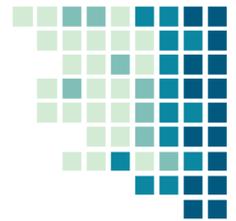




Associazione Blockchain Italia

Non profit per la ricerca interdisciplinare e la divulgazione scientifica sulle tecnologie blockchain



OSSERVAZIONI AL DOCUMENTO MISE

PROPOSTE PER LA STRATEGIA ITALIANA IN MATERIA DI TECNOLOGIE BASATE SU REGISTRI CONDIVISI E BLOCKCHAIN

SINTESI PER LA CONSULTAZIONE PUBBLICA

20 LUGLIO 2020

Preambolo

Il presente documento contiene le osservazioni dell'*Associazione Blockchain Italia (ABI)* al documento [Sintesi della strategia nazionale](#) posto in consultazione dal MISE in data 18 giugno 2020.

ABI è un ente senza scopo di lucro per la ricerca interdisciplinare e divulgazione scientifica che raduna esperti di varie discipline accomunati da competenza e vivo interesse sulle tecnologie a registro distribuito. Il suo scopo è quello di studiare la praticabilità e le implicazioni sociali, economiche, legali e tecniche connesse all'adozione di tecnologie blockchain e DLT favorendo il dialogo tra professionisti, accademici, esponenti del mondo imprenditoriale ed istituzioni. L'obiettivo a lungo termine dell'Associazione è di promuovere nel nostro Paese un ecosistema in grado di migliorare la competitività internazionale e di favorire l'iniziativa pubblica e privata.

Le osservazioni qui espresse sono state elaborate nell'ambito di un **tavolo tematico** costituito in seno all'Associazione il 18 giugno stesso per la discussione dei temi sollevati dal documento in consultazione. Gli associati hanno partecipato ai lavori con frequenza ed entusiasmo.

Questa Associazione esprime apprezzamento per il lavoro svolto dal MISE di preliminare inquadramento del fenomeno blockchain/DLT e del possibile impiego di risorse per lo sviluppo e applicazione di questa tecnologia. Oltre che con le presenti osservazioni, ABI si augura di poter fornire anche in futuro il proprio contributo alla strategia nazionale.

ASSOCIAZIONE BLOCKCHAIN ITALIA

No-profit per la divulgazione e ricerca scientifica sulle tecnologie blockchain
Via Correggio, 43 | 20149 Milano | C.F. e P.IVA 10411240962
www.associazioneblockchain.it | info@associazioneblockchain.it



Sommario

Preambolo	1
Osservazioni al documento	1
2.1.1 Italia e Blockchain/DLT	1
2.1.2 Quadro comunitario e collaborazione internazionale	1
2.1.4 Sperimentazioni.....	2
2.2 Sviluppo dell'economia circolare	2
2.3 Settori chiave verso cui indirizzare gli investimenti nel settore privato, fintech e modelli cooperativi.....	3
2.5 Raccomandazioni d'uso sulle differenti tipologie di DLT	5
2.7 Filiere 4.0	6
2.8 Raccomandazioni in merito all'adeguamento delle infrastrutture.....	7
2.11 Raccomandazioni relative alla value chain del cripto attività	7
2.12 Raccomandazioni relative all'applicazione della normativa antiriciclaggio	8
2.22.3 Identità digitale	8
2.22.4 Fonti certificative pubbliche.....	8
2.22.5 Sanità.....	9
2.22.7 E-procurement	9
2.22.8 Smart Contract e digitalizzazione dei servizi	9
Appendice: Sanità.....	→10

* * * * *



Osservazioni al documento

Per consentire un facile e immediato riferimento alle singole **raccomandazioni**, le **osservazioni** di seguito formulate seguono l'ordine espositivo e l'indice del documento in consultazione. Ciascuna osservazione è preceduta da una breve motivazione.

2.1.1 Italia e Blockchain/DLT

Considerato che le DLT, in via generale, introducono nuovi paradigmi tecnologici, organizzativi e concettuali, si raccomanda di sottolineare l'impegno del Paese alla riduzione del digital-divide.

OSSERVAZIONE #1

A fine elenco, aggiungere:

«7. L'Italia si impegna a ridurre il digital-divide legato all'adozione di tecnologie innovative favorendo campagne di sensibilizzazione, adozione e conoscenza delle tecnologie blockchain in modo da sviluppare un ecosistema capace di fornire pari opportunità».

2.1.2 Quadro comunitario e collaborazione internazionale

*La presente raccomandazione, al paragrafo 2, sottolinea giustamente l'importanza della protezione dei dati personali e l'esigenza della loro tutela nello sviluppo di soluzioni blockchain. A tale riguardo propone **nuove interpretazioni** ed eventuali **aggiornamenti** del **GDPR** per tener conto della natura decentralizzata e delle caratteristiche di immutabilità della tecnologia Blockchain/ DLT.*

OSSERVAZIONE #2

Questa Associazione non ritiene che siano necessarie né modifiche normative né nuove interpretazioni in quanto non ravvisa alcuna *incompatibilità ontologica* tra soluzioni blockchain e GDPR nella sua consolidata lettura, anche con riguardo ad architetture *permissionless*.

Tale convinzione poggia sulla corretta interpretazione della nozione di dato personale e di dato soggetto a tecniche di pseudonimizzazione come anche chiarito nel parere n. 4 del 20 giugno 2007 (WP136) del vecchio Gruppo di Lavoro ex articolo 29 (art. 29 della Direttiva 95/46/CE – Working Party). Si ravvisa infatti che i digest delle funzioni hash non possono considerarsi dati personali in sé laddove la *lista di corrispondenza* contenente il riferimento alle persone fisiche ad essi associate non sia a disposizione del pubblico¹.

Recentemente, in modo conforme a quanto sopra accennato, si sono espresse anche l'Agencia Española Protección Datos (AEPD) e lo European Data Protection Supervisor (EDPS) nel lavoro congiunto *Introduction to the Hash Function as a Personal Data Pseudonymisation Technique* (2019, §§ VI e VII a pag. 22).

Tutto ciò premesso, residuano senz'altro dei rischi connessi allo sviluppo di piattaforme DLT incompatibili con le disposizioni del GDPR². Tali progetti, considerata la loro natura decentralizzata e idoneità a prestarsi a condotte di stampo criptoanarchico, non potrebbero essere impediti da

¹ Per dirimere ogni incertezza sulla nozione di dato personale, il parere del WP29 propone un test articolato in tre step: *contenuto*, *scopo* e *risultato*. Per un approfondimento si rinvia a F. Rampone, *I dati personali in ambiente blockchain tra anonimato e pseudonimato*, in *Cyberspazio e diritto*, vol. 19, n. 61 (3-2018), pp. 457-478 (su SSRN in versione in lingua inglese).

