RECULL DE CONFERÈNCIES 2021 / DEBATS DE RECERCA 14: 246-267 (2022)
Societat Andorrana de Ciències, Andorra
DOI: 10.2436/15.8060.31.8 ISBN: 978-99920-61-65-7

Francesc Garcia i Grau

Enginyer en Informàtica (UAB), màster en seguretat de les TIC (UOC) i doctorand de l'UdA

Francesc Garcia i Grau

Credencials anònimes enllaçables: com aplicar la identitat autogestionada a les votacions electròniques amb cadena de blocs ('blockchain') i 'smart contracts'

Resum

Les credencials anònimes basades en atributs (ABC) donen els mitjans per implementar la identitat autogestionada (SSI) que trasllada la responsabilitat de la custòdia de les dades personals a l'usuari, i li permeten tenir el control sobre qui, on i quan vol difondre aquestes dades. Els sistemes de votacions electròniques pateixen de falta de transparència i de la necessitat d'anonimat. La transparència s'aconsegueix amb la utilització de la cadena de blocs (*blockchain*) i *smart contracts*, però l'anonimat esdevé una qüestió de confiança. La identitat autogestionada garanteix aquesta necessitat d'anonimat, però massa, ja que no és possible enllaçar diferents presentacions d'un mateix atribut, i per tant no és aplicable a les votacions electròniques. El que busca aquest projecte de recerca és poder donar dret a fer quelcom a un individu, preservant la seva privacitat, i un cop donat aquest dret, eliminar la necessitat de terceres parts de confiança, i assegurar que només podrà exercir aquest dret de manera única. Així, es defineix el concepte d'atributs anònims enllaçables dins les ABC, que garanteixen l'anonimat i la propietat de ser únics dins d'un àmbit donat, fent que aquests atributs siguin enllaçables i es puguin utilitzar en votacions electròniques, preservant l'anonimat i la propietat de ser únics, fins i tot davant un usuari malintencionat o una conxorxa entre diferents actors. Com a resultat d'aquesta recerca, es vol aconseguir un protocol que asseguri l'anonimat, és a dir, que no sigui possible saber qui hi ha darrere d'unes credencials donades, però que alhora aquestes credencials siguin úniques dins un àmbit donat per poder detectar l'ús repetit d'aquestes credencials. I amb aquest protocol demostrar que és possible aplicar-lo a unes votacions electròniques remotes basades en la cadena de blocs (*blockchain*) i *smart contracts*.

1. Introducció

Aquesta recerca neix de la juxtaposició de dos conceptes en voga en els darrers temps, les votacions electròniques i la cadena de blocs (*blockchain*). Com a conseqüència de la pandèmia de la COVID-19,[1] amb confinaments constants, les votacions electròniques prenen protagonisme però segueixen acusant un cert grau de desconfiança per part d'electors i institucions. Després d'una recerca sobre votacions electròniques i, més particularment, les implementades amb tecnologia de cadena de blocs (*blockchain*), s'han detectat mancances en el procés específic de l'autenticació i en com es gestiona l'anonimat. En tota la literatura consultada, l'autenticació es deixa a un tercer de confiança, i no s'estudia a fons. A més, no es tenen en compte possibles conxorxes entre participants. Pel que fa a l'anonimat, sempre s'assoleix mitjançant algoritmes costosos de barreja, en què no sempre es pot garantir no poder enllaçar una identitat amb un vot. En el nostre estudi, es planteja un enfocament diferent, es pretén proposar un sistema d'autenticació que proporcioni anonimat, en què no cal que es confiï en ningú. Aquest anonimat està garantit fins i tot quan es conxorxin diferents actors del sistema. L'objectiu principal és poder donar dret a fer quelcom a un individu, preservant la seva privacitat, de forma distribuïda. I un cop donat aquest dret, eliminar la necessitat de terceres parts de confiança, tot assegurant que només podrà exercir aquest dret de manera única. Així, es pretén aplicar el concepte d'obtenir un dret únic preservant la privacitat a les votacions electròniques basades en la cadena de blocs (*blockchain*) i *smart contracts*. És a dir, aconseguir un sistema de votacions electròniques basades en tecnologia de cadena de blocs (*blockchain*) i *smart contracts*, en què el dret a vot vingui donat per un atribut enllaçable d'unes credencials anònimes d'una identitat autogestionada.

En l'apartat 2 es descriu la recerca efectuada en els diferents camps de coneixement que ens ocupen i es fa una anàlisi del marc de referència en què es posiciona l'estudi. Tot seguit, en l'apartat 3, s'exposen els objectius de la recerca. La metodologia utilitzada s'exposa en l'apartat 4. Per acabar l'escrit, els resultats esperats s'enumeren en l'apartat 5.

L'àmbit en què se centra aquesta recerca és nou, fet que explica que les referències siguin recents. Moltes tecnologies emprades van sorgir després del 2014 i els recursos es troben en línia.

1- Elections during COVID-19. 2020. URL: https://www.coe.int/en/web/electoral-assistance/covid-19-response (cons. 2-11-2020).

2. Marc teòric

El marc teòric d'aquesta recerca neix de diferents eixos que s'han de combinar per assolir els objectius. La recerca efectuada es focalitza en tres camps de coneixement específics que es poden estudiar per separat.

Inicialment s'han centrat els esforços a definir el marc teòric de les votacions electròniques revisant la literatura. S'han definit un seguit de rols, processos i requeriments dels sistemes de votacions electròniques. Un cop fetes aquestes definicions, s'ha tornat a revisar la literatura que descrivia implementacions concretes per classificar-les amb els criteris definits abans. En aquesta anàlisi s'ha aprofundit en la criptografia utilitzada per assegurar els requeriments de les votacions. En aquest estudi s'ha pogut veure que els sistemes tenen en comú un mateix punt feble: la confiança. En aquest punt es va decidir que la recerca se centraria només en votacions electròniques remotes. Solen ser sistemes tancats en què, si una de les parts actua maliciosament o en conxorxa amb una altra de les parts, es deixen de complir alguns dels requeriments. Els sistemes més transparents, segons la recerca, són aquells que utilitzen la cadena de blocs (*blockchain*). Dins d'aquests sistemes n'hi ha de dos tipus: els que la utilitzen com un simple taulell de notícies per publicar l'auditoria del procés, i els que utilitzen la cadena de blocs (*blockchain*) amb *smart contracts* per implementar el protocol de votacions en la cadena. Un cop analitzats aquests resultats, s'ha decidit seguir la recerca amb els darrers, per poder assegurar la màxima transparència i confiança en el procés.

Tot seguit s'ha centrat la recerca en els articles trobats que parlen sobre implementacions de vot electrònic remot amb cadena de blocs (*blockchain*) i *smart contracts*. Alguns d'ells proporcionen un enllaç a GitHub[2] amb el codi que els implementa. Vist això, s'ha decidit posar en funcionament una cadena de blocs (*blockchain*) Ethereum[3] per poder desplegar cada un dels sistemes i fer-hi proves. S'han analitzat en profunditat dos de les opcions, ja que les altres, o bé eren proves de concepte o bé no s'ha trobat el codi per poder provar-les. En l'estudi, s'ha detectat que el punt més feble i que queda sempre fora de la cadena, i que per tant és menys transparent, és l'autenticació que en totes les propostes, si existeix, la duu a terme una tercera entitat de confiança.

2- GitHub: Where the world builds software · GitHub. 2020. URL: https://github.com (cons. 2-11-2020).

3- Home | ethereum.org. 2020. URL: https://ethereum.org (cons. 2-11-2020).

