studiarne le applicazioni** nella loro realtà
b. Sono ritenuti come più soggetti ad impatto **i settori del Banking & Insurance e dell'energy**
c. Gli use case ritenuti **più interessanti** sono quelli delle **finacial transaction** e quelli relativi alla **supply chain**
d. Ritengono che la tecnologia Blockchain possa principalmente **diminuire i costi di transazione** ed **abilitare la creazione di nuovi business model**
e. La Blockchain è vista principalmente come un **game changer** o adatta ad **applicazioni di nicchia ad alto valore**
f. Vedere come **elementi limitanti l'applicazione** della tecnologia le **normative stringenti** e la **"giovinezza" della tecnologia stessa.**
g. La **promozione della collaborazione** tra le **aziende del settore per il design** e **l'implementazione delle soluzioni** in ambito Blockchain **più efficaci** e con un **maggiore impattatto.**

Unendo i suddetti elementi **si può evincere che anche l'Italia sarà presto un attore del panorama mondiale** nelle applicazioni della **tecnologia Blockchain,** anche se pur con un **leggero ritardo rispetto alle altre realtà nazionali europee** come la Svezia e l'Estonia.

In un futuro non troppo lontano la Blockchain **potrebbe entrare in molti degli aspetti delle nostre vite**, portando **trasparenza**, **sicurezza** ed **efficienza**, aprirà le porte verso una nuova era: **la Blockcracy**[91].

[91] https://www2.deloitte.com/de/de/pages/strategy/articles/future-of-blockchain-en.html
Future of Blockchain, Florian Klein, Deloitte, 2017
Blockchain @ Rethinking banking: A view on how blockchain can change banking, Frank Thiele, Dirk Siegel, Blockchain Istitute, Deloitte, 2017

In questa direzione si stanno muovendo differenti governi, ma in particolare il **Governo di Dubai** si è posto come obiettivo da raggiungere en**tro il 2020 di diventare il primo Blockchain Powered Governament del mondo**. [92] La sua strategia è basata essenzialmente su 3 pillar:

a. **Government Efficiency: il** primo pillar della strategia è relative al miglioramento dell'efficienza del governo, ad esempio tramite l'introduzione di un **paperless digital layer** per tutte le transazioni all'interno della città sia pubbliche che private, andandosi a raccordare con tutte le altre iniziative della smart cities. Attualmente vi è un forte uso dei documenti cartacei come per esempio per i visti, ricevute di pagamento, rinnovi di license, i quali producono circa 100 milioni di documenti ogni anno, utilizzando la Blockchain si potranno risparmiare circa 114 Milioni di Tonnellate relative alle emissioni di CO2, circa 25.1 millioni di ore di lavoro per produrli e gestirli.
b. **Industry Creation:** creerà un Sistema che **abiliterà i cittadini e i partner ia creare nuovi modelli di business** usando la tecnologia Blockchain sia nel settore privato e sia nel settore pubblico, diversi settori ne beneficeranno, quali ad esempio: real estate, fin-tech, bancario, assicurativo, sanità, trasporti, energetico, commercio digitale e il turismo.
c. **International Leadership:** Dubai **permetterà l'accesso alla piattaforma** Blockchain per le controparti Mondiali per **potenziare, rendere sicuri e più convenienti I viaggi a Dubai.**

La Blockchain creerà un mondo più **trasparente**, incentiverà la **globalizzazione**, I **liberi scambi**, sarà l'antidoto per la stagnazione e di support per le crisi politiche, efficienterà le **transazioni finanziarie**, permetterà la gestione in maniera unitaria dei **dati** sanitari e personali del **cittadino**, abiliterà il **peer-to-peer dell'energia**, tutto ciò **porterà verso una crescita e nuovi posti di lavoro**. Agli **attori** non resta che scegliere se vogliono essere

[92] https://www.ibm.com/blogs/blockchain/2017/04/blockchain-in-dubai-smart-cities-from-concept-to-reality/
http://www.smartdubai.ae/dubai_blockchain.php

anche loro i protagonisti nella guida della rivoluzione o rimanere inermi ed essere gli spettatori passivi del cambiamento.

6. Bibliografia e Sitografia

EY Italy Blockchain Hub, Claudio Meucci, Giuseppe Perrone, Mariano Guzzetta, Gerardo Gabriele Volpone, Adriano Gimmelli, Gianlorenzo Simonazzi, Giuseppe Diego Mulè, 2017

"Tech Trends 2017: The Kinetic Enterprise", Deloitte University, 2017

"Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world", Don Tapscott, Alex Tapscott

"Blockchain: blueprint for a new economy", Melanie Swan, 2015

"Blockchain: back office block buster", Otonomos

"Blockchain: democratised trust", Eric Piscini, Joe Guastella, Alex Rozman, Tom Nassim, 2016

"Embracing disruption tapping the potential of distributed ledgers to improve the post-trade landscape", dttc, 01/2016

"Distributed ledger technology: beyond block chain", uk government chief scientific adviser, Matthew Hancock, Ed Vaizey

"Bitcoin: A Peer-to-Peer Electronic Cash System", Satoshi Nakamoto, 2008

"Technological Disruption of Capital Markets and Reporting? An introduction to Blockchain", Charted Professional Accountants of Canada, 2016

"Blockchain and its coming impact on Financial Services, Kurt Fanning, David P. Centers, ER The Journal of Corporate Accounting and Finance, 2016

"Blockchain Hitting the big Time, but is Ready?", Frontiers in Finance: for decision-maker in financial services, J. Cassidy, E. Maguire, D. Montes, 2016

"Bitcoin, Blockchain & Distribted Ledger: Caught between promise and reality, P. Evans-Greenwood, R. Hilard, I. Harper, P. Williams, Deloitte Australia

"Mastering Bitcoin - Second Edition", Andreas M. Antonopoulos, in pubblicazione

"The Byzantine Generals Problem", Leslie Lamport, Robert Shostak, and Marshal Pease

"Deep Shift Technology Tipping Points and Societal Impact: Global Agenda Council on the Future of Software & Society" Survey Report, World Economic Forum, September 2015

First Monday, Vol 2 N 9, Nick Szabo, 1997

The Land Registry in the Blockchain – testbed: a development project, Lantmäteriet, andshypotek Bank, SBAB, Telia Company, ChromaWay and Kairos Future
European Banking Authority, "EBA Opinion on 'virtual currencies'", European Banking Authority Opinion, 4th July 2014.

Britto A. et al., "The Ripple Protocol Consensus Algorithm", whitepaper, Ripple Labs Inc. , 2014.

Yoon S. Park, "The Inefficiencies of Cross-Border Payments: How Current Forces are Shaping the Future", VISA, 2008.

Barry C. et al, "Cross-Border Payments: Challenges and Trends", AITE Group report, January 2015

Knieff B., "Blockchain: What Is It Good for? Absolutely something", Aite Group report, December 2015, p. 13.

