Cybersecurity Trends

Edizione italiana, N. 2 / 2018

INTERVISTE VIP:

- Mauro CERUTI
- Michele MEZZA

Central Folder: Blockchain

GLOBAL CYBER SECURITY CENTER

ISSN 2559 - 1797 / ISSN-L 2559 - 1797

Global Cyber Security

La Fondazione GCSEC è un'organizzazione senza scopo di lucro, creata per promuovere la sicurezza informatica in Italia e nel resto del mondo. Il Centro, fondato e finanziato da Poste Italiane, ha sede a Roma e collabora con Istituzioni Italiane e Internazionali Governative, enti privati, istituti di ricerca e organismi internazionali.
La missione della Fondazione è quella di sviluppare e diffondere la conoscenza e la consapevolezza sulla sicurezza informatica, creando le condizioni per migliorare le capacità, le competenze, la cooperazione e la comunicazione tra i diversi attori coinvolti nell'uso e nella protezione di Internet.

Information Sharing
Creazione di modelli di information sharing pubblico - privato

Threat Intelligence
Analisi di modelli di attacco e delle tecnologie necessarie a velocizzare l'analisi stessa

Sensibilizzazione
Campagne di sensibilizzazione multi-livello

Formazione
Attività di formazione a corsi di specializzazione e master

Fondazione Global Cyber Security Center
Viale Europa, 175 – 00144 Roma
www.gcsec.org

GLOBAL CYBER SECURITY CENTER

Blockchain o no Blockchain questo è il dilemma…

Autore: Nicola Sotira

Blockchain: parola magica in tutti gli eventi, onnipresente in tutte le riviste tecniche, nei quotidiani e accarezzata da tutte le Fintech. In alcuni casi è riuscita anche a fare lievitare il valore di qualche startup che ne ha pubblicizzato l'utilizzo in applicazioni non sempre chiarissime. Non dovremo sorprenderci se il calcio dovesse adottare, un giorno, questa tecnologia, forse per implementare un Digital Ledger sulle decisioni dell'arbitro o dei guardalinee.

Di sicuro possiamo affermare che il tema è sempre più attuale e non può essere ignorato. I dati economici sul fenomeno Bitcoin/Blockchain sono chiari: le previsioni del World Economic Forum dicono che il 10% del prodotto interno lordo (PIL) globale sarà prodotto dalla tecnologia Blockchain e la banca d'investimento UBS parla di un volume d'affari di 300 miliardi di dollari entro il 2027. Quindi, possiamo facilmente prevedere che la tecnologia Blockchain non sparirà così presto dallo scenario digitale.

La parola chiave, che viene molto spesso associata alla tecnologia del Bitcoin e Blockchain, è sicurezza; si presume implicitamente che la tecnologia non sia solo *disruptive* ma anche intrinsecamente sicura e priva di rischi.

Occorre tenere a mente che il Bitcoin e in genere le criptovalute sono controllate da una chiave privata e che chiunque abbia accesso alla chiave privata può avere accesso alla valuta; particolare questo che pone alcuni rischi. L'accesso indebito alla chiave privata potrebbe avere come conseguenza il conto svuotato. Anche le terze parti, che potrebbero detenere per noi la criptovaluta, non sono immuni da questo rischio, come è già avvenuto, tra l'altro, nella storia del Bitcoin.

Una soluzione, che potrebbe sembrarci garantire adeguata sicurezza, sarebbe mantenere la valuta nel nostro sistema, ma anche quest'ultima soluzione non ci garantirebbe l'assoluta immunità dagli attacchi e richiederebbe, in ogni caso, una notevole esperienza nel settore della sicurezza informatica.

Non dobbiamo poi sottovalutare che nel settore dell'informatica ci sono problematiche quali virus, malware, vulnerabilità ecc. da cui l'infrastruttura che regge il tema criptovalute non è esente e che potrebbero causare danni significativi. Immaginiamo poi l'impatto che queste problematiche potrebbero avere negli scenari di *smart contract* visti come una delle principali applicazioni della tecnologia Blockchain. Anche in questo caso siamo lontani dalle ipotesi, se guardiamo indietro troviamo una serie di casi reali che per fortuna hanno avuto impatto limitato.

Inoltre, in merito a quello che viene sbandierato come il vero punto di forza delle criptovalute, ovvero quello che nessuna autorità centrale può censurarle o interferire con i suoi processi: oggi possiamo convertire il Bitcoin o in generale le criptovalute in valuta locale in ogni momento e senza problemi. Dobbiamo però pensare che le autorità centrali o i governi potrebbero interrompere questo processo rendendo, a questo punto, inutilizzabile, del tutto o in parte questa valuta.

In questo mio dissertare sul tema naturalmente non ho toccato gli aspetti legati alle attività criminali. Sono molti quelli che sostengono che la diffusione del Bitcoin o in generale delle criptovalute aumenterà le possibilità del mercato legato alle attività criminali. Ritengo che questo sia ancora un altro dominio con ulteriori spunti di riflessione. Questa non è una critica alle tecnologie citate, ma è solo un invito a leggere i temi del digitale anche in modo critico, informando in modo corretto e sempre tenendo gli occhi aperti. ■

Buona Lettura

BIO

Nicola Sotira è Direttore Generale della Fondazione Global Cyber Security Center GCSEC e Responsabile del CERT di Poste Italiane. Lavora nel settore della sicurezza informatica e delle reti da oltre venti anni con un'esperienza maturata in ambienti internazionali. Contesti nei quali si è occupato di crittografia e sicurezza di infrastrutture, lavorando anche in ambito mobile e reti 3G. Ha collaborato con diverse riviste nel settore informatico come giornalista contribuendo alla divulgazione di temi inerenti la sicurezza e aspetti tecnico legali. Docente dal 2005 presso il Master in Sicurezza delle reti dell'Università La Sapienza. Membro della Association for Computing Machinery (ACM) dal 2004 e promotore di innovazione tecnologica, collabora con diverse start-up in Italia e all'estero. Membro di Italia Startup nel 2014 dove con alcune società ha partecipato allo sviluppo e progetto di servizi in ambito mobile e collabora con Oracle Security Council.

Indice


Vi aspettiamo il 13 e 14 settembre a Sibiu
per la 6a edizione di «Cybersecurity-Romania»,
piattaforma di dialogo pubblico-privato
sull'Europa Centrale. Buone ferie!
https://cybersecurity-romania.ro

Il tempo della complessità. Verso un umanesimo digitale.

Intervista VIP a Mauro Ceruti

Mauro Ceruti

Autore: Massimiliano Cannata

"Comprendere il nostro tempo significa comprendere la mondializzazione che trascina l'avventura umana, divenuta planetariamente interdipendente, fatta di azioni e reazioni: politiche, economiche, demografiche, mitologiche, religiose. Per trovare un orientamento dobbiamo interrogarci sul divenire dell'umanità, che dai motori congiunti scienza/tecnica/economia ci spinge verso un "uomo aumentato" ma per nulla migliorato, e verso una società governata da algoritmi, tendente a farsi guidare dall'intelligenza artificiale e, nello stesso tempo, a fare di noi delle macchine banali. Il trinomio cui facevo riferimento prima: scienza/tecnica/economia conduce a catastrofi a loro volta interdipendenti: degradazione della biosfera e riscaldamento climatico, che portano a immense migrazioni; moltiplicazione delle minacce mortali con l'incremento delle armi nucleari, delle armi chimiche e con la comparsa dell'arma informatica, capaci di disintegrare le società. Tutto ciò provoca angosce, ripiegamenti su se stessi, deliranti fanatismi."

Il mutamento della condizione umana ben descritto da Edgar Morin, nella prefazione del saggio di Mauro Ceruti, *Il tempo della complessità* (ed. Raffaello Cortina), offre un interessante viatico per un radicale cambiamento del nostro sguardo sul mondo. Ceruti, che Morin definisce "uno dei rari pensatori del nostro tempo ad aver compreso e raccolto la sfida che ci pone la complessità dei nostri esseri e del nostro mondo", è oggi più che mai impegnato ad affrontare le difficoltà di quest'epoca mutante, che dovrà trovare la forza prima di tutto morale per affermare un nuovo umanesimo planetario.

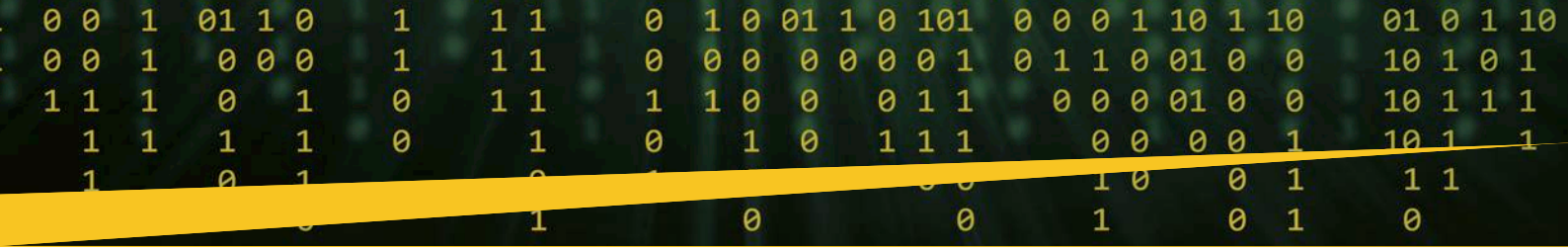
Docente di filosofia della scienza e filosofia della complessità presso l'università IUML di Milano, Mauro Ceruti, che sempre Morin definisce "spirito potente e creativo", è stato tra l'altro l'ispiratore dello splendido simposio *La sfida della complessità* tenutosi a Milano nell'ormai lontano 1984, che ha segnato una svolta nel campo della filosofia e della ricerca epistemologica.

Professore, il mondo è attraversato da instabilità, incertezze e dalla paura strisciante che possa scatenarsi una "prima guerra globale". A un filosofo non possiamo astenerci dal chiedere di aiutarci a ritrovare un orientamento. Da dove cominciamo?

Bisogna cominciare a ripensare le idee di progresso, di crescita, di globalizzazione all'interno di una *prospettiva complessa*, impegnandoci finalmente a misurare la crescita in termini diversi da quelli puramente quantitativi relativi al PIL, e mettendo in campo gli indicatori dello sviluppo umano. L'attuale modello, che non considera questo aspetto, è pienamente interno alle coazioni a ripetere di giochi a somma nulla, in cui il successo individuale viene fatalmente alimentato a scapito del bene comune. La necessità di cambiare pagina appare ormai stringente nel momento

BIO

Mauro Ceruti è uno dei pionieri nell'elaborazione del pensiero complesso. I suoi scritti, tradotti in numerose lingue, hanno segnato il dibattito filosofico negli ultimi trent'anni. Tra i suoi libri: *Il vincolo e la possibilità*, *La nostra Europa* con Edgar Morin, *La sfida della Complessità* con Gianluca Bocchi. È docente di epistemologia genetica e filosofia della scienza allo IULM di Milano.



in cui il dogma della crescita all'infinito è stato drasticamente messo in discussione dal perdurare della crisi economica europea e mondiale, e dai pericoli prodotti da uno sviluppo tecnico e scientifico che resta miope, dimenticando che una "comunità di destino" lega oggi in modo indissolubile tutti gli individui e tutti i popoli del pianeta fra loro e all'ecosistema globale, ciò che proprio Edgar Morin ha definito la nostra *"Terre-Patrie"*.

Un fatto è certo: il mondo che abitiamo è immerso nella diversità etnico-culturale, lo spazio entro cui ci muoviamo sfugge alle tradizionali categorie epistemologiche, nelle nostre città siamo sollecitati a continui confronti con l'alterità. Come possiamo definire questa epoca densa di luci e ombre?

I problemi planetari dei nostri giorni sono *complessi* e *multidimensionali*. Sono esiti di processi storici che avvengono, contemporaneamente, nei tempi brevi dell'attualità, nei tempi medi dei secoli della modernità, nei tempi lunghi della storia delle civiltà, dell'evoluzione della specie *Homo sapiens*, dell'evoluzione degli ominidi nostri antenati… Per affrontare i problemi dei nostri giorni, è necessaria una prospettiva policronica, che renda possibile vedere ogni evento all'intersezione di processi temporali ed evolutivi di dimensioni assai differenti. È solo adottando questa prospettiva per il presente e per il passato che potremo concepire le possibilità per il futuro.

Quale futuro per la "vecchia" Europa

Al tema dell'Europa Lei ha dedicato molti scritti, basti ricordare, tra gli ultimi, il bel lavoro realizzato con Edgar Morin* "La nostra Europa" *(Ed. Raffaello Cortina). Non crede che la debolezza del Vecchio Continente sia un dato con cui bisognerà fare i conti se vogliamo imboccare la strada di una ripresa solida?

Il problema politico fondamentale è oggi quello di tradurre sul piano istituzionale la tensione fondatrice dell'intera storia d'Europa. Una tensione che ha visto contrapposte la profonda diversità delle singole culture nazionali e il fatto che queste culture si siano sempre influenzate a vicenda e hanno fatto emergere, in forme diverse nelle diverse età storiche, un'*unità*, una vera e propria cultura europea. Partendo da questa consapevolezza, è necessario avviare una riflessione sugli stati nazionali, invenzione storica dell'Europa moderna volta ad affrontare la tensione fra *identità* e *diversità*, fra *unità* e *molteplicità*.

Ma è proprio lo stato nazionale, nella visione classica legata al Leviatano di Hobbes, delimitato in termini di identità e di territorio, ad aver mostrato la corda. Verso quali equilibri stiamo andando?

Dobbiamo sviluppare la conoscenza e la coscienza dell'irriducibilità e della complessità degli intrecci fra *Stati, nazioni, etnie*. Solo la comprensione di questi intrecci potrà consentire di delineare nuovi meccanismi politici e istituzionali, più adeguati alle *identità complesse* dei singoli e delle collettività. L'Unione Europea, in effetti, si è rivelata capace di disinnescare molte conflittualità storiche proprio perché, in parte, le sue istituzioni sono state modellate da un ripensamento della natura delle identità e dei territori nazionali.

Malgrado ci sia stato questo ripensamento, cui Lei fa riferimento, da più parti si paventa l'implosione dell'Europa. Dobbiamo essere pessimisti?

Oggi l'Europa è nuovamente dinanzi a un rischio di disgregazione interna e a una minaccia, esterna, ai suoi valori, alle sue regole di convivenza. La risposta deve essere all'altezza del pericolo. Siamo nel pieno di una *lotta agonica* da cui può nascere un'Europa finalmente unita, ma da cui può derivare anche un'Europa disgregata, terreno di colonizzazione per vecchie e nuove superpotenze. Nessuno potrà sottrarsi a questa scelta. Nessuno è al riparo dai pericoli, e nemmeno dalla responsabilità di costruire il proprio e l'altrui futuro.

I nazionalismi, "colpi di coda" di un mondo spaventato

Esiste un forte rigurgito di conservatorismo, agitato da chi vuole negare il progresso e l'innovazione, che non può essere ignorato. Cosa pensa al riguardo?

O si va avanti o si va indietro. E andare indietro significa scommettere sul potere taumaturgico degli Stati nazionali. Certo, in un momento di crisi, i cittadini hanno bisogno di comunità, di radici. Ma non dobbiamo dimenticare che gli Stati nazionali europei hanno già fallito rovinosamente, nel periodo della "grande guerra civile europea" fra il 1914 e il 1945. I nazionalismi dei nostri giorni sono il colpo di coda di *un mondo spaventato*.

In questa prospettiva nessun euroscetticismo può essere ammesso, non crede?

Non è più tempo. L'euroscetticismo è da "sonnambuli". Il ritorno alla piena sovranità degli Stati nazionali è fuori tempo massimo. Oggi questo ritorno è reso impossibile, se non in forme pericolose e regressive, dalla natura diventata transnazionale dei problemi fondamentali del nostro tempo: energia, migrazioni, esplosione delle conoscenze, terrorismo, economia, incontrollabilità degli sviluppi tecnologici…

La crisi della democrazia liberale è un ulteriore aspetto che merita di essere commentato. Il vento della xenofobia e il populismo (le ultime elezioni italiane ne sono testimonianza) vanno interpretate come una "temporanea risposta emotiva" o si tratta di minacce reali per la democrazia?

Gli individui non sanno più dove collocarsi, dentro la società. Assistiamo a una polarizzazione sempre più acuta fra il potere, da una parte, e individui incerti e tormentati, dall'altra. C'è un bisogno di partecipazione che fuoriesce dai quadri tradizionali della democrazia rappresentativa, e che rischia di trovare una scorciatoia: quella del leader carismatico. Per rispondere alla crisi della democrazia nei singoli Stati, bisogna osare *più democrazia* dove ancora questa è carente, cioè nelle *istituzioni sovranazionali*, e in particolare nell'Unione Europea.

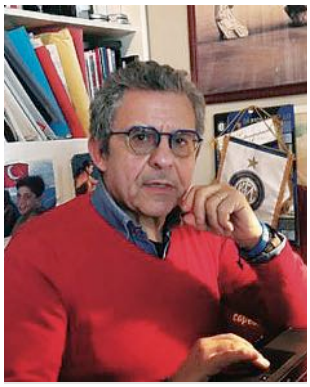
Una politica "afona", incapace di farsi sentire di fronte ai grandi oligopoli economici e alla grande finanza, rende il quadro ancora più complicato. Potremo voltare pagina?

La crisi della democrazia si intreccia con una più radicale *crisi del pensiero politico*. Mai come oggi, per la

(Continua a pagina 9)

Algoritmi e rivoluzione digitale: quale futuro?

