Susan Brown Slizys (USA, Art signature name) - Blockchain Universe

Il telefono blockchain

di *Vincenzo Rampolla*

Siamo alle porte di una rivoluzione. L’ondata di *blockchain phones* è un primo passo verso il *web* decentralizzato.

Ci risiamo con i termini incomprensibili. Sii chiaro … che significano?

Il mondo criptato è fatto di parole d'ordine! Scrollati di dosso le fantasie e la crudeltà del marketing, sotto la crosta spunta a volte il meglio.

La tecnologia *blockchain* è d'avanguardia, in anticipo sulla storia. Datti da fare. Leggi, pensa, osserva. Le cose cambiano. Apri gli occhi.

Quando ero matricola a Fisica la nuova tecnologia erano gli acceleratori di particelle che diffondevano la filosofia dell'energia, l'energia della materia. Dopo quasi 60anni si va nel senso opposto. La tecnologia regnante è l'Intelligenza Artificiale, l'AI che va disperatamente alla ricerca di una filosofia guida.

La sua improvvisa ascesa sta permeando ogni aspetto della nostra vita, per primo il linguaggio e sta trasformando i sistemi sociali, politici ed economici. Non accettiamo più una società che rifletta le vecchie barriere montate nei secoli, c'è bisogno di ristudiare il modo in cui pensiamo e impariamo. È tempo di smantellare le idee obsolete che predicano che la tecnologia è per le persone *tech* e i problemi sociali sono per le persone umanistiche.

Ti rendi conto? È ora di innovare la *forma mentis* dei giovani, scardinare le differenze tra liceo classico e scientifico, creare il cambio culturale nella ricerca e nell'industria e far crollare la distanza tra questi campi tribali. Quelli che dici "termini incomprensibili" sono il linguaggio di domani, anzi di oggi. Tutti devono assimilarlo e viverlo.

Senza preavviso spuntano sul mercato diversi telefoni criptati. Il grande arbitro e attore del nuovo gioco è Samsung. Ha annunciato che questo mese il Galaxy S10 includerà un semplice sistema di archiviazione, sicurissimo e adatto per chiavi private di criptovaluta.

Samsung fa coppia fissa con HTC (Taiwan), per mesi mercante di Exodus 1, con la *start up* Sirin Labs israeliana del primo telefono con *blockchain*, con i proventi di una ricca operazione di raccolta fondi ($160M) per costruire il suo telefono Finney e per ultimo con Electroneum, che ha iniziato a distribuire un telefono Android da $ 80 capace di fare *mining* di criptovaluta (acquisto e vendita).

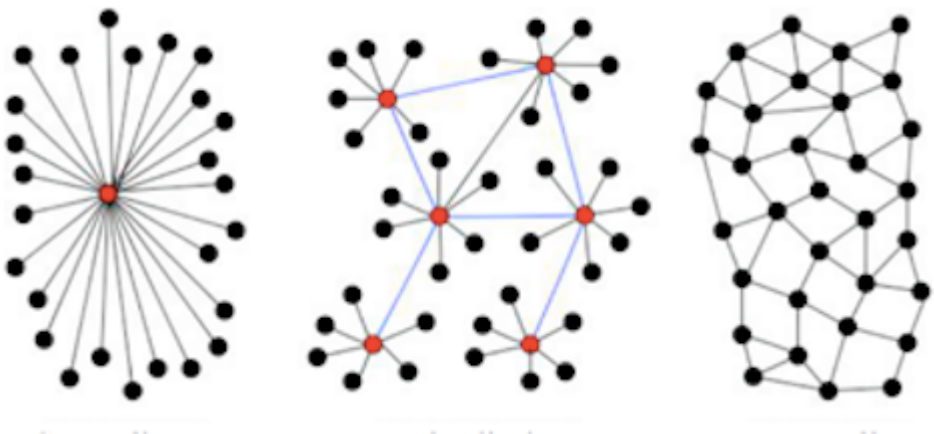
Si sguazza nel nuovo linguaggio. E qual'è il punto? Nei sogni più sfrenati degli appassionati, questi aggeggi saranno una droga di accesso a qualcosa chiamato Web 3.0 o *web* decentralizzato, la versione futura di Internet. *Blockchain* e tecnologie simili offrirebbero le *dapps* (*decentralized applications*), le nuove applicazioni simili alle *app* usate oggi, ma che vanno su reti pubbliche, non sui server privati â€‹â€‹dei big della tecnologia.

Allora … questo *web* decentralizzato, che diavolo è?

Web è rete, ragnatela, da *WWW, World Wide Web.* Rete di cosa? Rete mondiale decentralizzata di calcolatori che mette tutte le informazioni di ogni calcolatore a disposizione di altri utenti che vi possono accedere da ogni punto del pianeta.

