UNIVERSITAT POLITÈCNICA DE VALÈNCIA

etsinf

Escola Tècnica Superior d'Enginyeria Informàtica

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Un sistema de vot electrònic basat en la tecnologia blockchain

TREBALL FI DE GRAU

Grau en Enginyeria Informàtica

Autor: Cerdà i Cucó, Aleix

Tutor: López Rodríguez, Damián

Director experimental: Larriba Flor, Antonio Manuel

Curs 2019-2020

Resum

En els últims anys estem veient com l'estat democràtic, el més comú dels sistemes d'organització actuals, està canviant. Decisions que necessiten de la col·laboració entre diverses forces polítiques i el consens de gran part de la ciutadania pareix que indiquen que el nou paradigma ens portarà a alternatives on és requerirà la participació activa de la població en el procés democràtic.

Aquest canvi però, no serà possible si no actualitzem el mecanisme principal per a prendre decisions en grup de forma directa, la votació. Les últimes eleccions generals costaren prop de 140 milions d'euros, és necessita un sistema que faja de votar una tasca barata, còmoda (tant per a organitzadors com per a l'electorat) i accessible, sense oblidar la seguretat i els valors democràtics.

És per això, que presentem un sistema de votació electrònica enfocat en la confiança i la seguretat, que pretén convèncer tant aquelles persones amb grans coneixements criptogràfics i matemàtics com a aquelles que son noves en aquest camp, gràcies a la utilització de tècniques criptogràfiques i la involucració dels propis partits com a actors principals que posaran en joc la seua reputació en un sistema que els farà col·laborar, però que al mateix temps, els seus interessos antagònics els forçaran a comportar-se de forma honesta.

Paraules clau: e-voting, blockchain, vot electrònic, criptografia

Resumen

Durante estos últimos años hemos visto como el estado democrático, el más común de los sistemas de organización actual, está cambiando. Decisiones que necesitan la colaboración entre diversas fuerzas políticas y el consenso de gran parte de la ciudadania parece que indican que el cambio de paradigma nos llevará a alternativas en las que se requerirá la participación activa de toda la población en el proceso democrático.

Este cambio no será posible si no actualizamos el mecanismo principal para tomar decisiones en grupo de forma directa, la votación. Las ultimas elecciones generales costaron cerca de 140 millones de euros, se necesita un sistema que haga de votar un proceso barato, cómodo (tanto para la organización como para el electorado) y accesible, sin olvidar la seguridad y los valores democráticos.

Es por eso, que presentamos un sistema de votación electrónica enfocado en la confianza y en la seguridad, que pretende convencer tanto a las personas con grandes conocimientos criptográficos y matemáticos como a aquellas que son nuevas en el campo, gracias al uso de técnicas criptográficas i a la involucración de los propios partidos como actores pricipales que pondrán en juego su reputación en un sistema que les hará colaborar, pero que al mismo tiempo, sus intereses antagónicos les forzaran a comportarse de forma honesta.

Palabras clave: e-voting, blockchain, voto electrónico, criptografía

Abstract

In recent years we have seen how the democratic state - the most common of today's organizational systems - is changing. Decisions that need the colaboration of multiple political forces and the consensus of a great part of the citizenry seem to indicate that the new paradigm will lead us to alternatives where the active participation of the population in the democratic process will be required.

However, this change will not be possible if we do not upgrade the main mechanism for making group decisions, voting. The last general election costed us about 140 million euros. A new system is needed, one that makes voting a cheap, comfortable (both for organizers and for the electorate) and accessible, without forgetting security and the democratic values.

For this reason, we present an electronic voting system focused on trust and security which aims to convince both those with great cryptographic and mathematical knowledge and those who are new in this field, thanks to the use of cryptographic techniques and the involvement of the parties themselves as major actors that will jeopardize their reputation in a system that will make them collaborate and at the same time, their antagonistic interests will force them to behave honestly.

Key words: e-voting, blockchain, electronic vote, cryptography

Índex

Índex de figures

Índex d'algorismes

CAPÍTOL 1
Introducció

Diversos intents per establir un sistema de vot electrònic a distància s'han fet al llarg del temps. Podem parlar de les experiències en Estònia, Suïssa o els Estats Units amb eleccions a nivell estatal, també de partits polítics celebrant eleccions internes amb ferramentes d'aquest tipus, no obstant, cap d'aquestes experiències ha acabat amb l'adopció definitiva del sistema.

En aquest capítol es tractarà de fer una aproximació general al caràcter del treball, comparant la confiança que transmeten a la gent els sistemes de vot i els sistemes criptomonetaris, marcant així quina ha sigut la motivació i quins seran els objectius.

1.1 Motivació i objectius

Després de veure com durant anys les propostes de sistemes de vot electrònic no han aconseguit guanyar la confiança de la població, però les criptomonedes basades en blockchain han comptat amb un recolzament i una ràpida adopció entre un gran nombre de gent, no sols de persones especialitzades, es fa patent la necessitat de replantejar les estructures de dades i les autoritats que participen en un esquema de vot electrònic, intentant que les primeres siguen lo més obertes, transparents i públiques possible i que les segones tinguen molt complicat comportar-se de forma no honesta.

Moltes d'aquestes criptomonedes tenen una definició bàsica comú: són registres públics de transaccions, descentralitzats, distribuïts i immutables. Propietats molt desitjables per a un sistema de vot.

Plantegem així l'objectiu de treball, crear un sistema que busque guanyar la confiança tant de les persones que coneixen la criptografia com de les que no estan familiaritzades. Fent-nos valer de la tecnologia blockchain per aconseguir una votació i un recompte públic, així com de les ferramentes utilitzades Monero per mantenir la privacitat de les votants.

1.2 Estructura de la memòria

Aquesta memòria tractarà de fer un breu recorregut al context històric i tecnològic actual pel que fa a la criptografia i al vot electrònic amb la finalitat de posar en valor la nostra proposta. Així, el segon capítol te com objectiu donar el coneixement base necessari per a entendre el funcionament intern del sistema. En el tercer comentarem algunes propostes i treballs relacionats, utilitzant tant tecnologies diferents com similars. Pel que fa al quart, entrarem en detall en la nostra proposta comentant el seu funcionament, la seua posada a punt i les propietats que atorga al vot electrònic. Finalment, en la quinta part, tancarem la memòria amb les conclusions extretes d'aquest treball deixant idees per a futures línies de investigació.

CAPÍTOL 2
Coneixements previs

En aquest capítol intentarem proporcionar una serie de coneixements que seran referenciats per explicar la nostra proposta, així com quins recursos tecnològics hem utilitzat i perquè.

2.1 Notació

En aquesta secció proporcionaré una serie de termes per a facilitar la comprensió de la resta del treball.

- El producte i la exponenciació modular s'expressaran com $ab \pmod n$, i $c^d \pmod n$ respectivament.
- La concatenació de cadenes binàries s'expressarà com $a \| b$.
- Un grup finit definit per un número prim q es representarà com $\mathbb{F}_q$.
- H_s es una funció de resum (*hash*, [2]) que accepta com a entrada una cadena binària i retorna un element d'un grup finit, és a dir, $H_s(\{0,1\}^*) \rightarrow \mathbb{F}_q$.
- H_p es una funció de resum que accepta com a entrada un element d'un grup finit i retorna un punt d'una corba el·líptica, de forma que, $H_p(\mathbb{F}_q) \rightarrow E$.

2.2 Què és la criptografia?

En el sentit etimològic de la paraula, criptografia significa "escriure de forma oculta". Podríem dir doncs, que l'objectiu de la criptografia es el de modificar un missatge de forma reversible, ocultant així el missatge original però permetent a la destinatària desitjada recuperar-lo seguint un procediment prèviament acordat.

Al llarg de la història, depenent del context tecnològic, diferents tècniques han sigut utilitzades. Pot ser una de les més conegudes és el xifrat Caesar, que consisteix en substituir cada una de les lletres del missatge per la que fa 3 a la seua dreta en l'abecedari [3].

L'aparició dels ordinadors i la seua capacitat de comput va provocar un canvi de paradigma. Amb els xifrats utilitzats fins aleshores, un ordinador podia extraure el missatge original sense necessitat de saber el mètode per a desxifrar-lo, mitjançant força bruta. Va ser durant la segona guerra mundial, amb la màquina enigma, quan aquest canvi va quedar patent. Aquesta produïa missatges que les forces aliades sabien com analitzar, però que no tenien el temps per fer-ho. Així, en lloc de mesurar la seguretat del sistema segons la complexitat del sistema de xifrat, passarem a mesurar-la per la complexitat computacional, és a dir, segons el temps estimat que un ordinador tardaria en trobar el missatge original a partir del xifrat.

Mencionar que durant la primera guerra mundial s'utilitzà un sistema de xifrat amb seguretat incondicional, les *One Time Pad*, llibretes amb codis que permetien xifrar de forma que tots els missatges que compartien longitud amb el missatge xifrat tenen la mateixa probabilitat d'haver-lo generat, per tant la seua seguretat és incondicional, no hi ha cap mètode de força bruta que extraga el missatge original. El seu gran inconvenient és la necessitat de compartir la llibreta de forma física.

Els primers sistemes de xifrat estandarditzats per al seu ús en ordinador seguiren la idea d'aquells que els precediren, una sola clau que servia tant per a xifrar com per a desxifrar, *Clau simètrica*. Encara que molt ràpids i eficients, aquests sistemes tenen un gran inconvenient, necessiten que la clau que va a utilitzar-se siga compartida a través d'un canal segur. Assumint que tota comunicació no xifrada a través de Internet no és segura, aquest inconvenient representa un gran problema ja que amb comunicacions de banda a banda del planeta compartir la clau utilitzant un mitjà físic no és viable.

Són els sistemes de clau pública, que a continuació s'expliquen, els que permeten un intercanvi segur de missatges en canals no segurs, encara que són un poc més lents. Així, en l'actualitat, és comú utilitzar un esquema de clau pública per intercanviar una clau simètrica i establir així un canal de comunicació segur i d'alta velocitat.

Afegir que actualment el camp de la criptografia és molt ample i no es limita a comunicacions xifrades. Algunes de les propietats que permet afegir als missatges són:

- *Confidencialitat*: Ens ho permeten sistemes de xifrat com els descrits. És la capacitat d'enviar missatges i que el contingut sols puga ser revelat per la destinatària desitjada.

