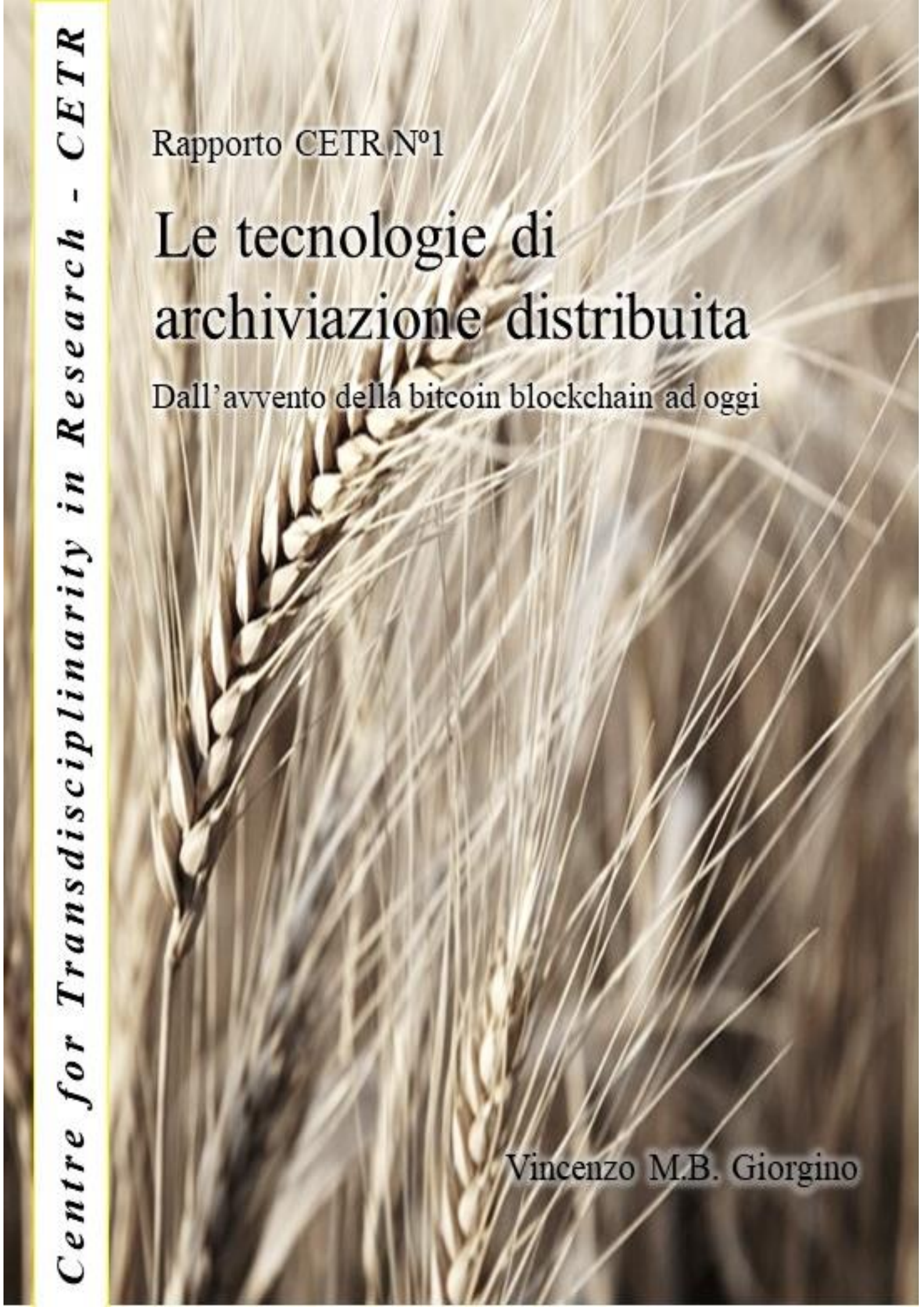


Centre for Transdisciplinarity in Research - CETR

Rapporto CETR N°1

Le tecnologie di archiviazione distribuita

Dall'avvento della bitcoin blockchain ad oggi

Vincenzo M.B. Giorgino

Rapporto CETR Nº1

Le tecnologie di archiviazione distribuita

Dall'avvento della bitcoin blockchain ad oggi

31 Maggio 2021

Vincenzo M.B. Giorgino

Indice

Premessa

L'attenzione verso le tecnologie d'archiviazione distribuita (TAD, in inglese l'acronimo è DLTs, Distributed Ledger Technologies) è data dalle enormi potenzialità che esse offrono per la vita sociale, a partire dalle transazioni economiche per finire a qualsivoglia forma di "contratto" tra due o più soggetti. Si tratta di archivi con proprietà e capacità superiori agli archivi tradizionali e che "possono essere condivisi da una rete di molteplici siti, geografie e istituzioni" (GOS 2016: 5).

Come a suo tempo per Internet, le aspettative sono molteplici. E le delusioni di ieri possono costituire le sagge basi per non alimentare nuove illusioni e soprattutto commettere errori di progettazione e di scelte politiche. Una progettazione consapevole può rappresentare una vera e propria rivoluzione sociale, molto più che una sia pur importante evoluzione tecnologica; questa darebbe consistenza all'emersione e all'affermazione di quella società collaborativa in rete definita da Castells "non capitalismo" e da altri società dei commons collaborativi (Rifkin 2014). Come già in passato per altre tecnologie – l'impiego del vapore, dell'elettricità ecc.. – ciò comporta il cambiamento di schemi mentali attraverso l'acquisizione di nuove capacità, abilità e saperi…" (GOS 2016: 55).

1.0. Cos'è la blockchain

La prima TAD che ha attirato attenzione ed interesse a livello internazionale è quel tipo di database definito blockchain, un'infrastruttura costituita da un archivio pubblico decentrato, gestito da una rete di partecipanti. Ciò significa che non ci sono terze parti a convalidare le interazioni e a mantenerne traccia, inoltre i dati vengono mantenuti per sempre, in forma trasparente e accessibile a tutti. La prima applicazione ha riguardato una valuta digitale, la bitcoin, ma, come vedremo, le interazioni tra partecipanti possono estendersi a forme non monetarie.

Una blockchain è un tipo di archivio dati che aggrega un certo numero di record in un blocco: questo elemento la differenzia da altre TAD. Ogni blocco è agganciato ad un altro blocco attraverso una firma crittografica. In sostanza abbiamo a che fare con un'importante novità: questi database non raccolgono solo dati, ma possono stabilire proprie regole di funzionamento. E' oltremodo importante comprendere attraverso quali regole e procedure si mette in atto l'obiettivo di validazione senza terze parti delle transazioni, processo che nella bitcoin blockchain è definito *consenso*.

Nick Szabo, un informatico accademico che ha fortemente contribuito alla nascita della bitcoin, va all'osso dicendo che una blockchain è tale se ha dei blocchi e delle catene (2017: 10), le catene sono alberi Merkle (cioè un albero per lo più binario), o simili strutture crittografiche con la stessa integrità di non falsificazione ex post.

E aggiunge:

"Dire che i dati sono post-falsificabili o immutabili significa che non possono essere alterati una volta vincolati alla blockchain. Contrariamente ad alcuni punti di vista diffusi questo non garantisce nulla circa la provenienza di un dato, o la sua verità o falsità, prima che fosse vincolato alla blockchain. Ciò richiede protocolli aggiuntivi, che spesso includono costosi controlli tradizionali. Le blockchain non garantiscono la verità; conservano solo la verità e le menzogne da successive alterazioni, consentendo di analizzarli in modo sicuro e quindi di essere più sicuri di scoprire le bugie" (Szabo 2017: 11).

La conferma dell'accuratezza dell'archiviazione – o *consenso* – avviene in modi diversi a seconda del tipo di blockchain. Se i partecipanti all'archivio sono preselezionati da un qualsiasi grado di accentramento e di proprietà allora si tratta di un archivio autorizzato (*permissioned* blockchain o privata); in tal caso la validazione avviene attraverso un numero circoscritto di attori sulla base delle scelte dei proprietari; in essa l'archivio è controllato dall'organizzazione e i permessi all'accesso sono gestiti da essa. Se è totalmente decentrato, senza alcun proprietario, allora è definito "senza autorizzazione" (*permissionless* blockchain o pubblica[1]) e la validazione avviene da parte dell'insieme degli attori. Aggiungo che la blockchain pubblica è quella basata sul mining, come spiegato in seguito, cioè su incentivi economici per la sua validazione crittografica. L'accesso ai dati è libero.

