Analytica
FOR INTELLIGENCE AND SECURITY STUDIES

Cyber spazio: il futuro tra innovazione e sicurezza.

Parla William Nonnis.

Serangelo Denise

Analytica for intelligence and security studies

Interviste

Cyber spazio: il futuro tra innovazione e sicurezza.

Serangelo Denise

Correzioni e revisioni a cura del Dottor PANEBIANCO Andrea

Torino, giugno 2020

William Nonnis, Full Stack & Blockchain Developer del Ministero della Difesa, classe 1982, da oltre vent'anni si occupa di sviluppo software, siti web e web application, si occupa di studio, progettazione e sviluppo blockchain dal 2012 ed è tra i 10 Top Influncer Blockchain Developer per MondoCrypto.
Si definisce un purista della blockchain, attualmente la sua più grande attività e ambizione sicuramente è quella di divulgare questo protocollo in modo da fornire vantaggi orizzontali alla portata di tutti.
Successivamente è stato inserito nello Staff Tecnico Italian Open Lab (studio, progettazione e sviluppo su Blockchain, AI, IoT e Applicazioni WEB, per il Ministero della Difesa). Attualmente risulta in forza presso la Struttura di Progetto Energia (che fa capo al Ministro della Difesa), dove Il compito della Struttura di Progetto Energia e il miglioramento dell'efficienza energetica ed il risparmio a capacità dello stesso di ottimizzare l'utilizzo dell'energia all'interno della Difesa con diffusione nella PA, questo comporta la possibilità di uno studio, progettazione e sviluppo, su l'utilizzo della blockchain e sulle infrastrutture critiche.

Dottor Nonnis, lei è uno dei massimi esperti in Italia in fatto di Blockchain, una innovativa, quanto sconosciuta, tecnologia che può rivoluzionare il mondo cibernetico.

Potrebbe spiegarci in cosa consiste questa nuova frontiera tecnologica nel dettaglio?

Il dettaglio tecnologico è sicuramente importante, però l'aspetto più rilevante di questa tecnologia è il **"cambiamento".** Il mio cavallo di battaglia da anni è l'attenzione che dobbiamo prestare ad un **cambio di paradigma culturale e sociale**, che porterà ad una **trasformazione radicale e profondissima nei rapporti sociali.** Tutto questo partendo da un tassello fondamentale: **formazione e informazione** a beneficio della comunità (cittadini, professionisti, aziende ecc). Questi infatti **si baseranno sulla fiducia e la trasparenza tra le parti**. Inoltre assisteremo a una metamorfosi culturale, per far sì che tutte le ingenti potenzialità di questa innovazione possano essere utilizzate appieno. La definisco una tecnologia sociale che impatta dal basso verso l'alto e coinvolge con responsabilità il singolo individuo in ogni sua attività in base al settore coinvolto. L'uomo al centro di tutto per apportare benefici e semplificazioni nella nostra vita quotidiana

Quali sono le caratteristiche della blockchain che la rendono appetibile per il mondo del business?

Ricordiamo che parliamo di Blockchain (quella vera cioè pubblica e permissionless). Brevemente riassumiamo le sue principali caratteristiche e potenzialità: è un registro digitale pubblico distribuito di transazioni liberamente accessibili e basato sul consenso tra i partecipanti alla rete stessa; permette la notarizzazione, ovvero la marcatura temporale di una transazione e per questo si serve dell'impiego intensivo della crittografia e della firma digitale.

L'elemento innovativo, anche rispetto ad altri sistemi tecnologici, è che non esiste più una logica di centralizzazione, anche nelle sue forme evolute decentralizzate, ma una forma distribuita e orizzontale delle informazioni.

Un sistema centralizzato, tanto per chiarire, è un computer connesso a un server centrale dove è possibile recuperare informazioni. Quello decentralizzato è esemplificabile con un sistema bancario che è tenuto a inviare alla Banca Centrale Europea le transazioni svolte nella giornata. Nel sistema distribuito tutti i partecipanti alla rete di servizi hanno la possibilità di effettuare mining (modo utilizzato dal sistema bitcoin e dalle criptovalute in generale per emettere moneta) o validazioni.

