

CRYPTOVERSE:

Un tuffo nella tana del bianconiglio

Ing. Jacopo Grecuccio

4

La Pascalina

- Il primo esemplare funzionante di macchina «automatica» in grado di eseguire calcoli fu costruito attorno al 1642 dal matematico francese Blaise Pascal
- La «Pascalina» era in grado, tramite una serie di ingranaggi meccanici, le operazioni di sottrazione e somma
- Successivamente (1673) un altro matematico, Leibniz, realizzò una seconda macchina calcolatrice in grado di svolgere, oltre alle operazioni di somma e sottrazione, anche le operazioni di moltiplicazione e divisione



Il calcolatore di Babbage

- Nel 1833 Charles Babbage teorizzò la prima «macchina analitica»
- Questa macchina rappresenta di fatto il primo antenato dei moderni computer («calcolatori»)
- La macchina, in linea teorica, doveva fungere da calcolatore programmabile, tuttavia Babbage realizzò solo il «mulino» (unità aritmetica) e non completò mai il prototipo
- Nonostante la macchina di Babbage rimase solo un concetto teorico nel 1842, la contessa Ada Byron scrisse i primi programmi della storia, pensati appunto sul modello della macchina analitica

Il calcolatore di Babbage

- Negli anni successivi l'idea di Babbage fu ripresa e sviluppata, portando alla realizzazione della macchina «differenziale» (1858)
- Negli stessi anni (1854) George Boole inventò l'omonima algebra booleana ed il codice binario
- A cavallo tra la fine dell' 800 e gli inizi del 1900 nacquero altri prototipi di macchine elettro-meccaniche e vennero brevettate le prime schede perforate (1896)
- Nel 1904 Jhon Fleming inventa il «tubo a vuoto», il primo antenato dei moderni transistor