Esiste un terzo tipo, ibrido, definito *Consortium* blockchain (Buterin 2015). Nella blockchain consorziata il *consenso* è controllato da un insieme di nodi pre-costituiti, e l'accesso ai dati può essere limitato o libero.

Negli ultimi due tipi i dati delle transazioni possono essere modificati dai proprietari così come le regole.

I principali criteri esistenti per il *consenso* nella blockchain pubblica:

- La **Proof of work** (PoW) caratterizza la BTC ed ETH (quest'ultima ancora per poco). Essa può essere vista come il "diritto" a partecipare al sistema TAD. Gli utilizzatori non possono modificare i dati, protetti dagli hash crittografici, garanti dell'autenticità della transazione. Il meccanismo architettato da Satoshi Nakamoto (2009) si basa sulla distribuzione di incentivi ai validatori detti miner . E' però è oltremodo costoso perché per la bitcoin si spendono 600M di $ all'anno ed inoltre nel tempo gli incentivi ai minatori (vedi paragrafo successivo) sono destinati a calare.

- La **Proof of stake** è stata messa a test da Ethereum nel novembre 2020 e dovrebbe a breve diventare operativa. La **proof of stake** è l'alternativa più economica ma più difficile da

[1] PKI: In crittografia una **infrastruttura a chiave pubblica**, in inglese **public key infrastructure** (**PKI**), è un insieme di processi e mezzi tecnologici che consentono a terze parti fidate di verificare e/o farsi garanti dell'identità di un utente, oltre che di associare una chiave pubblica a un utente, normalmente per mezzo di software distribuito in modo coordinato su diversi sistemi. Le chiavi pubbliche tipicamente assumono la forma di certificati digitali.

wikipedia https://it.wikipedia.org/wiki/Infrastruttura_a_chiave_pubblic

realizzare: oltre a decidere chi aggiorna il *consenso* sulle transazioni essa previene anche possibili biforcazioni sottotraccia. In essa i blocchi sono creati dai coniatori (*minter*) che scommettono i loro gettoni su quali blocchi sono validi.

Ci sono diversi altri criteri, basti saperlo; in ogni caso ciò mostra come non esista una tecnologia con un funzionamento omogeneo - la blockchain al singolare - ma vari possibili protocolli di validazione delle transazioni e degli incentivi.

2.0. La bitcoin blockchain

Si deve ad un misterioso Satoshi Nakamoto (pseudonimo di un individuo o gruppo) la pubblicazione in rete nel 2009 di un ormai celebre white paper ”Bitcoin: A Peer-to-Peer Electronic Cash System””(https://bitcoin.org/bitcoin.pdf?).

Secondo il protocollo lì definito, l’agente che opera nel contesto bitcoin si identifica tramite uno pseudonimo. La moneta bitcoin viene costantemente creata nella rete sino al limite prestabilito di 21M di unità divisibili ognuna per otto decimali. La distribuzione di nuove unità si basa sulle transazioni che avvengono in essa e che sono crittografate automaticamente al loro verificarsi, senza intermediari.

A certificare le transazioni sono tutti i *minatori*, cioè quei partecipanti alla rete di Bitcoin che decidono di risolvere un puzzle matematico. I calcoli di tutti i partecipanti sono coordinati da una funzione matematica definita *consenso*, come anticipato all’inizio. La soluzione avviene ogni circa 10 minuti e chi risolve il quesito ottiene x bitcoin messi in circolazione dal sistema in una quantità prestabilita. I minatori, transazione dopo transazione, costruiscono blocchi e la loro attività di convalida è appunto remunerata attraverso l’emissione di nuova moneta.

Ogni blocco si lega al precedente con un numero di sequenza e un meccanismo matematico: il tutto a formare una catena di blocchi. Essa è unica, indipendente (un singolo nodo non può modificare il funzionamento), irreversibile, programmabile, rintracciabile (Il Sole 24 Ore 2016: 19) e contiene la memoria di tutte le precedenti transazioni.

I compensi in bitcoin, in origine corrispondenti a 25 btc, vanno decrescendo ogni quattro anni del 50%: ora – dal luglio 2020 - sono di 6,25 btc. La competizione per convalidare e acquisire il

premio dovrebbe rendere difficile ogni tentativo di monopolizzare la moneta. In realtà, la complessità dei quesiti matematici implica l'impiego di una grande potenza dei computer di chi sceglie di "minare", con un conseguente grande dispendio di energia. E'un costo che non tutti si possono permettere, di qui il fenomeno di progressiva centralizzazione rilevato dal 2014, in cui il 20-30% delle bitcoin era già in possesso di pochi grandi giocatori. A fine 2020 (Kharif 2020) il 95% delle btc pare in possesso di circa il 2% dei nodi. Sebbene ci sia consenso diffuso su questo accentramento, alcuni lo contestano sulla base di una ridefinizione dei criteri su cui si basa (Schulze-Kraft R. 2021, per i dettagli dello studio vedi: Schulze-Kraft R. 2020)[2].

Ogni partecipante ha un portafoglio elettronico (wallet) che contiene non solo le transazioni del suo titolare ma tutte le transazioni. Il mezzo per garantire al contempo riservatezza e pubblicità sta nelle due chiavi di identificazione. Le chiavi pubbliche individuano con uno pseudonimo il titolare, mentre le chiavi private permettono di agire nella transazione, cioè di convalidare un dato trasferimento da un portafoglio ad un altro.

Se un messaggio è criptato con una chiave pubblica, sarà possibile leggerlo solo se si dispone della corrispondente chiave privata e viceversa. Criptando una richiesta di transazione con il portafoglio privato si genera una firma digitale che serve a verificare la fonte e l'autenticità della transazione.

Pertanto i costi delle bitcoin sono coperti dalla creazione di nuova moneta, che si può considerare una forma di socializzazione del signoraggio[3].

La garanzia che la transazione sia automaticamente effettuata con valori disponibili dall'acquirente o dal venditore è data dal fatto che essa va a buon fine solo se essi sono presenti nel portafoglio, alla luce di tutte le transazioni precedenti e visibili a tutti.

Poiché non esiste un server centrale con servizi di protezione dati, né un deposito per essi, i dati del portafoglio sono essenziali ed è suggerito di tenerli al di fuori di ogni dispositivo

[2] In sintesi, l'autore sostiene che il criterio usuale basato sul numero di indirizzi non è una base affidabile perché un indirizzo Bitcoin non è un "account". Un utente può controllare più indirizzi e un indirizzo può contenere i fondi di più utenti. L'autore crea otto categorie di entità in base alle loro partecipazioni in Bitcoin, dai Gamberetti (<1 BTC) alle Balene (1.000-5.000 BTC) e Megattere (> 5.000 BTC). Durante l'ultimo anno – 2020 - nella parte più ampia dello spettro le balene e le megattere sono le più grandi entità non di scambio che insieme controllano circa il 31% delle Bitcoin, mentre entità più piccole che sostengono fino a 50 BTC controllano quasi il 23% della fornitura. In sintesi risulta che circa il 2% delle entità di rete controlla 71,5% di tutte le Bitcoin.

[3] con esso si intende il reddito derivante dalla coniazione di moneta: nel nostro sistema esso viene percepito dalle banche centrali.

in rete (può suonare ironico il fatto che una tecnologia tanto sofisticata richieda il ricorso ad una archiviazione offline così primitiva come un appunto su un foglio di carta, da riporre in un luogo sicuro).

Se due nodi risolvono nello stesso momento il problema, hanno diritto a costruire entrambi il proprio blocco, e il sistema obbliga entrambi a costruirlo sulla catena più lunga disponibile (quindi con più operazioni, perciò più veloce ed efficiente), questo per evitare una situazione di ambiguità che aprirebbe la porta ad una frode (D'Aliessi 2016). Il sistema è protetto anche da un eventuale attacco da parte di chi riesca a disporre del 50% del potere complessivo di tutta la rete blockchain in quanto ogni attaccante è in competizione con tutti gli altri nodi. Poiché in genere un personal computer necessita di un anno per risolvere il problema matematico, si costituiscono dei consorzi detti "mining pool". Va però detto che a tutt'oggi un solo operatore ha il 47% della potenza di calcolo complessiva.

