UNIVERSITÀ POLITECNICA DELLE MARCHE

FACOLTÀ DI ECONOMIA "GIORGIO FUÀ"

Corso di Laurea triennale in Economia e Commercio

Applicazioni della tecnologia blockchain per i governi

Application of blockchain technology for governments

Relatore:

Prof. Staffolani Stefano

Rapporto Finale di:

Aurora Pierpaoli

Anno Accademico 2021/2022

INDICE

INTRODUZIONE

Il crittografo David Chaum ha proposto per la prima volta un protocollo simile alla blockchain nel 1982 chiamato "Computer systems established, maintained and trusted by mutually suspicious groups." Haber e Scott hanno fatto un ulteriore passo avanti in questo studio sviluppando una catena di blocchi crittograficamente protetta: miravano a sviluppare sistemi in cui i documenti non potessero essere manomessi. Nel 1992, c'è stato un ulteriore incremento da parte di Dave Bayer che, incorporando alberi di Merkle (una tecnica crittografica per comprimere una grande struttura di dati) nel disegno, ha migliorato l'efficienza, consentendo di inserire più documenti in un solo blocco. La blockchain è stata utilizzata per la prima volta nel 2008 ad opera di Satoshi Nakamoto, pseudonimo di un autore o di un gruppo di autori la cui identità è tuttora sconosciuta, e implementata, sulla base delle precedenti ricerche, per fungere da libro mastro della nascente valuta digitale, il Bitcoin. Quest'ultima è stata lanciata come servizio digitale nel gennaio 2009. L'ascesa del valore dei Bitcoin negli anni ha portato a discutere ampiamente delle criptovalute e della tecnologia di contabilità distribuita nel mainstream. Il clamore di tali argomenti è legato quindi sia al dirompente ruolo che le criptovalute possono rivestire nella società e nell'economia odierna e futura, sia alla nuova tecnologia che si trova alla base delle criptovalute: la blockchain.

Blockchain è un'abbreviazione per una serie di tecnologie di contabilità distribuita che possono essere programmate appositamente per registrare e tenere traccia di qualsiasi cosa di valore, dalle transazioni finanziarie, alle cartelle cliniche o ai titoli di proprietà. Oggigiorno ovviamente vengono già utilizzati dei processi per tenere traccia dei dati, ma con la crescente tecnologia i dati sono aumentati, come è aumentata la necessità di una loro superiore tracciabilità. Risulta quindi essenziale analizzare e capire come la blockchain possa garantire oggi e in futuro una tracciabilità "superiore" in termini di efficienza ed efficacia. La tecnologia blockchain possiede infatti degli elementi che la rendono unica e innovativa, rispetto a ciò che finora è stato utilizzato. Essenzialmente gli elementi che la rendono un'innovazione capace di cambiare il futuro di numerosi processi sono tre: la modalità con cui essa tiene traccia e archivia i dati, come promuove la fiducia e come facilita le transazioni peer-to-peer senza il coinvolgimento di intermediari.

Essendo la blockchain una vera e propria tecnologia e non una singola rete, può essere implementata in numerosi modi e ha del potenziale pressoché illimitato nel sostegno alle interazioni online.

Come è stato in principio con l'avvento di Internet, allo stesso modo la blockchain porta con sé un potenziale enormemente spendibile, ma anche questioni complesse su governance, diritto internazionale, sicurezza, privacy ed economia. Anche questa tecnologia è soggetta a delle problematiche di tipo pratico-applicativo e deve essere inquadrata in una cornice giuridica, economica e politica che la renda utilizzabile al massimo delle sue potenzialità. In questo senso si apre la prospettiva di poter utilizzare la blockchain proprio da quei soggetti che sono caratterizzati da numerosi vincoli legali ed etici, riservatezza e vasta dimensione dei processi: i governi. La tecnologia blockchain può supportare le organizzazioni governative nelle transazioni e nello scambio di informazioni in cui la fiducia e l'autenticazione risultano essere dei prerequisiti essenziali.

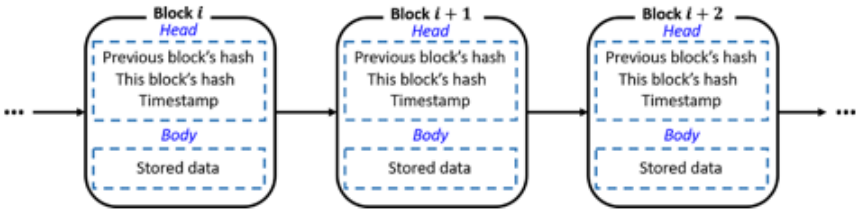
1. LA TECNOLOGIA BLOCKCHAIN

Blockchain è una tecnologia peer-to-peer (P2P) che implementa un registro distribuito e archivia i dati con un approccio sicuro, immutabile e di sola aggiunta tramite consenso o accordo tra i pari (peers) in una rete. Il termine blockchain si riferisce quindi all'intera rete di tecnologie di contabilità distribuita che crea uno speciale tipo di database chiamato libro mastro. Letteralmente il termine libro mastro identifica un registro della contabilità in cui sono riuniti tutti i conti che compongono un dato sistema contabile. Concettualmente la dinamica secondo la quale vengono registrati i dati si rifà proprio all'antica dinamica contabile utilizzata per la redazione del libro mastro in cui le informazioni non vengono riscritte, ma aggiunte progressivamente in base alle modifiche che subiscono. Nella pratica, ciò che accade quando si apportano modifiche alle informazioni registrate, non è una riscrittura delle stesse, ma l'aggiunta di un blocco che segnala il cambiamento dell'informazione. Difatti la blockchain deve il suo nome al modo in cui memorizza le informazioni: in batch chiamati blocchi. Questi blocchi sono collegati insieme in modo sequenziale a formare una linea continua. Una catena di blocchi, una blockchain.

Ogni blocco è costituito da tre elementi:

- Dati: la tipologia dei dati conservati all'interno di ogni blocco dipende dal fine con cui la blockchain viene utilizzata. Ad esempio, nel Bitcoin, i dati di un blocco contengono i dettagli sulla transazione, come il mittente, il destinatario e l'ammontare di monete.
- Hash: un hash nella tecnologia blockchain è un elemento di unicità che può essere comparabile ad un'impronta digitale o ad una firma. Esso identifica un blocco e il suo contenuto, ed è sempre univoco.
- Hash del blocco precedente: questo elemento è esattamente ciò che rende tale la blockchain, in quanto ogni blocco contiene le informazioni del blocco precedente.

Figura I.1 – A Blockchain-Based G-Code Protection Approach for Cyber-Physical Security in Additive Manufacturing, J. Comput. Inf. Sci. Eng. 2021



1.1 FUNZIONI HASH CRITTOGRAFICHE

Nel linguaggio matematico e informatico, l'hash è una funzione non invertibile, che mappa una sequenza di caratteri con un ordine prestabilito (denominata stringa) di lunghezza arbitraria in una stringa di lunghezza predefinita. Esistono numerosi algoritmi che realizzano funzioni hash con particolari proprietà che dipendono dall'applicazione della stessa. Più precisamente una funzione crittografica di hash è una classe speciale delle funzioni di hash, che proprio per alcune proprietà di cui dispone è adatta all'uso in crittografia. Sono queste ultime quelle utilizzate nella tecnologia blockchain. Infatti la crittografia è la disciplina che tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio non comprensibile o intelligibile a persone non autorizzate a leggerlo, garantendo così il requisito di confidenzialità o riservatezza tipico della sicurezza informatica.

Per capire in maniera immediata e semplicistica il meccanismo di queste funzioni è possibile portare due esempi di applicazioni pratiche con cui si è a contatto nella vita quotidiana. Tuttavia, occorre attuare una semplificazione, pensando alle funzioni hash come codici di controllo. Il primo esempio riguarda i codici a barra che si trovano in ogni prodotto in vendita nei supermercati: l'ultima cifra è un codice di controllo che viene generata sulla base delle cifre precedenti. Allo stesso modo è creato il codice fiscale, l'ultimo carattere, che è sempre una lettera alfabetica, non è strettamente legato a nessun dato personale, ma è calcolato prendendo in considerazione tutti i caratteri alfanumerici che l'hanno preceduto. La presenza di questi codici di controllo serve a garantire che non vi siano stati errori rispettivamente nella creazione del codice a barra o del codice fiscale, errori che possono essere di copiatura o di lettura. Il codice di controllo è strettamente a garanzia dell'integrità del codice stesso. Per quanto riguarda le funzioni di hash il meccanismo è molto simile: in queste funzioni matematiche vengono inseriti grandi

blocchi di dati al fine di ottenere un piccolo codice alfanumerico che ha sempre una lunghezza prestabilita e costante. Ovviamente, come anticipato, il contenuto della stringa dipenderà da tutti i dati presi in esame. In particolare, poi le funzioni di hash crittografiche hanno ulteriori caratteristiche che, come prima specificato, le rendono adatte all'applicazione nella tecnologia blockchain.

