Algoritmi e Protocolli per la Sicurezza

L.M. Ingegneria Informatica

Anno Accademico 2021-2022

Docenti: V. Iovino - I. Visconti

Project Work

Gruppo Kryptos:
Spingola Camilla 0622701698
Sica Ferdinando 0622701794
Turi Vito 0622701795
Marseglia Mattia 0622701697

Sommario

WP1

L’ambito in cui si inserisce il Sistema da realizzare è quello di rivoluzionare la metodologia di voto attraverso l’introduzione di un voto elettronico/remoto tramite il quale ciascun cittadino possa esprimere la propria preferenza in un qualsiasi referendum confermativo o abrogativo.

Attraverso il referendum abrogativo si decide se abrogare o meno una legge mentre con il referendum confermativo il popolo decide se confermare o meno una legge di riforma costituzionale già approvata dal Parlamento, ma senza la maggioranza qualificata dei due terzi.

Inoltre, in caso di referendum abrogativo, è necessario il raggiungimento del quorum di partecipazione previsto dall’art. 75, comma 4, ossia il referendum risulta valido se ha partecipato alla votazione la maggioranza degli aventi diritto di voto.

Gli obiettivi contrastanti del popolo, dei singoli cittadini, delle diverse fazioni politiche e del governo stesso chiaramente potrebbero introdurre rischi di falsificazione del corretto esito del referendum.

Il voto si svolge in quattro fasi. La prima consiste nell’eventuale registrazione alla piattaforma (T0-T1). La seconda si svolge al termine della prima e consiste in una finestra temporale T1-T2 in cui ciascun cittadino potrà esprimere il proprio voto o cambiarlo in caso di ripensamenti. La terza, svolta nella finestra temporale T2-T3, permette al cittadino di inviare la conferma del voto; infine, nell’ultima fase, svolta nella finestra temporale T3-T4, si ha la pubblicazione dei voti e quindi del risultato.

Tipicamente il votante può scegliere a favore o contro il referendum ed eventualmente può decidere di non esprimere una preferenza (scheda nulla).

In tale scenario si inserisce la figura del Ministero del Voto (MV) che al termine delle elezioni si impegna nella divulgazione dell’esito ottenuto, dei relativi meccanismi per verificare la correttezza dell’esito e si occuperà di ingaggiare la società adibita alla realizzazione del software necessario al corretto svolgimento del voto.

Assumiamo che in casi specifici si possa coinvolgere anche la giustizia, che ha un'identità ben nota J. Ha senso che J venga utilizzato solo in caso di controversia, evitando quindi il più possibile il suo coinvolgimento. Tuttavia, potrebbe essere necessario il coinvolgimento soprattutto in caso di un comportamento scorretto da parte della società o in caso di una contestazione condotta dal cittadino. Tutto ciò che riguarda l’intervento della giustizia risulta fuori dal sistema digitalizzato, e può quindi soltanto essere fonte di analisi in fase di progettazione.

Volendo formalizzare:

Completeness.

Siano V1,…,Vn i potenziali votanti e MV il Ministero del Voto. Sia R il referendum indetto e P la minima percentuale di votanti richiesti per considerare il referendum valido. Ogni Vi può partecipare tra il tempo T1 e T2 alla votazione con un input xi che sarà un valore appartenente all’insieme {00,01,11} con i =1,...,m, con m<=n.

Il valore 00 verrà considerato come voto sfavorevole al referendum, il valore 01 verrà considerato come votazione nulla, il valore 11 verrà considerato come voto favorevole al referendum.

I cittadini che non prenderanno parte alla votazione non saranno considerati nel conteggio finale. Nel caso in cui la percentuale di cittadini che prendono parte alla votazione (m) risulta minore della percentuale minima di votanti richiesti (P), il referendum viene annullato.

Una volta che il cittadino ha espresso la propria preferenza può ottenere una iniziale conferma della presa in esame del proprio voto, che potrà essere modificato nell'intervallo temporale T1-T2, e che dovrà essere, in una fase T2-T3, confermato dal cittadino stesso (in caso di mancato invio della conferma il voto espresso precedentemente verrà considerato nullo).

Nella fase finale (T3-T4) ci sarà, in seguito ad una operazione da parte della Società, la pubblicazione dell'esito del referendum.

Threat model.

Il Venditore di favori:

un avversario che potrebbe essere interessato a conoscere più informazioni sul voto espresso da alcuni votanti specifici, perché per esempio ha fatto un patto con loro (dare uno specifico voto ottenendo in cambio un allettante favore) e vuole sapere se hanno mantenuto la promessa. Per farlo dovrà attaccare a partire dall'istante T1. Questo avversario, poiché non vuole fare favori a chi non lo merita, potrebbe inizialmente ricorrere alla coercizione per poi assicurarsi che il voto di cui ha interesse non venga modificato entro il termine del referendum, facendo un investimento medio-basso (essendo un privato). Non ha accesso alla comunicazione punto-punto.

Il Ficcanaso:

un avversario che potrebbe essere interessato a conoscere maggiori informazioni sulle percentuali del "sì" o del "no" del referendum, al fine di utilizzare queste informazioni per scopi personali (es. un trader potrebbe essere interessato a prevedere l'andamento del mercato in funzione della votazione e avere dei profitti considerevoli, oppure un malintenzionato potrebbe essere interessato a conoscere l'andamento della votazione al fine di programmare eventuali azioni "correttrici" a suo favore). Per fare ciò il suo attacco avviene durante la fase di votazione, quindi nella finestra temporale T1-T2 o in alcuni casi T1-T3, e consiste nel raccogliere informazioni o attraverso l'ascolto di tutte le persone che comunicano il loro voto, o attraverso un attacco al sistema di gestione dei dati del referendum. Eventualmente nel caso in cui la votazione non stia proseguendo nella direzione da lui desiderata, potrebbe anche decidere di fare coercizione verso una o più persone, per le relative preferenze, oppure opere di divulgazione, anche su larga scala, per riorientare l'esito del referendum, tutto ciò facendo un investimento al più medio-basso (essendo un privato). Non ha accesso alla comunicazione punto-punto.

La viscida governance della società

questo avversario è rappresentativo dei proprietari della Società ingaggiata dal Ministero del voto, adibita alla realizzazione del software necessario al corretto svolgimento del referendum. Gli scopi per cui potrebbe decidere di condurre un attacco sono molteplici: ad esempio conoscere in anticipo l'esito della votazione in modo da prevedere l'andamento del mercato e ottenere dei profitti considerevoli (così come il ficcanaso) o modificare le votazioni in modo da ottenere come esito del referendum quello desiderato (ad esempio poiché potrebbe essere un referendum che apporta implicitamente vantaggi o svantaggi alla Società stessa). I possibili attacchi condotti possono verificarsi fino all'istante T4 e verosimilmente potrebbero essere molto efficaci data la loro influenza nella creazione e gestione del software per il referendum stesso (si potrebbero escludere quantomeno eventuali opere di coercizione), non sono da escludere attacchi mediatici per il raggiungimento degli scopi sopra descritti. Per fare ciò si suppone possa condurre investimenti medio-alti. Non ha accesso alla comunicazione punto-punto.

Gli Sviluppatori procaccianti:

uno o più avversari facenti parte della Società adibita allo sviluppo del software per la votazione che potrebbero avere degli interessi nel creare un sistema che sia funzionante ma che sia influenzabile da parte di chi lo realizza (es. modificare in corso d'opera i dati della votazione etc…), o che influenzi chi lo utilizza nella votazione per il referendum (es. pop-up, inserzioni, ostacoli nell'effettuare una preferenza piuttosto che un'altra etc…), potrebbero rappresentare una minaccia reale al sistema pur non avendo accesso alla comunicazione punto-punto. Gli attacchi che mirano all'influenzabilità del sistema, tuttavia, hanno senso solo se la tecnologia utilizzata non è condivisa e trasparente. Però, poiché il sistema da realizzare deve essere frutto di una progettazione e di un'analisi che permetta a tutti di verificarne la bontà, ragionevolmente questi tipi di attacchi risultano essere fortemente

esposti a eventuali pubbliche denunce che minerebbero la credibilità e la reputazione degli sviluppatori, oltre che della Società stessa.

Lo Schieramento polarizzato:

un gruppo di avversari che potrebbe essere una fazione politica, parastatale, economica o un'organizzazione di vario genere. Questo gruppo è polarizzato perché i membri sono interessati a favorire un certo risultato del referendum. La loro azione si compie durante la finestra di votazione T1-T3 e consiste nella manipolazione dei voti inviati o dei voti salvati nel sistema, in un'eventuale opera di coercizione su media scala o di attacchi mediatici per far sì che l'esito sia quello da loro desiderato. Poiché in questi casi ci sono molti interessi economici è plausibile che facciano un investimento medio-alto. Non hanno accesso alla comunicazione punto-punto**.**

L'ISP cospiratore:

il provider della rete internet, il quale può agire sulla rete di suo dominio per compromettere la votazione dei propri clienti; l'interesse dell'ISP potrebbe essere quello di far sì che non si raggiunga il quorum per un referendum abrogativo oppure, venendo corrotto, potrebbe evitare che vengano mandate le conferme di voto nella fase T2-T3 in modo da rendere nulle tutte le votazioni dei suoi clienti. L'attacco avviene durante la fase T1-T3, agendo direttamente sui pacchetti che passano per la propria rete manipolandoli arbitrariamente o compromettere il regolare utilizzo della rete internet dei suoi clienti al fine di impedire a precisi nuclei abitativi o località (di cui si potrebbero avere informazioni circa le preferenze di voto) di prendere parte al referendum. Ha accesso alla comunicazione punto-punto ed è plausibile ipotizzare un investimento medio-alto.