Alcune voci sono critiche rispetto alle modalità del dibattito e sulle caratteristiche dei programmi sviluppati. Lo sviluppatore di *Adapt*, Bulkin, fa cenno allo spirito acritico - permeato di alterigia, che circonda la costruzione di "sistemi sociali assistiti da computer" quali sono i sistemi decentrati come la blockchain, e come in essi le discussioni sulle implicazioni sociali siano pressoché assenti. Egli auspica il potere del "non sapere" come regola aurea per muoversi con consapevolezza in sistemi sociali complessi per loro natura. E nota che il decentramento non è stato pienamente attuato dall'inizio, e che le scelte alla base di "Ethereum, Eos, Cosmos, Cardano, Stellar sono piccoli puntini in uno spazio di possibilità in cui potremmo trovare altre soluzioni, magari più praticabili e sostenibili" (Bulkin 2018). Altre critiche molto recenti vengono dall'interno della comunità di sviluppatori con l'accusa di eccesso di centralizzazione nelle decisioni (Hearn M. 2016).

I problemi aperti sono diversi, ma tre sembrano le priorità tecnico-ideologiche dei fautori e sviluppatori di bitcoin blockchain: scalabilità, decentramento e sicurezza (Asolo 2018). Buterin (2018) indica come non si possano conseguire i tre obiettivi insieme; di fatto solo due sono perseguibili e sono quelli alla base della creazione di bitcoin blockchain e di ethereum: decentramento e sicurezza, a spese della scalabilità. Dato per scontato il significato di decentramento, definito sopra, con l'ultima proprietà si intende la possibilità di gestire transazioni su ogni data rete, la quale può essere costituita da milioni di utilizzatori (*Vedi la voce scalabilità nel glossario minimo in appendice*). Ad es. bitcoin blockchain può gestire 7 transazioni al secondo, ethereum 15 al sec, mentre VISA 24.000 per sec.

La sicurezza invece pertiene all'immutabilità dell'archivio dati e alla sua resistenza ai vari

tipi di attacchi, anche se ci sono contributi critici su questo punto (si veda il saggio di Eyal e Sirer (2013). Per Nick Szabo (2017), uno dei protagonisti della nascita di bitcoin, più un'istituzione dipende da leggi locali, abitudini, o linguaggio, meno è socialmente scalabile. Una tecnologia con alto grado di scalabilità sociale permette ad un crescente numero di persone di poter agire socialmente, diminuendo i costi cognitivi necessari per l'interazione. Per molte tecnologie ormai parte della società attuale, è dato per scontato l'effetto di riduzione dell'impegno cognitivo nelle relazioni - lui li chiama protocolli intersoggettivi - ad esempio la legge, il mercato o il denaro.

Oggi Internet ha prodotto un'alta scalabilità sociale attraverso il *matchmaking*, favorito da social network come Facebook, Twitter o piattaforme come Uber ebay AirBnB etc… e ha liberato in forma esponenziale gli attori sociali dal vincolo dato dalla massima dimensione che un gruppo sociale può avere in base alle nostre possibilità cognitive - cioè 150 persone circa secondo l'antropologo Dunbar - rispetto a quanto permettevano altre tecnologie in precedenza.

Per Szabo, la blockchain dà invece il suo contributo nella *minimizzazione della fiducia*. Internet è stato concepito, secondo questo autore, come un'architettura controllabile da una persona o organizzazione che si relaziona ad altre sulla base della conoscenza e fiducia reciproche:

"When we currently use a smartphone or a laptop on a cell network or the Internet, the other end of these interactions typically run on other solo computers, such as web servers. Practically all of these machines have architectures that were designed to be controlled by a single person or a hierarchy of people who know and trust each other. From the point of view of a remote web or app user, these architectures are based on full trust in an unknown "root" administrator, who can control everything that happens on the server: they can read, alter, delete, or block any data on that computer at will. Even data sent encrypted over a network is eventually unencrypted and ends up on a computer controlled in this total way. With current web services we are fully trusting, in other words we are fully vulnerable to the computer, or more specifically the people who have access to that computer, both insiders and hackers, to faithfully execute our orders, secure our payments, and so on. If somebody on the other end wants to ignore or falsify what you've instructed the web server to do, no strong security is stopping them, only fallible and expensive human institutions which often stop at national borders" (Szabo 2017).

Questo è il problema che Satoshi Nakamoto ha affrontato con successo nel 2009. E, per Szabo, tornando alla bitcoin blockchain, Nakamoto ha privilegiato la sicurezza sulla prestazione e il prezzo richiesto per la necessaria ridondanza sta nell'alto consumo di energia: l'integrità basata sulla matematica esige una piena diffusione tra tutti i nodi. In conclusione, richiamando le attuali sperimentazioni per aumentare la scalabilità sociale, Szabo nota come non siano tanto

le limitazioni delle attuali tecnologie di rete a lasciare ancora fuori da esse una gran parte di potenziali partecipanti, ma "i limiti della mente e delle istituzioni che non sono di solito sufficientemente riprogettate o sviluppate per avvantaggiarsi dei miglioramenti tecnologici resi disponibili negli ultimi decenni" (Szabo 2017: 14).

In linea generale, la scalabilità appare concepita da Szabo in una dimensione riduzionista, per cui ogni variabile di origine sociale (linguaggi, istituzioni, norme e culture…) siano ostacoli da superare per una piena scalabilità "sociale" (nel senso dell'autore). Sfugge del tutto il fatto che tali strumenti sono frutto di lavoro relazionale volto a definire confini tra sfere socio-economiche diverse, e la non scalabilità è del tutto voluta per garantire l'esistenza di un certo tipo di legami sociali: un tema che necessita uno sviluppo che va oltre i limiti di questo testo e sarà ripreso in un altro contributo.

Resta interessante l'osservazione di Szabo per cui le visioni utopiche basate su sistemi progettati da zero hanno poco futuro rispetto al lavoro di ingegneria inversa[4].

A riprova che anche questa "internet del valore" è un processo relazionale, stanno i diversi significati attribuiti alla bitcoin alla sua origine. Da un lato alcuni visionari l'hanno vista come un sistema senza gerarchie di controllo, basato su una forma di fiducia distribuita tra pari, dall'altro speculatori della finanza tradizionale l'han vista come una nuova succulenta opportunità di predazione, lo stesso dicasi per la criminalità organizzata che l'ha intesa come una forma riciclaggio di denaro proveniente da traffici illeciti. Si tratta di incidenti di percorso di un esperimento che resta.

[4] Il processo di **reverse engineering** (anche chiamato in italiano **ingegneria inversa**) consiste nell'analisi dettagliata del funzionamento, progettazione e sviluppo di un oggetto (dispositivo, componente elettrico, meccanismo, software, ecc.) al fine di produrre un secondo oggetto che abbia un funzionamento analogo, magari migliorando o aumentando l'efficienza dello stesso, senza in realtà copiare niente dall'originale; inoltre, si può tentare di realizzare un secondo oggetto in grado di interfacciarsi con l'originale... In senso stretto, l'attività di ingegneria inversa consiste nella comprensione del funzionamento e della realizzazione di un dispositivo fisico o virtuale al fine di produrre il nuovo dispositivo. Il termine reingegnerizzazione, invece, comprende, oltre all'analisi, anche il ridisegno (wikipedia).

Tabella 1. Confronto tra modello bancario tradizionale e bitcoin blockchain nelle transazioni.

BANCA	**BITCOIN Blockchain**
Il soggetto ha un conto corrente privato	il soggetto ha un indirizzo digitale pubblico
Esiste un modo per dimostrare di avere il controllo del numero di conto, ad esempio un codice PIN	
3. La banca, a sua volta, ha la documentazione di quanto denaro è imputabile a questo numero di conto, mantenendo così l'ammontare del denaro della persona su un registro privato o database interno.	Internet è il sistema di identificazione nella rete Bitcoin
4. La persona può quindi utilizzare un sistema di comunicazione elettronica per identificare se stessa alla banca come titolare del conto autentico e può richiedere che il denaro associato al numero di conto venga trasferito sul conto di qualcun' altro in una banca diversa.	I minatori
5. Quindi questo fa sì che la banca modifichi il registro - cambiando il saldo e chieda alla banca del destinatario di fare lo stesso.	Le due parti interessate possono vedere la transazione confermata.

