volerelaluna LA POLITICA PUNTOACAPO

Blockchain o Ball and Chain? Il diabolico incrocio tra criptovalute e intelligenza artificiale

Autore: Franco Marra

Volerelaluna ha ospitato nelle settimane scorse vari interventi sul tema dell'Intelligenza Artificiale (AI), delle sue sfide e dei suoi pericoli. Franco Marra, che già ha contribuito a questa analisi (https://vll.staging.19.coop/societa/2024/03/04/internet-la-promessa-tradita/), interviene ora con un secondo contributo, sui rapporti fra AI e criptovalute. Il tema è di grande rilevanza, ma porta in un territorio estremamente oscuro, in cui il rischio di non capire cosa sta succedendo è elevato. Marra ha fatto un grande sforzo di semplificazione, riscrivendo più volte l'articolo. Anche così, il profano fa fatica. Poiché pensiamo che aiutare a capire sia un compito di questo sito, abbiamo proposto a Marra di presentare quanto ha scritto in un incontro, il 4 giugno alle ore 18, in cui faremo un tentativo didattico: lui comincerà a raccontare, e i presenti, passo dopo passo, interverranno per farsi spiegare i punti più astrusi. Proviamo… (la redazione)

Il concetto di criptovaluta è ostico, ma chi ha giocato a Monopoli ne ha una conoscenza intuitiva. La differenza è che i soldi, invece di darteli la banca all'inizio del gioco, te li devi sudare in una gara a chi fa prima a risolvere un puzzle calcolando un *hash*.

Ma cos'è un hash? Per capirlo bisogna partire dalla crittografia (o, per capirci, "scrittura nascosta"). Pensiamo alla relazione che esiste tra un racconto e il suo riassunto. Cambiando in una certa misura il racconto la fedeltà del riassunto svanisce. Ma supponiamo di essere di fronte a un riassunto "perfetto" (qualunque cosa questo termine voglia dire). Se il riassunto fosse abbastanza corto lo si potrebbe usare come titolo "perfetto" del racconto. Il racconto avrebbe un solo titolo e titoli anche leggermente variati corrisponderebbero a racconti del tutto diversi. Con la matematica si può fare, purché l'originale sia digitale, ossia codificato in un blocco di bit. Applicando delle trasformazioni crittografiche si ottiene un suo riassunto in bit, il suo hash. Se si vuole verificare che il racconto sia in copia originale lo si fa tritare dall'algoritmo di hash, e poi si confronta il risultato con l'hash di prima. Se sono diversi, il racconto è stato modificato.

E ora raccontiamo la storia dall'inizio.

Nei primi anni del terzo millennio nasce il Partito Pirata svedese. Per gli aderenti a questo movimento Internet è uno spazio pubblico libero, al di fuori del potere dei governi, delle multinazionali dell'*Information Technology* o dell'industria dei media. Il bersaglio dei Pirati è il *copyright*, il diritto d'autore: il nome stesso del movimento richiama la pirateria *on-line*, l'attività che porta alla fruizione di contenuti multimediali, musica, filmati, senza riconoscimento dei relativi diritti. Viene fondato un sito di *file sharing*, "The Pirate Bay", che adotta un particolare protocollo per distribuire contenuti protetti da copyright, il *BitTorrent*. Usando il BitTorrent, un prodotto multimediale, trasmesso in

segmenti identificati e verificati dai loro hash, viene condiviso ennuplicandolo con chiunque sia interessato alla sua fruizione. Basta il furto originale a spese del detentore dei diritti e il contenuto si propaga viralmente. Un protocollo che avrà ai nostri tempi un inatteso successo in un campo del tutto diverso, quando le comunità di Internet culturalmente eredi dei Pirati decideranno di usare Internet come piazza per i loro commerci come se fosse un tabellone del Monopoli. Dovranno però prima inventare una rappresentazione digitale del mercato e implementare in rete l'idea di valuta.