Altro importante aspetto del sistema distribuito introdotto dalla blockchain è l'immutabilità del dato: una volta che una transazione è iscritta, non si può né modificare né cancellare e quindi otteniamo finalmente la certezza di una transazione.

Quali sono i principali ambiti applicativi e i progetti in corso in Italia e all'estero su questo tema?

In Italia ad oggi ci sono progetti molto validi in tanti settori che sono in parte realizzati e alcuni in fase di realizzazione che vanno dal food (foodchain e Quadrans), ecosistema per far girare valore tra aziende (AtromG8, EvoDigitale e Biotai).

Un altro progetto molto interessante sono i titoli di studio su blockchain con Università Poliarte Accademia di Belle Arti e Design, dove all'interno del progetto troviamo ReS On Network (è un Hub Research con sede in UK e in USA e Italian branch, che si occupa dello studio delle Reti e delle Infrastrutture critiche) e con il supporto di Partner per la formazione e lo sviluppo della piattaforma (AtromG8, EvoDigitale e Biotai).

Quali sono i punti che un CEO e top manager dovrebbero tenere in considerazione per le loro aziende pensando al futuro del blockchain?

Sicuramente iniziare a studiare realmente i processi interni aziendali della propria attività, valutare i costi e benefici, ma mettendo sempre l'uomo al centro della tecnologia. Le aziende hanno una grande occasione di innovare con la Blockchain, AI, IoT, creare valore, business e accedere a dei fondi Europei inutilizzati (o parzialmente) per queste tecnologie. Quindi anche i CEO e TOP Manager devono passare attraverso una **formazione e informazione** in questo caso a beneficio del loro processo aziendale, ma soprattutto farsi guidare da chi realmente ha le competenze e sa formare i componenti di un'azienda. Per questo dico sempre alle aziende chiedete sempre chi è già dentro in questo campo da anni. Devono essere per primi loro a capire questo cambiamento epocale. Assimilare che si sta passando dopo tanti secoli di economie e business improntati su figure e istituzioni di intermediazione fiduciaria verso approcci e relazioni dirette, garantite da protocolli che assicurano reciprocamente gli attori di un qualsiasi contratto o scambio.
Quindi saranno in grado di portare le aziende che rappresentano verso il futuro. Un buon futuro per loro, per l'azienda e per tutti gli stakeholder coinvolti.

La tecnologia blockchain è intrinsecamente legata al mondo delle criptovalute.

Uno degli usi di questa tecnologia è per il trasferimento di denaro eseguito con l'aiuto, appunto, delle criptovalute. Si tratta di transazioni estremamente sicure e senza addebiti.

In un mondo sempre più esposto ad hacker e violazione della privacy, la blockchain diventa uno strumento essenziale per la verifica delle informazioni.

Le criptovalute sono anche uno strumento molto usato per il finanziamento delle attività terroristiche, pensa che in futuro, i blockchain possano aiutare oppure ostacolare il tracciamento dei flussi di denaro diretti verso organizzazioni eversive e terroristiche? In che modo?

La Blockchain come ben sapete è nata per transazioni finanziarie, cioè il Bitcoin. Quindi è arrivato Ethereum. A me piace identificare la scintilla della necessità della blockchain con la crisi della Lehman Brothers. I registri per tutti noi erano ancora qualcosa di sacro.

Tutta la nostra fiducia era riposta in quello che veniva scritto sui registri.

Coloro che hanno permesso di far crollare una banca gigantesca come Lehman Brothers, che secondo lo stereotipo era troppo grande per fallire (too big to fail), non ha solo fatto fallire una banca ma ha fatto crollare la fiducia nel sistema generale.

Oggi non possiamo più permetterci di affidare i registri delle nostre attività commerciali, dei nostri soldi, delle nostre vite a soggetti di cui dobbiamo fidarci.

Dobbiamo essere in grado di poter verificare in ogni momento e con strumenti semplici i registri che governano le nostre società, ma questi stessi registri devono essere nostri.

Nostri, verificabili, immutabili, trasparenti e ubiqui.

Niente e nessuno più che si frappone nelle relazioni tra gli individui, tra le aziende, tra le aziende e gli individui. Solo un protocollo di regole condivise e transazioni di qualsiasi natura e genere che possono essere in qualsiasi momento controllate e verificate da chiunque.