Una funzione crittografica di hash ideale deve infatti possedere le seguenti proprietà fondamentali:

- deve identificare univocamente il messaggio, in modo che anche due messaggi tra loro simili siano identificati da valori di hash sempre differenti;
- deve essere deterministico, in modo che lo stesso messaggio si possa tradurre solo e sempre nello stesso hash;
- deve essere semplice e veloce calcolare un valore hash da un qualunque tipo di dato o serie di dati;
- deve essere molto difficile o quasi impossibile generare un messaggio dal suo valore hash, se non provando tutti i messaggi possibili. Questo implica che pur conoscendo il valore hash non si può risalire ai dati che lo hanno generato.

Grazie all'hashing quindi nella blockchain a ogni blocco viene assegnato un identificatore originale. La conseguenza di questa creazione di informazioni uniche è una connessione protetta tra ogni coppia di blocchi. La suddetta protezione è creata dal rigoroso ordine con cui i dati devono essere inseriti all'interno dei blocchi per dare luogo al valore hash, dalla presenza del valore hash del blocco precedente e dalla precisione di rilevazione di modifiche di cui è capace la funzione hash. Un tentativo minimo di manomissione, anche involontaria, dei dati viene immediatamente e facilmente identificato dalla verifica del valore hash. Più precisamente, la manomissione di un blocco all'interno di una blockchain provoca il cambiamento dell'hash del blocco. Tale automatica modifica rende il blocco successivo non valido. Questo avviene in quanto il suddetto blocco conteneva l'hash del blocco precedente. Per cui la modifica di un singolo blocco rende non validi tutti i blocchi successivi. Questa configurazione offre alla blockchain un alto livello di sicurezza.

Un altro tipo di algoritmo legato alle funzioni hash, che si occupa di implementare la sicurezza della blockchain, è il meccanismo Proof-of-Work.

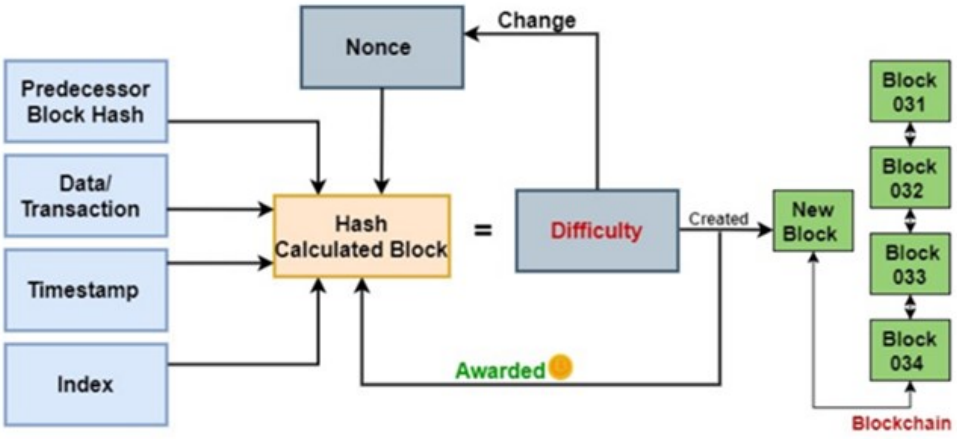
1.2 PROOF-OF-WORK

Il Proof-of-Work (PoW) è uno degli algoritmi di consenso maggiormente utilizzati all'interno della blockchain. Quest'ultimo viene realizzato in Bitcoin ed è il meccanismo

più testato e consolidato, in quanto ve ne sono altri ma risultano più complessi o meno affidabili. L'algoritmo di consenso è una parte fondamentale di questa tecnologia, in quanto viene utilizzato per il processo decisionale tra i nodi della rete. Per comprendere chiaramente il ruolo sostanziale svolto dal Proof-of-Work occorre riepilogare sinteticamente i passaggi fondamentali che costituiscono la tecnologia blockchain. La blockchain è un registro distribuito che contiene un insieme di blocchi di dati in sequenza, collegati tra loro tramite crittografia. Il registro è distribuito in una rete peer-to-peer che è anche il mezzo tramite cui gli utenti comunicano tra loro. Si va a creare quindi una piattaforma in grado di gestire applicazioni e transazioni in maniera decentralizzata. Ogni transazione implica la creazione e l'aggiunta di un nuovo blocco alla catena. L'aggiunta del blocco alla catena avviene tramite il consenso tra i peer di una rete (o anche detti nodi). Il consenso tra coloro che fanno parte della rete rende possibile verificare con sicurezza che vengano aggiunte e registrate all'interno della blockchain solamente transazioni valide. Gli algoritmi di consenso sono appunto i meccanismi che permettono tali verifiche e di conseguenza creano fiducia nella rete. Difatti un algoritmo di consenso eseguito da tutti i peer nella rete è ciò che determina il blocco successivo da concatenare al libro mastro e anche ciò che fornisce forte integrità ai dati memorizzati, in quanto concede a tutti i peer di concordare su un'unica versione della catena senza un'autorità centrale.

La verifica di ogni nuovo blocco utilizza un algoritmo PoW il cui lavoro è quello di generare una soluzione crittografica. Ciò avviene grazie ai nodi esistenti nella rete che utilizzano il proprio hardware per risolvere il problema crittograficamente complesso. Con l'utilizzo del PoW la creazione dell'hash di successo diventa più complessa (e quindi più sicura) in quanto non solo deve essere coerente con i dati (tra cui il timestamp che indica la sequenza cronologica dei blocchi), il nonce e l'hash del blocco precedente, ma deve trovare corrispondenza con l'hash di difficoltà. Il **nonce** è un valore che non ha alcun significato, non essendo correlato alle informazioni della transazione, ma viene aggiunto intenzionalmente al blocco per poter soddisfare le condizioni per generare un valore hash finale di successo. L'**hash di difficoltà** è invece un hash che viene automaticamente generato, in precedenza, dalla stessa blockchain. La soluzione crittografica, pertanto, consiste nella coincidenza dei valori dell'hash di difficoltà e del nuovo hash generato. In questo caso la transazione si considera verificata e un nuovo blocco viene aggiunto alla blockchain.

Figura II.1 – “A pattern for Proof of Work Consensus Algorithm in Blockchain”, EuroPloP’ 2021



1.3 SMART CONTRACTS

Una tecnologia complementare alla Blockchain sono gli smart contracts. Se lockchain è la tecnologia in cui le transazioni vengono archiviate e mantenute, i contratti intelligenti possono essere descritti come i meccanismi per automatizzare queste transazioni.

Gli smart contracts sono stati ideati per la prima volta da Nick Szabo, che ha studiato l'idea dell'automazione dei contratti, come un modo per implementare i contratti cartacei legalmente vincolanti. Nick Szabo ha introdotto il termine smart contract per riferirsi a un insieme di specifiche promesse in forma digitale: clausole contrattuali convertite in codici auto-eseguibili. Questa tecnologia è nata con l’idea di ridurre i costi contrattuali tra i partner delle transazioni e di prevenire eccezioni non intenzionali o atti dannosi nel corso dell'esecuzione del contratto. L’esecuzione degli smart contracts tramite computer ha avuto fin da subito l’obbiettivo di delineare contratti più funzionali dei precedenti contratti cartacei, garantendo uno scambio di dati sicuro con chiunque avesse soddisfatto i vincoli previsti e impostati nei suddetti contratti digitali.