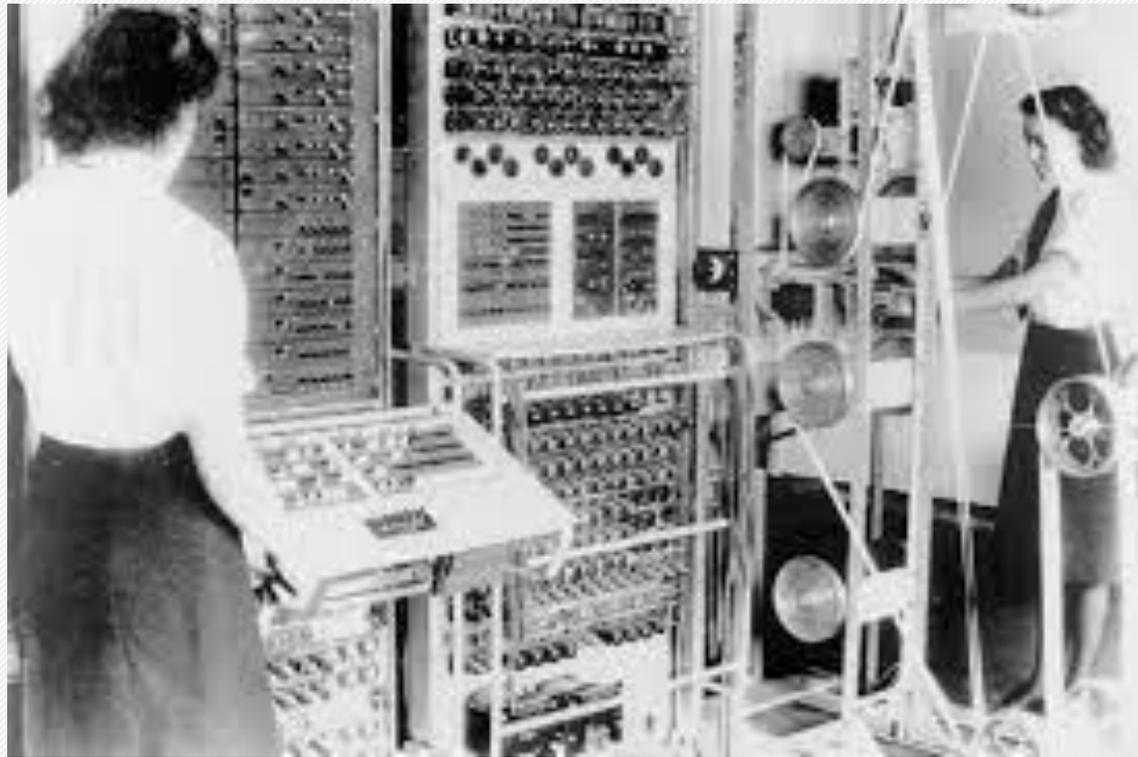
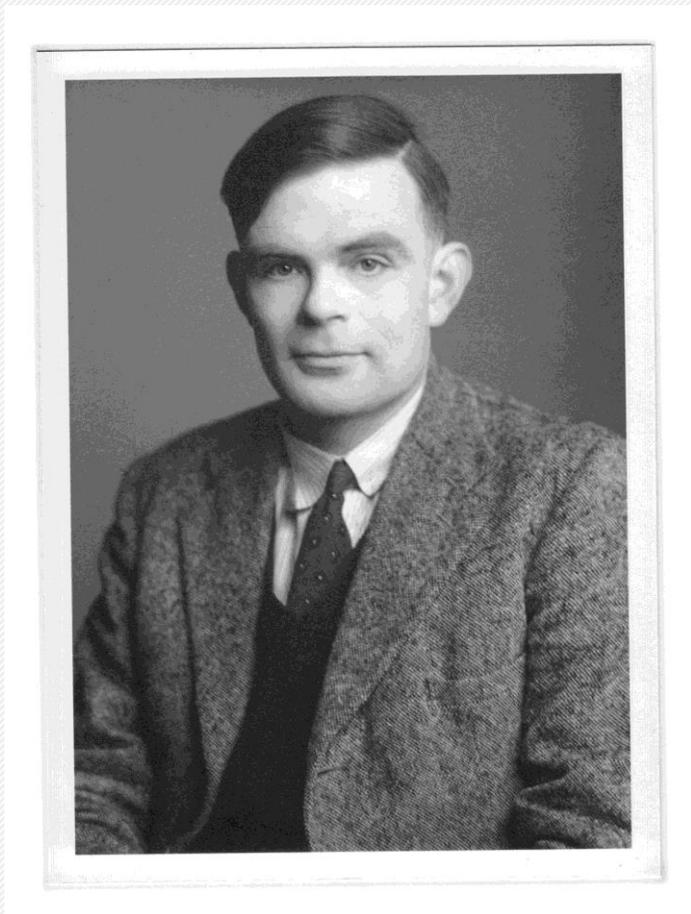
La seconda guerra mondiale

- A cavallo tra la seconda metà degli anni '30 e la fine della seconda guerra mondiale, la necessità di sviluppare calcolatori sempre più veloci e «flessibili» crebbe a dismisura, principalmente per via di scopi di spionaggio tra le potenze alleate ed i tedeschi
- Molti tra i progetti nati in quegli anni infatti erano stati creati per poter «rompere» i meccanismi di crittografia utilizzati dalle forze naziste
- Il progetto che, tra tutti, riuscì a vincere la battaglia contro la macchina Enigma (tedesca) fu Colossus.

Alan Turing ed il progetto Colossus

- Il progetto fu condotto dal matematico e crittografo inglese Alan Turing a Bletchley Park, località inglese a pochi chilometri da Londra
- Lo scopo del progetto Colossus era cercare di decifrare circa 2000 messaggi segreti che venivano intercettati ogni giorno dalle forze alleate
- Il progetto Colossus portò allo sviluppo di una macchina in grado di decifrare in maniera automatica i messaggi tedeschi, e rappresentò un vantaggio importantissimo per la vittoria della seconda guerra mondiale
- Successivamente al progetto Colossus, Alan Turing teorizzò il primo calcolatore totalmente programmabile: la Macchina di Turing
- Alan Turing è considerato il padre dell'informatica moderna