Intervista VIP a Michele Mezza



Michele Mezza

Autore: Massimiliano Cannata

Algoritmi di libertà: la potenza del calcolo tra dominio e conflitto (ed. Donzelli) il saggio di Michele Mezza, giornalista, inviato per il Giornale Radio Rai in Urss e in Cina, docente dell'Università Federico II di Napoli e direttore del centro di ricerca sul *mobile* PollicinAcademy è stato il focus di un partecipato dibattito che si è svolto alla FIEG di Roma. I meccanismi di profilazione e individualizzazione della comunicazione sono al centro della scena, come dimostrano i casi di *Facebook*, di *Cambridge Analytica*, e di Google, il tutto trova alimento nella potenza di calcolo, che sta ridisegnando le forme della democrazia con delle conseguenze ancora difficili da prevedere per la collettività. Con l'aiuto di un autore che conosce molto bene le culture del digitale (curatore di un blog per l'*"Huffington Post"* dirige la comunità web www.mediasenzamediatori.org) proviamo a comprendere meglio la natura di questo *"salto quantico"*, che segnerà sempre più il cammino della nostra quotidianità.

Algoritmi: è la parola chiave di questa delicata fase dello sviluppo scientifico e tecnologico. Algoritmi che entrano nella politica, nell'economia, nell'informazione, nell'impresa. Cosa succede adesso?

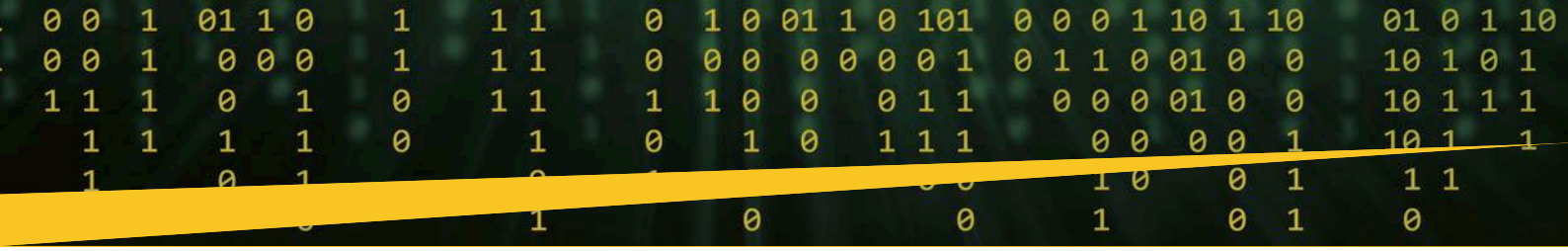
A tutte le latitudini geo politiche, in tutto il mondo, assistiamo ad un indebolimento delle forme tradizionali del potere che si sovrappone a una pressione sociale che reclama trasparenza delle *governance* e condivisione delle decisioni. Da qui si dipana poi la matassa delle nuove relazioni politiche e istituzionali che attraverso la rete stanno re-impaginando le forme del potere, con ogni tipo di dinamica, dai processi più direttamente innovatori, a forme che ricadono in un populismo digitale. Siamo ai primi passi di un processo che sta di fatto archiviando la precedente piramide della società gerarchica plasmata dalla fabbrica fordista. Però vorrei iniziare il nostro dialogo con una raccomandazione.

La ascolto…

Prima degli algoritmi nella scena politica entrano le persone, gli individui, i segmenti sociali che hanno richiesto e praticato la nuova società digitale. Dobbiamo provare a concentrarci meno sui meccanismi tecnologici e più sulle persone in carne ed ossa che stanno interpretando e richiedendo un nuovo modo di vivere di cui il sistema digitale è la conseguenza, non la causa. Queste persone chiedono innanzitutto partecipazione e protagonismo, ridisegnando la relazione fra governati e governanti in una forma paritaria, come accade in una normale conversazione. Ho scritto

BIO

Giornalista, Michele Mezza è stato inviato del Giornale Radio Rai in Urss e in Cina. Nel 1993 ha collaborato al piano di unificazione del Gr. Nel 1998 ha elaborato il progetto di Rai News 24. Attualmente dirige il centro di ricerca sul mobile *PollicinAcademy* e la comunità web www.mediasenzamediatori.org, oltre a curare un blog per l'*Huffington Post*. Insegna all'Università Federico II di Napoli. Tra i suoi titoli: *Sono le news bellezza! Vincitori e vinti nella guerra della velocità digitale; Giornalismi nella rete. Per non essere sudditi di Facebook e Google.*



questo libro per avviare e mettere all'ordine del giorno una seria riflessione culturale sull'effettiva possibilità di negoziare l'algoritmo per rendere il calcolo uno strumento dialettico e non un vincolo inesorabile.

L'insegnamento di Olivetti

Adriano Olivetti, richiamato nell'interessante prefazione del filosofo della scienza, Giulio Giorello, aveva intravisto nell'automazione la condizione perché si verificassero nuove conquiste per l'umanità. Dobbiamo pensare che il celebre imprenditore di Ivrea era forse troppo ottimista?

Penso che sia stato estremamente isolato, ma non ottimista. La sua visione, che lo portò a concepire un'accelerazione straordinaria dell'innovazione tecnologica, il "Programma 101", il primo personal computer, che decentrava all'individuo la potenza di calcolo prima riservata a pochi grandi apparati centralizzati, era proprio basato sull'idea che l'informatica fosse una tecnologia di libertà, come spiega nel discorso del 1959 tenuto al cospetto dell'allora presidente della Repubblica Giovanni Gronchi. Le nuove tecniche basate sul calcolo avrebbero – questa la tesi di fondo – emancipato l'uomo dal controllo sociale e dal lavoro alienante.

Non crede che qualcosa si sia inceppato, a giudicare dalle paure che stanno attraversando l'opinione pubblica spiazzata da questa nuova impetuosa ondata di innovazioni dirompenti?

Quello che non si è verificato, rispetto a quanto auspicato da Olivetti, riguarda il mancato processo di partecipazione e di negoziazione di queste nuove tecnologie. Quale tecnica si può considerare di per sé la soluzione di tutti i mali? Quale tecnologia del passato: dal fuoco alla scrittura, dalla staffa al timone a vento, fino alla stampa e al vapore, senza un conflitto sociale, una contrattazione delle parti ha prodotto mai effetti positivi? Credo nessuna. Il problema risiede nel fatto che la rete, il pensiero computazionale, non è stato ancora oggetto di un nuovo contratto sociale che possa civilizzare le tecniche, valorizzare le potenzialità di liberazione e nel contempo limitare le degenerazioni che tutte le opzioni sociali presentano.

L'algoritmo può trasformare il significato in azione

"L'individuo che vuole partecipare alla costruzione di senso – si legge nel saggio – ed entra nel circuito relazione della rete, in quello stesso momento vede intaccata la sua autonomia, insieme a ogni residua consapevolezza cognitiva e comunicativa". Il soggetto, per dirla in sintesi, sta diventando una pedina da profilare al servizio dei grandi padroni della Rete. Si tratta di una deriva ineluttabile?

L'algoritmo, come sostiene il grande matematico americano Alexander Galloway, è un meccanismo che, trasformando il significato in azione, diventa inconsciamente eseguibile: ebbene bisogna che l'azione dialettica dei soggetti sociali trasformi quell'avverbio, inconsciamente, nel suo contrario, *consapevolmente*. Questo è il senso di quanto comincia a verificarsi in rete. Se solo avessimo fatto quest'intervista qualche settimana fa, *Facebook* sarebbe stato visto ancora come un gigante inattaccabile della rete e *Cambridge Analytica*, la società che ha profilato milioni di individui deformando la loro volontà elettorale, sarebbe ancora in attività, cosa che non è più. Dunque qualcosa sta accadendo, anche i giganti sono in fibrillazione.

> *In rete, come nella vita ordinaria, è chi ascolta che decide se una fonte ha più o meno credibilità o attendibilità, non è uno status professionale.*

"La rete – ha detto nel corso del dibattito che si è tenuto alla FIEG – non è un semplice media, è una protesi della vita, proviamo a civilizzarla con un negoziato sociale". Cosa vuol dire in concreto?

Questo è uno dei più inspiegabili e gravi equivoci in cui cadono anche brillanti osservatori della rete, come ad esempio l'economista Branko Milanovic, o anche molti mass mediologi che tendono ad omologare la rete al sistema dell'informazione. La rete è una protesi diretta della vita umana, non un travestimento dei media. Non vale in rete il meccanismo tradizionale dei sistemi dell'informazione, basato sulla credibilità, la professionalità. In rete, come nella vita ordinaria, è chi ascolta che decide se una fonte ha più o meno credibilità o attendibilità, non è uno status professionale.

Per questo motivo in rete anche grandi testate non riescono ad imporre il proprio peso e il proprio prestigio?

Più probabilmente è questa la ragione per cui Facebook prevale su Google come fonte diretta. Come mai, bisogna infatti chiedersi, in rete una fonte vicina, intima e conosciuta, prevale su una fonte, prestigiosa, lontana e professionale? Se non riflettiamo su questa differenza alla fin fine ci sembrerà che con l'avvento del digitale è cambiato poco nel modo in cui circolano le informazioni, solo i mezzi, dalla carta al bit, quando invece è proprio la dinamica sociale che guida la circolazione delle notizie che è radicalmente mutata.

Il dato come asset sociale

Stiamo sperimentando la contendibilità della nostra autonomia da parte di un potenza di calcolo che risiede in poche mani. Esistono strumenti che possono invertire questo pericoloso trend?

Questo è il vero nodo, e non riguarda i social che sono un aspetto appariscente ma marginale di un mondo più

vasto rappresentato dal pensiero computazionale, che oggi chiamiamo direttamente, evidenziando un vincolo inesorabile, intelligenza artificiale. Gli algoritmi, spiega Craig Venter, il celebre genetista, non servono a far giocare i giornalisti con i network ma a riprogrammare la vita umana. È su questo piano che dobbiamo collocare la riflessione sul sistema digitale: qual è oggi il motore che guida le nostre azioni? La potenza di calcolo, la calcolabilità del futuro che grazie ai big data permette di tracciare piste di scorrimento per ogni azione di ogni singolo utente. Questo potere va contrastato, ma non inibito perché ci offre straordinarie opportunità di libertà, come sosteneva appunto Olivetti. Per contrastarlo bisogna cominciare a ragionare sulla negoziazione del numero e sull'affidabilità dei sistemi algoritmici che, spiega molto bene Giulio Giorello, non sono mai inevitabili e univoci, ma presentano sempre soluzioni che possono essere rovesciate e trasformate.

Nella società dell'informazione il dato è un asset sociale. L'algoritmo assume e licenzia (vedi il caso di Amazon), la blockchain automatizza le organizzazioni e può fare a meno di sindacati, partiti, istituzioni. Dobbiamo pensare che gli strumenti della democrazia e le sofferte conquiste di libertà che hanno segnato secoli di storia sono giunti al capolinea?

Già a metà degli anni 90 Paul Viriliò, il filosofo della dromologia, la scienza che studiava la velocità, parlava di democrazia automatica, ossia di un modo di organizzare la convivenza sociale basato su meccanismi e congegni preordinati, come i sondaggi, o i referendum, che non offrivano realmente spazio a un approccio critico e dialettico. Oggi il tema diventa ancora più pressante: può il sistema di calcolo sostituire l'incidente della differenza di giudizio, l'eccezione del dissenso? Pensiamo proprio alla *blockchain*, che oggi sembra diventare la panacea di tutti i mali. Si tratta di un automatismo che appiattisce ogni discussione: la quotazione della moneta la decide la *blockchain*, il sistema sanitario lo gestisce la *blockchain*, la mobilità la pianifica la blockchain. Ma chi controlla la *blockchain*?

Risponda Lei alla domanda.

Nel libro, facendo una battutaccia, dico che la *blockchain* del bitcoin è controllata sicuramente da due persone: una è il titolare dell'algoritmo di base che ne bilancia il funzionamento, il secondo è colui che ha una pistola puntata alla tempia del titolare dell'algoritmo che bilancia il funzionamento. È di certo un paradosso che coglie il rischio che dietro un apparente decentramento si nasconda poi un'ulteriore centralizzazione. È comunque evidente che siamo ad una svolta che reclama un'innovazione di processo della democrazia: non tanto in relazione alle tecnologie diffuse, quanto per le tipologie delle persone che abitano ormai il pianeta, persone che tendono a sottrarsi ad ogni irreggimentazione, a reagire direttamente ad ogni forma di comando dall'alto. Il populismo, che pure oggi è una forma di linguaggio esteso della politica, ne è una prima applicazione, ma siamo ancora all'inizio del percorso.

Guardiamo alla più stretta attualità. Un capitolo del saggio è dedicato al "partito momentaneo e al fenomeno del ribellismo molecolare". Le ultime elezioni politiche cosa hanno da insegnarci sul terreno del delicato binomio: algoritmi e libertà?

In tutto il mondo, in ogni scacchiere geopolitico, le tradizionali macchine di organizzazione del consenso sembrano in affanno, se non proprio fuori giri. Si tratta di ragionare sul fatto che la cassetta degli attrezzi della nostra politica è ancora quella mutuata dal fordismo, quella che Baumann chiamava la società del lavoro di massa, consumo di massa, media di massa e, continuando, potremmo dire, partiti di massa, sindacati di massa, voto di massa, ecc. Quella in cui viviamo è invece una società caratterizzata dal lavoro individuale, dai consumi personalizzati, dai *media on demand*. Dunque cambiano tutte le dinamiche, tutte le relazioni, tutte le tecnicalità della politica. Giocando con la macchina del tempo potremmo dire che se Lenin si riaffacciasse risponderebbe alla domanda del suo celebre saggio sul partito "Che fare?", con la risposta: un bot.

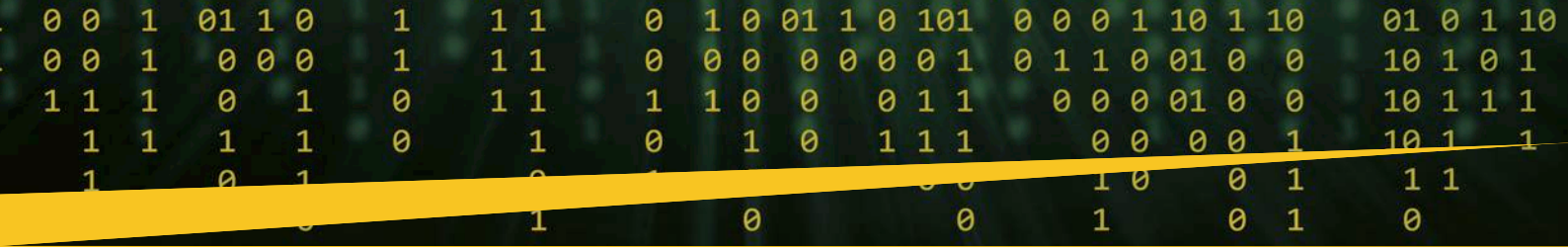
Ammetterà che fare politica non è semplice, per non dire che è un'impresa intercettare flussi elettorali sempre più volatili.

Oggi per fare politica e organizzare il consenso bisogna fronteggiare una poderosa massa di differenze, un pullulare di individui, una moltitudine di personalità che hanno proprio nell'essere diversi il proprio valore comune. Ma come si organizza la diversità? Non certo partendo dalle identità quanto dagli obbiettivi, cercando cioè di aggregare occasionalmente, momentaneamente, energie individuali che in quel momento hanno un obbiettivo comune. Cito come esempio, al netto dei contenuti e del risultato, l'Assemblena nazionale Catalana, una forma partito che in pochi mesi ha aggregato una grande folla di aderenti, unificando figure sociali ed interessi immediati molto diversi, se non antagonisti fra loro in nome di un obbiettivo: l'indipendenza. Così sono nate le primavere arabe, i movimenti *Occupy Wall Street*. Bisogna cercare, però, di evitare l'errore di valutare questi movimenti con il metro del partito classico: la tenuta, la strategia, la convinzione, perché siamo di fronte a stati d'animo, a momentanee sensazioni che si trasformano in azione.

Quando la potenza di calcolo si separa dagli Stati

La potenza del calcolo si separa da quella degli Stati, divenendo prerogativa dei tycoon che hanno ormai superato ogni "indicatore di potenza compatibile". Se la separazione di Stato e calcolo segna la fine dell'Europa westfaliana, quali equilibri geopolitici si faranno strada?

Anche su questo tema in pochi mesi si è verificata una clamorosa inversione di tendenza. Nel mio studio si parla di "algoritmo nazione", ossia di un ritorno prepotente dello Stato come entità, come impresario, della potenza di calcolo. Penso alla Cina, o alla Russia o anche agli Stati Uniti di Trump, dove il vertice statale, di natura autocratica, tende ad identificarsi proprio con il monopolio della potenza computazionale. Ha ragione Putin quando afferma che: chi controllerà l'intelligenza artificiale controllerà il mondo, terreno che lo vede impegnato per primo. Non considero certo positivo questo contraccolpo, bisogna però attrezzarsi a



leggere altre ragioni: lo strapotere dei grandi monopoli dell'algoritmo, che stava riducendo il pianeta ad un salotto di pochi protagonisti, da Bezos, a Zuckerberg, a Jack Ma, a Larry Page, ha inevitabilmente sollecitato la reazione degli apparati statali che non hanno accettato di rimanere sotto schiaffo della Silicon Valley. Per dirla in sintesi: è in atto un ripensamento dell'idea di Stato che tenderà ormai a coincidere per ogni comunità con il proprio algoritmo: ogni regime non può, infatti, non avere un motore tecnologico coerente e funzionale con il proprio modello sociale.