Il miserabile Ministero del voto:

si tratta dell'organo di governo che è alla base dell'organizzazione delle votazioni remote. Il Ministero del Voto si occuperà della ricerca della Società attua alla realizzazione del software per votare, della divulgazione e della verifica dei risultati del referendum. Un attaccante di questo tipo potrebbe effettuare attacchi mediatici su larga scala per influenzare l'esito del referendum ed eventualmente potrebbe avere accesso senza troppe difficoltà a dati sensibili riguardanti il referendum; essendo un organo molto vasto potrebbe fare un investimento alto. Quest'organo di governo potrebbe anche pattuire un'alleanza con la Società adibita alla realizzazione del software relativo al referendum per avere totale controllo sui risultati del referendum o sulla divulgazione degli stessi. Quest'organo è fortemente scoraggiato ad effettuare questo tipo di attacco, in quanto ha la volontà di preservare una buona reputazione, di evitare le punizioni che ne seguirebbero da parte della giustizia, per di più considerando che l'obiettivo principale di questo organo è quello di realizzare un sistema di voto online sicuro e funzionante. Non hanno accesso alla comunicazione punto-punto**.**

Il Ladro d'identità:

un avversario che potrebbe voler venire a conoscenza delle credenziali di una o più persone per poterne modificare il voto. Il suo attacco avviene entro la fine delle votazioni in quanto ciò di cui ha bisogno sono unicamente le credenziali fornite, quindi entro T2. Una volta ottenute, potrà accedere al sistema e modificare il voto espresso dal votante autentico. Per poter ottenere le credenziali potrebbe attaccare eventuali falle nel sistema o estorcendo fisicamente le stesse, al più effettuando un investimento basso. Non ha accesso alla comunicazione punto-punto.

Il DDoSSer:

un avversario che ha l'ambizione di non permettere il regolare svolgimento delle votazioni. Il suo attacco avviene nella seconda e terza fase, quindi T1-T2 e/o T2-T3. L'attacco consiste nel non permettere l'accesso alla "piattaforma" per votare, rendendo quindi nella prima fase impossibile l'invio/modifica del voto (soprattutto in casi di referendum abrogativo, che richiede un numero

minimo di votanti, questo potrebbe creare non pochi problemi), nella seconda invece evitando l'invio confermativo del voto, annullando le preferenze espresse precedentemente; per fare ciò effettuerebbe al più un investimento medio-basso supponendo sia un privato, altrimenti anche un investimento medio se associato ad un'organizzazione (es. una società concorrente a quella adibita allo sviluppo del software). Non ha accesso alla comunicazione punto-punto.

No Evox:

questo personaggio non rappresenta un reale avversario del sistema nel senso che non può minarne il corretto funzionamento, ma è una figura ostile alla digitalizzazione del voto che pertanto potrebbe essere interessato a scoraggiarne l'impiego mettendone in discussione la credibilità. Dunque, le sue azioni possono al più rientrare in mistificazioni riguardo alle modalità di svolgimento dell'intero processo.

NB.

Per quanto concerne il venditore di favori, il ficcanaso, il ladro d'identità e il DDoSSer, questi potrebbero raggiungere un investimento alto se riuscissero a formare una coalizione numerosa, anche se un'alleanza di avversari difficilmente non fallisce in quanto non è detto che tutti possano fidarsi di tutti.

Proprietà

Integrità:
In presenza di avversari il Sistema di voto dovrebbe comunque garantire che:

- *I.1* la preferenza di un onesto votante possa variare solo se richiesto dallo stesso così da garantire la correttezza del risultato.
- *I.2* l'ingiustizia dovrebbe essere improbabile o almeno scoraggiata attraverso sanzioni.

Privacy:
In presenza di avversari il Sistema di voto dovrebbe comunque garantire che:

- *P.1* L'identità dei votanti rimanga confidenziale.
- *P.2* La preferenza di un votante rimanga confidenziale.
- *P.3* I risultati della votazione rimangano confidenziali fino al termine del voto.

Disponibilità:
In presenza di avversari il Sistema di voto dovrebbe comunque garantire che:

- *D.1* Il livello di prestazioni del sistema rimanga invariato per gli utenti legittimi, i quali dovrebbero sempre poter disporre delle funzionalità a cui sono abilitati.

Autenticità:
In presenza di avversari il Sistema di voto dovrebbe comunque garantire che:

- *A.1* di ciascun voto salvato sia verificata l'identità dell'origine, ovvero che rappresenti realmente la preferenza espressa da un onesto votante (i.e. assicurare che nell'esito finale non siano conteggiati voti non realmente espressi da onesti votanti, ma generati malevolmente dal sistema stesso o da qualsiasi altro avversario).

Credibilità:
In presenza di avversari il Sistema di voto dovrebbe comunque garantire che:

- *C.1* a parità di argomenti, di incisività, nonché di pubblico interesse del referendum, il numero di partecipanti allo stesso in modalità remota deve essere comparabile a quelli registrati negli ultimi anni per le votazioni in modalità tradizionale.

Trasparenza:
In presenza di avversari il Sistema di voto dovrebbe comunque garantire che:

- *T.1* una qualunque persona interessata allo svolgimento del referendum deve poter in maniera semplice e chiara analizzarne e verificarne la correttezza del risultato.
- *T.2* una qualunque persona interessata allo svolgimento del referendum deve poter analizzare e verificare in maniera semplice il meccanismo di funzionamento.

WP2

Si assume che ogni volta che sarà menzionato un certificato si farà riferimento all'intera lista di certificati fino alla radice (I.E. Certification Authority).

Caratteristiche della chain

Per la realizzazione del sistema di votazione si è scelto di utilizzare "ItalyChain", una blockchain permissioned:

- la governance è affidata alle province, nello specifico ci saranno 107 validatori ognuno rappresentativo di una di queste.
- Una transazione contiene al suo interno il destinatario (l'indirizzo ricevente, che può essere o un altro individuo o uno smart contract), la firma (che viene generata quando il sender firma con la propria chiave privata la transazione e conferma che è stato lui stesso ad autorizzare tale transazione), i dati (campo che contiene dati arbitrari, nel caso del referendum sono presenti anche informazioni sulla preferenza del sender).
- Un blocco contiene al suo interno un numero finito di transazioni, un identificativo univoco del blocco precedente, la data nel quale è stato emesso, l'identificativo del validatore che lo ha realizzato e informazioni relative allo stato della blockchain.
- Ogni 10 secondi viene verificato e aggiunto alla blockchain un nuovo blocco.
- Scelto un validatore attivo, in maniera randomica, esso ha lo scopo di creare e pubblicare un nuovo blocco validando le transazioni che non sono ancora state prese in esame fino a quel momento.
- Una volta pubblicato un nuovo blocco, viene inserito nella blockchain solo e unicamente se i 2/3 dei validatori ne verificano e ne approvano il contenuto, di conseguenza deve esserci un numero minimo di validatori online pari a 3.
- Nel caso in cui un determinato blocco non risultasse valido, quindi non approvato dai 2/3 dei validatori, comporterà delle sanzioni per il validatore che lo ha proposto.
- Tutti i blocchi che sono stati inseriti nella blockchain sono accessibili da chiunque.
- Tale blockchain supporta l'utilizzo e la pubblicazione di smart contract.

Caratteristiche dello smart contract

La Società pubblica uno smart contract sulla blockchain specificando:

- Identificativo del referendum e percentuale minima di votanti richiesti (P), se necessaria ai fini della validità della votazione.
- Un parametro Paga PA (che sarà il compenso da parte del Ministero del Voto per la società per il lavoro svolto, rilasciato al termine del referendum)
- Una Public Key PKSocietà della società utilizzata per le firme (ECDSA) e per la cifratura (ECIES) e un corrispondente certificato CertS.
- La finestra temporale nella quale è concesso il voto che corrisponde all'intervallo temporale T1-T2.
- La finestra temporale nella quale l'utente dovrà confermare la precedente partecipazione al voto, corrispondente all'intervallo temporale T2-T3.
- La finestra temporale nella quale la società dovrà inserire nello smart contract la propria SKSocietà, corrispondente all'intervallo temporale T3-T4.

Nella transazione per la pubblicazione dello smart contract è contenuto anche il collaterale versato dalla Società, che in caso di problemi con lo svolgimento del referendum verrà inviato alla Giustizia.

Il Ministero del Voto divulga attraverso i propri canali standard lo smart contract sopra descritto, cosicché chiunque possa verificarne il funzionamento e la correttezza, incentivando il singolo cittadino a prendere parte al referendum.

Analisi delle finestre temporali:

T0-T1

Supponendo che la votazione presa in esame risulti essere la prima votazione in modalità remoto/elettronica, è necessario prevedere una prima fase, antecedente alla finestra temporale dedicata alla votazione (T1-T2), in cui i cittadini abilitati e intenzionati a votare, qualora non ne fossero ancora in possesso, devono procedere ad ottenere la propria identità digitale (SPID). I cittadini potranno usare la propria identità digitale per accedere al sistema di votazioni svolte in modalità remoto/elettronica.

Prima dello scadere del blocco T1, il Ministero del Voto si impegnerà a depositare sullo smart contract la paga PA accordata con la Società, se così non fosse lo smart contract non accetterà votazioni.

T1-T2

Per ogni specifica votazione il sistema genererà, per ciascun utente che desidera prenderne parte, una coppia (PKV, SKV), ovvero rispettivamente la chiave pubblica, eventualmente consultabile dall'utente stesso, e la chiave privata associata al votante, utilizzata dal sistema; inoltre verrà coniato un NFT, specifico di tale votazione, che sarà associato a tale Chiave Pubblica (tra i due esisterà una relazione biunivoca). L'NFT sancirà il diritto di tale Chiave Pubblica di prendere parte alla votazione, lo smart contract verificherà quindi se a tale Chiave Pubblica corrisponde un NFT e se quell'NFT è associato alla specifica Chiave Pubblica, prima di validare la transazione. Solo con queste condizioni potrà essere convalidata la preferenza espressa dall'utente che altrimenti riceverà un messaggio di errore. L'utente potrà utilizzare l'applicazione, appositamente sviluppata per le votazioni, accedendo ad essa utilizzando la propria identità digitale. In seguito al corretto login verrà visualizzata la votazione corrente, o le votazioni, al quale l'utente può partecipare e, scelta quest'ultima, avrà la possibilità di esprimere la preferenza tra le alternative (favorevole, sfavorevole, voto nullo). Dopo aver scelto il voto verrà inviata una transazione ad un validatore della ItalyChain, che si occuperà della sua validazione e dell'eventuale inserimento in un blocco, una volta che ciò è accaduto, verrà inviata una notifica all'utente, la quale confermerà l'inserimento nella chain della preferenza. Altrimenti, se non devesse ricevere tale notifica entro un tempo limite, dovrà ripetere il processo fin quando non riceverà quest'ultima.

T2-T3

A termine della finestra temporale concepita per esprimere la propria preferenza (T1-T2), affinché il voto espresso venga correttamente conteggiato, l'utente dovrà confermarlo senza avere però la possibilità di modificarlo, effettuando nuovamente l'accesso al sistema. Tale conferma sarà inviata attraverso una transazione ad un validatore della ItalyChain, che si occuperà della validazione e dell'eventuale inserimento in un blocco cui seguirà, come nella fase T1-T2, una notifica all'utente, la quale confermerà l'inserimento nella chain della conferma. Altrimenti, se non devesse ricevere tale notifica entro un tempo limite, dovrà ripetere il processo fin quando non riceverà quest'ultima.

