Suggerimenti e ulteriori elementi utili per un affinamento della strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain

30 settembre 2020

Gruppo tematico CifrisChain
Iniziativa Nazionale De Componendis Cifris

Premessa

L'Italia decise nel 2018 di dotarsi di una **strategia nazionale in materia di tecnologie basate su registri condivisi e Blockchain** e quindi, nel dicembre dello stesso anno, il Ministero dello Sviluppo Economico selezionò una commissione ("gruppo di 30 esperti") che fu incaricata di fornire un quadro della situazione, identificare gli sviluppi della tecnologia blockchain e le conseguenze socio-economiche derivanti dall'introduzione di soluzioni basate sulla stessa.
Il risultato della commissione dovrebbe confluire in un documento "*Proposte per una strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain*", una cui prima sintesi è stata pubblicata[1] il 18 giugno 2020, data in cui è stata aperta una breve consultazione pubblica. Al termine della consultazione, il 20 luglio 2020, le osservazioni raccolte sono state comunicate alla commissione, per l'elaborazione della proposta finale della strategia.
Il documento di sintesi, oltre a riportare policy e strumenti sui temi connessi a queste tecnologie, individua alcuni casi d'uso e settori di applicazione, come ad esempio la tutela del *made in Italy* con una maggiore trasparenza per i consumatori.

L'iniziativa nazionale **De Componendis Cifris**, nata nell'ottobre del 2017, si pone l'obiettivo di animare la comunità crittografica Italiana, sia nelle sue componenti accademiche, sia nelle sue ramificazioni nel mondo del lavoro e dell'impresa. In particolare, la De Cifris auspica che l'Italia sviluppi e adotti cifrari (e schemi crittografici) robusti e flessibili, pronti ad accogliere nuove tecnologie e nuovi scenari applicativi. Con ricercatori di oltre trenta sedi universitarie e centri di ricerca, la De Cifris è ormai la community nazionale più rappresentativa nel panorama crittografico del Paese. Al suo interno operano alcuni gruppi tematici, tra cui **CifrisChain**. Visto che la blockchain è una delle applicazioni più importanti della Crittografia moderna, si ritenne opportuno creare **CifrisChain** per permettere agli esperti crittografi di esplorarne le potenzialità, come è stato fatto in due convegni nazionali e numerosi seminari.

In questo documento, **CifrisChain** vuole offrire alla commissione spunti e riflessioni, contando di fornire un valido contributo alla stesura del documento finale.

[1] https://www.mise.gov.it/images/stories/documenti/Proposte_registri_condivisi_e_Blockchain_-_Sintesi_per_consultazione_pubblica.pdf

Stesura di questo documento

Coordinamento

- Prof. Massimiliano Sala, professore ordinario presso l'Università degli Studi di Trento, Dipartimento di Matematica, Acting Director di **De Componendis Cifris**

- Prof. Ivan Visconti, professore ordinario presso l'Università degli Studi di Salerno, Dipartimento di Ingegneria dell'Informazione ed Elettrica e Matematica applicata, coordinatore di **CifrisChain**

Contributi

Hanno contribuito:

- Prof. Marco Baldi, professore associato presso l'Università Politecnica delle Marche, Dipartimento di Ingegneria dell'Informazione, coordinatore del gruppo tematico **PQCifris** (gruppo sui cifrari post-quantum)

- Prof. Norberto Gavioli, professore associato presso l'Università degli Studi dell'Aquila, Dipartimento di Ingegneria e Scienze dell'Informazione e Matematica, coordinatore del gruppo tematico **MathCifris** (gruppo sugli aspetti matematici della Crittografia)

- Dr. Phd Federico Pintore, Research Associate presso University of Oxford, Mathematical Institute

- Prof. Giovanni Schmid, Ricercatore presso CNR, ICAR - Scienze Computazionali e dei Dati (CDS Lab)

- Prof. Vincenzo Vespri, professore ordinario presso l'Università degli Studi di Firenze, Dipartimento di Matematica e Informatica

- Prof. Filippo Zatti, professore associato presso l'Università degli Studi di Firenze, Dipartimento di Scienze per l'Economia e l'Impresa

Indice

Suggerimenti e ulteriori elementi utili per un affinamento della strategia italiana in materia di tecnologie basate su registri condivisi e Blockchain

Cosa è una blockchain?

