

ByteSt@mp

The Internet Timestamp Service

www.bytestamp.net

Procedura di votazione elettorale sulla *blockchain*

Libro Bianco ver 1

Il presente libro bianco descrive una metodologia per poter condurre una consultazione elettorale sfruttando la tecnologia di consenso distribuito nota come *blockchain*.

ByteSt@mp ha realizzato dei *Proof Of Concept* funzionanti che sono stati già sperimentati da diversi utenti del *web*.

Il primo di questi fu proposto in occasione delle elezioni USA 2016, per la precisione il 16 ottobre 2016 è stata la prima volta che qualcuno ha votato sulla *blockchain*. Questa applicazione è consultabile al link <http://www.bytestamp.net/vots/new>.

In seguito è stato proposto anche per altre competizioni elettorali.

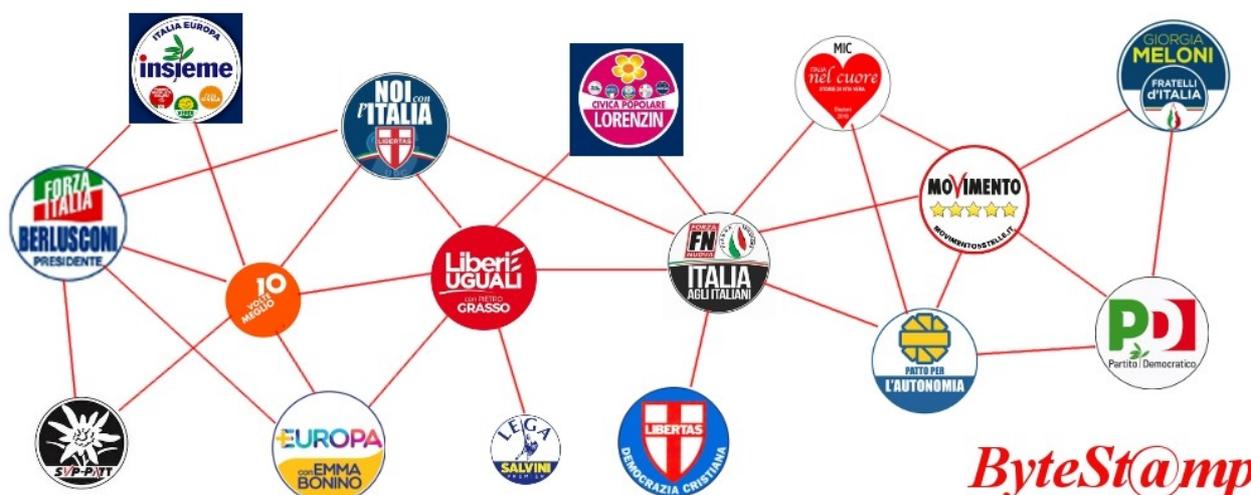
Si tratta però sempre di un *Proof Of Concept*, che di per sé presenta limitazioni e vulnerabilità.

Il procedimento descritto di seguito, invece, espone una metodologia che potrebbe usare un **vero** stato sovrano per condurre una **vera** consultazione elettorale.

Si è cercato di prendere in considerazione tutte le criticità derivanti dall'utilizzo della *blockchain* e del voto elettronico in generale.

Tuttavia, poiché molte altre problematiche sono sfuggite all'analisi, la procedura descritta sarà sicuramente soggetta a revisioni nelle successive versioni di questo libro bianco.

Vota sulla Blockchain!



Il sistema elettorale realizzato da ByteSt@mp al momento è un Proof Of Concept che presenta alcune lacune.

In un sistema reale l'ID di votazione verrebbe assegnato da un'autorità e quindi sarebbe univoco per ogni elettore, così da risolvere il problema di una votazione doppia.

Per risolvere il problema dell'anonimia si consideri la seguente procedura.

In occasione delle votazioni, il governo genera degli ID di votazione, tanti quanto sono gli elettori.

Tutti questi ID di votazione sono caricati sulla Blockchain insieme alla firma digitale dell'autorità che li ha emessi.

Tale caricamento avviene con una procedura simile a quella attuale di ByteSt@mp per il caricamento dei documenti.

Cioè non viene scritto in chiaro il vero ID di votazione ma solo l'impronta informatica dello stesso concatenato con la firma digitale.

Per i tecnici: si scrive in blockchain qualcosa come

$MD5(IDvotazione, FirmaDigitale(IDvotazione))$

Inoltre il governo genera anche una coppia di chiavi pubblica e privata. Quella privata la firma digitalmente e la scrive in blockchain con le stesse modalità. Quella pubblica la rende pubblica.

Dopodiché arriva il giorno delle votazioni.

Tutti ci rechiamo alle urne elettorali esattamente come ci andiamo oggi.

Solo che nella sezione elettorale invece di esserci e un'urna ci sono DUE urne.

In una delle due urne ci sono tanti ID di votazione quante sono le persone che devono votare in quella sezione elettorale. Questi ID di votazione sono prestampati e sigillati e ovviamente sono vigilati dalle persone che presiedono il seggio.