Un cop detectades les carències dels sistemes estudiats, es decideix endinsar-se en els sistemes d'autenticació. La recerca se centra, aleshores, en sistemes de credencials, però de manera més concreta en les credencials basades en atributs, estudiant-ne algunes en concret com U-prove [37] o Idemix [17], i la que finalment s'ha escollit com a marc de referència, la identitat autogestionada (*self-sovereign identity*).[4,5]

Així doncs, a l'apartat 2.1, s'introdueix la tecnologia de cadena de blocs (*blockchain*) amb les seves bases i implementacions de referència. Seguidament, a l'apartat 2.2, s'estudien les votacions electròniques, es defineixen els conceptes, els seus processos i s'aprofundeix en dos implementacions específiques que s'ajusten als requeriments del projecte per les seves característiques. Tot seguit, a l'apartat 2.3, s'enumeren i s'analitzen els sistemes d'autenticació, i es categoritzen en quatre famílies. I, per acabar, l'apartat 2.4 descriu amb profunditat el sistema d'autenticació escollit per implementar la solució.

4- Sovrin. Sovrin protocol. 2018. URL: https://sovrin.org (cons. 23-2-2020).

5- Hyperledger Indy - Hyperledger. 2020. URL: https://www.hyperledger.org/use/hyperledger-indy (cons. 18-10-2020).

2.1. Tecnologia de cadena de blocs (*blockchain*)

La tecnologia distribuïda basada en la cadena de blocs (*blockchain*) o simplement la cadena de blocs (*blockchain*) està en posició de canviar dràsticament l'intercanvi d'informació digital, com afirma Marvin Van Wingerdeen en la seva tesi "Blockchain-enabled self-sovereign identity" [28]. Internet afavoreix l'intercanvi d'informació de manera ràpida, i això fa que no estigui resolt el problema següent: cada cop que s'envia informació a algú, se li envia una còpia d'aquesta informació, no la informació en si mateix. Per tant, la transaccionalitat no està assegurada. Per això, cal que terceres parts actuïn com a intermediaris per garantir aquesta transaccionalitat. Aquestes terceres parts concentren, aleshores, un gran poder. La tecnologia de la cadena de blocs (*blockchain*) busca trencar aquesta concentració de poder, assegurant la transaccionalitat de manera distribuïda amb un protocol de consens entre tots els participants.

2.1.1. Definició de cadena de blocs (*blockchain*)

En les tecnologies emergents, costa arribar a un consens per definir-les formalment i de forma acadèmica. Mougard, a [24], descriu el potencial de la cadena de blocs (*blockchain*) des de tres perspectives:

• Des d'un punt de vista de negoci, la cadena de blocs (*blockchain*) és una xarxa en què s'intercanvien valors digitalment *peer-to-peer*, és a dir, d'extrem a extrem, sense intermediaris.
• Des d'un punt de vista legal, la cadena de blocs (*blockchain*) és un protocol de xarxa que valida transaccions sense necessitat de confiar en un tercer.
• I, a l'últim, des d'un punt de vista tècnic, la cadena de blocs (*blockchain*) és un suport processador dorsal (*back-end*) de base de dades públiques, distribuïdes i immutables.

La Distributed Ledger Technology (DLT) és l'ànima (*core*) de la cadena de blocs (*blockchain*). Bàsicament, un *distributed ledger* (DL) és una base de dades distribuïda, mantinguda per un conjunt de nodes que executen un programari específic [22]. Dins la cadena de blocs (*blockchain*), els registres de les transaccions del DL s'agrupen en blocs que s'enllacen entre ells. Si tots els nodes que conformen la xarxa tenen els mateixos permisos i poden afegir blocs, es diu que és una DL pública (*permissionless*). En canvi, si només un conjunt de nodes tenen la possibilitat d'afegir blocs, s'anomena DL privada (*permissioned*). En l'àmbit de la cadena de blocs (*blockchain*), a partir d'aquests dos tipus generals, prenen forma tres tipologies de DL, cada una amb les característiques següents [10]: els *public ledgers*, que són públics (*permissionless*) amb nodes anònims, i no requereixen cap grau de confiança entre nodes. També hi ha els *private ledgers*, que són privats (*permissioned*) i operats per una única entitat que ha de tenir la total confiança dels membres de la xarxa. Finalment, trobem els *consortium / hybrid ledgers*, que són privats (*permissioned*), però que en aquest cas són operats per un conjunt de nodes de confiança anomenats operadors, i en què els membres han de confiar en una majoria d'aquests operadors.

2.1.2. Tecnologia de capes de la cadena de blocs (*blockchain*)

La cadena de blocs (*blockchain*) té múltiples capes tecnològiques. Es poden definir tres capes bàsiques a la cadena de blocs (*blockchain*), basant-se en les descrites per Melanie Swan en l'article "Blockchain: blueprint for a new economy" [27]:

• La capa de persistència: formada per un DL públic amb registres que emmagatzemen les transaccions.
• La capa de protocol: composta pel programari de protocol que gestiona aquestes transaccions.
• La capa d'aplicació: que és la capa de negoci en què s'implementa, per exemple, la criptomoneda en el cas del bitcoin (BTC). Passem a descriure breument cada una de les capes en particular.

La capa de persistència: la criptografia és una peça fonamental de la tecnologia de cadena de blocs (*blockchain*). La criptografia assegura la integritat de la cadena de blocs (*blockchain*) i permet transaccions autenticades i assegura un cert grau d'anonimat als membres de la xarxa.
La capa de protocol: un exemple de com s'emmagatzema una transacció (Tx) de pagament simple amb el protocol Bitcoin es mostra en l'exemple següent: el Pau vol enviar una transacció (Tx) a la Mònica. Per iniciar la Tx, el Pau necessita la clau pública de la Mònica i la seva pròpia clau privada. El Pau fa servir un programa específic anomenat moneder (*wallet*) per dur a terme la transacció. El moneder crea una Tx amb la clau pública de la Mònica com a receptor, signada amb la clau privada del Pau. El moneder emet aquesta transacció de forma global a la xarxa de membres. Cada membre de la xarxa comprova que el Pau pot fer aquesta Tx (p.e.: té prou saldo). La Tx, un cop acceptada, s'agrupa amb altres per formar un bloc. Un cop el bloc està llest, es "mina" per provar-ne la validesa i consensuar un nou estat de la cadena de blocs (*blockchain*).
La capa d'aplicació: la capa més alta és la capa d'aplicació, en què s'implementen les criptomonedes (n'hi ha més de 7000 en data setembre del 2020).[6] Les criptomonedes es creen generalment d'acord amb dos aproximacions: comencen des de zero, sense que n'hi hagi en circulació, o bé comencen amb un conjunt de monedes prefabricades. Bitcoin va iniciar-se sense cap moneda en circulació. Les noves monedes es generen en validar blocs. A la data d'escriptura d'aquest document,[7] la persona que afegeix un bloc a la cadena rep 6,25 BTC com a recompensa pel seu esforç. Aquesta recompensa no és fixa i es va reduint en el temps. Aquesta reducció es produeix cada cop que s'assoleixen 210.000 blocs (cosa que passa aproximadament cada quatre anys), i la

6- Cryptocurrency Prices, Charts and Market Capitalizations | CoinMarketCap. URL: https://coinmarketcap.com/ (cons. 14-11-2020).
7- Will Kenton. Bitcoin Mining Definition. Oct. del 2020. URL: https://www.investopedia.com/terms/b/bitcoin-mining.asp (cons. 2-11-2020).

recompensa passa a ser la meitat del seu valor. Així, la recompensa va passar dels 50 BTC al 2009 a 25 a partir del 2013, a 12,5 durant el 2018, i a partir de l'11 de maig del 2020 ha passat a valdre 6,25 BTC. El total i la freqüència de generació d'una criptomoneda venen definits pel protocol. En el cas del bitcoin, hi ha un sostre de 21 milions de bitcoins. Per la seva banda, l'Ether [38], una altra criptomoneda, comença com una moneda prefabricada pels seus desenvolupadors. Quan una moneda és prefabricada, una part del total de les monedes en circulació són assignades a una adreça abans de la creació de la cadena de blocs (*blockchain*).