- *Integritat*: Cap agent extern no autoritzat pot modificar el contingut del missatge. Per tal d'aconseguir-ho utilitzem funcions de resum [2], entre altres solucions.

- *Autenticitat i no-repudiació*: Amb la utilització d'algorismes de firma aconseguim saber que el missatge ve d'una font reconeguda i que eixa font no podrà negar la firma.

2.3 Criptografia de clau pública

Introduïts en 1975 per Whitfield Diffie i Martin Hellman en el seu treball [4], són sistemes que utilitzen una clau per a xifrar i una altra diferent per a desxifrar, és per això que també són coneguts com a sistemes de clau asimètrica.

El concepte és molt senzill:

- M i Y representen tots els missatges i xifrats possibles, respectivament.
- X i D són dos funcions tal que X accepta com a entrada un missatge i retorna un xifrat ($X : M \rightarrow Y$); i D accepta com a entrada un xifrat i retorna un missatge ($D : Y \rightarrow M$).
- X i D són inverses, és a dir, $X(D(y)) = y$ i $D(X(m)) = m$, per a tot $m \in M$ i $y \in Y$.
- Tant X com D sols tenen una inversa, és a dir, sols existeix una D que permeta recuperar els missatges xifrats amb X i sols existeix una X que produïsca xifrats desxifrables amb D.
- Una parella (X, D) és computacionalment senzilla de calcular.
- Donada X, trobar la D corresponent no és possible o és un procés computacionalment car.

A nivell pràctic les funcions per a xifrar i desxifrar, X i D, són conegudes per tot el món, estandarditzades i catalogades com a sistema, i allò que es genera són sols uns paràmetres per a completar-les. D'aquesta manera, el paràmetre que completa la funció de xifrat X, i que per tant es pot distribuir, l'anomenarem clau pública K_{pb}, i el paràmetre que completa la funció de desxifrat D, i que es manté secret, l'anomenarem clau privada K_{pr}.

Així, podem generar un parell de claus (K_{pb}, K_{pr}), i publicant K_{pb}, aconseguir que qualsevol persona puga xifrar missatges que sols nosaltres podrem desxifrar.

El sistema proposat per Ralph Merkle i Martin Hellman en [5] utilitzant el problema de la motxilla discreta il·lustra perfectament la idea i és de lectura recomanada.

2.3.1. RSA

RSA va ser proposat per Rivest, Shamir i Adleman en [6] l'any 1978. Tot i tenir més de 40 anys continua sent el sistema de referència hui en dia sent el més utilitzat en l'actualitat [7] tant per a xicotetes aplicacions com per a sistemes amb més recorregut com el *DNIe* [8].

A continuació es presenten els algorismes de generació de claus, Algorisme 2.1, xifratge, Algorisme 2.2, i des-xifratge, Algorisme 2.3.

Algorisme 2.1 Generació de claus RSA

1: S'escullen p i q, dos números naturals, prims i diferents
2: $n \leftarrow p \cdot q$
3: $\phi \leftarrow (p-1)(q-1)$
4: S'escolleix a l'atzar un número e tal que $1 < e < \phi$ i $mcd(e, \phi) = 1$
5: Es calcula d de forma que $1 < d < \phi$ i $mcd(e, d) = 1 (\mathrm{mod}\, \phi)$
6: $K_{pb} \leftarrow (n, e)$
7: $K_{pr} \leftarrow (d)$
8: **return** (K_{pb}, K_{pr})

Algorisme 2.2 Xifrat RSA

Require: K_{pb}, és a dir, els components de la clau pública: n, e
Require: m, el missatge a xifrar, un número s'encer $(\mathrm{mod}\, n)$
1: $y \leftarrow m^e (\mathrm{mod}\, n)$
2: **return** y

Algorisme 2.3 Desxifrat RSA

Require: K_{pr}, o siga, la clau privada: d
Require: y, el missatge a desxifrar
1: $m \leftarrow y^d (\mathrm{mod}\, n)$
2: **return** m

La seua seguretat està lligada a la dificultat de calcular els factors prims d'un número semiprim i gran, és a dir, un número producte de dos prims grans. El número semiprim en aquest cas és n, i els números que tractem de mantenir secrets són p i q, ja que coneixent aquests el calcul de la clau privada d és trivial.

És important destacar que tot i no existir un mètode general de factorització lo suficientment eficient com per a que l'amenaça d'un atac de força bruta siga real, sí que existeixen algorismes que en certes instancies del problema funcionen bé. És per això que la generació de p i q ha d'estar sotmesa a tests per a evitar que n siga vulnerable [9][10].

2.3.2. Corbes el·líptiques

Les corbes el·líptiques són corbes planes definides pel polinomi 2.1 i que a més no són singulars, és a dir, són corbes continues. Aquesta segona propietat s'assegura complint amb la inequació 2.2 Podem veure exemples de corbes vàlides en la figura 2.1 i de corbes amb punts singulars en la figura 2.2.

$$y^2 = x^3 + ax + b \tag{2.1}$$

$$4a^3 + 27b^2 \neq 0 \tag{2.2}$$

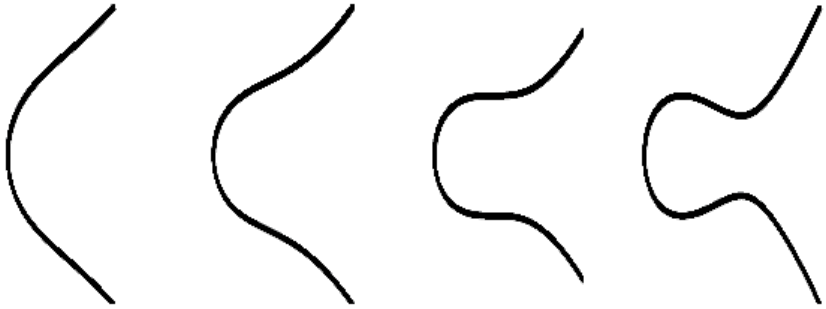

Figura 2.1: Representació gràfica de corbes el·líptiques vàlides.

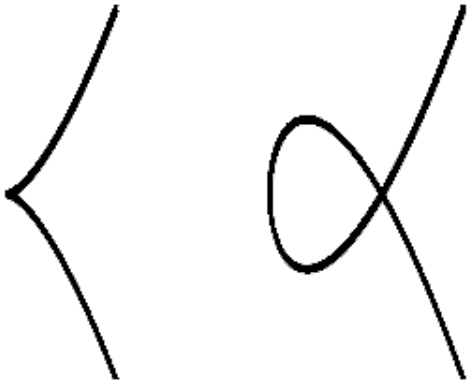

Figura 2.2: Representació gràfica de corbes el·líptiques amb singularitats.

Va ser H. W. Lenstra la primera persona en utilitzar les corbes el·líptiques en la criptografia en [11], encara que no va ser fins el 1985 quan N. Koblitz i V. Miller van proposar de forma independent en [12] i [13], respectivament, un sistema criptogràfic inspirats en el treball de Lenstra.

Aquest sistema proposa un esquema de clau pública on la seguretat depen del problema del logaritme discret. Per tal de plantejar el sistema, es defineix un grup $\mathbb{G}$ tal que:

- Els elements del grup són punts d'una corba el·líptica.
- L'element identitat és el punt en l'infinit, 0, afegit artificialment per la necessitat de tindre un punt neutre.
- El invers d'un punt P és el punt $-P$, el simètric respecte l'eix x.
- L'operació de suma es definida de forma que donats tres punts alineats (P, Q, R) diferents de zero es compleix que $P + Q + R = 0$, per tant, $P + Q = -R$. Vist gràficament en la figura 2.3.

D'aquesta manera, l'operació definida com a suma, compleix les característiques necessàries per definir un grup abelià:

- Clausura: Si a i b són membres de $\mathbb{G}$, $a + b$ és membre de $\mathbb{G}$.
- Associativa: $(a + b) + c = a + (b + c)$.

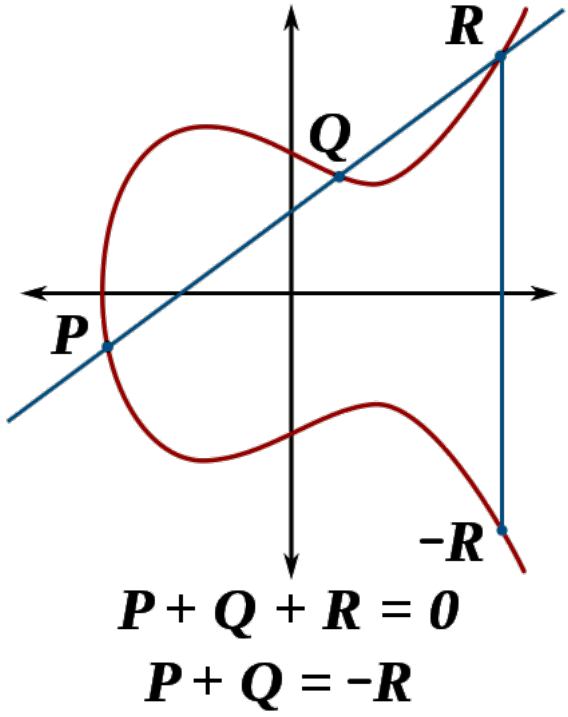

Figura 2.3: Representació gràfica de l'operació suma tal com s'ha definit per al grup.

- Commutativa: $a + b = b + a$.
- Existeix un element identitat 0 tal que $a + 0 = 0 + a = a$.
- Per a tot punt a, existeix un punt b tal que $a + b = 0$.

Així podem definir la multiplicació escalar com $nP = P + P + \ldots + P$, és a dir, afegir P n vegades.

Existeixen algorismes per completar la multiplicació escalar de forma molt eficient $(\mathcal{O}(\log n))$ [14], així, donat un punt P i un número n trobar Q tal que $nP = Q$ és una tasca senzilla. Donat P i Q trobar n és més complicat, i és el problema del logaritme[1], no obstant, existeixen patrons que ens permetrien trobar un algorisme eficient. Per tal d'evitar-ho necessitem reduir el domini de la corba.