T3-T4

Terminata la finestra temporale predisposta per la conferma dei voti, la società deputata alla realizzazione dello smart contract pubblicherà la propria SK tramite una transazione, che verrà inviata ad un validatore della ItalyChain al fine di rendere ottenibili, e quindi visualizzabili, tutte le preferenze espresse riguardo al referendum. Successivamente attraverso tale chiave, sarà calcolato l'esito finale della votazione la cui pubblicazione sarà poi affidata al Ministero del Voto attraverso i propri canali ufficiali. Data l'estrema trasparenza dell'operazione, sarà alla portata di chiunque verificare che i risultati siano stati valutati con trasparenza, senza brogli.

Precisazione:

Il voto, oltre ad essere un diritto, è prima di tutto un dovere, nello specifico l'atto di voto consiste, tralasciando la fase di configurazione iniziale, nelle due transazioni, una nella finestra T1-T2 e una nella finestra T2-T3. Pertanto, si fa affidamento al buon senso dell'utente nell'inviare anche la seconda transazione, siccome il dovere viene completato solo dopo l'invio della stessa. In caso contrario la preferenza espressa nella finestra temporale T1-T2 verrà considerata equivalente ad un voto nullo, ovvero un voto conteggiato per il raggiungimento del quorum richiesto per la validità del referendum ma che non avrà peso per la vincita del sì o del no.

Funzionamento:

In particolare, il voto x richiede di calcolare:

- **C = SHA256(r || x)**
  r è una stringa random lunga 256-bit.
  L'impiego della randomness ha la necessità di mascherare il contenuto del messaggio (hiding). Essendo il message spacing estremamente piccolo, se non venisse impiegata la randomness, sarebbe troppo facile riuscire a risalire al messaggio anche attraverso approcci di ricerca esaustiva. Sarebbe un invio non malleabile del voto (binding).
  (Si sta considerando di trovarsi sotto l'assunzione del Random Oracle).
- **R = Enc(PkV, r)**
- *Tramite l'algoritmo di ECIES, attraverso la chiave pubblica del votante, verrà cifrato r. Il valore R serve per poter salvare il valore di randomness sulla blockchain, in modo tale che quando successivamente l'utente avrà la necessità di mandare la randomness per poter convalidare il proprio voto, potrà inviarlo anche operando da un dispositivo diverso rispetto al precedente.*
- **E = Enc(PkSocietà, C)**
  Tramite l'algoritmo di ECIES, attraverso la chiave pubblica della società, verrà cifrato C.

Il votante invia quindi tramite una transazione il messaggio m = (R,E).

Queste informazioni verranno inviate attraverso una "transazione" sulla blockchain (una transazione viene accettata se, e unicamente se, la verifica della firma risulta corretta; in particolare l'utente invierà **(m,Sigma)**, dove Sigma =Sig(SkV , m)).
Lo smart contract terrà memoria solo dell'ultimo messaggio m inviato, gli altri rimarranno comunque memorizzati nella blockchain (in blocchi precedenti).
Lo smart contract inoltre verificherà che alla chiave pubblica da cui proviene ciascuna transazione contenente una preferenza di voto, sia associato un NFT (simbolo del diritto al voto di quella chiave pubblica). In questo modo si evita che siano conteggiati voti provenienti da chiavi pubbliche e private associate ad utenti non autenticati tramite SPID, ma generate artificialmente per la conoscenza dell'algoritmo di generazione, falsificando l'esito del referendum.
Lo smart contract si occuperà di verificare che non si sia superato il tempo T2 (altrimenti risulta non valida la votazione in quanto inoltrata dopo la scadenza prefissata).

Dopo il tempo T2, il votante dovrà confermare la preferenza precedentemente espressa con un'altra transazione. Questa conferma sarà effettuata attraverso l'invio della randomness r con un meccanismo non esplicito all'utente. Alla blockchain verrà richiesto il valore R associato alla specifica chiave pubblica del votante, dal quale si potrà risalire con un algoritmo di decifratura alla randomness r, attraverso la chiave privata del votante stesso. In questo modo si fa sì che l'utente possa successivamente confermare il proprio voto anche da un dispositivo differente rispetto a quello utilizzato in fase di votazione.

L'invio di r richiede:

- **r = Dec(SkV, R)**

Il votante invia quindi tramite una transazione il messaggio r (verrà quindi inviato **(r,Sigma),** dove Sigma =Sig(SkV , r)), la cui correttezza verrà comunque accertata dallo smart contract che verificherà se **Enc(PkV, r) == R**.
Nel caso in cui il votante avesse, durante la finestra temporale T1-T2, modificato la propria preferenza, l'unica randomness che verrebbe inviata sarebbe quella associata all'ultima preferenza espressa.

Dopo il tempo T3, sarà terminata la fase di invio delle conferme dei voti. La società pubblicherà sullo smart contract la propria chiave privata. A questo punto, potrà essere computato il risultato finale del referendum, a patto che la chiave privata fornita dalla società risulti corretta.
La preferenza di ciascun votante potrà essere calcolata attraverso:

- C=Dec(SkSocietà,E)
- If SHA256(r || 00) == C
  x = 00 (il voto è no)
  elif SHA256(r || 01) == C
  x = 01 (il voto è nullo)
  elif SHA256(r || 11) == C
  x = 11 (il voto è sì)
  else
  voto nullo

Qualora la chiave privata fornita dalla società non fosse corretta, il che può essere verificato essendo a conoscenza della chiave pubblica e dell'algoritmo usato per generarla (curve ellittiche), sarà impossibile procedere alla decifratura, così come nel caso in cui la società si rifiutasse di fornirla.
Il risultato finale del referendum sarà divulgato dal Ministero del Voto, insieme alle istruzioni attraverso le quali ogni cittadino potrà verificare che il proprio voto sia stato correttamente conteggiato. A questo punto sarà resa pubblica l'associazione tra ciascuna chiave pubblica e il voto espresso. In questo modo ogni cittadino, a partire da tali chiavi pubbliche potrà controllare che i voti tenuti in conto siano associati ad identità dotate dell'NFT sopra menzionato e che abbiano quindi l'autorizzazione a votare.

Qualora la Società dovesse rifiutarsi di fornire la propria chiave segreta, o equivalentemente dovesse fornirne una non corretta, si aprirebbe un caso di disputa in cui verrebbe chiamata in causa la Giustizia e in cui chiaramente sarebbe banale accertare la responsabilità e l'errato comportamento della società. Quest'ultima quindi perderebbe il collaterale depositato sullo smart contract e non verrebbe pagata per il lavoro svolto, ovvero non incasserebbe la cifra accordata con il Ministero del Voto, che risiede anch'essa nello smart contract. Il ruolo della Giustizia sarebbe invece la punizione penale di tale gesto, che minerebbe indubbiamente anche la professionalità e la reputazione della Società. In tal caso ovviamente le votazioni sarebbero annullate e andrebbero effettuate nuovamente in un secondo momento.
Qualora a seguito della pubblicazione degli esiti, e della consultazione da parte di ciascun votante della corretta presa in carico del proprio voto, il cittadino dovesse sollevare l'accusa che il suo voto sia stato modificato o non conteggiato, si aprirebbe un caso di disputa in cui sarebbe chiamata in causa la Giustizia. In merito all'accusa riguardante il fatto che il suo voto non sia stato conteggiato è impossibile che ciò sia accaduto in quanto al momento della scelta della preferenza, segue la comunicazione di conferma della transazione il che significa che necessariamente deve essere stata aggiunta alla chain, il conteggio è poi frutto di un algoritmo pubblicamente verificabile contenuto nello smart contract. In merito invece alla possibilità che il voto sia stato modificato, qualora la transazione associata a quella chiave pubblica fosse soltanto una, questa dovrebbe necessariamente

contenere la preferenza espressa dal votante, in quanto un blocco aggiunto alla chain non può essere poi successivamente modificato.
Essendo i messaggi inviati sulla chain e firmati con la chiave privata dell'utente stesso, per ipotizzare una qualsiasi modifica al voto, è necessario supporre che l'artefice di tale imbroglio sia in possesso della chiave privata dell'utente.
I dati sulla blockchain, come sappiamo, non possono essere in alcun modo modificati, supponendo che questa cosa sia falsa si ricreano due scenari differenti:

1. Il malintenzionato riesce a modificare la prima transazione, il che significa che potrebbe tranquillamente cambiare la preferenza espressa dal votante, rieffettuando il medesimo procedimento che dovrebbe effettuare l'utente onesto.
2. Il malintenzionato riesce a modificare la seconda transazione, il che significa mandare non la randomness realmente usata nel calcolo della C, ma una nuova randomness r'. Questo gesto implicherebbe che lo SHA256 ottenuto all'atto di calcolo della preferenza del votante, non sarebbe corrispondente a nessuna delle tre preferenze realmente ammesse e dunque il voto sarebbe considerato non valido, in caso opposto significherebbe che il malintenzionato ha trovato una collisione.

Tali due scenari sarebbero però impossibili dal momento che richiederebbero la conoscenza della chiave privata dell'utente e la possibilità di modifica del contenuto di una transazione.
Quindi l'unica modifica possibile si sarebbe potuta ottenere attraverso un'ulteriore transazione, anch'essa visualizzabile sulla blockchain (dunque tracciata), il che avrebbe però richiesto di fare accesso al sistema con le credenziali dell'utente ed essere dunque in possesso dell'identità digitale del votante.

La scelta di pubblicare tutti i dati necessari per la decifratura rende il sistema il più trasparente possibile.
Inoltre, le chiavi pubbliche e private di ciascun votante e ovviamente della Società verranno modificate per ciascuna elezione, in modo tale da garantire forward security e privacy.
Inoltre, la pubblicazione solo e unicamente dell'ultimo r scelto garantisce che i voti precedentemente espressi non siano pubblici.