Wright A., De Filippi P., "Decentralized Blockchain Technology and the Rise of Lex Cryptographia," 2015

https://www.icbpi.it/smart-contracts-la-vera-rivoluzione-della-Blockchain/

https://blockgeeks.com/guides/smart-contracts/

http://www.Blockchaintechnologies.com/Blockchain-smart-contracts

http://www.coindesk.com/ethereum-decentralized-app-network-launch/

http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

https://www.fjordnet.com/conversations/the-trust-trade-off-permissioned-vs-permissionless-Blockchains/

https://www.ibm.com/blogs/think/2016/07/checking-the-ledger-permissioned-vs-permissionless-Blockchains/

https://etherevolution.eu

https://en.Bitcoin.it/wiki/Block

https://github.com/tendermint/tendermint/wiki/Block-Structure

https://en.Bitcoin.it/wiki/Block_hashing_algorithm

http://www.coindesk.com/sweden-moves-next-stage-Blockchain-land-registry/

http://www.coindesk.com/sweden-taking-chance-Blockchain-land-registry/

https://qz.com/947064/sweden-is-turning-a-Blockchain-powered-land-registry-into-a-reality/

http://www.financemagnates.com/cryptocurrency/innovation/sweden-tests-property-transactions-Blockchain-chromaway/

https://chromaway.com/landregistry/

https://e-estonia.com/component/electronic-id-card/

http://e-resident.gov.ee/become-an-e-resident/

http://www.wired.co.uk/article/estonia-e-resident

https://blogs.thomsonreuters.com/answerson/e-estonia-power-potential-digital-identity/

http://www.coindesk.com/deloitte-creates-Blockchain-proof-of-concept-for-tracing-artworks/

http://www.the-Blockchain.com/2016/05/18/deloitte-rolls-Blockchain-proof-concept-art-world/

http://www.wired.co.uk/article/Blockchain-conflict-diamonds-everledger

http://www.Blockchain4innovation.it/iot/la-rivoluzione-nel-fashion-passa-per-la-Blockchain/

http://www.thefashionlaw.com/home/what-is-Blockchain-and-what-does-it-have-to-do-with-fashion

http://www.managingip.com/Article/3667444/Blockchain-IP-and-the-fashion-industry.html

https://www.nytimes.com/2017/03/04/business/dealbook/Blockchain-ibm-Bitcoin.html?_r=0

https://www.provenance.org/whitepaper

http://www.ansa.it/canale_terraegusto/notizie/vino/2017/04/13/vino-arriva-etichetta-intelligente-wine-Blockchain-ey_763092ee-10d6-4155-917d-4e4e06d5de87.html

http://www.lastampa.it/2017/04/17/tecnologia/idee/lidea-di-una-startup-italiana-usare-la-Blockchain-per-tracciare-la-filiera-del-vino-QIhzYu11J5A6kZlG6gUxTP/pagina.html

https://en.wikipedia.org/wiki/R3_(company)

http://fortune.com/2016/11/21/goldman-sachs-r3-Blockchain-consortium/

http://www.statisticbrain.com/resume-falsification-statistics/

http://www.nytimes.com/2007/04/27/us/27mit.html

http://money.cnn.com/2012/05/13/technology/yahoo-ceo-out/index.htm

http://www.ilgiornale.it/news/politica/laurea-falsa-fedeli-si-auto-assolve-e-accusa-contro-me-1342771.html

Corporate Governance and Blockchain, David Yermack, 2015

Gartner Hype Cycle for Emerging Technology, 2016, Gartner

Pratical Blockchain: A Gartner Trend Insight Report, David Furlonger, Ray Valdes, Gartner, 2017

https://medium.com/@TweetFromHilary/from-ipo-to-ico-blockchains-finance-revolution-b34c46ef281b

http://investingnews.com/daily/tech-investing/fintech-investing/blockchain-technology-stocks/

https://etherevolution.eu/cose-un-blockchain-ico-perche-importante/

https://www.cryptocompare.com/coins/guides/how-does-an-ico-work/

Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: DAO, release n.81207, 25/07/2017

Trendon T. Shavers and Bitcoin Savings and Trust, SEC, Civil Action No. 4:13-CV-416 (E.D. Tex., complaint filed July 23, 2013)

Erik T. Voorhees,SEC, Rel. No. 33-9592, 03/06/2014

BTC Trading, Corp. and Ethan Burnside, SEC, Rel. No. 33-9685, 08/122014

Bitcoin Investment Trust and SecondMarket, Inc., SEC, Rel. No. 34-78282 (July 11, 2016)

SEC, Sunshine Capital, Inc., File No. 500-1, 11/04/ 2017)

Bitcoin and Other Virtual Currency-Related Investments, SEC, 07/05/2014

http://yoniassia.com/coloredbitcoin/

https://bitcointalk.org/index.php?topic=101197.0

https://coloredcoins.org

http://www.bitcoinx.org

http://szabo.best.vwh.net/idea.html

https://www.usenix.org/legacy/publications/library/proceedings/ec98/fujimura.html

https://en.bitcoin.it/wiki/Colored_Coins

https://www.draglet.com/blockchain-applications/digital-tokens/colored-coins

Colored Coins White Papere, Yoni Assia, Vitalik Buterin, Meni Rosenfeld e Rotem Lev

https://nexchange.com/article/8637

http://fortune.com/2017/03/31/initial-coin-offering/

http://www.coindesk.com/overstock-first-day-blockchain-stock-trading/

http://www.nasdaq.com/article/how-stock-exchanges-are-experimenting-with-blockchain-technology-cm801802

http://business.nasdaq.com/marketinsite/2016/Building-on-the-Blockchain.html

http://www.reuters.com/article/us-usa-sec-settlement-idUSKBN16T1SW

http://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html

https://www.lhv.ee/en/

http://www.cuber.ee/en_US/

http://www.reuters.com/article/nasdaq-blockchain-idUSL1N1FA1XK

Schedule 13 D

Art. 120 A (Partecipazioni rilevanti ex 117), 120B (strumenti finanziari e/o delle partecipazioni aggregate) e 120 C (strumenti finanziari) del TUF

http://www.investopedia.com/terms/c/corporate-raider.asp

https://www.forbes.com/sites/steveschaefer/2011/02/15/private-equity-calling-plays-out-of-corporate-raider-playbook/#6100d12941df

https://www.strategy-business.com/blog/Corporate-Raiders-and-Their-Minions-A-History?gko=2ec7f

https://www.entrepreneur.com/article/78422

https://hbr.org/1987/05/from-competitive-advantage-to-corporate-strategy

http://www.investopedia.com/ask/answers/031815/what-role-agency-theory-corporate-governance.asp

Stewardship Theory or Agency Theory: CEO Governance and Shareholder Returns, Lex Donaldson, James H. Davis

Theory of the firm: Managerial behavior, agency costs and ownership structure, Michael C.Jensen .William H.Meckling

https://www.morganstanley.com/spc/knowledge/managing-equity/understanding-your-awards/restricted-stock.html

https://www.nceo.org/articles/stock-options-restricted-phantom-sars-espps

http://www.investopedia.com/terms/r/restrictedstock.asp

http://www.menke.com/blog/how-to-structure-stock-ownership-plans-for-management-employees/

http://www.ilsole24ore.com/art/finanza-e-mercati/2017-09-04/la-cina-mette-freno-ico-bitcoin-caduta-160613.shtml?uuid=AEyvsMNC

http://www.repubblica.it/economia/finanza/2017/09/06/news/il_bitcoin_non_teme_la_cina_e_torna_a_correre-174782399/

https://www.economyup.it/fintech/la-vera-strategia-della-cina-dietro-il-bando-delle-ico-ed-il-crollo-del-bitcoin/

https://www.money.it/Divieto-ICO-in-Cina-non-uccidera-criptovalute

“State of Blockchain Q2 2017” Coindesk, 08/2017

Bitcoin and the Blockchain as Possible Corporate Governance Tools: Strengths and Weaknesses, Penn State Journale of Law & International Affairs, Fiametta S. Piazza, 07/2017

http://revfin.org/corporate-governance-and-blockchains-by-david-yermack/

Streamlining Corporate Actions Processing with Blockchain, White Paper, R. Samudrala, G. R. admnabhan Tata Consultancy Services

How Blockchain Tech Will Change Auditing for Good”, Coindesk http://www.coindesk.com/blockchains-and-the-future-of-audit/ Matthew Spoke.