Escollim un número prim p de forma que podem reduir el domini de la corba sobre $\mathbb{F}_p$. D'aquesta manera, el polinomi i la inequació que defineixen la corba (2.1, 2.2) es modifiquen resultant en el polinomi 2.3 i la inequació 2.4.

$$y^2 \equiv x^3 + ax + b (\mathrm{mod}\, p) \tag{2.3}$$

$$4a^3 + 27b^2 \not\equiv 0 (\mathrm{mod}\, p) \tag{2.4}$$

Finalment calcularem un punt base G que actuarà com a generador d'un subgrup de la corba. És a dir aquest nou subgrup és el conjunt de punts que obtenim

[1] Encara que siga una divisió l'operació que s'intenta resoldre, $Q : P = n$, se li diu problema del logaritme i no problema de la divisió per coherència amb altres sistemes criptogràfics.

al multiplicar G pels números fins a n tal que $(n+1)G(\mathrm{mod}\, p) = G$ i sobre el que funciona el sistema criptogràfic, sent el producte d'un escalar pel punt generador la clau pública i l'escalar la clau privada. En aquest sistema les claus privades les expressarem en lletres minúscules, a, i les claus privades en majúscules, A, de forma que $A = aG$.

Com hem vist la seguretat del sistema està molt lligada als paràmetres utilitzats, és per això que existeix una llista amb corbes i paràmetres considerats segurs [15].

Per al problema del logaritme discret en grups finits sobre corbes el·líptiques no existeix cap algorisme que millore temporalment el rendiment exponencial. És per això que els sistemes basats en corbes el·líptiques permeten utilitzar claus en grups més petits que sistemes com el RSA mentre mantenen una seguretat comparable [16].

2.4 Firmes en anell

Les firmes en anell són un tipus d'algorisme de firma que permet aplicar la propietat d'*autenticitat*, explicada en la Secció 2.2, a grups en lloc de a elements individuals. Així, ens permeten saber que un missatge firmat amb un anell de claus ha estat enviat per una persona que te almenys una clau privada lligada a una de les claus públiques de l'anell, però sense desvetlar quina és la clau en qüestió.

El primer sistema d'aquest tipus va ser introduït per Chaum en [17]. Aquesta primera aproximació però, necessita que algun element de forma activa actue com a coordinador de grup, limitant l'ús d'aquest.

Més tard, l'any , Rivest va proposar en [18] un esquema que elimina la figura de coordinadora de grup, permetent que la firmant puga utilitzar tantes claus públiques com desitge sense cap tipus de consentiment, o inclús coneixement, de les propietàries de la resta de claus, donant-li ambigüitat completa entre totes les claus utilitzades.

En el nostre cas, utilitzarem la versió de la firma en anell proposada en [19], [20], que introdueix la *KeyImage*, una espècie de rebut de la firma derivat del parell de claus pública-privada utilitzats per a signar seguint l'operació 2.5. D'aquesta manera, si guardem les *KeyImage* de cada vot vàlid rebut, podem saber si la clau privada utilitzada ja havia signat algun altre anell i per tant, si s'està votant per segona vegada.

$$KeyImage = aH_p(A) \tag{2.5}$$

Els algorismes a utilitzar per a generar la firma i per a validar aquesta són els algorismes 2.4 i 2.5, respectivament.

Algorisme 2.4 Firma en anell

Require: $N \leftarrow$ Número de claus públiques que utilitzarem per signar.
Require: $P = \{P_1, P_2, \ldots, P_N\} \leftarrow$ Llista de claus públiques que formaran l'anell.
Require: $s \leftarrow$ Index de la clau pública de la signant en la llista P.
Require: $x \leftarrow$ Clau privada associada a la clau pública de la signant (P_s).
Require: $m \leftarrow$ Missatge a firmar.
1: $r \leftarrow$ Llista de números aleatoris sense valor en la posició s.
2: $\alpha \leftarrow$ Número aleatori.
3: $L, R, c \leftarrow$ Llistes buides.
4: $K \leftarrow xH_p(P_s)$ //*KeyImage*. Destacar que $H_p(P_s)$ és un punt de la corba.
5: $L_s \leftarrow \alpha G$
6: $R_s \leftarrow \alpha H_p(P_s)$
7: $c_{(s+1)(\bmod N)} \leftarrow H_s(m, L_s, R_s)$
8: $i \leftarrow (s+1)(\bmod N)$
9: **while** $i \neq s$ **do**
10: $L_i \leftarrow r_i G + c_i P_i$
11: $R_i \leftarrow r_i H_p(P_i) + c_i K$
12: $c_{(i+1)(\bmod N)} \leftarrow H_s(m, L_i, R_i)$
13: $i \leftarrow (i+1)(\bmod N)$
14: **end while**
15: $r_s \leftarrow \alpha - c_s x(\bmod N)$
16: **return** (P, K, c_0, r)

2.5 Blockchain

Introduïda l'any 2009, en [21], pel compte anònim Satoshi Nakamoto, una blockchain és una estructura de dades distribuïda i descentralitzada que, utilitzant diferents tècniques criptogràfiques per a establir una política d'escriptura, busca oferir immutabilitat. Com el nom indica, aquesta estructura de dades està basada en blocs que queden lligats en ordre cronològic, de forma que tot bloc nou conté una referència a l'anterior.

En aquest treball la blockchain s'introduia com a ferramenta per aconseguir crear una moneda de codi lliure que no depenguera de cap banc ni estat, el Bitcoin.

La blockchain, com tots el sistemes distribuïts, es veu afectada pel teorema del CAP [22], cap sistema distribuït pot oferir al mateix temps una forta consistència (*C*) entre tots els nodes, donar servei en tot moment (*Availability, A*), i resistència a particions en la xarxa (*Partition tolerance, P*). Tant donar servei en tot moment com ser resistents a particions són propietats binaries per tant la propietat que normalment veu reduïda la seua prioritat és la de consistència. Allò que aportarà consistència en el cas de les blockchain és el mateix que atorga immutabilitat, el protocol de consens. Aquest protocol que és executat per tots els nodes que desitgen mantenir la blockchain tracta de dictar quins blocs són vàlids i per tant afegits a la cadena. El protocol de consens introduït en aquesta mateixa proposta de Nakamoto s'anomena *Proof of work*, prova de treball, i estableix que per a que un bloc siga vàlid el seu hash ha de començar amb un número de zeros determi-

Algorisme 2.5 Validació firma en anell

Require: $N \leftarrow$ Número de claus públiques que formen l'anell.
Require: $\{P_1, P_2, \ldots, P_N\} \leftarrow$ Llista de claus públiques que formen l'anell.
Require: $K \leftarrow$ *KeyImage* associada a la firma.
Require: $c_0 \leftarrow$ Primer valor de la llista c.
Require: $\{r_1, r_2, \ldots, r_N\} \leftarrow$ Llista de números aleatoris utilitzats per signar.
Require: $ListK \leftarrow$ Llista de totes les *KeyImage* utilitzades en firmes vàlides.
Require: $m \leftarrow$ Missatge signat.
if K in $ListK$ **then**
  return *False*
end if
$L', R', c' \leftarrow$ Llistes buides.
$L'_0 \leftarrow r_0 G + c_0 P_0$
$R'_0 \leftarrow r_0 H_p(P_0) + c_0$
$c'_1 \leftarrow H_s(m, L'_0, R'_0)$
while $i < N$ **do**
  $L'_i \leftarrow r_i G + c'_i P_i$
  $R'_i \leftarrow r_i H_p(P_i) + c'_i$
  $c'_{(i+1) \pmod N} \leftarrow H_s(m, L'_i, R'_i)$
  $i \leftarrow (i+1) \pmod N$
end while
if $c'_0 == c_0$ **then**
  return *True*
else
  return *False*
end if

nat. Així, es reserva un camp per a provar valors que modifiquen el contingut del bloc i per tant el hash resultant. D'aquesta manera, si s'intentara modificar un bloc passat, per tal que s'accepte la cadena resultant, es tindria que re-calcular un hash vàlid per al bloc en concret i per a tots els blocs posteriors, tasca no abordable amb mitjans raonables.

La seua capacitat de mantenir un registre públic de transaccions de forma segura, immutable, descentralitzada i distribuïda ha fet que siga rellevant en molts altres camps, no sols el monetari per al que estava pensat en un principi. S'ha vist aplicada en educació, sanitat, alimentació, entre molts altres [23].

2.6 Claus públiques d'un sol ús i Monero

De forma similar a Bitcoin, Monero és una criptomoneda que funciona amb la tecnologia blockchain. Està basada en el treball de Nicolas Van Saberhagen en [19] i te un fort focus en la privacitat de les usuàries. Intenta que tota transacció, tot i aparèixer en el registre públic que és la blockchain, siga privada i oculte la identitat tant de qui la realitza com qui la rep així com la quantitat traspassada.

Una de les ferramentes clau per aconseguir tan alt nivell de privacitat són les claus públiques d'un sol ús (*OTPKs*). Aquestes es deriven d'un parell de claus públiques (A, B) i, per evitar que la *OTPK* de (A, B) siga sempre igual, un nombre aleatori r:

$$OTPK = H_s(rA)G + B \tag{2.6}$$

Així la propietària de les respectives claus privades (a, b) pot recuperar la clau privada x d'aquesta nova *OTPK* amb un procés similar al intercanvi Diffie-Hellman [4][2]:

$$x = H_s(aR) + b \tag{2.7}$$

Monero utilitza les firmes en anell per donar ambigüitat a la emissora de la transacció, les *OTPKs* per ocultar qui la rep i lligar les monedes transferides a ella i finalment la *KeyImage* per evitar que els fons lligats a una determinada *OTPK* siguen utilitzats dos vegades, ja que encara que aquesta clau s'utilitze en diferents anells, la *KeyImage* seguira sent la mateixa.

[2]Destacar que R, siguent rG, s'afegeix a la transacció i és un parametre públic que no aporta cap informació de identitat al ser derivat d'un número aleatori.

CAPÍTOL 3
Treball relacionat

El problema del vot electrònic ha estat present durant molt de temps, molta gent ha intentat trobar solució però fins ara cap ha aconseguit acontentar tant a l'administració com a les votants. En aquesta secció tractarem de donar context tecnològic a la nostra proposta.

3.1 Sistemes de vot electrònic

Fora del paradigma de les blockchain i les firmes en anell podem trobar propostes majoritariament basades en aquestes primitives criptogràfiques que a continuació seran explicades, mixnets [24], proves de coneixement zero [25] i *blind-signatures* [26].