La versione originale di blockchain è ormai consolidata come quella proposta da Satoshi Nakamoto nel suo dirompente articolo e da lui sviluppata (congiuntamente con altri) nelle prime versioni di Bitcoin. Riassumendola dal punto di vista strutturale, si tratta di una lista concatenata di blocchi di dati tale che sia pubblicamente verificabile (tutti possono leggerla) e con storia immutabile (i blocchi già incorporati nella blockchain non possono essere modificati), ma che cresce nel tempo con l'aggiunta di nuovi blocchi. Caratteristica imprescindibile è l'uso della firma digitale, che quindi garantisce l'*identità* di chi scrive sulla blockchain (identità nel senso di possesso di una chiave crittografica privata). Tutto ciò rende la blockchain un'importantissima applicazione della Crittografia.
La "tecnologia blockchain" si è molto evoluta dalla proposta di Nakamoto, spinta sia dalle applicazioni sia soprattutto dall'evoluzione della scienza crittografica. Difatti, la blockchain del Bitcoin è ferma ad algoritmi crittografici degli anni '90, mentre gli ultimi 25 anni sono stati ricchi di **innovazioni crittografiche importanti** di rilevanza pratica, tra cui citiamo:
la **Crittografia post-quantum**, le **ring signature**, le **zero-knowledge proof**, la **secure multi-party computation**, la **Crittografia omomorfa** e la **functional encryption**.
Alcune di queste sono confluite in sistemi blokchain sperimentali di successo, tra cui citiamo Monero e Zcash, e la comunità scientifica le considera ormai potenti e collaudati strumenti, che tuttavia necessitano di **tre azioni governative**:

1. promuovere la loro **standardizzazione** (ora assente),
2. promuovere **formazione avanzata** (sono strumenti ignoti tranne che ai crittografi)
3. promuovere la loro **sperimentazione** su altri casi reali.

Vedremo ora alcuni aspetti che a nostro parere richiedono particolare attenzione, e poi riprenderemo la discussione su queste tre azioni.

Gruppo tematico CifrisChain
Iniziativa Nazionale De Componendis Cifris

Pubblica Verificabilità e Immutabilità

Le liste concatenate di blocchi e i registri distribuiti, intesi come archivi replicati tra più organizzazioni in modo da offrire resilienza ai tentativi di manomissione, sono solo due dei possibili approcci per realizzare sistemi (decentralizzati) pubblicamente verificabili.
In realtà la pubblica verificabilità può essere basata su meccanismi più flessibili che non impongono l'immutabilità, grazie all'uso di sistemi **crittografici più avanzati**. Applicazioni importanti non mancherebbero per sistemi di questo tipo, basta pensare alla conformità con la normativa europea GDPR, la cui applicazione incontra almeno due criticità connesse all'immutabilità del dato: il diritto all'oblio (che imporrebbe la cancellazione dei dati riferiti a un individuo) e la sostituzione di dati anonimizzati con altri (qualora i primi venissero deanonimizzati per eventi esterni, accidentali o dolosi).

Decentralizzazione e governance di una blockchain

Ci sono tre aspetti principali di governance di una blockchain:

1. decidere chi può interagire con la blockchain,
   nel Bitcoin e nelle altre blockchain pubbliche chiunque abbia un PC e una connessione Internet può farlo (totale decentralizzazione), nelle blockchain private c'è un'organizzazione che autentica i partecipanti autorizzati;
2. decidere chi crea il nuovo blocco nella catena,
   qui ci sono forti differenziazioni tra le blockchain esistenti, anche quelle pubbliche, con un grado altamente variabile di centralizzazione;
3. decidere chi decide, cioè, decidere le stesse regole di funzionamento,
   nel Bitcoin e altre blockchain pubbliche vi è un tentativo di meccanismo democratico, per cui le modifiche entrano in azione (teoricamente) solo dopo un'ampia discussione e un'approvazione quasi plebiscitaria delle stesse, mentre sia in certe blockchain pubbliche sia in tutte quelle private vi è un organismo (tipicamente una fondazione) che aggiorna man mano il software e quindi cambia le regole.

Come si vede, la "decentralizzazione" possiede molte sfaccettature e prima di dare un qualunque valore legale alle informazioni depositate su una blockchain, si rende necessario a nostro parere un suo esame approfondito, specialmente della governance de facto che si instaura, al di là dei propositi dichiarati. Questo esame non può prescindere da una comprensione profonda dei meccanismi crittografici interni: la tecnologia in questi contesti non è affatto neutra.

