

Blockchain per il bene comune? | Economia e Politica

Andrea Pannone - 04/02/2019 [papers]

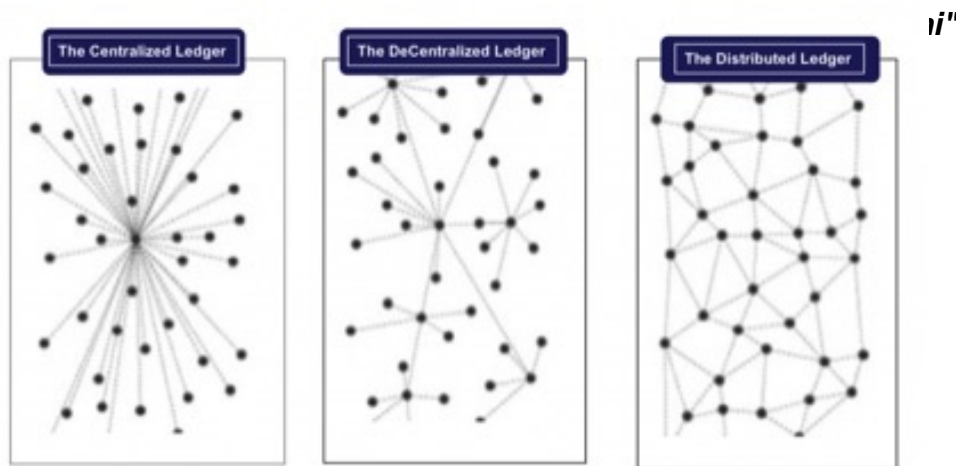
Abstract

In recent months, the focus on blockchain - the technology created to encourage online cryptocurrency exchange like Bitcoin - has grown exponentially among scholars and politicians. Blockchain is a particular type of distributed ledger written by decentralized, usually anonymous groups of agents rather than known centralized parties. Consensus is attained by making the ledger publicly viewable and verifiable. While some characterize the blockchain's state-of-the-art as a 'speculative vision', others seem to agree that its only limitation is the imagination of the user community. In this paper we try to understand if the characteristics of blockchain can be useful to tackle and solve the main problems related to the use of an important category of economic goods: the common goods.

*La **Blockchain** è nata per lo scambio di criptovalute come Bitcoin, ma può essere molto utile anche per affrontare il problema della scarsità dei beni comuni.*

1. La 'novità' di blockchain

Negli ultimi mesi è cresciuta esponenzialmente tra studiosi e politici l'attenzione su **blockchain** - la tecnologia nata per facilitare lo scambio online di **criptovalute** come **Bitcoin**^[1] - quale strumento per coordinare e rendere efficienti un'ampia varietà di transazioni decentralizzate non intermedie da soggetti terzi. In termini estremamente semplificati una **blockchain** è un libro mastro, ovvero la base fondamentale della contabilità, condiviso da una rete decentralizzata di computer per l'archiviazione digitale e il tracciamento dei dati associati a un prodotto o servizio lungo tutta la catena del valore (ossia dalla fase di produzione fino al consumatore/utilizzatore). La **blockchain** può essere considerata una tecnologia che appartiene alla categoria delle tecnologie **Distributed Ledger**, ossia un insieme di sistemi concettualmente caratterizzati dal fatto di fare riferimento a un registro distribuito, governato in modo da consentire l'accesso e la possibilità di effettuare modifiche da parte di più nodi di una rete (vedi figura sotto).



Blockchain [/caption] Come

suggerisce il nome una **blockchain** è organizzata in una sequenza lineare di piccoli insiemi di dati crittografati chiamati "blocchi", che contengono gruppi di transazioni con data e ora (timestamp).