Sebbene le idee iniziali per i contratti intelligenti siano state concepite per la prima volta nel 1997, è stato solo con lo sviluppo dei libri mastri distribuiti e dei loro meccanismi di consenso alla fine degli anni 2000 e 2010 che i contratti intelligenti sono stati implementati e sviluppati come previsto da Szabo. Attualmente, il termine smart contract è usato in modo diverso in numerose discipline. Alcuni definiscono uno smart contract come un contratto legale, che potrebbe essere interpretato dal software (o almeno in alcuni suoi aspetti). Mentre altri considerano i contratti intelligenti come programmi di codice che vengono eseguiti una volta soddisfatte le condizioni predefinite. Questi script normalmente operano su piattaforme blockchain. Infatti, l'attuale generazione di smart

contracts, per sfruttare appieno le proprie capacità, richiede la tecnologia blockchain. L'interdipendenza degli smart contracts con la blockchain ha fatto prediligere l'interpretazione adottata anche da Ethereum Foundation e IBM, per cui lo smart contract, oggi, non è necessariamente connesso all'idea classica del contratto, ma può anche essere ampliato per includere qualsiasi tipo di programma per computer fondato sulla blockchain.

L'attuale generazione di contratti intelligenti basati su blockchain richiede i seguenti elementi: un linguaggio di programmazione, una piattaforma con libro mastro distribuito e una virtual machine.

Gli smart contracts sono specificati dai linguaggi di programmazione, che possono essere differenti a seconda della particolare piattaforma blockchain. Le caratteristiche del linguaggio di programmazione ovviamente determinano il tipo di contratti intelligenti che potrebbero essere scritti per ogni piattaforma blockchain. Esempi comuni di linguaggi di programmazione per contratti intelligenti nelle piattaforme blockchain includono Solidity, così come linguaggi popolari come Python, C++, GOlang e JavaScript. La piattaforma del libro mastro distribuita serve per l'archiviazione dei contratti intelligenti e dei dati ottenuti come risultato della loro effettuazione. Anche se i contratti intelligenti sono archiviati nel registro distribuito, la loro esecuzione è condotta da una macchina virtuale ai margini della rete che elabora le regole del contratto, la Virtual machine.

Uno smart contract è un codice informatico che viene distribuito sulla blockchain per far rispettare, monitorare ed eseguire accordi quando sono state precedentemente accordate e definite le condizioni. È proprio grazie ai linguaggi e alle piattaforme degli smart contracts che la blockchain è stata resa programmabile per numerose applicazioni in svariati ambiti.

2. LE DIROMPENTI CARATTERISTICHE DELLA BLOCKCHAIN

La spiegazione del meccanismo della Blockchain e in particolare di alcune sue componenti si è resa necessaria per comprendere al meglio come è stato possibile pensare di utilizzare questa tecnologia per alcune funzioni dei governi e per quali fondamentali ragioni.

Inizialmente, senza entrare nel merito delle singole attività e azioni che questa tecnologia è in grado di ricoprire per gli organi statali, è opportuno definire le caratteristiche che la rendono innovativa e particolarmente idonea a tale scopo. L'origine di tali caratteristiche trova giustificazione nella spiegazione tecnica in precedenza esposta.

Le peculiarità della blockchain sono essenzialmente tre: la modalità di archiviazione dei dati utilizzata, la creazione di fiducia nei dati e la decentralizzazione. Esse sono tra loro estremamente connesse. Infatti, l'archiviazione dei dati avviene tramite una modalità non distruttiva, che tiene traccia di ogni operazione in modo trasparente, immutabile e sicuro. Inoltre, la progettazione della blockchain come tecnologia decentralizzata e distribuita su una vasta rete di computer contribuisce a ridurre la possibilità di manomissione dei dati e conduce al secondo fattore che rende unica la blockchain: la creazione di fiducia nei dati. Come in precedenza analizzato, prima che un blocco possa essere aggiunto alla catena, devono succedersi dei passaggi. Innanzitutto, deve essere risolto un puzzle crittografico, creando così il blocco. Il computer che risolve il puzzle condivide la soluzione con tutti gli altri computer della rete (si tratta del proof-of-work). La rete verifica quindi questo proof-of-work e, se corretto, il blocco viene aggiunto alla catena. La combinazione di questi complessi enigmi matematici e la verifica da parte di molti computer garantisce sicurezza a ogni singolo blocco della catena. La creazione di fiducia porta all'opportunità di interagire direttamente con i dati, in tempo reale. Ciò conduce al terzo aspetto innovativo della tecnologia blockchain: l'assenza di intermediari. L'assenza di intermediari implica delle conseguenze di grande portata, in quanto libera il processo dalla mediazione e dal lavoro di un terzo soggetto e in tal senso riduce l'errore possibile nella totalità dell'azione, avendo eliminato un passaggio. Inoltre, la decentralizzazione contrae notevolmente i tempi, i costi e la complessità delle operazioni.

Un altro aspetto fondamentale da considerare in tal senso è anche la capacità della blockchain del mantenimento della riservatezza dei dati all'interno di essa (i metadati di ogni transazione sono crittografati), in quanto attualmente, quando vengono condotte negoziazioni ciò che preme le parti è spesso mantenere privati i propri dati finanziari,

economici o aziendali, all'altra. Per fare ciò le negoziazioni sono affidate a intermediari di fiducia, come istituti finanziari o liberi professionisti, che permettono appunto di mantenere tali informazioni riservate. Questi intermediari creano fiducia tra le parti e sono in grado di verificare le informazioni presentate, mantenendole riservate. Questo approccio limita l'esposizione e il rischio, ma aggiunge un ulteriore step allo scambio, mentre tramite la blockchain risulta possibile mantenere la sicurezza e la velocità della transazione.

2.1 CONDIVISIONE DEI DATI

Sempre in relazione alla riservatezza di determinati dati è da specificare la presenza di diverse tipologie di blockchain. Alcune blockchain possono essere completamente pubbliche e aperte a tutti per la visualizzazione e l'accesso. Altre possono essere limitate a un gruppo selezionato di utenti autorizzati, come un'azienda, un gruppo di banche o agenzie governative. Le reti pubbliche funzionano su Internet e tra gli esempi più noti vi è la blockchain utilizzata dal Bitcoin. Esistono anche blockchain ibride pubblico-private. Ciò che cambia tra queste è chi può entrare a contatto con i dati e con che tipologia di dati. Inoltre, le blockchain non si dividono solamente in pubbliche e private, ma possono essere ulteriormente classificate in blockchain autorizzate e senza autorizzazioni. Specificamente la blockchain pubblica senza autorizzazione è un tipo di blockchain in cui chiunque può partecipare, leggere, scrivere e confermare le transazioni nella rete; è una rete che così strutturata crea un'elevata trasparenza: tutti coloro che partecipano alla rete possono effettuare transazioni tra loro e possono vedere tutte le transazioni. Poi vi è la blockchain con autorizzazione pubblica: questo è un tipo di blockchain in cui chiunque può unirsi e vedere le transazioni, ma esiste una restrizione per scrivere e confermare le transazioni. Solo alcuni utenti autorizzati possono realizzare le transazioni. La blockchain con autorizzazione privata presenta invece una restrizione riguardante la partecipazione e la lettura delle transazioni nella rete. Solo i partecipanti autorizzati possono intervenire e prendere visione delle transazioni e solamente i nodi preselezionati possono convalidare le transazioni. Infine, vi è la blockchain privata senza autorizzazione, per cui esiste una restrizione per partecipare e leggere le transazioni nella rete, ma chiunque può avere accesso al meccanismo di convalida delle transazioni.

Si possono quindi configurare diverse casistiche. Ad esempio, in alcune reti con accesso privato, i membri possono vedere tutti i dati, mentre il pubblico può vedere solo i dati

selezionati. In altre, tutti possono prendere visione di tutti i dati, ma solo alcune persone hanno accesso per poterne aggiungere di nuovi.

Un governo, ad esempio, potrebbe avvalersi di un sistema ibrido per registrare e verificare i diritti di proprietà dei suoi cittadini, mantenendo però private le loro informazioni personali. Oppure potrebbe consentire a tutti di visualizzare i registri di proprietà, ma riservarsi il diritto esclusivo di aggiornarli. La possibilità di scelta di una determinata condivisione dei dati o della partecipazione di determinati soggetti ad un processo lascia ampie possibilità di progettazione della rete. Questo è un aspetto estremamente positivo per i governi che scelgono di avvalersi di questa tecnologia, in quanto possono spaziare nella progettazione di alcune procedure, dando loro le sfumature che più si allineano con le direttive politiche e di governo, mantenendo costante però l'efficacia e l'efficienza dei processi.