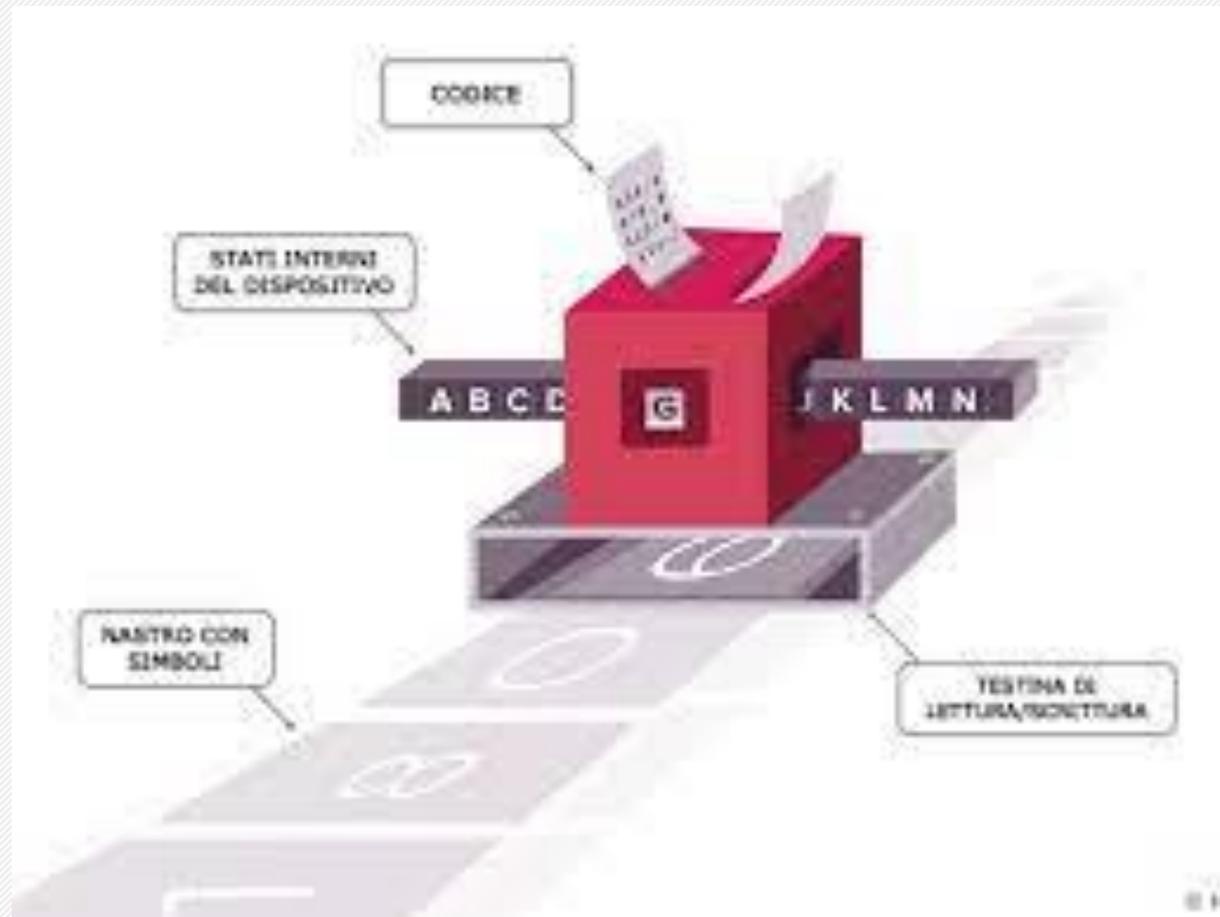
Alan Turing ed il progetto Colossus



La Macchina di Turing (1936)

- La macchina di Turing è una macchina «ideale» composta da due componenti principali:
 - Un nastro di lunghezza potenzialmente infinita sul quale suddivisa in «caselle» all'interno di ognuna delle quali sono scritti dei simboli appartenenti ad un determinato «alfabeto»
 - Una testina in grado di spostarsi leggere e scrivere (Input/Output) sul nastro
- La macchina analizza il nastro una cella alla volta, iniziando dalla cella più a sinistra del nastro
- Ogni volta che la macchina legge una cella dal nastro ed in accordo con il suo stato interno:
 - Cambia il suo stato interno
 - Ed (eventualmente) scrive un simbolo sul nastro, oppure sposta la testina a sinistra o destra di una posizione

La Macchina di Turing (1936)