In conclusione vorrei che si soffermasse su una proposta forte che emerge nella trattazione e che si può riassumere nell'affermazione: "mettiamo l'algoritmo sul tavolo", per svelare le finalità e i principi che orientano la ricerca in campi delicati come la genetica, in modo da valutare se è possibile trascrivere in termini pubblici e sociali la potenza del calcolo, che deve diventare spazio pubblico, un "bene comune", per usare un termine caro all'ultimo Rodotà.

Si tratta di un auspicio, di un progetto realizzabile, di un programma politico?

È innanzitutto un conflitto. Bisogna partire dai soggetti negoziali: interrogandosi su chi oggi ha interesse e possibilità a portare al tavolo della trattativa i giganti del calcolo. Proviamo a fare qualche ipotesi: le città, come luoghi che valorizzano le piattaforme e i dispositivi tecnologici, le università, come centri di sapere che testano e producono algoritmi, e le categorie professionali, come i medici e i giornalisti. Credo meno ad un'azione di normativa statale: da un lato per la lentezza e approssimazione di un intervento centrale, dall'altro perché non possiamo regalare ai monopoli della rete la bandiera della libertà che un intervento autoritario statale potrebbe concedergli. Insomma dobbiamo ritrovare intelligenza e fantasia per mettere in campo quello che ha rappresentato un termine fondante per lo sviluppo del software: un linguaggio per l'autonomia e la libertà degli individui.

Altri tempi, forse troppo lontani per cultura, assetti sociali, visione non crede?

Negli anni 60 si creò quel ciclo virtuoso che dal *free speech* arrivò, attraverso le stesse persone, negli stessi luoghi, con gli stessi linguaggi, al *free software*. Poi la battaglia fu vinta dai grandi privatizzatori, da Steve Jobs e Bill Gates, ma credo che quell'imprinting non sia stato mai estirpato. Del resto proprio uno dei padri dell'informatica, Alan Turing, ci ha insegnato che l'innovazione la troviamo sulla stretta linea che separa l'intraprendenza dalla disubbidienza. Intraprendenza, come è facile constatare, ce n'è davvero molta, ora è venuto il momento di dare metodo e strategia alla disubbidienza. ■

Il tempo della complessità. Verso un umanesimo digitale.

(Prosegue da pagina 5)

gestione di enormi problemi nazionali e sovranazionali, c'è bisogno di visione, di cultura, di consapevolezza della nuova condizione umana globale. E mai come oggi, la politica seleziona una classe dirigente *senza visione*, senza cultura, senza consapevolezza. E perciò legata a una miope tattica di autoconservazione di sé, in una condizione di degrado morale e materiale. Senza affrontare questa drammatica crisi culturale, sarà impossibile rigenerare la democrazia e ridare nel contempo peso e credibilità alla politica.

Verso un umanesimo planetario

Il "nuovo umanesimo" vagheggiato da Lei e da Edgar Morin, che ci riporta alla grande utopia di Kant richiamata nell'ultimo capitolo del libro, è una prospettiva realizzabile o rimane un "sogno da filosofi"?

Il nuovo *umanesimo planetario*, se sarà, sarà prodotto dalla coscienza della *comunità di destino* che lega ormai tutti gli individui e tutti i popoli del pianeta, nonché l'umanità intera all'ecosistema globale e alla Terra. L'umanità può sperare di risolvere i suoi problemi vitali solo riconoscendosi come una comunità di destino, comunità una e molteplice, condizione emergente della condizione umana nel pianeta. Vorrei ribadire che l'universalismo che ne deriva *non oppone la diversità all'identità, l'unità alla molteplicità.*

Si tratta di un capovolgimento profondo, che richiama tutti a un livello più alto di responsabilità. Ne saremo capaci?

Non abbiamo altra scelta. L'identità della specie umana contiene la possibilità, per quanto improbabile, dell'emergenza di una nuova umanità. La condizione umana nell'età globale ha in sé la possibilità di una concreta universalizzazione del principio umanistico. Che vuol dire trasformare il dato di fatto dell'interdipendenza planetaria nel processo di costruzione di una civiltà planetaria, promuovendo un'evoluzione verso la convivenza e la pace. È un compito difficile e improbabile, ma allo stesso tempo creativo e ineludibile, che nel tempo della complessità ci è posto dalla sfida di far nascere l'umanità planetaria, una e molteplice. ■

La blockchain è molto di più della sola valuta digitale

Autore: Joe Pindar

Se pensiamo alla Blockchain la associamo inevitabilmente alla valuta digitale Bitcoin e al settore finanziario. Quando i mezzi d'informazione parlano dei Bitcoin, lo fanno per riportare episodi in cui la criptovaluta viene usata dagli hacker per chiedere il pagamento di un *ransomware*. Di riflesso, è naturale che si focalizzi l'attenzione sulla Blockchain, la tecnologia su cui si fonda Bitcoin. La Blockchain abilita la sicurezza delle transazioni Bitcoin senza la supervisione di un intermediario di fiducia o di un organo direttivo come la *Financial Conduct Authority* nel Regno Unito e la *Securities and Exchange Commission* negli Stati Uniti.

Con l'assenza di questi organi direttivi ed intermediari, il Bitcoin è diventato in poco tempo famoso per essere un mezzo di pagamento usato per servizi e beni illegali. Ciononostante, gli usi legittimi del Bitcoin sono via via cresciuti e sia gli organismi finanziari sia le aziende hanno iniziato a riconoscerne le potenzialità. Le banche e molte altre istituzioni finanziarie sono costantemente alla ricerca di sistemi che permettano loro di ridurre i costi delle transazioni e di semplificare i processi. L'automazione della Blockchain e le sue qualità han fatto sì che molte banche, tra le quali Barclays, la considerino una tecnologia interessante. Infatti, secondo uno studio diretto dalla banca Santander, le tecnologie della Blockchain potrebbero ridurre i costi di infrastruttura delle banche di circa 15 - 20 miliardi di dollari all'anno entro il 2020. Tuttavia, sebbene l'implementazione della Blockchain nel settore finanziario possa sembrare di per sé eclatante, è importante capire il funzionamento della tecnologia prima di prendere in considerazione gli altri settori in cui può essere implementata.

Gli usi della Blockchain nel settore pubblico e privato

Non esiste un unico tipo di Blockchain, ma è disponibile per enti pubblici e privati, e le diversità tra i due settori sono cruciali per capirne gli usi potenziali. La principale differenza è data dal fatto che nella Blockchain pubblica chiunque può avere accesso ai dati, mentre la Blockchain privata è chiusa e solo le persone fisiche o le aziende dotate di permesso di accesso possono visualizzare i dati. La variante pubblica della Blockchain viene normalmente associata alla criptovaluta, mentre le Blockchain private, che consentono il controllo all'accesso ai dati, sono quelle utilizzate più spesso dalle aziende.

Una caratteristica che viene normalmente associata alla Blockchain è la sua facile accessibilità e la possibilità di permettere la realizzazione di transazioni anonime. Tuttavia, questo avviene soltanto nelle Blockchain pubbliche. Le persone fisiche possono incontrarsi, realizzare delle transazioni e dopodiché disperdersi nuovamente, senza nemmeno il bisogno di conoscere l'identità di ognuna delle controparti. Per alcune transazioni, l'anonimato e l'accessibilità continueranno ad essere delle qualità attraenti. Ecco alcuni esempi interessanti di applicazione della Blockchain:

- Le aste d'arte di alto valore in cui gli offerenti spesso non vogliono che si sappia contro chi stanno facendo un'offerta per un'opera d'arte, perciò la case d'asta sono le uniche a conoscere l'identità dell'acquirente.
- Segnalazione di criminali alle forze dell'ordine attraverso servizi come *Crimestoppers*.

Indipendentemente da queste caratteristiche interessanti, pare che in futuro la maggior parte delle Blockchain riguarderà il settore privato. Per gran parte dei casi d'uso e applicazioni delle aziende è necessario che si conoscano le identità delle persone coinvolte. Per questo motivo un'autorità centrale dovrà attivare un servizio di autenticazione ed identificazione per verificare gli utenti, in modo tale che la Blockchain consenta l'accesso ed uso ai soli utenti autorizzati e che sia quindi adeguata all'uso aziendale.

Dalla frode assicurativa all'agricoltura passando per una vasta gamma di settori

Fondare una trust distribuita con una Blockchain è una caratteristica utile per molti settori e casi d'uso. In particolare, l'impiego della Blockchain nelle organizzazioni

finanziarie e assicurative permette loro di snellire l'elaborazione delle transazioni finanziarie e le attività di backoffice.

Tuttavia, la tecnologia – una "mutually distributed digital ledger" che impiega la crittografia per rendere le voci non falsificabili e permanenti – ha già attirato l'attenzione di molti altri settori, come l'agricoltura, le imprese assicurative e di logistica. La Blockchain infatti può essere utile in diversi ambiti: dalla gestione della *supply chain* ai processi interni. Il suo punto di forza risiede nel fornire una tecnologia che garantisce l'integrità, la disponibilità, la rendicontazione ("accountability") ed il controllo ("auditability") di ogni dato in essa registrato.

Una delle aree che stanno adottando la Blockchain è quella che mira a combattere la frode assicurativa usando una piattaforma che serve a garantire la provenienza dei prodotti di alta qualità. Chronicled, per esempio, è un'azienda fondata con lo scopo di tracciare la provenienza degli articoli di moda di alto valore. Iniziando dalle scarpe per passare alle apparecchiature medicali, la start-up è focalizzata sulla protezione dei beni di alto valore la cui provenienza farebbe normalmente affidamento su certificati cartacei e ricevute che potrebbero andare facilmente perduti o essere manomessi. È stato quindi creato un "fingerprint" digitale a più livelli su una Blockchain che non

può essere manomessa né cambiata, digitalizzando una grande quantità di dati riguardanti ogni singola scarpa o dispositivo. In questo modo è possibile controllare che gli articoli non siano stati rubati, dato che le agenzie assicurative possono facilmente verificare il Blockchain ledger e poi risalire alle entità coinvolte.

Un altro esempio riguarda l'industria agricola, all'interno della quale alcune aziende stanno cercando di istituire un ecosistema guidato dalla Blockchain che gestisca la registrazione, il pagamento ed il trasporto dei raccolti e dei prodotti agricoli. Tale sistema garantisce che ogni passo del processo della *supply chain* sia registrato sulla Blockchain. Con la registrazione della *supply chain*, gli acquirenti, come per esempio i supermercati, possono verificare che il prodotto che ricevono sia esattamente quello che hanno pagato. Con la possibilità di tracciare il viaggio dal contadino al negozio, l'affermazione ad esempio che i chicchi di caffè provengano da un commercio etico in Colombia può essere facilmente confermata – fugando ogni dubbio riguardante la qualità del prodotto.

La Blockchain è il futuro

Entrambe le Blockchain, quella pubblica e quella privata, offrono una vasta gamma di opportunità alle aziende e ai consumatori. Attraverso l'introduzione di una piattaforma *peer-to-peer* facilmente accessibile, sicura, efficiente e a prova di manomissione, la Blockchain rivoluzionerà radicalmente il modo in cui avvengono le transazioni commerciali, emancipando economicamente i consumatori. È evidente che la Blockchain segni l'inizio di una svolta digitale, contribuendo a ridefinire il modo in cui il valore e le opportunità sono creati e distribuiti.

BIO

Joseph Pindar è il Direttore della Strategia di Prodotto focalizzato sulla sicurezza e protezione dati. Lavora nella divisione del CTO, parte della business Unit *Gemalto Enterprise & Cybersecurity* (ex SafeNet).
Si dedica alla creazione e alla comunicazione della conoscenza situazionale rivolta a product manager e leader ingegneristici. Joe contribuisce altresì ad elaborare le linee guida e a definire le priorità nel processo di sviluppo per adeguarlo alle esigenze di mercato. Lavora inoltre con diverse Business Unit in Gemalto al fine di creare efficaci piani di mercato. Le tendenze e le tecnologie che Joe considera eccellenti in questo momento sono Blockchain, IoT, e sicurezza per il Cloud Foundry. Joe è anche membro fondatore della Trusted IoT Alliance, che lavora per BNY Mellon, Bosch, Cisco, Foxconn e altre sette start-up, usando la tecnologia Blockchain per garantire la sicurezza dell'Internet delle cose.
Prima di iniziare a lavorare presso Gemalto, Joe ha lavorato nel settore dello storage e per il governo del Regno Unito. Ha coperto diverse posizioni, tra le quali assistenza tecnica alla prevendita, consulenza sulla sicurezza e ricerca, architettura di rete e sviluppo ingegneristico. In qualità di membro del "blue team" Joe è stato premiato per la sua ricerca sull'allineamento dell'Information Assurance e la cyber Security con la strategia aziendale. Joe possiede un master in ingegneria dell'Università di Sheffield, una certificazione ISCS2 CISSP e contribuisce regolarmente all' ICS2 dirigendo webinar che vertono su argomenti riguardanti la Blockchain, l'IoT e le regolamentazioni emergenti.
Per ulteriori informazioni:
https://safenet.gemalto.com/blockchain/

Guardando verso il futuro, potremmo persino intravedere come i dispositivi "Internet of Things" di casa nostra, ad esempio i dispositivi di riscaldamento e di intrattenimento, useranno una Blockchain privata per prendere decisioni. È probabile che un numero sempre maggiore di aziende inizi ad utilizzare le Blockchain private per concludere affari con i fornitori e partner. Questi potranno fornire una selezione di dati a una Blockchain pubblica usata per raccogliere dati economici (l'uso della *supply chain*) e dati dei consumatori (sistemi di intrattenimento).

La Blockchain ha tutte le carte in regola per rivoluzionare molti più ambiti oltre al settore finanziario. È importante che, per trarne il maggior vantaggio possibile, le aziende si affidino al più presto a questa tecnologia, per mantenersi così ai vertici della competitività.

In conclusione, la Blockchain non riguarda soltanto il settore finanziario ed è molto di più di una parola che va di moda: rappresenta il futuro della sicurezza distribuita. ■

Blockchain, pro e contro di un paradigma contemporaneo

KASPERSKY lab

Da qualche anno e in ambiti diversi si parla sempre più spesso di Blockchain, indicando non tanto una semplice tecnologia, quanto un paradigma teorico. Per molti non sarebbe altro se non la rappresentazione in chiave digitale di quattro concetti: decentralizzazione, trasparenza, sicurezza e immutabilità.

Autore: Morten Lehn
General Manager Italy di Kaspersky Lab

Inizialmente con il termine ci si riferiva per lo più alla tecnologia per la gestione distribuita delle transazioni economiche associate al mondo delle criptovalute, in particolare di quelle che stanno alla base dei Bitcoin.

In realtà le prospettive aperte da questa nuova frontiera, che nell'opinione di tanti trasformerà in modo radicale il nostro futuro, sono tantissime, anche molto lontane dal mondo del finance e dei pagamenti digitali.

Si va dalle applicazioni in campo assicurativo a quelle finanziarie, da quelle industriali a livello 4.0 a quelle sanitarie, da quella della pubblica amministrazione alle prospettive in ambito retail, da quelle della sicurezza in ambito IT fino a tutta la nuova generazione dell'IoT, includendo anche la dimensione dell'advertising, dell'espressione politica e dell'idealismo democratico.

Incarnazione anche del possibile sviluppo per una nuova forma di democrazia, la Blockchain si contraddistingue per la sua natura strutturale fatta di trasparenza, immutabilità dei dati e immunità dalla corruzione.

Come dice il termine stesso, potremmo pensare alla Blockchain come ad un grande database, un elenco composto da tanti blocchi di record di transazioni o di informazioni, collegati tra loro proprio come in una catena; ogni blocco ha contenuti aperti, ma protetti crittograficamente tramite hashing (una funzione algoritmica che non si può invertire e che mappa una stringa di lunghezza arbitraria in una stringa di lunghezza predefinita) e contiene informazioni del blocco precedente insieme ad informazioni nuove.

L'insieme delle informazioni contenute da ciascun blocco e il loro storico sono confermati, riconosciuti e validati dai diversi partecipanti al sistema stesso, motivo per il quale non possono essere intaccati; possono essere modificati solo con l'approvazione da parte dei nodi della rete e con la conferma da parte dei "miner" (che potremmo definire come coloro che controllano o si occupano del processo): le transazioni possono essere quindi considerate come immodificabili a meno che non ci sia un intervento massiccio di conferma da parte dei nodi della rete.

Il cambiamento rispetto a paradigmi concettuali precedenti è rappresentato dal concetto di Distributed Ledger, ovvero da una logica di collegamenti distribuiti dove viene rappresentato un nuovo concetto di "fiducia" tra soggetti: non esiste più un centro prestabilito o un ente super

BIO

Norvegese di nascita, Morten Lehn a luglio 2014 è stato nominato General Manager Italy di Kaspersky Lab, diventando il punto di riferimento dell'azienda per il mercato italiano.
Prima di ricoprire questa carica è stato Sales Director sempre in Kaspersky Lab, occupandosi delle attività di tutto il sales team dell'azienda, per il segmento B2B Corporate ed Enterprise, B2C Consumer e per le vendite online. Prima di approdare in Kaspersky Lab nel 2013, ha lavorato presso il distributore di informatica Bludis, in qualità di Sales Manager dal 2002 al 2009 e in seguito di Sales Director, rispondendo direttamente al CEO dell'azienda. In precedenza Lehn è stato Business Development Manager in Unified Messaging Systems AS, dove ha gestito la start up della filiale italiana dell'azienda, e Sales Manager in Euroline AS.

partes, ma ogni elemento è indissolubilmente legato ad altri elementi a catena.