“Double Entry System Bookkeeping and Accounting Explained”, Business Case Analysis, https://www.business-case-analysis.com/double-entry-system.html , Marty Schmidt.

“Cost? Trust? Something else? What’s the killer-app for block chain technology?”, Gendal Brown blog, http://gendal.me/2015/01/15/cost-trust-something-else-whats-the-killer-app-for- block-chain-technology/ , Richard Gendal Brown

The term "Triple Entry Accounting," was first used by Ian Grigg in 2005, three years before Bitcoin. http://blockchainabc.blogspot.it/p/blog-page.html

“Triple Entry Bookkeeping With Bitcoin”, Bitcoin Magazine, https://bitcoinmagazine.com/articles/triple-entry-bookkeeping-bitcoin-1392069656 , Jason M. Tyra., “If you call it a blockchain, it’s not a single-entry system”, Financial Timeshttp://ftalphaville.ft.com/2015/10/30/2143506/if-you-call-it-a-blockchain-its-not-a-single-entry-system/, Izabella Kaminska.

Knieff B., “Blockchain: What Is It Good for? Absolutely Something”, Aite Group report, December 2015, p. 13.

Blockchain Technology, A Game changer in Accounting”Nicolai Andersen, Deloitte, 03/2016

“Blockchain & Audit”, Christine Stark

“The Trust Machine”, The Economist (h t t p : / / w w w. e c o n o m i s t . c o m / n e w s /leaders/21677198-technology-behind-bitcoin-couldtransform-how-economy-works-trust-machine/)

“The great chain of being sure about things”, TheEconomist

(h t t p : / / w w w. e c o n o m i s t . c o m / n e w s /briefing/21677228-technology-behind-bitcoin-letspeople-who-do-not-know-or-trust-each-other-builddependable(

“How Blockchain Tech Will Change Auditing for Good”, M. Spoke, (https://www.coindesk.com/blockchains-and-thefuture-of-audit/)

(Deloitte Explores Blockchain Tech for Client Auditing”, P. Rizzo (https://www.coindesk.com/deloitte-blockchainauditing-consulting)

R3 (http://r3cev.com)

Rubix, Deloitte, (http://rubixbydeloitte.com)

Triple Entry Accounting (http://blockchainabc.blogspot.fr/p/blog-page.html)

Trusting records: is Blockchain technology the answer? ", Records

Management Journal, Vol. 26 Iss 2 pp. 110 – 139, Victoria Louise Lemieux , (2016),"

www.otonomos.com

https://www.youtube.com/watch?v=LAwCCi7lLcY

https://www.youtube.com/watch?v=X7n6XVSKOxc

https://www.youtube.com/watch?v=XgdRuSW0b50

http://fintank.net/2016/01/18/otonomos/

http://www.finanzprodukt.ch/fintech/otonomos-disrupting-business-incorporation-funding-and-governance-by-using-the-blockchain/

http://fortune.com/2017/08/01/blockchain-shareholders-law/

https://angel.co/projects/209838-otonomos-launches-blockchain-powered-company-dashboard

European Enerfy Pilot Exit Report, Hugh Halford Thmpson, BTL, 05/2017

http://btl.co/

http://uk.reuters.com/article/us-bp-eni-blockchain/bp-eni-deepen-blockchain-trading-in-european-gas-idUKKBN18W1N2

https://it.wikipedia.org/wiki/BP_(azienda)

https://de.wikipedia.org/wiki/Wien_Energie

https://www.eni.com/it_IT/azienda/profilo-compagnia.page

https://tallysticks.io/

http://treasurytoday.com/2017/01/invoice-financing-reimagined-ttff

https://www.youtube.com/watch?v=X7NZGk3V6js&pbjreload=10

https://www.youtube.com/watch?v=o_t7F9VoXow

https://www.youtube.com/watch?v=lisL_5d4fSU

Rielborazione dati da fonti Multiple: Grant Thornton, Gartner Group, TallysticksDeutsche Bank, Center for Strategic and International Studies, Association of Certified Fraud Examiners, , E&Y, Audit Analytics, Institute of International Auditors

https://www.youtube.com/watch?v=YIH4MJf6kH8

https://www.youtube.com/watch?v=X7NZGk3V6js

www.http://moneyfacts.co.uk,

www.nibusinessinfo.co.uk,

Blockchain Technology and Applications from a Financial Perspective, Unicredit, technical Report Version 1.0 Data & Analytics February 26, 2016

https://www2.deloitte.com/de/de/pages/strategy/articles/future-of-blockchain-en.html

Future of Blockchain, Florian Klein, Deloitte, 2017

Blockchain @ Rethinking banking: A view on how blockchain can change banking, Frank Thiele, Dirk Siegel, Blockchain Istitute, Deloitte, 2017

https://www.ibm.com/blogs/blockchain/2017/04/blockchain-in-dubai-smart-cities-from-concept-to-reality/

http://www.smartdubai.ae/dubai_blockchain.php

7. Riassunto

7.1. Osservazioni Iniziali

Le grandi aziende leader, se vogliono continuare a guidare ed innovare, non possono continuare ad ignorare la rivoluzione portata dalla Blockchain nei loro differenti ambiti, in quanto la Blockchain nei prossimi 10 anni cambierà molti settori rispetto a come li conosciamo noi oggi. Per le aziende che non si saranno adattate si potrà immaginare lo stessa sorte che hanno avuto le imprese che nei primi anni duemila non si sono adattati alla rivoluzione digitale del web, le quali sono rimaste sempre di più fuori dal settore fino ad arrivare al fallimento. Considerando i nuovi trend in ambito digital e tecnologico, che negli ultimi anni stanno caratterizzando il mercato, si possono scorgere degli elementi caratterizzanti che accomunano le tecnologie emergenti: tutte loro sono ***enabler*** di nuovi servizi. Data la presenza di questi trend, la sicurezza delle informazioni e dei dati guadagnerà nel prossimo futuro un ruolo sempre più importante, per questa ragione, la Blockchain sarà al centro dell'interesse mondiale, essendo la tecnologia che più è affine alle problematiche relative alla sicurezza, alla trasparenza, all'interoperabilità e alla privacy. Essa occuperà un importante parte del panorama tecnologico mondiale, secondo le stime del *World Economic Forum,* il protocollo Blockchain trasporterà entro il 2025 circa il 10% del PIL mondiale, grazie ai suoi elementi di ***distruption*** e di trasversalità lungo le ***industry*** e i mercati di applicazione.