3. BLOCKCHAIN E GOVERNI: UNO STUDIO IN EVOLUZIONE

Finora la maggior parte del lavoro di ricerca nell'area blockchain si è concentrato sugli aspetti tecnici, come i processi peer-to-peer e lo scambio di informazioni nel dominio privato. Tuttavia, la crescita esponenziale degli studi sulla tecnologia blockchain giustifica la necessità di una ricerca sempre più improntata nel soddisfare i bisogni della società e questo può avvenire tramite l'applicazione nelle organizzazioni governative. È possibile affermare che in questo campo la blockchain è ancora nella sua fase iniziale, poiché accademici e politici stanno affrontando la scarsità di ricerche presenti attualmente nel panorama mondiale e nazionale. Gli studi disponibili riguardo l'adozione della tecnologia blockchain nelle organizzazioni governative sono ancora manchevoli rispetto a quelli relativi agli ambiti prettamente tecnici. Tuttavia, essendo chiara l'importanza che potrebbe rivestire la tecnologia blockchain all'interno delle organizzazioni governative, oggi sono le stesse organizzazioni nazionali e internazionali che si stanno mobilitando per approfondire gli studi connessi: ci sono in atto più di 200 iniziative, in fase di lancio o di pianificazione, promosse da parte degli stessi governi (Berryhill et al., 2018).

3.1 EUROPEAN BLOCKCHAIN PARTNERSHIP E ILLINOIS BLOCKCHAIN INITIATIVE

Tra le iniziative rilevanti da segnalare vi è il progetto realizzato dall'Unione Europea. Dal 2018, 29 paesi (tutti gli Stati membri dell'UE, la Norvegia e Lichtenstein) e la Commissione europea hanno collaborato per formare la European Blockchain Partnership (EBP), con lo scopo di mettere in atto il potenziale blockchain per i servizi a beneficio dei cittadini, della società e dell'economia. La suddetta partnership sta costruendo un'infrastruttura, la European Blockchain Services (EBSI), che è la prima infrastruttura Blockchain a livello Ue, guidata dal settore pubblico e che si mobilita nel pieno rispetto dei valori e dei regolamenti europei (EBSI (europa.eu)). La visione della EBSI è sfruttare la blockchain per la creazione di servizi transfrontalieri per le amministrazioni pubbliche e per i loro ecosistemi, in modo da poter agevolare la verifica delle informazioni e rendere i servizi affidabili. Dal 2020, EBSI sta implementando una rete di nodi blockchain distribuiti in tutta Europa, supportando diverse applicazioni focalizzate su casi di utilizzo selezionati. Le casistiche attualmente utilizzate da EBP per lo sviluppo dei suddetti servizi sono nell'ambito: dell'identità, del diploma, della sicurezza sociale e della tracciabilità dei documenti. Questo per la realizzazione di diversi obiettivi: creare un modello di

identità autonoma in Europa, che consenta agli utenti di controllare la propria identità oltre confine; far ottenere ai cittadini il controllo digitale delle proprie credenziali educative, riducendo notevolmente i costi di verifica e migliorando la fiducia nell'autenticità dei documenti; creare documenti specifici in ambito sanitario che possano essere verificabili e attendibili in tutta l'Ue.

Uscendo dall'ambito europeo invece è possibile citare lo stato dell'Illinois, che è stato tra i primi a mostrare interesse nel campo e nello studio della tecnologia blockchain. Recentemente lo stato dell'Illinois ha realizzato il suo primo report governativo ufficiale riguardo la blockchain. Questo è stato realizzato da un consorzio di agenzie statali, dell'Illinois e della Contea, che ha preso il nome di Illinois Blockchain Initiative. L'obiettivo dell'iniziativa è determinare come questa tecnologia rivoluzionaria può essere sfruttata per creare servizi statali più efficienti, integrati e fidati, fornendo al contempo un ambiente accogliente per la comunità blockchain (Blockchain in Illinois - Home). Infatti, la blockchain e i ledger distribuiti hanno mostrato di avere il potenziale per trasformare la distribuzione dei servizi pubblici e privati e per ridefinire la relazione tra il governo e il cittadino in termini di condivisione dei dati, trasparenza e fiducia. Andando nel concreto, uno degli ultimi progetti che lo stato dell'Illinois sta sviluppando grazie alla collaborazione dell'Illinois Blochckain Initiative e dell'Illinois Longitudinal Data System, è la creazione di un sistema-dati nell'ambito dell'educazione. Lo sviluppo di una versione "2.0" del sistema dei dati sull'istruzione avverrà grazia all'utilizzo di nuovi set di dati (forniti dalla partecipazione delle agenzie per l'istruzione, l'occupazione, il commercio e i servizi all'infanzia) e della tecnologia blockchain. La nuova piattaforma è ideata per semplificare la gestione della sicurezza dei dati, garantendo che le informazioni sensibili siano contrassegnate utilizzando "terminologie specifiche" e "classi di dati" e che gli utenti che abbaino accesso all'hub possano avere visione dei dati solo in base ai loro ruoli. Secondo gli sviluppatori del progetto questo consentirà ai leader del governo di reperire informazioni senza precedenti sulle scuole e sui programmi educativi dello stato. Aspetto cruciale per orientare le politiche di governo e la consapevolezza dei cittadini.

Questi due esempi di iniziative fanno comprendere l'enorme fiducia che si sta dando alla blockchain, anche nell'ambito pratico. La fiducia riposta nell'utilizzo della tecnologia nel settore governativo sta producendo feedback positivi e rispettando pienamente le aspettative in gioco. Infatti lo stesso stato dell'Illinois dopo l'annuncio della pubblicazione del rapporto blockchain finale sull'InterPlanetary File System (che è esso stesso un sistema di archiviazione di file peer-to-peer correlato a blockchain e registri

distribuiti), in una lettera allegata al rapporto ha riassunto i risultati ottenuti, scrivendo: “Questa task force ritiene che la tecnologia blockchain e la sua crittografia integrata possano facilitare metodi altamente sicuri per interagire con il governo e mantenere registri senza carta, aumentando l'accuratezza dei dati e fornendo migliori protezioni di sicurezza informatica per i residenti dell'Illinois. Sebbene la tecnologia debba ancora essere perfezionata, il governo ha l'opportunità di aiutare a plasmare e adottare soluzioni innovative" (Illinois Releases Its First Official Government Report on Blockchain (govtech.com)). Tale dichiarazione insieme ai sempre più numerosi impieghi apre un nuovo mondo di ricerca che vuole vedere la blockchain in azione verso il diretto servizio delle esigenze dei governi, dei cittadini e delle imprese. Il percorso di evoluzione è sicuramente agli albori e presenta ancora notevoli sviluppi, in gran parte ancora ignoti, essendo attualmente la blockchain stessa una tecnologia dinamica, ma si prospettano numerose applicazioni in grado di rivoluzionare l’assetto governativo e definire in un’ottica migliore le relazioni statali e extra-statali.

4. APPLICAZIONI DELLA BLOCKCHAIN PER I GOVERNI

Prima di esporre le possibili applicazioni della blockchain all'interno delle organizzazioni governative è stato necessario esporre i meccanismi principali su cui si basa questa tecnologia. La conoscenza di tali aspetti è essenziale per comprendere in primo luogo come si possano realizzare applicazioni pratiche e in secondo luogo perché tale tecnologia risulti particolarmente adatta allo scopo. Infatti, a livello teorico sono state esposte tutte le caratteristiche della blockchain che la rendono uno strumento in grado di fornire sicurezza, privacy, fiducia nei dati e nelle transazioni, facilità e velocità nei processi. L'esposizione teorica è stata anche accompagnata da esempi di applicazioni odierne, che hanno fornito e stanno fornendo evidenze empiriche nel medesimo senso. Ciò non significa che l'utilizzo della blockchain, come già suggerito, sia privo di aspetti negativi o possibili difficoltà applicative, ma che attualmente è già utilizzata per creare vantaggi nel settore pubblico e privato e che sarà in grado di ricoprire gradualmente un ruolo di maggiore rilievo in numerosi campi. Esempi di applicazioni che la blockchain può assumere per implementare le funzioni e l'efficienza dei governi, che si approfondiscono in tale documento, sono le seguenti:

- Il voto elettronico
- Il trasferimento dei titoli di proprietà
- Il registro dei brevetti
- Il registro dei dati sanitari
- L'identità digitale.