Per quanto riguarda il finanziamento di attività terroristiche ha pienamente ragione ma queste vengono finanziate anche con i contanti, con il riciclaggio dei soldi ecc.

Attribuire alla tecnologia questa colpa non credo sia giusto. Ricordiamoci che la tecnologia viene sempre utilizzata mediante un click dall'uomo. L'esempio più pratico e banale che conosciamo tutti è quello del coltello: si può utilizzare per tagliare la carne o alimenti o per uccidere le persone. Dipende sempre dall'essere umano, che in questo caso ribadisco va istruito con **formazione e informazione** per l'utilizzo delle tecnologie. Detto questo le statistiche sono particolarmente confortanti e ci indicano che le transazioni di criptovalute per scopi illegali sono una piccolissima percentuale, circa l'1% del totale. Il motivo è abbastanza chiaro: nella blockchain tutto è tracciato e immutabile e la titolarità dei wallet è pseudonima. Quindi, in qualche modo e con un pò di difficoltà, è possibile risalire al proprietario.

Sicuramente la blockchain da un grande supporto alla tutela del dato da eventuali attacchi hacker e alla privacy, perche in una blockchain pubblica non tutto viene reso pubblico. Prendiamo esempio da bitcoin: noi possiamo vedere due indirizzi e l'importo trasferito, stop. Se volessimo vedere i dettagli bisognerebbe avere le chiavi private in possesso esclusivo dei proprietari dei wallet. La blockchain può aiutare ad eliminare e far emergere la piaga sociale che sono i pagamenti in nero a beneficio di tutta la comunità.

In Italia è assai difficile allontanarsi dalla logica che vuole internet e le tecnologie ad esso collegate come qualcosa di cui diffidare.

In un'era in cui la IoT (Internet of things) sembra ormai realtà come si colloca il nostro paese in questa corsa tecnologica?

Siamo pronti al cambiamento che ci investirà oppure rimarremo tagliati fuori dalla competitività economica a causa di queste catene culturali.

Oggi in Italia opponiamo ancora resistenza verso il digitale nonostante siamo la nazione al mondo che utilizza e compra più device. Ma come ben sappiamo comprare un device non vuol dire conoscere internet e la tecnologia. Oggi il diffondersi massivo della tecnologia IoT o meglio l'IoE (Internet del Tutto) ci mette nelle condizioni di evolverci per poter apprezzare meglio ed essere più efficienti nella nostra quotidianità.

Prendiamo ad esempio gli assistenti personali intelligenti (esempio Alexa, Google Home, ecc.), ma anche tutti gli elettrodomestici intelligenti e totalmente connessi. Per poterli sfruttare al meglio e renderli al nostro esclusivo servizio dobbiamo avere più consapevolezza e di conseguenza più controllo, altrimenti queste macchine, con la loro intelligenza e la loro invasività. diventano solo un cavallo di troia al servizio dei loro produttori che le usano per ricavarne informazioni sui nostri comportamenti. E chiaramente, anche, rivendere questi dati trasformati in informazioni al miglior offerente.

E' fondamentale altresì che chi produce IoT certifichi sia apparato hardware che software. E qua entriamo anche in un grande problema di sicurezza nazionale, dove ad oggi nessuna società produttrice di ioT certifica ne Hardware ne software. Questo genera ovviamente tante paure e perplessità. Reputo che l'Italia sia pioniera e visionaria in ambito tecnologico, ma molte volte purtroppo veniamo frenati da un'eccessiva burocrazia.

Giusto per fare un esempio, lo Stato italiano ha avuto la lungimiranza di regolamentare per prima nella UE, tramite l'art. 8-ter del 11 febbraio 2019, l'utilizzo delle DLT e degli SMART CONTRACT (anche se è una norma da migliorare in alcuni aspetti). Così facendo, la nostra Nazione, ha dimostrato grande attenzione ed interesse per la straordinaria innovazione tecnologica. Questo potrà potrebbe permetterci di diventare un paese pionieristico assolutamente all'avanguardia nel digitale. Per attuare questo ambizioso progetto, l'Italia comunque dovrà affidarsi al supporto di quelle nazioni in cui la tecnologia blockchain risulti già essere di utilizzo quotidiano (Estonia, Lituania, Finlandia, Malta), calando o adattando i contesti quotidiani di tali Stati anche alla nostra Nazione sia per il concetto di utilizzo Pubblico verso il cittadino che per l'utilizzo tra cittadino e azienda privata. In poche parole, poiché molto stiamo già facendo, non facciamoci sfuggire questa grossa opportunità di valorizzazione della Nazione.