Diverses capes d'aplicació poden compartir la mateixa capa de protocol i la mateixa capa de persistència [27]. També, diverses combinacions de capa d'aplicació i protocol poden compartir la capa de persistència.

2.1.3. *Smart contracts* (SC)

Els SC afegeixen una subcapa més en la capa d'aplicació i un grau més de complexitat a les transaccions bàsiques de la cadena de blocs (*blockchain*), que només permeten moviments de criptomonedes entre membres. Els SC permeten la programació de transaccions i són essencialment trossos de codi que, gràcies al mecanisme de consens de la cadena de blocs (*blockchain*), poden assegurar que s'executin correctament. Cada SC resideix a la cadena de blocs (*blockchain*) i té la seva adreça pública. A diferència d'un compte "normal", els SC no posseeixen una clau privada; la seva integritat ve donada en formar part de la cadena de blocs (*blockchain*).

La plataforma basada en SC més popular és Ethereum.[8] Quan un SC es desplega sobre Ethereum, la seva adreça adquireix la capacitat de tenir certa quantitat d'Ether (la criptomoneda associada a Ethereum), espai d'emmagatzematge i el seu codi associat [20]. A Ethereum, per executar un contracte cal gastar "gas". Aquest gas és com un combustible que equival a fraccions d'Ether. Això és així per evitar que un programa entri en un bucle infinit i col·lapsi la xarxa. Quan al contracte se li acaba el gas, s'atura. Per tant, un usuari, quan vol executar un SC, cal que enviï una transacció a l'adreça del contracte amb dos informacions: la quantitat de gas màxima que està disposat a gastar i les dades d'entrada per a l'execució del codi.

8- Home | ethereum.org. 2020. URL: https://ethereum.org (cons. 2-11-2020).

Un problema de seguretat amb SC és que no hi ha un mètode generalitzat de verificació formal [3] del codi dels SC.

2.2.Votacions electròniques

La idea de la votació electrònica és tan vella com l'ús de l'electricitat en si. El juny de 1869, Thomas A. Edison ja va registrar i obtenir la patent 90646 per un sistema electrogràfic de gravació de vots per a les eleccions al Congrés [30]. Però va tenir el rebuig per part dels congressistes, ja que ho van percebre com una pèrdua de debat en la manera de fer. La idea de poder exercir el vot electrònicament permet un recompte més ràpid. A més, si el vot es pot exercir via Internet, obre un gran ventall d'escenaris, i permet a un nombre d'electors més gran, que per la raó que sigui no poden accedir físicament a les urnes, exercir aquest dret. Però tots aquests beneficis es veuen eclipsats per la desconfiança. Qui ens assegura que ningú altera els vots, n'afegeix o els esborra? Un sistema de votació electrònica fa referència a l'ús d'ordinadors o equips de vots informatitzats per exercir el vot en unes eleccions; utilitzar aquest sistema no és fàcil ja que cal garantir els requeriments de seguretat per al vot electrònic. L'ús de criptografia avançada permet assegurar el vot electrònic i fer-lo aplicable [7]. Un sistema de votació electrònica remot és el que permet exercir aquest vot a través d'Internet.

2.2.1. Conceptes

En la recerca feta s'han pogut sintetitzar cinc rols per als diferents actors del sistema. A l'article "A review of contemporary e-voting: requirements, technology, systems and usability" [29], Wang et al. defineixen un vot com la selecció d'un candidat dins d'una llista de candidats. Aquesta selecció o seleccions es plasmen en una butlleta que serà dipositada a l'urna. La persona que fa aquesta elecció i l'emet té el rol de "votant". El rol "registrar", esmentat en els articles [29, 21], és l'encarregat de fer el registre, a partir d'una llista de possibles votants amb dret a vot, identificar-los i atorgar-los aquest dret. És qui gestiona el registre censal. El rol *pollster* o *collector*, definits a [1, 29, 11], actua com a agent i presenta les butlletes de manera que una persona humana pugui entendre-les i en recull les respostes (els vots). També aplica la criptografia necessària, obté les validacions i els

rebuts necessaris, i s'encarrega de dipositar el vot a l'urna. Es pot considerar la part client del sistema.
El rol *validator*, esmentat als articles [29, 1], és el responsable de verificar l'autenticitat dels vots duent a terme les operacions criptogràfiques necessàries per fer les validacions depenent del tipus de verificació escollida. I per acabar l'enumeració dels rols, el rol *tallier* o *tallying authorities*, definit als articles [29, 8, 1, 2], és el responsable de desxifrar els vots, contar-los i publicar-ne els resultats.
A més, les votacions han de preveure sis fases o processos. La primera fase que es pot trobar en els articles [11, 12, 30, 6, 21, 14, 1, 29] s'anomena *registration/preparation*. Consisteix a recopilar la llista dels votants, és a dir, confeccionar el cens electoral. A més, en aquesta fase es preparen les butlletes i tota la logística necessària per dur a terme les votacions. La segona fase, recollida en els articles [29, 12, 11, 23, 14, 1, 13], és el procés de *validation/authentication*, que comprèn la verificació de credencials dels votants, i permet el vot només a aquells que s'han registrat, controlant que només ho facin un cop. La tercera fase, definida als articles [29, 1, 21, 11, 16, 6, 8], s'ocupa de l'emissió i la recollida de les butlletes. La quarta fase és la de *verification*, que s'ha extret dels articles [29, 1, 21, 4, 12, 2]. Aquest procés verifica cada una de les butlletes. Només les butlletes vàlides seran comptades en la fase següent, que és la fase de *tallying*. Al final d'aquesta cinquena fase es publica l'escrutini. Resta una sisena fase, que és la de *claiming*. Qualsevol reclamació es té en compte en aquesta fase i s'investiga, i també s'aprofita per fer una auditoria. Al final d'aquesta fase es publiquen els resultats finals de les votacions.

2.2.2. Requeriments

Un cop establerts els conceptes i els processos del vot electrònic, la recerca s'ha centrat en buscar i establir els requeriments específics per al vot electrònic remot. Aquests requeriments es poden trobar en nombrosos articles. En general es defineixen un conjunt de requeriments obligatoris i una altra sèrie de requeriments opcionals desitjables.
S'han recollit vuit requeriments obligatoris. El primer es coneix com a *correctness* (*completeness and soundness*) i apareix en els articles [21, 29, 1, 4, 12, 7]: el sistema ha d'assegurar que no està afectat per cap comportament

fraudulent per cap de les parts participants ni per procediments defectuosos; no ha de ser possible alterar vots, descomptar vots vàlids o incloure vots invàlids en l'escrutini final. El segon és la *privacy*, que es pot descriure com en els articles [29, 7], en què es presenten quatre propietats que ha de complir: no s'ha de poder enllaçar una butlleta a qui l'ha emesa (*voter-vote unlinkalibility*); no s'ha de poder saber des de quina IP s'ha emès una butlleta (*voter-vote IP untraceability*); no es pot afegir informació identificable a la butlleta, i, per acabar, les autoritats no hi poden afegir informació identificable. El tercer requeriment és l'*unreusability*: com descriuen els articles [4, 29], només compta un vot vàlid per votant, és a dir, un votant només pot votar un cop. Això és el que es coneix com a prevenció del *double-voting*. El quart requeriment és l'*eligibility*, definit als articles [1, 29, 8, 14, 7, 6, 16, 11]: el sistema ha d'assegurar que només els votants poden votar i que només poden votar una vegada. El cinquè requeriment és la *robustness*, citat als articles [29, 6, 14, 1], que diuen que un sistema es diu robust si és capaç de funcionar correctament amb un cert grau de tolerància a possibles votants maliciosos o a fallades parcials del sistema; normalment, requereixen sistemes distribuïts en alta disponibilitat i tolerants a fallades. El sisè és el *verifiable*, descrit als articles [4, 13, 29, 14, 21]: d'una banda, cada votant ha de poder verificar que el vot emès és el que s'ha enregistrat (*individual verifiability*); de l'altra, l'escrutini i les proves de correcció corresponents han de ser publicades i qualsevol ha de poder verificar l'escrutini de les eleccions (*universal verifiability*). El setè és l'*usability*, mencionat a l'article [29], que té un paper important per determinar la reeixida del sistema. Finalment, el vuitè és la *fairness*, citat als articles [16, 11, 9, 12, 4, 6, 7, 21, 14, 8, 1, 29]: els resultats no es poden conèixer abans que acabin les votacions per no influir en els votants que encara no han votat.