Caratteristiche dell'autenticazione (SPID):

SPID (Sistema Pubblico di Identità Digitale) è il sistema unico di accesso con identità digitale ai servizi online della pubblica amministrazione italiana e dei privati aderenti. Con un'identità digitale i cittadini e le imprese possono accedere a tali servizi e fruirne da qualsiasi dispositivo. Per ottenere l'identità digitale bisogna farne richiesta a uno degli Identity Provider, tra quelli autorizzati dall'AgID (Agenzia per l'Italia Digitale).
Il Sistema SPID è costituito da un insieme aperto di soggetti pubblici e privati, accreditati dall'AgID che gestiscono i servizi di registrazione e di messa a disposizione sia delle credenziali sia degli strumenti di accesso in rete per conto delle pubbliche amministrazioni, in modo che cittadini e imprese possano usufruirne.
Gli attori individuabili in un sistema SPID sono:
-**Gestore delle identità** (Identity Provider o IdP), che fornisce le credenziali di accesso al sistema (identità digitali) e gestisce i processi di autenticazione degli utenti.
-**Fornitore di servizi** (Service Provider o SP), eroga il servizio in seguito alla ricezione di autorizzazione da parte dell'IdP.
-**Gestore di attributi qualificati** (Attribute Authority o AA), che fornisce attributi per qualificare gli utenti (stati, ruoli, titoli, cariche), per regolare la fruizione dei servizi.
Con lo SPID i Service Provider, per consentire l'accesso ai servizi da essi erogati, potrebbero avere necessità di informazioni relative ai soggetti richiedenti. Dunque, dovranno segnalare ai Gestori delle Identità quali sono gli attributi di cui hanno bisogno, i quali dovranno essere attestati con l'asserzione emessa a seguito dell'autenticazione dei soggetti richiedenti i servizi, previa autorizzazione da parte dell'utente. Possono però richiedere solo il set minimo di attributi pertinenti al servizio offerto, mantenendoli solo per il tempo necessario alla verifica stessa, secondo quanto specificato nell'articolo 11 del decreto legislativo n. 196 del 2003.
I fornitori di servizi scelgono il livello di sicurezza SPID necessario per accedere ai propri servizi. Esistono infatti tre livelli di sicurezza:
-**Il primo livello** permette di accedere ai servizi online attraverso un nome utente e una password scelti dall'utente;
-**Il secondo livello** permette l'accesso con nome utente e password più un codice temporaneo di accesso (one-time password), fornito tramite SMS o app;
-**Il terzo livello**, oltre al nome utente e la password, richiede un supporto fisico per l'identificazione, ad esempio una smart card (non genericamente supportato).
A livello 1 SPID, i file delle credenziali devono essere protetti non contenendo le password in chiaro, per cui vengono usate tecniche come salt e hashing. A livello 2 e 3 SPID, vale quanto indicato a livello 1 con i necessari allineamenti per i moduli crittografici e di sicurezza software/hardware.
Un Service Provider può aggiungersi alla rete SPID scambiandosi dei metadati con l'Identity Provider con il quale si vuole accoppiare. Lo SPID si basa su una federazione SAML 2.0.(dal 1º maggio 2022 con OpenID Connect). OpenID Connect (OIDC) è uno strato di autenticazione del framework autorizzativo OAuth 2.0. Lo standard è controllato dalla fondazione OpenID Foundation.
SAML (Security Assertion Markup Language) è uno standard informatico per lo scambio di dati di autenticazione e autorizzazione (dette asserzioni) tra domini di sicurezza distinti, tipicamente un Identity Provider e un Service Provider o anche un Attribute Provider. SAML richiede che l'utente (detto "principal") sia registrato presso almeno un Identity Provider, che deve provvedere ad autenticarlo, facendo sì che il Service Provider possa affidarsi a lui per identificare il principal. Più nello specifico affinché un utente possa accedere ai servizi disponibili in rete attraverso SPID, devono verificarsi i seguenti passaggi:
1) Il titolare dell'identità digitale richiede l'accesso ad un servizio;
Il Fornitore dei Servizi, per poter procedere, deve individuare il gestore dell'Identità digitale in grado di autenticare il soggetto richiedente, fa scegliere quindi all'utente il proprio gestore dell'identità digitale.

2) Il Fornitore dei Servizi indirizza il soggetto titolare dell'identità digitale presso il Gestore dell'Identità Digitale individuato al passaggio precedente, richiedendo l'autenticazione con il livello SPID associato al servizio richiesto e l'eventuale attestazione di attributi necessari per l'autorizzazione all'accesso;
3) Il Gestore dell'Identità Digitale verifica l'identità del soggetto sulla base di credenziali fornite dallo stesso. Se tale verifica ha esito positivo viene emessa, ad uso del Fornitore dei Servizi, un'asserzione di autenticazione SAML attestante gli attributi eventualmente richiesti.
4) Il titolare dell'identità digitale viene quindi reindirizzato, portando con sé l'asserzione prodotta, verso il Fornitore dei Servizi;
5) Il Fornitore dei Servizi può, a questo punto, avere la necessità di verificare attributi qualificati riferibili all'utente;
6) Il Fornitore dei Servizi, raccolte tutte le necessarie asserzioni SAML, verifica le policy di accesso al servizio richiesto e decide se accettare o rigettare la richiesta.

Caratteristiche della Comunicazione con Validatore:

Per la comunicazione con il Validatore, e quindi per la pubblicazione di una transazione, si è scelto di utilizzare la rete Tor (The Onion Routing Protocol), rete che cerca di proteggere la privacy e mantenere l'anonimia; in particolare:
Tor è un network di tunnel virtuali. I dati vengono mandati attraverso diversi nodi/server (chiamati relays), ovviamente appartenenti alla rete Tor, scelti dall'utente. L'ultimo di questi server è colui che comunica direttamente con il servizio che stiamo richiedendo. Questa serie di server viene chiamato circuito.

Il termine Onion, cipolla in italiano, descrive intrinsecamente come vengono cifrati i dati. In particolare, ogni volta che si passa per uno specifico relay il pacchetto viene cifrato/decifrato utilizzando una specifica chiave. Il client che inizia la connessione concorda le chiavi con i diversi server per il quale il pacchetto transiterà, e, com'è giusto che sia, i singoli server conoscono solo la propria chiave. Il client, quindi, cifrerà per ogni relay il suo messaggio che verrà poi decifrato e reindirizzato passando tra diversi server, fino ad arrivare all'ultimo, detto anche "Exit Node", che si occuperà della comunicazione con lo specifico servizio richiesto dall'utente.
Nel caso cui fossero scelti 3 relay (il numero consigliato), l'utente cifrerà il messaggio con le chiavi dei rispettivi relay, iniziando con quella dell'exit node.
Supponendo di aver concordato con i vari relays rispettivamente K1,K2,K3, partendo dal Message si ottiene:

- c3 = Enc (K3, M)
- c2 = Enc (K2, c3)
- c1 = Enc (K1, c2)

Inviando C1 al primo relay questo sarà in grado di decifrarlo con la propria chiave, ottenendo c2, e di inviare il pacchetto al secondo relay, che decifrerà a sua volta, ottenendo c3, ed infine inviando il pacchetto all'ultimo relay che, con questa ultima decifratura, otterrà il messaggio effettivo.
All'interno del messaggio ci sono le informazioni necessarie per effettuare il collegamento con il servizio specifico richiesto dall'utente.
Per quanto riguarda la risposta da parte del servizio, il processo è l'inverso di quanto visto prima. Ogni relay cifrerà con la sua chiave e invierà il pacchetto al precedente, arrivando infine al client, come un nuovo c1', che sarà in grado di decifrare siccome è dotato delle chiavi necessarie per farlo.

- La scelta di almeno tre relay differenti "garantisce" la privacy e l'anonimia perché così facendo:
- Nel caso del primo relay
    - Esso conosce chi è il client ma non chi è il destinatario della comunicazione.
- Nel caso del secondo relay
    - Esso conosce i due altri relay ma non sa chi è il client né il destinatario.
- Nel caso del terzo relay
    - Esso conosce con chi è il destinatario ma non il client che ha richiesto il servizio.

WP3

Completeness:

Attraverso un'ispezione, si può osservare direttamente che se tutti gli attori del sistema seguono il protocollo prescritto, non c'è contestazione, nessun coinvolgimento della Giustizia e il risultato del referendum risulterà corretto.
Si noti che la giustizia è coinvolta solo in casi di disputa, e le azioni che può intraprendere sono legate al mondo fisico, più nello specifico, quando vi sono comportamenti malevoli in relazione al corretto funzionamento del sistema (i.e. mancata comunicazione della corretta Sk da parte della società, contestazioni da parte del cittadino o un no-evox, etc..). Ovviamente il sistema avrà un comportamento tale da rendere evidente agli occhi di chiunque una eventuale problematica e di conseguenza ad eventuali contestazioni corrisponderebbe una prova tangibile da parte del sistema che ciò sia o meno avvenuto. L'accertamento di eventuali imbrogli decreterà la validità o meno del risultato finale ottenuto, e quindi la necessità di un intervento correttivo quando possibile.

La viscida governance della società

La governance della società in questo contesto possiede a differenza degli altri attaccanti la chiave privata SkSocietà, la quale sicuramente risulta un vantaggio non indifferente.
Se il suo obiettivo fosse quello di ottenere l'esito desiderato dalle votazioni, potrebbe condurre attacchi fino alla pubblicazione dei voti effettuata nella finestra T3-T4.
In particolare, potrebbe decidere di:

- alterare il conteggio finale: Non è possibile, infatti il tutto è gestito all'interno dello smart contract, immutabile e pubblico, dunque seppure in possesso della SkSocietà, da questa non potrà trarne vantaggio.
- far accettare transazioni artificialmente prodotte tramite chiavi pubbliche e private ben fatte ma non generate tramite canali ufficiali. Questo tipo di attacco è stato gestito in quanto, per poter esprimere una preferenza, lo smart contract verificherà che l'onesto votante sia in possesso di un NFT consegnatogli quando accede per la prima volta a quella specifica votazione tramite canali ufficiali; dunque, delle public key generate "artificialmente" non sarebbero abilitate al voto.