4.1 APPLICAZIONE DELLA BLOCKCHAIN NEL VOTO ELETTRONICO

Il sistema di voto tradizionale nella maggior parte dei paesi si basa su urne e quindi su voti dotati di fisicità materiale. Alcune nazioni utilizzano anche sistemi di voto elettronico, che tuttavia presentano molte sfide, come l'integrità dei dati, l'autenticazione e la privacy. Invero entrambi i sistemi sono non completamente trasparenti e controllabili, basti pensare al caso italiano. Ancora oggi si mantiene un sistema di voto cartaceo a conteggio manuale, in quanto lo si ritiene in grado di garantire in maniera migliore, rispetto al sistema elettronico, i principi fondamentali del voto, sanciti per legge: personale, eguale, libero e segreto. Tuttavia, questo non ha fatto mancare accuse per brogli elettorali, ovvero tutte quelle operazioni illecite di alterazione del voto che tendono

a distorcere una consultazione elettorale. Ciò fa comprendere che gli attuali sistemi di voto utilizzati non garantiscono una sicurezza assoluta, che permette quindi di prendere in considerazione altri metodi. Dopo lo sviluppo e l'ampliamento della tecnologia blockchain, i ricercatori hanno proposto di utilizzare questa tecnologia nel dominio e nella gestione del voto elettronico, per superare appunto gli svantaggi delle pratiche precedenti. Il sistema di voto elettronico esistente si basa su un unico fornitore che controlla il database e presenta quindi un design centralizzato. Tale fornitore gestisce anche gli strumenti di monitoraggio. Nell'attuale sistema di voto elettronico si crea però una mancanza fondamentale: gli elettori non possono verificare in modo indipendente il voto espresso per sviluppare fiducia tra loro e il dipartimento governativo, che organizza le elezioni.

La blockchain può essere utilizzata come alternativa migliore per controllare i risultati e registrare i voti. Questa soluzione consente di fornire trasparenza a elettori e candidati per quanto riguarda il conteggio dei voti, e allo stesso tempo è in grado di gestire la segretezza delle schede elettorali.

Generalmente i voti sono registrati, gestiti, contati e controllati da un'autorità centrale, il Voto Elettronico abilitato da Blockchain (BEV) potrebbe invece potenziare il ruolo degli elettori consentendo loro di svolgere i suddetti compiti, tenendo una copia del record di voto. Il record storico del voto non può essere cambiato, perché altrimenti gli altri elettori vedrebbero che il record differisce dal loro. Questo rende impossibile aggiungere un voto illegittimo, perché il resto degli elettori sarebbero in grado di verificare che tale voto che non è compatibile con le regole elettorali.

Il maggiore potenziale del BEV è nei contesti organizzativi. Prendendo il concetto e sviluppandolo un ulteriore passo avanti, il BEV potrebbe essere combinato con i contratti intelligenti per agire automaticamente in determinate condizioni pre-concordate. Ad esempio, i risultati delle elezioni potrebbero innescare l'implementazione automatica delle promesse del manifesto di propaganda politica, delle scelte di investimento o di altre decisioni logistiche. Molti analisti hanno considerato la blockchain un supporto per trasformazioni profonde, in grado di aumentare il coinvolgimento e persino il ripristino dei collegamenti tra cittadini e istituzioni politiche, fino a pensare alla possibilità di utilizzarla per attuare la democrazia "liquida", combinando la democrazia diretta (per cui i cittadini votano regolarmente su specifiche decisioni politiche) con un sistema delegato. Tra il 2017 e il 2020 alcune organizzazioni governative hanno condotto progetti pilota basati sulla blockchain in vari dipartimenti pubblici, compresi i sistemi di voto elettronico

(Blockchain Project Dutch Government, 2017). Il governo estone ha iniziato a utilizzare la blockchain all'interno dalla propria organizzazione governativa e ha poi adottato seriamente la blockchain nel sistema di voto (Ufficio elettorale statale dell'Estonia, 2017). Nel 2017, anche la Corea del Sud ha adoperato con successo il voto elettronico basato sulla tecnologia blockchain nelle elezioni del governo locale. In questo periodo sono stati sviluppati due sistemi di voto elettronico basati su blockchain: Helios e WAVE.

4.2 APPLICAZIONE DELLA BLOCKCHAIN PER IL TRASFERIMENTO DEI TITOLI DI PROPRIETA'

Il governo svolge il ruolo di custode di un registro immobiliare tradizionale. In diversi paesi possono avere nomi e specializzazioni diverse, ma lo scopo è lo stesso: fornire certezza sui diritti di proprietà tracciando i registri delle transazioni (i titoli di proprietà). Questo meccanismo viene utilizzato in maniera similare anche per i registri di alcune tipologie di beni mobili (automobili, barche, aerei, ecc.), azioni e altri titoli e diritti societari. Tuttavia, secondo un rapporto realizzato delle Nazioni Unite del 2011, le Governance deboli hanno portato alla corruzione nell'occupazione e nell'amministrazione della terra e dei titoli di proprietà in più di 61 paesi nel mondo. Da tale indagine è emersa una corruzione di variabile natura, dalle tangenti su piccola scala, fino all'abuso del potere del governo a livello nazionale, statale e locale. L'applicazione dei diritti di proprietà è un mezzo che incentiva gli investimenti, consente di favorire l'accesso ai capitali agli imprenditori e fornisce risorse per evitare la povertà. Ciò nonostante, gran parte dei poveri non hanno diritti di proprietà. Circa il 90% della terra nell'Africa rurale è privo di documenti o non è registrato. Allo stesso modo, la mancanza di proprietà terriera rimane tra gli ostacoli all'imprenditorialità e allo sviluppo economico in India. Queste sono alcune delle principali problematiche legate all'inefficienza dei registri di proprietà nei paesi in via di sviluppo. Tuttavia, anche nei paesi maggiormente sviluppati, i sistemi in atto sono controllati da autorità centralizzate, per cui si basano essenzialmente su un atto di fiducia posto da parte dei cittadini stessi nei confronti delle istituzioni, in quanto rimangono vulnerabili all'errore accidentale o premeditato.

La promessa del governo di servire la società in modo equo potrebbe quindi essere rafforzata da una tecnologia che limita l'appropriazione indebita e la corruzione. La tecnologia blockchain esclude e riduce al minimo le colpe umane e la corruzione, fornendo un libro mastro irrevocabile e immutabile, e risulta un sistema più completo del semplice contratto sociale basato sulla pura promessa e fiducia politica e legale. La

blockchain può ridurre attriti e conflitti, nonché i costi associati alla registrazione della proprietà: sarebbe possibile eseguire tutte o la maggior parte delle elaborazioni tramite smartphone. Inoltre il passaggio di proprietà potrebbe avvenire direttamente tra acquirente e venditore, che concordando alcune condizioni reciprocamente accettabili, e per la verifica degli ulteriori elementi legali (come quelli presenti per il passaggio di proprietà degli immobili) si rifanno al meccanismo progettato tramite blockchain. Poi i contraenti, a seconda delle modalità prescelte, entrerebbero in uno specifico smart contract che viene eseguito sulla blockchain stessa. Tutti i termini e le condizioni esistono nello smart contract e quando sono soddisfatti, il titolo di proprietà viene automaticamente trasferito. Nell'esecuzione di tale processo i dati non possono essere manipolati e subire modifiche inattese.