L'IoT collega persone, luoghi e prodotti, e così facendo, offre opportunità per la creazione di valore. Esistono però ancora una serie di problemi tecnici e di sicurezza che non sono stati affrontati. La sicurezza è una delle principali problematiche dell'IoT che ne ha ostacolato la diffusione su larga scala. I dispositivi IoT soffrono spesso di vulnerabilità, che li rende un facile bersaglio per gli attacchi DDoS (Distributed Denial of Service).
Come può essere applicata la tecnologia blockchain all' IoT e quali sono i rischi reali per la sicurezza delle informazioni che condividiamo (o condivideremo) con questo sistema? Come farvi fronte?

Gli IoT sono ormai delle estensioni della nostra esistenza. Come detto prima, dobbiamo abituarci a chiamarli IoE. Fanno parte di noi, sono in noi. E proprio per questo dobbiamo prenderci cura in

modo più deciso e consapevole di come interagiamo con loro. Ma soprattutto di come loro e di conseguenza noi interagiamo con i depositari dei dati che raccolgono.

La sicurezza degli IoE deve essere affrontata da 3 punti di vista differenti:

1. Essendo interconnessi con tutto sono facilmente raggiungibili da malintenzionati che possono usarli come strumenti attivi di attacchi o minacce verso altri obiettivi. Oggi per un hacker è facile fare incetta di decine di migliaia di IoE e poi ordinare loro attacchi DDoS verso servizi cloud o server o entità digitali importanti. O possono essere usati come porta di ingresso del nostro fortino domestico (ho usato il termine 'fortino' in modo ironico nel sapere come è gestita la sicurezza nelle nostre case) per poi prendere possesso di tutto ciò che è in rete e quindi raggiungibile (frigoriferi, lavatrici, aspirapolvere, tablet, smartphone, pc, smart TV, allarmi, videocamere, ecc.). Quindi possono essere le armi con cui vengono compiute azioni atte ad arrecare danni.
2. Dobbiamo accertarci che la raccolta dei dati riferiti ai nostri comportamenti, alle nostre abitudini siano dovuti solo ed esclusivamente a migliorare il servizio. La loro presenza non deve essere rivolta allo sfruttamento di quello che è surplus comportamentale da dare in pasto alle macchine intelligenti che poi li trasformano in prodotti da vendere al mercato dei comportamenti futuri. **Ritengo essere questo in assoluto il pericolo più importante a cui rivolgere la nostra attenzione**. C'è in gioco la nostra libertà e la nostra idea di essere individui autodeterminanti. Dopo secoli di cammino verso questa meta fondamentale per la nostra evoluzione rischiamo un clamoroso passo indietro dovuto all'uso sconsiderato e deliberatamente voluto da chi costruisce questi strumenti che dovrebbero servire solo per rendere la nostra vita più efficiente.
3. E' nostra cura provvedere alla manutenzione e all'aggiornamento di queste macchine. Un PC lo aggiorniamo diverse volte l'anno. Così come lo smartphone o il tablet. Mentre tutti gli altri device vengono abbandonati a se stessi e messi a disposizione di chiunque voglia

accedervi. Torniamo quindi sempre al solito punto: **istruzione**, **formazione**, **consapevolezza**, **protezione**, **libertà**.

La blockchain è un registro che deve essere popolato da dati specifici per lo scopo per cui è stata creata. I dati vengono inseriti da quello che si chiama Oracolo. Spesso l'Oracolo è un IoT. Per tutto quello che abbiamo appena detto se l'IoT non ha le caratteristiche e la cura adeguate il rischio di inserire in blockchain dati 'sporchi', la cui natura è data da strumenti non certificati e insicuri, è molto elevato.