Ogni blocco contiene un riferimento al suo blocco precedente e una risposta a un puzzle matematico complesso, che serve a convalidare le transazioni che contiene[2]. Nella sua forma più elementare la **blockchain** serve come mezzo per registrare, in modo sicuro e verificabile, un particolare stato di cose che è stato concordato dalla rete (Wright & De Filippi 2015). Come tale, la **blockchain** può essere utilizzata in qualsiasi sistema che comprende informazioni preziose, inclusi denaro, titoli, azioni, diritti di proprietà intellettuale e persino voti o dati di registro di identità (Davidson et al., 2016; Tapscott & Tapscott, 2016)[3]. Osserviamo che la necessità di crittografare i dati deriva proprio dal fatto che tutto quello che viene registrato su una blockchain è visibile a tutti i nodi della rete e quindi se si registrassero informazioni sensibili senza essere crittografate esse diventerebbero pubbliche. La **blockchain** viene crescentemente descritta come una "tecnologia estremamente disruptive che avrebbe in prospettiva la capacità di riconfigurare tutti gli aspetti della società e delle sue attività". In realtà, come ormai chiaro, non si tratta di una tecnologia 'nuova' ma piuttosto una 'ricombinazione creativa' di tre elementi tecnici comprovati quali un'architettura di rete *peer to peer*, la crittografia e un protocollo specifico di disciplina di incentivi[4]. Senza enfatizzare le opportunità o i rischi derivanti dalla sua diffusione, in questo articolo cerchiamo di interrogarci se alcune caratteristiche di **blockchain** possano essere utili per risolvere i problemi relativi all'utilizzo di un'importante categoria di beni economici: i [beni comuni](#).

2. Beni comuni e tragedia

Come noto la teoria economica considera questi beni come beni di importanza primaria per i soggetti di una comunità, che sono a consumo 'rivale' (il consumo da parte di un soggetto determina una riduzione della disponibilità residua per gli altri soggetti) e 'non escludibile' (nessuno dei soggetti può essere escluso a priori dal suo utilizzo). Tra questi beni possiamo annoverare un'ampia gamma di risorse, sia naturali (come foreste, oceani e altre risorse rinnovabili) sia costruite dall'uomo (come sistemi di irrigazione, reti elettriche, spettro elettromagnetico, Internet, ecc.). Ai fini di evitare un impoverimento o, peggio, una distruzione delle stesse (il cosiddetto fenomeno della tragedia dei *commons*, vedi ad esempio sul punto Pannone 2018), determinata da un livello di consumo guidato esclusivamente dal principio della massimizzazione dell'utilità individuale, si ritiene indispensabile una qualche forma di regolamentazione esterna alla comunità: o da parte del mercato, attraverso la definizione di precisi diritti di proprietà che proteggano l'uso esclusivo delle risorse da parte di chi le acquista, o dallo [Stato](#), attraverso l'emanazione di leggi che ne limitino le possibilità di utilizzazione individuale e collettiva. Ad ogni modo, l'evidenza storica relativa alla gestione di risorse comuni ha mostrato come entrambi le soluzioni, privatistica o statalista, quando non totalmente inadeguate, presentino gravi limiti nell'evitare 'la tragedia'. (si veda ad esempio Stavins 2011) [5]. D'altra parte, come mostrato nel mio articolo sul punto (vedi ancora Pannone 2018), in presenza di informazioni immediate e condivise sulla capacità potenziale di un common lungo un dato arco temporale, come anche di feedback adeguati alle decisioni individuali e collettive, i soggetti di una comunità potrebbero generare fenomeni di *antirivalità* e *inclusione* capaci di rendere compatibile la soddisfazione del bisogno personale con la sostenibilità e la salvaguardia della risorsa comune nel futuro. Vogliamo pertanto chiederci ora se e come la diffusione di **blockchain** possa fornire in modo efficace questo tipo di informazioni e feedback così da favorire una gestione dei beni comuni non necessariamente sottoposta a regolazione preventiva (***unmanaged commons***).

3. Come può Blockchain evitare la tragedia dei commons

Alla luce delle argomentazioni fin qui esposte, l'idea è che blockchain permette di registrare, in modo inconfutabile, permanente e condiviso, l'accesso di ciascun individuo a un common e la relativa utilizzazione dei suoi benefici potenziali in ciascun periodo di tempo, dando contemporaneamente a tutti l'informazione della loro disponibilità residua nello stesso o in altri periodi di tempo[6]. La stessa

possibilità di accesso all'uso potrebbe essere poi condizionata sia a priori, in base a un protocollo che equiripartisce tra i soggetti la disponibilità della risorsa lungo un dato arco temporale sia a posteriori, in base alla comune conoscenza dei periodi di 'picco d'uso' e della possibile valorizzazione della stessa risorsa nei periodi di tempo in cui rimane inutilizzata. Tale valorizzazione potrebbe avvenire in due modi:

1. a) attraverso la decisione individuale di differire, ammesso che ciò possa essere fatto a parità di utilità[7], la propria abitudine di consumo in periodi fuori picco,
2. b) re-immettendo in gioco a vantaggio della comunità (quindi di fatto producendo valore comune), in modo gratuito o dietro una stabilita ricompensa (sotto forma di gettoni chiamati token), la parte della risorsa a cui avrebbe diritto ma che non avrebbe possibilità o interesse contingente ad utilizzare.