Els requeriments addicionals però desitjables que s'han trobat són cinc. L'*uncoercability* o resistència a la coerció, extret del articles [29, 8, 12, 16, 9, 23, 11]. La coerció té a veure amb la compra de vots en què el votant ha de convèncer el comprador que ha votat sobre el que hi ha establert en la compra.

Aquest requeriment no és exclusiu de les votacions electròniques i és un problema conegut, important i de difícil solució en el vot per correu. En l'*efficiency*, esmentada en els articles [9, 1, 29], cal que la càrrega de càlcul sigui prou lleugera per poder obtenir els resultats en un temps raonable. En la *mobility*, descrita en els articles [29, 1, 9], un sistema és mòbil si no hi ha restriccions geogràfiques a l'hora d'emetre el vot. La *vote-and-go*, definida en els articles [12, 29], és quan un cop el votant ha emès el seu vot i ha acabat el seu procés de vot, ja no cal cap més acció per part seva. La *practicability*, mencionada en els articles [29, 6], requereix que el sistema no depengui d'assumpcions que siguin difícils d'assolir en escenaris a gran escala.

2.3. Sistemes d'autenticació

Des de l'inici de l'era digital, els sistemes informàtics (SI) han tingut la necessitat d'identificar la persona (o SI) a l'altre costat d'una comunicació. Aquesta identificació es coneix com a autenticació. En la literatura existent s'han trobat diferents tipus d'autenticació en el món digital, que es poden classificar en els grups següents per ordre cronològic d'aparició.

2.3.1. Autenticació independent

Des de l'aparició dels sistemes operatius de temps compartit, a l'inici de la dècada dels 60 [33], cada SI posseeix la seva base de dades d'usuaris en què es guarden dades privades (DP) de cada usuari, el mètode d'autenticació i un secret (que pot ser una paraula clau, dades biomètriques o quelcom que sabem o tenim).

Aquest tipus d'autenticació té un seguit d'avantatges i inconvenients:

- Avantatges: és un sistema fàcil d'implementar, ja que només cal guardar una taula amb la correspondència nom/secret. El secret és en forma de paraula clau. És intuïtiu, l'usuari té un nom i un secret, i amb això en té prou per autenticar-se.
- Inconvenients: si el secret es fa públic qualsevol pot suplantar l'usuari. El fet que augmenti el nombre de serveis fa que l'usuari hagi de gestionar molts noms/secrets, ja que no sempre es pot utilitzar el mateix nom i, a més, és aconsellable fer servir diferents secrets per a cada nom. D'altra banda, diversos SI posseeixen dades privades que no sempre estan tan ben custodiades com caldria, i sovint hi ha fugues de dades personals [35].

2.3.2. Proveïdors d'autenticació o *identity managers* (idm)

Les especificacions d'un idm estan definides en el document "A framework for identity management - Part 1: Terminology and concepts" [18]. Degut als inconvenients abans esmentats, durant la dècada dels 2000 apareixen terceres parts, com Google (Google Id),[9] Facebook (Facebook login)[10] o OpenId,[11] que ofereixen als diferents SI la delegació de l'autenticació. Les especificacions d'un idm estan definides en el document "A framework for identity management - Part 1: Terminology and concepts" [18].

Apareixen nous estàndards, com el Security Assertion Markup Language (SAML) [36] o l'OAuth [15], que permeten a una entitat delegar l'autenticació feta per un tercer i confiar-hi. Aquesta solució permet tenir un únic usuari amb una única contrasenya per a diversos sistemes, però no soluciona la custòdia de la informació privada, que segueix estant fora de la custòdia de l'usuari. L'idm genera un testimoni d'autenticació (*token*), que és un conjunt de bytes amb el format del protocol, ja siguin SAML o OAuth, que té un temps de validesa, i que quan es presenta fa que l'SI final permeti l'accés als serveis.

Aquest tipus d'autenticació té un seguit d'avantatges i inconvenients:

- Avantatges: és un sistema intuïtiu. L'usuari té un nom i un secret, i amb això en té prou per autenticar-se. Les credencials són úniques per a tots els serveis. Aquest sistema permet el *Single Sign On* (SSO), i només cal autenticar-se un cop si diversos serveis fan servir el mateix idm.

I, finalment, les dades d'autenticació són úniques i són en un sol lloc.

- Inconvenients: és un sistema més complex d'implementar; cal estar d'acord sobre el tipus de testimoni d'autenticació (*token*) que cal utilitzar. A més, té dependència d'un tercer que, si no està disponible, fa que es perdi l'accés als serveis temporalment o definitivament si el tercer desapareix. Aquest tercer passa a tenir un gran poder, provoca centralització i a més té informació sobre quins serveis utilitza un usuari, fet que li permet confeccionar un perfil de cada usuari. També, si el secret es fa públic, qualsevol pot suplantar-lo en tots els serveis alhora. I, finalment, les dades privades segueixen estant en les bases de dades dels diferents SI i no sempre estan custodiades com caldria. Sovint hi ha fugues de dades personals [35].

9- Google. Google identity platform. URL: https://developers.google.com/identity (cons. 4-10-2020).

10- Facebook. Facebook login. URL: https://developers.facebook.com/docs/facebook-login (cons. 4-10-2020).

11- OpenID Foundation website. 2012. URL: https://openid.net/ (cons. 23-2-2020).

2.3.3. Credencials basades en atributs verificables

També, a principis dels anys 2000, apareixen aquest tipus de credencials. L'enfocament d'aquests sistemes busca preservar la privadesa de les dades, evitar-ne la disseminació a la xarxa i traslladar la custòdia de les dades a l'usuari. Es basa en unes entitats de confiança (EC) que generen proves criptogràfiques irrefutables sobre atributs d'un usuari. Aquestes proves s'anomenen atributs verificables (AV). L'usuari pot, a posteriori, utilitzar els AV per provar la validesa dels atributs a un tercer.

Aquest mecanisme té un seguit d'avantatges i inconvenients:

- Avantatges: l'usuari és qui custodia els seus AV i els proporciona a qui vol, quan vol.
- Inconvenients: els inconvenients principals són l'ús de criptografia asimètrica que requereix potència de càlcul, la falta d'un estàndard consolidat, i la poca adopció; encara hi ha pocs sistemes que l'implementin.

L'ús de la tecnologia Privacy-preserving Attribute Base Credencial (Privacy-ABC), que descriu Jan Camenish a [5], permet fer assercions (atestats) sobre identitats i preservar-ne la privacitat.

Existeixen dos projectes fonamentats sobre Privacy-ABC: Idemix [17] i U-prove [37].

2.3.4. L'anonimat

Quan es parla d'anonimat s'ha de definir què vol dir i com s'aplica en cada context. Andreas Pfitzmann i Marit Hansen, en l'article [25], defineixen formalment la terminologia utilitzada en aquest àmbit.

Anonimat: l'anonimat es defineix com la propietat que fa indistingible un individu determinat dins d'un conjunt d'individus que s'anomena conjunt d'anonimat. En el cas que ens ocupa això es tradueix en què no hi ha forma d'identificar qui fa una acció donada o qui envia un missatge dins el sistema.