Un mercato è uno spazio in cui si scambiano cose, e una valuta è il metro di misura che consente la stima del valore relativo delle cose, una *unità di conto*. Una mela vale due carote quando il suo prezzo espresso in valuta è il doppio di quello della singola carota. È il simbolo intercambiabile di un qualche sostituto degli ortaggi e di tutte le altre merci, un bene materiale (*sottostante*) stabile nel tempo, raro e maneggevole, ambito da tutti sopra ogni altra merce. Parliamo dell'oro, che può assumere nel digitale una nuova e inusitata forma, un gruppetto di bit ottenuto con molta fatica algoritmica e a un costo elevato da un altro blocco di bit: il suo hash. Per analogia con l'estrazione dell'oro, questo "scavo" matematico si chiama *mining,* e chi ci lavora è un *miner*. Il miner intasca in un suo borsellino digitale, il *wallet*, il premio per la sua fatica: il prezzo dell'oro digitale che ha "scavato", un valore per il costo del calcolo riconosciuto dalla comunità in cui opera, espresso in qualche valuta convenzionale che faccia da unità di conto come i soldi del Monopoli. Userà quella somma per far commercio di beni reali nella rete comunitaria: ogni guadagno e ogni spesa andrà ad aumentare o a diminuire il contante nel suo wallet, e il valore di ogni transazione verrà registrato in una voce, un *token,* nel blocco di bit che ha fatto da miniera. Questo diventerà una pagina del registro, il *ledger*, di tutte le transazioni fatte sul mercato, che rimarranno anonime. Per verificare in futuro se questa pagina del ledger è stata alterata basterà ricalcolare il suo hash e confrontarlo con quello originale, memorizzato in un altra pagina dello stesso registro. Per essere verificabile, questo registro sarà pubblico, ennuplicato in visione per tutti gli attori del mercato con il protocollo di comunicazione erede del BitTorrent dei Pirati.

Ma il nostro miner non è il solo a far sudare gli algoritmi. Ogni blocco viene estratto in una gara con gli altri miner che agiscono sul mercato, dove vince e incassa il premio il più veloce. Se validato dalla comunità il nuovo blocco viene aggiunto come ultima pagina al ledger, legato dal suo hash, ultimo anello della catena della *blockchain* che ne costituisce l'impaginato. Questa gara algoritmica è devastante dal punto di vista energetico, per la complessità del calcolo che viene eseguito da molti miner ogni 10 minuti circa, il tempo richiesto dall'algoritmo di hash. Si crea valore a spese dell'ambiente, secondo la più tipica tradizione capitalista estrattiva e di sfruttamento delle risorse naturali. Alla faccia degli iniziali buoni propositi e manifesti politici dei Pirati.

La prima criptovaluta, del 2009, è stata il *bitcoin*. Sui *bordi* della rete, negli *exchange* dove si scambia la criptovaluta con quella del mondo reale, si fa speculazione facendo così assumere alla valuta della Rete il ruolo oggi predominante di *riserva di valore*

per il mondo esterno. Gli speculatori comprano criptovaluta come una volta compravano oro, scommettendo sul suo futuro aumento di valore assicurato dall'anonimato delle transazioni, assai gradito a chi non vuol mettere in piazza i propri affari e dal numero limitato a priori dei bitcoin in circolazione. Questa è la notizia che rimbalza sui media.

Ben presto, nel 2013 al bitcoin segue l'*ether*, una criptovaluta della piattaforma Ethereum. Segue poi una pletora di altre criptovalute associate alle loro blockchain dall'intento più o meno speculativo, a popolare quello che ormai si chiama Web 3.0, il web delle transazioni economiche.

Nel 2014 fanno il loro esordio i *Non-Fungible Token* (NFT), voci che registrano diritti di proprietà su oggetti digitali unici come arte crittografica, oggetti da collezione digitali e giochi online usando nelle transazioni i loro hash, come rimedio alla riproduzione di massa e distribuzione non autorizzata di copie in Internet. Si tratta di token quindi non più "fungible", ma associati per sempre a un determinato bene. Per estensione anche fisico, purché digitalizzabile, di cui divengono i *digital twin*, i gemelli digitali. Repliche virtuali di oggetti, processi, luoghi, infrastrutture, sistemi e dispositivi e che stanno assumendo un'importanza crescente nella IoT, l'*Internet of Things* e nell'industria 4.0, ma anche di tutto quel nostro portato esperienziale che vive in chiave digitale.