A livello internazionale sono state già intraprese varie iniziative. La piattaforma statunitense per la registrazione degli immobili, Bitland, ha annunciato l'introduzione di un sistema catastale basato su blockchain in Ghana, dove il 78% dei terreni non è registrato. Il Ghana è un paese caratterizzato da un lungo arretrato di casi di controversie nei tribunali riguardanti le proprietà terriere. Bitland registra le transazioni in modo sicuro, con coordinate GPS e inserimento di descrizioni, scritte e foto satellitari. Bitland ha in programma di espandersi anche in Nigeria in collaborazione con il Fondo OPEC per lo sviluppo internazionale. Anche la società di bitcoin BitFury e il governo della Georgia hanno firmato un accordo per lo sviluppo di un sistema per la registrazione dei titoli di proprietà tramite blockchain. Con il sistema attuale per l'acquisto o la vendita dei terreni in Georgia, l'acquirente e il venditore devono utilizzare il registro pubblico e pagare una cifra variabile tra i 50 - 200 dollari a seconda della velocità con cui desiderano che la transazione venga autenticata. Questo progetto pilota permetterà invece di spostare il processo di registrazione sulla blockchain, determinando un abbattimento notevole dei costi (che dovrebbero aggirarsi intorno a delle commissioni pari a 0,05 - 0,10 dollari) e una maggiore rapidità dell'autenticazione.

4.3 APPLICAZIONE DELLA BLOCKCHAIN NEL SISTEMA DEI BREVETTI

I brevetti offrono ai loro proprietari il diritto esclusivo di sfruttare le innovazioni per un periodo specifico. Il sistema di brevetti è stato progettato per incentivare l'innovazione. Senza di esso gli inventori non sarebbero motivati a investire tempo e denaro per sviluppare un'idea, che gli altri potrebbero poi copiare e sfruttare senza aver partecipato

minimamento ai costi di sviluppo. La protezione data agli innovatori non coincide però perfettamente con l'incentivare l'innovazione. Infatti, per incentivare l'innovazione il sistema di brevetto deve bilanciare la protezione degli innovatori con la protezione della concorrenza. Se gli innovatori non risultassero protetti, l'esposizione alla concorrenza scoraggerebbe gli investimenti e la ricerca in innovazioni. D'altra parte, se i concorrenti non fossero in qualche modo tutelati, sarebbero loro ad essere scoraggiati nell'investire in migliorie e nuove idee, creando anche minore efficienza sul mercato.

Tuttavia, anche con l'attuale sistema vi sono delle problematiche che rendono la registrazione dei brevetti macchinosa. Ad esempio, può capitare che, per via di diverse casistiche e fattori, sia la concorrenza a sfruttare il brevetto prima dell'innovatore stesso. Un ulteriore problema è costituito dalle spese da effettuare per acquisire la protezione dei brevetti in diverse regioni che scoraggia le aziende al ricorso alla registrazione del brevetto e le porta a preferire il rischio di introdurre le loro innovazioni nel mercato senza alcuna protezione e tutala. Infine, una importante criticità è la complessità stessa del sistema di brevetto. Prendendo come riferimento l'Unione Europea, ci sono diverse politiche e sistemi in atto in ogni paese, che nonostante i recenti sviluppi, non hanno ancora dato luogo a un sistema di brevetto UE unificato. Inoltre, anche se in ogni Stato membro è possibile la registrazione di un brevetto a livello Europeo, il costo di tale procedura e delle traduzioni delle convalide e dei rinnovi nei diversi sistemi lo rende relativamente costoso.

Oggi diversi aspetti del sistema di brevetto sono digitalizzati, ma non ci sono state importanti modifiche in relazione alla struttura stessa del sistema. L'utilizzo della blockchain potrebbe consentire un meccanismo più fluido riducendo le controversie che possono nascere in relazione al contratto e potrebbe offrire un'opportunità per correggere alcuni aspetti del sistema di brevetto.

Come più volte descritto, la blockchain grazie all'hashing e al proof-of-work permette la registrazione di determinati dati all'interno di un blocco in maniera criptata. Tali dati possono essere verificati da chiunque, ma nessuno può interpretare il contenuto dell'hash. Tuttavia, i titolari del documento originale possono dimostrare che il documento esisteva al momento in cui la transazione è stata effettuata ripetendo il processo di hashing su una copia identica del loro documento originale (utilizzando lo stesso algoritmo di hashing per produrre lo stesso hash, comporta il possesso del documento originale). Questo presenta l'interessante possibilità di registrare pubblicamente l'esistenza di un documento senza rivelarne il contenuto. Tale processo può essere utilizzato a favore degli innovatori,

per proteggere il loro lavoro, registrando un hash della descrizione dei loro brevetti sulla blockchain. La distribuzione della tecnologia blockchain all'interno del sistema di brevetto potrebbe ridurre le inefficienze nella ricodifica e segnare il tempo delle singole registrazioni in modo efficiente, anche in diversi sistemi di brevetti nazionali.

4.4 APPLICAZIONE DELLA BLOCKCHAIN NEI REGISTRI DELLA SANITÀ

I dati inerenti al settore sanitario richiedono generalmente requisiti di autenticazione, interoperabilità e condivisione, a causa dei vincoli legali alla quale sono sottoposti e per le numerose applicazioni per cui la loro conoscenza è richiesta. Tali requisiti possono essere soddisfatti in maniera rigorosa dall'utilizzo della tecnologia blockchain. Quest'ultima ha il potenziale per realizzare e mantenere un registro della salute pubblica. Le informazioni mediche possono essere cartelle cliniche e dati inerenti all'identità e alle diagnosi di ogni singolo individuo. Molte cartelle cliniche vengono create e archiviate quotidianamente, ma queste cartelle sono conservate in reparti, settori e strutture ospedaliere differenti; inoltre, quelle cartacee sono sottoposte al rischio di perdita e quelle digitali ad attacchi informatici e dispersione di informazioni. Per tali motivi risulterebbe utile, se non ormai necessario, creare un sistema centralizzato di cartelle cliniche sanitarie. La blockchain può contribuire in questa direzione in maniera decisiva: se il registro di salute pubblica fosse costruito su una struttura blockchain i dati non incorrerebbero nel rischio di manipolazione e risulterebbero all'interno di un unico inequivocabile sistema.
In tal modo, in primo luogo si potrebbe rispondere all'esigenza della condivisione dei dati. Oggi tale condivisione è difficoltosa in quanto è rara l'esistenza di registri sanitari completi inerenti ad un unico individuo. I pazienti stessi spesso non hanno una visione unificata dei loro dati sanitari, che sono appunto distribuiti tra diverse strutture ospedaliere e sanitarie statali.
In secondo luogo, si potrebbe rispondere all'esigenza della mobilità. La mobilità è un requisito crescente nel settore sanitario poiché i pazienti stanno diventano sempre più mobili, sia a livello nazionale che internazionale, e richiedono quindi che le loro informazioni soddisfino lo stesso livello di portabilità. Anche i dispositivi medici stanno evolvendo, sono dispositivi, dotati di sensori e accesso a internet, per cui sempre più capaci di dar luogo a numerosi dati pronti "all'uso". La blockchain potrebbe soddisfare l'esigenza di una condivisione in tempo reale, garantendo l'accesso ai dati da qualsiasi

luogo e su qualsiasi dispositivo, contemperando la sicurezza e la protezione prevista e richiesta dalla legge.

Infine, oltre alla utilità nell'ambito prettamente sanitario, riguardante la migliore gestione delle informazioni mediche dei pazienti e quindi della possibilità di questi di avere ovunque cure adeguate, ci sono altre implicazioni notevoli per i governi. Difatti sulla base di questi registri sanitari gestiti su piattaforme blockchain i governi potrebbero programmare e offrire alcune iniziative di pubblica utilità per aiutare finanziariamente i cittadini più bisognosi. Ad esempio, nel 2018 il governo indiano ha lanciato il programma Ayushman Bharat. Questo programma voluto dal Primo Ministro, Jan Arogya Yojna, ha previsto di fornire assicurazioni sanitarie al 40% della popolazione indiana più povera. La grandezza e la bontà di tale progetto sono però ostacolate dal dover rintracciare e registrare ogni potenziale beneficiario e successivamente nel conservare la sua cartella clinica, soprattutto nel caso di uno stato con una popolazione numerosa come quella indiana. Un sistema blockchain, progettato con apposito smart contract, in grado di rintracciare automaticamente i requisiti patrimoniali e sanitari dei soggetti idonei a beneficiare di tale provvedimento, semplificherebbe notevolmente il processo. Questo, in generale, permetterebbe agli stati sociali di orientare intelligentemente le proprie politiche di welfare in ambito sanitario, avendo a disposizione dati attendibili e completi, e anche di applicarle con maggiore facilità, verificando che a beneficiarne siano i soggetti idonei per legge.