Il punto b) merita di essere approfondito. Maggiori sono gli incentivi esterni alla produzione di commons maggiori sono le probabilità che la piattaforma si polarizzi verso logiche di mercato in cui le motivazioni 'estrinseche' all'azione prevalgono o quanto meno distorcono significativamente le motivazioni 'intrinseche' alle logiche della comunità. E' il caso ad esempio di Backfeed (vedi Pazaitis et al. 2017), una innovativa piattaforma di produzione decentralizzata di [commons](#) basata su blockchain, che fornisce funzionalità sofisticate per sviluppare incentivi associati a finanziamenti esterni alla comunità degli utilizzatori ed espressi attraverso criptovalute spendibili verso altri beni[8]. In questo modo i soggetti partecipanti vengono aggregati e coordinati secondo un meccanismo assimilabile a quello degli scambi basati sull'interesse individuale. L'affermazione di una logica realmente alternativa, comunque, dovrebbe allora essere quella per cui i token debbano essere 'conciati' all'interno della comunità con un valore di scambio tra i benefici dello stesso common o di common diversi che potrebbe essere determinato in base alla quantità/tempo di lavoro necessario alla loro produzione/utilizzazione. L'informazione relativa alla provenienza del valore (lavoro) sarebbe registrata, in modo non modificabile (a meno ovviamente di attività di hackeraggio piuttosto complesse) nei dati del token i quali potrebbero essere accettati e incrementati di valore in base alla priorità preferenziale della richiesta. Ad esempio, supponiamo che Antonio e Francesco vogliono entrambi comprare una mela usando la criptovaluta di blockchain. Vittorio coltiva e vende mele e necessita di avere token per comprare acqua. Antonio possiede token per l'acqua mentre Francesco dispone di token per visitare musei. Supponiamo che raccogliere mele e acqua richieda lo stesso tempo di lavoro, mentre visitare il museo del luogo richieda la metà del tempo necessario a produrre i primi due. Lo scambio di Antonio ha la priorità in quanto Vittorio, come coltivatore e venditore di mele, preferisce i token per comprare acqua. Mentre infatti Antonio ha bisogno solo di spendere un token per ottenere una mela, Francesco deve prima spendere due dei suoi token per acquistare il token per l'acqua da Antonio, poi può spendere il suo token di acqua per comparare la mela da Francesco. Il meccanismo creerebbe una domanda addizionale di due token di acqua (da parte di Vittorio e Francesco) che corrispondono all'offerta di due token per musei (da parte di Francesco) e una mela (da parte di Vittorio). Questo aumenterebbe il valore dei token per l'acqua accrescendo l'interesse della comunità per la preservazione della risorsa. Notiamo in generale che il sistema fornisce piena trasparenza a tutti gli utenti, in quanto tutti i comportamenti dichiaratamente coerenti con l'obiettivo comune sono soggetti alla valutazione peer-to-peer, che determina ulteriormente il valore effettivamente percepito della rete/comunità. Notiamo anche come questo tipo di protocollo di validazione delle operazioni sia basato su una sorta di prova di valore (*Proof of value*) invece che sulla soluzione di un puzzle matematico (*Proof of work*) come avviene nelle cosiddette attività di *mining* della blockchain di Bitcoin, con evidenti risparmi in termini di potenza di calcolo e consumo energetico.[9] In conclusione, nel sistema ipotizzato, tutte le attività sono chiaramente monitorabili e quindi visibili all'intera comunità, e i comportamenti incoerenti con le logiche della comunità stessa possono essere di fatto individuati e sanzionati e i relativi latori emarginati. Anche se anonima e quasi

fittizia, la fiducia può essere costruita all'interno della comunità degli utenti. L'ipotesi implicita al concetto di tragedy of commons, ossia il problema dell'assenza di comunicazione tra coloro che condividono le risorse può essere respinta e l'ampiezza della rete telematica può estendere la scala della cooperazione ben al di là del semplice livello locale (vedi Volont e van Andel 2018). Ovviamente anche per blockchain, come per ogni altra attività telematica, non è possibile evitare del tutto i rischi connessi all'uso improprio di dati sensibili, alla loro protezione generale e alla loro sovranità, che può inibire in modo rilevante l'effettiva diffusione di questa tecnologia.