3.0. Più di un *database*: Ethereum e i "contratti intelligenti".

Il primo passaggio da tenere a mente è il fatto che si può passare, con opportune modifiche del sistema di codifica, da un'archiviazione di transazioni finanziarie a quella di dati relativi a qualsiasi cosa: titoli di proprietà, identità, decisioni di voto ecc… Per queste finalità è stata concepita Ethereum, una piattaforma con una sua blockchain, basata su di un linguaggio di programmazione più potente di bitcoin blockchain e pensata per applicazioni distribuite, in specie *smart contract*.

Gli *smart contract*

Per "contratto intelligente" si intende uno strumento che usa un codice di un software per agire/realizzare delle intenzioni umane eseguendo in modo dinamico delle istruzioni inserite in token (gettoni) associati ad una transazione, "piuttosto che contare su testi legali interpretati da tribunali, corpi regolatori o altre istituzioni legali" (DCO: 7). In altri termini, si tratta di "contratti" digitali auto-eseguiti che utilizzano la blockchain per documentare e verificare l'esecuzione di quanto descritto.

Sono cinque i punti alla base di uno smart contract:

1. viene scritto il codice che esegue una funzione specifica;

2. il codice è messo in produzione attraverso l'allocazione in una rete distribuita;

3. l'agente uno entra nel contratto inviando dei token ad un indirizzo controllato dal codice;

4. ulteriori agenti interagiscono con il contratto con lo stesso metodo;

5. il codice prende i token ed esegue alcune funzioni con essi, redistribuendoli potenzialmente alle parti nelle fasi 3 e 4.

Gli *smart contract* di Ethereum sono pacchetti (bundle) di codici che possono essere registrati sulla blockchain in modo che gli utilizzatori possano usarli per concordare e realizzare compiti specifici (vedi Wright e De Filippi 2015), per esempio un contratto di assicurazione (Mainelli and Von Ginten 2014).

Nel caso specifico, le TAD permettono la costituzione di organizzazioni autonome distribuite (DAO) attraverso le quali i soggetti possono stabilire contratti intelligenti con un minimo di intervento umano (per ulteriori precisazioni sullo stato dell'arte degli *smart contract* e sui fraintendimenti correnti in merito vedi De Filippi et al. 2021). L'esempio del Bitcoin può servire: le TAD offrono dei servizi finanziari a basso costo all'interno del sistema esistente ma possono anche sfidare la centralizzazione proprietaria che comporta la moltiplicazione di centri separati. Dal monopolio governativo nella creazione di moneta si passa all'emergere di nuove forme di valuta dove "identità e relazioni tra le persone diventano i mezzi di sostegno e di sottoscrizione delle transazioni in una comunità" (GOS: 57).

Se è vero che le tecnologie sono costruzioni sociali, sembra di intravedere in queste l'onda lunga della cultura libertaria del '68, rielaborata alla luce dello sviluppo capitalistico e della sua fase attuale. Esse permettono di sostituire le attuali organizzazioni gerarchiche - sia nel mercato che nello stato - con sistemi più distribuiti.

4.0. La tokenizzazione.

Per introdurre questo processo fondamentale conto in primis sulle argomentazioni offerte da Wenkler in vari interventi. Egli osserva come grazie all'HTTP, il protocollo di base del web, gli utilizzatori abbiano potuto accedere alla pubblicazione decentralizzata: chiunque può gestire un server Web e pubblicare i propri contenuti. E chiunque abbia un browser Web può accedere a quel contenuto, soggetto a limiti posti dagli stati e dall'ISP (=Internet Service Provider). Ma l'HTTP è un protocollo senza stato (*stateless*) cioè senza memoria - una volta terminato lo scambio, la connessione viene chiusa senza mantenere i dati di sessione o altro (http://www.html.it/) - perciò ha bisogno di un data layer[5] per ogni applicazione. Esso fino a poco tempo fa era fornito da aziende come Google (ricerca), Facebook e Twitter (social), Amazon e eBay (commercio) (Wenger A. 2016). Secondo Wenkler, poiché non si sapeva come mantenere la memoria delle connessioni in modo decentralizzato, si deve al *data layer* la spinta alla centralizzazione del web che lo ha caratterizzato sino ad oggi.

In passato molti protocolli sono stati creati da ricercatori - spesso ciò rimanda al ruolo dello stato, trattandosi di enti di ricerca statali o finanziati dal settore pubblico - come TCP/IP e HTTP[6], mentre il profitto nasceva dalle applicazioni connesse ad essi e vendute da imprese private. In altri termini, l'unico modo per ricavare profitti da un protocollo era quello di creare software che lo rendeva operativo e quindi provare a vendere questo software (o, più recentemente, ad ospitarlo). Poiché la creazione di questo software (ad es. Web server/browser) è un atto separato, molti dei ricercatori che hanno creato alcuni dei protocolli di maggior successo oggi in uso hanno avuto scarsi guadagni finanziari diretti. Successive iterazioni di questi protocolli sono state spesso gestite da organizzazioni no-profit che hanno tentato di risolvere con

[5] Il Data Layer è un codice che può essere usato per portare eventi e variabili in Google Tag Manager; in altri termini esso è un vettore Javascript creato da Google Tag Manager.

Un vettore è una struttura più o meno complessa di dati presente in tutti i linguaggi di programmazione: un vettore JavaScript ha la funzione di immagazzinare più variabili.

[6] Il protocollo HTTP (*HyperText Transfer Protocol*, "protocollo di trasmissione di documenti ipertestuali") creato da un gruppo di ricerca del CERN di Ginevra diretto da Tim Berners-Lee, svolge il ruolo di intermediazione nel modello richiesta-risposta all'interno dell'architettura *client*-server, vale a dire che permette lo scambio di informazioni tra due nodi della rete gestendo sessioni di comunicazione, richieste e quant'altro connesso a questo processo. Un esempio è quello di un web browser, che svolge la funzione di *client* (cliente), sul nostro computer mentre un'applicazione (un software, un documento digitale, ecc.) disponibile su un altro computer connesso alla rete e ospitante una risorsa web, svolge la funzione di server. Il server risponde all'interrogazione in arrivo dal *client* fornendo la risorsa digitale richiesta come ad esempio una pagina HTML.

più o meno successo i vari interessi commerciali sorti attorno a questi protocolli (le aziende che producevano e vendevano software e hardware basati su di essi): quanto più denaro si trattava tanto più la cosa diventava difficile.

La tecnologia blockchain ha aperto la strada ad una soluzione decentrata del problema della memoria e dell'archiviazione dei dati di ogni sessione (Wenger 2016, vedi anche Wenger 2013 e 2014).

Rammento inoltre che se si verifica un attacco ad un server proprietario centralizzato, ad es. Airbnb o Twitter, tutta la rete ne è colpita e i dati presenti possono essere distrutti e persi. Al contrario, se qualcuno attacca un server decentrato, i dati non saranno mai distrutti perché sono presenti in ognuno dei nodi partecipanti alla rete.

Tutto nasce dal protocollo della bitcoin, in quanto esso ha il potenziale per consentire molteplici innovazioni:

"Il cuore di bitcoin è un'innovazione fondamentale: un libro mastro pubblico distribuito. … Al giorno d'oggi non esiste un altro protocollo ampiamente utilizzato nel mondo che lo permetta: con bitcoin chiunque può fare una dichiarazione (una transazione) e farlo registrare in un registro globale visibile e fisso. A causa del linguaggio di programmazione, il libro mastro è in realtà intelligente e una volta che le transazioni sono registrate in esso, diventa possibile costruire versioni automatizzate di contratti derivati, cioè tipi di contratti come depositi, impegni, fino al commercio di azioni distribuito" (Wenger 2014).

Ciò consentirà, secondo Wenger, la creazione di protocolli che possono minare la posizione dominante delle aziende del modello FAANG (Facebook, Apple, Amazon, Netflix e Google).