Date tutte queste informazioni, si sottintende come, utilizzando una Blockchain, si possa ottenere (in via teorica) un database sicuro, affidabile e non manipolabile. È impossibile imitare una transazione mostrando una conferma di pagamento falsa. È impossibile dire di esser stati puntuali nel pagamento ma che la transazione ha richiesto troppo tempo. Si dice addirittura che si può negoziare con una banca, ma non con la Blockchain. Tutte le azioni sembrano "scolpite nella pietra", senza che ci sia bisogno del coinvolgimento di enti terzi.

Ma è davvero tutto come sembra? Apparentemente sì, e anche i possibili dubbi sollevati dal concetto paradigmatico di Blockchain mostrano già soluzioni e confutazioni puntuali. Se il pericolo esiste, è da ricercare nella sicurezza del mondo informatico e nelle capacità sempre più sottili dei cybercriminali di inserirsi in sistemi teoricamente inattaccabili per sfruttarne tutti i possibili spiragli.

Innanzitutto i database distribuiti non sono qualcosa di nuovo, ma risalgono alla fine degli anni '80.

Dopo che i computer più potenti si sono uniti nelle reti locali e globali, è sorto un immediato bisogno di attivare un preciso blocco di dati che fosse trasferito senza coinvolgere il nodo centrale. La Blockchain è, quindi, solo una delle varietà migliorate e potenziate dei database distribuiti che può essere utilizzata per le transazioni finanziarie in maniera affidabile e confidenziale.

Nel modello ideale della Blockchain, il governo o un'istituzione centrale gioca un ruolo marginale o nullo in ogni transazione o passaggio. Sono le persone e le organizzazioni a doversi accordare tra loro sul fatto che la Blockchain sia un sistema affidabile da utilizzare nelle transazioni. Ma il mondo reale ha altre regole. Affinché le transazioni con Blockchain funzionino nel mondo reale, si ha bisogno di un sistema che gestisca gli incidenti (o i problemi) e questo vuol dire mettere a punto delle norme che gli organi giurisdizionali possano utilizzare per far rispettare le regole. Visto che la Blockchain sta per farsi strada in molte aziende e nei mercati verticali, molto presto si arriverà anche ad una normativa in questa direzione.

Secondo gli esperti ci sono una serie di miti o fatti/chiave ai quali si fa riferimento quando si parla di Blockchain, che possono essere considerati da punti di vista diversi. La loro confutazione in chiave prima negativa, poi risolutiva mostra quale sia l'impegno degli esperti del settore nell'andare oltre i possibili ostacoli per aprire davvero la strada del futuro e la capacità di questo nuovo paradigma: invogliare le persone a cercare nuovi sistemi affinché possa migliorare.

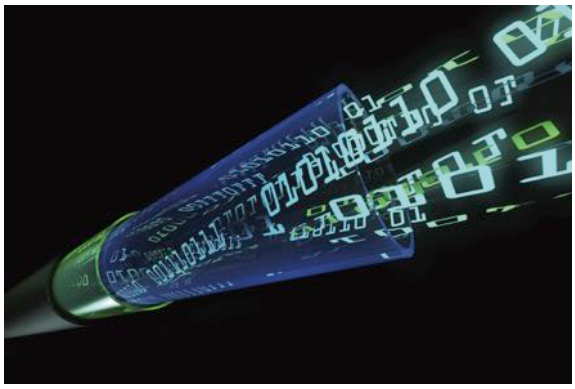
1. La Blockchain è un paradigma efficiente, diretto e naturale per coordinare attività umane e meccaniche

In realtà tutti i nodi che sorreggono la Blockchain fanno esattamente le stesse azioni: verificano transazioni in conformità alle stesse regole ed eseguono identiche operazioni, registrano le stesse informazioni all'interno di una Blockchain, memorizzano l'intera cronologia, che è la stessa per tutti, per tutto il tempo. Quindi non c'è parallelismo, nessuna sinergia e nessuna assistenza reciproca. Ci sono solo duplicazioni istantanee, per milioni di volte. A livello ideale si potrebbe considerare come l'opposto stesso dell'efficienza. Agli esperti da tempo preoccupa l'insufficiente velocità delle transazioni nel

sistema Bitcoin e, per ovviare a tale problema, hanno inventato la *Lightning Network*. I partecipanti a una certa rete che hanno bisogno di un tasso di transazione più veloce creano un canale separato e, come garanzia dell'integrità, effettuano un deposito sulla rete Bitcoin principale. A questo punto possono iniziare a scambiare pagamenti in separata sede e a qualsiasi velocità. Quando non hanno più bisogno di questo canale, i partecipanti registrano i risultati delle interazioni nella Blockchain pubblica e, presupponendo che nessuno abbia violato le regole, viene restituito loro il deposito versato. Infine è vero, la tecnologia alla base può essere farraginosa, ma è garanzia di affidabilità alla rete.

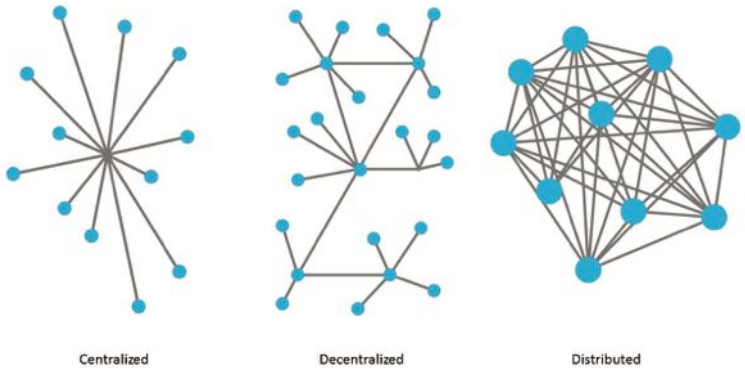
2. La Blockchain è eterna

Ogni client superiore di rete di Bitcoin memorizza l'intera cronologia delle transazioni e questo registro raggiunge una grandezza di 100GB. È la capacità



d'immagazzinamento di un portatile economico o di uno smartphone più avanzato. Più transazioni vengono elaborate sulla rete Bitcoin, più velocemente cresce il suo volume. E il suo maggiore aumento è avvenuto negli ultimi due anni. La crescita della Blockchain di Bitcoin non è nemmeno la più veloce; la rete rivale, Ethereum, ha accumulato 200 GB di cronologia di dati, in soli due anni dal suo lancio e in sei mesi di utilizzo attivo. Quindi, la durata della vita della Blockchain, in circostanze attuali, è limitata ad un decennio. La crescita della capacità degli hard disk è decisamente indietro rispetto a questi numeri. Oltre alla necessità di memorizzare un grande quantitativo di dati, questi devono essere anche scaricati.

Chiunque abbia mai cercato di utilizzare un portafoglio per la criptovaluta memorizzato localmente, ha scoperto con stupore e sgomento di non poter eseguire o ricevere pagamenti finché l'intero processo di download e verifica non sia stato completato. Gli utenti di Bitcoin sono divisi tra entusiasti, che scaricano e memorizzano sul proprio computer, e le persone comuni, che usano i portafogli online e hanno fiducia nei server. Esiste già un altro metodo più avanzato e affidabile: invece di immagazzinare e processare l'intera Blockchain di 100GB, si possono scaricare e verificare solo i block header e le transazioni proof-of-correct collegate direttamente.



3. La Blockchain è in crescita e il denaro convenzionale presto sparirà

La rete Bitcoin è in grado di processare un massimo di sette transazioni al secondo, per milioni di utenti in tutto il mondo. Oltre a questo, le transazioni Bitcoin-Blockchain vengono registrate solo una volta ogni 10 minuti. Per

aumentare la sicurezza dei pagamenti, è una pratica standard quella di attendere 50 minuti in più dopo che viene visualizzato un nuovo registro affinché si possa ricominciare. Per fare un paragone, Visa processa migliaia di operazioni al secondo e, se necessario, può facilmente aumentare la sua larghezza di banda. Dopo tutto, le tecnologie bancarie classiche possono espandersi. Se il denaro convenzionale scomparirà, insomma, non sarà a causa delle soluzioni Blockchain.

4. La Blockchain è decentralizzata, quindi è indistruttibile

I miner "indipendenti" sono fusi in pool, si basano sul presupposto che sia meglio avere un reddito piccolo ma stabile piuttosto che un enorme guadagno. Kaspersky Lab ha individuato 20 grandi pool di mining, con i primi 4 che controllano più del 50% di tutta la potenza di calcolo. Ottenere accesso a questi soli quattro centri di controllo darebbe la possibilità di raddoppiare i propri Bitcoin. Questo, come si può immaginare, svaluterebbe alquanto la criptovaluta. La minaccia ancora più grave potrebbe verificarsi nel caso in cui la maggior parte dei pool, insieme alle loro potenze di calcolo, si trovassero all'interno di un singolo paese, il che renderebbe molto più facile ottenere il controllo sui Bitcoin da parte di una nazione.

Non è facile, comunque, apportare cambiamenti nel protocollo di una rete decentralizzata. Per tenere la situazione sotto controllo le soluzioni sono già state avanzate: una è la possibilità di votare sulle modifiche (ciò che è stato fatto per la cripto-moneta Tezos, ad esempio). Si pensa che questo metodo ridurrà significativamente la necessità di ricorrere alle forchette e a momenti di tensione emotiva tra utenti.

5. Il carattere anonimo e aperto della Blockchain è una buona cosa

La Blockchain è aperta e tutti vedono tutto, perciò non esiste in questo sistema un anonimato reale. Alcune rivelazioni potrebbero essere tollerabili per la gente comune, ma letali per le aziende, ad esempio. Tutte le parti contraenti, le vendite, i clienti, le cifre presenti in un conto e tanti altri piccoli dettagli potrebbero diventare pubblici. I creatori della cripto-moneta Dash (l'antica Darkcoin) sono stati i primi a risolvere il problema dell'anonimato,

mediante la funzione PrivateSend. È piuttosto semplice: hanno progettato un tumbler all'interno della stessa moneta. Un sistema ancora più affidabile è la moneta Monero, davvero anonima. Innanzitutto, utilizza le firme elettroniche che consentono a un partecipante del gruppo di firmare un messaggio facendo le veci del gruppo stesso ed evita anche che qualcuno possa risalire all'utente che ha firmato. In questo modo il mittente nasconde le proprie tracce e, allo stesso tempo, il protocollo evita che si spenda la moneta due volte. In secondo luogo, Monero utilizza non solo una chiave privata per il trasferimento di denaro, ma impiega anche una chiave aggiuntiva per visualizzare cosa c'è nel portafoglio. Infine, alcuni mittenti potrebbero generare portafogli da un solo uso per mantenere separati i fondi privati da quelli che arrivano dai mercati (raccomandazione fatta a Bitcoin già tempo fa).

6. I miner garantiscono la sicurezza della rete

I miner, a livello ideale, si occupano del controllo e della gestione del processo della Blockchain, consumando energia elettrica per assicurarsi che la riscrittura della cronologia delle transazioni richieda la stessa quantità di tempo impiegato per scrivere la cronologia originale (data la stessa potenza di calcolo complessiva). C'è però un rischio, chiamato "51% attack", che riguarda anche le soluzioni Blockchain e che si avrebbe se più della metà della potenza di calcolo attualmente utilizzata per l'attività mining fosse nelle mani di uno specifico gruppo di miners. Allora si potrebbe furtivamente scrivere una cronologia finanziaria alternativa che diventerebbe realtà. I miner "eccessivi" non possono smettere la loro attività di mining; questo aumenterebbe drasticamente la probabilità che una singola persona, o un singolo gruppo, controlli più della metà della potenza di calcolo restante. Il mining è ancora redditizio, e la rete è ancora stabile, ma la situazione potrebbe cambiare.

I miner della rete Proof Of Work consumano molta elettricità e il numero di megawatt utilizzati non dipende da questioni di sicurezza o di senso comune, ma da ragioni puramente economiche: se il tasso di cambio rende il mining un'operazione che genera profitti, il processo continuerà a espandersi.

Per questo motivo è uno dei territori più interessanti di questi tempi per i cybercriminali e forse uno degli aspetti davvero pericolosi da monitorare e da prendere di petto quando si parla di Blockchain.

I miners malevoli possono rivelarsi un problema anche per gli utenti indiretti: possono consumare risorse sottraendole ai device, possono portare ad un aumento dei consumi di energia elettrica, possono danneggiare dispositivi già compromessi, impedire la corretta fruizione dei server erogati dalle macchine e possono veicolare anche altri generi di minacce. Per dare un'idea della portata del fenomeno, basti pensare che con l'operazione *"Mine a Million"*, Kaspersky Lab ha identificato un sofisticato gruppo di hacker, che ha guadagnato milioni attraverso malware di mining, per la precisione circa 7 milioni di dollari nella seconda metà del 2017.

Anche in questo, come negli altri casi esposti in precedenza, è importante sottolineare come gli esperti del settore abbiano già messo a fuoco una delle caratteristiche paradigmatiche della Blockchain, svelandone le criticità e immaginando anche le possibili conseguenze negative. Come nel caso di *Lightning Network* o di *Monero*, quando si è trattato del problema dell'efficienza del paradigma o dell'anonimato/trasparenza delle transazioni/informazioni, anche nel caso di mining malevolo le soluzioni ci sono e sono già a disposizione di tutti: si tratta, per questo caso specifico come per gli altri, di metodi per superare tutti i possibili ostacoli di uno dei sistemi che governerà il futuro. In questo caso le soluzioni sono quelle che rimandano al mondo della cybersecurity e che si rivolgono a utenti di tutti i livelli: dai privati alle PMI, fino alle grandi imprese.

La Blockchain è solo una delle prossime tappe previste nel nostro futuro che avrà un impatto importante, proprio perché arriverà a toccare molti aspetti della nostra esistenza. È quindi fondamentale essere informati sin da ora, non farsi trovare impreparati quando il futuro arriverà e affrontare le nuove sfide che la tecnologia ci mette di fronte, valutandone tutte le criticità e trovando tutte le possibili soluzioni, sempre in modo consapevole e, soprattutto, tecnologicamente sicuro. ■

PSD2 e NUOVE MONETE

Autore: Francesco Corona

PSD2 e nuove monete virtuali

Con la Direttiva Europea PSD2 (Revised Payment Service Directive) vengono a delinearsi modelli di banca aperta (open banking) nell'ambito dei pagamenti elettronici: di fatto vengono abbandonati i tradizionali modelli basati sulla fiducia tra cliente e banca, sostituiti con modelli basati su logiche del consenso del tipo *blockchain*, nelle quali vedremo nuovi soggetti intermediari delle transazioni quali ad esempio Apple, Google, Facebook, Amazon, già dotati di proprie infrastrutture tecnologiche, affacciarsi su questo nuovo scenario. Il cliente potrà decidere in completa autonomia quale piattaforma utilizzare per gestire i propri fondi ed erogare pagamenti.

Stiamo inoltre assistendo ad una fase sempre crescente di dematerializzazione monetaria, la PSD2 faciliterà, nei prossimi anni, questo processo già avviato per altro con la prima Direttiva 2007/64/CE (c.d. PSD, Payment Services Directive), nella quale tutti i prestatori di servizi di circolazione monetaria sono sostanzialmente posti sullo stesso piano, attuando così un meccanismo concorrenziale nel quale il ruolo pubblico diviene in sostanza quello di regolatore dell'offerta di moneta ed in modo auspicabile anche quello di eventuale "fornitore". Viene pertanto a meglio delinearsi il ruolo pubblico in considerazione del fatto che la stessa Authority nominata al controllo dovrà da un lato supervisionare le transazioni economiche di tutti gli intermediari in una tipica catena di valore (Clienti-Intermediari-Banche-Authority), e dall'altra garantire il monitoraggio e controllo delle transazioni sul proprio territorio nazionale onde determinare puntualmente i flussi monetari dei pagamenti digitali per meglio implementare le proprie politiche fiscali.

È del marzo 2017 l'accordo raggiunto tra il Fisco italiano e Google, con il pagamento di 306 milioni di euro da parte del colosso americano, per risolvere il contenzioso fiscale con l'Italia conclusosi dopo una estenuante e lunga trattativa. Altri paesi europei si sono trovati in analoghe situazioni critiche utilizzando stesse procedure di accomodamento transattivo. Ora sapendo che la PSD2 non farà altro che aumentare i volumi monetari di Apple, Google, Facebook, Amazon ed altri ancora è necessario scongiurare gestioni anomale e nuovi contenziosi.

Si impone pertanto una strategia economica che vada a proteggere la sovranità nazione dallo strapotere di questi colossi del digitale. Una via percorribile diversa da quella del reiterato ed estenuante contenzioso fiscale è l'utilizzo di una **moneta digitale statale di tipo scritturale**, con emissione da parte del Ministero del Tesoro di concerto con il Ministro Infrastrutture e Sviluppo Economico (MISE) per misurare da un lato il valore di asset pubblici

BIO

Francesco Corona è docente e direttore del master di Hacking ed Ingegneria della Sicurezza presso Link Campus University Rome, già docente a contratto presso la Facoltà di ingegneria gestionale di Roma2 Tor Vergata Dipartimento di Ingegneria dell'Impresa. Ha svolto intensa attività di ricerca in ambito MIUR ed attività professionale d'impresa nel settore della sicurezza per conto di primari player nazionali ed internazionali. Nel 2013 consegue il prestigioso Premio Nazionale per l'innovazione e il premio ICT Confindustria. f.corona@unilink.it

e privati ed infrastrutture critiche, dall'altro tutte le transazioni digitali chiuse sul territorio nazionale fornendo i parametri di cambio con altre monete a corso legale come l'Euro. L'esempio italiano di una moneta scritturale governativa con fondamento giuridico esiste, è reale, ma di essa si è persa ogni traccia. Tale moneta da ripristinare con estrema urgenza prende il nome di **FRANCO ORO**, regolamentata dal decreto ministeriale del 25 novembre 1982 (Ministero del Tesoro di concerto con il Ministero Poste e Telecomunicazioni – vedi Gazzetta Ufficiale del 28 dicembre 1982).