Integrity:

L'ISP cospiratore:

Il provider della rete internet potrebbe agire sulla rete di dominio compromettendo la votazione dei propri clienti. Ovviamente in un tale scenario indubbiamente la proprietà D.1 potrebbe essere messa sotto attacco. Infatti, l'ISP è fondamentalmente in grado di guardare quello che è il traffico, ovviamente cifrato, di un utente. Anche i pacchetti inviati tramite la rete Tor non vengono meno a questa precisazione, di conseguenza tramite Deep Packet Inspection l'ISP potrebbe analizzare la dimensione, il volume e il tipo riconoscendo i dati del traffico di Tor, vietandone l'inoltro, o addirittura, nel caso di un ISP molto malevolo, vietare la connessione con un qualsiasi Relay di Tor. Per ovviare a questa problematica gli sviluppatori di Tor hanno creato "Pluggable Transports", che trasforma il traffico di Tor in modo che l'ISP veda "un traffico dall'aspetto innocente". Per la seconda problematica sono stati realizzati dei particolari server detti "Bridge Node" che fungeranno da ponte per comunicare con un relay (questi Bridge non sono pubblici quindi un ISP non è in grado di bloccarli). Bisogna precisare che questi tipi di attacchi non coinvolgerebbero solo votanti del referendum ma qualunque utente che desidera usufruire dei servizi di Tor; dunque, esporrebbe l'ISP ad una gogna mediatica. Seppure dovessero verificarsi, attacchi di questo genere verrebbero però svelati, in quanto il sistema prevede un meccanismo di comunicazione della conferma della transazione, firmata dal validatore che l'ha presa in carico, che sarebbe dunque impossibile da replicare da parte dell'ISP. Inoltre, essendo le transazioni pubblicamente consultabili, chiunque potrebbe verificare che la propria transazione, conoscendo la propria chiave pubblica, sia stata effettivamente inserita nella blockchain, dunque la proprietà I.2 risulterà essere sicuramente verificata, così come la D.1. Discorso analogo vale anche per le proprietà A.1 e I.1. Per venire meno queste proprietà, infatti, bisognerebbe ipotizzare una sorta di "men in the middle attack". Uno scenario di tale genere però è completamente da escludere, poiché tramite l'utilizzo di Tor, l'ISP non sarebbe in grado di distinguere un qualunque messaggio inviato nella rete internet da un voto per il referendum. Quindi, è da escludere la possibilità che l'ISP possa modificare il contenuto della preferenza espressa dal votante.
Anche la realizzazione di eventuali coalizioni tra l'ISP e altri attori sarebbe da escludere, infatti come si evince dall'analisi sopra effettuata l'ISP non sarebbe in grado di apportare alcuna possibilità in più di minare l'integrità, l'autenticità o la disponibilità agli altri attori.

Lo Schieramento polarizzato:

Questo gruppo di avversari vuole favorire un certo risultato del referendum, cercano infatti di manipolare su larga scala i voti inviati nella finestra di votazione T1-T2. Questo minerebbe in caso di successo addirittura la correttezza del risultato, la proprietà più importante; il che implicherebbe violare: le proprietà di integrità I.1, I.2 e quella di autenticità A.1. In questo caso le modalità di attacco si scindono in due tipologie:

- nel mondo reale (coercizione fisica, pubblicità e mass media, etc…):
  poiché riguarda il mondo reale, non è gestibile dal sistema digitalizzato, al quale arriverebbero transazioni corrette senza suscitare alcun dubbio sulla veridicità di queste. Tuttavia, questi gruppi con buona probabilità sono spesso bilanciati da un'organizzazione di comparabile potenza economica che vorrebbe incentivare la preferenza opposta e che implicitamente ne neutralizzerebbe l'azione.
- attaccando il sistema stesso:
  - Cercando di modificare le preferenze ancora non validate (in combutta con un validatore malevolo) in un blocco della chain
    ma questa cosa è impossibile poiché le transazioni nella finestra temporale T1-T2 nascondono la propria preferenza tramite SHA256 con randomness all'interno; dunque, sarebbe impossibile anche solo conoscerne il contenuto,

oltre al fatto che risultano firmate con la chiave privata del votante per cui sarebbe impossibile modificarne il contenuto.

- Cercando di alterare il conteggio finale
  Non è possibile, infatti il tutto è gestito all'interno dello smart contract, immutabile e pubblico.
- Cercando di far accettare transazioni artificialmente prodotte tramite chiavi pubbliche e private ben fatte ma non generate tramite canali ufficiali
  Questo tipo di attacco è stato gestito in quanto, per poter esprimere una preferenza, lo smart contract verificherà che l'onesto votante sia in possesso di un NFT consegnatogli quando accede per la prima volta a quella specifica votazione tramite canali ufficiali; dunque, delle public key generate "artificialmente" non sarebbero abilitate al voto.

Dunque, anche se abbiamo supposto possano fare investimenti medio-alti gli unici attacchi empiricamente validi sono quelli nel mondo reale. Potrebbero collaborare con l'ISP cospiratore, ma senza ottenere considerevoli miglioramenti, infatti, l'accesso al canale per i loro scopi non gli consentirebbe comunque di poter modificare eventuali preferenze a loro piacimento come già espresso nell'analisi relativa all'ISP.

La viscida governance della società

La governance della società in questo contesto possiede a differenza degli altri attaccanti la chiave privata SkSocietà, la quale sicuramente risulta un vantaggio non indifferente.
Se il suo obiettivo è quello di ottenere l'esito desiderato dalle votazioni, può condurre attacchi fino alla pubblicazione dei voti effettuata nella finestra T3-T4.
In particolare, potrebbe decidere di:

- Modificare i voti ancora non inseriti nella chain nella finestra temporale T1-T2 in combutta con uno o più validatori malevoli (minerebbe la correttezza oltre che le proprietà I.1, I.2, oltre che A.1): questo attacco non è realizzabile poiché le transazioni sono firmate con la chiave privata dell'utente da lui non nota. Inoltre, per poter anche solo leggere la preferenza, dovrebbe essere in possesso della randomness utilizzata dal votante, la quale è contenuta in R ma cifrata sempre con la chiave privata dello stesso, dunque, non accessibile prima della finestra T3-T4.

Gli sviluppatori procaccianti:

si identificano come dei dipendenti della Società adibita allo sviluppo del sistema per le votazioni, la quale ha stipulato un'intesa con il Ministero del Voto depositando un collaterale che in caso di eventuali problematiche verrebbe perso e dato alla Giustizia mentre in caso di buona riuscita del sistema guadagnerebbe il compenso depositato dal ministero. Da ciò possiamo già dedurre che un tipo di attacco da parte degli sviluppatori, che renda il sistema influenzabile da essi stessi, potrebbe essere facilmente intuibile data la trasparenza del sistema e porterebbe sia alla perdita del collaterale dato dalla società che al mancato guadagno per il loro lavoro. Anche un attacco di tipo divulgativo, quindi per esempio a livello di pop-up o inserzioni che influenzano la scelta del votante, sarebbe pubblicamente verificabile. In sostanza tutti gli attacchi praticabili dagli sviluppatori porterebbero a far sfigurare pubblicamente la Società, che ne risulterebbe gravemente colpita, e all'intervento della Giustizia nei loro confronti. Inoltre, l'utilizzo della tecnologia blockchain in quanto trasparente e condivisa porterebbe un attacco allo sviluppo del sistema a pubblica esposizione, permettendo a tutti di verificare la bontà o meno del lavoro svolto dagli sviluppatori; ciò garantisce il rispetto della proprietà di integrità I.2. Una eventuale collaborazione tra Società e Ministero del Voto per scopi malevoli non è pensabile in quanto la buona riuscita del referendum è nell'interesse del Ministero che ha unicamente quest'obiettivo in ambito istituzionale, inoltre essendo sotto l'occhio della Giustizia un broglio del genere porterebbe a gravi conseguenze penali per entrambe le parti; infine bisogna anche tener conto della difficoltà di una eventuale alleanza di questo genere tra

due parti comunque molto vaste. Tuttavia, un eventuale attacco da parte degli sviluppatori in termini di integrità risulterebbe essere comunque inefficace per le proprietà individuate. La proprietà I.1 resta intatta in quanto eventuali cambiamenti del voto fatti in maniera artificiosa potrebbero essere scoperti grazie alla trasparenza della tecnologia utilizzata e grazie alla randomness che è a conoscenza solo dell'utente, finché non viene inviata in fase di conferma.

Il ladro di identità:

è un attaccante che vuole venire a conoscenza delle credenziali degli utenti; essendo un attacco che viene effettuato al portale web (che utilizza SPID) la società non può contrastare quest'attaccante, in quanto il sistema da essi sviluppato non si occupa dell'autenticazione ma entra in gioco solamente nella fase di votazione, inoltre la Società non ha alcuna informazione sulle identità fisiche dei votanti che utilizzano il sistema, quindi eventuali collaborazioni tra ladro d'identità e società possono essere scongiurate. Il sistema di funzionamento del referendum prevede per la fase di registrazione l'utilizzo di SPID precedentemente descritto.

Le minacce associate al ciclo di vita delle identità digitali possono essere classificate, in base al momento in cui intervengono, in tre diverse categorie:
1) **quelle riguardanti la fase di registrazione**: queste sono relative al furto di identità o al ripudio della registrazione. Tali minacce possono tranquillamente essere dissuase utilizzando dei metodi che verifichino che il richiedente sia effettivamente l'utente titolare dell'identità dichiarata e che lo stesso non possa poi successivamente disconoscere la registrazione.
2) **quelle riguardanti la fase di emissione**: queste sono relative a furti/usurpazione di identità, o ad uno scorretto meccanismo di trasporto per l'emissione delle credenziali. Per mitigarle basta usare un trasporto affidabile (buste sigillate con posta raccomandata nel mondo fisico, oppure sessioni protette per spedizione nel mondo digitale), evitando anche eventuali manomissioni. Sicuramente è poi fondamentale che ci si accerti che la persona destinataria delle credenziali sia la medesima che ha partecipato al processo di registrazione.
3) **quelle associate ai token**: queste sono sicuramente la categoria più vasta, fanno riferimento al furto di token. Per token intendiamo qualcosa che abbiamo (software o hardware), qualcosa che conosciamo (password, PIN) oppure qualcosa che siamo (impronte digitali). In tale scenario si inquadrano per esempio il furto di un token fisico (es. cellulare), la cui gravità può essere mitigata con l'impiego di token multi-fattore (dati biometrici, PIN). Un altro esempio è la scoperta delle risposte alle domande di suggerimento, che potrebbe essere evitata rendendole più complesse. Potrebbero esserci attacchi fatti da siti civetta che simulano il sito originale facendo credere all'utente di essere il fornitore di servizi (DNS re-routing) e ottenendo in questo modo la password dell'utente. Il furto di una password potrebbe essere un rischio, mitigabile però attraverso l'utilizzo di token difficilmente duplicabili come token crittografici hardware. E allo stesso modo sarebbe utile utilizzare delle tecniche di autenticazione dinamica che fanno sì che la conoscenza di una parola non fornisca informazioni per successive autenticazioni. Questo discorso vale anche nel caso in cui si volesse supporre che ci sia un codice malevolo presso gli Identity Provider, tale che quando gli utenti chiedono di accedere inserendo user e password, tale codice invii questi dati a siti malintenzionati che vogliono raccoglierli. Ciò però risulta risolto se si considera che l'utente ha la necessità (per la maggior parte delle operazioni) ad effettuare un'autenticazione a due fasi (per esempio via sms), ulteriormente mitigato se il sito è sottoposto a delle misure di sicurezza solide.
Per evitare invece gli "attacchi da dizionario" si potrebbero usare token con una elevata entropia e che causino il blocco dopo un numero limitato di tentativi. In merito al furto di identità bisogna considerare che questo è punito penalmente con una reclusione fino a tre anni per il gestore di identità. Il furto di identità risulta ulteriormente mitigato dal fatto che il gestore dell'identità digitale, su richiesta dell'utente, segnala via e-mail o via sms, rispettivamente alla casella di posta o sul riferimento telefonico indicato dall'utente ogni avvenuto utilizzo delle credenziali di accesso.