Facciamo l'esempio del Food dove i dispositivi IoT sono veramente tanti. Nel momento in cui non si mette in sicurezza l'intera infrastruttura (definita critica in questo caso) il rischio che l'informazione sia manipolata esiste. Ma non manipolata perche modificano il dato in blockchain. Il problema è a monte, nei componenti IoT che non vengono garantiti da chi li ha prodotti e da chi poi deve averne estrema cura.

Ecco perche bisogna sempre avvalersi di audit autorevoli e professionali in campo Cyber con esperti che possono dare un supporto alla rete e all'infrastruttura. Non mettersi mai in mano a pseudo esperti.

Il 25 aprile 2020 la Cina ha presentato al mondo la il Blockchain-based service network (Bsn), ossia una piattaforma commerciale per sviluppare servizi basati sulla tecnologia dei registri distribuiti, su cui Pechino ha messo al lavoro ministeri e grandi colossi di stato da sei mesi. L'obiettivo, come si legge in uno dei documenti ufficiali dell'iniziativa, è fornire un'infrastruttura pubblica, che offra a sviluppatori e piccole aziende risorse per costruire servizi e applicazioni basate sulla blockchain a costi accessibili. O, come è meglio spiegato verso la conclusione dei documenti, diventare "l'internet delle blockchain".

Uno standard comune di trasmissione a livello globale, le cui chiavi di accesso sono in mano alla Cina. Il Bsn, una volta avviato completamente, sarà la sola rete globale di infrastrutture innovative realizzata in modo autonomo da realtà cinesi.

Cosa significa questo per il futuro della blockchain e quali implicazioni ha sullo sviluppo delle diverse tecnologie? Quali implicazioni si sicurezza ci potranno essere?

Sicuramente la Cina ha dato un nuovo scossone economico e tecnologico appunto con la Blockchain. I rappresentanti della piattaforma hanno riferito che attualmente BSN ha 128 nodi pubblici. 76 di questi si trovano in Cina, 44 sono in fase di settaggio, altri 8 si trovano al di fuori della Cina su tutti e sei i continenti (il 6 è l'Antartide). Fino alla fine del 2020, il numero di nodi dovrebbe arrivare a 200. Questo comporta che la Cina si conferma ancora leader mondiale nelle tecnologie. Questo grazie ad una visione e strategia di avere un digital divide molto basso. Pensiamo solo che iniziano a fare coding e AI dalle elementari! Avrà un po' di difficoltà come credibilità a livello di nodi perchè comunque una grossa parte dei nodi e in Cina. Questo porta l'utente medio ad aver paura a realizzare Dapps sulla loro piattaforma. Dovuto anche al problema di gestione e trattamento dei dati personali dove notoriamente non eccellono.

C'e da dire però che, notizia di pochi giorni fa, risulta che il nuovo codice civile cinese all'esame della sessione annuale dell'Assemblea nazionale del popolo in corso a Pechino contiene norme per la tutela dei dati personali e della privacy. Quindi dobbiamo attendere sviluppi e affidarci al buon senso di chi detiene le tecnologie.

Blockchain e sicurezza dello spazio cibernetico, quale futuro per queste due tecnologie?

Lo spazio cibernetico "Quinto Dominio" è una dimensione creata dall'uomo trasversalmente ai domini tradizionali terrestre, marittimo, aereo e spaziale le cui principali caratteristiche sono l'assenza di geospecificità e le limitate capacità di attribuzione.
Nel cyber space i governi svolgono una serie di attività che vanno dallo spionaggio al warfare. Gli attacchi posso essere classificati in funzione del loro scopo per manipolare informazioni, propaganda, hacktivismo, cyber crime, spionaggio elettronico, terrorismo e per facilitare attacchi cinetici (attacco militare tradizionale).
Negli ultimi anni le capacità offensive in grado di recare gravi danni sono aumentate incrementando la vulnerabilità dei dati personali e degli erogatori di servizi trasformati dalla digitalizzazione in Infrastrutture Critiche (I.C.).
In risposta a queste minacce il Parlamento Europeo ha adottato la direttiva National Information System sulla sicurezza dei sistemi delle reti per prevenire e contrastare gli attacchi cyber. I settori che rientrano nell'ambito dell'applicazione del decreto sono quelli relativi al settore energetico, trasporti, finanza, sanità e forniture sia pubbliche che private. In Europa l'area della ricerca e sviluppo è affidata al comparto sicurezza che si occupa della protezione delle reti e delle informazioni militari sia su territorio nazionale che estero insieme al Comando Interforze per le Operazioni Cibernetiche e al Computer Network Operation operanti anche in ambito NATO.