² Anche il Parlamento Europeo, nella Risoluzione del 3 ottobre 2018, ha suggerito che nell'ambito dello studio delle DLT si affrontino adeguatamente le problematiche attinenti la protezione dei dati personali, soprattutto in ordine alla necessità di garantire il diritto all'oblio, riservando particolare attenzione ai principi di accountability o di privacy by design introdotti dal GDPR.



alcuna normativa punitiva. Questa Associazione crede piuttosto che certificazioni di tipo “*GDPR compliance*” possano essere assai più efficaci indirizzando il pubblico verso soluzioni sicure, funzionando al tempo stesso da stimolo per una crescente attenzione ai temi privacy in questo settore.

Si suggerisce pertanto la costituzione di un **comitato di esperti** presso il Garante per la protezione dei dati personali (composta da giuristi e informatici esperti di DLT) per la redazione di linee guida e buone prassi da seguire per la realizzazione di piattaforme e soluzioni blockchain rispettose della privacy.

A tale proposito, ABI è pronta ad offrire il proprio contributo considerato che alcuni gruppi di lavoro al suo interno stanno già affrontando il tema dei requisiti generali di compatibilità privacy-blockchain.

2.1.4 Sperimentazioni

*Questa Associazione fa fatica a riconoscere in via generale la necessità di istituire **sandbox normative** come ambiti giuridicamente definiti nei quali, in deroga alle disposizioni vigenti, si possa realizzare un progetto blockchain. Invero, si ritiene che lo sviluppo di soluzioni blockchain possa (e anzi debba) svolgersi nei limiti di legittimità del quadro legislativo e regolamentare esistente, fermo restando che sono sempre possibili interventi modificativi dell’ordinamento per rimuovere ostacoli normativi, da valutare caso per caso.*

OSSERVAZIONE #3

Eliminare la raccomandazione. In alternativa, indicare quali sono gli ostacoli normativi che impediscono lo sviluppo di progetti blockchain e chiarire il contenuto e il funzionamento di una possibile sandbox normativa in grado di rimuovere tali ostacoli.

2.2 Sviluppo dell’economia circolare

*Non è chiaro, come sostenuto nella presente raccomandazione, in che senso le «Blockchain/DLT, possono giocare un ruolo importante nell’economia circolare per la definizione e abilitazione di **modelli sostenibili** di produzione e consumo in grado di indirizzare gli interessi di tutti gli attori dell’ecosistema, e in particolare del cittadino/consumatore, verso la loro introduzione a tutela dell’ambiente».*

Si sottolinea peraltro, che per iniziativa privata si stanno sviluppando modelli di governance per rimodulare gli obiettivi di impresa verso interessi sociali e sostenibilità ambientale (es.: assessment per benefit corporation)

OSSERVAZIONE #4

Si richiama l’attenzione anche al New Circular Economy Action Plan, varato dalla Comunità europea a marzo 2020, ove viene ribadito, per i settori chiave dell’economia circolare identificati, l’importanza di un *product passport*, di un *resource mapping* e di una *consumer information*. L’Action Plan identifica con un piano di lavoro misurabile i settori chiave dell’economia circolare ed essendo un progetto europeo guiderà gli effort degli Stati Membri.

*L’impiego di utility token per promuovere **comportamenti virtuosi dei cittadini** si presta a soluzioni potenzialmente incompatibili con i diritti fondamentali dell’individuo. Anche escluso questo caso, l’incentivazione verso particolari condotte “virtuose” delle persone fisiche rischia di indirizzare la popolazione verso l’uniformità culturale e l’ortodossia sociale.*

OSSERVAZIONE #5

Lo Stato non dovrebbe attribuire utility token ai cittadini «per promuovere l’adozione di **comportamenti virtuosi**», ma solo quale controprestazione per particolari servizi resi alla



comunità attraverso apposite iniziative di cittadinanza attiva (es.: pulizia di aree pubbliche, servizi di didattica e di assistenza).

Gli utility token potrebbero invece essere utilizzati con minori restrizioni per incentivare le condotte virtuose di persone giuridiche, ad esempio per il perseguimento degli obiettivi dell'Agenda 2030 o per il rilascio e la circolazione di certificati ambientali.

Per individuare tali servizi, si raccomanda di promuovere delle "call for innovation" per coinvolgere in maniera sistematica Startup e PMI innovative in progetti con organismi pubblici.

2.3 Settori chiave verso cui indirizzare gli investimenti nel settore privato, fintech e modelli cooperativi

*Raccomandiamo di accogliere nella Strategia Nazionale le seguenti osservazioni in merito all'uso delle tecnologie in oggetto in modo da orientare le politiche di sviluppo economico nella direzione di quelle che sono secondo noi le migliori **leve economiche e competitive** per il sistema paese.*

- Agroalimentare, Made in Italy e Terziario avanzato

L'Associazione ha costituito diversi tavoli di lavoro tematici fra i quali uno avviato a giugno 2019 ed ancora in corso dedicato alla tracciabilità agroalimentare blockchain-based, ritenendo questo settore come strategico per il sistema Paese. Obiettivo del suddetto tavolo è lo sviluppo di un white paper da presentare alle istituzioni e al comparto industriale nel quale saranno individuate le linee guida per l'applicazione della tecnologia blockchain al settore, in relazione anche all'armonizzazione delle numerose proposte di legge regionali approvate, presentate o ancora in corso di valutazione.

OSSERVAZIONE #6

Riteniamo fondamentale lo sviluppo di standard nel settore **Agroalimentare** per la definizione delle ontologie e dei vocabolari controllati a supporto dell'interoperabilità tra sistemi informativi eterogenei pubblici e privati di cui il paese ha urgente necessità. Le blockchain ci aprono nuove possibilità di pensare e di supportare nuovi ragionamenti di sistema fra vari attori; ne raccomandiamo l'uso come tecnologie d'elezione per lo sviluppo di nuovi modelli basati su logiche consortili per la valorizzazione sia delle nostre produzioni d'eccellenza sia del nostro tessuto imprenditoriale locale (a partire dai presidi agroalimentari DOP locali organizzati in consorzi di produttori fino allo sviluppo della rintracciabilità reale e completa di filiera). Individuiamo nell'applicazione delle tecnologie blockchain a nuove logiche consortili una delle leve economiche di maggior rilievo nazionale per lo sviluppo e la valorizzazione dei prodotti agroalimentari italiani riuscendo a contrastare contesti di concorrenza fortemente alterati da grandi investimenti in marketing per riportare l'attenzione sulla qualità del prodotto (eccellenza italiana). Promuoviamo le tecnologie blockchain come enabler principale per il passaggio da logiche di storytelling in favore di logiche di fact-checking effettivo e completo, prevedendo a contorno la pianificazione di campagne nazionali ed internazionali di sensibilizzazione dei consumatori su questi aspetti.