7.2. Blockchain: a disruptive Technology

La tecnologia Blockchain nasce come protocollo sottostante alla criptovaluta chiamata *Bitcoin*. Nel 2009 la parola *Bitcoin* viene utilizzata per la prima volta, da ***Satoshi Nakamoto*** nel suo celeberrimo *paper* intitolato *"Bitcoin: a Peer-to-Peer Eletronic Cash System"*. Nakamoto introduce e descrive una valuta digitale, il cui scambio viene permesso senza l'ausilio di un terzo fidato, ma direttamente tra le due parti. La sua apparizione è da ricollegare molto probabilmente alla crisi del 2008, alla minore fiducia dei consumatori nelle classiche istituzioni bancarie e al modello centralizzato delle stesse. Il meccanismo attraverso cui avvengono le transazioni della criptovaluta, come già detto, è la Blockchain, essa è un registro, un libro contabile ***(ledgers***), il cui contenuto è diffuso sui nodi (*nodes*) di una rete decentralizzata (*distributed*) basata sul protocollo ***peer-to-peer***, essa viene aggiornata dai minatori (*"miners"*), i quali aggiungono i blocchi l'uno dopo

l'altro, legandoli in maniera sequenziale in base ad un ordine temporale, inserendo indelebilmente e in maniera cifrata all'interno di questi blocchi le transazioni che ricevono dagli utilizzatori del Bitcoin. La Blockchain può essere monitorata da tutti, ma al contempo non è di proprietà di alcun soggetto, in quanto essa è un database diffuso e distribuito su una rete di nodi indipendenti tra loro, quindi per modificarne o aggiungere i blocchi, servirebbe avere il controllo del 50%+1 (*Consensus*) per questa ragione non esiste un unico *single point of control*. La modalità con cui vengono aggiunti i blocchi e con cui vengono immessi nel mercato dei nuovi Bitcoin viene chiamata ***mining***, essa viene assolta dai Minatori ("*miners"*). Inoltre esso rappresenta anche il processo attraverso con cui le transazioni sono verificate ed aggiunte alla *pubblic ledger*. L'azione dei *miners* è basata essenzialmente nel risolvere problemi matematici, in base alle informazioni contenute nel blocco. I *miners* sono incentivati a svolgere questa attività dal ricevere in cambio una ricompensa. Per questa ragione, il primo *miners* che risolve il problema, condivide la soluzione con gli altri minatori come prova del lavoro (*Proof-of-work*), gli altri minatori accetteranno la prova del lavoro e cosi il blocco viene aggiunto alla Blockchain. La rete è basata su una architettura *peer-to-peer* costruita al di sopra del protocollo internet. I nodi della rete sono tutti sullo stesso piano in quanto non ci sono né server, ne servizi centralizzati e ne gerarchie tra i nodi stessi. Le firme digitali, con le quali vengono criptate le transazioni, sono degli schemi matematici che consistono in due parti, la prima è l'algoritmo per la creazione della firma che usa la chiave privata per firmare il messaggio e la seconda parte è l'algoritmo di verifica della firma che fornisce la chiave pubblica. Le firme digitali ottemperano a 3 compiti: (1) Forniscono la prova che il possessore della chiave privata è chi possiede i fondi ed è autorizzato a spenderli, (2) Attestano che la prova dell'autorizzazione è incontrovertibile, (3) La firma prova che la transazione non po' essere modificata dopo essere stata firmata. L'algoritmo di verifica legge il messaggio, la chiave pubblica che lo ha firmato, la firma e darà come output vero, se la firma è valida per quel determinato messaggio e per quella determinata chiave pubblica. Ogni transazione, per essere inscritta in Blockchain, richiede che sia validata tramite una firma digitale, essa è generata da una chiave privata, il cui possesso assegna il controllo e ne dimostra il possesso dei Bitcoin contenuti nella transazione. Il sistema è

basato su un sistema asimmetrico avanzato di chiavi, con due diversi tipi di chiavi chiamate chiavi pubbliche e chiavi private, a cui sono assegnati due diverse funzioni: criptazione e decriptazione. Esse sono collegate ad un sistema di criptografia su una funzione matematica (ad esempio l'*Elliptic Curve Moltiplication*), essa è una funzione di tipo *one-way*, quindi irreversibile, poiché può essere calcolata facilmente solamente in un verso ed è difficilmente calcolabile nel verso opposto. La chiave privata è un numero casuale, al quale viene applicata la funzione ellittica per ottenere la chiave pubblica. Alla chiave pubblica vengono applicate due funzione per ottenere l'indirizzo Bitcoin. Il Bitcoin address è una stringa formata da numeri e lettere, essa può essere condivisa con tutti per ricevere i pagamenti sul proprio *wallet*.. Il meccanismo di creazione della chiave pubblica permette di creare firme digitali infalsificabili, in quanto la chiava privata può essere usata per firmare i messaggi e questa può essere validata per una *public key,* senza rilevare la chiave privata, essendo *one-way*. Possiamo articolare l'evoluzione dell'applicazione della Blockchain in diverse ondate: Blockchain 1.0, Blockchain 2.0 e Blockchain 3.0.

La Blockchain 1.0 è legata, nel suo primo utilizzo, ai Bitcoin ed i wallet, quindi come protocollo per effettuare e ricevere i pagamenti. Il Bitcoin è usato per contenere e trasferire valore tra i partecipanti nel network. Un passo avanti nella tecnologia Blockchain è stato ottenuto grazie alla possibilità di inserire nella Blockchain dei contratti digitali (*Smart Contracts*) e di altri protocolli quali le *Smart property*, le applicazioni decentralizzate (*DAPP*), le organizzazioni e le società centralizzate.

La Blockchain 1.0 si era caratterizzata per permettere la decentralizzazione del denaro e dei pagamenti, di contro la Blockchain 2.0, ha permesso di decentralizzare il mercato e il trasferimento di ogni tipo asset, in quanto il registro decentralizzato permette di registrare e confermare ogni tipo di contratto e di proprietà. Gli asset sottostanti possono essere di qualunque tipo, ad esempio come il registro del catasto, il registro dei veicoli, delle licenze, dei matrimoni, delle licenze, della motorizzazione, carte identità, passaporti, documenti notarili, diritti di proprietà intellettuale, contratti tra privati e assicurazioni. L'innovazione non si insinua solamente nei rapporti tra privati, ma coinvolge anche i rapporti e i documenti tra la pubblica amministrazione e il cittadino in