A queste tecnologie si aggiunge l'impiego delle Intelligenze Artificiali (I.A.), sistemi in grado di apprendere, svolgere compiti e risolvere problemi. Sono distinguibili in due categorie: Debole (software che risolve problemi e prende decisioni autonomamente) e Forte (sistema che emula le capacità intellettive della mente umana sviluppando propri processi di ragionamento). Gli Assistenti Virtuali ne sono un esempio che sfruttando algoritmi di machine learning e di analisi comportamentale producono risposte sulla base delle esigenze degli utenti. Le I.A più efficienti prevedono l'interazione di un gran numero di device che elaborando metadati permetterebbero di farle evolvere. La tecnologia Internet nata come una rete distribuita con il tempo per praticità è stata trasformata in una centralizzata che però nel prossimo futuro non sarà in grado di soddisfare la crescente domanda dei cittadini/utenti. Saranno quindi le strutture decentralizzate a permettere di lavorare su architetture informatiche più potenti ed efficienti. Non sarà necessario un ente centrale per la gestione delle informazioni che potranno invece essere scritte, validate e confermate grazie a meccanismi di trasparenza e affidabilità migliorandone la qualità e la sicurezza dei servizi.

Quali saranno in futuro le minacce che potranno essere fronteggiate grazie a questa tecnologia e quali invece sono le nuove minacce che si affacciano grazie al loro utilizzo?

Le minacce in futuro possono essere fronteggiate con tutte le tecnologie sviluppate e utilizzare in maniera corretta, ma sappiamo benissimo che la certezza della sicurezza in ambito digitale non esiste, possiamo avvicinarci al 90% ma abbiamo sempre un grosso problema che il 100% non esisterà mai.

Le minacce vengono sempre e solo dall'Uomo. Le tecnologie, il digitale sono degli strumenti passivi. Dipende solo ed esclusivamente da noi che uso farne. Una minaccia da fronteggiare subito è l'inevitabilità. Dopo secoli di oscurantismo in cui l'uomo non era padrone del proprio destino ora siamo al passo conclusivo di quel sentiero tracciato dai Lumi.

L'uomo al centro di tutto. L'Uomo come fine di tutto. Non dobbiamo cadere nell'errore di ritenere che il nostro destino ora sia segnato da un destino digitale già scritto. Oggi purtroppo si sente troppo spesso l'uso di questo termine: è inevitabile che siamo tracciati, è inevitabile che le macchine ci controllino, è inevitabile che il nostro futuro dipenda dalle macchine. Invece è tutto evitabilissimo, dipende sole ed esclusivamente da noi. Il nostro destino e il nostro futuro è assolutamente determinabile dalle nostre coscienze, dalla nostra volontà e dai nostri desideri di autodeterminazione. Un magnifico futuro totalmente digitale dove le macchine sono al nostro servizio, di una vita piena di agi e confort.

Nel settore militare l'uomo rimane al centro del Sistema Difesa ma la tecnologia sta diventando sempre più presente e pervasiva. In un settore così sensibile possiamo lasciare sempre più spazio alle 'macchine'?

Lasciare lo spazio alle macchine mettendo però sempre al centro l'Uomo. E' fondamentale che l'Uomo sia al centro e f**ormato ed informato** per l'utilizzo delle tecnologie. Dipenderà solo dall'Uomo farsi governare dalle macchine intelligenti o l'Uomo con la sua intelligenza governare le macchine. E' una scelta solo sua.
Io punto tutto sull'Uomo, pur con le sue debolezze, le sue contraddizioni, la sua irrazionalità alla fine prevarrà Lui.

Può spiegarci quali sono le principali applicazioni del blockchain nell'ambito militare? Come potrebbe rivoluzionare questo settore?