Le considerazioni espresse per il settore Agroalimentare sono direttamente traslabili e applicabili al **Made in Italy** in quanto rappresentative degli stessi meccanismi legati alla rintracciabilità dei prodotti e allo sviluppo di nuovi modelli di governance. Nello specifico, il Made in Italy potrà avere ulteriore vantaggio dallo sviluppo di un supporto normativo moderno dedicato all'implementazione di Organizzazioni Autonome Decentralizzate (DAO) a diretto supporto dei distretti produttivi olonico virtuali (un tempo eccellenza italiana).

Le stesse considerazioni da noi espresse per il Made in Italy in particolare in merito alle DAO e alle **reti olonico-virtuali** valgono per il **terziario avanzato e modelli cooperativi** in quanto legate agli stessi meccanismi appena discussi.



- Infrastrutture critiche. Comunicazioni elettroniche

OSSERVAZIONE #7

Riteniamo importante evidenziare che le tecnologie blockchain sono riconosciute come middleware di sicurezza per l'IoT, specialmente se implementate in concomitanza all'uso dei TEE (*Trusted Execution Environment*).

- Reti energetiche

La rete elettrica attinge in maniera indifferente e indistinguibile da fonti fossili e fonti rinnovabili per cui esiste un sistema complesso e parallelo ai marketplace di commodities per il trasferimento dei certificati di sostenibilità ambientale (es.: green assets, carbon credits).

Le stime più accreditate prevedono che la richiesta di energia elettrica crescerà del 30% entro il 2040, soprattutto per via della trasformazione della mobilità da fonti fossili a mobilità elettrica e che la rete elettrica nazionale si sta trasformando progressivamente da rete centralizzata a rete decentralizzata dove l'interazione con le produzioni locali si trasformerà in un rapporto bidirezionale di consumo e cessione di energia verso la rete nazionale (grid) e locale (micro-grid).

OSSERVAZIONE #8

Considerato l'aumento di domanda di energia elettrica³, nonché l'importanza strategica delle politiche a lungo termine di sostenibilità ambientale e riduzione delle emissioni di CO₂, si raccomanda lo sviluppo di un sistema di rintracciabilità blockchain-based dei green assets promosso dallo Stato al fine di favorire lo sviluppo di un ciclo virtuoso legato alla rintracciabilità e trasparenza delle informazioni di sostenibilità.

- Incentivazione di comportamenti virtuosi in coerenza con gli SDG (Sustainable Development Goals)

La promozione di comportamenti virtuosi attraverso l'attribuzione di token può essere preteso, anche nella prospettiva degli SDG, solo verso le persone giuridiche e non anche verso le persone fisiche le quali godono di un grado di tutela dei diritti fondamentali non mutuabile al mondo delle imprese.

OSSERVAZIONE #9

Si raccomanda di valutare attentamente il rischio di potenziale tecnocontrollo prima di promuovere meccanismi di incentivazione delle condotte "virtuose" delle persone fisiche. A tale riguardo, si rinvia a quanto già osservato al precedente paragrafo 2.2.

- Costruzioni Edili - Estensione BIM

A settembre 2019, questa Associazione in collaborazione con l'Associazione TSEI ha costituito un tavolo di studio congiunto per lo studio di soluzioni blockchain nel settore real estate. I lavori sono terminati lo scorso giugno, dopo oltre otto mesi di intenso e vivace scambio culturale tra le due associazioni, dando vita al progetto REChain, presentato nel corso del convegno annuale TSEI 2020⁴.

REChain (aperto alla partecipazione di tutti gli attori della filiera immobiliare, pubblica amministrazione inclusa) ha la particolarità di considerare l'immobile sotto molteplici prospettive: unità abitativa, garanzia reale, sottostante di prodotti finanziari, elemento produttivo di un'azienda, oggetto di esecuzioni immobiliari, ecc. Questa molteplicità di vedute è la principale caratteristica di REChain e offre una soluzione ad alcuni annosi problemi che affliggono il comparto immobiliare, motore dell'economia dell'intero Paese.

³ Rif. <https://www.iea.org/reports/world-energy-outlook-2019/electricity>

⁴ Il rapporto descrittivo del progetto REChain è reperibile sul sito ABI www.associazioneblockchain.it.



REChain, peraltro, sfrutta la tecnologia blockchain proponendo un nuovo modello di governance delle informazioni immobiliari passando da un'impostazione gerarchica, proprietaria e frammentata ad una orizzontale, partecipativa e comune tra tutti gli attori della filiera.

Diversi soggetti hanno già espresso interesse a partecipare allo sviluppo di REChain. Questa Associazione sarebbe lieta di **presentare al MISE il progetto** più nel dettaglio.

OSSERVAZIONE #10

La raccomandazione in commento fa riferimento all'impiego della blockchain nel **BIM (Building Information Modeling)**. Tuttavia, si tratta di un'applicazione a **vocazione prettamente privata** più che pubblica, peraltro già esplorata in numerose pubblicazioni e senz'altro oggetto di sperimentazioni già in corso.

Con riguardo al settore real estate, la strategia nazionale dovrebbe piuttosto occuparsi di soluzioni blockchain in una "prospettiva pubblica", ovvero avendo riguardo al governo del territorio, alla mappatura del patrimonio immobiliare, alla razionalizzazione dei processi nell'ambito delle esecuzioni immobiliari, all'accesso e formazione dei titoli abilitativi, alla costituzione, estinzione e trasferimento di diritti reali.

2.5 Raccomandazioni d'uso sulle differenti tipologie di DLT

In via generale, l'intera raccomandazione è poco chiara.

Essa, tuttavia, pare distinguere solo tra soluzioni permissionless e permissioned trascurando il ruolo fondamentale che possono assumere le soluzioni ibride ovvero piattaforme blockchain integrate con sistemi informativi tradizionali. Inoltre, è importante precisare che le tecnologie permissionless non sono tecnologie appartenenti alla "cosa pubblica", ma di fatto sono solo pubblicamente accessibili e mantenute da soggetti anonimi dislocati in ogni parte del mondo.

Ciò detto, le blockchain pubblicamente accessibili, come Bitcoin o Ethereum, si evolvono sulla base delle decisioni di soggetti (anonimi o fondazioni) che operano su un piano di diritto privato e sfuggono in generale a qualsiasi giurisdizione o, nel migliore dei casi, sfuggono al potere di controllo e sindacato dell'autorità nazionale.