Unlinkability (no enllaçabilitat): la no enllaçabilitat de dos temes d'interès (temes d'interès, com per exemple individus, accions, missatge...), des del punt de vista d'un observador, significa que dins del sistema (que conformen aquests temes i possiblement d'altres) l'observador no pot distingir si els IoI estan relacionats o no. Per exemple, en un escenari amb més de dos individus, dos missatges enviats des del mateix conjunt

Referències

[1] Rachid Anane, Richard Freeland i Georgios Theodoropoulos. "E-voting requirements and implementation". A: Proceedings - The 9th IEEE International Conference on E-Commerce Technology; The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services, CEC/EEE 2007. 2007, p. 382 - 389. ISBN: 0769529135. DOI: 10.1109/CEC-EEE. 2007.42

[2] Roberto Araujo, Ricardo Felipe Custodio i Jeroen Van De Graaf. "A verifiable voting protocol based on Farnel (extended abstract)". A: Lecture notes in computer science (including its subseries "Lecture notes in artificial intelligence" and "Lecture notes in bioinformatics"). Vol. 6000 LNCS. 2010, p. 274 - 288. ISBN: 364212979X. DOI: 10.1007/978-3-642-12980-3_17

[3] Nicola Atzei, Massimo Bartoletti i Tiziana Cimoli. "A survey of attacks on Ethereum smart contracts (SoK)". A: Lecture notes in computer science (including its subseries "Lecture notes in artificial intelligence" and "Lecture notes in bioinformatics"). Vol. 10204 LNCS. 2017, p. 164 - 186. ISBN: 9783662544549. DOI: 10.1007/978-3-662-54455-6_8

[4] Marwa Mahmoud Badr, Amany Mahmoud Sarhan i Hatem Abdulkader. "Verifiable e-voting system with receipt-freeness". A: 2014 10th International Computer Engineering Conference: Today Information Society What's Next? ICENCO 2014. 2014. ISBN: 9781479952410. DOI: 10. 1109/ICENCO.2014.7050429

d'anonimat no són enllaçables per un observador. Això vol dir que la probabilitat que aquests dos missatges hagin estat enviats pel mateix individu és prou propera a

$$\frac{1}{\#\text{individus}}$$

on #individus és el nombre d'individus en el conjunt d'anonimat.

Per tant, l'existència d'anonimat implica la no enllaçabilitat. Cal destacar, també, que quan no és no enllaçable es diu que és enllaçable.

Pseudoanonimat: un pseudònim és un identificador d'un individu altre que el seu nom real. Un individu és pseudoanònim si utilitza el pseudònim en comptes del seu nom real. El pseudoanonimat és l'ús de pseudònims com a identificadors. Noteu que amb l'ús de pseudònims es pot garantir l'anonimat sense perdre l'enllaçabilitat sempre que s'utilitzi el mateix pseudònim i que no sigui pública la correspondència pseudònim / identitat real. De totes maneres, si s'abusa de l'ús d'un mateix pseudònim en diferents àmbits, un observador podria inferir aquest lligam i desfer l'anonimat.

Aquest estudi s'ha centrat en aquesta última solució: l'autenticació basada en atributs que garanteix més privacitat i control sobre les dades personals. A partir de l'inici dels anys 2000 s'han consolidat tot un seguit d'evolucions tecnològiques que han permès la implementació d'aquest tipus d'autenticació.

2.4. El sistema d'autenticació autogestionada (*self-sovereign identity*, SSI)

En l'apartat 2.3 s'han enumerat un seguit de solucions d'autenticació que presenten una sèrie d'inconvenients per als nostres objectius: d'una banda, la pèrdua del control per part de l'usuari i la disseminació a la xarxa tant de les dades d'autenticació com de les dades privades. De l'altra, la centralització de poder sense garantir ni preservar la privacitat, una certa facilitat de suplantació de la identitat i, finalment, punts febles o, dit d'una altra manera, punts suculents en què centrar els esforços d'atac. Així és com apareix, a principis del 2012 [34], el nou concepte de la identitat autogestionada (*self-sovereign identity)*, basada en atributs verificables, que pretén oferir una identitat portàtil per a qualsevol persona, organitzar un dispositiu que no

[5] Jan Camenisch i Anna Lysyanskaya. "An efficient system for non-transferable anonymous credentials with optional anonymity revocation". A: Advances in cryptology | Eurocrypt 2001. Ed. de Birgit Pfitzmann. Berlin, Heidelberg: Springer Berlin Heidelberg, 2001, p. 93 - 118. ISBN: 978-3-540-44987-4

[6] Thomas E. Carroll i Daniel Grosu. "A secure and anonymous voter-controlled election scheme". A: Journal of network and computer applications (2009). ISSN: 10848045. DOI: 10.1016/j. jnca.2008.07.010

[7] Orhan Cetinkaya. "Analysis of security requirements for cryptographic voting protocols (extended abstract)". A: ARES 2008 – *Proceedings of the Third International Conference on Availability, Reliability and Security*. 2008. ISBN: 0769531024. DOI: 10.1109/ARES.2008.167

[8] Veronique Cortier i Ben Smyth. "Attacking and xing Helios: an analysis of ballot secrecy". A: *Journal of computer security* (2013). ISSN: 0926227X. DOI: 10.3233/JCS-2012-0458

[9] Chin-Ling Chen et al. "A secure anonymous e-voting system based on discrete logarithm problem". A: Applied mathematics & information sciences 8.5 (set. 2014), p. 2571 - 2578. ISSN: 1935-0090. DOI: 10.12785/amis/080556. URL: http://www.naturalspublishing.com/Article.asp?ArtcID=5932

[10] Joost De Kruij i Hans Weigand. "Understanding the blockchain using enterprise ontology". A: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). Vol. 10253 LNCS. 2017, p. 29 - 43. ISBN: 9783319595351. DOI: 10.1007/978-3-319-59536-8_3

depengui de cap autoritat centralitzada, que mai no es pugui suplantar, i, a més, en què l'usuari tingui el control, en cada moment, del que vol desvelar i a qui ho vol revelar. En un sistema autogestionat (*self-sovereign)*, els usuaris existeixen independentment dels serveis. Christopher Allen resumeix els principis de l'SSI en deu punts [32]:

• Existència: els usuaris han de tenir una existència independent. El cor de tota SSI es basa, en última instància, en el "jo". L'objectiu d'una SSI ha de ser simplificar el fer públics i accessibles alguns aspectes d'aquest "jo" que ja existeix.

• Control: l'usuari ha de tenir el control de la seva identitat, gràcies a algoritmes criptogràfics segurs que garanteixen la vigència continuada de la seva identitat i el control de les seves dades personals.

• Accés: els usuaris han de tenir accés a les seves pròpies dades. Un usuari sempre ha de ser capaç de recuperar fàcilment totes les dades de la seva identitat.

• Transparència: els sistemes i els algorismes han de ser transparents. Els sistemes que s'utilitzen per administrar i operar una xarxa SSI han de ser oberts. Els algoritmes han de ser lliures, de codi obert, coneguts i com més independents de qualsevol arquitectura en concret millor.

• Persistència: les identitats han de ser de llarga durada. Preferiblement, les identitats han de durar per sempre o, com a mínim, el temps que l'usuari desitgi.

• Portabilitat: la informació i els serveis sobre la identitat han de ser transportables. Les identitats no les ha de tenir un SI de tercers, encara que sigui un SI de confiança que s'espera que funcioni en l'interès de l'usuari.

• Interoperabilitat: l'ús de les identitats hauria de ser tan ampli com sigui possible. Les identitats són de poc valor si només funcionen en nínxols limitats.

• Consentiment: els usuaris han d'acordar l'ús de la seva identitat. L'intercanvi de dades només s'ha de produir amb el consentiment de l'usuari.

• Minimalista: s'ha de minimitzar la divulgació d'atestats. Quan es publiquen dades, la revelació hauria d'incloure la quantitat mínima de dades necessària per dur a terme la tasca que es vol.