L'intreccio tra decentramento e centralizzazione viene chiarito dalla figura a pagina successiva con esempi che ci riportano a piattaforme note.

	Centralizzazione organizzativa	Decentralizzazione organizzativa
Centralizzazione logica	Paypal	*new* Bitcoin
Decentralizzazione logica	Excel	e-mail

Tabella 2 : Centralizzazione Organizzativa e Logica vs Decentralizzazione.

La colonna "centralizzazione organizzativa" sulla sinistra contiene sistemi controllati da una singola organizzazione (EBay e Microsoft negli esempi, [potrebbe anche essere un'istituzione statale]). Viceversa, la colonna " decentralizzazione organizzativa" a destra contiene sistemi che non sono sotto il controllo di alcuna entità, sia essa a scopo di lucro o altro. La riga " decentralizzazione logica" nella parte inferiore contiene sistemi con più database e in cui il partecipante controlla interamente il proprio database (es. invio di un un file Excel da A a B con B che lo legge e modifica solo sul suo dispositivo). Anche con la posta elettronica controlliamo ciascuno i nostri database separati. Viceversa, la riga "centralizzazione logica" in alto contiene sistemi che appaiono come se avessero un unico database globale (l'autore usa il verbo "apparire" perché tecnologicamente potrebbero esserci molti sistemi di database separati coinvolti). "Centralizzazione organizzativa" significa che chiunque nel mondo ottiene la stessa risposta quando interpella il sistema. La rilevanza della blockchain sta nel rendere possibile il quadrante in alto a destra. Il caso in alto a sinistra esisteva già: ad es. Paypal mantiene un database centralizzato logicamente per la sua infrastruttura di pagamento. Fino ad ora tutti questi sistemi dovevano essere controllati da un'unica organizzazione… prima dell'esistenza della blockchain **non** esistevano sistemi decentralizzati a livello organizzativo e centralizzati dal punto di vista logico. Questo è il motivo per cui Bitcoin è una tecnologia così fondamentale. Quando invio Bitcoin a qualcuno, sia il debito che il credito sono registrati nella blockchain anche se quel database non è controllato da un'organizzazione (ridotto e adattato da Wenger 2014, 2013). Pertanto, con la blockchain, possono essere introdotti dei gettoni crittografici in modo da fornire incentivi per la creazione di protocolli e per governare la loro evoluzione. Wenger (2016) argomenta:

"Puoi pensarli come gettoni che potresti comprare in un luna park per andare in giro: diversi operatori possono avere le loro giostre e impostare il proprio prezzo in termini di gettoni. Hai solo bisogno di acquistare gettoni una volta in cambio di valuta fiat (= moneta cartacea inconvertibile a corso legale, emessa da uno Stato e accettata come mezzo di pagamento indipendentemente dal suo valore intrinseco) e poi usarli in questo circuito. … …

Un'azienda a scopo di lucro può così sviluppare un nuovo protocollo e creare valore per se stessa (e i suoi investitori) mantenendo alcuni dei token. Se il protocollo diventa ampiamente utilizzato, il valore dei token aumenterà. … Esiste già una varietà di protocolli di questo tipo, tra cui Storj, SIA e Filecoin".

Con i token, quindi, i creatori di un protocollo possono "monetizzarlo" direttamente e in effetti ne trarranno beneficio in quanto altri costruiranno aziende in base a quel protocollo. Dato questo nuovo incentivo, ci si può aspettare che molte risorse siano dedicate all'innovazione del protocollo. … C'è anche un limite naturale di tariffa su quanta parte della ricchezza può essere trattenuta. Poiché il protocollo è pubblico (per definizione) se un creatore tenta di conservare troppi token, c'è un incentivo per tutti gli altri a replicare il protocollo con un nuovo token, nessuno dei quali viene trattenuto. Inoltre, ci si può aspettare anche un processo più democratico di decisione. Quanto sopra dipende, come riconosce Wenger, anche da come saranno classificati questi token dagli enti istituzionali: biglietti per un giro di giostra o una specie di titoli obbligazionari cartolarizzati (s*ecurities)*? Lui spera si scelga il primo dei due.

I token digitali

I token non sono invenzione recente. Conchiglie, pietre, bastoncini e di recente voucher, carte premio, punti raccolta ecc.. sino ai codici QR hanno costituito parte della creatività umana nel definire specifici rapporti economici e nel mantenerne traccia all'interno di specifiche relazioni sociali.

Cos'è allora un token digitale? E' una risorsa digitale scarsa che può essere trasferita (non semplicemente copiata) tra due parti su Internet senza richiedere il consenso di alcuna altra parte (Srinivasan 2017). Essi rappresentano diritti di accesso ad un sottostante valore economico (proprietà) o permesso d'accesso a servizi di qualcuno o a un bene collettivo. Ogni token appartiene ad un indirizzo blockchain ed è accessibile tramite un portafoglio ad hoc che comunica con la blockchain e gestisce la chiave pubblica-privata.

Già nel 2014 Balaji S. Srinivasan (2017) sosteneva che la bitcoin era qualcosa di più che una forma di denaro e un protocollo: si tratta di un modello e una piattaforma per un autentico *crowdfunding* aperto, distribuito e liquido a tutti gli effetti. Per l'autore il token non è capitale

azionario, essendo più simile a delle chiavi API a pagamento[7]. Rispetto ai tradizionali strumenti finanziari essi rappresentano un enorme passo avanti e aprono la strada a progetti prima non alla portata del *venture capital* (per un aggiornamento relativo alla capitalizzazione nei grafici citati da Srinivasan vedi https://coinmarketcap.com/charts/)

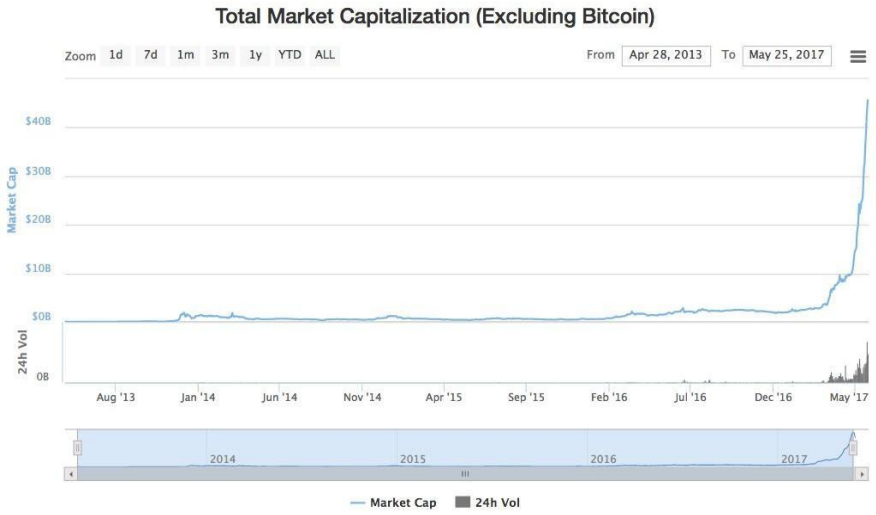


Grafico nº1 L'aumento esponenziale di token non Bitcoin nel 2017. Fonte: https://coinmarketcap.com/charts/