OSSERVAZIONE #11

Questa Associazione non ritiene che in generale si debbano compiere scelte aprioristiche tra soluzioni permissionless e permissioned.

Peraltro, per i servizi della pubblica amministrazione, si può fare ricorso a piattaforme pubblicamente accessibili promosse e governate da soggetti pubblici italiani o europei (es.: EBSI) che mantengono la caratteristica di controllo sull'evoluzione della piattaforma.

Gli attuali **algoritmi di crittografia** impiegati dalla maggior parte delle blockchain sono raccomandati come sicuri dai maggiori organismi internazionali come il NIST o il BSI fino al 2030 con il rischio che i dati personali inseriti oggi in una blockchain possano essere decriptati da elaboratori tradizionali fra uno o due decenni. Va inoltre aggiunto che la comunità scientifica internazionale sta studiando algoritmi quantum-resistant in grado di resistere alla decodifica pressoché immediata di dati, protetti da tradizionali algoritmi, da parte di nuovi calcolatori quantistici che potrebbero vedere la luce anche prima del prossimo decennio.

OSSERVAZIONE #12

Questa Associazione ritiene fondamentale sottolineare che le attuali tecniche di pseudonimizzazione, considerata l'obsolescenza degli algoritmi in uso⁵, non possono garantire la tutela delle persone fisiche in ordine alla loro riservatezza e trattamento dei dati personali. Si raccomanda pertanto un'attenta valutazione delle architetture e dei processi di aggiornamento

⁵ Rif. <https://www.keylength.com/en/>



delle misure di sicurezza richiamando l'importanza sui principi di privacy by design e svolgendo regolari data protection impact assessment.

Queste considerazioni depongono a favore dell'adozione di soluzioni permissioned o ibride nelle quali le liste di corrispondenza dei dati personali siano accessibili solo a soggetti determinati e individuati a cui attribuire il ruolo e le responsabilità di **titolare del trattamento** o di **responsabile del trattamento**. Come già accennato, questa Associazione sta lavorando a schemi di compatibilità tra soluzioni blockchain e GDPR e sarebbe lieta di condividere le proprie riflessioni con un costituendo comitato di esperti di cui si ravvisa l'opportunità presso l'autorità Garante per la protezione dei dati personali (vedi sopra, § 2.1.2).

- *diritti e proprietà intellettuale preferibilmente appartenenti ad associazioni non profit, enti di ricerca o università supportate dalla comunità open source*

OSSERVAZIONE #13

È opinione di questa Associazione che lo Stato non debba perdere il potere di controllo sull'evoluzione della piattaforma tecnologica **mantenendo diritti e proprietà intellettuale** dei nuovi sviluppi ovvero dando preferenza a soluzioni *open source*.

Peraltro, già da tempo questi temi sono stati affrontati e risolti anche in sede europea con l'adozione delle licenze EULA di cui, quindi, si raccomanda l'adozione.

- *organizzazione, controllo e ownership dell'infrastruttura stabilita da regole, pratiche e processi automatizzati e non direttamente da singole entità*

OSSERVAZIONE #14

L'automazione dei processi di corporate governance risponde un'idea, peraltro utopica, di stampo cryptoanarchico che non trova riscontro nella pratica (se non in termini limitatissimi, es.: *onboarding*) e che non è compatibile con gli assetti istituzionali di uno stato democratico.

- *sistema di incentivo al mantenimento della sicurezza dell'infrastruttura incorporato nel protocollo*

La sicurezza di una piattaforma blockchain della pubblica amministrazione non deve essere garantita secondo logiche premiali tipiche di progetti permissionless. Le soluzioni permissioned o ibride permissionless-permissioned (ovvero interoperanti con piattaforme tradizionali) costituiscono probabilmente un miglior punto di equilibrio tra esigenze di sicurezza, rispetto della normativa, enforcement della stessa e perseguimento di interessi pubblici. La pubblica amministrazione ha il compito di verificare e adattare le misure di sicurezza assumendosi la responsabilità del controllo e dell'evoluzione del sistema.

OSSERVAZIONE #15

Questa Associazione ritiene che la sicurezza di un'infrastruttura blockchain adottata dalla pubblica amministrazione debba essere garantita con assunzione diretta della responsabilità degli organismi pubblici coinvolti. La sicurezza, resilienza e verifica del funzionamento del sistema informativo, può essere piuttosto aumentata attraverso l'ampia partecipazione di nodi indipendenti.

2.7 Filiera 4.0

La presente raccomandazione, per affinità dell'argomento trattato, può sistematicamente essere inserita nel § 2.3. del documento di sintesi.



OSSERVAZIONE #16

Si raccomanda di riorganizzare il documento di sintesi considerato che Filiere 4.0, Made in Italy e Agroalimentare sono tutti settori riconducibili agli stessi concetti di rintracciabilità e nuovi modelli di governance. Le Filiere sono la generalizzazione delle filiere agroalimentare così come il Made in Italy è una specializzazione della filiera su prodotti esclusivamente italiani.

2.8 Raccomandazioni in merito all'adeguamento delle infrastrutture

- Cybersecurity

Quest'Associazione evidenzia la necessità dell'adeguamento capillare delle attuali infrastrutture di rete nazionali alla banda larga per evitare l'incremento del digital-divide legato all'accesso ai servizi resi con modalità innovative.

OSSERVAZIONE #17

Alla luce della natura tuttora altamente sperimentale delle tecnologie che si ispirano alla blockchain (inclusi *smart contracts* e *distributed applications*), si richiama l'attenzione sull'opportunità di valutare preliminarmente l'adozione di soluzioni tecnologiche già consolidate, basate su standards e best practice riconosciuti in ambito cybersecurity. Il confronto con le soluzioni tecnologiche consolidate fornirà inoltre un criterio di paragone nella valutazione delle caratteristiche di integrità, sicurezza, scalabilità e continuità delle soluzioni blockchain-based proposte.

Solo qualora le soluzioni tecnologiche consolidate non dovessero dimostrarsi adeguate al conseguimento degli obiettivi che si intende perseguire, si valuterà l'opportunità di adottare soluzioni blockchain-based, documentando le motivazioni che inducono a preferire queste ultime.

Particolare attenzione dovrà essere prestata alla definizione e valutazione della superficie di attacco (attack surface) potenziale correlata all'adozione delle soluzioni tecnologiche blockchain-based, e alle distributed applications, tenendo conto delle criticità derivanti dalla possibile emersione di "catastrophic bugs" nello sviluppo applicativo di queste ultime.