4.5 APPLICAZIONE DELLA BLOCKCHAIN PER LA GESTIONE DELL'IDENTITA' DIGITALE

L'identità digitale è un'identità online creata da un individuo nel cyberspazio. L'identità digitale riconosce il titolare dell'identità tramite alcuni identificatori digitali come indirizzo e-mail, nome di dominio o URL. Al giorno d'oggi, i servizi governativi, i servizi personalizzati e le applicazioni dei servizi aziendali conservano e trasformano di conseguenza le informazioni personali degli utenti. L'identità digitale sul web è ancora archiviata su sistemi centralizzati e gestita da soggetti terzi che a loro volta hanno la possibilità di manomettere e cancellare i dati dell'utente senza autorizzazione. Ciò porta a una situazione di precarietà e preoccupazione in tema di furto di identità e sicurezza, che richiede soluzioni di Identity Management molto rigorose. L'identità digitale è quindi una questione che assume oggi una portata rilevante e che deve essere affrontata in tal senso.

Gli ambienti di Identity and Access Management (IAM) includono molti utenti e fornitori di servizi. I sistemi IAM funzionano mediante la fornitura, a ciascun utente, di un account e un insieme di funzionalità che consentono agli utenti di dimostrare la proprietà degli account e quindi ricevere servizi in base alle loro esigenze e capacità. Poiché l'identità digitale degli utenti è frammentata tra i vari fornitori di servizi, gli utenti finiscono per avere un'esperienza terribile che si sostanzia in innumerevoli registrazioni con nome utente e password monotoni. Tale dinamica conduce ad un sistema non sicuro, poiché gli utenti utilizzano la stessa password in molti siti web. Questo assieme alla mancanza di un efficace meccanismo di controllo degli accessi, ostacola sicuramente la sicurezza e la privacy delle informazioni riservate dell'individuo. Nel tempo non sono infatti mancati episodi di hacking di sicurezza di alto profilo e fughe di dati privati, dove, quelli non crittografati, sono stati violati e sottoposti a furti. Il problema principale, come già anticipato, risiede nel fatto che i dati privati sono inseriti in archivi centrali e sono quindi sia sotto il controllo di intermediari, che di autorità terze. Per cui i principali fattori che minano la sovranità dei dati sono i sistemi di privacy centralizzati e le strutture di gestione delle informazioni poco chiare. Di conseguenza, la blockchain, caratterizzata invece da decentralizzazione, trasparenza e disponibilità, si delinea come una tecnologia in grado di restituire la sovranità dei dati agli utenti. Un sistema di gestione dell'identità basato su blockchain consentirebbe la gestione dell'identità digitale incentrata sull'utente stesso: è quest'ultimo che trasferisce direttamente l'utilizzo e il controllo delle informazioni sulla propria identità, agli altri soggetti, aumentando la sicurezza e contemporaneamente bloccando l'uso dei dati personali al di fuori del proprio consenso. Per cui la caratteristica cardine di un sistema di gestione delle identità basato su blockchain è il decentramento. Un identificatore decentralizzato è un servizio di identificazione/certificazione che stabilisce un registro distribuito o un sistema decentralizzato utilizzando appunto la tecnologia blockchain. Quest'ultimo a differenza dell'identificazione/autenticazione esistente viene emesso da un'agenzia, ma, come illustrato viene gestito dall'interessato stesso. Gli individui possono archiviare i certificati emessi da una singola organizzazione finanziaria o affiliata, nonché creare identità separate per l'uso previsto. La blockchain permette di fornire all'infrastruttura fiducia e di conseguenza fornirla a tutti coloro che fanno parte della rete.

I governi svolgono molti ruoli, che vanno dall'emissione e mantenimento delle identità degli individui, all'identificazione, fino alla fornitura di fonti di identificazione. Per cui i servizi di governo digitale sono i primi che trarrebbero numerosi vantaggi nel creare

fiducia tra il governo e i suoi cittadini, nell'ambito dell'identità digitale. Molti paesi stanno attuando politiche che consentono la condivisione di informazioni, inclusi dati governativi e dati relativi alle politiche, attraverso la digitalizzazione per indurre la partecipazione attiva dei cittadini al processo decisionale e garantire la trasparenza dei processi. Tra queste iniziative è necessario inserire lo sviluppo di sistemi di identità digitale basati su blockchain, che possano incentivare l'innovazione e portare vantaggi economici ai governi, fornendo un'autenticazione online sicura e affidabile. In particolare, questi sistemi ridurrebbero anche i costi associati al servizio clienti e aumenterebbero la soddisfazione degli utenti con transazioni rapide e sicure.

La Corea del Sud, che è nota come leader globale nell'innovazione tecnologica e nello sviluppo dei servizi online governativi, ha recentemente lanciato l'iniziativa Decentralized Identity (DID) e ha istituito la Decentralized Identity Alliance Korea Association. La DID Alliance è un'associazione industriale aperta che è stata istituita per i servizi di identità decentralizzata nel tentativo di sviluppare un framework standardizzato e intercambiabile per garantire l'affidabilità della verifica dell'identità digitale.

5. BLOCKCHAIN E BIG DATA

Prima di arrivare alla conclusione di tale documento è importante trattare un ultimo essenziale tema che permette di comprendere ulteriormente come la blockchain può svilupparsi nel futuro, andando ad integrarsi con un'altra tecnologia che segna ormai la nostra era: i big data.

Il traffico dati è aumentato a livello globale a un ritmo senza precedenti nell'ultimo decennio, da qui l'interesse speciale per i "big data". Si stima che il mercato dei big data raggiungerà i 229,4 miliardi di dollari entro il 2025 e ridurrà significativamente la spesa in vari settori verticali come sanità, trasporti, produzione e intrattenimento. I big data possono essere identificati come una nuova generazione di tecnologie studiate per analizzare una grande quantità di dati e catturarne le caratteristiche principali. I big data hanno dimensioni elevate da non poter essere archiviati, gestiti, analizzati e catturati da strumenti di database convenzionali e richiedono metodi di ridimensionamento orizzontale significativi per un'elaborazione efficiente. Sebbene il settore privato stia guidando lo sviluppo di applicazioni per i big data, anche il settore pubblico ha iniziato a ricavare informazioni utili per supportare il processo decisionale in tempo reale dalla rapida crescita dei dati da più fonti, tra cui il web, i sensori biologici e industriali, i video, le e-mail e le comunicazioni sociali. Molti articoli pubblicati su riviste scientifiche e rapporti aziendali hanno proposto modalità con cui i governi possono utilizzare i big data come aiuto per servire i propri cittadini in maniera più efficiente e superare diverse sfide a livello nazionale come l'aumento dei costi sanitari, la creazione di posti di lavoro, i disastri naturali e il terrorismo. È stato mostrato, però, anche un certo scetticismo sul fatto che i big data possano effettivamente migliorare le operazioni strategiche del governo, poiché questi ultimi dovrebbero sviluppare nuove capacità e adottare nuove tecnologie per trasformare le informazioni in azioni, attraverso l'organizzazione e l'analisi dei dati. A tale sfida si affianca l'esigenza di risolvere alcune problematiche tecniche associate agli attuali sistemi di big data, come la sicurezza e la privacy dei dati, la scalabilità dei computer, la gestione dei dati, l'interpretazione dei dati, l'elaborazione dei dati in tempo reale e l'intelligenza dei big data. Tuttavia, un reale utilizzo pratico dei big data da parte delle istituzioni governative e l'implementazione del suddetto sistema possono trovare un'unica soluzione: il ricorso alla tecnologia blockchain. La blockchain ha il potenziale necessario per trasformare gli attuali sistemi di big data fornendo funzionalità di sicurezza e privacy efficienti e capacità di gestione della rete per abilitare servizi e applicazioni di big data emergenti. In tal modo i governi dovrebbero comunque dotarsi di una nuova

struttura tecnologica, ma che permetterebbe di soddisfare più esigenze contemporaneamente. Con la blockchain le istituzioni governative potrebbero mettere in atto le applicazioni precedentemente esposte e da queste ricavare ed elaborare dati per orientare il proprio operato. I big data forniscono al governo una migliore comprensione del proprio popolo: abitudini, interessi, gusti, preferenze, fino ad arrivare a prevedere ciò che vogliono le persone e di conseguenza offrire pubblicità e programmi appropriati ai bisogni e alle preoccupazioni. I big data e la blockchain possono aiutare le istituzioni governative nell'instaurare e progettare una governance intelligente e appropriata fornendo servizi veloci, efficaci, affidabili e maggiormente personalizzati ai propri cittadini.