Un'eventuale altra possibile criticità potrebbe essere l'utilizzo da parte dell'utente di browser o sistemi operativi non aggiornati (quindi vulnerabili a virus) i quali potrebbero esporlo al furto di identità. Un problema di tale genere ovviamente non è direttamente legato a SPID che comunque cerca di mitigarlo inibendo l'accesso a utenti che utilizzano sistemi obsoleti.
Bisogna inoltre sottolineare che SAML utilizza delle asserzioni che hanno una validità di tempo dell'ordine di qualche minuto e che una volta utilizzati non possono essere "riutilizzati" in modo malevolo.
Si potrebbe avere il timore che un Service Provider di sana pianta possa associare ad un utente azioni non realmente effettuate da quest'ultimo. Seppure tale attacco potrebbe accadere, sarebbe facilmente provabile in quanto il gestore dell'Identità Digitale deve mantenere traccia dei processi di autenticazione effettuati.
Ovviamente per il nostro sistema è necessario che l'autenticazione venga effettuata in accordo alla sicurezza SPID di tipo 2.
Inoltre, SPID beneficia già delle agevolazioni fornite dall'impiego di meccanismi quali sessioni temporizzate, HTTPS, e TLS. L'utilizzo di SAML e di vari gestori di identità e vari gestori dei servizi SPID che compongono una federazione di vari nodi, assicura che nel caso in cui uno dei sistemi si fermi o sia posto sotto attacco, solo questo non possa più erogare il servizio mentre gli altri nodi non ne sarebbero interessati, evitando quindi l'effetto domino.
Qualora dovesse essere perpetuato un furto di credenziali, inoltre, l'onesto votante che ne risulta vittima potrebbe appellarsi alla giustizia, che cercherebbe di ristabilire l'accesso all'account e punire penalmente l'attaccante. Se questo tipo di attacco andasse in porto, dal punto di vista dell'integrità la proprietà I.1 risulterebbe intaccata in quanto il voto fatto da un onesto votante non sarebbe più quello corretto e ciò intaccherebbe la buona riuscita delle votazioni; tuttavia, se il votante si rende conto del furto nella finestra T1-T2 può far sì che il suo voto venga ancora conteggiato, ripristinando la propria identità digitale ed essendo quindi abilitato ad effettuare una nuova votazione. La Giustizia successivamente interverrà per far sì che la vecchia votazione effettuata malevolmente dall'attaccante non venga considerata nei risultati. Se l'onesto votante si accorge del furto dopo la finestra T1-T2 non avrà la possibilità di effettuare la sua votazione e i risultati dovranno poi essere sottoposti a revisione. La proprietà di integrità I.2 resta robusta in quanto un furto di credenziali può essere facilmente intuito grazie alla tecnologia utilizzata che rende tracciabili, chiare, e quindi intuibili, tutte le informazioni inviate. Questo tipo di attaccante, infine, intacca anche la proprietà di autenticità A.1 in quanto il voto di un onesto votante non sarebbe più autentico.

Il miserabile Ministero del Voto:

Si tratta dell'organo di Governo che è alla base dell'organizzazione delle votazioni remote. Come già specificato nel WP1, potrebbe essere in combutta con la Società, quindi in possesso della Chiave Segreta di quest'ultima, e ha lo scopo di ottenere informazioni circa i voti o la modifica degli stessi andando a minare le proprietà I.1 ed A.1.
Per quanto riguarda la proprietà A.1, l'utilizzo degli NFT permette l'invio della preferenza solo ad una persona fisica, rendendo di fatto il sistema sicuro e funzionante; quindi, ci focalizzeremo sull'altra. Supponendo che l'attaccante sia in possesso della Chiave Privata dell'utente, questo risulta essere distruttivo per il nostro sistema perché sarebbe in grado di modificare senza alcun problema il voto, rendendo di fatto invalida la proprietà I.1. Da notare però che seppure si fosse in possesso di tale chiave, la modifica andrebbe fatta con un'ulteriore transazione che sarebbe comunque di fatto pubblicamente verificabile. L'unico modo per l'attaccante di ottenere tale Chiave è quello di utilizzare direttamente l'algoritmo di generazione, a patto di avere gli input necessari a disposizione, andando di fatto a renderlo insicuro. Tuttavia, essendo il codice utilizzato per lo sviluppo, pubblico, chiunque può verificarlo ed eventualmente segnalare tali criticità. Si ipotizza quindi che tale algoritmo sia stato verificato da esperti del settore e validato dai più garantendo la sua inattaccabilità. L'alternativa sarebbe quella di andare ad attaccare il meccanismo di login, cercando di accedere e ottenere la possibilità di modificare il voto; tuttavia, tramite la tecnologia SPID, come

precedentemente discusso, e la 2FA risulta complesso riuscire ad accedere al sistema senza essere l'effettivo proprietario dell'identità digitale.
Un possibile attacco che potrebbe essere effettuato da questo tipo di avversario, per minare l'integrità e l'autenticità del voto, potrebbe essere un attacco un po' meno diretto. Ovvero potrebbe pensare di condizionare le effettive preferenze dei votanti attraverso coercizioni su larga scala perpetuate tramite, ad esempio, i mass media. Tale attacco ovviamente essendo legato al mondo reale non può essere evitato attraverso un sistema digitale, per cui sarebbe necessario l'intervento della Giustizia.

Confidentiality:

Il Venditore di favori.

Quest'ultimo potrebbe essere interessato a conoscere più informazioni sul voto espresso da alcuni specifici votanti, per sapere se eventualmente hanno rispettato il patto accordato. Quest'ultimo quindi nello specifico potrebbe attaccare le proprietà P.1 e P.2. Poiché l'unica associazione che realmente viene messa in atto è quella tra chiave pubblica e voto espresso, non vi sarà modo, se non attraverso la conoscenza dell'identità digitale del votante (conosce le credenziali per l'accesso e quindi consultare la chiave pubblica), di ricreare l'associazione tra la chiave pubblica e il votante stesso inteso come cittadino, a meno che non sia il cittadino stesso a rivelarlo. Inoltre per garantire forward security la coppia (PkV,SkV) viene associata ad una singola votazione e non viene più utilizzata. Dunque, la proprietà P.1 viene preservata. Non potendo conoscere l'identità del votante, sapere il contenuto del voto, per questo tipo di avversario, perde di utilità. L'unica possibilità di attacco che rimane a questo tipo di avversario è la vera e propria coercizione, legata però al mondo fisico e non alla digitalizzazione del voto, che, come tale, solo in parte potrà essere controllata dal nostro sistema. Con coercizione in tale contesto si intende che il votante viene costretto da tale avversario ad esprimere la propria preferenza in sua presenza. Si è cercato di ovviare a questo problema offrendo all'utente la possibilità di cambiare il proprio voto e di esprimerlo in un secondo momento in cui si sente libero di farlo. È chiaro però che un avversario così invadente presumibilmente non avrà problemi a venire a conoscenza della chiave pubblica del votante in questione. Dunque, questa è l'unica situazione in cui le proprietà P.1 e P.2 potrebbero non essere soddisfatte completamente, a fronte però dell'ottenimento della massima trasparenza. Inoltre, va comunque analizzata la situazione per cui problematiche esistenti e fortemente legate al mondo reale non possano essere risolte attraverso un sistema informatico, ma soltanto mitigate, anche perché ragionevolmente un avversario di questo tipo non minerà l'esito del referendum essendo impossibilitato a portare avanti un attacco su larga scala.

L'ISP cospiratore:

Tale avversario potrebbe minare la proprietà P.1, infatti vi è una problematica della rete Tor che mina l'anomia e la privacy, non ancora risolta, e indipendente dal numero di relay scelto. L'attacco si verifica quando il primo nodo, quindi quello con il quale il Client comunica, e l'ultimo nodo hanno lo stesso proprietario malevolo. Come già specificato sopra questi due nodi singolarmente conoscono il client e il destinatario, di conseguenza una collaborazione tra questi due potrebbe creare non pochi problemi; infatti, analizzando i dati, la dimensione e altre informazioni, ci si potrebbe ricondurre agli indirizzi IP di mittente e destinatario. Tuttavia, i dati all'interno di essi non verrebbero in alcun modo intaccati, quindi le proprietà P.2 e P.3 risultano integre. Per ovviare a tale problematica è utile scegliere come primo nodo uno del quale ci si fida, rendendo, di fatto, impossibile tale attacco. Inoltre, una possibile mitigazione, proprio come la rete BitCoin, potrebbe essere avere un numero maggiore di nodi rendendo la rete sempre più sicura.
Tale attacco richiede un dispendio non indifferente di risorse economiche, perché ovviamente aumentando il numero di server dei quali si è proprietario aumenta la possibilità di essere scelto nelle posizioni chiave. Risulta quindi plausibile che un ISP, o eventualmente singoli attaccanti che cooperano, possano attuarlo.

La viscida governance della società

La governance della Società in questo contesto possiede a differenza degli altri attaccanti la chiave privata SkSocietà, la quale sicuramente risulta un vantaggio non indifferente.
Se il suo obiettivo fosse quello di conoscere l'esito delle votazioni al fine di trarne profitti di mercato, presumibilmente potrebbe realizzare tale attacco nella finestra temporale T2-T3 durante quindi la fase in cui i votanti inviano attraverso l'operazione di conferma la propria randomness, infatti prima

di questo momento la governance non ha modo di conoscere quest'ultimo autonomamente essendo una informazione conosciuta esclusivamente dal votante e necessaria per capire la preferenza espressa da questo. Detto questo però dal momento in cui queste randomness vengono inviate, la governance è in grado di ottenere le rispettive preferenze e quindi prendendo coscienza dell'andamento delle votazioni. Questo minerebbe fortemente la proprietà P.3. Infatti, seppur non può conoscere fino all'invio di tutte le randomness, l'esito completo, già informazioni parziali potrebbero risultargli soddisfacenti.