Alla luce delle medesime considerazioni svolte al paragrafo 2.5 relative alla sicurezza nel tempo degli algoritmi di crittografia, si raccomanda di monitorare la costante evoluzione di questa tecnologia e delle sue applicazioni anche attraverso la partecipazione dell'Italia a progetti europei.

2.11 Raccomandazioni relative alla value chain del cripto attività.

La Commissione Europea ha predisposto un **Action Plan per lo sviluppo del Fintech** nel quale auspica la creazione di un framework regolamentare che dovrebbe essere il più possibile neutro dal punto di vista tecnologico e favorevole all'innovazione; ciò anche al fine di creare un quadro normativo adatto ad accogliere nuovi modelli di servizio e business basati su nuove tecnologie. Risulta pertanto fondamentale che la strategia italiana in materia di tecnologie basate su registri condivisi e blockchain venga definita tenendo conto delle linee guida europee al fine di evitare un disallineamento, sul piano normativo, tra l'Italia e gli altri Stati europei che porterebbe ad avere barriere poco utili per lo sviluppo del mercato.

OSSERVAZIONE #18

Avendo l'Italia già dato recentemente prova di grande capacità di innovazione proprio nel settore delle tecnologie blockchain con lo sviluppo del progetto **Spunta Assegni**, può essere importante fare proprie, magari sviluppandole ulteriormente, le linee guida recentemente adottate dall'ABI nell'ambito dello sviluppo del progetto di una moneta digitale europea.



Utile ai fini del presente lavoro può essere altresì la lettura del quaderno “*Aspetti economici e regolamentari delle cripto-attività*” pubblicato dalla Banca d’Italia del marzo 2019 e nel quale vengono analizzati i profili economici, contabili e prudenziali delle “criptoattività” tipo bitcoin ed illustrata la regolamentazione delle piattaforme di scambio adottata nelle varie giurisdizioni.

2.12 Raccomandazioni relative all’applicazione della normativa antiriciclaggio

La recente relazione annuale del Direttore dell’UIF (Autorità italiana di riferimento per il contrasto del riciclaggio) ha messo in evidenza il possibile rischio dell’utilizzo delle criptovalute per commettere reati di riciclaggio, autoriciclaggio e finanziamento del terrorismo. Tale rischio risulterebbe ancor più accresciuto con la diffusione della pandemia COVID-19 (in tal senso vedasi la comunicazione UIF del 16 aprile 2020).

OSSERVAZIONE #19

Il *cryptolaundering*, quale specie del più ampio genus del cyberlaundering, si presenta tra le forme più insidiose di reimmersione del provento nel circuito economico legale (in tal senso si veda anche il documento “*Criptovalute e riciclaggio*” dell’Associazione Prestatori di Servizi di Pagamento). Lo sforzo finora profuso nel contrasto al cryptolaundering nella IV e nella V Direttiva AML è stato nella direzione della canalizzazione dei flussi finanziari verso gli operatori professionali e di una loro corresponsabilizzazione, sotto comminatoria di sanzioni, a presidio degli obblighi di know your customer e customer due diligence.

Un’eventuale disintermediazione finanziaria potrebbe in realtà avere effetti controproducenti per lo sviluppo del settore. La reale area di criticità è rappresentata, infatti, proprio dal circuito di pagamento elettronico peer to peer, potenzialmente svincolato dalla gestione centralizzata di una banca o di un altro intermediario finanziario. Pur volendo ignorare i benefici offerti in termini di inclusione finanziaria, servizi di pagamento più veloci e con costi di transazione minori, una decisa svolta di criminalizzazione del mercato criptovalutario avrebbe l’effetto controproducente di indurre all’ulteriore immersione nell’illegalità, ghettizzando l’ecosistema criptovalute e determinandone l’esclusivo popolamento da parte di *bad actors*.

2.22.3 Identità digitale

L’applicazione della blockchain alla self sovereign identity promette di rivoluzionare radicalmente i rapporti in rete, rimettendo l’utente al centro dell’interazione con i fornitori di servizi dell’informazione e riconsegnandogli il controllo dei propri dati personali.

OSSERVAZIONE #20

Si raccomanda per mantenere e sviluppare l’interoperabilità con il settore pubblico e privato europeo, l’aggiornamento nel tempo dei sistemi di autenticazione (es.: SPID) e di certificazione dell’identità (es.: CIE, Firma Digitale, PEC) per uniformarsi ai prossimi regolamenti eIDAS (ad esempio per lo sviluppo delle liste CRL di revoca online dei certificati; in corso di valutazione per la versione v2 del regolamento europeo).

2.22.4 Fonti certificative pubbliche

Meccanismi di sottoscrizione e marcatura temporale di un documento digitale sono già operativi nel nostro Paese e costituiscono piena prova della paternità e del tempo in cui esso si è formato. In tal senso, la blockchain non aggiunge nulla rispetto alle soluzioni già esistenti, dotate peraltro di copertura legale.

OSSERVAZIONE #21

Questa Associazione tiene a sottolineare il fatto che una blockchain permissionless potrebbe non avere una granularità temporale esatta per la marcatura delle transazioni; possono infatti



trascorrere anche diversi minuti prima dell'inserimento di un blocco in blockchain come bitcoin o ethereum. Visto il potenziale impatto dirompente di queste tecnologie nelle nostre società, si richiama inoltre l'attenzione riguardo alla necessità di valutare attentamente i costi di inserimento e la capacità richiesta in termini di numero di transazioni al secondo oltre al rispetto dei Service Level Agreement (SLA) definiti per il settore pubblico.

2.22.5 Sanità

Considerato che la spesa annuale relativa al Sistema Sanitario Nazionale si avvicina ai 120 miliardi di euro e considerato che il settore biomedicale italiano è tra i più importanti al mondo con un fatturato complessivo di oltre 1,6 miliardi di euro e più di 150 milioni di margine operativo lordo, questa Associazione ritiene strategico per il sistema Paese orientare le politiche di sviluppo economico in ambito sanitario motivando l'uso di tecnologie blockchain per l'efficientamento del SSN e per il miglioramento della prevenzione, diagnosi e qualità delle cure stesse.

*Si rimanda quindi allo specifico studio allegato a questo documento in **Appendice**.*

2.22.7 E-procurement

Con riguardo a quanto suggerito nella presente raccomandazione si rinvia alle perplessità già espresse in questo documento nelle osservazioni ai §§ 2.22.4 e 2.22.8 poiché è dubbio che l'implementazione di processi di e-procurement su blockchain/DLT e l'impiego di smart contract possa effettivamente «semplificare la verifica di requisiti di partecipazione [nonché] aumentare drasticamente la trasparenza e verificabilità delle procedure».