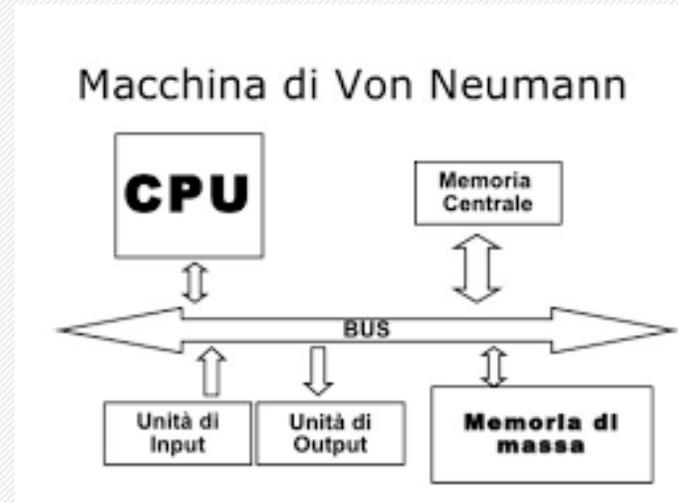


Successivi sviluppi

- I primi calcolatori basati su tubi a vuoto vennero progettati nel 1944 e 1951 ed erano denominati ENIAC ed EDVAC
- L'ENIAC fu il primo calcolatore elettrico realizzato mediante l'uso di valvole termoioniche (o «tubi a vuoto»). Era costituito da 18000 valvole ed occupava una stanza 9x15 metri. L'ENIAC era in grado di calcolare 5000 addizioni e 360 moltiplicazioni per secondo. Il computer veniva «programmato» mediante l'utilizzo di schede perforate

Successivi sviluppi

- Nel 1944 von Neumann propone il primo modello «logico-funzionale» di calcolatore programmabile
- Il modello era sviluppato in maniera «astratta» dalla specifica tecnologia di realizzazione, ed è tutt'oggi valido per ogni tipologia di calcolatore esistente («smartphone, PC, ecc)



Il transistor

- Nel 1947 Shocley, Bardeen e Brattain inventano il primo transistor dando di fatto inizio all'era dei moderni computer
- Negli stessi anni vengono anche prodotte le prime memorie magnetiche, che sostituirono le schede perforate
- A partire dagli anni '60 il «calcolatore» passa dall'essere utilizzato prevalentemente come macchina di calcolo, a macchina per l'elaborazione di dati

L'era del personal computer

- Nel 1964 la DEC realizzò il primo personal computer della storia, con lo scopo che questo possa essere utilizzato da singole persone o piccoli gruppi. Il PDP-8 venne immesso nel mercato nel 1965 ad un prezzo di 18000 dollari
- Nel 1970 negli Xerox Labs di Palo Alto nasce il primo concept di personal computer con:
 - Il primo display
 - Il primo collegamento ad una rete Ethernet (LAN)
 - Il primo collegamento ad una stampante laser
- Dallo «Xerox Alto» venne poi derivato lo Xerox Star, commercializzato nel 1981 a cui si ispirarono effettivamente poi i successivi personal computer

L'era del personal computer

- Nel 1964 la DEC realizzò il primo personal computer della storia, con lo scopo che questo possa essere utilizzato da singole persone o piccoli gruppi. Il PDP-8 venne immesso nel mercato nel 1965 ad un prezzo di 18000 dollari
- Nel 1970 negli Xerox Labs di Palo Alto nasce il primo concept di personal computer con:
 - Il primo display
 - Il primo collegamento ad una rete Ethernet (LAN)
 - Il primo collegamento ad una stampante laser
- Dallo «Xerox Alto» venne poi derivato lo Xerox Star, commercializzato nel 1981 a cui si ispirarono effettivamente poi i successivi personal computer

L'era del personal computer

- Nel 1964 la DEC realizzò il primo personal computer della storia, con lo scopo che questo possa essere utilizzato da singole persone o piccoli gruppi. Il PDP-8 venne immesso nel mercato nel 1965 ad un prezzo di 18000 dollari
- Nel 1970 negli Xerox Labs di Palo Alto nasce il primo concept di personal computer con:
 - Il primo display
 - Il primo collegamento ad una rete Ethernet (LAN)
 - Il primo collegamento ad una stampante laser
- Dallo «Xerox Alto» venne poi derivato lo Xerox Star, commercializzato nel 1981 a cui si ispirarono effettivamente poi i successivi personal computer