una molteplicità di casistiche relativamente ai suoi diritti (voto, identità, possesso...) e ai documenti attestanti (patente, carta identità, certificati di nascita, di matrimonio, di proprietà immobiliare, brevetti, licenze…), sia per asset fisici e sia per asset intangibili. Gli *Smart Contract* sono l'oggetto informatico abilitante l'ondata della Blockchain 2.0, in quanto essi abilitano ed automatizzano diversi servizi. Gli Smart Contract sono la versione digitale, in linguaggio informatico ed ad esecuzione automatica dei contratti tradizionali. I contratti tradizionali sono accordi tra una o più parti nel quale vengono scambiate uno o più prestazioni in cambio di denaro o di altre prestazioni. Questo schema implica la necessità che vi sia tra le parti la fiducia relativamente al fatto che l'altro soggetto adempia ad i suoi obblighi contrattuali. Gli Smart Contract sottendono lo stesso schema contrattuale, ma non necessitano della fiducia, in quanto eseguono autonomamente il contratto evitando la discrezione nell'interpretazione del contratto ed auto eseguendo le clausole legati ad eventi specifici. Il protocollo Bitcoin non è adatto all'implementazione dei servizi della Blockchain 2.0, per questa ragione sono state sviluppate diverse piattaforme abilitanti tra queste vi è la piattaforma Ethereum. *Ethereum* è una piattaforma basata sulla Blockchain e su un protocollo aperto, sopra la quale è possibile costruire ed usare applicazioni decentralizzate (*DAPP*), basate sulla tecnologia Blockchain. *Ethereum* è il primo computer virtuale decentralizzato del mondo, dato che non risiede in alcun luogo fisico ma nella rete, essendo composto da diversi computer in diverse parti del mondo. A differenza del protocollo Bitcoin, *Ethereum* è stata disegnato come una piattaforma non rigida, adattabile e flessibile alle esigenze del suo sviluppatore, ciò porta ad una grande facilità nell'implementazione di nuove applicazioni che utilizzano la piattaforma.

Nella *Wave 3.0* la Blockchain si propaga dall'ambito dei *financial services* verso tutte le *industry* portando la possibilità di re-configurare servizi e gli standard negli stessi. La Blockchain si presenta come un nuovo paradigma organizzativo *cross-industry,* portatore di una maggiore efficienza e scalabilità, che vede le varie interazioni come transazioni, economiche e non, con un valore e diversi attributi, che possano essere iscritti nella *distributed ledger*. Un caso particolarmente interessante è quello dell'applicazione portata avanti dal NASDAQ. Essa sta utilizzando la Blockchain per supportare le

transazioni Over The Counter, in quanto essa può portare una diminuzione di costi e di tempo grazie all'automazione e alle disintermediazione grazie alla creazione di un network trusted. Il sistema non supporterebbe solamente le transazioni ma permetterebbe di portare un miglioramento anche in ambiti affini come il corporate voting. Un altro caso di rilievo è quello implementato dal governo estone, il quale ha creato la prima identità digitale del cittadino sul network blockchian. La e-identity può fornire al cittadino, tramite una ottimizzata user experience, differenti funzionalità, come quella di carta d'identità valida in tutta l'unione europea, di identificativo per l'accesso ai conti bancari legati a quel singolo cittadino, di tessera per il trasporto pubblico, di documento per l'accesso alle prestazioni sanitarie nazionali e la relativa richiesta di prescrizioni sanitarie, di Firma digitale per la validazione dei documenti e dei atti, di piattaforma per abilitare il voto digitale nelle elezioni nazionali.

7.3. Gli effetti della distruptive innovation sulla CG e sull'Auditing

7.3.1. Le ICO e i Colore Coins: l'emissione dei titoli di Capitale di Rischio e di Finanziamento tramite la Blockchain

Emettendo le azioni della società sulla Blockchain, usando il sistema delle *ICO* (*Initial Coin Offer*) o dei *Colored Coins* sarà possibile dare una maggiore trasparenza sulla ownership dei titoli, sia quelli di capitale e sia quelli di finanziamento. L'emissione attraverso *ICO tokenizza* i diritti derivanti dal quella partecipazione e permette di venderli facilmente come una semplice criptovaluta. Una volta effettuato l'acquisto, la chiave relativa a quella moneta viene assegnata al wallet dell'acquirente, per poter dimostrarne il possesso. Gli *smart contract*, tramite *un Blockchain explorer* leggeranno il registro pubblico distribuito e daranno informazioni in tempo reale riguardanti il possesso dei diversi titoli da parte dei diversi attori. Le ICO sono un composto tra il *crowfunding*, le classiche *IPO* societarie e la piattaforma Blockchain, in quanto hanno come scopo la raccolta di capitale di rischio per *l'issuer* (*IPO*), la raccolta avviene in forma diffusa tramite la rete (*Crowfunding*) e il tutto avviene tramite transazioni in Blockchain. *L'issuer dell'ICO* emette una propria criptomoneta, avente valore unitario ed incorpora i diritti connessi al possesso del titolo di credito sottostante alla parte di capitale di rischio acquisito. L'emissione di capitale

avviene attraverso un asta, alla fine della quale verranno emesse le monete *ICO*, le quali andranno a formare il capitale di rischio della società *issuer*. L'utilizzo delle ***ICO*** come modalità di emissione dei titoli porta diversi vantaggi ai vari stakeholder, ad esempio è possibile per la società *issuer* far acquistare agli investitori, da qualunque parte del mondo, partecipazioni senza dover pagare fee delle piattaforme di vendita, degli intermediari effettuanti la vendita e dell'ente tributario. *Le ICO* stanno suscitando un sempre maggiore interesse ed in molte nazioni si stanno adoperando per regolamentarne il fenomeno e renderlo alternativo alle attuali fonti di raccolta di capitale delle aziende. Le diverse nazioni stanno avendo differenti approcci all'emissione di token nelle ICO come forme di finanziamento per le esperienze blockchain, i due più importanti esempi sono gli USA e la Cina. La Cina ha mostrato un approccio molto restrittivo verso le ICO, nel settembre 2017 diversi istituti cinesi hanno considerato il crowfunding attraverso le ICO una forma di finanziamento illegale e non approvato. La motivazione alla base del provvedimento è quella di voler evitare una eventuale bolla speculativa, dovuta all'uso fraudolento dello strumento. Vietando le ICO, quindi l'emissione delle criptovalute, si privilegerà il Bitcoin, il quale non viene emesso ma esso può soltanto essere minato e del quale la Cina è il più grande minatore, producendo così prima un deprezzamento in seguito alla notizia del blocco, al quale seguirà un rialzo dovuto alla maggiore richiesta dovuta alla mancanza di altre criptomonete concorrenti. Negli Stati Uniti vi è stato un intervento della SEC che nel medio lungo termine mira a creare un corpus di regolamentazioni. Questo approccio può essere visto come premiante della riconosciuta qualità innovativa della tecnologia Blockchain, in quanto la regolamentazione non va a limitare fortemente l'attività ma va solo ad imporre degli obblighi d'informazione per tutelare l'investitore. La SEC, come primo passo ha prodotto un report nel quale analizzano le ICO e affermano l'equivalenza dei token delle ICO alle securities regolate dal *Security Act del 1933* e al *Security Exchange Act 1934*, ciò impone agli enti emittenti di seguire le regole previste dalla SEC per le emissioni delle azioni sul listino nazionale.