Il settore energetico. Dal 2013 sono in forza presso la Struttura di Progetto Energia (che fa capo appunto al Ministro della Difesa) dove mi occupo di studio, progettazione e sviluppo della Blockchain. Questo progetto ha tra gli altri gravosi compiti quello dell'efficientamento ed il risparmio energetico oltre che nelle strutture della Difesa anche nella Pubblica Amministrazione stessa (scuole, edifici pubblici ecc). Il progetto di ottimizzazione dell'utilizzo dell'energia all'interno della Difesa ha come diretta conseguenza e volontà la propagazione in tutta la Pubblica Amministrazione. Per ottenere un risultato ottimale il progetto ha bisogno di studio, progettazione e sviluppo in blockchain. Questo per assicurare protezione e garanzia delle infrastrutture critiche. Ritengo che la blockchain nel settore energetico abbia un ruolo fondamentale e nella Pubblica Amministrazione in particolar modo. La Blockchain (quella vera cioè pubblica e permissionless) nella Pubblica Amministrazione è una vera e propria necessità sia per i servizi da erogare all'utente che per la sicurezza dei dati.

Come possiamo ipotizzare l'uso delle blockchain nella tutela delle infrastrutture critiche?

Sicuramente la blockchain da una grande mano alle infrastrutture critiche, ma ha bisogno di tutti gli elementi, cyber, IoT, AI, ecc. La Blockchain insegna che le tecnologie devono essere un vettore importante e impattante a livello culturale e sociale per poter perpetuare il processo di evoluzione dell'Uomo in relazione al suo habitat e al miglioramento di una convivenza improntata sempre più su rapporti di reciproca fiducia e di relazioni solide e stabili. Di conseguenza le infrastrutture critiche nel settore energia (acqua e gas inclusi), trasporti, finanza, sanità, aggiungerei istruzione, giustizia sono importantissime per ogni singola nazione dove uno Stato deve garantire ai cittadini questi asset di primissima necessità.

Ecco questo è il ruolo della Blockchain nelle infrastrutture critiche e il supporto è fondamentale per tutte le sue principali caratteristiche che conosciamo.

Il massiccio collegamento alla rete può trasformare le infrastrutture critiche in vulnerabili?

Un massiccio collegamento non studiato, progettato e sviluppato da professionisti in maniera corretta crea un danno pazzesco. Vedi i vari attacchi del passato alle centrali iraniane nel 2006, Estonia 2007 nel settore energia e altri innumerevoli casi che purtroppo hanno un'incidentalità in costante aumento. Le infrastrutture critiche gestite male mettono in ginocchio uno Stato e questo la maggior parte delle persone non lo capisce. Quando si colpiscono settori come energia (acqua e gas inclusi), trasporti, finanza, sanità, ecc, crei un danno sociale notevole. Di conseguenza bisogna sempre affidarsi a professionisti e ogni singolo stato deve avere i suoi professionisti interni.

La vulnerabilità delle infrastrutture è dato fondamentalmente da 3 fattori (ma non solo):

- La superficie di attacco. Tanto più sono i nodi che compongono una rete tanto più questa ha punti di accesso. E' più facile entrare in un castello con un unico accesso o in un palazzo con 100 entrate?
- La velocità con cui può essere sferrato un attacco. Se posso accedere ad uno dei nodi della rete attraverso una strada lenta è più facile che io venga intercettato preventivamente e soprattutto abbia una via di fuga lenta e possa portare via poche cose. Per fare esempio concreto il 5G (a dispetto dell'attivismo complottista sterile e folcloristico) offre uno strumento notevolissimo ai malintenzionati. Perchè ora possono agire con tempistiche e una capacità di trasferimento dati notevolissima per compiere i loro atti malevoli. Ma il 5G porterà tanti di quei benefici che non possiamo certo privarcene perchè qualcuno ne farà un uso improprio.

- Le infrastrutture vanno protette già nella fase di progettazione e costruzione. È antistorico è inefficace vedere la sicurezza come un elemento da aggiungere a piacimento. Non è un componente che possiamo aggiungere al bisogno. Nel medioevo si proteggevano i castelli con il fossato attorno e il ponte levatoio. Oggi è impensabile un approccio simile. La sicurezza deve essere by design. Deve essere insita e inclusa in fase di analisi, di progettazione e di sviluppo finale. Altrimenti è totalmente inutile.