4. Verso un nuovo ecosistema e il ruolo dello Stato

Osserviamo che l'utilità di blockchain nel superamento della tragedia dei commons non deriva dall'essere una tecnologia 'nuova' (vedi paragrafo 1) quanto dalla sua capacità di essere funzionale alla risoluzione qualitativa dei problemi di coordinamento decisionale implicati dall'uso di risorse comuni che abbiamo analizzato nei paragrafi precedenti. Solo quindi la consapevolezza di tali problemi e la volontà di farvi fronte, unita all'affermarsi tra gli utilizzatori del common di una cultura della comunicazione, della reciprocità e della condivisione, può fare in modo che la soluzione tecnologica fornita da blockchain sia di effettivo aiuto alla costruzione di un ecosistema auto-organizzato, in grado di condurre a una 'felice risoluzione dei conflitti' sui beni comuni[10]. Alla praticabilità di questa costruzione, ovviamente, non sarebbe estranea la proprietà di blockchain di garantire contestualmente un meccanismo di ricompensa/convenienza individuale che può diventare complementare, anziché in contrasto, con l'affermarsi di una diffusa cultura della collaborazione. L'effettiva realizzazione di un tale ecosistema, chiaramente, richiede l'attuazione di processi di apprendimento complessi da parte dei membri della comunità e non è scontata a priori, data la forte incertezza che fatalmente accompagna decisioni e strategie che richiedono tempi significativi per essere portate a compimento. Forte incertezza, comunque, non vuol dire che questa strada non sia perseguibile con successo, sempre che resti chiaro l'obiettivo e il vantaggio di generalizzare i comportamenti co-operativi dei molteplici decisori. In questa stessa prospettiva diventa cruciale il ruolo dello Stato e delle sue istituzioni, sia nel fornire alla collettività le infrastrutture[11], i segnali e le informazioni necessarie a un suo coordinamento in chiave collaborativa, sia nel garantire attraverso adeguati strumenti legislativi la tutela dei beni comuni e la loro utilizzazione a vantaggio dell'interesse collettivo[12]. * *Fondazione Ugo Bordonì. Le idee esposte nell'articolo sono di esclusiva responsabilità dell'autore e non corrispondono necessariamente a quelle dell'Ente di appartenenza.*

Bibliografia Antonelli, C., Kraft, J., Quatraro, F., (2010), 'Recombinant Knowledge and Growth: The Case of ICTs', *Structural Change and Economic Dynamics* 21, 1 (2010) 50-69. Davidson, S., De Filippi, P. and Potts, J., 2016. "Economics of Blockchain." Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2744751 Dawes, R. (1973), "The Commons Dilemma Game: An N-Person Mixed-Motive Game with a Dominating Strategy for Defection." *ORI Research Bulletin*, vol. 13, no. 2 (Sept.), 1-12. De Filippi P., Wright A., 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia', unpublished paper, 2015, www.ssrn.com. FAO (2018), *The State of World Fisheries and Aquaculture*, FAO Fisheries and Aquaculture Department, Report 2018, Rome. Hardin, G., (1968), "The Tragedy of the Commons". *Science* 162 (3859): 1243–1248. Hoste, G., Dvorak M., Jacobson M., (2009), *Matching Hourly and Peak Demand by Combining Different Renewable Energy Sources*. VPU Final Report, Stanford University, Palo Alto, California, <http://www.stanford.edu/group/efmh/jacobson/Articles/I/CombiningRenew/HosteFinalDraft>. Nakamoto, S. 2008. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available online: <https://bitcoin.org/bitcoin.pdf> Pannone A. (2018), *La tragedia dei beni comuni e l'inganno della scarsità*, Working Paper (Fondazione Ugo Bordonì) Pazaitis A., De Filippi, P., Kostakis V., 'Blockchain and Value Systems in the Sharing Economy: The Illustrative Case of Backfeed', *Technological Forecasting & Social Change* 125 (2017): 105–115. Rifkin, J. (2014), *La società a costo*