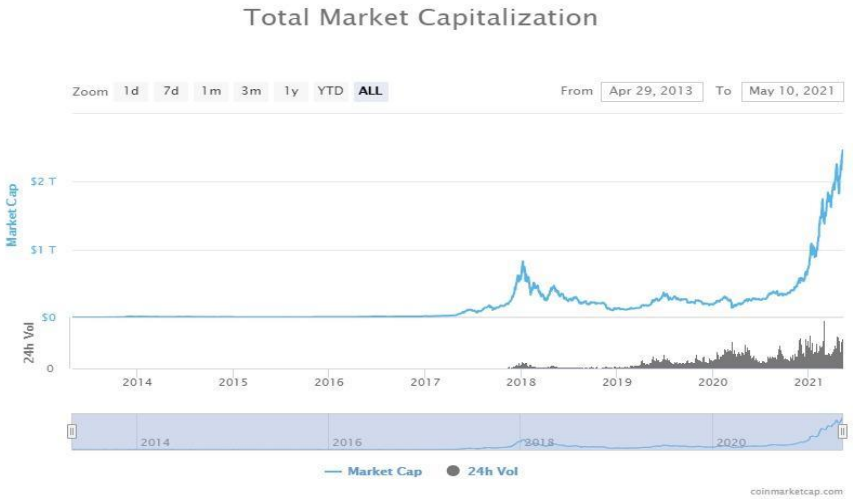
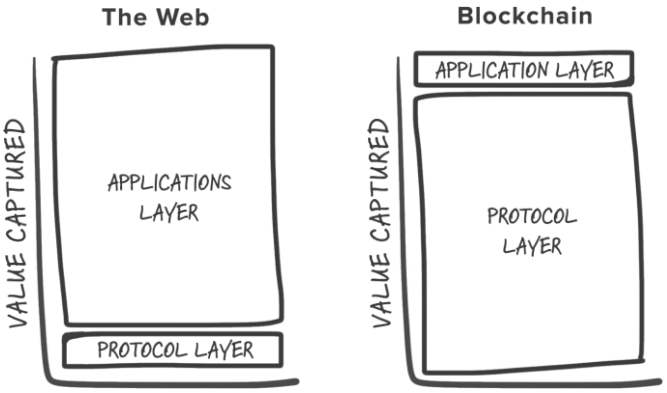


Grafico nº2 L'aumento esponenziale di token non Bitcoin ai nostri giorni: Fonte: https://coinmarketcap.com/charts

[7] **Application Programming interface**, o *interfaccia di programmazione di un'applicazione*, in informatica, si indica ogni insieme di procedure disponibili al programmatore, di solito raggruppate a formare un set di strumenti specifici per l'espletamento di un determinato compito all'interno di un certo programma. Spesso con tale termine si intendono le librerie software disponibili in un certo linguaggio di programmazione. Wikipedia: API).

E’ utile anche fare riferimento all’interpretazione che fornisce Monegro (2016), secondo il quale i protocolli originali di Internet mostrarono problemi di sicurezza nella protezione dei dati ed inoltre non prevedevano incentivi per gli utilizzatori allo scopo di sostenere l’innovazione degli stessi protocolli.

La generazione precedente di protocolli condivisi (TCP/IP, HTTP, SMTP, SSL etc.) ha prodotto un valore enorme, catturato in forma di dati sullo strato in cima. L’autore perciò sostiene che in termini di produzione di valore abbiamo a che fare con protocolli magri e applicazioni grasse (la prima figura qui sotto, Monegro J. 2016).



Nella blockchain avviene il contrario: il valore si concentra nel protocollo condiviso e solo una frazione di esso è distribuita tramite lo strato delle applicazioni: protocolli *grassi* e applicazioni *magre*. Un esempio? La rete Bitcoin ha una capitalizzazione di mercato di 1000 miliardi di dollari (nel febbraio 2021, ed erano 10 miliardi al tempo del blog di Monegro (2018), mentre le compagnie costruite su di esso valgono al massimo alcune decine di milioni.

Due punti comuni alla maggior parte dei protocolli basati sulla blockchain permettono che ciò succeda: il primo è l’archivio condiviso, il secondo è il token crittografico di accesso con un certo valore speculativo. Il secondo elemento permette l’accesso al servizio offerto dalla rete (transazioni per Bitcoin, potere di calcolo per Ethereum, ecc…).

Secondo l’autore, a parte iniziative deliberatamente fraudolente, la speculazione ha un valore positivo perché è il motore dell’adozione tecnologica. I suoi due aspetti – il boom e l’esplosione della bolla – sono benefici: il primo attrae capitale finanziario attraverso profitti

anticipati, parte dei quali sono reinvestiti nell'innovazione, mentre la bolla può di fatto sostenere l'adozione di lungo periodo della nuova tecnologia, dato che i prezzi scendono e gli investitori ne approfittano per promuovere e creare valore intorno ad essa.

Oltre alla speculazione, un secondo aspetto riguarda la fase in cui l'applicazione comincia ad aver successo: accade che nuovi utilizzatori sono attratti dal protocollo del token, la domanda di token aumenta, gli investitori esistenti mantengono i propri gettoni anticipando futuri aumenti di prezzo, limitando così ulteriormente l'offerta.

Queste due tendenze aumentano il prezzo (supponendo una scarsità sufficiente nella creazione di nuovi token), la capitalizzazione di mercato appena aumentata del protocollo attira nuovi imprenditori e nuovi investitori, e il ciclo si ripete.

Ciò che è significativo di questa dinamica è l'effetto che ha sul modo in cui il valore viene distribuito nello strato (stack): la capitalizzazione di mercato del protocollo cresce

sempre più velocemente del valore combinato delle applicazioni create presenti nello strato superiore, dal momento che il successo del livello o strato applicativo spinge ulteriori speculazioni a livello di protocollo. Inoltre, l'aumento del valore a livello di protocollo attira e incentiva la concorrenza a livello di applicazione. Insieme a una base dati condivisa, che riduce drasticamente le barriere all'ingresso, secondo Monegro, il risultato finale è un ecosistema di applicazioni vivace e competitivo con un valore complessivo distribuito a un vasto gruppo di azionisti. Questo è il modo in cui i protocolli tokenizzati diventano "grassi" e le sue applicazioni "magre". ... …

"La combinazione di dati aperti condivisi, con un sistema di incentivi che impedisce mercati acchiappa-tutto, rappresenta un cambiamento rilevante e cambia il gioco a livello di applicazione creando un'intera nuova categoria di aziende con modelli di business fondamentalmente diversi a livello di protocollo"

(Monegro 2016).

Molte delle regole stabilite sulla costruzione di aziende e sugli investimenti nell'innovazione non si applicano a questo nuovo modello: di fatto si apprende strada facendo.

Come si può comprendere da queste note, le posizioni sulla tokenizzazione sono piuttosto varie e le certezze in merito sono scarse.

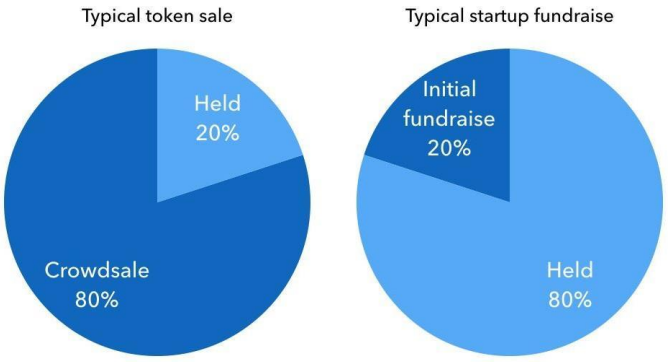
Si può condividere l'osservazione che la creazione di nuovi protocolli sia difficile in quanto essi non sono legati a incentivi: solo la creazione di specifiche applicazioni su di essi ha

portato a profitti (Outlook, Gmail ecc…). Ma la possibilità della loro decentralizzazione, connessa alla creazione di un token, rende appetibile per il pubblico sostenerne la creazione. In tal modo, le persone acquisiscono una proprietà parziale della rete ottenendo un token, che può accrescere il suo valore nel futuro. Essi acquistano una chiave privata, una sorta di password che non può essere modificata da alcuno (se per es si perde l'accesso e la risorsa). Essa, nel caso di Bitcoin appare così:

5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF Mentre per Ethereum può essere così:

3a1076bf45ab87712ad64ccb3b10217737f7faacbf2872e88fdd9a537d8fe266

Tramite l'emissione dei token è possibile effettuare un *crowdfunding* tramite una *crowdsale.* Quest'ultima consiste nella creazione e lancio di vendita di token per il finanziamento di un progetto. In genere il 10-20% dei token viene trattenuto da chi li emette e il restante 80-90% messo in vendita. Una piccola parte della prima tranche va immediatamente agli sviluppatori del protocollo a riconoscimento del loro lavoro, con la maggior parte destinata a finanziare il lavoro futuro. Ciò fornisce al progetto due fonti di finanziamento: i fondi raccolti nella vendita iniziale e la possibilità di vendere o erogare i token trattenuti in futuro (Ehrsam 2016). Notare che avviene il contrario nel caso delle start-up vedi grafico sotto.