Quando vado a votare, vengo identificato con la mia carta di identità e poi PESCO dalla prima urna un ID di votazione pre-generato.

Nessuno sa quale ID di votazione ho pescato.

Poi vado in cabina elettorale e voto, davanti agli occhi di tutti, così da risolvere il problema della ricattabilità al momento del voto.

Posso votare usando un dispositivo messo a disposizione dall'ente, su cui gira un *software* di cui mi devo fidare, oppure posso votare usando il mio *smartphone*, su cui gira un altro *software* di cui comunque mi devo fidare.

Nell'uno e nell'altro caso i software malevoli non possono modificare il voto perché io sarò in grado di controllarlo a posteriori sulla *blockchain*.

Quando voto NON scrivo sulla *blockchain* il voto in chiaro come fa oggi il *Proof Of Concept* di ByteSt@mp.

Invece scrivo sulla *blockchain* il mio ID di votazione e il mio voto **CRIPATI** con la chiave pubblica che il governo aveva generato e reso pubblica prima.

In questo modo si risolve il problema di non dover mostrare l'andamento delle votazioni durante la consultazione elettorale per non influenzare l'andamento delle elezioni.

Se si scrivessero i voti in chiaro sulla *blockchain*, tutti potrebbero leggerli anche prima della fine della consultazione elettorale.

Sempre in cabina elettorale, mi scrivo il mio ID di votazione da qualche parte per non dimenticarlo.

Poi esco dalla cabina elettorale e metto il mio tagliando di votazione in un'altra urna, quella degli ID di votazione usati.

Questo può porre qualche problema di anonimata se sono poche persone a votare in una sezione elettorale.

Si pensi al caso limite che in una sezione vada a votare una sola persona.

Ma è un problema che esiste anche oggi.

Anzi, con la *blockchain* il problema si potrebbe risolvere perché tutti i voti vanno indistintamente nella *blockchain* prescindendo dalla sezione elettorale, e quando esco dalla cabina elettorale invece di mettere l'ID di votazione nell'urna degli ID usati, potrei distruggerlo davanti a tutti.

Al termine della consultazione elettorale, il governo rende pubblica la chiave privata scritta in precedenza sulla *blockchain*.

Tutti possono controllare che tale chiave è stata firmata dall'autorità e tutti possono vedere che era stata generata prima delle elezioni perché la sua impronta informatica è scritta in *blockchain*, con lo stesso procedimento con cui oggi si ottiene il *ByteStampProof*.

Inoltre tutti possono decriptare tutti i voti messi in *blockchain* e criptati con la corrispondente chiave pubblica.

Quindi io posso vedere che il mio voto è stato correttamente computato perché lo leggo sulla *blockchain* associato al mio ID di votazione che mi sono scritto in cabina elettorale.

Se qualcuno mi ricatta o mi sono venduto il voto, posso sempre dirgli che il mio ID di votazione è un altro, che corrisponde al voto che lui vuole. Infatti dalla *blockchain* io vedo anche i voti di tutti gli altri.

Del resto, non posso fargli vedere il tagliando originale che ho distrutto o messo nell'urna degli ID usati quando sono uscito dalla cabina elettorale. Quindi lui deve fidarsi di me quando gli dico che il mio ID è quello.

Inoltre tutti quanti possono controllare che gli ID di votazione siano quelli generati dal governo e da esso firmati digitalmente. Così si risolve anche il problema della doppia votazione e dei voti falsi infilati nella *blockchain* magari da qualche paese estero.

Inoltre si può sempre controllare che gli ID di votazione che restano inutilizzati nei vari collegi elettorali non corrispondano a nessun voto sulla blockchain. Quindi sappiamo che per ogni voto abbiamo verificato una carta di identità.

By ByteSt@mp - (c) MIDA SRL - Tutti i diritti riservati - *All Rights Reserved*

<http://www.bytestamp.net/docs/qdoc/it/9d2144f3955e972f34e856374affceea>

Il presente documento è stato registrato sulla BlockChain di Datacoin in Data/Ora UTC

2018-02-25 19:58:48 UTC

nel blocco numero **2300967**

identificativo transazione:

c1f3078badc8664f604e90089d9815ac47ddd07881ea58d224ab0d1748f39293

#ByteStampProof

per avere la conferma, visitare il seguente link:

<http://www.bytestamp.net/docs/qdoc/it/9d2144f3955e972f34e856374affceea>

La proprietà del medesimo è stata registrata sulla blockchain all 'indirizzo datacoin

D8GafEsbyssg4TQN71KTbd8QdRg846MxCQ

che appartiene a ByteSt@mp, come dichiarato in blockchain alla transazione

78c8b327930ec9ec4e280801e2ebba190add5bcbeca295dba9992d5e2cb455bb

E come risulta dal dal ByteStamp Digital Asset reperibile a questo link:

<http://www.bytestamp.net/blocks/qtx/it/cbe368fc6ede65273da515fbc791499b06d9474c815172731ab5da88c4aafae0>