marginale zero. Mondadori Stavins, R., (2011), The problem of the commons: Still unsettled after 100 years. *American Economic Review* 101(1): 81–108. doi:10.1257/aer.101.1.81 Tapscott A., Tapscott, D., *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World* (New York: Penguin, 2016). Varian, H., (2010). “Computer Mediated Transactions”. Working Paper, Univ. of California at Berkley. Vercellone C., Bria F., Fumagalli A., Gentilucci E, Giuliani A., (2015), *Managing the commons in the knowledge economy*. The work leading to this publication has received funding from the European Union’s Seventh Frame.. 2015, pp.110. Volont L., van Andel W., (2018) *The Blockchain: Free-Riding for the Commons. From Potential Tragedy to Real Comedy*, <https://www.onlineopen.org/the-blockchain-free-riding-for-the-commons> Weitzman, M., (1998), Recombinant growth, *Quarterly Journal of Economics* 113, 331-360. [1] Bitcoin, introdotta dal misterioso hacker Satoshi Nakamoto in un paper del 2009, è il primo esempio concreto di una rete di pagamenti distribuita dotata di un meccanismo di incentivazione intrinseco (Van Valkenburgh et al., 2014). L'innovazione di Bitcoin ha suscitato un interesse crescente ad esplorare il potenziale della tecnologia blockchain in altri campi dell'attività umana. Nuove applicazioni sono state sviluppate con la blockchain, tra cui valute digitali, **smart contract** (protocolli informatici che facilitano, verificano, o fanno rispettare, la negoziazione o l'esecuzione di un contratto, permettendo talvolta la parziale o la totale esclusione di una clausola contrattuale), insieme a molti servizi finanziari e non finanziari (Wright and DeFilippi, 2015). Per una descrizione abbastanza dettagliata di blockchain in un linguaggio non eccessivamente tecnico si veda il link <https://www.blockchain4innovation.it/esperti/blockchain-perche-e-cosi-importante/>. [2] Affinché un nuovo blocco di transazioni venga aggiunto alla blockchain è necessario appunto che sia controllato, validato e crittografato. Solo con questo passaggio può poi diventare attivo ed essere aggiunto alla blockchain. Per effettuare questo passaggio nella blockchain di una criptovaluta come Bitcoin, ad esempio, è necessario che ogni volta che viene composto un blocco venga risolto un complesso problema matematico che richiede un notevole impegno anche in termini di potenza e di capacità elaborativa. Questa operazione viene definita come “*Mining*” ed è svolta dai “*Miner*” (vedi nota 9). [3] Tornando all'esempio del Libro Mastro, è praticamente impossibile (o comunque estremamente difficile) modificare i dati iscritti nella blockchain univocamente, in quanto sarebbe necessario violare tutte le copie del libro mastro possedute da tutti i partecipanti della blockchain e occorrerebbe farlo simultaneamente. Allo stesso modo non può nemmeno esistere un “falso Libro Mastro” in quanto tutti i partecipanti sono in possesso di una unica versione autentica che possono impugnare per un confronto e per la verifica. [4] D'altra parte che innovare mediante ricombinazioni di conoscenze è un tratto caratteristico delle tecnologie dell'informazione e della comunicazione (ICT). Sul punto vedi Weitzman 1998, Antonelli et al. 2010. Ad esempio, molte delle recenti innovazioni su Internet sono derivate dal fatto di essere costituite completamente da bit “*..They were programming languages, protocols, standards, software libraries, productivity tools and the like. There was no time to manufacture, no inventory management, and no shipping delay. You never run out of HTML, just like you never run out of email. New tools could be sent around the world in seconds and innovators could combine and recombine these bits to create new web applications.*” (Varian 2010, p. 2). [5] La possibilità di forme di regolazione dei beni comuni basate sull'auto governo degli utilizzatori di un common (come alternativa a Stato e mercato) è emersa grazie all'imponente lavoro sperimentale del premio Nobel per l'economia Elinor Ostrom condotto su diverse comunità locali dell'Asia e del Sud America. Si ritiene comunque che tali forme, accumulate da una autolimitazione condivisa del consumo di risorse comuni - sostenuta dall'etica che innerva la storia di una comunità, sia effettivamente praticabile solo in ambiti circoscritti, dove sono efficacemente applicabili sanzioni morali e punizioni contro la violazione dei protocolli di gestione del bene comune. [6] La proprietà di blockchain di essere un registro distribuito può quindi migliorare la trasparenza, la tracciabilità e fiducia tra coloro che sono coinvolti nelle transazioni (vedi par. 1). La tecnologia - ora in fase di sperimentazione nel settore della pesca e nel settore della sicurezza alimentare – quindi detiene un