Gli sviluppatori procaccianti:

si identificano come dei dipendenti della Società adibita allo sviluppo del sistema per le votazioni. Una eventuale collaborazione tra Società e Ministero del Voto per scopi malevoli non è pensabile in quanto la buona riuscita del referendum è nell'interesse del Ministero che ha unicamente quest'obiettivo in ambito istituzionale, inoltre essendo sotto l'occhio della giustizia un broglio del genere porterebbe a gravi conseguenze penali per entrambe le parti; infine bisogna anche tener conto della difficoltà di una eventuale alleanza di questo genere tra due parti comunque molto vaste. Tuttavia, se un attacco del genere andasse in porto ne sarebbero intaccate le proprietà di privacy P.2 e P.3 in quanto le informazioni sul voto sarebbero le uniche maneggiate dagli sviluppatori della società. Più nello specifico la società può ottenere informazioni circa il voto dei cittadini solo una volta che essi avranno inviato la loro randomness, quindi nella finestra temporale T2-T3 nella parte conclusiva della votazione. In questa parte conclusiva la società potrebbe divulgare informazioni circa i voti e quindi riguardo i risultati della votazione stessa. L'identità dei votanti resterebbe comunque riservata, non permettendo alla società di divulgare informazioni circa il voto di specifici cittadini che agli occhi degli sviluppatori rimarrebbero una coppia (PK,SK), di conseguenza P.1 risulta robusta rispetto a questo tipo di attacco.

Il ladro di identità:

Le potenzialità e le implicazioni di utilizzare SPID come sistema di autenticazione sono state già precedentemente discusse nell'analisi di integrità. Se questo tipo di attacco accadesse, l'attaccante potrebbe verificare il voto di un utente, quindi, intaccherebbe le proprietà P.1 e P.2, mentre la proprietà P.3 risulterebbe solo in parte messa sotto attacco in quanto l'avversario potrebbe venire a conoscenza solo di un numero limitato di identità.

Il ficcanaso:

Quest'ultimo potrebbe essere interessato a conoscere maggiori informazioni sulle percentuali del "sì" o del "no" del referendum, al fine di utilizzare queste informazioni per scopi personali.
Quest'ultimo quindi nello specifico potrebbe intaccare le proprietà P.2 e P.3.
Tuttavia, tale attacco potrebbe portare dei seri benefici a tale attaccante solo se effettuato tra T1-T2, questo perché potrebbe anticipare, e non di poco, il risultato della votazione.
Si nota che tale attaccante ha la necessità di conoscere la Chiave Segreta della Società, ottenibile o collaborando con la Società o rompendo lo schema di generazione delle chiavi. Tale Chiave serve per poter attaccare quando "conviene", quindi quando i risultati non sono pubblici e trarre più beneficio da ciò.

L'attaccante potrebbe agire in due momenti differenti con altrettanti diversi benefici, nello specifico:

- Attacco tra T1-T2
    - L'attaccante per recuperare un voto in questo punto dovrebbe conoscere la Chiave Segreta della Società, in modo da poter decifrare E e quindi ottenere C (che ricordiamo essere lo SHA256(r || x); una volta ottenuto C dovrebbe conoscere la r (ottenibile solo e unicamente attraverso la Chiave Privata dell'utente) o riuscire a trovare una combinazione SHA256(r' || x') riuscendo, di fatto, a recuperare il voto (o a trovare una collisione); tuttavia con tale

algoritmo, dato il breve tempo a disposizione, sarebbe impossibile decifrare ogni singolo voto.

- Attacco dopo T2
    - In questo momento l'utente ha pubblicato la sua randomness, tuttavia è richiesto comunque conoscere la Chiave Segreta della Società che verrà pubblicata immediatamente dopo T3 rendendo, di fatto, inutile attaccare in questo momento perché ormai allo scadere delle elezioni. Inoltre, seppur ci fosse una collaborazione con la Società il tempo necessario a decifrare tutti i voti (in teoria di numero molto elevato) non sarebbe sufficiente perché la Chiave Segreta deve essere pubblicata in tempi molto brevi, pena l'intervento della Giustizia, rendendo di nuovo inutile operare in queste condizioni.

Di conseguenza le proprietà P.2 e P.3 vengono invalidate solo se l'attaccante, partendo da una conoscenza della Chiave Privata della Società, riesce a ricalcolare i valori che portano a quello specifico SHA256 (che potrebbe anche portare all'individuazione di una collisione invece che ai valori corretti) o tramite la conoscenza della Chiave Privata dell'utente; dunque tali proprietà rimangono preservate.

Il miserabile Ministero del Voto:

Si tratta dell'organo di governo che è alla base dell'organizzazione delle votazioni remote. Come già specificato prima, potrebbe essere in combutta con la Società, quindi in possesso della Chiave Segreta di quest'ultima, e ha lo scopo di diffondere informazioni circa i voti o la modifica degli stessi andando a minare la proprietà P.3.

L'attaccante possedendo la Chiave Segreta della Società potrebbe in qualunque momento ottenere il valore di C (che ricordiamo essere pari a SHA256 (r || x)) e, partendo da questo valore, riuscire a trovare una combinazione SHA256(r' || x') che porterà, di fatto, al recupero del voto (o ad una collisione); tuttavia con tale algoritmo ad oggi sarebbe impossibile decifrare ogni singolo voto. Anche con un investimento elevato (che risulta plausibile per un ente così importante) richiederebbe componenti all'avanguardia che comunque impiegherebbero un tempo troppo elevato per essere utili. Quindi possiamo dire che la proprietà P.3 risulta soddisfatta.
Anche questo attaccante potrebbe minare la privacy e l'anonimia di Tor con l'attacco precedentemente descritto (proprietario del primo e dell'ultimo relay).

Efficienza:

Il Sistema progettato risulta essere sufficientemente efficiente. Gli attori che sono chiamati ad avere un ruolo attivo sono i votanti stessi nei giorni individuati per il referendum, così come la Società, il cui onere è la realizzazione dello smart contract, e la pubblicazione della propria chiave segreta a termine delle elezioni. Per quanto riguarda il Ministero del voto ha un coinvolgimento più marginale, circoscritto alla divulgazione dello smart contract e dei risultati finali delle elezioni. La giustizia invece interviene solo nei casi di disputa in cui è necessario accertare le responsabilità penali. Dunque, questi ultimi due attori non hanno la necessità di essere online e reattivi durante la fase di votazione né di calcolo dell'esito finale. Anche il ruolo della società nella finestra temporale T1-T2 è passivo. Dunque, gli unici protagonisti sono i votanti ai quali viene chiesto il piccolo sacrificio di esercitare il voto attraverso una duplice transazione. Si sarebbe potuto fare a meno di richiedere questa seconda transazione relegando la detenzione della randomness a degli organi di fiducia, che avrebbero poi provveduto a rilasciarla al momento dello spoglio. Si è preferita però la prima soluzione in quanto, seppur richiedesse uno sforzo maggiore al votante, era un'ulteriore fonte di trasparenza, evitando il coinvolgimento di parti verso cui sarebbe stato necessario fare ulteriori assunzioni di fiducia e di collaborazione. Per mitigare tale sforzo richiesto al cittadino si è inoltre proposta una soluzione che consentisse, pur mantendendo privata la randomness fino al momento dell'invio, che la conferma del voto potesse essere effettuata anche da un dispositivo differente. Per questo scopo, infatti, nella prima transazione il votante cifrerà anche la randomness utilizzata con la sua chiave pubblica, custodendola sulla blockchain, per rimandarla poi successivamente, al termine della finestra T1-T2, a fronte di un overhead minimo richiesto. Si noti che si sarebbero potuti concepire dei protocolli più complessi affinchè la randomness inviata dal votante nella finestra temporale T2-T3 non fosse subito utilizzabile dalla Società per iniziare e calcolare le preferenze dei votanti. L'aspetto negativo di queste informazioni disvelate in anticipo potrebbe essere un eventuale condizionamento dell'andamento del voto. In realtà però è stato valutato che l'impatto sarebbe stato minimo, trovandoci nella finestra temporale T2-T3 tutt'al più i votanti, conoscendo la momentanea evoluzione della votazione avrebbero potuto scegliere di non effettuare la seconda transazione. L'unica forma di sabotaggio perpetuabile in questa finestra temporale potrebbe essere impedire il raggiungimento del quorum per il referendum, in quanto la preferenza espressa non può più essere modificata. In realtà però anche un voto per il quale non viene inviata la randomness non potrà essere decifrato e dunque il suo contenuto verrà considerato al pari di un voto nullo ma verrà comunque conteggiato come voto effettuato e dunque convergerà nella valutazione del quorum. L'impiego di una blockchain permissioned piuttosto che di una permissionless ha inoltre dato un'importante garanzia di efficienza, essendo richiesto uno sforzo minimo da parte dei validatori, si ha la possibilità di garantire che siano effettuate un grande numero di transazioni al minuto, tale da poter reggere la richiesta, oltre che dal punto di vista ambientale comporta un impatto molto meno dannoso.

Il DDoSSer:

questo avversario ha l'ambizione di non permettere il regolare svolgimento delle votazioni. Il suo attacco avviene tra T1-T3. L'attacco consiste nel non permettere l'accesso alla "piattaforma" per votare, rendendo quindi, di fatto, impossibile l'invio/modifica/conferma del voto attaccando la disponibilità D.1. Questo attacco può essere svolto in tre modi:

- Inviando ingenti transazioni artificiali così da sovraccaricare il sistema formato comunque da un numero limitato di validatori

  Questo tipo di attacco è combattuto da più cose, la prima è che il sistema potrebbe preprocessare le transazioni andando a verificare immediatamente la presenza dell'NFT associato alla chiave pubblica che vuole effettuare questa transazione, andando a limitare un aumento critico di overhead nella gestione delle transazioni,

inoltre per come è progettata la chain può gestire blocchi di grandezza finita il cui valore non è limitato superiormente, dunque risulta complesso mettere in crisi già in partenza una struttura di questo tipo con investimenti medio-bassi.

- Cercando di manomettere più validatori possibili

  Per progettazione il sistema funziona anche con solo tre validatori online; dunque, in questo caso richiederebbe di manomettere fisicamente 105 validatori in provincie diverse… decisamente un attacco fuori portata.

- Attaccando i server che permettono la navigazione sul sito per votare regolarmente

  Condurre questo attacco è possibile, avvalorato dal fatto che ci saranno ingenti accessi al sistema durante i giorni di voto; è quindi necessaria una enorme scalabilità per la gestione delle richieste di accesso al server per far sì che il portale possa garantire un livello di prestazioni adeguato.