Pubblica Verificabilità e Confidenzialità

La pubblica verificabilità è un aspetto irrinunciabile in una blockchain, che però pare in conflitto con le esigenze di confidenzialità che nascono in molti contesti applicativi, come ovviamente quello medico-sanitario. Fortunatamente, i **sistemi crittografici avanzati** cui accennavamo permettono di coniugare questi due aspetti, come dimostrato in ZCash (crittovaluta che impiega **zero-knowledge proof**) e Monero (che impiega **ring signature**). Questa è un'ulteriore prova della potenza tuttora inespressa di questi **sistemi** (e non solo in ambito blockchain).

Servizi per il cittadino

In ambito europeo, con notevole ritardo rispetto alla nascita della tecnologia blockchain, è nata da poco l'interessante iniziativa European Blockchain Partnership, a cui il documento di sintesi spesso rimanda.
Pur apprezzando lo sforzo europeo, riteniamo la tecnologia blockchain matura per sostenere servizi pubblici trasparenti e comodi, come sempre più richiesti dai cittadini.
Tra questi servizi ne selezioniamo alcuni di evidente impatto e relativa semplicità realizzativa:

1. il voto elettronico; esistono moltissime categorie di voto, non si pensi solo alle elezioni politiche, ma anche alle votazioni in un'assemblea di un ente no-profit, alle elezioni per un Rettore in un ateneo, alla scelta di una commissione di concorso, etc.; attraverso queste tecnologie il voto elettronico può essere realizzato offrendo valide garanzie di sicurezza (se ben progettato), permettendo di esprimere il diritto di voto in contesti altrimenti complessi o poco agevoli (per esempio sostituire il voto per posta). A maggior ragione, emergenze sanitarie come quella che stiamo vivendo mettono sotto pressione i sistemi di voto tradizionali, che richiedono spostamento di persone, condivisione di oggetti e quindi un'organizzazione difficile e costosa, che rischia di scoraggiare molti votanti (soprattutto per piccole realtà). Non vediamo come un sistema di voto elettronico sicuro (e realizzabile su larga scala) possa evitare lo sfruttamento di **algoritmi crittografici avanzati**.

2. l'utilizzo su larga scala di dispositivi in possesso dei cittadini per realizzare un servizio digitale di impatto su tutta la comunità, grazie alla loro mutua interazione; il caso più lampante è il contact tracing che tante polemiche ha sollevato per il suo avvio affrettato dall'emergenza sanitaria. Un **protocollo crittografico avanzato**, analizzato scrupolosamente e dotato di rigorose **proof of security**, fornirebbe molte più garanzie agli utilizzatori, tranquillizzandoli, e certamente la sua adozione ne gioverebbe.
3. la notarizzazione di eventi di pubblico interesse, come l'ottenimento di lauree, di abilitazioni, della residenza, semplificherebbe enormemente le attuali procedure amministrative, ma si incaglia subito sulla dicotomia confidenzialità/pubblica verificabilità, che non si può superare con **metodi crittografici** antiquati. Alcune sperimentazioni già esistono, le quali spesso non sono state progettate con uso accorto della Crittografia e hanno talvolta fornito risultati deludenti, quindi rischiano di scoraggiare l'adozione di questi importantissimi servizi.

A nostro parere, non vi è dubbio alcuno che le blockchain possano essere molto utili per la pubblica amministrazione. Con gli opportuni accorgimenti (nulla vieta una gestione *permissioned* affidando la *governance* a entità pubbliche eterogenee) e gli opportuni **metodi crittografici avanzati**, si possono gestire i dati personali secondo i regolamenti vigenti (compreso il diritto all'oblio), nonché si possono salvaguardare le informazioni gestite da amministrazioni diverse, facendole collaborare senza necessità di condividere dati delicati (e.g., tramite **secure multi-party computation**), arrivando più in generale a una gestione del rapporto Stato-Cittadino basata su fiducia e trasparenza, senza sacrificare la privacy, senza minacciare le competenza e l'autonomia di nessuna amministrazione pubblica, senza costruire un sistema centralizzato omniconsciente (preda ideale di qualunque cyber criminale).

Sicurezza Post-Quantum

Le attuali blockchain potrebbero essere sovvertite da un quantum computer e non è da escludere che ciò accada tra alcuni anni, poiché gli schemi di **firma digitale** per validare le transazioni si basano su **sistemi crittografici** degli anni '90, che sono attaccabili con l'algoritmo di Shor, mentre l'**hash crittografico** (usato anche per le ***proof of work***) deve essere riconsiderato tenendo conto dell'algoritmo di Grover. SIccome le blockchain eventualmente adottate dalla PA ospiterebbero applicazioni pensate per durare nel lungo periodo, bisognerebbe esaminare con attenzione le iniziative già esistenti nel mondo accademico che mirano a progettare blockchain basate su **algoritmi crittografici post-quantum**, dunque sicure anche di fronte a un computer quantistico. Ancora una volta bisogna ricorrere a **schemi crittografici avanzati**.