Nell'autunno del 2022 un'organizzazione nata con scopi etici e cooperativi assicurati dall'adozione di metodologie *open source* di produzione e gestione del codice, **scopre un'irresistibile vocazione al profitto grazie all'esplosivo successo mediatico del suo prodotto di Intelligenza Artificiale Generativa, *ChatGPT***. Il suo vate, la nuova superstar della galassia digitale, è Sam Altman, un giovane imprenditore informatico statunitense (1985). Successo mediatico che diviene presto successo di mercato grazie a robuste iniezioni di dollari della Microsoft, che infine acquisisce la società dopo vicende da *soap opera* apparse sui media di tutto il mondo ((https://vll.staging.19.coop/societa/2024/02/20/la-saga-di-sam-altman-lintelligenza-artificiale-e-la-vittoria-del-profitto/). Sam Altman nel 2021 aveva già fatto nascere Worldcoin, un'impresa per gestire una criptovaluta basata sull'identificazione biometrica dell'identità tramite scansione dell'iride. Questa società ha come fine dichiarato lo sviluppo di "*tools for humanity*" finalizzati allo sviluppo di un'economia mondiale basata sui principi di quella di Internet. Tra questi, spicca il cosiddetto *orb*, lo strumento di scansione dell'iride umana. Chi si sottopone alla scansione viene ricompensato proprio con dei worldcoin, spendibili nella cyber-comunità creata da Altman, di cui viene a far parte. Ora mettiamo insieme le cose.

La tecnologia dell'intelligenza artificiale ha bisogno di una grande quantità di lavoro umano dedicato all'identificazione certa dei dati estratti da Internet (https://vll.staging.19.coop/in-primo-piano/2024/04/03/clic-senza-frontiere-cosa-ce-alla-base-dellintelligenza-artificiale/). Questo *esercito industriale di riserva* (per dirla alla Marx), arruolato nel terzo mondo tramite piattaforme internet di *microtask* come

Mechanical Turk di Amazon, è impiegato con un salario di sussistenza a etichettare quelle immagini o situazioni che formano i gangli delle reti neurali artificiali, e a decidere sulle scelte impraticabili per le macchine o a censurare gli orrori di Internet (decapitazioni, pedofilia e altre piacevolezze): prima rovistavano tra i rifiuti delle discariche degli *slum* rischiando la salute fisica, ora rischiano quella mentale rovistando nelle discariche del web per un paio di dollari all'ora.

Quello che allora si intravede tra le brume del digitale è un crocicchio diabolico sede di un possibile incontro tra le tecnologia delle criptovalute e dell'intelligenza artificiale. Come nel *crossroad* nel delta del Mississippi dove il diavolo insegnò a Robert Johnson a suonare il blues svettava un albero, in questo incrocio troviamo gli hash delle iridi degli arruolati di Sam Altman, registrati tramite NFT nella blockchain del worldcoin. Forza lavoro per la sua Intelligenza Artificiale, consumatori nel suo mercato e, tramite i loro digital twin, oggetto di diritti da lui posseduti. La vendita digitale dell'anima in cambio di una manciata di soldi da Monopoli, transazione registrata permanentemente in un registro sicuro e affidabile e associata univocamente all'umano tramite uno dei suoi dati biometrici, tra i più personali e identitari: la sua iride. A me ricorda molto la versione digitale della palla al piede a cui si incatenavano gli schiavi. Una *ball and chain*. E certo non quella cantata da Janis Joplin nel Monterey Pop Festival del 1967 (1), una grande cover dell'omonimo brano blues di Big Mama Thornton.

note:

(1) «Il Festival Internazionale di Musica Pop di Monterey (Monterey Pop Festival) è stato un festival musicale che si è svolto dal 16 giugno al 18 giugno 1967. Vi parteciparono più di 200.000 persone ed esso è anche riconosciuto come uno degli apici del movimento hippie e il precursore del festival di Woodstock, che si svolse due anni più tardi» (Wikipedia).