L'era del personal computer

- A partire dagli anni '80 i personal computer iniziano, a diffondersi a velocità sempre crescente, anche negli ambienti non scientifici.
- Oltre che la capacità di diffusione, i personal computer crescevano esponenzialmente nelle funzionalità e nella potenza di elaborazione ogni circa 18 mesi, come teorizzato dalla legge empirica di Moore
- Negli anni '90 internet ed il web fornirono un'ulteriore spinta al mercato dei personal computer, portando di fatto un computer in quasi ogni casa del pianeta
- Successivamente all'invenzione degli Smartphone il mercato dei PC ebbe una forte frenata, spostando di fatto i volumi su questa nuova categoria di dispositivi

Ethereum: «il computer globale»

- Nel 2013, sull'onda dell'innovazione portata da Satoshi Nakamoto con Bitcoin, l'informatico Vitalik Buterin propone per la prima volta l'idea di «un computer globale» a disposizione di tutti
- Il «computer globale», secondo Buterin, sarebbe dovuto essere:
 - Pubblico e decentralizzato
 - A disposizione di tutti
 - «programmabile»
- Questo computer globale sfrutta la tecnologia blockchain, utilizzata da Satoshi per tenere traccia dei trasferimenti di valore tra «indirizzi», per tenere traccia dei cambiamenti di stato di una macchina distribuita

CRYPTOVERSE:

Un tuffo nella tana del bianconiglio

Ing. Jacopo Grecuccio

5

Outline

- Lo scripting Bitcoin ed i suoi limiti
- Il progetto Ethereum
- La EVM ed il concetto di stato

La rivoluzione di Satoshi

- A partire dal 2009 lo sviluppo di Bitcoin aprì subito una vastità di nuovi scenari all'interno della comunità informatica e non solo
- Oltre agli importanti risvolti sociali ed economici che la possibilità di un sistema decentralizzato per lo scambio di valore portava con se, l'idea di Satoshi racchiudeva in se ancora più potenziale rispetto a quello espresso dalla mera applicazione di Bitcoin
- La tecnologia blockchain, assieme ad un meccanismo di consenso distribuito, venne vista da alcuni come uno strumento che consentisse di andare oltre il mondo delle crypto-valute e portare ad una nuova rivoluzione tecnologica al pari di Internet

Gli script in Bitcoin

- Nella prima lezione, abbiamo visto come un UTXO può essere «speso» solo dal possessore della chiave privata, corrispondente all'indirizzo pubblico a cui l'UTXO stesso è associato.
- Tuttavia questo è solo un caso semplice delle condizioni con cui un UTXO può essere speso.
- Allargando la definizione di «spesa» di un UTXO: ogni UTXO può essere speso da ogni transazione (successiva) che fornisce un set di input che soddisfano un insieme di condizioni, specificate nella transazione che ha generato l'UTXO stesso
- Questo insieme di condizioni è noto come «Script». Uno script quindi non è nient'altro che un insieme di regole che vincolano la spesa di un certo UTXO.
- Gli script in Bitcoin vengono «specificati» utilizzando un linguaggio simile ad un linguaggio di programmazione

Limiti dello scripting

- Nonostante lo «scripting» di Bitcoin rappresenta il primo esempio di applicazione della blockchain e delle reti decentralizzate per garantire che un insieme di regole vengano soddisfatte, il linguaggio e l'implementazione dello stesso presentavano dei limiti
- Il linguaggio con cui gli script Bitcoin vengono «specificati» è infatti un linguaggio di tipo «non-Turing complete», ovvero non permettono di descrivere formalmente qualsiasi algoritmo

Limiti dello scripting

- Nonostante lo «scripting» di Bitcoin rappresenta il primo esempio di applicazione della blockchain e delle reti decentralizzate per garantire che un insieme di regole vengano soddisfatte, il linguaggio e l'implementazione dello stesso presentavano dei limiti
- Il linguaggio con cui gli script Bitcoin vengono «specificati» è infatti un linguaggio di tipo «non-Touring complete», ovvero non permettono di descrivere formalmente qualsiasi algoritmo
- Gli UTXO sono di per se indivisibili, pertanto sarebbe inefficiente implementare dei meccanismi che ne prevedano una spesa frazionata (value blindness) (es. spesa di un UTXO in maniera frazionata nel tempo)