Immagini, video streaming, sistemi operativi, testi, databases, backup di floppy disk di vecchia data e soprattutto nodi della rete ben definiti navigano sul *web*, viaggiano in *Internet*, grazie al *browser*, il navigatore, con l'applicazione *dapp* che rende possibile il *web* decentralizzato.

Semplice, no? Sì.



Centralizzata Distribuita Decentralizzata

Gli schemi mostrano strutture centralizzate di collegamento di calcolatori periferici convergenti su un unico potente elaboratore centrale; strutture di *distributed processing,* distribuite su diversi calcolatori centralizzatori di potenza ridotta e interconnessi e strutture aperte decentralizzate, senza calcolatori centrali o distribuiti (immagini da MIT Technical Report).

Allora è tutto chiaro. Neanche per sogno.

La domanda è: quante persone vogliono veramente o hanno bisogno di uno smartphone con blockchain? Che intendono fare a breve termine? Quanti hanno bisogno di memorizzare chiavi su un telefono e usarle per pagare?

Non fai che ripetere che il principale ostacolo all'uso generalizzato di criptovaluta e di *dapps* sia la pratica di queste tecnologie da parte di chi non è particolarmente esperto e i termini ti fanno paura. Eppure non c'è persona che non dorma con lo *smart* sul comodino e continuiamo a dirci che a partire dalla gestione delle chiavi crittografiche, le esperienze nuove e di livello dell'utente non possono che stimolarne l'adozione.

È vero? Sì, ma la cosa non è semplice. Adeguati ai tempi.

La sicurezza delle chiavi è fondamentale: perdi le chiavi, perdi i soldi.

Perché V.Buterin, creatore di Ethereum, secondo produttore di criptovalute dopo Bitcoin, sembra così entusiasta del recupero delle chiavi sociali, caratteristica particolare di Exodus 1?

In due parole, gli utenti possono scegliere persone cui affidare parti delle proprie chiavi, ripartite a dovere. Se le perdono, le recuperano pezzo per pezzo. Nello smartphone si scarica un'apposita *dapp* che con un algoritmo proprietario e sicuro, ti fa recuperare i dati.

Buterin guarda lontano, in un futuro in cui le persone useranno *blockchains* per mantenere il massimo controllo sulle loro identità digitali e sui dati personali, più di quanto non sia possibile oggi. *Il recupero delle chiavi sociali è probabilmente un primo passo verso un'identità non burocratica né di controllo*, ha dichiarato.

Exodus 1 è da poco sul mercato italiano. È il primo *blockchain phone* di HTC.

Lo smartphone ha un portafoglio per criptovaluta sicuro**,** in un'area di software separata e protetta, usata per memorizzare le chiavi delle criptovalute e i relativi dispositivi di protezione**.** Exodus 1 è un top di gamma con doppia fotocamera, 3D audio e Sonic Zoom. È anche aperto agli sviluppatori di terze parti che vogliano costruire le proprie chiavi e relativi portafogli.

Si acquista in criptovalute, 0,15 bitcoin o 4,78 ethereum, circa € 830.

E allora … Continui a parlarmi del telefono. Cerchi di rifilarmi un Exodus 1? Neanche per idea. Cerco di arrivare al dunque. Svegliati.

Per attrarre utenti al di fuori della schiera di appassionati e speculatori, questi telefoni dovranno fare ben altro che custodire le chiavi e parlo del telefono perché tutti ne hanno uno in tasca.

A fine 2018, Samsung e HTC hanno annunciato un programma di collaborazione per diversi progetti *blockchain*, inclusi i servizi di bellezza *dapps* Cosmee e Enjin, una piattaforma di gioco basata su *blockchain*.

HTC ha anche rivelato una collaborazione con Opera, produttore norvegese di *browser* e di piattaforme integrate di AI, per facilitare l'impiego della crittografia, per effettuare micro pagamenti su siti Web e per nuove *dapps*.

Siamo agli albori di una nuova generazione del Web, i*n cui nuovi servizi decentralizzati sfideranno lo status quo*, dichiara il Direttore della Divisione Cripto di Opera.

Andiamoci piano. Anche se questi telefoni decollano, il *web* decentralizzato appare lontano. La costruzione della sua offerta di base è in embrione. Un flusso di nuovi utenti genererebbe nuove applicazioni, che a loro volta ispirerebbero lo sviluppo di nuove infrastrutture, ma il meglio che può dare il primo telefono *blockchain* è scuoterci, meravigliarci,

incuriosirci. Prepararci a un futuro rivoluzionario.