Les mixnet són xarxes formades per uns nodes proxy anomenats *mixnodes* que tenen l'objectiu de generar comunicacions difícils de seguir i traçar. La idea és que cada node te un parell de claus d'un sistema de clau pública. La usuària agafa les claus públiques dels nodes i utilitzant aquestes encripta i re-encripta el missatge múltiples vegades creant una espècie de Matryoshka o nineta russa. D'aquesta manera el missatge queda ocult baix una serie de capes d'encriptació que han de ser resoltes en un ordre determinat, és per això que a cada capa se li afegeix una referència al següent node. A més, aquests nodes també mesclen els missatges per enviar-los al següent node en un ordre aleatori.

D'altra banda, l'objectiu de les proves de coneixement zero és el de definir un mecanisme amb el que es pot demostrar coneixement d'un valor x sense donar més informació respecte al valor, més enllà de que el coneixes. Tenint en compte una entitat V verificadora i una entitat P que vol provar que coneix un valor x, aquestos sistemes compleixen tres propietats:

- Complet: Si P coneix x i V segueix el protocol, V quedarà convençuda de que P coneix x.
- Solid: Si P no coneix x, la probabilitat d'enganyar a V, si aquesta es comporta de forma honesta, és molt baixa.
- Coneixement zero: Si P te coneixement de x, V, comportant-se de forma honesta o deshonesta, no pot aconseguirà més informació de x que el fet de

que P el coneix. V, seguint el protocol, pot comprovar si P te coneixement de x sense cap interacció amb P.

Pel que fa a les *blind-signatures*, es tracta d'un tipus de firma en la que el missatge es firma en un estat ocult, però que pot validar el contingut original sense ocultar. Normalment és utilitzada per aconseguir que una entitat identificadora signe el missatge ocult quan es presenta juntament a una identitat vàlida per després enviar-lo sense ocultar però amb la firma de la entitat sense la identitat anteriorment validada. Així, s'aconsegueix demostrar que la emissora del missatge te una identitat vàlida sense lligar la identitat al missatge, sols mostrant la firma que s'ha obtingut al mostrar la identitat de forma privada.

Havent fet aquest repàs a les tecnologies, passem a la proposta de Michael J. Radwin en [27] que està basada en proves de coneixement zero i en *blind-signatures*. Aquest esquema necessita una sola autoritat i està compost de quatre fases (inicialització, registre, votació i recompte). Per votar, cada una de les votants crea una autorització amb l'ajuda de l'autoritat i és eixa una de les debilitats senyalades al mateix paper, i és que l'autoritat pot aprofitar les abstencions per a fabricar vots.

També podem comentar el treball de Ohkubo et. al. en [28] on, de forma similar a l'anterior, les votants necessiten l'ajuda de l'entitat administradora per aconseguir l'autorització de vot. En aquest esquema s'utilitza un esquema de mixnets per tal d'anonimitzar les votants. Per tant el número d'entitats que participen augmenta fins a tres, necessitant l'entitat administradora, un grup de *mixnodes* i un grup per realitzar el recompte.

3.2 Sistemes de vot amb blockchain

Com hem comentat abans, Secció 2.5, la capacitat de la blockchain de proporcionar un registre de públic accés immutable dona peu a pensar sistemes de vot centrats en ella. D'aquesta manera farem un breu resum d'algunes propostes de sistemes de vot que utilitzen la blockchain.

En [29], Lee proposa un sistema de vot molt senzill en el que cada opció de vot te una adreça pública associada, les votants s'identifiquen com a votant vàlida i realitzen una transacció a l'adreça de l'opció per la que volen votar. Per tal d'evitar que se sàpiga qui ha votat que, el procés de identificació és dut a cap per dos entitats diferents, l'organització de la votació en sí i una organització externa que s'assumeix honesta. És aquesta organització externa la que atorga permís a les votants vàlides per escriure en la blockchain.

Noizat introdueix en [30] un sistema basat en blockchain i Merkle trees [31]. Aquest sistema atorga privacitat mitjançant l'esquema de multi-firma 2-de-3 [32], d'aquesta manera cada votant utilitza tres claus públiques, la de l'aplicació de vot, la de l'organització de la votació i la de l'opció de vot desitjada.

Una alternativa basada en Zcash [33] proposada per Tarasov i Tewari en [34]. Zcash es tracta d'una bifurcació intencional de la cadena de Bitcoin centrada en la privacitat de les transaccions. En aquest protocol dos tipus de transaccions estan permeses, transaccions de tipus t que funcionen de la mateixa manera que

les transaccions en la cadena original de Bitcoin, i transaccions de tipus z que són privades. Cada opció està lligada a un parell de claus que permeten fer transaccions de tipus z i t, d'aquesta manera per votar a una opció li envies una transacció z a l'opció desitjada amb una moneda, i una vegada acabada la votació s'envia des de l'adreça t a l'organització totes les monedes rebudes. L'opció que més monedes envie guanya la votació. Destacar que existeix el perill que una opció fraudulenta no retorne les monedes en acabar la votació ja que aquestes monedes tenen valor monetari.

3.3 Sistemes de vot amb firmes en anell

De igual forma que la blockchain, les firmes en anell, explicades en la Secció 2.4, són un sistema que per les seues característiques intrínseques aporten propietats desitjables a un esquema de vot, com l'anonimitat de grup, vols demostrar que estàs dins del grup de persones autoritzades a votar (cens) sense donar a coneixer quina eres en concret.

Tant Salazar et. al. en [35] com Chen et. al. en [36] proposen sistemes basats en aquests tipus de firmes.

El treball de Salazar et. al. utilitza una variant de la firma en anell [37] en la que cada signatura produeix un codi únic que, de forma similar a la *KeyImage*, sense fer dèbil l'ambigüitat atorgada pel sistema de firma permet evitar el doble vot. Cal mencionar que en aquesta proposta el recompte corre a cap d'una sola entitat. Que aquesta entitat tinga el control complet sobre el recompte és un punt dèbil i podria donar lloc a problemes de corrupció, aquesta entitat per si mateixa seria capaç de proporcionar un recompte simultani a la votació donant una gran avantatge a qualsevol persona interessada coneixedora.

D'altra banda, la proposta de Chen et. al. està centrada en aconseguir un sistema sense cap tipus de rebut comprovant de vot per evitar qualsevol intent de compra-venda de vots. Amb aquesta meta en ment, modifica la firma en anell de forma que sols l'entitat designada per la votant és capaç de comprovar la validesa de la signatura i que a més siga capaç de generar proves falses per poder convèncer a un element coercitiu. No obstant, aquesta modificació fa necessària una confiança completa amb les entitats que s'encarreguen del recompte ja que es necessita de la seues claus privades per verificar les signatures.

3.4 Sistemes de vot amb blockchain i firmes en anell

En [38], Wei et al. introdueixen un sistema de vot basat en la blockchain de Ethereum i els seus contractes intel·ligents (*smart contracts*) [39]. També basant-se en el sistema d'anonimització de Monero 2.6 utilitza la mateixa variant de firmes en anell per ocultar la identitat de la votant i al mateix temps evitar el doble vot. Aquesta proposta utilitza la capacitat de demostrar que una $OTPK$ ha sigut generada a partir d'un parell de claus públiques per fer el recompte, així, una transacció a la $OTPK$ derivada del parell de claus públiques d'una de les opcions constitueix un vot. Per tal d'evitar que siga possible un recompte simultani

a la votació es necessita una entitat que guarde la clau privada d'una de les parts públiques associada a cada opció, aquesta entitat deixa un deposit en forma de Ethereum que sols podrà recuperar si una vegada acabat el recompte fa públiques les claus privades que ha estat guardant, per tal de fer possible el recompte.

Wu et. al. proposen en el seu treball [40] un esquema de vot basat en les firmes en anell i la blockchain de Bitcoin. Aquesta proposta busca aprofitar la immutabilitat que ofereix Bitcoin com a garantia de seguretat. No obstant, són necessàries dos entitats per deslligar el procés d'identificació i el de vot, i per a que el sistema funcione cal confiar plenament en la honestedat d'aquestes dos entitats que seran l'autoritat de registre (*AR*) i l'autoritat d'elecció (*AE*). El paper de la AR será el de generar una reserva de claus per a la blockchain i donar-los liquiditat per poder realitzar transaccions. D'altra banda l'AE s'encarrgarà del recompte, publicarà la seua adreça de Bitcoin per rebre transaccions que tindran com a concepte el vot amb la firma en anell. Així, qualsevol persona cridada a votar acreditarà la seua identitat a l'AR que li proporcionarà una clau privada i la corresponent clau pública. Amb aquestes publicarà la firma en anell que l'AE verificarà. Com hem comentat abans, aquest sistema deixa molt de poder en les mans de l'AR i l'AE i te com a requisit que aquestes siguen honestes.

CAPÍTOL 4
La nostra proposta

Entenem que a les votacions es genera informació molt delicada, que ha de ser correctament anonimitzada i correctament tractada, que en cas d'aquesta aplegar a ser aconseguida de forma maliciosa podria afectar de forma personal a les persones involucrades. Per aquest motiu les usuàries no utilitzarien cap sistema en el que no confiaren plenament, i és molt complicat per a persones no familiaritzades amb la criptografia confiar en sistemes completament basats en les matemàtiques.

Per tal d'aconseguir aquesta confiança, la nostra proposta involucra de forma activa components que les persones reconeixeran de les votacions en paper, els partits. Lligarem doncs la tasca de recomptar i validar vots, que tradicionalment realitzen les apoderades dels partits en cada taula de votació, amb els partits com a entitat que recomptaran i validaran amb un procés públic tots els vots enviats a la blockchain.

D'aquesta manera, en el cas que un partit actue de forma fraudulenta, tota persona que observe la votació podrà senyalar al culpable i la seua reputació serà greument afectada. A més, els partits tenen interessos antagònics i l'equilibri de Nash [41][42] els porta a que no hi ha millor estratègia que comportar-se de forma honesta.

Aquest capítol el dediquem a explicar de forma detallada el funcionament d'aquest sistema de vot, les seues característiques i propietats.

4.1 Funcionament

4.1.1. Preparació

Abans de començar la votació, els paràmetres de la clau RSA (2.3.1) per encriptar els vots han de ser generats amb la col·laboració de tots els partits.