Ethereum

- Il progetto Ethereum è stato proposto da Vitalik Buterin nel 2013
- Il progetto venne subito supportato da un sostenuto gruppo di sviluppatori che collaborarono al suo sviluppo dal 2014 al 30 Luglio 2015, data in cui venne rilasciata la «main-net» e venne effettivamente minato il primo «blocco»
- Ethereum nasce con l'ambizione di superare i limiti dello scripting su Bitcoin, al fine di creare un infrastruttura globale e decentralizzata che possa essere usata come un «computer globale» sul quale sviluppare ed eseguire le così dette «applicazioni decentralizzate» (Dapps)
- Ad oggi la rete Ethereum è il secondo più grande eco-sistema blockchain, dopo Bitcoin.
- La crypto-valuta utilizzata nella rete Ethereum e denominata Ether è la seconda crypto-valuta per capitalizzazione di mercato, dopo Bitcoin

La Ethereum-Virtual-Machine

- Uno dei componenti tecnologici chiave introdotti dal progetto Ethereum è la così detta Ethereum-Virtual-Machine (EVM)
- La EVM è un «ambiente di esecuzione virtuale» che, per semplificare, può essere immaginato come in «calcolatore» virtuale
- Come ogni computer «fisico», la EVM è in grado di «capire» ed eseguire una serie di «istruzioni macchina», che possono essere combinate in maniera sequenziale per eseguire una determinata funzione o un programma

La Ethereum-Virtual-Machine

- Immaginando la EVM come una CPU virtuale, possiamo assimilare la blockchain di Ethereum ad un sistema di storage virtuale (es. «hard-disk») distribuito all'interno del quale la EVM può leggere e scrivere dati
- Avendo quindi a disposizione un ambiente di esecuzione (EVM) ed una memoria (Blockchain) è possibile progettare dei programmi che siano in grado di leggere/scrivere/elaborare un certo insieme di dati per implementare un qualsiasi algoritmo
- Così come il nostro PC, quando in funzione, consuma energia elettrica per eseguire un determinato programma, anche la EVM durante la sua esecuzione «consuma» una certa quantità di energia virtuale, chiamata «gas»

Ethereum ed il concetto di «stato»

- In un «normale» calcolatore, ogni volta che una o più istruzioni macchina vengono eseguite il suo «stato» interno cambia
- In primissima approssimazione, quando un calcolatore «fisico» è in esecuzione, il suo stato è rappresentato da:
 - L'indirizzo in memoria della prossima istruzione da eseguire
 - L'insieme di tutte le informazioni contenute all'interno della memoria
 - Il «codice» ed i parametri dell'istruzione attualmente in esecuzione

Ethereum ed il concetto di «stato»

- Allo stesso modo, anche la EVM utilizza il concetto di «stato»
- In Ethereum lo stato è composto da oggetti chiamati «accounts», ognuno di essi identificato mediante un indirizzo di 20-bytes
- Ogni account è caratterizzato dalle seguenti proprietà:
 - Nonce: un contatore utilizzato per conteggiare il numero di «cambiamenti di stato» di un account all'altro, e garantire che una singola transizione venga processata una volta soltanto (più dettagli a seguire)
 - Bilancio: numero di Ether a disposizione del singolo account
 - Contract-code (più dettagli successivamente)
 - Storage: una sorta di spazio di memoria aggiuntivo relativo al singolo account
- La blockchain è utilizzata per memorizzare SOLO le transizioni di uno o più account da uno stato ad un altro

Ethereum ed il concetto di «stato»

- In generale Ethereum prevede l'esistenza di due tipologie di accounts:
 - Gli accounts «posseduti dall'esterno» (Externally-Owned-Accounts, EOA), che sono accounts «controllati» da chiavi private nello stesso modo in cui avviene per gli indirizzi bitcoin
 - Gli accounts di «contratto»: i quali sono «agenti autonomi» paragonabili ad un qualsiasi programma informatico. Il comportamento di questi account è regolato infatti dal «codice» con cui sono stati programmati (una serie di istruzioni macchina della EVM)