• Protecció: cal protegir els drets dels usuaris. Quan hi ha un conflicte entre les necessitats de la xarxa SSI i els drets dels usuaris individuals, la xarxa hauria de posar-se al costat de la

[11] Stephanie Delaune, Steve Kremer i Mark Ryan. "Verifying privacy-type properties of electronic voting protocols: A taster". A: Lecture notes in computer science (including its subseries "Lecture notes in artificial intelligence" and "Lecture notes in bioinformatics"). Vol. 6000 LNCS. 2010, p. 289 - 309. ISBN: 364212979X. DOI: 10.1007/978-3-642-12980-3_18

[12] Chun I. Fan i Wei Zhe Sun. "An efficient multi-receipt mechanism for uncoercible anonymous electronic voting". A: *Mathematical and computer modelling* 48.9-10 (2008), p. 1611 - 1627. ISSN: 08957177. DOI: 10.1016/j.mcm.2008.05.039

[13] J. Paul Gibson et al. "A review of e-voting: the past, present and future". A: *Annals of telecommunications* 71.7-8 (ag. 2016), p. 279 - 286. ISSN: 0003-4347. DOI: 10.1007/s12243-016-0525-8. URL: http://link.springer.com/10.1007/s12243-016-0525-8

[14] Wei Han, Dong Zheng i Ke Fei Chen. "Filling the gap between voters and cryptography in e-voting". A: *Journal of Shanghai Jiaotong University (Science)* 14 E.3 (2009), p. 257 - 260. ISSN: 10071172. DOI: 10.1007/s12204-009-0257-2

[15] D. Hardt. The OAuth 2.0 authorization framework. RFC 6749. http://www.rfc-editor.org/rfc/rfc6749.txt. RFC Editor, oct. del 2012.

[16] Freya Sheer Hardwick et al. "E-voting with blockchain: an e-voting protocol with decentralisation and voter privacy". A: (2018). ArXiv: 1805.10258. URL: http://arxiv.org/abs/1805.10258

[17] IBM. "Specification of the identity mixer cryptographic library". A: *Information Security* (2010), pàg. 1 - 52.

preservació de les llibertats i els drets de les persones per sobre de les necessitats de la xarxa.

2.4.1. Arquitectura d'identitat autogestionada (*self-sovereign identity*, SSI)

Els sistemes SSI es basen en el model de credencials verificables proposat pel W3C a [31]. Aquest model proposa diversos conjunts de definicions: conceptes, rols i elements. Primer, cal definir els conceptes sobre els quals es basa tot el model. L'identificador és una cadena de caràcters, cada entitat té un o un conjunt d'identificadors. Un atestat o *claim* és una asserció que algú fa sobre una identitat. Es defineix un conjunt d'actors: entitats que interactuen entre elles de manera segura i confiable. L'usuari o *holder* és una entitat independent que controla i posseeix els seus identificadors. Un emissor o *issuer* és l'entitat que certifica un atestat. Un consumidor o inspector és l'entitat que verifica o consumeix l'atestat. I un agent és una combinació de funcionalitats i emmagatzematge que es comunica via missatges amb d'altres agents. La seva funcionalitat permet interactuar i actuar en nom d'un usuari a través de regles de negoci.

Es defineixen també un conjunt d'elements: un magatzem de material d'autenticació, que s'anomena moneder o *wallet*, en què l'usuari guarda el material criptogràfic per a l'autenticació. Un registre distribuït d'identificadors (R_{id}) és qui guarda la correspondència entre l'identificador i la informació associada a aquest identificador, necessària per al funcionament del sistema. I un repositori d'atestats ($R_{atestats}$) és on els agents guarden els atestats. En aquest paradigma, el material d'autenticació es manté privat i les dades per permetre aquesta autenticació s'emmagatzemen de manera distribuïda en una base de dades accessible per a tothom que fa de registre d'identificadors. Per tant, cada usuari tindrà un o més identificadors d'aquests, que s'anomenen *distributed identifiers* (DID). La idea és que la comunicació es dugui a terme amb protocols d'extrem a extrem, que es fonamenten en el registre de DID (figura 1). Tant les dades d'autenticació (DA en la figura 1) com les dades privades (DP en la figura 1) són propietat de l'usuari i només s'intercanvien entre extrems. La custòdia de les dades és responsabilitat de l'usuari i és qui decideix quina informació vol compartir. Aquesta solució es basa en la utilització de criptografia asimètrica. Quan una part

[18] ISO Central Secretary. Information technology - Security techniques - A framework for identity management - Part 1: Terminology and concepts. Standard. Geneva, CH: International Organization for Standardization, 2011.

[19] Octavio Lazaro-Mancilla et al. "Paralelismo entre el método científico, los cinco procesos de un proyecto y el método de la ingeniería". A: *Academia Journals* (nov. 2014).

[20] Loi Luu et al. "Making smart contracts smarter". A: Proceedings of the ACM Conference on computer and communications security. Vol. 24-28 oct. 2016, p. 254 - 269. ISBN: 9781450341394. DOI: 10.1145/2976749.2978309

[21] Víctor Mateu, Josep M. Miret i Francesc Seb. "A hybrid approach to vector-based homomorphic tallying remote voting". A: *International journal of information security* (2016). DOI: 10.1007/s10207-015-0279-8. URL: http://www.mendeley.com/research/hybrid-approach-vectorbased-homomorphic-tallying-remote-voting

[22] David Mills et al. "Distributed ledger technology in payments, clearing, and settlement". A: *Finance and economics discussion series* 2016.095 (2016), p. 971 - 1023. ISSN: 19362854. DOI: 10.17016/feds.2016.095

[23] Tal Moran i Moni Naor. "Split-ballot voting: everlasting privacy with distributed trust". A: ACM Trans. Inf. Syst. Secur. (2010). DOI: 10.1145/1698750.1698756. URL: http://www.mendeley.com/research/splitballot-voting-everlasting-privacy-distributed-trust

[24] William Mougayar. *The business blockchain*. 2016, p. 180. ISBN: 9781119300311.

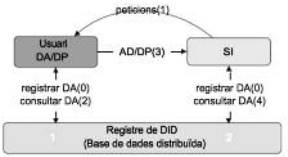

Figura 1. Autenticació amb SSI

A vol autenticar una altra part B, A envia una petició amb un *nonce* (un número aleatori que només ell coneix) a B. Aquesta petició es coneix com a repte. Quan B rep el repte, calcula la signatura amb la seva clau privada i la retorna a A (resposta al repte). Així, A pot verificar la signatura (resposta al repte) amb la clau pública de B. Aquest és el mecanisme d'autenticació que s'utilitza en aquest sistema, sense la necessitat de tenir una tercera part de confiança.

Explicació de la figura 1: (0) l'usuari i l'SI generen el seu identificador (DID) i els registren (registrar DA) juntament amb la seva clau pública a la base de dades distribuïda. Això només cal fer-ho una vegada durant tota la vida del DID, en el moment de la seva creació i abans d'utilitzar-lo per primer cop. (1) L'SI consulta el registre de DID i fa una petició (peticions), ja sigui d'autenticació o de DP de l'usuari. (2) L'usuari valida qui li ha fet la petició (consultar) amb criptografia asimètrica. (3) L'usuari, si la validació és correcta, respon a la petició (AD/DP) segons sigui la petició. (4) L'SI consulta el registre de DID i comprova, amb criptografia asimètrica, la resposta abans de processar-la.

Aquest tipus d'autenticació té un seguit d'avantatges i inconvenients:

- Avantatges: el sistema no depèn de cap tercer ja que el registre és distribuït. L'usuari és qui custodia les seves DP i les proporciona a qui vol i quan vol. A més, l'usuari és lliure d'utilitzar diferents DID i claus per als serveis.
- Inconvenients: és complex d'implementar; cal disposar d'una base de dades distribuïda. Fa ús de criptografia asimètrica que requereix potència de càlcul. La gestió dels DID i les claus associades és complexa. La recuperació en cas de pèrdua de les claus privades que ens identifiquen és difícil. I hi ha poca adopció; encara hi ha pocs sistemes que l'implementin.