Gli unici dati ufficiali del 2015 danno più di 863 milioni di siti Internet nel mondo di cui circa la metà in Europa e 39 milioni in Italia. Tra i fornitori emerge Wix con 75 milioni e Webnode con 18. Nel settembre 2013 Neocities nasce per creare siti *web* ad ogni utente sparso sul pianeta. Oggi la sua rete sociale supera 223.000 unità. Fornisce il linguaggio HTLM per adattare e impaginare i documenti disponibili nel *web,* ha una linea di controllo, la gestione del caricamento dei file, la garanzia delle prestazioni di velocità, il dialogo con altri fornitori di siti *web* e dà l'assistenza tecnica.

Neocities può vantare oggi più di 2.6 miliardi di collegamenti, 1 miliardo di accessi sulla sua rete e 29.6 milioni di aggiornamenti; eppure è un fornitore di dimensione microscopica rispetto ai big mondiali, ma è stato il primo a dichiarare la morte di **HTTP** (*Hypertext Transfer Protocol*), il protocollo adottato mondialmente per standardizzare la distribuzione dell'informazione nel *web* (documenti, musica, video, giochi …).

HTTP ha fatto il suo tempo. È nato distribuito, ma l'attuale miliardo di utenti lo limita. Lo rende centralizzato, impoverito dalla manciata di servizi che ancora è capace di offrire. Sapendo che il costo totale per ogni Gigabyte trasferito è oggi di 1 centesimo, la spesa totale per Neocities è vicina a 1 milione. Inaccettabile.

Per l'intera rete Internet, per la sicurezza dei centri di controllo dei nodi principali e per la manutenzione dei cavi della fibra ottica il protocollo è inefficiente e Neocities riflette. Che succede se ogni mio file invece di inviarlo in base al nome in una rete di milioni di computer lo invio in base al contenuto, quello che ovviamente è nel file?

Perché non chiamare il file con un altro nome, legato alla dimensione, con una chiave crittografata (*cryptographic hash*) calcolata proprio in base alla dimensione? E se cambio anche un solo bit nel mio file? La chiave *hash* sarà completamente diversa. Con il registro delle chiavi, con 20 accessi su 10 milioni di nodi, posso subito individuare il nodo dove il mio file è andato a finire.

I costi si sbriciolano. Neocities agisce e rimpiazza il protocollo in essere con un nuovo protocollo più evoluto, l'**IPFS** (*Interplanetary File System*) e dà il via alla rivoluzione della rete decentralizzata Internet.

Con IPFS non ci sono limitazioni di memoria. Si trasferiscono files piccoli e grandi, anche grandissimi che sono automaticamente divisibili in sotto files potendo i nodi IPFS scaricare i files non da un unico server centrale ma simultaneamente da centinaia.

La rete IPFS è *blockchain*, un reale strumento di aggregazione distribuito, decomposto in finissime maglie e aperto ad accogliere ogni tipo di dati e soprattutto nodi web univoci, come avviene con la procedura attuale, con la differenza che per assegnare un sito *web* a un nodo IPFS è sufficiente una sola istruzione.

Da quell'istante il sito *web* è accessibile da ogni nodo della rete, senza doverlo collegare a nessun registro di riferimento. L'assenza di un server centrale elimina il bisogno del benestare di un ente di certificazione e i costi si riducono drasticamente.

Neocities ce l'ha fatta e la fase iniziale della rivoluzione richiede ora un'attenta serie di sperimentazioni per pianificare le diverse tappe della migrazione dalla procedura attuale distribuita HTTP a quella decentralizzata IPFS.

Il primo passo? Concentrarsi sulla creazione di un archivio storico di tutti i siti, organizzato secondo i nuovi protocolli. Con a disposizione le chiavi crittografiche può mutare un file di lunghezza arbitraria in una chiave di lunghezza corta e predefinita, unica e sicura, che impedisce di risalire al messaggio di partenza.

È il contenuto del file o di un suo blocco che determina il suo indirizzo e la sua posizione nella rete non il nodo o il computer in cui è registrato.

Con una semplice istruzione il file viene decomposto in blocchi e organizzato in una struttura ad albero in cui i blocchi sono interconnessi con nodi di collegamento.

La tecnologia *blockchain* e il *web* decentralizzato sono rivoluzionari: chiunque può inserirsi in una rete aperta, non è richiesta un'entità di controllo, i dati fluiscono liberamente generando un vantaggio competitivo attraverso la condivisione e garantendo all'utente un maggiore controllo sui propri dati.

È di ieri l'esempio dell'Estonia in cui il Governo utilizza la tecnologia *blockchain* per proteggere i dati governativi e consentire ai cittadini un maggiore controllo sui propri medici, sui dati e sugli operatori sanitari, sull'identità digitale, la

gestione della forza lavoro e l’archiviazione dei dati decentrati nei reparti.