7.3.2. Il Corporate Voting e l'effetto apportato dalla Blockchain Technology

La Blockchain può abilitare il voting per ogni tipo di votazione, principalmente potrà essere un valido sostituto per il *corporate proxy voting*, permeato da molti problemi ed inefficienze, quali ad esempio la lista dei votanti inesatta, l'incompleta distribuzione dei diritti di voto e la caotica tabulazione dei voti. In un sistema di voting in Blockchain, i soggetti legittimati al voto, ad ogni votazione riceveranno un *token* (*votecoins*), che al momento del voto sarà trasmesso con una transazione. La transazione viene registrata nella Blockchain e sarà immutabile e trasparente verso tutti gli attori del network, in questo modo vi sarà più fiducia e maggiori possibilità che lo shareholder voti la mozione. Questa nuova modalità faciliterebbe gli shareholder, in quanto porterebbe vantaggi in termini di tempo, trasparenza e accuratezza del voto, incentivandone la partecipazione degli stessi, in modo particolare quella dei piccoli azionisti. Grazie alla sua maggiore velocità può essere un deterrente per le pressioni effettuate dal management durante le votazioni nei confronti dei soggetti dissidenti che votano contro la loro mozione. Un ulteriore problema risolvibile *è l'empty voting*, ciò quella classe di schemi e strategie che permette tramite il prestito o utilizzando una combinazione di derivati su azioni per ottenere i diritti di voto temporaneamente senza avere una esposizione economica al flusso di cassa connesso alla sottostante azione. La Blockchain potrebbe facilitare gli scambi dei diritti di voto, mediante la creazione di un marktplace p2p, rendendo trasparente le transazioni e gestendo i rapporti tra i due soggetti utilizzando gli smart contract. Lo smart contract, potrebbe gestire in maniera ottimale il lending temporaneo del diritto di voto, in quanto potendo imporre dei limiti alla sua utilizzazione e potendone monitorare in automatico l'eventuale inadempimento ed attivare, in base alle necessità, azioni esecutive e/o correttive dell'azione sottostante. Ciò limiterebbe fortemente l'uso fraudolento ottemperato da alcune delle parti nei confronti del lender, in quanto in caso di utilizzo del diritto di voto contrario, a quanto pattuito dalle parti in fase di dealing, si attiveranno automaticamente in capo alla parte fraudolente azioni sanzionatorie. Inoltre la maggiore trasparenza garantita dalla Blockchain potrebbe portare ad ottenere una migliore valutazione del pricing in quanto, grazie alla trasparenza, si potrà basare la valutazione su dati aggiornati in real time e su un data set completo di transazioni. La trasparenza, rendendo evidente la transazione tra le parti, potrà fornire agli altri

shareholder, al management e ai regulator le informazioni relative ad essa, permettendo così eventualmente di effettuare azioni per contrattaccare o fermare l'azione d'acquisto La Blockchain può influire su altri aspetti del corporate Voting come ad esempio nel facilitare il rapporto tra i differenti attori nel processo di riconciliazione tra i registri aziendali, quelli del Deposito Centrale Titoli (Monte Titoli) e della società di asset managment richiede circa 25 – 30 giorni dall'annuncio fino alla chiusura del voto. Grazie alla Blockchain si possono ridurre fortemente i tempi richiesti dalla procedura utilizzando le potenzialità del registro distribuito della Blockchain, in modo da condividere le informazioni con il network di attori senza doverle inviare, in quanto già distribuito presso la rete, quindi accessibile a tutti. Grazie alla Blockchain potrà essere creato e disegnato un workflow automatico per la comunicazione delle informazioni ai differenti attori, le istruzioni per il voto, le notifiche ed i voti espressi.

7.3.3. La Blockchain e i miglioramenti apportati alla trasparenza nelle aziende

Grazie alla Blockchain si avrebbe un'automazione per le dichiarazioni riguardanti il possesso di pacchetti azionari al di sopra della soglia per le partecipazioni rilevanti, attualmente la dichiarazione avviene attraverso autodichiarazione e con un arco temporale ampio, ad esempio, per le società SEC il limite è pari a 10 giorni ed in Italia è circa 90 giorni. Invece grazie alla Blockchain, l'accertamento di una posizione sopra alle soglie potrà avvenire in un lasso di tempo breve, in quanto grazie ad uno *smart contract,* verrà scansionata la Blockchain, per trovare tutte i titoli, in quella determinata azienda, legate allo stesso soggetto e verrà verificato il valore aggregato totale rispetto alle soglie limite, in caso di superamento delle soglia, verrà effettuata una transazione in Blockchain ,contenente il valore della posizione da esso detenuto, verso le autorità di vigilanza adibite al controllo e verso la società. Una maggiore trasparenza riguardante le ownership ha una moltitudine di effetti altamente diversificati sui differenti attori. I Corporate Raider, basano la propria strategia sull'acquisto di società considerate sottovalutate dal mercato, in quanto il prezzo assegnato loro dallo stesso mercato è inferiore al valore che si otterrebbe vendendo in maniera atomistica i diversi asset della stessa azienda. Questa situazione può scaturire da una cattiva considerazione dell'azienda data dal mercato, da

insight interni alla stessa, quindi da un mismatch tra le informazioni pubbliche e quelle private. Soprattutto nell'ultimo caso la Blockchain potrebbe essere una forte limitazione per loro in quanto se gli elementi dell'azienda sono resi pubblici e alla portata di tutti, il *mismatch* tra informazioni private e pubbliche si potrebbe affievolire e quindi loro si vedrebbero ridurre il loro vantaggio competitivo. Inoltre una prassi tipica dei corporate raider è quella di acquisire la maggioranza della società target mediante una acquisizione ostile. Per tale ragione, essi cercheranno di tenere, nella fase embrionale del processo, la strategia nascosta, in modo da non allertare né il mercato, il quale produrrebbe un impennata dei prezzi dei titoli dell'azienda target, né l'attuale management e proprietà, che potrebbero attivare delle difese all'hostile takeover, ad esempio delle *poison pills, golden parachute*, *super-majority voting, green mail*, … La Blockchain potrebbe far emergere e rendere evidenti i loro schemi di acquisizione della società target, permettendo così ai differenti attori di mettere attivare in tempi consoni le *antitakeover defense*. Gli azionisti di maggioranza, detenendo la maggioranza del capitale sociale e quindi eleggendo la maggioranza del Board stesso, saranno in possesso di una completa informazione o almeno maggiore rispetto a quella detenuta dagli altri soci o dal resto del mercato. Perciò la trasparenza può essere ritenuta come un elemento sfavorevole ai soci di maggioranza, in quanto detenendo una maggiore livello informativo, che rappresenta un vantaggio competitivo, una maggiore trasparenza potrà portare solamente un diminuzione dello stesso. Considerando anche gli effetti dell'Agency Theory di primo tipo, la Blockchain potrebbe essere un elemento fortemente positivo nel ridurre la stessa, in quanto porterebbe alla luce i comportamenti negativi del Management come ad esempio *l'earning management, backdating* delle azioni dei *manager*, l'acquisto da parte degli stessi delle azioni dei competitor…. Considerando la posizione dei azionisti di maggioranza, gli effetti della Blockchain è sono da ritenere a somme positive in quanto, anche se una maggiore trasparenza porta una perdita di valore della loro posizione dei *major shareholder*, ma è anche una efficace soluzione *all'Agency Theory I.* Una maggiore trasparenza ha un effetto positivo sui piccoli azionisti e sui fondi con gestione passiva, in quanto loro hanno un livello informativo fortemente inferiore agli azionisti di maggioranza. La carenza informativa è dovuta al fatto che il loro livello di informazione

si attesta alle comunicazioni obbligatorie per legge, la maggiore trasparenza portata dalla Blockchain potrebbe affievolire questa differenza informativa, rendendo accessibili le informazioni che prima non erano nella loro portata. Un ulteriore elemento innovativo che potrebbe apportare al *Check sulla ownership,* è dato dalla possibilità di tracciare i titoli detenuti da Manager come parte variabile e bonus della loro remunerazione. Grazie alla Blockchain e alla trasparenza portata da essa, potranno essere monitorate tutte le azioni fatte dai manager sulla stesse e legare ad essi degli *Smart Contract* che, al compimento di azioni non ritenute opportune, attivino delle azioni che limitino, blocchino o sanzionino l'azione fraudolenta. Numerose possono essere le azioni in questione:

1. Vendita delle *Management Stock Option*: E' comune l'utilizzo delle cosiddette *Restricted Stock Option*, le quali sono date *al top management*, esse sono soggette a restrizioni nella loro circolazione per evitare vendite premature e in periodi specifici precedenti a possibili cadute di valore del titolo. La loro possibile vendita molte volte è in parte postergata alla fine del contratto del manager e talvolta anche per diversi anni dopo questa. La Blockchain potrebbe notificare tutti i passaggi degli stessi titoli e vagliare la loro aderenza alle regole specificate alla loro emissione, mediante l'uso di *smart contract*, in modo tale da evitare che esse vengano vendute impropriamente.
2. Manipolazione delle Stock Option: oltre alla vendita delle *Stock Option* i manager potrebbero effettuare ulteriori azioni che mirano ad aumentare le loro revenues derivanti dai titoli come il *backdating* della data di emissione e/o di esercizio della option relativa al Manager oppure la manipolazione del *vesting period* dello stesso. La Blockchain essendo immodificabile non permette cha avvengano delle manipolazioni da parte degli attori degli elementi registrati al suo interno rendendola così *tamper-proof by design*. Su ogni informazione registrata in Blockchain viene apposto un timestamp indelebile, una volta che è stato apposto esso non può essere rimosso e quindi le informazioni registrate sono salve da manomissioni.
3. Acquisto di azioni di competitor diretti e non: i manager, avendo informazioni sensibili e privilegiate rispetto al resto del mercato, potrebbero avvantaggiarsi

usando questa asimmetria informativa par fare dell'arbitraggio ed avere ulteriori guadagnati collaterali in caso di riduzione del valore della compagnia stessa in rapporto con il valore dei competitor. Inscrivendo i titoli in Blockchain, gli smart contract potrebbero monitorare gli acquisti dei manager così da poter bloccare e impedire l'acquisto per gli stessi di azioni ed altri titoli relativi ai competitor e altre azioni in contrasto con quanto predefinito da policy e contratti aziendali ed etiche a cui loro stessi hanno aderito.

7.3.4. Gli improvement nel Firm Accounting

La Blockchain può abilitare la raccolta e la notarizzazione sicura e certificata dei dati aziendali, rilevati al fine di redigere le scritture contabili necessarie alla determinazione del risultato della gestione annuale, ciò può essere fatto in modo tale da rendere immutabili le registrazioni contabili, quindi renderle impassibili ad essere soggette *all'Accruals Earning Management*, da eliminare l'intermediazione dei revisori e da controllare le transazioni tra parti correlate. Con questa modalità di contabilizzazione i dati sono registrati in modo permanente, in quanto su di essi vi è impresso un *time stamp tamperproof*, che permette di evitare l'alterazione ex post del dato stesso. La Blockchain può essere un *game changer* anche nelle comunicazioni richieste tra le aziende e con attori esterni all'azienda come revisori, banche, autorità fiscali, tribunali, governo ed altre istituzioni della PA. Permettendo la registrazione nel ledger distribuito delle informazioni è possibile facilitare la loro condivisione in maniera sicura e potendo tracciare chi ne ha accesso ed eventualmente revocare lo stesso in caso di comportamenti non ritenuti consoni dal data owner. La Blockchain abilita la raccolta in real-time dei dati contabili della società, nel sistema attuale la raccolta in real-time è una operazione proibitiva, in quanto richiederebbe elevati costi dovuti dal dover fare numerose operazioni altamente *time consuming*, che includono la raccolta dei dati stessi (anche automatizzata in parte) e il successivo audit interno della procedura stessa per la verifica del funzionamento della piattaforma. Utilizzando la Blockchain per la gestione degli accounting record aziendali si effettuerà il passaggio da un *double entry system* per arrivare ad sistema contabile basato *sul triple entry system*. Il sistema attuale basato sul *double entry system*, richiede

una doppia scrittura contabile in capo alle due parti della transazione per la stessa operazione. Quindi ogni parte dovrà effettuare la propria scrittura contabile in maniera indipendente dall'altro, ciò, oltre a portare una duplicazione delle scritture, può portare all'effettuazione di diversi errori, alla creazione delle inconsistenze tra i diversi i due differenti registri contabili delle *firm* nella transazione, a delle inaccuratezze ed inoltre richiede che vi siano tra le parti una diametrale corrispondenza tra i due registri a seguito delle riconciliazioni tra gli stessi. Utilizzando la Blockchian e quindi un sistema basato su un Triple entry system, si porterà una maggiore efficienza ed efficacia nel sistema. Il Triple entry system porterà alla creazione di un solo registro unico ma diffuso presso i diversi attori della rete, al suo interno verranno registrate tutte le informazioni relative alle transazioni. L'avere un registro unico distribuito abiliterà l'aggiornamento automatico dello stesso tramite una sola scrittura contabile e permetterà di informare ed avere accesso alle stesse a tutte le controparti.

7.3.5. Il Blockchain Audit Model

La Blockchain apporterà sostanziali innovazioni che modificheranno totalmente il settore della revisione aziendale rispetto all'attuale conformazione, il ruolo del revisore andrà sempre di più a comprendere l'attestazione dell'efficienza e dell'efficacia delle piattaforme abilitanti le procedure e sempre meno attinenti alla valutazione dei singoli elementi. Possiamo pensare che il cambiamento non sia immediato e radicale, quindi possiamo immaginare che in una prima fase preliminare il sistema Blockchain vada ad efficientare tramite il supporto all'attuale operatività del revisore per poi andare sempre di più a sostituire processi di verifica e controllo. Quindi nella fase preliminare si potrebbe applicare la tecnologia per verificare l'integrità dei documenti contabili. In un seconda fase di sviluppo essendo possibile *un real-time accounting*, non sarà più necessario il giudizio sulle informazioni derivato dal lavoro di un soggetto terzo indipendente, come il revisore, in quanto i diversi stakeholder riporranno la fiducia nei dati immutabili e certificati presenti all'interno del network distribuito. Grazie alla trasparenza introdotta dal *real-time Accounting* sarà possibile monitorare efficacemente ed efficientemente le transazioni tra le parti correlate ed individuare quelle eventualmente sospette di un

possibile conflitto d'interessi tra gli stessi. La normativa attuale si base generalmente sulla disclosure volontaria fornita, in merito a quelle transazioni, dal Management del soggetto stesso, su quelle transazioni che lui stesso ritiene che siano state fatte con soggetti che possano essere considerati delle parti correlate, questa modalità è da considerare come una via fortemente lacunosa, quindi mediante l'utilizzo della tecnologia Blockchain si porterà a limitare sempre di gli errori dovuti ad una mancata individuazione di operazioni sospette e che potrebbero arrecare un ingente danno alla società ad esempio portando a conclusione un negozio a prestazioni con non proporzionate. La Blockchain potrà portare innovazione ed un miglioramento anche nella limitazione *dell'Accruals Earning Management.* Grazie all'irreversibile *timestamp* apposto sopra alle transazioni, ai manager è reso impossibile applicare strategie mirate *all'accruals earning management* come il backdating dei contratti di vendita ad un periodo relativo ad un precedente report periodico oppure la pratica di capitalizzare delle spese agli anni successivi ed ammortizzarle in diversi anni.