OSSERVAZIONE #22

Per favorire la competitività delle nostre imprese e il loro accesso al Digital Single Market europeo, si raccomanda di sviluppare la piena interoperabilità con gli standard di eSignature, eTimestamp ed eSeal⁶.

2.22.8 Smart Contract e digitalizzazione dei servizi

La presente raccomandazione propone di «avviare sperimentazioni volte alla possibilità di digitalizzare i flussi di lavoro che implementano servizi in forma di smart contract, in modo da massimizzare la trasparenza, l'accessibilità da parte degli utenti, l'interoperabilità con altri servizi, e l'apertura selettiva dei dati».

OSSERVAZIONE #23

Questa Associazione ritiene che l'adozione di smart contract per la fornitura di servizi della Pubblica Amministrazione al cittadino non aggiunga alcunché rispetto a «l'accessibilità da parte degli utenti, l'interoperabilità con altri servizi, e l'apertura selettiva dei dati». Piuttosto è la *Single Source of Truth* delle blockchain che può favorire l'interoperatività tra sistemi informativi.

Anche con riguardo alla trasparenza, l'idea che un codice accessibile e verificabile da chiunque fornisca maggiore trasparenza è frutto dell'errata idea per cui l'attività amministrativa possa essere fissata in un codice informatico. Peraltro, la trasparenza è già efficacemente raggiunta grazie alle norme sull'accesso civico (D.Lgs. 14 marzo 2013, n. 33 e s.m.) e sull'accesso agli atti amministrativi della pubblica amministrazione (L. 7 agosto 1990, n. 241, art. 22 e ss.). Ogni altra considerazione in ordine alla maggiore trasparenza che potrebbe essere aggiunta con applicazioni blockchain appare, se non errata, quantomeno prematura.

Ciò detto, si invita questo Ministero a considerare che gli smart contract – come definiti all'art. 8-ter del D.L. del 14 dicembre 2018, n. 135 (c.d. Decreto Semplificazioni 2018) – sono programmi

⁶ Rif. <https://ec.europa.eu/digital-single-market/en/eidas-smes>



per elaboratore operanti su blockchain, come tali connotati da un **alto grado di rigidità**. Il loro utilizzo, se non nel ristrettissimo ambito di applicazioni contabili, rischia di ingessare i processi alla base dell'azione amministrativa impedendo l'adozione di soluzioni elastiche per venire meglio incontro alle esigenze del cittadino e per riflettere le infinite varietà del caso concreto. Lo smart contract, insomma, rischia di elevare la burocrazia al livello del codice eseguibile, con il risultato di vincolare la discrezionalità amministrativa, anziché avvicinare le istituzioni al cittadino-utente⁷.

Peraltro, con specifico riguardo all'art. 8-ter sopra citato, questa Associazione ritiene che si tratti di una disposizione di impossibile applicazione, che contiene in essa una contraddizione in termini giuridici. Se da un lato è infatti definito lo smart contract come «*programma per elaboratore*», non può poi sostenersi poco dopo che «*Gli smart contract soddisfano il requisito della forma scritta*» (comma 2). La forma scritta è infatti attribuito di un contratto non di un programma per elaboratore che, tutt'al più, è un'opera dell'ingegno (art. 2, comma 1, n. 8, L. 633/41).

Per le ragioni appena esposte, si suggerisce di abrogare tutto l'art. 8-ter la cui utilità è dubbia, anche al di là del comma 2, poiché nulla aggiunge rispetto alla libera iniziativa di chiunque e alla legittimità (o illegittimità) di utilizzare una DLT, o qualsiasi altra tecnologia il futuro ci riservi⁸. Nel nostro Paese, peraltro, sono ampiamente diffuse e godono già di riconoscimento legale la posta elettronica certificata e le firme digitali ed elettroniche qualificate o avanzate (dell'art. 20 del CAD, comma 1-bis), strumenti collaudati che risolvono egregiamente il problema della forma scritta e della paternità/autenticità dei documenti e dichiarazioni espresse in forma digitale.

⁷ Non si intende con ciò disconoscere l'importanza dell'automazione di taluni processi (direzione in cui vanno i progetti EBSI). Tuttavia, nei termini così indefiniti suggeriti nella raccomandazione, si tratta di un obiettivo generico allo stato perseguibile con le tradizionali soluzioni informatiche senza necessario ricorso agli smart contract.

⁸ L'abrogazione eviterebbe altresì all'AgID la difficoltà di risolvere l'aporia della norma con l'emanazione delle attese Linee Guida per «*l'identificazione informatica delle parti interessate*». Per ogni approfondimento critico sull'art. 8-ter del Decreto Semplificazioni 2018, si rinvia a F. RAMPONE, *Smart contract: né smart, né contract*, in *Riv. dir. priv.* 2019, vol. 2, p. 241.

SANITÀ

L'odierno avanzamento tecnologico pervasivo in ogni aspetto sanitario, da ambiti ospedalieri protetti fino a scenari di telemedicina personale, in congiunzione alla progressiva accelerazione nella digitalizzazione di tutte le informazioni disponibili sta generando una raccolta dati sempre più imponente e sempre più complicata da gestire e comprendere nel suo complesso. La centralità del paziente unita al coordinamento intelligente delle azioni mediche a suo favore, presenta notevoli potenzialità per la riduzione dei costi delle cure somministrate dai sistemi sanitari, spingendo inoltre a un più generale miglioramento della prevenzione, diagnosi e qualità delle cure stesse, sempre più personalizzate. Tuttavia, riuscire a raggiungere l'obiettivo di un coordinamento intelligente delle cure ha risvolti complessi collegati alla gestione, all'interoperabilità e alla comprensione di informazioni eterogenee organizzate in data silos fisici (dati mantenuti e accessibili esclusivamente da una unità operativa) e data silos logici (dati organizzati logicamente esclusivamente per gli usi di una specifica unità operativa). La situazione peggiora se si aggiunge il fatto che le informazioni registrate spesso non sono strutturate o lo sono solo parzialmente e non completamente, ossia le informazioni non sono categorizzate e organizzate in modo da essere facilmente interrogabili da sistemi informatici (ad es. un referto medico è un documento di altissimo valore qualitativo e cognitivo, ma non è tradotto e organizzato in modo da essere facilmente "compreso" da algoritmi automatici).