Le classificazioni proposte per i token sono solo indicative, perché il campo è in movimento e i significati cambiano man mano che le tecnologie si evolvono e le sperimentazioni portano nuova acqua al mulino dell'innovazione. Di recente, Voshmgyr (2019) ha suggerito di considerare due specie di token: quelli nativi (o token protocolli) e quelli emessi al livello dello

strato applicativo. I primi sono parte dello schema di incentivi dell'infrastruttura decentrata. I token nativi sono posti su un primo strato mentre quelli applicativi sono creati su una sidechain, cioè una blockchain separata compatibile con la principale. I secondi nel caso di Ethereum possono essere emessi con poche linee di codice, permettendo una maggior scalabilità sociale, per dirla nei termini di Szabo.

Uno standard è ad esempio ERC-20, che ha le regole base per creare i token di Ethereum, token fungibili, cioè con lo stesso valore. Nel 2018 è stato introdotto ERC-721 per i token non fungibili (NFT). Questi ultimi sono strumenti più complessi che servono a rappresentare ogni tipo di collezionabile, prodotto artistico, proprietà o diritti di accesso personalizzati e altro ancora (e saranno parte del terzo rapporto CETR).

In genere i token appartengono ad un'unica rete, non possono essere scambiati fuori di essa perché le TAD sono diverse tra loro e ognuna richiede un portafoglio specifico. Alcuni programmi vanno però nella direzione dell'interoperabilità, come Cosmos o Polkadot, facilitandone l'uso e la diffusione di massa.

Difficile prevedere se prevarrà la visione verticale, tipica delle blockchain cosiddette private, volta a rendere più efficiente il sistema economico e più intrusivo il controllo dei comportamenti sociali da parte dello stato, oppure ci sarà anche spazio per la cogestione ed autogestione dei dati da parte di cittadini riuniti in associazioni di tipo cooperativo.

Siamo solo agli inizi di una trasformazione dei nostri rapporti sociali ed economici: quando questi strumenti saranno usati da tutti quasi inconsapevolmente, come le mail oggi, cioè senza avere minimamente idea della complessa rete tecnologica e sociale che regge l'architettura della comunicazione digitale, allora il mondo sarà cambiato e nulla sarà più come prima, compresi noi stessi.

Note bibliografiche

Asolo B. 2018 "Breaking Down the Blockchain Scalability Trilemma" Bitcoinist.com, June 10) https://bitcoinist.com/breaking-down-the-scalability-trilemma/

Bulkin A. 2018b "From Icarus to basic sanity: blockchain technology and the power of not knowing" *CoinFund,* Jul 9.

https://blog.coinfund.io/from-icarus-to-basic-sanity-blockchain-technology-and-the-power-of-

not-knowing-459fcaf30ccc

Buterin, V. 2015 "On Public and Private Blockchains", Ethereum blog, 7 August. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchainblockchains/

D'Aliessi M. 2016 "How Does the Blockchain Work?" *Onezero*, June 1.

https://onezero.medium.com/how-does-the-blockchain-work-98c8cd01d2ae

De Filippi P., Wray C. and Sileno G. 2021 "Smart Contracts", *Internet Policy Review*, Vol. 10, N.2.

Ehrsam F. 2016 "How to Raise Money on a Blockchain with a Token" Nov 2https://blog.gdax.com/how-to-raise-money-on-a-blockchain-with-a-token-510562c9cdfa

Eyal e Sirer 2013 "Majority is not Enough: Bitcoin Mining is Vulnerable", Cornell University. arXiv:1311.0243 [cs.CR]

Hearn M. 2016 The resolution of the Bitcoin experiment", *Mike's Blog*, Jan. 14.

https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7

GOS (Government Office for Science) 2016 *Distributed Legder Technology: beyond blockchain*, London, OGL.

Il Sole 24 Ore 2016 *La moneta virtuale. Come funzionano i bitcoin e che cosa ci possiamo fare*, supplemento *Nova Lezioni di futuro*, N.11, 4 febbraio.

O'Dwyer R. 2015 "The Revolution will (not) be decentralized: Blockchains"

https://blog.p2pfoundation.net/the-revolution-will-not-be-decentralised/2015/03/23

Karapetsas L. 2015 *Ethereum White Paper* November 21.

https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper

(In italiano: 2016 *Libro Bianco di Ethereum. Una piattaforma di nuova generazione per i contratti intelligenti e le applicazioni decentralizzate* (Pedretti L.M.)

https://github.com/ethereum/wiki/wiki/%5BItalian%5D-Libro-Bianco

Kharif O. 2020 "Bitcoin Whales' Ownership Concentration Is Rising During Rally" *Bloomberg*, 18 novembre.

Mainelli M. and Von Gunten C. 2014 "Chain of a Lifetime: How Blockchain Technology Might Transform Personal Insurance - Long Finance"

Available at SSRN: https://ssrn.com/abstract=3676416

Manski S. e Manski B. 2018 "No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World" *Law Critique*, 29: 151-162.

Monegro J. 2016 Fat Protocols AU 08, 2016 http://www.usv.com/blog/fat-protocols)

Mougayar W. (2015). "Understanding the blockchain", January 16.
https://www.oreilly.com/ideas/understanding*the*blockchain

Nakamoto S. 2008 “Bitcoin: A Peer-to-Peer Electronic Cash System”

Rifkin 2014 *La società a costo marginale zero*, Milano, Mondadori.

Scott B. “Open Source Finance Hacking: The Potentials and Problems”

Schulze-Kraft R. 2020 “How Many Entities Hold Bitcoin?“ *glassnode*, 28 gennaio. https://insights.glassnode.com/bitcoin_holders/

Schultze-Kraft R. 2021 “No, Bitcoin Ownership is not Highly Concentrated – But Whales are Accumulating”, glassnode https://insights.glassnode.com/bitcoin-supply-distribution/#:~:text=Insights-,No%2C%20Bitcoin%20Ownership%20is%20not%20Highly%20Concentrated%20%E2%80%93%20But%20Whales%20are,less%20concentrated%20than%20often%20reported.

Srinivasan B.S. May 27, 2017 “Thoughts on Tokens are early today, but will transform technology tomorrow” https://news.earn.com/thoughts-on-tokens-436109aabcbe

Szabo N. 2017 “Money, blockchains, and social scalability” Feb. 09, *Unenumerated*

http://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html

Tomaino N. 2017 “On Token Value” Aug 6. https://thecontrol.co/on-token-value-e61b10b6175e

Varoufakis Y. 2014 “Digital Economies: Markets, Money and Democratic Politics Revisited”, audio transcript of the keynote delivered in Seattle, CFA Institute, Annual Conference *The Future of Finance*, 5th May.

Voshmgir S. 2019 *Token Economy. How Blockchains and Smart Contracts Revolutionize the Economy*, Wroclaw, Amazon Media.

Wenger A. 2013 “Bitcoin As Protocol” October 31.http://www.usv.com/blog/bitcoin-as-protocol

Wenger A. 2014 “Bitcoin: Clarifying the Foundational Innovation of the Blockchain”December 15. https://continuations.com/post/105272022635/bitcoin-clarifying-the-foundational-innovation-of

Wenger A. 2016 “Crypto Tokens and the Coming Age of Protocol Innovation”

https://continuations.com/post/148098927445/crypto-tokens-and-the-coming-age-of-protocol

video https://www.blockchaincurated.com/crypto-tokens-coming-age-protocol-innovation/

Wright e De Filippi 2015 “Decentralized Blockchain Technology and the Rise of Lex Cryptographia” (March 10). Available at SSRN:

https://ssrn.com/abstract=2580664 or http://dx.doi.org/10.2139/ssrn.2580664

Appendice

Glossario minimo

Consenso Decentrato

Passiamo dal modello basato su un database che regola dal centro la validità delle transazioni ad un modello in cui l'autorità e la fiducia vengono trasferite alla rete virtuale decentrata, consentendo ai suoi nodi di registrare continuativamente e in sequenza le transazioni in un registro pubblico, creando un'unica catena: la blockchain appunto. Ogni blocco contiene un hash - un'unica impronta digitale – del blocco che lo precede; in tal modo la crittografia serve a garantire l'autenticazione della sorgente della transazione, eliminando la necessità di un intermediario centrale. L'insieme di crittografia e blockchain fa sì che non ci sia mai un duplicato di una transazione.