Per quel che riguarda la rete Tor un DDosser potrebbe negare l'accesso ai Guard Node rendendo o inutilizzabile la rete o aumentando il rischio di altri attacchi (ad esempio se il primo e l'ultimo nodo appartengono ad uno stesso proprietario malevolo). Tuttavia, disponendo di poche risorse e considerando che la rete Tor è abbastanza estesa, potrebbe causare il blocco di un numero limitato di Guard Node ma non di tutti rendendo però le operazioni di voto più lente.

Transparency:

Essendo il sistema basato sull'utilizzo di ItalyChain, una blockchain permissioned progettata in maniera tale da garantire totale trasparenza, sarà di conseguenza caratterizzato da una completa verificabilità pubblica di ciò che accade e di tutte le informazioni che viaggiano sul sistema; in questo modo eventuali frodi sarebbero agli occhi di tutti e non potrebbero essere nascoste. Infine, l'utilizzo di una blockchain fa sì che il ruolo svolto da persone fisiche sia minimo rispetto al funzionamento del sistema, in modo che eventuali problematiche relative alla corruzione delle parti in gioco siano del tutto minimizzate, richiedendo l'intervento di ministero del voto o di giustizia soprattutto e unicamente in caso di dispute.

Benefici nell'uso di SPID

In SPID tutti gli attori si applicano per mantenere l'intero sistema sicuro ed efficiente, tramite il monitoraggio attivo e l'analisi costante di quanto è successo, in termini di performance, occupazione di spazi fisici e logici, di disponibilità dei sistemi, di esecuzione del corretto funzionamento delle applicazioni, di assenza di tentativi di accesso non autorizzati e di corretta esecuzione dei processi di conservazione dei log. Qualora nel corso delle operazioni di verifica e monitoraggio, il team di gestione rilevi anomalie nel funzionamento del servizio, sono attivate le analisi al fine di comprenderne cause e conseguenze nonché determinare le azioni da intraprendere. Gli eventi significativi che hanno impatto sul servizio sono notificati alla cosiddetta Service Control Room del Gestore dell'Identità Digitale.

Infine, avere diversi Identity Provider assicura che l'utente possa scegliere, che non ci sia una banca centralizzata delle identità, si evita che ci sia un singolo point of failure, e si garantisce al cittadino che venga sfruttata al massimo la tecnologia disponibile perché si incentiva lo sviluppo di un vero e proprio mercato.

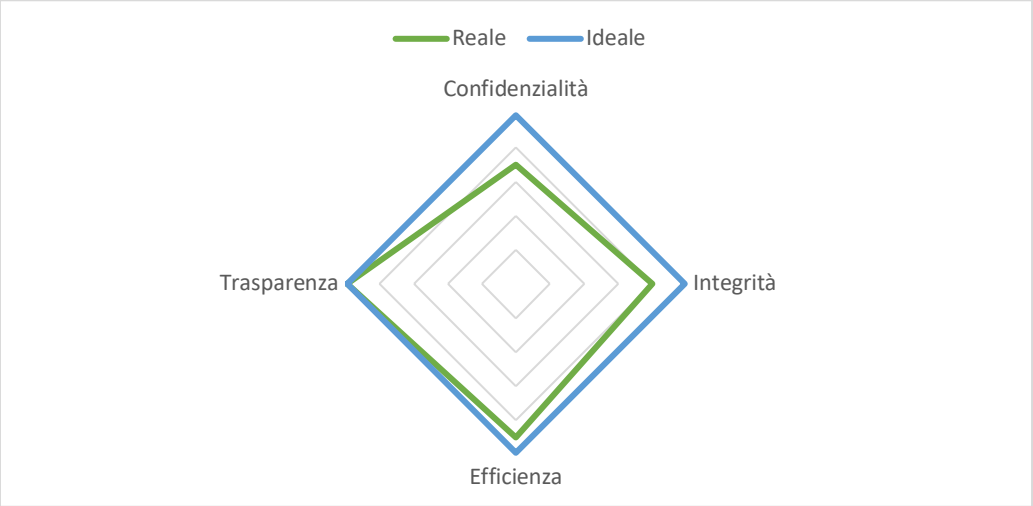
Recentemente Spid ha abbracciato lo standard OpenId Connect, che riesce a prevenire potenziali attacchi tramite l'intercettazione delle comunicazioni, soprattutto nel caso di applicazioni per dispositivi mobili. Inoltre, SPID OpenID Connect prevede l'uso delle sessioni lunghe revocabili, a parità di sicurezza, evitando continui inserimenti di password.

Attualmente, dunque una sola criticità che si può individuare riguardo a SPID è legata alla necessità, che probabilmente subentrerà qualora dovesse essere utilizzato anche in ambito bancario, di avere un meccanismo di autorizzazione della transazione stessa. Per cui potrebbe diventare importante la parte di firma dell'operazione e non solo il mero accesso a doppio fattore. Nella nostra specifica applicazione, il sistema SPID viene utilizzato per la sola autenticazione dell'utente, quindi tale criticità nel sistema di voto elettronico non sussiste in quanto l'autenticità della transazione viene accreditata attraverso meccanismi differenti.

Tool used

Tool used in WP2	**Follows from**	**Used for property**
La proprietà di Hiding del commitment	Proprietà del Random Oracle di SHA256 usato per istanziare il commitment	P.2, P.3
La proprietà di Binding del commitment	Proprietà del Random Oracle di SHA256 usato per istanziare il commitment	I.1
Non riconducibilità della transazione	Caratteristiche della ItalyChain, Tor	P.1
CCA-security di Enc	Assunzione su Enc	P.2, P.3
Unforgeability di Sig	Assunzione su Sig e caratteristiche della ItalyChain	l.1, A.1
Trasparenza delle operazioni su blockchain	Caratteristiche della ItalyChain	I.2, T, C
Determinismo dell'algoritmo di generazione di PK da SK per ciascuna votazione	Assunzione sull'algoritmo su elliptic curve	I.2
Scalabilità (blocco di grandezza finita, creazione di un blocco ogni 10s, etc…)	Caratteristiche della ItalyChain	D.1
Autenticazione degli attori in una transazione, integrità e confidenzialità del messaggio	TLS	A.1, I.1, P.2

Grafico Radar



Come possiamo vedere dal grafico radar soprastante, la peculiarità principale del nostro sistema è la trasparenza. Date le grandi perplessità dovute all'utilizzo di una piattaforma elettronica per il voto online, il nostro focus è stato quello di rendere il sistema il più trasparente possibile affinché tutti i detrattori di questa modalità (no-evox) potessero avere chiaro il funzionamento del sistema. Per rendere tale il nostro sistema, il nostro punto cardine è stato l'utilizzo della blockchain, grazie alle sue intrinseche proprietà come, appunto, la sicurezza, l'immutabilità e la trasparenza.
La scelta di una blockchain di tipo permissioned ci ha permesso di evitare l'ausilio di meccanismi di validazione delle transazioni di tipo PoW (Proof of Work), rendendo lo sforzo dei validatori minimo, tuttavia come possiamo vedere dal grafico, l'efficienza non è al massimo. Tale valore è dettato dal fatto che il sistema mette in gioco molti servizi diversi, come appunto il login con SPID e la comunicazione della transazione tramite rete Tor; si richiede inoltre di effettuare un secondo accesso per validare il proprio voto, oltre a dover aspettare la conferma di ogni transazione effettuata dall'utente. Di conseguenza il processo di voto risulta essere non troppo veloce.
Per quanto riguarda l'integrità il nostro sistema mantiene comunque intatte le proprietà individuate per questa classe. Gli attacchi che sono inevitabili sono quelli relativi alla coercizione e al furto delle credenziali. Ovviamente questa tipologia di attacchi risulta essere relativa al mondo fisico, il quale non può essere controllato dal nostro sistema. Le altre tipologie di attacco che possono minare l'integrità, e che non possono essere controllate dal sistema, sono quelle relativi all'influenzabilità del votante, ampiamente discusse in precedenza.
Dal punto di vista della confidenzialità del sistema, il valore risulta essere quello più basso del grafico radar; ciò è dettato dal fatto che ci sono varie criticità inevitabili che attaccano tale proprietà. Uno dei primi problemi riscontrati è la possibilità da parte della Società di poter divulgare i risultati della votazione (l'identità del votante resta intatta) una volta pubblicata la randomness da parte dei votanti. Questa problematica, tuttavia, risulta essere in parte scongiurata sia dal fatto che la giustizia è sempre vigile sull'andamento della votazione, sia perché ci sono interessi economici (collaterali).
La problematica relativa alla coercizione risulta sempre essere inevitabile anche dal punto di vista della confidenzialità. Una mitigazione alle minacce alla confidenzialità è stata introdotta attraverso l'impiego della rete Tor, che seppure non integralmente, come già discusso in precedenza, cerca di preservare la privacy dei dati che transitano per tale rete.

WP4

Tale WP ha lo scopo di di simulare la realizzazione del progetto descritto e analizzato nei precedenti WP : un sistema di e-vote basato su BlockChain.
Lo svolgimento di tale WP è coperto dai file riportanti nella cartella SicurezzaDef. Nello specifico gli attori previsti sono: un Validatore, quattro Votanti e la Societa, ciascuno rappresentato da uno specifico programma. Questi diversi programmi comunicano tra di loro mediante l'impiego di Socket, simulando in questo modo l'invio del voto correttamente cifrato e firmato e della annessa randomness, da parte dei votanti al validatore e l'invio della chiave privata della Societa al validatore.
L'intero progetto si inserisce in un contesto TLS.
Come simulazione della BlockChain il validatore farà riferimento a metodi contenuti all'interno della classe SmartContract, simulando l'aggiunta di blocchi attraverso la scrittura su un file di testo "ItalyChain.txt" (da eliminare prima di ogni esecuzione).
Le altre classi ovvero, Utils.java, Cryptare.java, SmartContract.java, MyKeyManager.java, AppendingObjectOutputStream.java e toVote.java contengono metodi funzionali allo svolgimento della simulazione di votazione.
L'autorizzazione a votare per ciascun votante, descritta nel documento come possesso di un NFT, è stato simulato attraverso la verifica dello Smart Contract del possesso di un certificato pre-generato da parte di ciascun votante, utilizzando KeyStore e TrustStore.
I due tool, Tor e SPID, di cui si è fatto utilizzo nella progettazione in WP2 e nell'analisi in WP3, non sono stati simulati all'interno di questo WP.