3. Objectius

Després de l'estudi dels sistemes de votacions electròniques basades en la cadena de blocs (*blockchain*), s'han detectat dos punts de millora en els quals es basa aquesta recerca: l'autenticació i l'anonimat. L'autenticació no s'aborda en cap dels articles consultats ja que es delega a un tercer de confiança. I l'anonimat s'assoleix utilitzant algoritmes de barreja costosos, amb proves de correcció (proves matemàtiques conforme s'ha executat correctament l'algorisme).

Els objectius principals són:

• Obtenir un sistema de credencials anònimes amb atributs enllaçables.

• Utilitzar aquestes credencials en un sistema de votacions electròniques amb tecnologia de cadena de blocs (*blockchain*) i *smart contracts*, utilitzant el paradigma de la identitat autogestionada.

Així doncs, la recerca busca definir un sistema de credencials que parteix d'un protocol d'autenticació anònim basat en atributs i vol que aquests atributs siguin enllaçables sota certes condicions, a fi i efecte de poder utilitzar-lo en votacions electròniques. Aquest sistema l'anomenarem sistema d'identitats autogestionades anònimes amb atributs enllaçables. Per tant, es tracta, d'una banda, de proposar el càlcul d'un identificador anònim però únic, detectant un usuari que el vulgui utilitzar més d'un cop. Però també, per altra banda, de definir el protocol que garanteixi la transparència i robustesa, i impossibiliti el compromís de l'anonimat davant una conxorxa entre actors. Un cop definit el protocol i integrat dins de la identitat autogestionada, se'n vol provar l'ús en votacions electròniques sobre la cadena de blocs (*blockchain*), integrant-lo en un dels sistemes estudiats en la literatura.

En utilitzar el mètode d'enginyeria, s'han de definir un conjunt de requeriments que han de satisfer la solució trobada.

Els requeriments funcionals de les credencials amb atributs enllaçables són: les credencials seran atributs verificables; un cop emeses, seran anònimes i seran úniques sota certes condicions (per exemple, per a unes votacions donades). Es podrà enllaçar l'ús repetit d'un mateix atribut de les credencials sota certes condicions (per exemple, per a unes votacions donades). Un cop emeses serà l'usuari qui les custodiï.

Els requeriments funcionals del sistema de vot electrònic són: ser distribuït mitjançant tecnologia de cadena de blocs (*blockchain*) i *smart contracts*; ser resistent davant qualsevol component que actuï de manera maliciosa de manera individual o amb conxorxa amb d'altres, i ser eficient, anònim i escalable.

4. Metodologia

La metodologia proposada és el mètode d'enginyeria [19] que s'aplica a qualsevol desenvolupament i que utilitzen, per exemple, Kalpanan Singh i altres experts en l'article

[25] Andreas Pfitzmann i Marit Hansen. "Anonymity, unlinkability, undetectability, unobservability, pseudonymity and identity management - A consolidated proposal for terminology". A: Version v0 31 (febr. 2008).

[26] Kalpana Singh et al. "A novel credential protocol for protecting personal attributes in blockchain". A: Computers and electrical engineering 83. February (2020), p. 106586. ISSN: 00457906. DOI: 10.1016/j.compeleceng.2020.106586

[27] Melanie Swan. "Blockchain: blueprint for a new economy". 2015, p. 149. ISBN: 9781491920497.

[28] Marvin Van Wingerde. "Blockchain-enabled self-sovereign identity. An exploratory study into the concept self-sovereign identity and how blockchain technology can serve the fundamental basis self-sovereign identity management". Tesi doctoral 2017. DOI: 10.13140/RG.2.2.17693.82406. URL: https://www.researchgate.net/publication/326914271

[29] King-Hang Wang et al. "A review of contemporary e-voting: requirements, technology, systems and usability". A: Ubiquitous International 1.1 (2017), p. 31 - 47. ISSN: 2520-4165. URL: http://www.reo.gov.hk/pdf/20162017estimates/reo%7B%5C_%7Destimates%7B%5C_%7D1617-e.pdf%20http://www.ikelab.net/dspr-pdf/vol1-1/dspr-paper3.pdf

[30] Jan Willemson. "Bits or paper: Which should get to carry your vote?" A: Journal of information security and applications 38 (2018), p. 124 - 131. ISSN: 22142126. DOI: 10.1016/j.jisa.2017.11.007. URL: https://doi.org/10.1016/j.jisa.2017.11.007

[31] Brent Zundel et al. "Verifiable credentials data model 1.0. W3C Recommendation". https://www.w3.org/TR/2019/REC-vc-data-model-20191119/. W3C, nov. 2019.

[26]. Un cop establerts els requeriments, es fa un estudi teòric de la solució proposada del problema. Seguidament, un cop validada teòricament, es passa a implementar-la mitjançant una prova de concepte (PoC). Una PoC és una simulació d'un sistema real en un laboratori. Amb aquesta PoC es validen els resultats teòrics. Un cop contrastats i validats els resultats teòrics empíricament, s'instrumentalitza la PoC per recollir mesures per poder caracteritzar la solució; amb aquests resultats s'extreuen conclusions i s'avalua si la solució proposada compleix els requeriments inicials i si és viable. Finalment, amb el disseny teòric, la implementació i els resultats obtinguts s'elabora la tesi de la recerca. Aquesta recerca té dos objectius principals i s'ha dividit en les dos fases següents per arribar a aquests objectius.

4.1. Fase 1: Credencials anònimes enllaçables

Aquesta fase correspon al primer objectiu fixat en l'apartat 3: obtenir un sistema de credencials anònimes amb atributs enllaçables. Un cop fet l'estudi teòric del protocol descrit a "A novel credential protocol for protecting personal attributes in blockchain" [26] per Kalpanan Singh i altres, es pretén modificar-lo per permetre que els atributs siguin enllaçables en un àmbit donat sense perdre l'anonimat. Un cop fet això, es volen reproduir les proves experimentals dutes a terme en l'article esmentat abans i, aquest cop, tant sobre el protocol original com sobre el modificat per nosaltres.

Els resultats experimentals descrits a l'article són de dos tipus: un primer resultat binari que demostra empíricament que el sistema funciona, i un segon resultat que ens dona un temps de resposta del sistema per cada operació, fet que ens servirà per fer l'anàlisi comparativa entre les dos solucions. L'escenari que se simula correspon als casos d'ús, en què la Mònica demana primer una prova de majoria d'edat que utilitzarà després de manera anònima en una transacció sobre la cadena de blocs (*blockchain)*. Per simplicitat, totes les operacions criptogràfiques es duran a terme amb serveis web codificats en el llenguatge GO; els paquets de criptografia de GO seran els de la branca principal de GO, excepte per al paquet golang.org/x/crypto/bn256,[12] que es fa servir per a les operacions de *pairing* que s'importaran de GO sub-repository.[13]

12- bn256 · pkg.go.dev. 2020. URL: https://pkg.go.dev/golang.org/x/crypto/bn256 (cons. 26-1-2021).
13- Go Sub-Repository Packages - GoDoc. 2020. URL: https://godoc.org/-/subrepo (cons. 26-1-2021).

En el protocol apareixen quatre actors que modelarem de la manera següent:

• U es modela com una interfície de serveis web de la forma /us/<operació>.

• IV es modela com una interfície de serveis web de la forma /iv/<operació>.

• CP es modela com una interfície de serveis web de la forma /cp/<operació>.

• SP es modela com la transacció startTrading() a la cadena de blocs (*blockchain*). Aquesta transacció comprova l'atribut sense saber qui li està presentant, i si no pot verificar aquest atribut, rebutja la transacció.