MONETA SCRITTURALE: Quando si parla di moneta cosiddetta scritturale si indica l'insieme degli strumenti gestiti e organizzati dalle banche e dagli altri intermediari abilitati a prestare servizi di pagamento. La prestazione dei servizi di pagamento, attraverso moneta scritturale – spiega la Banca d'Italia – è un'attività consentita per legge esclusivamente ai soggetti abilitati, quali banche, istituti di moneta elettronica, istituti di pagamento.

Il Franco Oro


Spedizione in abbonamento postale - Gruppo I — Anno 123° — Numero 355

GAZZETTA UFFICIALE

DELLA REPUBBLICA ITALIANA

PARTE PRIMA — Roma - Martedì, 28 dicembre 1982

AVVISO AGLI ABBONATI

Si comunica che i canoni di abbonamento alla Gazzetta Ufficiale 1983 sono stati pubblicati nella Gazzetta Ufficiale n. 347 del 18 dicembre 1982.

I Signori Abbonati sono pregati, nel loro interesse, di versare il nuovo canone utilizzando il modulo di conto corrente precompilato meccanograficamente già inviato.

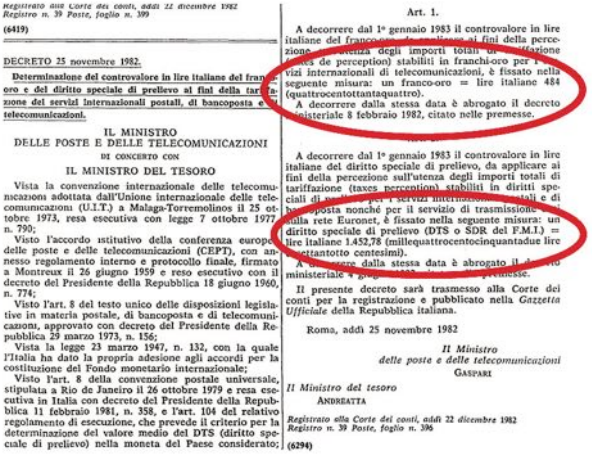
Per ulteriori informazioni e chiarimenti telefonare ai numeri (06) 85082221 - 85082149.

SOMMARIO

La nascita del **FRANCO ORO** (che nulla ha a che vedere con il Franco Germinal) risale alla fine degli anni '70, e risulta essere una moneta scritturale internazionale a valore giuridico riconosciuta dal Fondo Monetario Internazionale e da tutti gli stati membri. Scopo di questa moneta era la misura dei servizi e delle infrastrutture di telecomunicazione (circuiti telefonici) di ogni singolo Stato che aderiva alla convenzione di Malaga del 25 ottobre 1975. Quando gli asset in telecomunicazione facevano parte del patrimonio sovrano di uno Stato, il legislatore governativo si preoccupava bene di misurare puntualmente l'utilizzo dei propri servizi e delle proprie infrastrutture.

Era stata pertanto definita una convenzione internazionale attraverso la quale si potevano misurare e compensare gli utilizzi di asset nazionali strategici come le reti di telecomunicazione da parte di altri operatori non nazionali. Un caso tipico era il cosiddetto **Traffico Telefonico di Transito** che costituiva circa il 15% del business di un operatore di telecomunicazione (anni '80) e consisteva nel cedere a pagamento l'utilizzo di circuiti telefonici nazionali, nelle fasce di fuso orario notturno, ad un operatore estero che poteva utilizzarli in momenti di picco durante le proprie fasce giornaliere diurne perché operante in zone di fuso orario differenti. Ad esempio l'allora operatore internazionale italiano Italcable (gruppo STET poi Telecom Italia) affittava i circuiti telefonici italiani dalle 22:00 di sera alle 4:00 del mattino successivo alle concorrenti americane Mercury e Bell Atlantic che si trovavano ad operare negli Stati Uniti in fasce diurne sovraccariche, lo stesso dicasi per Mercury e Bell Atlantic verso Italcable durante le ore notturne americane e contestualmente diurne europee.

Tali meccanismi scritturali di valutazione economica che utilizzavano una moneta governativa in stile **token** per misurare le specifiche transazioni, e con diritto di prelievo (DTS) garantito dal Fondo Monetario Internazionale,


Registrato alla Corte dei conti, addì 22 dicembre 1982
Registro n. 39 Poste, foglio n. 399

(6419)

DECRETO 25 novembre 1982.

Determinazione del controvalore in lire italiane del franco oro e del diritto speciale di prelievo ai fini della tariffazione dei servizi internazionali postali, di bancoposta e di telecomunicazioni.

IL MINISTRO DELLE POSTE E DELLE TELECOMUNICAZIONI
DI CONCERTO CON
IL MINISTRO DEL TESORO

Vista la convenzione internazionale delle telecomunicazioni adottata dall'Unione internazionale delle telecomunicazioni (U.I.T.) a Malaga-Torremolinos il 25 ottobre 1973, resa esecutiva con legge 7 ottobre 1977 n. 790;

Visto l'accordo istitutivo della conferenza europea delle poste e delle telecomunicazioni (CEPT), con annesso regolamento interno e protocollo finale, firmato a Montreux il 26 giugno 1959 e reso esecutivo con il decreto del Presidente della Repubblica 18 giugno 1960, n. 774;

Visto l'art. 8 del testo unico delle disposizioni legislative in materia postale, di bancoposta e di telecomunicazioni, approvato con decreto del Presidente della Repubblica 29 marzo 1973, n. 156;

Vista la legge 23 marzo 1947, n. 132, con la quale l'Italia ha dato la propria adesione agli accordi per la costituzione del Fondo monetario internazionale;

Visto l'art. 8 della convenzione postale universale, stipulata a Rio de Janeiro il 26 ottobre 1979 e resa esecutiva in Italia con decreto del Presidente della Repubblica 11 febbraio 1981, n. 358, e l'art. 104 del relativo regolamento di esecuzione, che prevede il criterio per la determinazione del valore medio del DTS (diritto speciale di prelievo) nella moneta del Paese considerato;

Art. 1.

A decorrere dal 1° gennaio 1983 il controvalore in lire italiane del franco oro [illegible] ai fini della percezione sull'utenza degli importi totali di tariffazione (taxes de perception) stabiliti in franchi-oro per i servizi internazionali di telecomunicazioni, è fissato nella seguente misura: un franco-oro = lire italiane 484 (quattrocentottantaquattro).

A decorrere dalla stessa data è abrogato il decreto ministeriale 8 febbraio 1982, citato nelle premesse.

A decorrere dal 1° gennaio 1983 il controvalore in lire italiane del diritto speciale di prelievo, da applicare ai fini della percezione sull'utenza degli importi totali di tariffazione (taxes de perception) stabiliti in diritti speciali di [illegible] per i servizi internazionali e di bancoposta nonché per il servizio di trasmissione dalla rete Euronet, è fissato nella seguente misura: un diritto speciale di prelievo (DTS o SDR del F.M.I.) = lire italiane 1.452,78 (millequattrocentocinquantadue lire e settantotto centesimi).

A decorrere dalla stessa data è abrogato il decreto ministeriale 4 [illegible] precedente.

Il presente decreto sarà trasmesso alla Corte dei conti per la registrazione e pubblicato nella *Gazzetta Ufficiale* della Repubblica italiana.

Roma, addì 25 novembre 1982

Il Ministro delle poste e delle telecomunicazioni
GASPARI

Il Ministro del tesoro
ANDREATTA

Registrato alla Corte dei conti, addì 22 dicembre 1982
Registro n. 39 Poste, foglio n. 396

(6294)

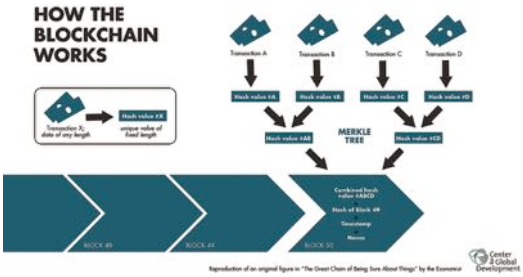
potrebbero ben risolvere la corretta attribuzione di valore al sistema dei pagamenti elettronici nel nuovo modello PSD2-blockchain. Tali modelli soddisfano le attività richieste ai nuovi intermediari garantendo i seguenti obiettivi per tutti gli attori in gioco:

1. Valutazione puntuale dei flussi monetari scritturali nello specifico settore dei pagamenti elettronici.
2. Regolamentazione di compensazioni tra i diversi payers (clienti, Intermediari, banche, fisco). Essendo inoltre la moneta scritturale di emissione pubblica, il suo utilizzo genera valore indotto e quindi politiche fiscali mitigate e con aliquote molto vantaggiose anche prossime allo zero (defiscalizzazione).
3. Assenza di costi di stampa della moneta/conio.
4. Spinta ad investire nella moneta scritturale governativa e quindi creazione di un vero borsino di monete scritturali europeo parallelo alle monete legali o alle criptomonete.
5. Creazione di strumenti di misura di specifici asset pubblici e/o privati oggetto di negozi giuridici.
6. Operazioni di crowdfunding.

PSD2 - Aspetti di sicurezza

Come dicevamo, i soggetti interessati (Clienti-Intermediari-Banche-Authority) faranno parte di una catena di valore economico (transazione) ciascuno con il proprio blocco di informazioni collegate e con le proprie chiavi di accesso. Pertanto una transazione economica a buon fine sarà composta da differenti blocchi di proprietà della Banca o di una Authority governativa che disporrà dei consensi e quindi delle chiavi di accesso di tutti i singoli soggetti. Questi modelli detti *blockchain* hanno già dimostrato una loro intrinseca robustezza con i pagamenti basati su **bitcoin**, ma di recente le loro infrastrutture sono state oggetto di ripetuti attacchi hacker, in particolare citiamo per ultimo l'attacco del

gennaio 2018 alle infrastrutture della criptovaluta giapponese NEM con sottrazione di circa 523 milioni di monete, equivalenti a 58 miliardi di yen ovvero circa 534,8 milioni di dollari. In conseguenza a questa vicenda, **Coincheck exchange** ha limitato i prelievi di tutte le valute e il NEM si è trovata a perdere oltre il 20% sul listino prima di riprendere le proprie quotazioni al rialzo, chiudendo gli scambi con un -10% rispetto alla sessione di apertura.



Esempio di un modello blockchain

In questo scenario complesso basato su modelli fiduciari del tipo *blockchain* i criteri che guideranno la scelta saranno maggior sicurezza ed innovazione. I nuovi *players* entrano in campo grazie a questa direttiva che obbliga *de facto* la facilitazione all'accesso ai conti correnti dei clienti da parte delle applicazioni di terze parti, ovviamente previo il consenso dei correntisti, e quando parliamo di applicazioni stiamo parlando in modo significativo di APP tipicamente *mobile*. Ciò significa che le banche dovranno permettere un accesso sicuro ai conti dei loro clienti implementando delle API *(Application Programming Interface)* con garanzia di sicurezza nel loro utilizzo per ciascun soggetto incluso nella catena del valore di una transazione economica.

Le caratteristiche del framework utilizzato dalle APP tramite API sono evidentemente rilevanti per ciò che concerne il dominio delle informazioni associate a ciascun blocco e quindi alla transaction-chain ed in particolare il valore monetario in moneta corrente, *token* (inteso anche come moneta scritturale governativa) o criptovaluta oggetto delle transazione *(Smart contracts)*, i dati minimali da condividere con tutti gli intermediari *(Shared data)* e i dati specifici della transazione (*big data* possibilmente criptati). I meccanismi di sicurezza prevedranno inoltre *Strong Customer Authentication* (SCA) ed una *blockchain* modificabile solo dal soggetto delegato alla supervisione della transazione (es. Banca e/o Authority); ogni transazione dovrà essere cifrata con la chiave privata degli utenti in gioco oppure con chiavi di sessione da esse derivanti. Il Database (big data) potrà a sua volta essere sottoposto a tecniche avanzate di criptazione onde garantire la sicurezza delle informazioni nella *blockchain*. Per ciò che concerne gli standard di sicurezza, il riferimento alle normative ISO 27001, PCI DSS, CPAS, può fungere da base iniziale sulla quale si adatteranno successivi meccanismi biometrici (ISO/IEC 15408 o FIPS 140-2) in grado di aumentare i livelli di sicurezza ed innovazione.

Nel fiorente mercato delle criptovalute i token sono la rappresentazione di una particolare risorsa o utility intesa come asset, che di solito risiede in una blockchain. I token possono rappresentare praticamente tutti i beni che sono fungibili e commerciabili, dalle materie prime ai punti fedeltà fino ad altre criptovalute. La creazione di token è un processo semplice in quanto non è necessario modificare i codici da un particolare protocollo o creare una blockchain da zero. Tutto quello che bisogna fare è seguire un modello standard sulla blockchain – come ad esempio sulle piattaforme TRON o EOS – che ti permettono di creare token. Questa funzionalità di creazione di token personali è resa possibile dall'utilizzo di smartcontract, codici programmabili che sono autoeseguibili e non necessitano di terze parti per funzionare. I token sono creati e distribuiti al pubblico attraverso una Initial Coin Offering (ICO), che è un mezzo di crowdfunding, attraverso il rilascio di una nuova criptovaluta o token per finanziare lo sviluppo di un progetto. Tale offerta è simile ad un'offerta pubblica iniziale (IPO) di stock.

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$181.454.961.372	$10.742,90	$6.916.480.000	16.890.687 BTC	4,23%	
2	Ethereum	$86.390.144.462	$882,55	$2.069.890.000	97.887.413 ETH	1,40%	
3	Ripple	$37.086.150.350	$0,948621	$309.644.000	39.094.802.192 XRP *	-0,15%	
4	Bitcoin Cash	$21.233.301.096	$1.249,66	$415.205.000	16.991.263 BCH	0,70%	
5	Litecoin	$12.211.312.060	$220,38	$855.190.000	55.410.758 LTC	1,14%	
6	NEO	$9.297.470.000	$143,04	$424.566.000	65.000.000 NEO *	4,75%	
7	Cardano	$8.617.821.195	$0,332387	$96.652.500	25.927.070.538 ADA *	-0,27%	
8	Stellar	$6.635.875.911	$0,359316	$37.051.500	18.468.077.989 XLM *	-0,63%	
9	IOTA	$5.485.291.832	$1,97	$62.013.400	2.779.530.283 MIOTA *	7,13%	

Quotazione principali criptomonete (fonte https://coinmarketcap.com/coins/)

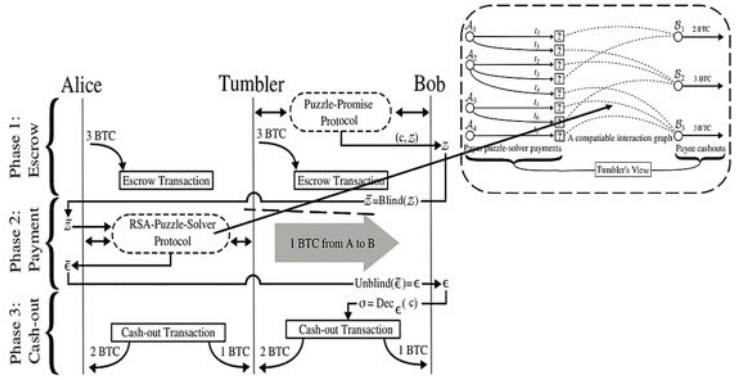
#	Name	Platform	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	EOS	Ethereum	$6.075.582.810	$8,71	$332.768.000	697.384.149	7,13%	
2	TRON	Ethereum	$2.783.988.864	$0,042343	$221.355.000	65.748.192.476	2,12%	
3	VeChain	Ethereum	$2.520.606.539	$5,31	$91.518.700	475.069.837	-1,72%	
4	Tether	Omni	$2.212.983.674	$0,998125	$2.486.720.000	2.217.140.814	-0,29%	
5	OmiseGO	Ethereum	$2.130.842.362	$20,88	$131.458.000	102.042.552	16,74%	
6	ICON	Ethereum	$1.499.633.711	$3,89	$25.532.600	385.966.364	-2,35%	
7	Binance Coin	Ethereum	$1.080.955.641	$10,92	$97.127.800	99.014.000	9,99%	
8	DigixDAO	Ethereum	$966.294.000	$483,15	$60.640.600	2.000.000	17,27%	

Quotazione principali token (fonte https://coinmarketcap.com/coins/)

Sicurezza avanzata: il modello TumbleBit

Il modello TumbleBit merita una attenzione particolare, esso è strutturato su tre fasi specifiche: Escrow, Payment, Cash-out, e consente l'utilizzo di un intermediario **untrusted** fuori dal dominio della *blockchain* che garantisce il buon fine del pagamento elettronico, a questo si aggiungano i necessari meccanismi di sicurezza ed anonimato standard.

Questo modello già compatibile con ***bitcoin blockchain*** risulta scientificamente affrontato in [B007], le sue specifiche di implementazione software sono recuperabili in [B008] mentre gli standard di sicurezza si fondano su meccanismi di chiavi RSA ed ECDSA ben congegnate. L'utilizzo di questo modello è particolarmente indicato per transare in domini PSD2-bockchain l'acquisto di beni molto costosi come ad esempio carburanti, metalli preziosi ed oro dove risulta necessaria l'uscita temporanea da una blockchain prima di perfezionare il pagamento finale con invio di denaro cash.