Le transazioni in Ethereum

- Se in Bitcoin le transazioni possono essere viste come un trasferimento di valore da un indirizzo all'altro, esse in Ethereum assumono un significato diverso e più generale
- In Ethereum infatti, una transazione può essere vista come un «messaggio firmato» inviato ad un altro account
- Ogni qual volta che un account invia un messaggio ad un altro account, causa inevitabilmente almeno un cambiamento nel suo stato ed eventualmente anche un cambiamento nello stato del ricevente

Le transazioni in Ethereum

- Gli EOA possono inviare messaggi (verso altri EOA o «contratti») creando e firmando delle transazioni (in modo molto simile a ciò che avviene in Bitcoin)
- Gli account di tipo «contratto» sono account che generalmente sono in «attesa di messaggi». Ogni qual volta essi ricevono un messaggio, il loro codice si «attiva» per svolgere una determinata funzione, coerente con la sua programmazione

Le transazioni in Ethereum

- Ogni transazione (o messaggio) in Ethereum contiene le seguenti informazioni:
 - L'indirizzo dell'account destinatario
 - La «firma digitale» del mittente
 - La quantità di Ether da trasferire al destinatario
 - Un campo dati (opzionale)
 - Due valori START-GAS e GASPRICE (più dettagli in seguito)

Gli Smart-Contracts

- Gli account di tipo «contratto», anche noti come «Smart-Contracts», sono quindi dei programmi il cui codice è scritto all'interno della blockchain
- In generale ognuno di questi programmi può implementare una funzione qualsiasi
- Le funzioni di uno Smart-Contracts sono «attivate» ogni volta che l'indirizzo corrispondente riceve un messaggio corrispondente ad uno specifico formato ed eventualmente avente un determinato set di input (specificati nel campo «dati» della transazione)

Gli Smart-Contracts

- Ogni qual volta che un pezzo di codice di un «contratto» viene eseguito, il mittente del messaggio che ne ha attivato l'esecuzione viene consumata una certa quantità di «gas»
- Il «gas» rappresenta quindi il carburante che viene utilizzato dalla Ethereum-Virtual-Machine per eseguire il codice dei contratti
- L'esecuzione «effettiva» del codice degli Smart-Contracts avviene durante la fase di «mining» in Ethereum

Il mining Ethereum

- In Ethereum l'algoritmo di consenso o di «mining» funziona in maniera molto simile a quello di Bitcoin, ma ha alcune differenze:
 - Lo scopo dell'algoritmo è quello di raggiungere un «consenso» distribuito sullo stato di tutti gli account, piuttosto che sulla loro «contabilità» come avviene per Bitcoin
 - Durante la fase di «chiusura del blocco», oltre alla verifica delle firme di ogni transazione e del «bilancio» di ogni account, il miner esegue localmente (sul suo calcolatore) tutto il codice degli Smart-Contracts che sono stati attivati dalle transazioni contenute nel blocco
- Come ricompensa per il lavoro svolto, il miner riceve una certa quantità di Ether «nuovi di zecca» e tutto il totale delle «gas fees» (commissioni di transazione) contenute nel blocco

Il modello del «gas»

- Ogni qual volta viene inviata una transazione verso un account di tipo contratto, devono essere specificati due parametri (oltre alla firma, l'indirizzo ed i dati):
 - START-GAS: rappresenta il massimo numero di unità di «gas» che l'esecuzione della transazione (e quindi del codice del contratto) può impiegare
 - GAS-PRICE: il prezzo (in Ether) che l'utente è disposto a pagare per ogni singola unità di «gas» utilizzata
- Per ogni transazione in Ethereum viene quindi pagata una commissione detta gas fee, ed uguale al prodotto del GAS-PRICE per il totale del gas effettivamente «consumato» durante l'esecuzione della transazione

Il modello del «gas»

- Il modello del «gas» in Ethereum ha due scopi:
 - Remunerare i miner che eseguono il codice dei contratti, rendendo possibile lo sviluppo delle così dette applicazioni decentralizzate
 - Evitare attacchi o comportamenti di tipo Denial-Of-Service. Infatti un modello in cui il costo computazionale non esisterebbe alcune applicazioni o utilizzatori potrebbero «approfittare» della potenza di calcolo messa a disposizione intasando la rete e rendendola inutilizzabile per altri
- Nonostante l'applicazione di questo modello, l'esplosione dell'utilizzo dell'infrastruttura Ethereum per applicazioni decentralizzate ha contribuito ad un esplosione dei costi necessari al suo utilizzo (una transazione semplice, ad oggi, tra i 20 ed i 50 \$ con il cambio attuale ETH/USD)