Que un sol partit o una sola entitat tinguera el poder de desxifrar els vots i portar un recompte en temps real aniria en contra de una de les característiques desitjables dels sistemes de vot electrònics, i és que saber com va la votació abans de que esta acabe pot modificar el resultat de la mateixa.

Per tal d'evitar tindre aquest problema utilitzarem el protocol proposat per Damgård et al. [44], basat en el treball de Frankel et al. [43] que permet la eli-

minació d'una tercera part que actue com a intermediari honest. Aquest protocol ens permet generar els paràmetres públics de RSA mentre la clau privada es comparteix entre l parts, sent necessari un grup de, mínim, k parts per a recuperar la clau privada s.

Per a generar els paràmetres públics de la clau RSA normalment s'escullen de forma privada p i q, dos números grans i prims, que es multiplicaran per obtenir el mòdul que forma part de la clau pública. En aquest cas, per distribuir la clau privada, p i q, seran computats com la suma de les diferents parts escollides pels partits ($n = (p_1 + p_2 + \ldots + p_i + \ldots + p_l)(q_1 + q_2 + \ldots + q_i + \ldots + q_l)$). És obligatori que els partits publiquen una transacció [47] durant el procés per evitar que de forma maliciosa canvien la seua part. Per realitzar aquest procés correctament utilitzarem una variant [45] del treball de Shamir en [46]. En acabar el protocol cada partit tindrà s_i, una part de la clau privada. Podem veure una representació de l'aportació de cada partit en la figura 4.1.

Una vegada acordat el valor de n, els partits calculen de forma similar el valor de v, encara que en aquest cas necessitaran fer proves de primalitat sobre aquest nombre.

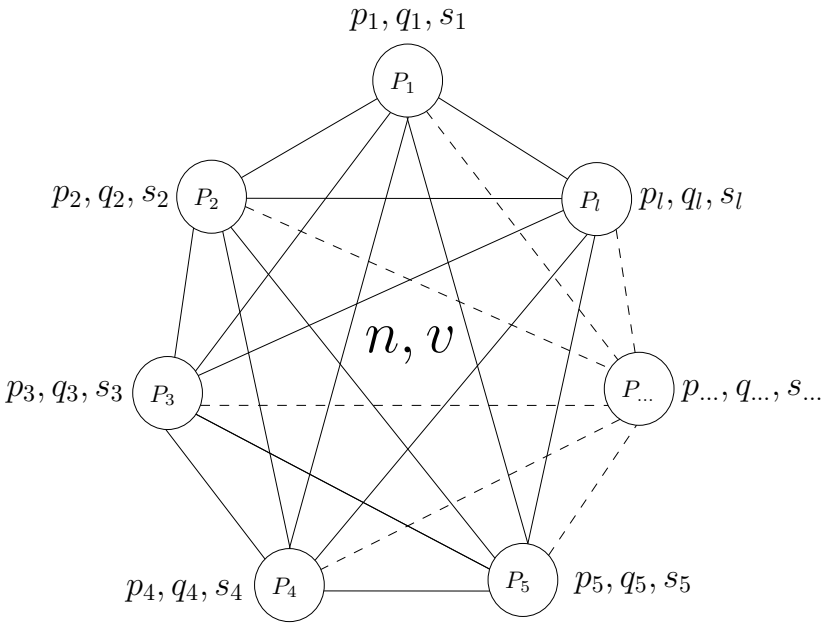

Figura 4.1: La generació dels paràmetres per al xifrat RSA se fa de forma conjunta entre tots els partits. Així, n i v es deriven de les parts de tots els partits p_i i q_i, de forma que cada partit tindrà una part s_i de la clau privada s.

A més, cada partit te la seua pròpia clau pública i privada per a signar els blocs que publicarà a la blockchain. Durant el proces de generació dels paràmetres per al xifrat RSA, és necessari que totes les comunicacións entre les parts siguen públiques i apareguen a la blockchain publicats pel partit que les ha realitzat. Finalment, la part pública de la clau RSA (n, v) serà publicada pels partits a la blockchain.

4.1.2. Registre

Per a qualsevol votació, l'administració central que l'organitza serà l'encarregada de guardar les claus públiques de les votants, així com de generar a partir d'elles les claus publiques d'un sol ús ($OTPK$, Secció 2.6). És per això que necessita tindre el parell de claus públiques de totes les participants abans de que comence aquesta. Per tal d'aconseguir-ho, l'administració fa públic el cens de persones cridades a votar, aquestes que desitgen participar i no hagen aportat mai les seues claus públiques o vulguen canviar aquestes, generaran dos parells de claus de corba el·líptica (A, a) i (B, b) i es registraran donant el seu parell de claus públiques juntament a una mesura de identificació personal a especificar per l'organització de la votació. Hi han moltes opcions, que van d'anar en persona amb un document de identificació reconegut a l'ajuntament, fins al correu electrònic, passant per número de telèfon, estar registrat a una pàgina web determinada, etc. Depèn de les necessitats de cada votació.

Una vegada acaba el temps donat per a registrar les claus públiques, l'administració procedeix a calcular les $OTPK$ per a tots els parells de claus públiques registrats, i acabat el càlcul publicarà a la blockchain la llista de claus generades, cadascuna amb la seua R associada, tal que $OTPK = H_s(rA)G + B$ i $R = rG$ on r és un nombre aleatori, de forma que qualsevol participant pot recuperar la clau privada de la $OTPK$ derivada a partir de les seues claus públiques resolvent $H_s(aR) + b$ (Secció 2.6). Per tal d'estalviar el temps computacional que empraria cada votant calculant quina es la seua $OTPK$, a més, la pròpia administració pot enviar directament quina $OTPK$ li correspon, o dividir la llista en llistes més petites amb criteris coneguts, com primera lletra del cognom, i/o per zones territorials.

També cal enviar a la blockchain una transacció amb els paràmetres de configuració restants de la votació, com per exemple les opcions a votar.

En la figura 4.2 es troba una il·lustració del procés.

4.1.3. Enviament del vot

En un a votació típica, quan es vota es vol assegurar que aquella entitat que ha votat forma part del cens i que no ha votat prèviament, que ninguna tercera part podrà relacionar de forma no ambigua el sentit del vot i qui l'ha emès, i que els vots es mantindran secrets fins que acabe el període de votació i comence el recompte.

Per tal d'assegurar aquestes condicions, el proces de vot és el següent:

Primer, la persona que vol votar seleccionarà una de les opcions disponibles per a dirigir el vot, a aquesta opció li concatenarà cadena aleatòria que anomenarem mascara per a evitar que tots els vots que van dirigits a la mateixa opció, una vegada encriptats, tinguen la mateixa forma. Una vegada emmascarada l'opció de vot, per completar l'ofuscació d'aquest, serà encriptat amb els paràmetres RSA publicats a la blockchain, aquests són la potència i el mòdul a aplicar (v i n):

$$evote = (vot||mascara)^v (\mathrm{mod}\, n) \tag{4.1}$$

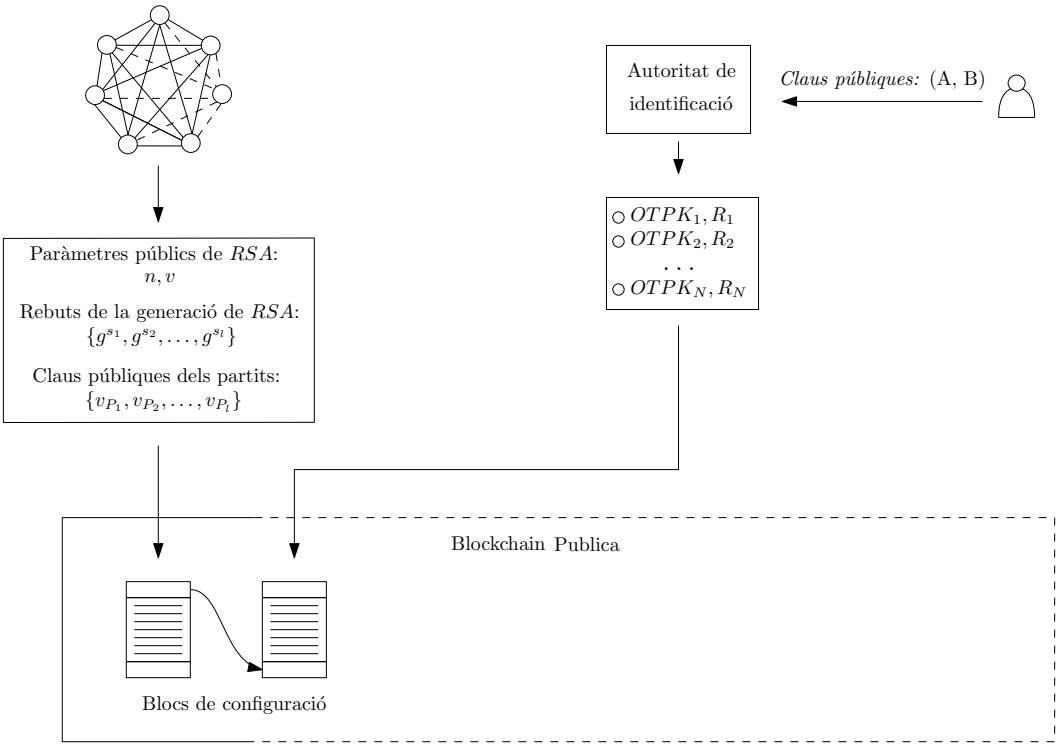

Figura 4.2: Tota persona que vulga votat es registra a l'administració identificant-se seguint el protocol acordat. L'administració calcula i publica totes les *OTPK*s. També s'afegeixen tots els paràmetres públics de la votació, com els valors a utilitzar en el xifrat RSA.

Amb aquest procés ens assegurem que ninguna persona ni entitat per si mateixa pot saber quin és el sentit del vot fins que no acaba el procés de votació, ja que utilitzant la màscara, encara que dos vots tinguen la mateixa opció, seran diferents i encriptant amb les claus RSA donades per les autoritats de recompte, ens asegurem que siga necessària la col·laboració d'almenys k entitats per poder desxifrar el contingut.