Schema di riferimento del modello Tumblebit [B007]

Considerazioni finali

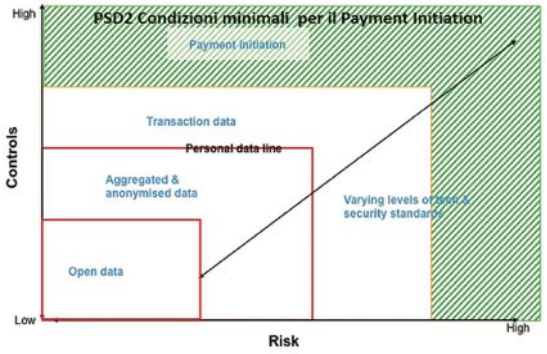
Come dicevamo, la PSD2 introduce una serie di nuovi intermediari che si frappongono tra Cliente e Banca e che possiamo di seguito riepilogare:

- PISP: Payment Initiation Service Provider, è un prestatore di servizi di pagamento che si pone come intermediario tra il cliente ed il suo conto fornendo l'impulso al pagamento. Deve garantire un canale sicuro con la Banca, deve fornire una Strong Customer Authentication con il cliente.
- AISP: Account Information Service Provider, sono servizi di aggregazione di informazioni derivanti da più conti del Customer rendendole disponibili attraverso un'unica interfaccia. Gli AISP potranno collegarsi ai conti e recuperare informazioni, ma possono svolgere solo questo tipo di operazioni.
- CISP: Card Issuer Service Provider, sono operatori che effettuano il controllo fondi principalmente tramite carte di credito.

Mentre i soggetti tradizionali rimangono:

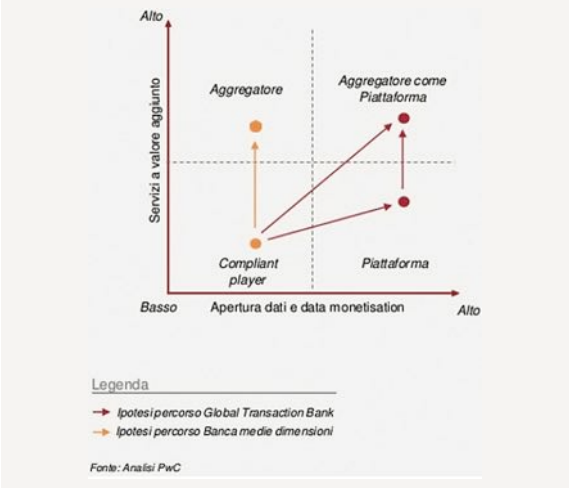
- Customer: il cliente che genera la transazione e che autorizza l'intermediario (PISP).
- Banca: Istituto di credito detentore del conto del cliente.
- Authority: Agenzia relegata a supervisionare la correttezza delle transazioni e dei contratti sottostanti ed alla rispondenza alla normativa nazionale ed europea in termini fiscali e di tutela dei clienti.

Le condizioni minimali di accessibilità alla PSD2 (Compliant player) prevedono da parte di un intermediario la capacità di 1) saper gestire dati in modelli Open Data, 2) saper aggregare dati e renderli anonimi, 3) essere in grado di gestire transazioni sui dati. Tutto ciò premesso determina le condizioni di PSD2 Compliant alle quali si affiancano quelle di Aggregatore, di Piattaforma e di Aggregatore con Piattaforma.



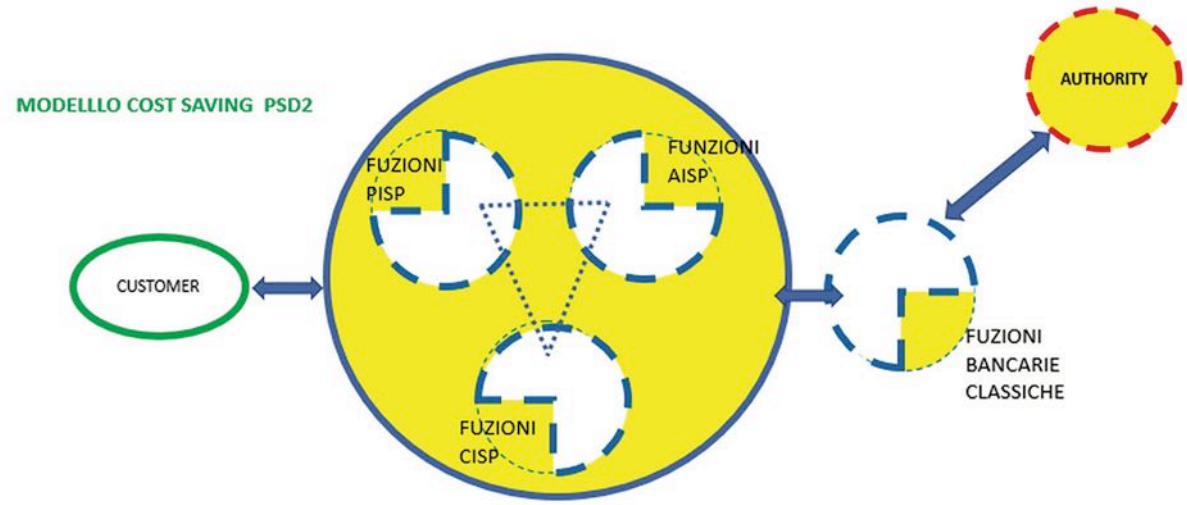
Condizioni minimali di accessibilità alla PSD2

Quindi gli operatori principali potranno semplicemente essere Compliant alla PSD2 oppure giocare un ruolo più incisivo come Aggregatori di Servizi che dispongono o non dispongono di proprie piattaforme VAS.



Aggregazione VAS/Piattaforme (fonte PwC)

Un operatore finanziario con tutti i requisiti di Aggregatore con Piattaforma VAS dovrà prima di tutto individuare e decentrare le proprie funzioni PISP, AISP e CISP per meglio soddisfare un approccio *cost saving* che salvaguardi gli investimenti già effettuati ed in secondo luogo fornire una quantificazione puntuale dei propri asset utilizzati nello specifico business (asset=paniere dei beni) e valorizzati con moneta scritturale a valore giuridico sullo stile del Franco Oro, quindi una moneta designata convenzionalmente nell'Area Strategica d'Affari per quantificare i pagamenti elettronici.



Individuazione delle funzioni PISP, CISP e AISP in un Aggregatore Finanziario dotato di piattaforme VAS

Questo approccio, che vede l'utilizzo di una **moneta virtuale scritturale a corso legale** come il Franco Oro inserita in modelli PSD2 blockchain costituisce *de facto* un sistema virtuoso ed ottimizzato di gestione del business per tutti gli attori in gioco: Clienti-Banche-Intermediari-Authority. Risponde ai requisiti della direttiva europea, incentiva la defiscalizzazione ed apre la strada ad enormi opportunità sia per il settore finanziario, sia per nuovi investitori che potranno operare in contesti sicuri e con le dovute garanzie di riservatezza. ■

BIBLIOGRAFIA

- [B001] https://masterthecrypto.com/differences-between-cryptocurrency-coins-and-tokens/
- [B002] Faramondi L., Leccese F., Peverini F. - Payments Service Directive 2 Implementation Model - 2017
- [B003] G. Lemme e S. Peluso - Criptomoneta e distacco dalla moneta legale: il caso bitcoin -Rivista di Diritto bancario n.11 2016.
- [B004] https://www.pwc.com/it/it/industries/banking-capital-markets/psd2.html
- [B005] Gazzetta Ufficiale del 28 dicembre 1982
- [B006] http://digilander.libero.it/onizuka.host/auriti/documenti/Auriti%20-%20Il%20Valore%20Indotto%20della%20Moneta.pdf
- [B007] E.Heilman , L.IShenibr , F. Baldimtsi, A. Scafuro, S. Goldberg, - TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub https://eprint.iacr.org/2016/575.pdf
- [B008] https://github.com/BUSEC/TumbleBit/tree/master/reference_implementation

web for your business

swiss webacademy

e

GLOBAL
CYBER SECURITY
CENTER

vi aspettano a:

CYBERSECURITY - ROMANIA
CONGRESS
6th Edition

CENTRAL EUROPEAN PLATFORM
SEPTEMBER 12th-14th, 2018
www.cybersecurity-romania.ro

SIBIU: ***Transylvanian atmosphere for making the point at the end of summer***

CYBERSECURITY - SWITZERLAND
CONGRESS
2nd Edition

WESTERN EUROPEAN PLATFORM
NOVEMBER 29th-30th, 2018
www.cybersecurity-switzerland.ch

PORRENTRUY: ***Swiss intimacy to forecast the next year at the end of autumn***

Trovare un equilibrio tra uomo e tecnologia

Aaron Higbee, Cofondatore e CTO di Cofense, parla del futuro della difesa dal *phishing* e chiede su cosa si baserà: uomini o macchine?

Autore: Aaron Higbee

La maggior parte degli attacchi informatici moderni inizia con una mail di *phishing*. Dato che il vettore è digitale, siamo istintivamente inclini a cercare una soluzione digitale. Dopotutto, i computer possono eseguire algoritmi complessi, non si stancano e possono fornire supporto 24 ore su 24, quasi sempre al massimo della loro capacità. Basti pensare allo scorso anno: gli hacker hanno usato gli attacchi di *phishing* per fermare aziende multinazionali, truccare le elezioni più pubblicizzate al mondo e hanno tenuto interi governi offline per lunghi periodi.

BIO

Aaron sovrintende tutti gli aspetti di sviluppi e ricerca che sono la base di Cofense. La soluzione leader di mercato prende l'abbrivio dai servizi di consulenza forniti dal Gruppo Intrepidus, che Aaron ha co-fondato. Prima di allora, è stato Principal Consultant e istruttore capo per la divisione Foundstone di McAfee. Ha anche lavorato nel campo della gestione della sicurezza e degli incidenti, della corretta ottemperanza ai mandati di comparizione, e della sicurezza dei datacenter per grandi Internet Service providers.
www.cofense.com

Inoltre, gli esseri umani sono un target vulnerabile e una facile preda per i sistemi digitali molto avanzati.

Che si tratti di una mail di *phishing* o di una truffa telefonica riguardante le tasse, gli hacker hanno perfezionato l'arte del *social engineering*. Sanno come scavalcare la nostra solita diffidenza e ci mettono nelle condizioni di agire in maniera impulsiva. Lo fanno applicando delle tecniche di psicologia umana, spesso sfruttando emozioni come la paura, la curiosità, la commozione o la sensazione di urgenza. O, in alcuni casi, la distrazione. Ad esempio, questi attacchi via email di lavoro avvengono nelle prime ore della giornata lavorativa, mentre i dipendenti bevono un caffè guardando la posta ricevuta la sera prima. Gli hacker creano inoltre *campagne stagionali* nel periodo di chiusura dell'anno fiscale e durante le festività, come Natale. Provocano risposte basate sullo stress mentre attingono alla nostra avidità con promozioni irresistibili o sconti allettanti. A tutto questo aggiungono le informazioni che si trovano facilmente sul *dark web* (o da un dipendente scontento). Non è difficile utilizzare i dipendenti per ottenere accesso alla rete, se sai come fare.

La potenza dell'informatica cresce di giorno in giorno. E noi? Siamo competitivi? Forse no, visto che siamo noi gli indiscussi punti deboli della sicurezza informatica. La soluzione più facile sarebbe rimuovere l'elemento umano dai processi informatici ma questo non giocherebbe certo a nostro favore…

Ci serve un'altra soluzione

Gli esseri umani hanno molti vantaggi sui loro "colleghi" meccanici e digitali. Anche il più entusiasta tra i *robophile* ammetterà che ci sono cose che gli esseri umani possono fare a livelli più alti di un computer, e alcuni aspetti chiave della protezione dal *phishing* ne sono un buon esempio.

Strano ma vero, i saluti sono un buon modo per capire se l'email che avete ricevuto è opera di un hacker. Per esempio, uno dei vostri contatti vi scrive "Caro Michele" invece che il solito e più breve "Michele" al quale siete abituati. Un computer non vede queste sfumature, ma una persona sì.

Sebbene venga generalmente considerata un'emozione negativa, il sospetto è radicato in noi con lo scopo preciso di proteggerci dalla nostra ingenuità. Per impiegare al meglio le capacità dei propri dipendenti le aziende dovrebbero considerare l'intuizione come una risorsa che può avere effetti positivi quando usata nel contesto giusto. Una risorsa che i computer non hanno.

Un altro vantaggio, per esempio, è la nostra capacità di dubitare. Un computer svolge senza discutere i compiti impostati da un amministratore di sistema, non va oltre, accetta ogni comando e lo esegue. Non si adatta, non aggiunge nulla, non "pensa". Se una mail arriva da una fonte attendibile, cosa importa al computer se l'account è "MichaelBreok@gmail.com" invece che il solito "MichaelBroek@gmail.com"?

Un'altra caratteristica importante dell'essere umano è l'imprevedibilità, o creatività. Molti hacker si guadagnano da vivere violando un sistema sicuro e approfittando delle loro vittime informatiche. Quindi, mentre da un lato la crescita del modello di business del *malware-as-a-service* significa che più persone inesperte sono coinvolte in questa corsa agli armamenti della sicurezza informatica, dall'altro coloro che creano il malware diventano invece degli specialisti delle vulnerabilità che vogliono sfruttare. In altre parole, sanno come una macchina reagisce a determinati input. Non si può dire lo stesso degli esseri umani.

Gli esseri umani potrebbero cadere vittime del tentativo di *phishing*, o ignorarlo. Potrebbero segnalarlo alla polizia, o al loro provider di sicurezza. Potrebbero addirittura inoltrare la mail ad un destinatario indesiderato, o registrare un dominio associato con il *malware* e fermare la campagna. Tutte queste possibili reazioni fanno sì che i criminali informatici impegnati in campagne di *phishing* debbano spesso limitare il loro "target audience", e dedicare del tempo a creare sistemi al fine di non far pervenire il *phishing* a determinati gruppi. Sebbene questo possa sembrare un vantaggio relativamente insignificante, qualsiasi barriera alla distribuzione del *phishing* è una vittoria.

Infine, i sostenitori dell'utilizzo dei dipendenti nella sicurezza informatica puntano al "paradosso dell'accuratezza", il quale afferma che è possibile avere un'accuratezza del 99,99% nelle difese, ma il restante 0,01% si tradurrà spesso in migliaia di allarmi di

sicurezza. Poiché gli amministratori IT non hanno il tempo di indagare su tutti questi *alert*, il paradosso della precisione richiede l'interazione umana per incrementare la sicurezza. Le aziende possono vedere i benefici derivanti dal coinvolgimento dei propri dipendenti nella sicurezza informatica nel momento in cui questi stessi dipendenti non agiscono come uno svantaggio. Ciò di cui le aziende hanno realmente bisogno sono dipendenti capaci di rispondere agli attacchi informatici e in modo appropriato anche in situazioni stressanti.

Analizziamo ora la situazione da un altro angolo: i punti deboli delle macchine rispecchiano le stesse debolezze degli umani che li progettano. Gli esseri umani progettano e monitorano le macchine. Tutta la sicurezza si basa su azioni progettate da umani. Fortunatamente, sappiamo come agire: pratica, pratica, pratica. È per questo che le esercitazioni e le simulazioni sono fondamentali per qualsiasi programma di addestramento militare – l'unico modo per sovrapporre le migliori pratiche sugli istinti espressi in situazioni di carico emotivo è quello di rendere le *best practices* istintive, o parte della memoria muscolare. I sondaggi dimostrano che il condizionamento comportamentale può ridurre la probabilità che i dipendenti rispondano a una email dannosa del 97% dopo solo quattro simulazioni – esercizi di apprendimento in cui le aziende "attaccano" i propri dipendenti. La logica alla base della sua efficacia è che questa tecnica non si limita a rendere gli utenti consapevoli dell'esistenza di una minaccia ma li costringe a esercitarsi a rispondere costantemente.

Quindi, se gli umani possono essere condizionati, avremo mai un ambiente di sicurezza privo di intelligenza artificiale?

Aspettarsi che la prossima generazione di professionisti della sicurezza informatica torni ai processi di sicurezza manuali è impossibile. I programmi *anti-malware*, i firewall e i filtri anti-spam sono essenziali per tenere lontano gran parte dei malware. Sacrificare queste risorse sarebbe semplicemente inefficiente.

Possiamo paragonare la sicurezza informatica alla costruzione di un forte: qualsiasi fortificazione attiva dovrebbe avere grandi mura all'esterno e una serie di rigide misure di sicurezza che regolano chi dovrebbe e non dovrebbe essere permesso all'interno. Ma per avere un forte veramente sicuro, sarà necessario assumere qualcuno per assicurarsi che nessuno stia scavalcando il muro, o fingendo di essere qualcun altro mentre entra dal cancello.

È anche importante assicurarsi che le guardie ricevano una formazione - perché spendere miliardi sui muri se le guardie consegnano le chiavi del cancello ad estranei? Eppure questo è essenzialmente ciò che accade quando i dipendenti fanno clic sui link di *phishing* e consegnano agli hacker ciò di cui questi hanno bisogno per accedere alla rete.

Uomini + Computer = Difesa profonda

I dipendenti possono essere sia le pedine più forti che le più deboli nella sicurezza informatica della vostra azienda. Hanno bisogno di tutto l'aiuto che possono ottenere dalla tecnologia avanzata - dopotutto, gli hacker possono e spesso impiegano processi automatizzati per inviare migliaia di email di *phishing* ogni ora.

