

# Blockchain, elezioni e GDPR

Armoniosa convivenza, completa incompatibilità o rapporto burrascoso?

## Premessa

La blockchain è caratterizzata da un data base distribuito (il che non è una novità assoluta in campo informatico: anche i database di conversione dei *domain name* in indirizzi IP, ad esempio, sono una forma di data base distribuito, già in essere sin dagli anni '80), nonché da un sistema di blocchi concatenati – da cui il nome – per cui ogni variazione, ogni anello della catena, contiene un riferimento crittografico alla situazione precedente. La violazione di un anello richiederebbe dunque la violazione dell'intera catena, necessiterebbe di una quantità di energia e di potenza di calcolo indisponibile e verrebbe comunque scoperta, data la natura distribuita del data-base.

Come responsabile dell'ufficio elettorale il fenomeno blockchain ha ovviamente attirato la mia attenzione primariamente per questo aspetto, ma, prima di affrontare il punto, al fine di inquadrarlo meglio, vi vorrei parlare brevemente dei polli.

## I polli e la blockchain

Partiamo dai polli<sup>1</sup>: oggi la blockchain entra dappertutto ed è stata quindi proposta anche per le filiere alimentari o il controllo delle foreste<sup>2</sup> o delle opere d'arte<sup>3</sup>, ma, poiché non mi risulta che la tecnologia attuale consenta di digitalizzare un pollo e di bloccarlo con un hash, significa che ad essere tracciabile non è il pollo in sé, bensì il percorso che segue da quando è uovo a quando finisce sul banco del supermercato. Ipotizziamo che qualcuno, nel corso della filiera, sia un po' mariuolo e che ad esempio un produttore cinese entri col codice di un produttore italiano e si attribuisca il marchio "Made in Italy", oppure che un camionista si fermi in un autogrill e scarichi un po' di pollame nostrano, allevato con certi criteri, e lo sostituisca con polli stranieri di allevamento intensivo e incontrollato, intascando la differenza di valore, oppure che il supermercato non voglia gettare pollame un po' vecchio e copi le etichette ed i relativi QR code del lotto della settimana seguente e li applichi al pollo precedente. In quale modo la blockchain può garantire il consumatore, dato che il valore principale, ovvero il pollo, è *offchain*? Certo, l'azienda potrà rispondere di essere una ditta seria, degna di fiducia, e che tutti i fornitori che contribuiscono alla catena sono seri e controllati, ma allora, se devo comunque fidarmi, un data base vecchio stile non raggiunge lo stesso risultato? E poi dove sono i nodi della *chain*? Qualcuno di voi ha scaricato una app "controlla il pollo" e contribuisce alla gestione delle catene? Insomma, capisco le necessità del marketing, però così a prima vista questo utilizzo è perfetto per acchiappare i polli, ma non nel senso dei volatili.

---

<sup>1</sup> <http://www.lastampa.it/2018/10/11/tecnologia/il-primo-alimento-italiano-tracciato-con-la-blockchain-un-pollo-CpHYnQDtJPnJsiXA1eYScL/pagina.html>

<sup>2</sup> <https://it.cointelegraph.com/news/spain-to-develop-blockchain-tech-application-for-transparency-in-forestry-industry>

<sup>3</sup> <https://www.lastampa.it/2018/11/01/tecnologia/artid-lancia-un-token-per-certificare-opere-YcG0Yf6ivNZNSrHCgFDhkN/pagina.html>

## ~~Il~~ polli Gli elettori e la blockchain

Veniamo all'applicazione che forse interessa maggiormente l'aspetto pubblico, ovvero le elezioni: con la blockchain si potrebbe passare al voto elettronico, garantendo sicurezza assoluta e consentendo una grande velocità di elaborazione, che potrebbe produrre i risultati definitivi in pochi minuti. Almeno, questo è quello che promettono i sostenitori, ma siamo proprio convinti della bontà dell'idea?

A titolo personale ho un sogno: mettere nelle cabine elettorali dei tablet, che prima di far accedere al voto chiedano di rispondere a tre domandine del tipo "chi elegge il Presidente della Repubblica", "chi nomina il Governo?": se non rispondi correttamente ad almeno due quesiti te ne torni a casa! Però poi mi sveglio e capisco che non si può. Non si può non solo perché la democrazia è quella cosa per cui il voto di un analfabeta e di un premio Nobel hanno lo stesso valore, ma anche per tutta una serie di difficoltà tecniche. Il sistema elettorale, così come è concepito oggi, implica certamente degli errori: errori di conteggio, errori di interpretazione delle schede, errori per la stanchezza e l'impreparazione del personale dei seggi. Però si tratta di errori che statisticamente tendono a compensarsi, almeno se non c'è malafede, e se anche un seggio fosse corrotto (per esperienza posso dire che è impossibile alterare significativamente i risultati se non si è tutti d'accordo, compresi i rappresentati di lista), sul totale nazionale sarebbe comunque sostanzialmente irrilevante. Poco significativo, invece, il discorso delle tempistiche: una Legislatura dovrebbe durare cinque anni, per formare un Governo occorrono, di solito, diverse settimane, quindi impiegare un minuto o mezza giornata per avere i risultati praticamente definitivi è assolutamente ininfluenza rispetto all'iter successivo. Una votazione elettronica certo risolverebbe alcuni problemi di interpretazione e di conteggio, ma ne inserirebbe di nuovi, che, al momento, appaiono irrisolvibili:

- Chi mi garantisce che il software è sicuro? Non è sufficiente che sia *open*, perché
  - devo essere sicuro che il compilato corrisponda a quello pubblicato,
  - devo essere sicuro che su ogni macchina sia effettivamente installata la versione ufficiale,
  - devo essere sicuro che il codice non contenga qualche *zero day* che venga attivato al momento giusto.
- Chi mi garantisce che l'hardware è sicuro? Pensiamo alle criticità messe recentemente in evidenza dalle vulnerabilità Spectre e Meltdown.
- Chi mi assicura che non è in corso un attacco *man in the middle* e il mio voto non viene osservato e/o alterato nel suo viaggio tra il mio dispositivo ed il data base centrale?
- Chi mi assicura che non c'è un *touchlogger*, un sistema equivalente al *keylogger*, installato sul dispositivo?

Con la blockchain potrei garantire che i dati, una volta inseriti nel data base, restino inalterati, d'accordo. Ma il problema, la criticità principale, risiede nel data base del Ministero dell'Interno oppure il punto debole sono i terminali periferici e la loro connessione al sistema centrale? Passando da un data base unico ad un sistema distribuito (distribuito dove?) potremmo migliorare un pochino la sicurezza dei dati finali, peraltro mai messi in dubbio, anche perché i dati elettorali sono distribuiti di fatto, attraverso l'esercito di cronisti e politici che presidia il Ministero nel momento delle elezioni, ma i rischi principali resterebbero tutti, dato che, come nel caso del pollo, le criticità maggiori sono *offchain*. Un sistema elettronico,

soprattutto, perde la sfida nel confronto col sistema attuale, più manuale, analogico, farraginoso, ma complessivamente più affidabile e facilmente verificabile *ictu oculi*.

Il discorso, peraltro, si può estendere ad altre realtà pubbliche: l'ANPR, ad esempio, ovvero l'Anagrafe Nazionale della Popolazione Residente, che sostituirà le circa 8000 anagrafi comunali in un'unica raccolta. Certo si potrebbe usare un database distribuito (non necessariamente con catene di blocchi) al posto di uno centralizzato, ma ci sarebbe un vantaggio? E ci sarebbe un vantaggio ad usare un sistema di blocchi concatenati per ogni variazione anagrafica, quando già il sistema attuale gestisce lo storico dei movimenti? Di nuovo, se si mette in dubbio l'onestà (un errore verrebbe registrato comunque, sia in un sistema blockchain che in un data base classico) del sistema, allora la blockchain può essere una soluzione, diversamente si tratterebbe unicamente di un inutile appesantimento.

## **Il GDPR e la blockchain**

Per altre applicazioni lascio la parola ai colleghi; per l'elettorale il problema non dovrebbe porsi, dato che il GDPR riguarda persone identificate o identificabili e si spera che il voto resti segreto, quindi sì, un sistema di voto elettronico sarebbe compatibile col GDPR, con o senza blockchain.

Diverso, invece, il discorso anagrafico, dato che bisognerebbe assicurarsi che i vari nodi siano gestiti solo da soggetti pubblici autorizzati e che i dati restino quindi accessibili solo a quanti hanno il diritto di trattarli. Irrilevante, invece, il problema del diritto all'oblio – beninteso, mi riferisco solo alla questione anagrafica e dello stato civile – dato che si tratta di dati di alto valore storico, che vengono conservati senza limiti temporali in piena conformità con i dettami del Regolamento UE.

## **Conclusioni**

Fin qui ho forse dato l'impressione di essere molto critico verso la blockchain e molto scettico verso la sua applicabilità in ambito pubblico, quindi è opportuno che precisi meglio il mio pensiero.

Per ciò che riguarda la blockchain in senso assoluto, sicuramente si tratta di un approccio innovativo e dalle grandi potenzialità, che però viene spesso inteso come la teriaca veneziana, che curava tutti i mali, ed è proprio nell'eccesso di aspettative che vedo il problema: si tratta di uno strumento da studiare, da utilizzare quando può veramente servire, ma che si deve applicare in modo corretto, consapevole e non eccessivo rispetto alla sua natura.

Per ciò che riguarda il settore pubblico in generale, ed il sistema elettorale in particolare, è sicuramente giusto studiare il fenomeno e tentare di applicarlo anche in chiave pubblica<sup>4</sup>: senza ricerca di sicuro non si arriva a nulla, mentre studiando e sbagliando si potrà arrivare forse ad una svolta, ma, al momento, non vedo come la tecnologia possa essere considerata abbastanza sicura da sostituire la buona vecchia accoppiata scheda-matita copiativa.

---

<sup>4</sup> <https://www.sardiniapost.it/innovazione/elezioni-voto-elettronico-distanza-al-lavoro-un-team-sardo-bolognese/>