CONCLUSIONE

La tecnologia blockchain dal 2008 ad oggi ha subito delle fasi evolutive e applicative che le hanno permesso di espandersi ed affacciarsi a numerosi campi di interesse, fino ad arrivare all'argomento approfondito in tale documento, ovvero l'utilizzo presso le istituzioni governative. Tale espansione può essere riassunta in cinque fasi essenziali, che delineano anche la presa di coscienza delle diverse potenzialità associate alla blockchain:

1) *La blockchain come libro mastro per la realizzazione dei Bitcoin*: nel 2008 Satoshi Nakamoto ha pubblicato un articolo introducendo il Bitcoin, la prima applicazione pratica della blockchain. Il bitcoin ha avuto successo in quanto valuta digitale supportata da un sistema peer-to-peer per i pagamenti online, dove tali pagamenti possono essere effettuati direttamente tra gli utenti della rete senza la necessità di una autorità centralizzata. Il Bitcoin nasce e si diffonde come una valuta non regolamentata, né di proprietà di alcuna banca/autorità centrale. Nel 2009, il Bitcoin è stato rilasciato come open source (versione 0.2) ed è stato creato il Genesis Block (il primo blocco in Blockchain) per abilitare la prima transazione Bitcoin.
2) *La Blockchain per la gestione di altro valore virtuale*: questa fase si è caratterizzata per la creazione di altre valute virtuali, in cui la blockchain è stata sviluppata come open source e varie criptovalute sono state create come risultato del riconoscimento del potenziale e della efficacia della blockchain.
3) *Applicazione come registro delle transazioni*: il funzionamento della blockchain, senza la necessità di una autorità centralizzata, per la gestione delle transazioni ha reso ideale l'applicazione di tale tecnologia non solo per la gestione delle informazioni riguardanti le criptovalute, ma anche per le transazioni di beni e servizi. Si è passati quindi dalla applicazione riguardante transazioni di beni astratti a transazioni di beni materiali, come il trasferimento di proprietà di veicoli o immobili.
4) *Applicazione come registro dei diritti*: In questa fase dell'espansione della blockchain, è stato elaborato l'utilizzato per la redazione di registri di proprietà e di diritti per garantire l'autenticità. Con l'ampliamento della fiducia in tale tecnologia si è allargata l'applicazione nel campo dei diritti e delle procedure istituzionali che richiedono verifiche e veridicità. Esempi di tali applicazioni sono la conservazione dei documenti ufficiali, fino ad arrivare ai voti espressi.
5) *Registrazione di procedure ed elaborazioni future (automazione)*: tale fase si caratterizza per l'obbiettivo di ricerca di automazione in ogni trattamento dati tramite

blockchain, in cui i programmi vengono utilizzati per registrare future procedure ed elaborazioni. Ad esempio, la Blockchain può essere utilizzata per depositare transazioni, esecuzioni automatiche di contratti intelligenti ed elaborazioni automatiche da parte di altri dispositivi associati.

Il percorso descritto è esemplificativo del processo di evoluzione subito e ancora in atto della blockchain. Oggi questa tecnologia sembra possedere tutte le caratteristiche necessarie per sopperire vaste carenze presenti negli attuali sistemi operativi pubblici e privati e soddisfare importanti esigenze di natura pratica-amministrativa per la società. È indubbio, infatti, che uno scopo chiave del progresso e dell'innovazione è la ricerca di un maggiore benessere per la collettività, e tale obbiettivo sembra essere pienamente abbracciato dalle applicazioni della blockchain. Inoltre, in un mondo sempre più connesso istantaneamente tramite i devices, internet e i social media appare doveroso ricercare degli strumenti per gli istituti governativi altrettanto immediati e in grado di creare delle reti di informazioni, valori e fiducia altamente integrate.

BIBLIOGRAFIA

- Zhangyue Shi, Chen Kan, Wenmeng Tian, Chenang Liu. "*A Blockchain-Based G-Code Protection Approach for Cyber-Physical Security in Additive Manufacturing*" - J. Comput. Inf. Sci. Eng., Agosto 2021
- Alfredo J. Perez, Sherali Zeadally. "*Secure and privacy-preserving crowdsensing using smart contracts: Issues and solutions*" – Elsevier, Luglio 2021
- Aishah Alfrhan, Tarek Moulahi, Abdulatif Alabdulatif. "*Comparative study on hash functions for lightweight blockchain in Internet of Things (IoT)*" - Elsevier e Zhejiang University Press, 2021
- Mohammad Hamdaqa, Lucas Alberto Pineda Met, Ilham Qasse. "*iContractML 2.0: A domain-specific language for modeling and deploying smart contracts onto multiple blockchain platforms*" – Elsevier, 2021
- P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand, V. Vasudevan. "*Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm*" – Elsevier, 2020
- Zain Ul Abadin, Madiha Haider Syed. "*A Pattern for Proof of Work Consensus Algorithm in Blockchain*" - Association for Computing Machinery, Austria 2021
- Josef Pieprzyk. "*Evolution of Cryptographic Hashing*" – Historia, Settembre 2010, Australia
- "*Explained: What Is Hashing in Blockchain?*" – Bybit Learn, 17 Dicembre 2020. https://learn.bybit.com/blockchain/what-is-hashing-in-blockchain/
- *EBSI, European Blockchain Services Infrastructure* – European Union Official Site https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi#:~:text=EBSI%20is%20the%20result%20of%20the%20European%20Blockchain,with%20the%20highest%20standards%20of%20security%20and%20privacy
- *Blockchain in Illinois* – Illinois government site https://www2.illinois.gov/sites/doit/pages/BlockChainInitiative.aspx
- "*Illinois Releases Its First Official Government Report on Blockchain*" – Government technology 2022 https://www.govtech.com/computing/illinois-releases-first-official-government-report-on-blockchain-.html

- Berryhill, J., Bourgery, T. and Hanson, A. (2018), "*Blockchains unchained: blockchain technology and its use in the public sector*" - OECD Working Papers on Public Governance, No. 28, p. 53.
- Thomas McGhin, Kim-Kwang Raymond Choo, Charles Zhechao Liu a, Debiao He. "*Blockchain in healthcare applications: Research challenges and opportunities*" – ELSEVIER, Journal of Network and computer application, 2019
- Sanjeev Verma, Ashutosh Sheel. "*Blockchain for government organizations: past, present and future*" - Emerald Insight, 2021
- Himanshu Falwadiya and Sanjay Dhingra. "*Blockchain technology adoption in government organizations: a systematic literature review*" - Emerald Insight, 2022
- Philip Boucher, Susana Nascimento, Mihalis Kritikos. "H*ow blockchain technology could change our lives*" – STOA, Brussels European Union 2017
- Ahmed Alketbi, Qassim Nasir, Manar Abu Talib. "*Blockchain for Government Services – Use Cases, Security Benefits and Challenges*" – IEEE Xplorer, 15th Learning and Technology Conference (L&T), 2018
- Tripti Rathee, Parvinder Singh. "*A systematic literature mapping on secure identity management using blockchain technology*"- Journal of King Saud University, Computer and Information Sciences, 2021
- Chang Soo Sung, Joo Yeon Park. "*Understanding of blockchain-based identity management system adoption in the public sector*" – Emerald Insight, 2021
- Oleksii Konashevych. "*Constraints and benefits of the blockchain use for real estate and property rights*" - Journal of Property, Planning and Environmental Law, bolume 12 capitolo 2, Emerald Insight, 2020
- Nir Kshetri, Jeffrey Voas. "*Blockchain in Developing Countries*" - IEEE Computer Society, Aprile 2018
- Zaher Ali Al-Sai, Laith Mohammad Abualigah. "*Big Data and E-government: A review*" - 8th International Conference on Information Technology (ICIT), 2017
- N. Deepa, Quoc-Viet Pham, Dinh C. Nguyen, Sweta Bhattacharya, B. Prabadevi, Thippa Reddy Gadekallu, Praveen Kumar Reddy Maddikunta, Fang Fang, Pubudu N. Pathirana. "*A survey on blockchain for big data: Approaches, opportunities, and future directions*"- Elsevier 2022