Il trucco per combattere questo flagello automatico è operare a un livello gestibile di sicurezza tecnica e aiutare le persone a cogliere potenziali minacce che la tecnologia potrebbe non bloccare. Un recente studio del MIT condotto dal CSAIL (Computer Science and Artificial Intelligence Laboratory) ha rivelato che il futuro della sicurezza informatica potrebbe essere in parte umano e in parte robotizzato, proprio per questo motivo.

Se non sai se affidarti all'uomo o alle macchine, la soluzione migliore è affidarsi a entrambi. Perché scegliere, se puoi avere tutto?

In fondo, dietro le macchine ci sono comunque uomini. ■

Una perla di cultura con una goccia di awareness

Autore: Laurent Chrzanovski

Oggigiorno, potremmo tutti comunicare in *piede equino*. Sarebbe il caso se un consorzio di industrie indiane e sovietiche avesse voluto usare a scopi commerciali il *frequency-hopping spread spectrum*, un sistema brevettato nel lontano 1941 col nome di *Secret Communication System* e destinato alla trasmissione con le torpedini della marina militare.

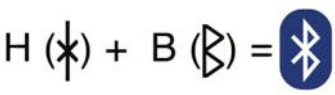
La statua gigante di Tamerlano sulla piazza principale della sua città natale di Shakriziabz (Uzbekistan)

Harald Gormsson battezzato dal monaco Poppus. Placca d'oro della chiesa di Tamdrup, ca. 1100 d.C.

Logicamente, alla ricerca di un nome facile da tenere a mente ma legato ad un grande personaggio storico soddisfacente per tutte le parti, questo ipotetico consorzio avrebbe optato per Tamerlano, il conquistatore che ci ha trasmesso numerosi patrimoni dell'Umanità, quali Samarcanda, Bukhara, Khiva, ma anche, tramite i suoi figli che conquistarono l'India settentrionale, il celeberrimo Taj Mahal. Il suo nome, Timur-i-lang, significa Timur lo schioppo o anche Timur dal piede equino, una conseguenza a vita di una pesante caduta dal suo cavallo in gioventù.

Il fato, però, aveva un piano diverso. Nel 1998, nel loro tentativo di connettere rapidamente senza cavo i diversi device informatici, fu un consorzio scandinavo fondato da Ericsson e Nokia a creare uno *Special Interest Group* (SIG) a questo scopo, in collaborazione coi giganti americani IBM ed Intel ed il giapponese Toshiba.

Durante la seduta tecnica nella quale vennero finalizzati i dettagli operativi nonché la messa sul mercato della tecnologia, si svolse un lungo dibattito sul nome da dare a questa nuova forma di connettività. Fu allora che un ingegnere della Intel, Jim Kardach, appassionato di storia, suggerì di usare il *dente blu (Blåtand)*. Questo soprannome, postumo[1], è quello di Harald Gormsson, il primo sovrano vichingo convertito al cristianesimo che riuscì, anche tramite questa nuova religione[2], a unire tutte le tribù della Danimarca, esattamente come la nuova tecnologia avrebbe permesso di unire tutti i device già muniti di una connessione wi-fi. Si trattava solo di una proposta all'interno del SIG, nell'attesa che le équipe marketing trovassero qualcosa di più seducente. Al contrario, queste ultime rimasero colpite da Harald e riuscirono a creare rapidamente un logo. Per fare ciò, hanno combinato, all'interno di un'ovale blu come il colore del dente, le lettere runiche H (di Harald) e B (di Blåtand).



Con più di 2.5 miliardi di strumenti TIC dotati di questa funzionalità, Bluetooth è destinato ad un brillante avvenire[3]. Ma è sicuro farne uso?

Come per tutti gli strumenti molto popolari, la risposta è sì, ma con la più grande cautela. Bluetooth è stato pensato per un uso libero, rapido ed affidabile, e non possiede una robustezza particolare. Numerosi metodi per piratare un device via Bluetooth ci sono noti, così come le contromisure da adottare[4].

A settembre del 2017, il Cert US[5] nonché numerose testate specializzate dettero l'allarme sull'esistenza di una nuova breccia, usata da un intruso soprannominato *"Dubbed Blueborne"* [6], che si sostituisce alla connessione legittima e permette così di infiltrare PC, smartphone e tablet tramite la funzionalità Bluetooth, indifferentemente dal sistema operativo (PC, iOS, Android, Linux-Kernel).

Apple e Microsoft hanno rapidamente garantito le patch necessarie, facendo sì che gli utilizzatori dei sistemi iOS10 e Microsoft, doverosamente aggiornati, siano ormai protetti, ma non gli smartphone ed altri device che usano Android.

Per noi tutti, la prima precauzione di base da prendere è di spegnere sistematicamente le connessioni Bluetooth quando non sono utilizzate, come fece notare giustamente il sottotitolo dell'articolo di Verge che svelò al pubblico il nuovo attacco: *"A good reason to turn off Bluetooth when you're not using it".*

Come altri exploit prima di lui, *Dubbed Blueborne* non poteva effettivamente derubare le sue vittime se non si trovavano nel perimetro di ricezione/trasmissione dello strumento del pirata e se la funzione Bluetooth del loro dispositivo non era attivata.

Se lavorate però nel quadro della sicurezza d'impresa, vi sono diverse misure supplementari da implementare nonché perimetri di sicurezza da stabilire.

A questo scopo, il National Institute of Standards and Technologies (NIST) ha pubblicato nel 2016 un manuale completo, la *"Guide to Bluetooth Security"*, oggi alla sua seconda edizione consultativa. Quest'opera, dedicata ai CISO, CSO e CIO ma anche ai Risk Manager, è un «must» da scaricare e da leggere per poter poi prendere le buone decisioni in funzione di ogni zona dell›ecosistema da difendere[7]. In complemento – o in alternativa – il supporto del corso *"Bluetooth Security"* del Prof. Antan Giousouf del Dipartimento di Sicurezza delle Comunicazioni dell'Università della Ruhr[8], col suo stile limpido e le sue numerose illustrazioni, permette di farsi rapidamente una visione olistica sulla problematica e di prendere le misure idonee, godendo di una lettura meno tecnica rispetto a quella della guida del NIST. ■

1 Questo soprannome appare per la prima volta in fonti datate una trentina d'anni dopo la morte del sovrano. Nessuna attestazione contemporanea è stata rinvenuta, tantomeno sulle iscrizioni ordinate dallo stesso Harald, come ad esempio la stele sacra con epigrafe runica che fece erigere nel santuario di Jelling: cfr. A. Pedersen, *Monumenterne i JellingFornyettraditionpåtærsklentil en nytid* (The JellingMonuments – Expressions of tradition on the threshold of a new era), in M. ManøeBjerregaard, M. Runge (eds.) At være i centrumMagtogminde – højstatusbegravelser i udvalgte centre 950-1450 Rapport fra tværfagligt seminar afholdt i Odense, 10. februar 2016, vol. 1, Odense 2017, pp. 5-22. SuHarald, si veda l'eccellente libretto del Prof. Sven Rosborn di Malmö (*A unique object from Harald Bluetooth's time?*, Malmö 2016),nonché l'opera collettivadi J. Langer, M. LutfeAyoub (eds.), *Unraveling the Vikings: Studies of Medieval Norse Culture* (Desvendandoosvikings: studos de cultura nórdicamedieval), Pessoa 2016

2 Cf. H. Janson, Vikingarochkristendom. *Någrahuvudlinjer i ochkringdenkyrkopolitiskautvecklingen i Nordenca*. 800-1100, in Historieforum: Tidskriftförhistoriskdebatt, nr 2 (2009), pp. 58-88

3 Informazioni tratte da "A short history of Bluetooth", articolo pubblicato dalla Nordic Semiconductor all'indirizzo: https://www.nordicsemi.com/eng/News/ULP-Wireless-Update/A-short-history-of-Bluetooth

4. cf. K. Haataja, K. Hyppönen, S. Pasanen, P. Toivanen, *Bluetooth Security Attacks. Comparative Analysis Attacks and Countermeasures*, Cham 2013 (Springer ed.), 88 pp.

5 Scheda tecnica su Dubbed Blueborne e le sue funzionalità : https://www.kb.cert.org/vuls/id/240311

6 https://www.theverge.com/2017/9/12/16294904/bluetooth-hack-exploit-android-linux-blueborne

7 https://csrc.nist.gov/publications/drafts/800-121/sp800_121_r2_draft.pdf

8 https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/seminar_giousof_bluetooth.pdf

CISO vs CIO: necessitiamo di nuovi modelli organizzativi?

Autore: Massimo Cappelli

L'incipit è sempre lo stesso. La società sta navigando nelle acque profonde del digitale: servizi online, cloud, app per mobile, wearable device, dematerializzazione, domotica connessa. Le aziende, siano esse clienti o fornitori di tecnologia/servizi, stanno veleggiando lungo le diverse correnti del cyber space, che possono implicare diverse opzioni strategiche come, ad esempio, costruire data center e mantenere il pieno controllo delle proprie informazioni, esternalizzare il servizio e affidarlo a qualcun altro attraverso il cloud o scegliere soluzioni ibride. Le decisioni strategiche non si esauriscono in una scelta di outsourcing o inbound.

L'azienda non è più dislocata in luoghi stabili ma è fluida e dinamica. Alcuni fenomeni propedeutici al cambiamento e alla diversificazione delle strategie sono pure lo smart working, il telelavoro o il *"BYOD"*. Con questi elementi otteniamo una geografia esplosa di "siti" lavorativi e di informazioni sparse in aree geografiche eterogenee in termini di connessioni, leggi, restrizioni, minacce. La digitalizzazione sta cambiando le posture difensive dell'azienda abbastanza marcatamente, abbattendo perimetri e confini. Qualunque sia la scelta strategica, questa influenzerà pesantemente anche le strategie di Information Security.

Il perimetro di attività di Information Security sta diventando di gran lunga superiore a quello della sicurezza classica. È sufficiente pensare al fatto che anche la sicurezza classica (Security & Safety) si può avvalere di sensoristica collegata alla rete: telecamere, casseforti, serrature, controllo accessi, nuovi device e wearable. Questi ultimi potranno supportare i lavoratori in ambienti a rischio, fornendo informazioni su come riparare passo dopo passo un impianto o allertando il dipendente su uno stato psico-fisico di stress o stanchezza che potrebbe metterne a rischio l'incolumità. Gli strumenti di Security & Safety saranno oggetto di monitoraggio da remoto quanto i servizi digitali e le infrastrutture a essi correlati.

Migliaia e migliaia di IP da monitorare costituiranno una superficie di attacco molto allettante per i malintenzionati. Il numero di minacce ibride da considerare aumenterà, così come le vulnerabilità da gestire, in un perimetro che travalicherà i confini della rete aziendale per andare a fondersi con quelli casalinghi, di spazi pubblici o aree di lavoro condivise.

La superficie di attacco si allargherà esponenzialmente con l'aumentare dei servizi e della loro interdipendenza e interoperabilità, visto che un servizio digitale poggia su catene tecnologiche che possono implicare "n" vulnerabilità ciascuna. Inoltre, soprattutto gli IOT, se si continua a privilegiare l'economicità rispetto la sicurezza, saranno permeabili ad attacchi anche non sofisticati.

L'Information Security avrà come sfida maggiore quella di essere *"real time"*. L'aumento della superficie di attacco, l'interdipendenza dei servizi, l'interoperabilità dei sistemi, l'utilizzo del machine learning o dell'intelligenza artificiale per sessioni di attacco, comporteranno una riduzione dei tempi operativi di intervento. Attualmente un APT ci mette meno di due ore per compiere il primo movimento trasversale e una fake news pochi secondi per essere diffusa in rete e condivisa. Il tempo di intervento si ridurrà sempre più in futuro e richiederà una prontezza e rapidità maggiore da parte delle strutture competenti, visti i meccanismi sanzionatori nazionali e internazionali che iniziano a essere predominanti e stringenti in termini di tempo di notifica.

BIO

Massimo Cappelli è operations planning manager presso la Fondazione GCSEC, oltre che responsabile delle attività di Early Warning, Brand Protection, Information Sharing e Cyber Threat Intelligence nella struttura CERT di Poste Italiane. Nella sua passata esperienza ha lavorato come consulente in Booz Allen Hamilton e Booz &Company nella practice Risk, Relisience and Assurance.

Un'azienda deve avere chiara e immediata la sua esposizione informativa e le contromisure poste in essere per la sua protezione, anche per rispondere alle Autorità adeguatamente e nei tempi richiesti.

Questo porta a interrogarci se il posizionamento organizzativo del CISO ha la giusta rilevanza strategica, operativa e tattica per contrastare i fenomeni emergenti e per mantenere una visione complessiva della situazione. L'attuale posizione lo vede per il 66% delle volte, secondo uno studio PwC, a riporto del:

- Chief Information Officer (CIO)
- Chief Operations Officer (COO)
- Chief Security Officer (CSO)
- Chief Risk Officer (CRO)

Poi ci possono essere ulteriori tipologie di riporti, oppure non esistere proprio come figura. Solo 8% circa riporta direttamente al CEO (o alla cosiddetta *C-suite*).

Alcuni studi, di cui purtroppo non ho avuto occasione di prendere visione in dettaglio, riferiscono che il CISO a riporto del CIO, ad esempio, comporta in caso di incidente di sicurezza una perdita finanziaria maggiore del 45% e un downtime del 14% più elevati, rispetto ad altri riporti. A mio avviso, le criticità legate al posizionamento del CISO a riporto di altre figure sono: l'insufficiente "indipendenza" economica; la mancanza di *"segregation of duty"*; la mancanza di autorevolezza gerarchica, la debole rapidità trasversale di azione a cui si aggiunge spesso la frammentazione a silos delle attività di Information Security.

Andiamo punto per punto:

- **Insufficiente indipendenza economica:** soprattutto se a riporto del CIO, spesso accade che sugli investimenti e sui costi chi solitamente ne risente in caso di tagli è il CISO. Si aggiunga il fatto che giustificare un investimento o un costo in assenza di beneficio, considerabile come quantificazione monetaria di un evitato impatto, non è di facile rappresentazione. Ancora oggi ci si interroga sul valore finanziario stesso del dato, sia esso personale, confidenziale o altro.
- **Mancanza di segregation of duty:** chi fa e chi controlla non possono riportare allo stesso responsabile. Si rischia l'effetto "sporco sotto il tappeto";
- **Mancanza di autorevolezza gerarchica:** il CISO non ha l'autorevolezza necessaria per indirizzare le strategie aziendali e si ritrova spesso a dover accettare il cambiamento senza compromessi, anche con perdite economiche derivanti da investimenti in corso non più in linea con gli indirizzi strategici;
- **Debole rapidità trasversale di azione:** pubblicare comunicazioni operative di alerting nella intranet o sui canali ufficiali aziendali o direttamente ai clienti; procedere a denunce all'autorità giudiziaria; postare smentite a fake news richiedono rapidità di azione senza dover attendere processi autorizzativi di 2 o 3 linee gerarchiche che possono impiegare giorni o settimane ad arrivare.
- **Frammentazione di attività a silos:** attività spezzettate fra diverse funzioni come monitoraggio rete, patch management, policy management, brand protection produce una serie di aree grigie sia di responsabilità sia di attività da svolgere con la conseguente perdita della visione di insieme integrata e aumento dei costi.

> *I tempi sono maturi per definire nuovi modelli organizzativi. La transizione a un modello organizzativo nuovo necessita di programmi di change management chiari e sequenziali ma di facile realizzo.*

L'evoluzione della società, delle abitudini e del modo di fare business deve portare con sé anche una nuova visione organizzativa. Nulla vieta che si possa ottenere lo stesso risultato con deleghe, potenziamento del coordinamento e forte collaborazione ma dubito che l'efficacia e l'efficienza che si otterrebbe sia paragonabile a quella in cui le attività di Information Security (comprensive anche a quelle dell'IT Security), convergano nella stessa funzione il cui responsabile sia a diretto riporto del CEO o perlomeno allo stesso livello del CIO.

L'era digitale richiede rapidità, i meccanismi sanzionatori prontezza di risposta. La visione di insieme è necessaria per garantire la sicurezza a tutto tondo. Essendo le contromisure un connubio di più attività che vanno dal front end della sensibilizzazione, passando per le policy fino ai monitoraggi dei servizi, è necessario riuscire ad avere il pieno controllo su tutti gli elementi caratterizzanti l'Information Security e dare una maggiore rilevanza al tutto.

In USA, recentemente si è iniziato a parlare di questo tema. Ci si pone l'interrogativo se non sia necessario elevare il ruolo del CISO e posizionarlo all'interno della C-suite. Stanno nascendo programmi in linea con il National Cyber Security Framework del NIST in cui si ha una visione completa *top down/bottom up* di tutte le categorie espresse dal NIST con livelli di controllo e di rappresentazione dello status di protezione a raggruppamento crescente e con un riporto gerarchico diretto al CEO. Per ognuna delle 5 "Function" e ognuna delle 22 categorie sono rappresentati tutti i sistemi afferenti o lo status delle attività svolte (Es. (Status per Detect <->Anomalies & Events <-> SIEM <-> Log piattaforma 1, Log piattaforma 2,…). Questo permette una serie di vantaggi non indifferenti, come ad esempio:

- Maggiore commitment in termini di Information Security da parte di altri dipartimenti aziendali;
- Economie di scala nelle scelte degli investimenti di lungo periodo, avendo chiara la strategia aziendale e dove andrà il business in futuro;
- Monitoraggio dei costi di esercizio e razionalizzazione della spesa, associandola ad analisi costi/benefici in base ad impatti evitati grazie all'insieme delle contromisure messe in piedi;
- Presidio completo dei piani di rientro in tutte le "Function" e relative sotto categorie, con possibilità di dettare i tempi e pianificare meglio le attività.