Seguidament, la votant signarà el vot per demostrar que ha sigut enviat per una persona que pertany al cens. Lligar la seua pertinença al cens i demostrar que és la primera vegada que vota en aquesta votació i que per tant el seu vot és vàlid, sense donar cap informació que permeta de forma no ambigua esbrinar qui és no és tasca fàcil.

En el cas del nostre sistema de vot, la votant seleccionarà N *OTPKs* d'entre les publicades a la blockchain, i que per tant pertanyen al cens, (incloent la seua pròpia) i realitzarà una firma en anell de la forma detallada a la secció 2.4. D'aquesta forma, demostra que coneix la clau privada d'almenys una de les *OTPKs* que apareixen a la firma, per tant coneix les claus privades d'almenys un parell (A, B) registrat per a la votació. A més, amb la utilització de la *KeyImage*, explicada en la secció 2.4, podem assegurar que la clau privada utilitzada per a signar no ha sigut utilitzada prèviament en la votació sense revelar cap informació de qui ha emès el vot. La *KeyImage* es usada també com a forma privada de seguir el nostre vot, ja que apareixerà en tota transacció a la blockchain que el continga, inclós el recompte. D'aquesta manera la persona que ha votat pot comprovar de forma privada i autònoma, que el seu vot no ha sigut alterat en cap moment.

Destacar que el número de claus $OTPK$ seleccionades, N, es tracta d'un paràmetre important per a la votació i que està lligat a la seguretat. Augmentar N augmenta el cost computacional de la firma i la validació, però augmenta també el nombre de claus que apareixen com a firmants en el vot, per tant fa més difícil lligar a una sola persona a un vot. Es pot considerar afegir una N mínima com a paràmetre de la votació en aquelles en que hi haja una gran preocupació per la seguretat, com a les eleccions per a les institucions estatals.

Per finalitzar el procés d'enviament, la votant seleccionarà un dels partits que participen i li enviarà el vot per a que aquest el processe, aquesta elecció pot ser aleatòria. Podem veure un diagrama d'aquest procés en la figura 4.3.

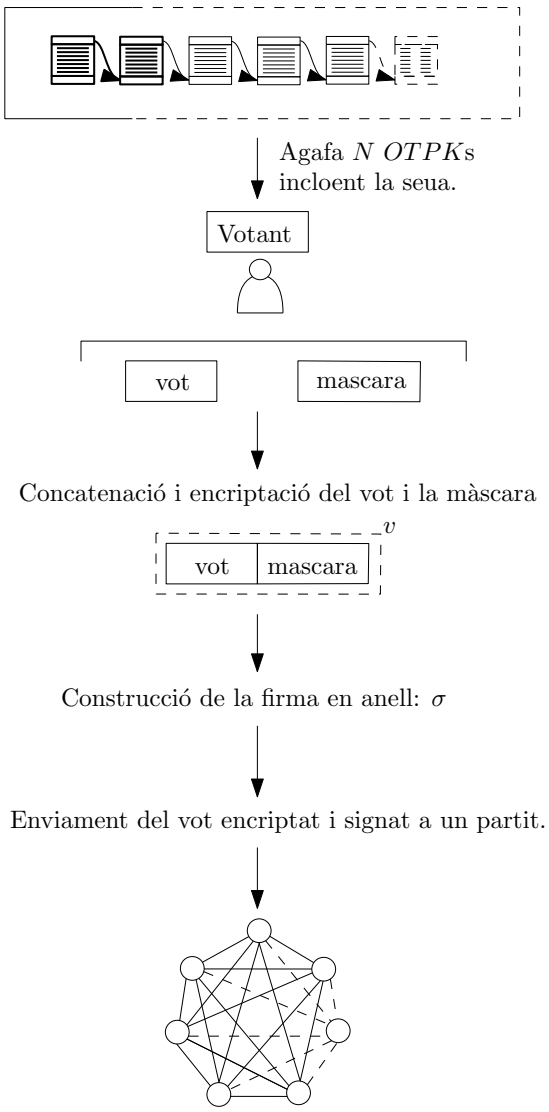

Figura 4.3: En aquest diagrama, dos rectangles contigus representen concatenació, mentre que un sol rectangle de línia discontinua representa encriptació RSA utilitzant exponenciació modular. La firma en anell, Secció 2.4, es construeix utilitzant les N $OTPK$s agafades de la llista pública a la blockchain. Una vegada signat, el vot s'envia a un partit, que es farà carrec de la seua validació i inclusió a la blockchain.

4.1.4. Processament del vot

Quan un partit rep un vot, aquest ha d'aplicar l'algorisme descrit en 2.4 que indicarà si la firma és vàlida o no. Seguidament, afegirà un bloc a la cadena en el que inclourà, a més dels paràmetres típics de les blockchain comentats en 2.5, el vot i el resultat de la verificació. Finalment, reenviarà el vot a la resta de partits per a que validen el vot i afegisquen a la blockchain el resultat de la seua validació, aquest procés està representat a la figura 4.4.

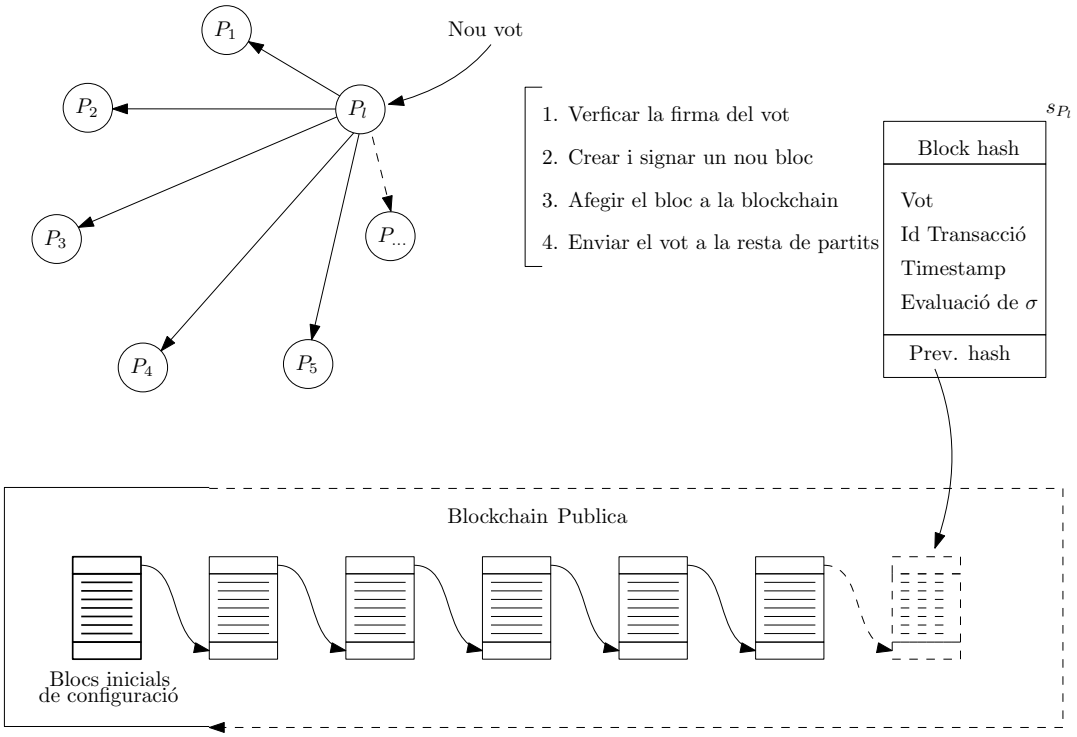

Figura 4.4: Passes a seguir per validar un vot, des de que aplega a un partit fins que aquest el difon amb la resta. Cada partit és responsable de que tots els vots que li han arribat siguen correctament afegits a la cadena. Tots els blocs publicats pels partits aniran signats amb la corresponent clau privada del partit.

Pel que fa al protocol de consens, a diferència de Bitcoin, que tal com hem comentat a la secció 2.5, utilitza Proof of Work, nosaltres hem decidit utilitzar "Proof of authority", és a dir, prova d'autoritat. En lloc d'utilitzar el treball computacional com a autorització per a escriure en la blockchain, gràcies a que les parts encarregades de recomptar els vots són conegudes, estan lligades a entitats físiques i, a més, tenen un gran incentiu per a no tenir comportaments fraudulents, podem permetre que aquestes entitats escriguen sense cap tipus de prova de treball. La naturalesa adversària dels partits en una votació ens porta a un equilibri de Nash [41][42], en el que no hi ha millor estratègia que ser honests.

En cas de bifurcació, al igual que Bitcoin, els partits seguirien la cadena més llarga. Cada partit és responsable d'assegurar que tots els vots destinats a ell han sigut correctament escrits.

4.1.5. Recompte de vots

Finalitzat el període de votació, els partits deixen d'acceptar vots i procedeixen al recompte d'aquests.

Per tal d'aconseguir-ho, els partits han de recuperar la clau privada (s) dels components RSA que van fer públics en la fase de preparació. Serà necessària la col·laboració d'un subgrup (Λ) d'almenys k partits, en condicions normals tots els partits col·laboren per alliberar la clau. Per recuperar la clau s a partir de les parts definides com $\langle s_0 = (x_0, y_0), s_1 = (x_1, y_1), \ldots, s_k = (x_k, y_k)\rangle$ utilitzarem els polinomis de Lagrange:

$$\mathcal{L}(x) = \sum_{j=0}^{k} y_j l_j(x) \tag{4.2}$$

$$l_j(x) = \prod_{\substack{0 \leq m \leq k \\ m \in \Lambda \\ m \neq j}} \frac{x - x_m}{x_j - x_m} \tag{4.3}$$

Una vegada recuperat el polinomi $\mathcal{L}(x)$, podem obtenir s:

$$s = \frac{\mathcal{L}(0)\Delta}{\Delta^3} \tag{4.4}$$

siguent Δ el factor utilitzat quan es va crear la clau RSA. [1]

Una vegada tots els partits tenen la clau privada s, cadascun fa el seu propi recompte, d'aquesta manera quan el partit acabe amb el recompte, publicarà a la blockchain un bloc amb totes les transaccions rebudes desxifrades, el resultat del recompte i la clau privada s, d'aquesta manera qualsevol persona pot re-calcular el recompte i comprovar que efectivament no hi ha hagut cap comportament deshonest i així validar per si mateixa la validesa dels resultats. La figura 4.5 és la representació d'aquest procés.