Le tecnologie blockchain, per loro natura, si pongono in prima linea come fondamento per sviluppare l'interoperabilità progressiva fra sistemi informativi sanitari nazionali. Tramite meccanismi puramente transazionali, verificabili e sicuri le blockchain offrono l'ulteriore vantaggio di facilitare l'implementazione della compliance normativa (GDPR, NIS Directive, ...) in scenari complessi che vedono la presenza di interazioni tra sistemi sanitari inter-regionali, soggetti terzi privati (laboratori di analisi, sanità privata, assicurazioni, ...) o di interazioni con flussi di dati provenienti da dispositivi portatili IoMT. Al contempo, nuove metodologie di analisi e trasformazione dei dati (ML, DL, NLP, ...) con il supporto dell'interoperabilità e accesso controllato a dati anonimizzati, stanno iniziando, a permettere l'estrazione di nuove forme di valore e conoscenza nascosta dai grandi data set sanitari oggi esistenti.

Motivazioni all'uso delle tecnologie blockchain nella sanità:

1. Data Integrity, Consistenza, Coerenza e Sicurezza

Primo scopo storico delle blockchain è stato quello di garantire *sicurezza, resilienza, integrità, consistenza e coerenza* di transazioni distribuite; con questa stessa tecnologia sarà possibile migliorare la sicurezza, riducendo

la superficie di attacco, l'auditing e la gestione dei dati del paziente, fornendo meccanismi di autenticazione regolamentati da Smart Contract che rilasceranno ticket di accesso temporanei alle risorse referenziate da URI nazionali e condivise da tutte le organizzazioni coinvolte nel processo.

L'immutabilità delle transazioni registrate in blockchain, così come le funzioni di controllo dei dati e degli stati in ingresso, oltre a garantire la consistenza e coerenza delle informazioni pone queste tecnologie come sorgente unica di verità - Single source of truth - laddove, allo stato attuale, possono esistere una moltitudine di fonti riguardo la stessa informazione cercata; basti considerare il fatto che attualmente non esiste un registro unico nazionale circa le prescrizioni terapeutiche farmacologiche **in corso di assunzione** da parte del paziente; esistono più fonti frammentate di verità quali le informazioni e posologie riferite dal paziente, quelle riferite dai familiari, quelle riferite dal medico di famiglia, quelle riferite da specialisti, ecc.

La **Single source of Truth** delle blockchain diventa *evidente, esemplare e innovativa* se si pensa alla possibile ed auspicabile implementazione di un sistema per la certificazione dei dati e convalida delle prove dei trials farmacologici, a fianco di altre funzionalità per l'accesso regolamentato a dati anonimizzati a scopi di ricerca. Potendo contare su dati in ingresso di alta qualità, evitando dati provenienti da pazienti suscettibili a potenziali effetti collaterali, interazioni con trattamenti in corso ed alterazioni volontarie dei risultati, i ricercatori potranno provare in modo certo **l'integrità dei dati utilizzati**, mantenuti, analizzati e verificati dai sistemi sanitari.

Inoltre, gli aspetti collegati alla *sicurezza, immutabilità e verificabilità* delle blockchain daranno la possibilità in concomitanza all'uso di tecnologie Secure Elements di sviluppare dei sistemi di **tracciabilità e anti-contraffazione** della catena logistica e dei presidi sanitari (protesi, strumenti chirurgici, farmaci, IoMT, ecc.) a vantaggio sia della salute del paziente sia del sistema ospedaliero potendo evitare alcune fonti di errore (ad es. per verificare senza l'ombra di dubbio la compatibilità di determinati impianti protesici, pacemaker, ecc. con risonanze magnetiche o per registrare in blockchain il gruppo sanguigno) e potendo evitare truffe collegate alla contraffazione dei beni.

2. Dati controllati dal paziente

A maggior tutela della privacy di dati altamente sensibili, le blockchain si pongono come la migliore tecnologia abilitante al controllo dei dati sanitari da parte delle stesse persone. L'implementazione degli standard legati alla Self-Sovereign Identity (SSI) [1] permetteranno ai pazienti di *concedere, monitorare e revocare* l'accesso ai propri dati sanitari, in forma completa o limitata a determinate viste, a singoli professionisti o anche intere organizzazioni. La facoltà di autorizzare l'accesso ai dati del paziente potrà essere delegata da lui stesso a caregivers, familiari, tutori, persone o enti di sua fiducia con gli stessi meccanismi remoti appena descritti o in caso di fallback a giudici e sistema sanitario nazionale.

Come scenario mai visto prima, il paziente (ma anche il garante nazionale), tramite meccanismi di auditing intrinseci alle blockchain, potrà verificare in ogni momento da chi, come, in che forma e perché sono stati usati i propri dati sanitari.



3. Amministrazione, gestione interna ed esterna / territoriale

Secondo studi Capgemini[2] e Deloitte [3] l'automazione, la riduzione di intermediari e la diminuzione del numero di transazioni amministrative tramite l'uso di Smart Contract su blockchain produce una sensibile riduzione dei costi di gestione delle pratiche ed una maggiore efficienza del sistema.

Il controllo in tempo reale dei **Centri di Costo** interni può favorire politiche di ripartizione accurata delle risorse economiche, di verifica dell'effettivo uso del presidio e di riduzione degli sprechi (dovuti per esempio a scadenza di farmaci inutilizzati). Così come la gestione transazionale dei pagamenti ticket, delle pratiche per l'ottenimento di un determinato presidio o status di invalidità e la risoluzione di dispute sulla base di dati condivisi e verificabili da un arbitro, possono avvantaggiarsi di nuovi modelli di automazione dei flussi di lavoro. Non di meno il coordinamento unificato degli stakeholders afferenti alle aziende ospedaliere come ASL, ARPA, soggetti convenzionati, farmacie, ma anche fornitori, laboratori e cliniche private può portare a una riduzione concreta dei costi di sistema generali.

Di fondamentale importanza diventa quindi la gestione centralizzata dell'*identità digitale del paziente* - Digital Identity Management - sia per l'attribuzione automatica dei costi collegati ai relativi **DRG** sia per la deframmentazione e deduplicazione dei dati con conseguente miglioramento della qualità e riduzione dei costi del SSN.

Sia le tecnologie blockchain che i DRG, a cavallo tra mondo amministrativo e mondo clinico, hanno in comune **per loro natura intrinseca** l'aspetto **transazionale** della propria applicazione. Nel quadro italiano, ogni attribuzione economica tra Regione, Azienda Ospedaliera e Centri di Costo interni (cliniche, servizi, ecc..) o esterni (soggetti convenzionati) rispetta regole transazionali strette e trasferisce informazioni e valore da un'entità ad un'altra.

Le blockchain in quest'ottica, possono fornire il miglior strumento di verifica dell'applicazione delle regole e di scambio automatico di informazioni e valore.