Anche la direttiva israeliana *"Proper Conduct of Banking Business Directive 361 (03/15) Cyber Defense Management"*, afferma che il Chief Cyber Defence Officer (nostro CISO) deve riportare direttamente a una figura senior executive; gli deve essere data l'autorità di influenzare qualsiasi decisione che possa impattare sull'esposizione al rischio cyber della banca; e deve essere in una posizione tale che non venga influenzato da potenziali conflitti di interesse.

A livello organizzativo, il CISO, nelle società virtuose, si posizionerà sempre più in alto. L'ostacolo maggiore a questa visione deriverà dagli attriti interni che gli altri dipartimenti potrebbero suscitare (es. CIO) ma anche dal debole *commitment* al cambiamento del top management. Quest'ultimo ostacolo non è facilmente sormontabile. Le società di consulenza possono supportare in questo passaggio da un'era informatica a un'era digitale, sensibilizzando il top management, ma spesso non riescono ad arrivare in cima alla piramide. I senior partner del settore Information Security delle società di consulenza si posizionano a un livello di discussione che al massimo raggiunge il CIO e il CSO. Questo cambiamento per essere attuato necessità di un convincimento a più alto livello ed è per questo che necessità di una spinta a livello di Direttori Generali o CEO stessi.

I tempi sono comunque maturi per definire nuovi modelli organizzativi. La transizione a un modello organizzativo nuovo necessita di programmi di *change management* chiari e sequenziali ma di facile realizzo in termini di tempo. La fase più critica è la valutazione dell'AS-IS che deve essere compiuto sulla base di un framework omnicomprensivo di Information Security (es. Framework NIST). L'analisi delle criticità e dei controlli con relativi KPI è una fase propedeutica alla predisposizione di un eventuale budget costi/investimenti da presentare l'anno successivo. In una grande azienda è un processo che per portare il modello a regime potrebbe chiedere dai 2 ai 3 anni in base alla collaborazione delle strutture e alla velocità di esecuzione. Pertanto il rischio è di essere già in ritardo rispetto al futuro digitale.

Link :

- https://businessinsights.bitdefender.com/cisos-should-report-directly-to-the-ceo-study-shows
- https://www.csoonline.com/article/3228886/leadership-management/should-cisos-join-ceos-in-the-c-suite.html ■

Bibliografia

Maciej Kranz, **Connetti la tua impresa all'IOT,** FrancoAngeli ed.

NUOVI MODELLI DI BUSINESS PER L'IMPRESA

Autore: Massimiliano Cannata

Si tratta del primo saggio che inaugura la nuova collana *Business 4.0* di FrancoAngeli diretta da Alessandro Giaume, che ha come mission lo studio degli impatti della trasformazione digitale e di *Industry 4.0* sul mondo dell'impresa. I cambiamenti in atto impongono una riflessione attenta che riguarda tutti gli ambiti della catena del valore. Osservare *best practices*, casi emergenti, sperimentazioni già avviate con successo può essere una chiave per capire la tendenza fondamentale del nostro tempo.

Questo studio che FrancoAngeli ha da poco mandato in libreria è la traduzione italiana di *Building the Internet of Things*, pubblicata dall'editore *Wiley* alla fine del 2016.

La struttura del volume evidenzia l'impostazione pragmatica di chi è abituato a misurare la performance e la qualità degli impatti di apparati e sistemi sulle attività di business. La questione centrale, quando si parla di "Internet delle Cose", non risiede tanto nel soffermarsi sulla descrizione degli strumenti, il nodo reale riguarda il know-how e le competenze manageriali che sono necessarie per affrontare un salto di paradigma, che investe l'organizzazione produttiva nel suo complesso. La possibilità di connettere ogni cosa ad ogni cosa – ottimizzando processi, riducendo i costi, migliorando i fattori della performance crea innovazione, ma genera nel contempo un diverso approccio di metodo, che si accompagna a una ridefinizione della *governance* e della stessa concezione del business.

Manifattura, logistica, retail, trasporti, energia… ma anche sanità, agricoltura, governo delle città, sono investiti molti settori industriali, tanto che numerosi studiosi parlano di nuovo orizzonte del capitalismo.

Maciej Kranz, vicepresidente *Corporate Strategic Innovation Group* di Cisco System si trova in un osservatorio privilegiato per raccontare la rivoluzione in corso. È uno dei pionieri dell'IOT (se ne occupa dal 2000 sempre per Cisco), ogni anno percorre migliaia di chilometri per incontrare clienti, partner, startup per accelerare l'innovazione interna e promuovere la co-innovazione. Questo lavoro – uscito poco più di un anno fa, finito subito nella classifica dei bestseller del *New York Times*, tradotto in cinese e in spagnolo – raccoglie numerosi **"casi d'uso"** dell'IOT in una pluralità di aree di business.

Quel che più ci interessa dalla prospettiva di *Cybersecurity Trends* attiene alla estrema concretezza con cui l'autore fornisce delle indicazioni precise a imprenditori e manager che devono guardare con fiducia i fenomeni di trasformazione, impegnandosi a trovare codici, competenze e linguaggio per indirizzare lo sviluppo della civiltà digitale, verso obiettivi di effettivo progresso.

A partire da quattro "corsie veloci" che consentono di vedere subito dei risultati, senza grossi investimenti: *operation* connesse (tramite dispositivi, sensori, contatori), *operation* in remoto, analisi e manutenzione predittiva, il saggio ci porta per mano a scoprire questo *"secondo tempo di Internet"*, cheforse – è vero – qualche paura la trasmette, ma *"Hic Rhodus hic saltus"*, come dicevano i Latini, è nelle difficoltà che siamo infatti spronati a crescere. ■

Renato Mannheimer, **Giorgio Pacifici, Italie - Sociologia del plurale,** Jaca Book ed.

UN ORIGINALE AFFRESCO DELL'ITALIA DI OGGI

Autore: Massimiliano Cannata

Un affresco del paese reale di oggi, percorso da cambiamenti radicali, attraversato dal vento della rivoluzione tecnologica, in bilico tra passato e futuro, questo in sintesi il cuore di un saggio agile e di piacevole lettura pensato e realizzato da due autori che conoscono il mondo.

Giorgio Pacifici, sociologo del cambiamento, tra i pochi intellettuali a tutto tondo, figura originale di pensatore capace di spaziare sui grandi temi del nostro tempo con lucidità e onestà. Il suo occhio attento va a individuare le fratture, i luoghi in cui l'innovazione si annida, non per dare giudizi di valore, piuttosto per individuare le possibili strade del progresso. Questa attitudine, che lo ha portato a spaziare dall'Asia all'America dove ha insegnato, lo ha recentemente condotto ad occuparsi di quelle che ha definito "Le maschere del male", un mistero per i credenti e un interrogativo per le coscienze laiche.

Renato Mannheimer, tra i sondaggisti più noti del nostro panorama, aggiunge allo sguardo cosmopolita di Pacifici la superba capacità nell'applicare una potente lente di misurazione e di osservazione quali-quantitativa dei fenomeni che attraversano la contemporaneità.

Colpisce il titolo al plurale, che suona come un elogio della *"varietà e della differenza"* per una Italia che spera di non essere mai più una *"mera espressione geografica"*, per usare lo sprezzante giudizio storico del Metternich.

Bibliografia - Cybersecurity Trends

Il fattore tecnologico è ancora una volta una cartina al tornasole dell'analisi sociale, come dimostra la stessa architettura del testo che riflette lo stile di un metodo dialogico, aperto, problematico. Il contesto culturale entro cui va infatti inserito questo lavoro è quello disegnato da Daniele Gambetta nell'antologia *"Datacrazia"* (di cui parleremo nel prossimo numero della rivista) e da autori come Michele Mezza (cfr. intervista) che in *"Algoritmi di Libertà"*, denuncia *la potenza del calcolo* che vede l'individuo controllato e prosciugato nella sua consapevolezza e autonomia cognitiva e comunicativa. La sfida è quella di tentare di partecipare alla costruzione di senso entrando nel circuito relazionale della rete, scongiurando il pericolo che un algoritmo possa decidere per noi, imprigionandoci in un meccanismo perverso.

Importante soffermarsi sulla definizione di OPERATORE GLOBALE coniata dagli autori perché, oltre ad essere di per sé innovativa, ci riporta al linguaggio degli studiosi della complessità e della termodinamica, abituati a ragionare *sui sistemi lontani dell'equilibrio, in quanto catalizzatori dei processi di cambiamento*. **L'operatore globale** fa pensare a un soggetto denso di articolazioni interne, che esprime poi il corpo sociale dell'Italia di oggi, che presuppone la messa in crisi dell'idea di sistema, mentre si liquefà il concetto di classe e le identità nel contesto digitale diventano *porose, fluttuanti*.

I dati (il saggio è ricco di un'analisi puntuale del corpo sociale italiano di oggi particolarmente interessante) riportati nel testo impongono una riflessione. Proviamo a richiamare i più allarmanti, quelli che fanno sentire la necessità di una cura sociale: tra la popolazione italiana si calcola che vi siano 4 milioni che vivono nella povertà assoluta, dentro un'area del malessere che sfiori i 7 milioni di unità. 50 mila sono i senza fissa dimora. A questo punto bisognerà chiedersi: Quali possono essere se ci sono, i fattori di coesione?

In una società polarizzata, in cui l'uso delle tecnologie è una cartina al tornasole del posizionamento sociale, forse sarà impossibile trovare una risposta che prescinda dallo sviluppare al più presto nuove competenze e professioni.

Basti pensare al fortunato gruppo della *"@ristocracy"*, che vive dentro l'area del benessere (esiste ancora a dispetto di quanto si possa pensare) e che vive il SOGNO TECNOLOGICO, perché ha imparato a usare gli apparati hi-tech quali strumenti di libertà.

Un punto di osservazione importante è rappresentato dall'area della creatività, da quei "vagabondi del virtuale" identificabili con quella categoria di giovani, che hanno attitudine per la mobilità e che hanno una mente globale, che possiedono le potenzialità per interpretare i processi di metamorfosi che caratterizzano il Paese e che potrebbero tramutarsi in classe dirigente, se solo il paese si accorgesse di loro. Una cosa è certa: difficile capire in questo momento di confusione quali saranno i ceti emergenti non solo in Italia, ma in Europa.

In conclusione si può dire che tra luci e ombre la lettura del saggio di Mannheimer e Pacifici ci lascia con il positivo desiderio di edificare un nuovo orizzonte di convivenza, basato su sensibilità etica e valori, in cui ciascuno potrà dire la sua, in un giusto bilanciamento di diritti e doveri, e dare un contributo fattivo per la costruzione della società del futuro. ■

Una pubblicazione

AGORA get to know! e

web for business swiss webacademy

A cura del Global Cyber Security Center

Redazione:
Laurent Chrzanovski e Romulus Maier
(tutte le edizioni)
Per l'edizione del GCSEC:
Nicola Sotira, Elena Agresti

ISSN 2559 - 1797
ISSN-L 2559 - 1797

Indirizzi:
Bd. Dimitrie Cantemir nr. 12-14,
sc. D, et. 2, ap. 10, settore 4,
040234 Bucarest, Romania
Tel: 021-3309282
Fax 021-3309285

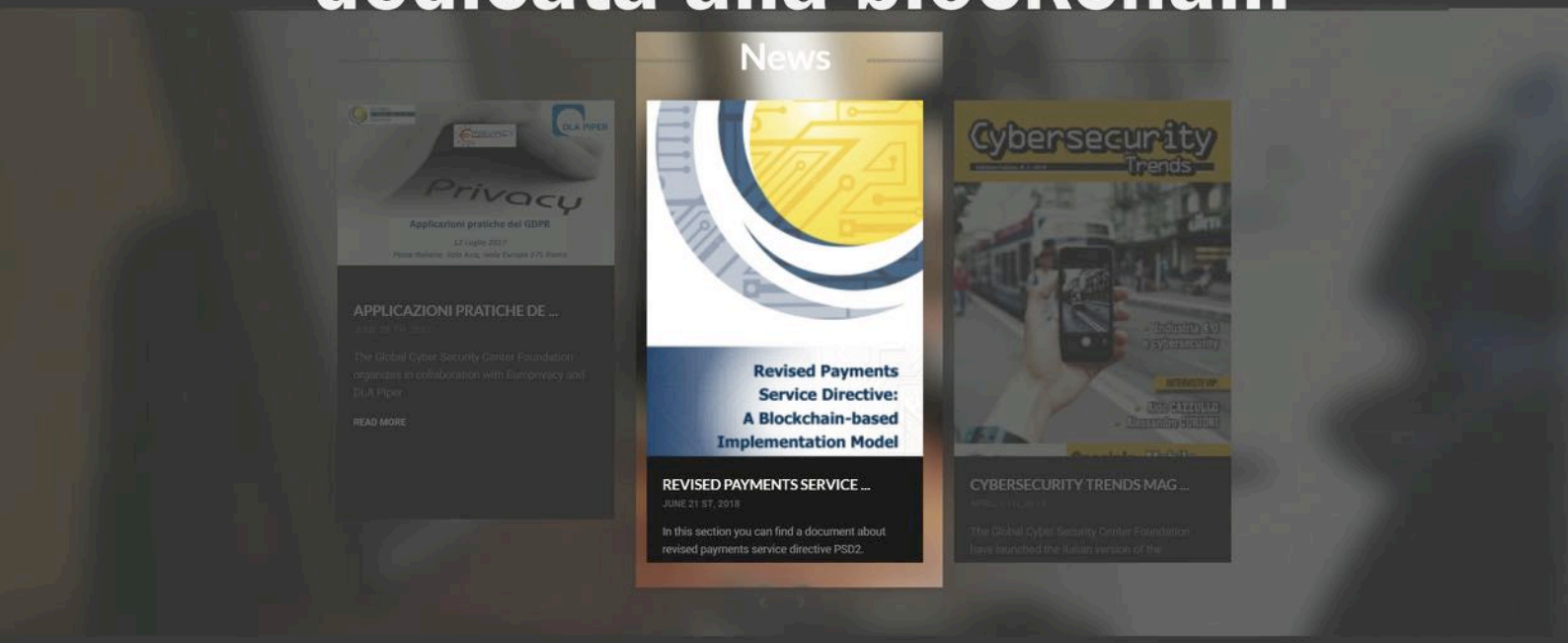
Viale Europa 175 - 00144 Roma, Italia
Tel: 06 59582272
info@gcsec.org

www.gcsec.org
www.cybersecuritytrends.ro
www.agora.ro
www.swissacademy.eu

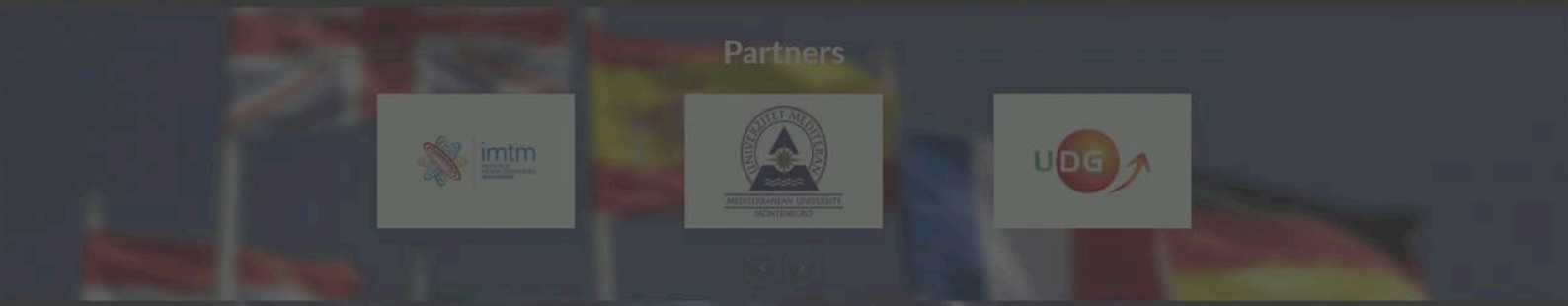
Revised Payments Service Directive:
A Blockchain-based Implementation Model

available in the reserved area "Publication"

Leggi la nuova pubblicazione del Global Security Center dedicata alla blockchain



Iscriviti al sito www.gcsec.org e scarica il testo integrale



web for your business
swiss webacademy

together with:

AGORA
poți să știi!

iCyber-Security
SAFEGUARDING YOUR DIGITAL WORLD

Present:

CYBERSECURITY ROMANIA CONGRESS
6th Edition

6th Central European Cybersecurity Congress

A Public-Private-User Dialog Platform
September 13-14, 2018, Sibiu, Romania
https://cybersecurity-romania.ro

With the support of: ITU

Under the High Patronage of:
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

In partnership with:

ANCOM
Autoritatea Națională pentru Administrare și Reglementare în Comunicații

ROMANIA SRI Patria a priori SERVICIUL ROMAN DE INFORMATII

ROMANIA CENTRUL NATIONAL CYBERINT SERVICIUL ROMAN DE INFORMATII

IGPR
POLIȚIA ROMÂNĂ

DIRECȚIA DE COMBATERE A CRIMINALITĂȚII ORGANIZATE I.G.P.R.

CERT.RO

GLOBAL CYBER SECURITY CENTER

Gendarmerie nationale
Une force humaine

RÉGION-IHEDN FRANCHE-COMTÉ

Centre de recherche de l'EOGN

REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX

POLICE GENEVE

IATA

FIC 2018

CCI TERRITOIRE DE BELFORT

SIBIU COUNTY COUNCIL

ULBS
Universitatea "Lucian Blaga" din Sibiu

1948
UNIVERSITATEA DIN PETROȘANI

Vallée de l'Energie