7.4. Blockchkain CG & Audit Use Case

7.4.1. Otonomos

Otonomos sarà una delle start up che innoverà il mondo delle imprese medio-piccole e grandi pre-IPO, in quanto permetterà di gestire interamente l'impresa in Blockchain. Otonomos assegna un wallet basato sul sistema delle cryptocurrencies, a quale corrispondono dei titoli (come azioni, opzioni, bonds, note, …). Su questi è implementato un sistema *di smart contract* che abilitano diverse funzioni:

a. Creazione in maniera telematica delle aziende, avviene in circa 72 ore, ad oggi la sua valenza legale è relegate solamente ad alcune nazioni virtuose come ad esempio lo stato del Dalaware, Singapore, Hong Kong , UK e le Isole Cayman.
b. Creazione ed aggiornamento in real time di un registro dei possessori dei detentori dei titoli (Capitalization Table), anche in situazioni di alta complessità e frammentazione della compagine sociale.
c. Gestire con estrema facilità il trasferimento delle azioni e degli altri titoli aziendali

d. Codifica ed automazione delle documentazione aziendale come lo shareholder agreements e di altri documenti governativi. Essi sono resi *self executing* tramite dei *decentralized computers,* il quale li abilita ad effettuare automaticamente delle azioni in corrispondenza di avvenimenti ritenuti rilevanti, che sono scelte in fase di stesura degli stessi secondo la logica *IF <<Something Happen>> Then <<do something>>.*
e. Abilitare l'automazione di alcune azioni aziendali, come ad esempio la ripartizione e l'accredito dei dividendi nei wallet degli differenti shareholder.

La soluzione non abilita l'azienda a fare maggiori *revenues* ma consente di efficientare i processi amministrativi aziendale permettendo così di salvare tempo e denaro.

7.4.2. BTL, British Petroleum , Wien Energy, ENI e EY.

La startup canadese BTL ha creato una piattaforma chiamata Interbit, per la quale ha ricevuto diversi finanziamenti Nella sua fase di testing la società ha creato un progetto pilota di dodici settimane incentrato sulle riconciliazioni per mezzo della tecnologia *Blockchain*. Il pilota, gestito sulla piattaforma *Blockchain* di BTL, Interbit, ha dimostrato con successo che questa tecnologia può abilitare un sistema di riconciliazione *trade-by-trade* (*near real-time*). Questo risultato fornisce la prova per il potenziale più ampio e trasformativo che la tecnologia Blockchain promette di fornire in tutta la gamma di attività back office che supportano le attività di trading nelle aziende energetiche. Il testing è stato fatto con diversi attori: British Petroleum , Wien Energy, ENI e EY. Il design interoperabile e flessibile della Blockchain offre notevoli vantaggi rispetto alla tecnologia del database tradizionale ad esempio essi possono essere considerati in termini di tracciabilità, auditabilità, sicurezza delle transazioni e automazione ed efficienza tra più controparti. Ad esempio, in aree come la regolamentazione e la conformità, logiche complesse possono essere integrati in contratti intelligenti che eseguono automaticamente direttamente sulla rete Blockchain anziché richiedere l'esecuzione individuale da parte di ciascuna società coinvolta in una transazione. Il design di Interbit, basandosi sulla Blockchain permetta la creazione di record immutabili, di favorire l'automazione e di garantire la validità dei dati inseriti nelle transazioni, di ridurre o eliminare gli oneri attuali previsti. Interbit grazie al

fatto che essa unisce le fasi della conferma di una transazione con il momento dell'inserimento e della registrazione della stessa in un record, si elimina totalmente la necessità di una riconciliazione post-trade e si protegge dall'errore umano e dalle intercettazioni della corrispondenza. Ciò consente di aumentare notevolmente i volumi di negoziazione, ridurre il rischio di credito, ridurre i costi e di aggiungere preziose funzionalità quale l'aggiunta di nodi di controllo o di regolamentazione.

7.4.3. Tallystic

Tallystic è un plug in add-on per i sistemi ERP, grazie al quale è possibile minimizzare gli errori durante il processo di fatturazione, ridurre i costi relativi alla revisione, diminuire il fabbisogno finanziario e del capitale circolante ed infine induce una maggiore sicurezza nelle transazioni. Tallystic propone due diverse soluzioni in Blockchain implementabili presso le aziende: (a)Tallystic Invocie Automation: è una soluzione che permette di efficientare tutto il ciclo dell'invoicing, partendo dalla sua generazione, al suo invio, passando dalla ricezione e pagamento fino alla sua riconciliazione, (b) Tallystic Invoicing Finanncing and exchange: essa è una soluzione nell'ambito del Invoice Financing. Possiamo riscontrare diversi vantaggi nell'applicazione della soluzione di Tallystic alle imprese in quanto permette la connessione dei loro database e alle loro informazioni al network al fine di gestire la condivisione delle stesse in base agli accordi tra le parti. Tra questi possiamo riscontrare Immutàbilità dei records (Registro dei dati storici e Overview in real-time dei dati finanziari della società), Distributed application (Invio automatico delle fatture e Riduzione di costi, errori e frodi) e Sicurezza (Condivisione sicura dei dati a soggetti terzi come revisori, entità regolatori ed investitori).

7.5. Osservazioni Finali

Avendo avuto la possibilità di esaminare il sentiment del top management della più grandi imprese italiane, grazie a questionari, agli incontri e call conference effettuate nella mia veste di consulente in ambito Blockchain Technology e membro del Blockchain Hub per l'area MED per Ernst & Young, posso sottolineare diversi elementi, ad esempio la Blockchain è vista principalmente come un game changer o adatta ad applicazioni di nicchia ad alto valore ed inoltre è opinione unanime che è necessaria la collaborazione

tra le aziende del settore per il design e l'implementazione delle soluzioni. In un futuro non troppo lontano la Blockchain potrebbe entrare in molti degli aspetti delle nostre vite, portando trasparenza, sicurezza ed efficienza, aprirà le porte verso una nuova era: la Blockcracy. La Blockchain creerà un mondo più trasparente, incentiverà la globalizzazione, I liberi scambi, sarà l'antidoto per la stagnazione e di support per le crisi politiche, efficienterà le transazioni finanziarie, permetterà la gestione in maniera unitaria dei dati sanitari e personali del cittadino, abiliterà il peer-to-peer dell'energia, tutto ciò porterà verso una crescita e nuovi posti di lavoro. Agli attori non resta che scegliere se vogliono essere anche loro i protagonisti nella guida della rivoluzione o rimanere inermi ed essere gli spettatori passivi del cambiamento.