Si no s'ha produït cap imprevist, aquestos blocs marquen el final de la votació.

4.2 Propietats

Després d'aquest petit recorregut pel funcionament del sistema, m'agradaria comentar les propietats d'aquest ja que ens permeten fer un anàlisi més detallat de les fortaleses i debilitats que pot presentar davant un escenari de vot real. Per tal de realitzar aquest anàlisi, utilitzem les definicions de Lambrinoudakis et al en [48] on redacten una llista de propietats desitjables per a qualsevol sistema de vot electrònic que vulga ser segur.

Considerem que el nostre sistema és verificable, precís, democràtic, privat i robust, entre altres, i a continuació explicarem les definicions i els motius pels

[1] Destaquem que $\Delta = l!$. És utilitzat per a computar els polinomis aleatoris seguint la proposta de Frankel et al. [45].

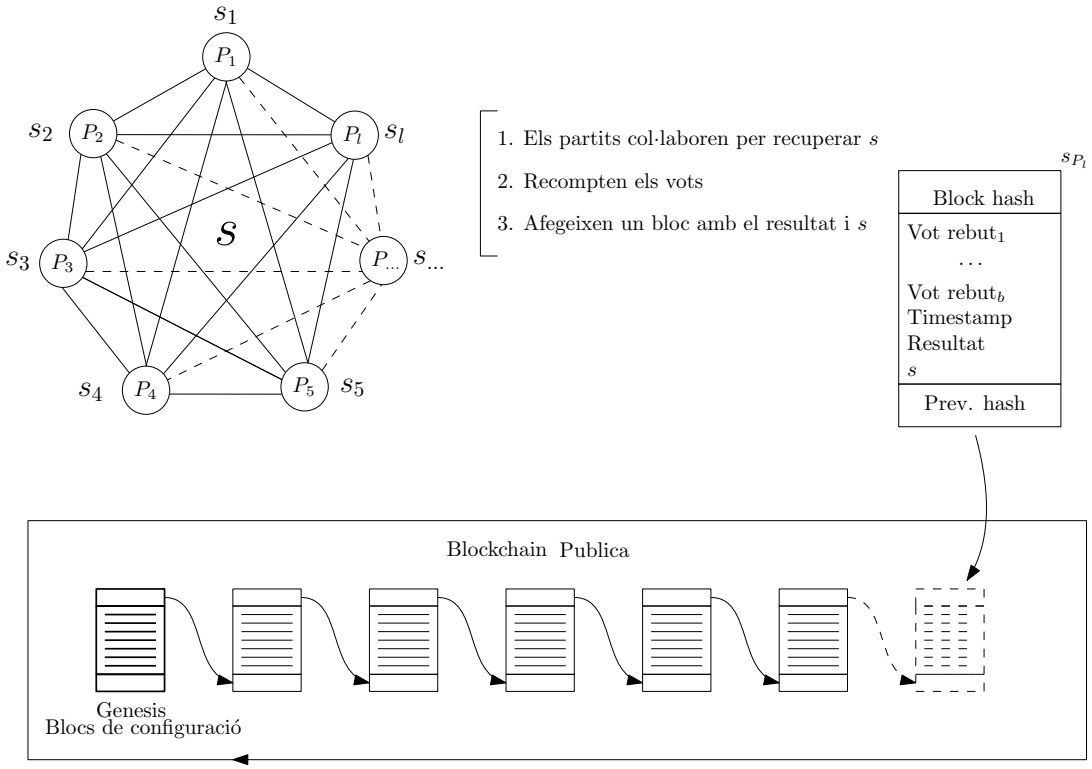

Figura 4.5: Els partits col·laboren per recuperar la clau privada s. Una vegada recuperada, cada partit pot efectuar el seu recompte i publicar-lo a la blockchain juntament amb tota la informació necessària per a que una tercera part puga comprovar el resultat.

que complim amb elles, així com les contradiccions que sorgeixen en el camí i com hem actuat al respecte.

4.2.1. Verificable

Parlem d'un sistema verificable si aquest proporciona mecanismes per a provar que la votació ha sigut portada a cap correctament.

La nostra proposta, gràcies a l'ús de la blockchain com a registre públic i immutable sense que quede registre del canvi, proporciona les ferramentes necessàries per a que qualsevol persona, participant o no, puga auditar el desenvolupament de la votació, ja siga durant aquesta o a posteriori.

Tota persona pot comprovar la integritat dels vots des de que apleguen a la xarxa blockchain fins que són recomptats (*Tallied-as-recorded*) utilitzant els mateixos algorismes de verificació que els partits i la clau privada alliberada al final de la votació per a desxifrar el contingut del vot. Però, a més, qualsevol persona que vote coneixerà la *KeyImage* associada al seu vot, i així, utilitzant-la com una mena de comprovant, pot seguir de forma privada el seu vot en tot moment, comprovant que aquest ha sigut enviat i guardat tal i tal i com volia (*Casted-as-intended, Recorded-as-casted*).

Considerem així, que les votacions portades a cap amb el nostre sistema són universalment verificables ja que en qualsevol moment i per qualsevol persona es pot verificar que la votació està sent justa.

4.2.2. Precís

Un sistema de vot electrònic és precís quan compleix que:

- Una vegada enviats, els vots no poden ser alterats
- Tots els vots vàlids han de ser recomptats
- Cap vot invàlid pot ser recomptat

La primera condició la complim ja que, com hem explicat al punt anterior, el nostre sistema és verificable. A més la blockchain no permet cap canvi sense que aquest aparega.

Pel que fa a les dos condicions restants, en les eleccions en paper aquest rol el compleixen les apoderades i interventores de cada partit a les taules electorals, en el nostre sistema els partits prenen una part activa i, posant en joc la seua reputació, són els responsables de comprovar que tot vot que els haja arribat estiga a la blockchain, i de correctament validar els vots abans de recomptar-los. Així, ens assegurem que tots els vots que apleguen a la xarxa arriben a la blockchain, tant vàlids com invàlids, i que sols els vàlids es tindran en compte per al recompte.

També podem afegir que a diferència de les eleccions en paper on la definició de vot vàlid queda a discreció de la taula (un xicotet desperfecte en el vot es difícil de valorar si ha sigut intencional i si per tant invalidaria el vot) en el nostre sistema la definició de vot vàlid és perfectament objectiva i clara.

4.2.3. Democràtic

Per a que una votació siga considerada democràtica sols aquelles persones que són cridades a votar poden exercir el vot, i sols poden fer-ho una vegada.

Gràcies a la implementació adoptada de la firma en anell, podem assegurar aquestes dos condicions.

D'una banda, sols les persones que s'hagen registrat per a la votació aportant les seues claus públiques (A, B) tindran un parell de claus privades (a, b) que permetran recuperar la clau privada de una $OTPK$, aquella que haja sigut generada a partir de (A, B), de la llista publicada a la blockchain, i per tant votar. Podem assegurar que cada persona pot recuperar sols una clau privada ja que el parell de claus públiques va lligat a la identitat.

També podem assegurar que cada persona que vote sols podrà realitzar com a màxim un vot vàlid perquè cada vot anirà lligat de forma pública a la seua *KeyImage*, ja que no aporta cap informació respecte a la la persona que ha votat. Aquesta es generada a partir de la clau privada utilitzada, per tant, si cada votant sols te accés a una clau privada, sols pot generar una única *KeyImage* vàlida, doncs comprovant si la *KeyImage* que va junt al vot ha aparegut en un altre vot, es pot comprovar si es tracta del primer vot d'aquella persona que vota.

4.2.4. Privat

Per poder afirmar que un sistema de vot és privat, en aquest, no s'ha de poder saber quin vot ha sigut emès per cap persona determinada, és a dir, la identitat que hi ha darrere de qualsevol vot ha d'estar protegida. A nivell pràctic, aquesta propietat suposa molts problemes, ja que sense saber qui ha votat, hem de poder determinar que està al cens, i que no ho ha fet abans.

La firma en anell ens permet utilitzar un grup de claus públiques, i sabent almenys la clau privada d'una d'elles, firmar de forma que és indistingible de quina de les claus públiques se coneix la clau privada. Així podem donar a tota persona votant la privacitat necessària repartint de forma ambigua l'autoria del vot entre les N claus públiques que apareixen a l'anell. Ningú pot assenyalar la clau pública que correspon a la persona que ha votat, excepte eixa mateixa persona.

4.2.5. Robust

Aquesta propietat exigeix que cap grup d'electores ni d'autoritats, de mida raonable, pot alterar el curs normal de la votació. En el cas del nostre sistema utilitzem la tecnologia blockchain amb accés restringit d'escriptura reservat per als partits i l'administració. Podem dir per tal que les persones cridades a votar no tenen cap forma d'alterar aquestos registres, l'única amenaça que ve per la seua part seria la de intentar tombar els nodes dels partits, estudi que escapa a l'àmbit d'aquest treball. D'altra banda, un intent de corrupció per part dels partits quedaria per sempre escrit a la blockchain, no sols la seua reputació es veuria greument afectada, la resta de partits podria ignorar al corrupte i seguir amb la votació. Una altra amenaça dels partits seria que s'ajuntaren els suficients per a poder reconstruir la clau que desxifra els vots abans d'hora. Aquesta és molt improbable ja que el número de partits que es necessiten per a recuperar la clau privada és adaptable segons el nivell de seguretat i la certesa que es tinga que els partits vagen a col·laborar a posteriori. Per a votacions amb un alt grau de importància és fàcil assumir que tots els partits posaran de la seua part al final, encara que siga sota pressió legislativa, per tant per a recuperar la clau abans de que acabe la votació necessitaria la col·laboració de tots els partits, no sols és pràcticament impossible, si no que a més cap estaria aconseguint cap avantatge individual ni de grup.

4.2.6. No-coerció

Creguem que també és important parlar de les debilitats. El nostre sistema, donant la *KeyImage* a la persona que vota com a comprovant de vot que li servirà per a fer un seguiment privat a aquest, deixa la porta oberta a que eixa mateixa persona tinga l'habilitat de demostrar-se autora del vot i per tant a que puga ser forçada a entregar eixe comprovant de vot mitjançant amenaces o suborns. D'altra banda, destacar que és aquest mateix comprovant el que ens permet aconseguir tant la verificabilitat de que el vot ha sigut contat amb la direcció de vot que es desitjava, com la capacitat de detectar el doble vot.