Contratti intelligenti (c.i.) e proprietà intelligenti

Sono i pilastri delle applicazioni decentrate. Un c.i. equivale ad un piccolo programma cui viene affidata una unità di valore e delle regole corrispondenti. Il principio base è di basarsi su una governanza decentrata senza necessità di intermediari centrali. Le parti concordano su regole più o meno complesse incardinate nella transazione che viene portata a compimento per via informatica. Le proprietà intelligenti sono risorse digitali o cose che sanno chi è il loro proprietario e la proprietà è connessa alla blockchain.

Vedi Mist di Ethereum ("a mix of marketplace discovery, management dashboard and creation platform, all-in-one" secondo Mougaray 2015): https://www.youtube.com/watch?v=IgNjs_WaFSc

Informatica basata sulla fiducia (o transazioni senza fiducia di tipo tradizionale)

La fiducia tipica delle autorità centrali viene trasferita nei codici dei c.i.

Scalabilità

La scalabilità indica la capacità di un sistema di gestire la crescita del lavoro al suo interno, pronto in ogni istante ad essere ampliato. Per esempio, essa può far riferimento alla capacità di un sistema di aumentare il passaggio di dati al suo interno (e la relativa capacità di elaborazione degli stessi) quando vengono aggiunte nuove risorse al sistema, tipicamente risorse hardware.

Un significato analogo di scalabilità viene attribuito quando si è in un contesto commerciale, la scalabilità di una compagnia indica la capacità per i suoi modelli di business di fornire una crescita economica al crescere delle dimensioni e degli affari della compagnia.

Al livello più basso possibile, la scalabilità significa fare di più di qualcosa, sia esso un lavoro, un processo o altro. Scalare una applicazione web significa allora permettere a più persone di accedere ad essa e utilizzarla nello stesso momento. La scalabilità è la sua capacità di offrire il

servizio gestendo un numero crescente di utenti che lo richiedono.

Diverse tipologie di scalabilità di un sistema informatico:

- **Scalabilità verticale**: aggiunta di risorse con l'obiettivo di aumentare, al contempo, la capacità del sistema. Per esempio: aggiungere più CPU al proprio server, oppure espandere la memoria del proprio storage o della propria memoria ram.
- **Scalabilità orizzontale:** aggiunta di nuove unità messe tra loro in parallelo perché funzionino come una sola, unica unità. Esempi: Clustering, Sistemi distribuiti e *load-balancing*. La scalabilità orizzontale si focalizza sia sull'aspetto hardware sia sull'aspetto software.
- **Scalabilità sociale** (Szabo N. 2017)

con questo concetto si intendono "i modi e le dimensioni in cui i partecipanti possono pensare e rispondere alle istituzioni e ai partecipanti man mano che cresce la varietà e il numero di partecipanti a tali istituzioni o relazioni". La scalabilità sociale riguarda i limiti sociali degli esseri umani, e contrasta con la scalabilità tecnica, che si riferisce al consumo di risorse e all'efficienza computazionale. Questo concetto è importante per la crittografia perché le blockchain rappresentano un compromesso fondamentale: scambiano la scalabilità tecnologica con la scalabilità sociale.

Nel contesto di Bitcoin, la rete è protetta da puzzle crittografici ad alta intensità energetica (noti come proof-of-work) e ogni volta che qualcuno avvia una transazione sulla rete Bitcoin, deve essere trasmessa a ogni nodo della rete. Entrambi questi processi sono intrinsecamente inefficienti e tecnologicamente meno scalabili rispetto ai sistemi di pagamento tradizionali. Tuttavia, questo sistema criptoeconomico elimina la necessità di una terza parte e consente a chiunque di partecipare alla rete rendendola più socialmente scalabile.

"Per aumentare la scalabilità sociale, dobbiamo scalare i mercati in tutto il mondo. Per scalare i mercati in tutto il mondo, abbiamo bisogno di denaro scalabile. Nel 21 ° secolo, il denaro scalabile richiede una sicurezza informatica scalabile "(Szabo 2017).

TAD

(Mougayar 2015) E' il luogo in cui vengono immagazzinati i dati in forma semi-pubblica all'interno di uno spazio lineare (il blocco). Tutti possono verificare il dato immesso perché corredato dalla firma del proprietario, l'unico che può aprirlo avendo le necessarie chiavi di accesso private: visibilità pubblica, accesso privato. Un po' come l'indirizzo di casa: tutti lo possono conoscere ma cosa c'è in casa lo sapete solo voi. Si possono immagazzinare monete, buoni, token ecc… Dal punto di vista della progettazione di software la blockchain può esser vista come un insieme di computer alla pari che obbediscono allo stesso processo consensuale per diffondere o registrare l'informazione che contengono e dove ogni interazione è verificata dalla crittografia.

Suggerimento per la citazione:
Giorgino V.M.B. 2021 *Le tecnologie di archiviazione distribuita: dall'avvento della bitcoin blockchain ad oggi*, Rapporto CETR N°1, Torino, CETR.

Vincenzo M.B. Giorgino,
Sociologo, professore aggregato di Sociologia economica presso il Dipartimento di Scienze economico-sociali e matematico-statistiche dell'Università di Torino. È fondatore del CETR - Center for Transdisciplinarity in Research (link) e coordinatore del gruppo di ricerca-azione WiseLifeLab.
I suoi principali interessi di ricerca: salute e benessere, grounded theory, ricerca-azione e metodologie trasformative, coproduzione ed economia collaborativa del *commoning*.
Tra le sue pubblicazioni recenti: co-curatore con Zach Walsh 2018 *Co-Designing Economies in Transition. Radical Approaches in Dialogue with Contemplative Social Sciences*, London, Palgrave.

Questo rapporto

L'attenzione verso le tecnologie di archiviazione distribuita (TAD, in inglese l'acronimo è DLTs, Distributed Ledger Technologies) è data dalle enormi potenzialità che esse offrono per la vita sociale, a partire dalle transazioni economiche per finire a qualsivoglia forma di "contratto" tra due o più soggetti. Si tratta di archivi con proprietà e capacità superiori agli archivi tradizionali e che "possono essere condivisi da una rete di molteplici siti, geografie e istituzioni" (GOS 2016: 5).

Come a suo tempo per Internet, le aspettative sono molteplici. E le delusioni di ieri possono costituire le sagge basi per non alimentare nuove illusioni e soprattutto commettere errori di progettazione e di scelte politiche. Una progettazione consapevole può rappresentare una vera e propria rivoluzione sociale, molto più che una sia pur importante evoluzione tecnologica; questa darebbe consistenza all'emersione e all'affermazione di quella società collaborativa in rete definita da Castells "non capitalismo" e da altre società dei commons collaborativi (Rifkin 2014). Come già in passato per altre tecnologie – l'impiego del vapore, dell'elettricità ecc.. – ciò comporta il cambiamento di schemi mentali attraverso l'acquisizione di nuove capacità, abilità e saperi…" (GOS 2016: 55).

Il CETR

Il Centro è stato istituito nel 2017 con l'obiettivo di favorire la cooperazione transdisciplinare per rispondere alle sfide ineludibili emerse nella nostra società. Tale cooperazione si qualifica per l'attenzione ai processi vitali ed alla loro protezione sociale in un contesto caratterizzato da emergenze.

Una parte strategica del progetto complessivo è data dal contributo ad un modello epistemologico enattivo, superando sia l'empirismo logico che il costruttivismo.

Lo scopo del Centro è la creazione di una rete operativa fondata sull'esperienza che includa le dimensioni emozionali e sensoriali nella comprensione del mondo, aprendo un dialogo metodologico efficace con quelle tradizioni di saggezza volte alla comprensione esistenziale di noi stessi e dell'ambiente vitale, contribuendo a quella che si sta definendo come scienza sociale contemplativa.

Ciò va nella direzione della co-progettazione di ecosistemi sociali saggi ed equi attraverso tecnologie di archiviazione distribuita per una trasformazione sociale orientata al *commoning*, in cui gli stessi dati digitalizzati sono soggetti alla sovranità dei partecipanti alla rete..