La cadena de blocs (*blockchain*) que s'utilitza és Hyperledger Sawtooth,[14] que és l'escollida pels autors de l'article del protocol de referència. En aquest punt es codifica en el llenguatge Python[15] un programa que durà a terme totes les interaccions entre actors per finalment intentar fer la transacció startTrading(). Aquest programa ha de preveure els casos següents:

• Un usuari amb un atribut de majoria d'edat ! permet la transacció.

• Un usuari sense un atribut de majoria d'edat ! rebutja la transacció.

• Un usuari amb un atribut de majoria d'edat però expedit per a un altre usuari ! rebutja la transacció.

Els resultats d'aquest experiment ens donaran la validesa de la solució. Un cop validat el protocol, afegirem comptadors de temps a cadascuna de les operacions per poder emmagatzemar mesures del temps consumit a cada pas i fer un estudi estadístic comparatiu dels temps de resposta de cadascun dels protocols.

4.2. Fase 2: Integració d'un sistema de votacions electròniques remotes basades en la cadena de blocs (*blockchain*) i *smart contracts* amb un sistema d'identitats autogestionades

Per la seva part, aquesta fase es dividirà en dos blocs: la integració dels atributs enllaçables a un sistema SSI i la integració d'aquest SSI modificat amb un sistema de votacions electròniques remotes basades en *blockchain* i *smart contracts*.

14- Hyperledger Sawtooth - Hyperledger. 2020. URL: https://www.hyperledger.org/use/sawtooth (cons. 18-10-2020)

15- Welcome to Python.org. 2020. URL: https://www.python.org (cons. 28-1-2021).

4.2.1. Integració dels atributs enllaçables en una SSI

Per a aquest objectiu s'ha decidit utilitzar la implementació d'una cadena de blocs (*blockchain*) amb *smart contracts* orientada a la identitat autogestionada anomenada Hyperledger Indy,[16] que està dissenyada específicament per identitats descentralitzades. Aquesta identitat inclou un SDK (*software development kit)*[17] per interactuar amb ella i proporciona tota la infraestructura necessària pel que fa a la creació i el manteniment dels DID i els documents DID vistos en el marc teòric. Ofereix també mecanismes que proporcionen credencials anònimes però, com el protocol de referència, aquestes credencials anònimes són "massa" anònimes i no permeten la seva utilització en votacions electròniques.

Per tant, la nostra proposta, basant-nos en el protocol dissenyat i provat a l'apartat 4.1, tracta de dissenyar, implementar i provar un sistema de credencials anònimes enllaçables dins d'aquesta solució. Els passos que se seguiran són: es desenvoluparan les estructures de dades i *smart contracts* necessaris, així com l'SDK per interactuar amb ells.

L'escenari en què es provaran aquestes modificacions es basa en l'Indy Walkthrough[18] però amb els actors i amb els rols de l'apartat 2.2.1. Així, els actors de l'apartat 2.2.1 seran assimilats als del protocol de l'apartat 4.1 de la manera següent:

- El votant, assimilat a U, és qui obtindrà l'atribut verificable que li dona accés a les votacions.
- El registre civil, assimilat a IV, és qui valida la identitat del votant.
- El registrar o autoritat censal, assimilat a CP, és qui proporciona l'atribut verificable equivalent al dret de vot als votants.
- El *collector*, assimilat a SP, és qui rep aquest dret de vot de forma anònima i qui pot comprovar si ja s'ha exercit aquest dret.

Es farà un programa en Python similar al de l'apartat 4.1 que orquestri les interaccions entre els diferents actors i la cadena de blocs (*blockchain*), simulant l'autenticació, l'obtenció del dret a vot i l'ús d'aquest dret. En aquest cas, les operacions criptogràfiques es faran amb l'SDK desenvolupat. Per tant, estaran subjectes a les limitacions del client. Anàlogament a l'apartat 4.1, es farà l'experiment amb els mateixos paràmetres i es recopilaran els resultats, es validaran i s'extrauran les conclusions.

16- Hyperledger Indy - Hyperledger. 2020. URL: https://www.hyperledger.org/use/hyperledger-indy (cons. 18-10-2020).

17- GitHub - hyperledger/indy-sdk: Everything needed to build applications that interact with an Indy distributed identity ledger. 2020. URL: https://github.com/hyperledger/indy-sdk (cons. 28-1-2021).

18- indy-sdk/indy-walkthrough.md at master · hyperledger/indy-sdk · GitHub. 2020. URL: https://github.com/hyperledger/indy-sdk/blob/master/docs/getting-started/indy-walkthrough.md (cons. 28-1-2021).

4.2.2. Cas d'ús

Es proposarà i s'implementarà un sistema de votacions electròniques remotes basat en la cadena de blocs (*blockchain*) i *smart contracts*, utilitzant l'SSI amb atributs anònims enllaçables descrita a l'apartat 4.2.1. D'entre les opcions de sistemes de votacions electròniques remotes basades en *blockchain* i *smart contracts* trobades en la literatura, s'escollirà la que segons les seves característiques ofereixi més escalabilitat. Es modificarà aquest darrer sistema eliminant els processos que aporten les funcionalitats ofertes per la nostra solució o adaptant-ne d'altres per aprofitar les funcionalitats aportades. Per exemple, es pot eliminar el procés d'anonimització de butlletes i ja no caldrà accedir al cens electoral a l'hora de comprovar el dret a vot, que vindrà donat per l'atribut verificable.

5. Resultats esperats

Aquesta recerca busca demostrar que és possible donar drets a algú, que aquest algú pot exercir aquest dret de manera anònima, i que el fet de preservar el seu anonimat no implica que no sigui enllaçable. També s'espera que les modificacions proposades no en facin decaure el rendiment o el converteixin en inaplicable en aplicacions reals. Per tant, es vol obtenir un protocol de credencials anònimes basat en atributs verificables que permeti detectar l'ús repetit d'aquests atributs.

A l'hora d'escriure aquest article, la fase 1 de definició i validació del protocol ja està molt avançada. Els resultats obtinguts en els experiments efectuats fins avui deixen entreveure la viabilitat del sistema. El cost computacional és acceptable. S'està elaborant un article científic amb el material obtingut en aquesta fase que es presentarà en breu en una publicació científica internacional.

Amb aquests resultats, es vol implementar un sistema de votacions electròniques basat en la cadena de blocs (*blockchain*) i *smart contracts* que ofereixi l'anonimat del vot aprofitant la propietat desenvolupada d'autenticació anònima basada en atributs i amb atributs enllaçables. A més, aquesta identitat anònima serà autogestionada, i s'espera que sigui eficient a gran escala, i que tot i tenir atributs enllaçables, en cap moment no es perdi l'anonimat.

Referències en línia

[32] C. Allen. "The path to self-sovereign identity". [Online; accessed 30-January-2020]. 2016. URL: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[33] Fernando J. Corbato, Marjorie Merwin Daggett, Robert C. Daley. "An experimental time-sharing system". [Online; accessed 25-January-2020]. 1962. URL: http://larch-www.lcs.mit.edu:8001/~corbato/sjcc62/

[34] Moxie Marlinspike. What is "sovereign source authority"? [Online; accessed 10-March-2020]. 15-02-2012. URL: https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html

[35] Allison Matyus. "Facebook faces another huge data leak affecting 267 million users" | Digital trends. [Online; accessed 07-March-2020]. Des. 2019. URL: https://www.digitaltrends.com/news/facebook-data-leak-267-million-users-affected/

[36] OASIS. Security assertion markup language (SAML) V2.0 Technical overview. [Online; accessed 23-February-2020]. 2008. URL: https://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html

[37] Christian Paquin i Greg Zaverucha. U-Prove cryptographic specification V1.1 (Revision 3). Released under the open specification promise. [Online; accessed 23-February-2020]. Des. 2013. URL: https://www.microsoft.com/en-us/research/publication/u-prove-cryptographic-specification-v1-1-revision-3/

[38] Proof of Stake FAQ. [Online; accessed 16-February-2020]. Juny 2019. URL: https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