Standardizzazione

Appare evidente, anche solo dalle brevi discussioni da noi intraprese poc'anzi, che un'operazione va fatta a monte, prima ancora di scegliere e quindi formalizzare un archetipo di blockchain da usare per la PA. Questa operazione è una standardizzazione dei **sistemi crittografici evoluti**, senza i quali le potenzialità della tecnologia blockchain rimarrebbero inespresse. Una volta fatto questo, allora si possono individuare in maniera rigorosa uno o più approcci teorici che permettono l'individuazione delle istanze più corrette ed efficienti della tecnologia blockchain, da calare nel contesto applicativo.
Il legislatore aveva previsto, all'interno del Piano Nazionale per la protezione Cibernetica e la Sicurezza Informatica approvato nel maggio del **2017**, la costituzione di un Centro Nazionale di Crittografia, nei cui compiti rientrano esplicitamente: "la progettazione di cifrari", "la realizzazione di un algoritmo nazionale" e, con grande anticipo sui tempi, "**la realizzazione di una blockchain nazionale**".
Indubbiamente il Centro sarebbe pienamente legittimato a standardizzare sia gli algoritmi crittografici avanzati sia le blockchain da utilizzare in ambito PA. Prendiamo atto che il Centro non è ancora stato costituito, nonostante varie iniziative di sollecito, compresi emendamenti presentati alla Camera dei Deputati. Non possiamo che auspicare la selezione in tempi brevi di organismi pubblici in grado di portare a compimento questa impegnativa opera di standardizzazione.

Alta formazione

C'è un grave ritardo nel finanziare programmi di crescita culturale e formativa sulla Crittografia in generale, e su queste sue applicazioni in particolare. Per colmare queste lacune, che rischiano di impedire al nostro Paese la piena fruizione della tecnologia blockchain, si ravvisa l'urgenza di indirizzare parte della formazione universitaria su questi temi. Visto il successo di iniziative locali molto focalizzate (in certi sedi i percorsi specialistici crittografici della laurea magistrale sono subissati da domande di immatricolazione), spinte da un dirompente interesse da parte dei giovani, non è impensabile l'istituzione di percorsi formativi verticali. Mentre certamente è auspicabile avere almeno un corso su questi temi all'interno dei percorsi di laurea in Matematica, Informatica e (alcuni tipi di) Ingegneria, bisognerebbe intraprendere azioni più

coraggiose che spingano a lauree e/o Master, anche multidisciplinari e aperte a discipline come l'Economia o il Diritto. A completare il ciclo formativo non può mancare l'istituzione di una o più scuole di dottorato di respiro nazionale.
Tutto ciò è però impossibile nell'attuale penuria di esperti, a mano che non si attivino specifici programmi per giovani ricercatori, invertendo quindi la rotta attuale che incoraggia i giovani a lasciare il nostro Paese.
Non bisogna trascurare però la base: è importante educare il cittadino alla scelta consapevole di servizi che la sicurezza informatica mette a disposizione. Troppo spesso si presuppone che l'utente abbia un minimo di familiarità con il mezzo con cui si confronta, perciò riteniamo che un'educazione alla sicurezza digitale, per quel che riguarda le basi minime del suo utilizzo e del suo funzionamento, faccia parte di un bagaglio indispensabile al cittadino contemporaneo e che debba entrare di tutto diritto a far parte della sua formazione sin dall'istruzione secondaria superiore.

Sperimentazione

Nelle nostre analisi fin qui svolte abbiamo volutamente trascurato un aspetto delle blockchain che è fonte di dissenso insanabile: l'algoritmo di consenso (nella nostra precedente terminologia: "chi aggiunge un blocco nuovo alla catena?"). Sebbene siano complicati da studiare e integrare tra loro, le funzionalità della blockchain che sfruttano **algoritmi crittografici avanzati** sono, nella loro generalità, ben chiari ai crittografi esperti. Altrettanto non si può dire su quale sia il migliore *consensus algorithm*.
Pur supponendo che qualche ente si prenda carico della **standardizzazione** accennata precedentemente, rimane il problema di calare i modelli teorici nelle realtà implementative. Questa inderogabile esigenza di un'ampia ed estesa **sperimentazione** incontra lo stesso limite dell'**alta formazione**, cioè la cronica mancanza di esperti crittografi, in un circolo vizioso che si può rompere solo con una decisa e mirata azione governativa.