notevole potenziale per migliorare l'accesso al mercato, in particolare per i piccoli pescatori e per gli agricoltori. La difficoltà di corrompere le informazioni nella catena di blocchi rafforza la tracciabilità dei prodotti ittici e alimentari lungo la catena del valore, cosa che permette ai suddetti soggetti di verificare gli impianti, la metodologia di lavorazione/conservazione e gli standard fitosanitari dei luoghi di provenienza e di transito dei prodotti, come anche di adempiere ai requisiti legali di importazione e certificazione dei Paesi in cui essi risiedono. Lo stesso consumatore può avere accesso a questa catena di informazioni aumentando l'incentivo a guidare produzioni alimentari più sicure, sostenibili ed ecocompatibili. (vedi FAO 2018). [7] Come dovrebbe essere chiaro dagli esempi fatti in precedenza l'utilizzazione di una risorsa vitale può essere differito senza variazioni di utilità ammesso che questo non contrasti con i bisogni fisiologici dell'individuo che richiedono una soddisfazione immediata (es. sete, freddo, ecc.), con le caratteristiche biologiche della risorsa (ad esempio, intermittenza dei benefici), con la flessibilità e la relativa intercambiabilità dei tempi di vita (ad esempio tempo di lavoro, tempo libero). [8] Sarà bene sottolineare la differenza tra 'criptovaluta' e 'token'. Una criptovaluta è una moneta digitale ed è quindi sostanzialmente una valuta virtuale (come Bitcoin o Ethereum. Un token è la rappresentazione digitale di un asset fisico o digitale: i membri di una comunità possono ricevere dei token relativi al progetto su cui hanno deciso di investire in cambio di moneta virtuale. L'iniziale offerta di token prende il nome di ICO (*Initial Coin Offering*) ed è emessa dal(i) soggetto(i) che cercano fondi e partecipazione a sostegno di un dato piano/progetto di attività. [9] Lo svolgimento delle attività di *mining*, infatti, richiede che i *miners* usino un'enorme quantità di energia elettrica per risolvere i calcoli complessi implicati dalle transazioni (vedi nota 2), al punto da far sorgere fondati dubbi sulla reale sostenibilità di blockchain e di Bitcoin qualora esse fossero adottate su scala molto ampia. Si stima che l'attuale consumo globale di energia per i server che eseguono il software bitcoin sia almeno di 2,55 gigawatt (GW), che equivale a un consumo di energia di 22 terawatt-ora (TWh) all'anno - quasi come il consumo energetico dell'Irlanda. Google, al confronto, ha utilizzato 5,7 TWh in tutto il mondo nel 2015 (G.F. "Why bitcoin uses so much energy", The Economist 9 luglio 2018 - <https://www.economist.com/the-economist-explains/2018/07/09/why-bitcoin-uses-so-much-energy>). Ovviamente il protocollo basato sulla *Proof of Value* è coerente con una intensa attività di ricerca orientata al superamento delle più preoccupanti difficoltà tecniche connesse all'applicabilità e alla sostenibilità di Blockchain. [10] La nostra analisi non vuole cioè accreditare alcun tipo di determinismo tecnologico. In questo senso il nostro approccio differisce notevolmente da Rifkin (2014) secondo il quale il progresso tecnico dovrebbe dare luogo, quasi inevitabilmente, al passaggio di una gamma sempre più ampia di beni e servizi, compresa l'energia, nel campo dei beni non rivali e non escludibili (vedi Vercellone et. Al 2015 nota 54) . [11] E' chiaro, ad esempio, che essendo molti beni comuni situati in contesti non metropolitani (es. aree rurali, montane, ecc.), la necessita di un'adeguata e diffusa infrastruttura di rete Internet è indispensabile all'utilizzazione di un sistema d'uso delle risorse basato su blockchain. [12] Non è possibile, in questo senso, non ricordare il lavoro innovativo svolto da Stefano Rodotà nella Commissione Ministeriale per la modifica delle norme del codice civile in materia di beni pubblici, da lui presieduta nel 2007, finalizzata all'affermazione in Italia del concetto giuridico di bene comune, da intendersi come un bene autonomo da un bene di proprietà privata e da un bene di proprietà pubblica (si veda al link https://www.giustizia.it/giustizia/it/mg_1_12_1.wp?contentId=SPS47617). Tra le altre cose la Commissione propose in via preliminare l'inclusione nel concetto di bene (definito dall'articolo 810 del Codice Civile italiano) di 'cose intangibili' come i beni finanziari e lo spettro elettromagnetico.

Blockchain per il bene comune?

[caption id="attachment_9746" align="aligncenter" width="300"]



blockchain[/caption]