A més, cal tenir en compte que la nostra proposta és un sistema de vot a distància, encara que no donarem aquest comprovant de vot continuaríem sent vulnerables a aquestes pràctiques, en lloc de facilitar el comprovant de vot facilitaries les credencials que te permeten votar. És per això que hem decidit seguir amb aquesta filosofia, hem volgut donar més importància a la seguretat de l'electorat de que el procés ha sigut democràtic, i que inclús desconfiant de totes les parts que tenen un paper actiu pots comprovar de forma autònoma que el procés ha sigut just.

Finalment afegir que es podria implementar l'opció de que en el cas que dos o més vots comparteixen *KeyImage* es tindria en compte l'últim, donant a aquell sota pressió la capacitat de canviar posteriorment el vot.

CAPÍTOL 5
Conclusions i treball futur

Per tal d'aconseguir complir els objectius plantejats ens hem fet valer de les tècniques d'anonimització utilitzades en Monero i els avantatges que presenta la *Proof of Authority* en aquest cas en concret. També, amb la introducció dels partits com a figures amb molt de pes social en el procés de votació, validació de vots i recompte hem volgut apropar els conceptes clàssics i típics de les eleccions en paper a la nostra proposta, donant-los així un paper de responsabilitat que els força a comportar-se de forma honesta.

Havent provat que el sistema compleix amb les propietats desitjables per als sistemes de votació electrònica a distància podem afirmar que s'ha assolit l'objectiu de plantejar un esquema centrat en la confiança i que al mateix temps manté la resta de propietats relacionades amb la seguretat.

No obstant, no podem afirmar amb certesa que aquesta proposta efectivament convenç al públic general, i és per això que considerem que el treball futur passa per implementar el sistema i enquestar a la gent per provar aquest punt.

També mencionar que la existència d'altres estructures de dades distribuïdes i descentralitzades, com la *blocklattice* [49] o el *hashgraph* [50] deixen oberta una clara via de investigació per a millorar el sistema en aquest treball proposat.

Bibliografia

[1] Disponible en https://nvotes.com/ Consultat el 2/7/2020.

[2] Bakhtiari, Sedigheh & Safavi-Naini, Reihaneh & Pieprzyk, Josef Cryptographic Hash Functions: A Survey *Department of Computer Science, University of Wollongong, Australia*, 1995

[3] A. Sinkov. Elementary Cryptanalysis - A Mathematical Approach *New Mathematical Library No.22, Mathematical Association of America*, 1966.

[4] W. Diffie & M. E. Hellman New Directions in Cryptography *IEEE Transactions of Information Theory* 22(6):644-654, 1976.

[5] Ralph Merkle & M. E. Hellman Hiding Information and Signatures in Trapdoor Knapsacks *IEEE Transactions of Information Theory*, 24(5):525-530, 1978.

[6] Rivest & Shamir & Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems *Commun. ACM*, 21:120-126, 1978.

[7] Koblitz, Neal & Menezes, Alfred A Survey of Public-Key Cryptosystems *SIAM Review*, 46, 2004.

[8] Disponible en https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_240&id_menu=[26_%2030] Consultat el 2/7/2020.

[9] Kulandei, Berlin & Ss, Dhenakaran An Overview of Cryptanalysis of RSA Public key System *International Journal of Engineering and Technology*, 9:3575-3579, 2017

[10] Carlos Cid Cryptanalysis of RSA: A Survey *SANS Institute*, 2003

[11] H. W. Lenstra, Jr. Factoring integers with elliptic curves *Annals of Mathematics*, 126:649-673, 1987.

[12] N. Koblitz Elliptic curve cryptosystems *Mathematics of Computation*, 48:203-209, 1987.

[13] V. Miller. Use of elliptic curves in cryptography. Advances in Cryptology *CRYPTO*, 218(483):417–426, 1986.

[14] Andrea Corbellini. Disponible en https://andrea.corbellini.name/2015/05/17/elliptic-curve-cryptography-a-gentle-introduction/ Consultat el 2/7/2020.

[15] SECG Disponible en https://www.secg.org/ Consultat el 1/7/2020.

[16] Ann Hibner Koblitz & Neal Koblitz & Alfred Menezes. Elliptic curve cryptography: The serpentine course of a paradigm shift. *Journal of Number Theory*, 11:781-814, 2009.

[17] David Chaum & Eugène van Heyst. Group signatures. *Lecture Notes in Computer Science*, 547:257-265, 1991.

[18] Ronald L. Rivest & Adi Shamir & Yael Tauman How to leak a secret. *Proceedings Of The 7th International Conference On The Theory And Application Of Cryptology And Information Security: Advances In Cryptology*, 554-567, 2001.

[19] Nicolas Van Saberhagen. Cryptonote Disponible en https://cryptonote.org/whitepaper.pdf Consultat el 2/7/2020.

[20] Shen Noether. Ring signature confidential transactions for Monero. *IACR Cryptol. ePrint Arch*, 2015. Disponible en https://eprint.iacr.org/2015/1098 Consultat el 29/6/2020.

[21] Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Disponible en https://bitcoin.org/bitcoin.pdf, 2008.

[22] Seth Gilbert & Nancy A. Lynch. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services. *SIGACT News*, 33(2):51–59, 2002.

[23] Zheng, Zibin & Xie, Shaoan & Dai, Hong-Ning & Chen, Xiangping & Wang, Huaimin. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14:352-375, 2018.

[24] David Chaum Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms *Communications of the ACM*, 24(2):84-88, 1981.

[25] Goldwasser, S. & Micali, S. & Rackoff, C. The knowledge complexity of interactive proof systems *SIAM Journal on Computing*, 18(1):186-208, 1989.

[26] David Chaum Blind Signatures for Untraceable Payments *Proceedings of Advances in Cryptology - CRYPTO, Santa Barbara, California, USA*, 199-203, 1982.

[27] Michael J. Radwin. An Untraceable, Universally Verifiable Voting Scheme. December 1995

[28] Miyako Ohkubo & Fumiaki Miura & Masayuki Abe & Atsushi Fujioka & Tatsuaki Okamoto. An improvement on a practical secret voting scheme. *Proceedings of Lecture Notes in Computer Science*, 1729:225–234, 1999.

[29] Kibin Lee & Joshua I James & Tekachew G Ejeta & Hyoung J Kim. Electronic voting service using block-chain. *Journal of Digital Forensics, Security and Law*, 11(2):8, 2016.

[30] Pierre Noizat *Handbook of digital currency*. Elsevier, 2015.

[31] Ralph C. Merkle. Protocols for public key cryptosystems. *Proceedings IEEE Symposium on Security and Privacy*, 122-134, April, 1980.

[32] Tim Ruffing & Pedro Moreno-Sanchez. Valueshuffle: Mixing confidential transactions for comprehensive transaction privacy in bitcoin. *Proceedings of the International Conference on Financial Cryptography and Data Security*, 10323:133-154, 2017.

[33] Sean Bowe & Ariel Gabizon & Matthew D Green. A multi-party protocol for constructing the public parameters of the pinocchio zk-snark. *Proceedings of the International Conference on Financial Cryptography and Data Security*, 10958:64-77, 2018.

[34] Pavel Tarasov & Hitesh Tewari. Internet voting using zcash. Disponible en https://dblp.org/rec/bib/journals/iacr/TarasovT17. Consultat el 2/7/2020.

[35] José Luis Salazar & Joan Josep Piles & José Ruíz-Mas & José María Moreno-Jiménez. Security approaches in e-cognocracy. *Computer Standards & Interfaces*, 32(5-6):256-265, 2010.

[36] Guomin Chen & Chunhui Wu & Wei Han & Xiaofeng Chen & Hyunrok Lee & Kwangjo Kim. A new receipt-free voting scheme based on linkable ring signature for designated verifiers. *International Conference on Embedded Software and Systems Symposia*, 18-23, IEEE, 2008.

[37] Patrick P. Tsang & Victor K. Wei. Short linkable ring signatures for e-voting, e-cash and attestation. *IACR Cryptology ePrint Archive*, 2004:281, 2004.

[38] Wei-Jr Lai & Ja-Ling Wu. An efficient and effective decentralized anonymous voting system. Disponible en https://arxiv.org/abs/1804.06674. Consultat el 29/6/2020.

[39] Vitalik Buterin Ethereum Disponible en https://ethereum.org/whitepaper/

[40] Yifan Wu. An e-voting system based on blockchain and ring signature. *University of Birmingham*, Treball final de master, 2017.

[41] Nash, John. Equilibrium points in n-person games *Proceedings of the National Academy of Sciences*, 36(1):48–49, 1950.

[42] Nash, John. Non-Cooperative Games *The Annals of Mathematics*, 54(2):286-295, 1951.

[43] Yair Frankel & Philip D. MacKenzie & Moti Yung. Robust efficient distributed rsa-key generation. *Proceedings of the Thirtieth Annual ACM Symposium on the Theory of Computing, Dallas, Texas, USA, May 23-26, 1998*, 663-672, 1998.

[44] Ivan Damgård & Maciej Koprowski. Practical threshold RSA signatures without a trusted dealer. *Advances in Cryptology - EUROCRYPT 2001, International Conference on the Theory and Application of Cryptographic Techniques, Innsbruck, Austria, May 6-10, 2001, Proceeding*, 152-165, 2001.

[45] Yair Frankel & Peter Gemmell & Philip D. MacKenzie & Moti Yung. Optimal resilience proactive public-key cryptosystems. *38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997*, 384-393, 1997.

[46] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612-613, 1979.

[47] Torben P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, 129-140, 1991.

[48] Lambrinoudakis, Costas & Gritzalis, Dimitris & Tsoumas, Vassilis & Karyda, Maria & Ikonomopoulos, Spyros. *Secure Electronic Voting: the Current Landscape.*, 101-122, 2003

[49] Colin LeMahieu Nano: A Feeless Distributed Cryptocurrency Network Disponible en https://content.nano.org/whitepaper/Nano_Whitepaper_en.pdf Consultat el 1/7/2020.

[50] Leemon Baird & Atul Luykx The Hashgraph Protocol: Efficient Asynchronous BFT for High-Throughput Distributed Ledgers Disponible en https://www.hedera.com/hh-ieee_coins_paper-200516.pdf *IEEE COINS*, 2020 Consultat el 1/7/2020.