L'applicazione del corretto DRG diventerebbe immediata e automaticamente verificabile, potendo contare su Smart Contract differenti eseguiti al verificarsi di eventi particolari come, per citare un esempio, l'attribuzione di un determinato iter o protocollo diagnostico a seconda che rispetti il Gold standard o meno.

Potendo contare sul libro mastro della blockchain condiviso tra gli stakeholders (cliniche ognuna con propria copia del libro mastro, ma anche ed in particolar modo soggetti giuridici distinti come Azienda Ospedaliera e fornitori privati o cliniche convenzionate) i rapporti di trust fra soggetti verrebbero garantiti dal supporto probatorio condiviso fra tutti gli attori in gioco. La Regione così come il SSN, senza la necessità di *complesse verifiche, audit e consulenze esterne* e con il supporto di dati certificati e pre-verificati, **otterrebbero un immediato ritorno economico.**

4. Gestione del percorso sanitario / Care-delivery management

La gestione del percorso sanitario del paziente in blockchain apre la porta a nuovi modelli di coordinamento territoriale e nuove tipologie di piani di cura.

Partendo dal punto iniziale di contatto dell'assistito con il SSN, il medico di famiglia potrà verificare in tempo reale i dati inseriti dagli operatori sanitari, laboratori di analisi esterni, caregivers, ecc. e potrà accedere allo stesso modo ai flussi informativi provenienti dai dispositivi IoMT personali.

Nuovi modelli previsionali degli accessi ospedalieri, prenotazioni di trattamenti e indirizzamento verso i migliori centri di cura, potranno svilupparsi in favore di un intervento pro-attivo del SSN per il miglioramento dello stato di salute nazionale e conseguente riduzione dei costi di intervento post-injury.

5. Dati generati dal paziente e telemedicina

In un mondo in cui l'aspettativa di vita diventerà sempre più alta, il problema dell'invecchiamento e della salute sarà sempre più presente e fattore di costo sempre più alto.

Entro alcuni anni, il 40% delle tecnologie IoT sarà dedicata al settore della salute [4], da 20 a 30 milioni di dispositivi portatili medicali (IoMT), sempre più economici, saranno connessi nel mondo e più di ogni altra categoria il relativo mercato globale raggiungerà i 117 miliardi di dollari nel 2020. Questi sistemi permetteranno non solo di monitorare h24 il paziente anche in luoghi difficilmente accessibili, informare e notificare i familiari, medici curanti, SSN, assicurazioni, nonché prevenire possibili eventi avversi, ma daranno anche la facoltà di interagire e condividere i propri dati tra dispositivi personali e applicativi sanitari eterogenei. **La sfida più impegnativa** per le infrastrutture e architetture IT sanitarie sarà quella di doversi evolvere sia per supportare la crescita esponenziale dei dispositivi portatili sia per analizzarne efficacemente i flussi informativi.

Le tecnologie blockchain hanno la capacità di colmare il gap di interoperabilità e di supportare per *scalabilità, affidabilità e sicurezza* la crescita esponenziale di questi dispositivi all'interno di un nuovo modello sanitario olistico e onnicomprensivo, dove ogni relazione tra informazioni potrà essere analizzata per ottenere un quadro complessivo della salute del paziente.

Nel contesto italiano queste stesse tecnologie potranno essere usate dalle stesse persone per registrare inequivocabilmente le proprie volontà terminali (DAT "Dichiarazioni Anticipate di Trattamento" - legge 22 dicembre 2017, n.219) come il testamento biologico, la donazione degli organi, gli eventi collegati a proprie patologie, oltre a mantenere informazioni come gruppo sanguigno, allergie, protesi ed altre informazioni basilari. Queste informazioni saranno preziose e potranno essere usate in contesti di emergenza laddove le tempistiche decisionali sono strette.

6. Il Nuovo Sistema Informativo Sanitario

In Italia, a partire dal 01/2019, il Nuovo Sistema Informativo Sanitario – NSIS [5] dovrebbe aggregare i flussi informativi provenienti da numerosi fonti e rendere disponibili, a livello nazionale e regionale, un patrimonio di dati, di regole e metodologie per misure di qualità, efficienza, appropriatezza e costo a supporto del governo del SSN, del monitoraggio dei LEA e della spesa sanitaria, condiviso fra i vari livelli istituzionali e centrato sul cittadino.

Nel contesto del NSIS, le tecnologie blockchain, potrebbero giocare un ruolo fondamentale in merito alla governance dei dati e alla certificazione delle attività compiute su di essi. In effetti, la Single Source of Truth potrà essere implementata pienamente soltanto attraverso i nuovi paradigmi dell'**Open Execution** [6], della **Secure Multiparty Computation** [7] offerti dalle blockchain. L'obiettivo sarà quello di verificare, convalidare e controllare il risultato dell'esecuzione di programmi operanti sui dati sanitari, certificando che dati in ingresso, Smart Contract eseguiti e risultati in uscita siano stati effettivamente quelli esposti, senza possibilità alcuna di alterazione (l'importanza diventa subito evidente nel caso dei trials clinici).

Soltanto passando prima attraverso processi progressivi di sviluppo di Sistemi Informativi Sanitari Regionali basati su blockchain, capaci di coordinare e connettere in una rete nazionale i sistemi sanitari territoriali pubblici o convenzionati, gli operatori privati ed i flussi informativi provenienti da dispositivi IoMT, potranno essere poste le basi per una modernizzazione del SSN e una protezione completa della Privacy.

Sorge dunque spontanea la necessità di aggiornare (per es. l'HL7) o sviluppare nuovi standard e linee guida per l'implementazione lato SIO di interfacce blockchain-ready, capaci di garantire la condivisione delle informazioni e l'interoperabilità dei sistemi sanitari locali, regionali e nazionali e per superare le costrizioni dovute ai data silos fisici e logici.

1 eIDAS Supported Self-Sovereign Identity

https://ec.europa.eu/futurium/en/system/files/ged/eidas_supported_ssi_may_2019_0.pdf

2 Blockchain : A Healthcare Industry View

https://www.capgemini.com/wp-content/uploads/2017/07/blockchain-a_healthcare_industry_view_2017_web.pdf

3 Blockchain: Opportunities for Health Care

<https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf>

4 Medical Internet of Things and Big Data in Healthcare

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4981575/8>

5 Nuovo sistema informativo sanitario – NSIS

<http://www.nsis.salute.gov.it>

6 Open Execution—The Blockchain Model



<https://blockchain.ieee.org/technicalbriefs/december-2018/open-execution-the-blockchain-model>

7 Secure Multiparty Computation

https://en.wikipedia.org/wiki/Secure_multi-party_computation