CRYPTOVERSE: Un tuffo nella tana del bianconiglio

Ing. Jacopo Grecuccio

6

Outline

- Le applicazioni di Ethereum
- I tokens
- Il 2017 ed il fenomeno ICO
- Le Stablecoins

Le applicazioni decentralizzate

- Un Dapp è un software, o insieme di software, in grado di essere accessibile ed eseguibile all'interno di una rete decentralizzata, che sfrutta la tecnologia blockchain come «base di dati» per memorizzare lo stato dell'applicazione e le informazioni interne ad essa legate
- Il progetto Ethereum è stata la prima infrastruttura funzionante che ha consentito la diffusione di questo tipo di applicazioni
- Gli impieghi delle Dapp oggi spaziano su svariati campi: dalla tokenizzazione, finanza decentralizzata, tracciabilità delle filiere, disintermediazione nei sistemi bancari, applicazioni assicurative, Web 3.0 ecc

I tokens

- Una prima applicazione degli Smart-Contracts e delle Dapp in generale fu l'implementazione dei così detti «token»
- Un «token», in linea di principio, è assimilabile ad un gettone posseduto da un certo account
- La generazione, la gestione ed il trasferimento di tokens è regolato dagli Smart-Contracts
- Un token si differenzia da una crypto-valuta (Bitcoin, Ether, ecc) per due aspetti principali:
 - I token non vengono generati durante il processo di mining
 - La blockchain non mantiene la contabilità dei token in maniera «diretta», ovvero la blockchain è di per se agnostica della loro esistenza. I token possono infatti essere visti come uno dei dati «custoditi» all'interno dello stato di un account. Solo lo Smart-Contract che ha generato il token specifico è in grado di «riconoscere» quel dato e stabilire la «contabilità» di un certo account

I tokens

- Esistono diverse tipologie «standard» di token, che si differenziano per il loro tipo di utilizzo.
- I token ERC-20 sono simili a dei «gettoni», tutti uguali tra loro, e vengono spesso utilizzati per rappresentare in modo digitale una serie di «oggetti» tutti uguali ed indistinguibili tra loro. Questo tipo di token hanno una supply-limitata e definita nella fase di «programmazione» dello Smart-Contract che li gestisce

I tokens

- I token ERC-721 sono invece simili a delle «carte collezionabili», ovvero ciascun token è diverso dagli altri oppure può avere al massimo una quantità predefinita di «copie identiche». Questi token, detti Non-Fungible-Tokens, rappresentano il «trend» del 2021 nel mondo crypto e sono attualmente utilizzati per «tokenizzare» opere d'arte fisiche, opere d'arte digitali, altri dati multimediali digitali, ecc
- Visto l'interesse attorno al mondo NFT, approfondiremo questo argomento ed i loro utilizzi nella prossima lezione

2017: l'esplosione delle ICO

- Nel 2017, in pieno periodo di bull-run per Bitcoin, i tokens vennero utilizzati per dare vita a dei sistemi di «crowdfunding» nel mondo crypto
- Molti progetti nascenti mettevano a disposizione di potenziali investitori un certo quantitativo di tokens (legati al loro progetto) in cambio di un finanziamento in denaro
- Questi token potevano dare diritto agli investitori, che diventavano token-holders, a dei vantaggi nell'utilizzo o dei dividendi sui ricavi una volta che il progetto sarebbe effettivamente stato realizzato e rilasciato sul mercato

2017: l'esplosione delle ICO

- Il «fiume» di denaro che in quel periodo veniva riversato all'interno del mercato crypto, creò in breve tempo uno scenario fertile per speculazioni finanziarie e truffe, trasformando di fatto le Initial-Coin-Offering in una delle note più negative associate al mondo crypto
- Alcuni token, vittime di speculazioni finanziarie (a volte anche deliberatamente innescate dai promotori del progetto stesso), subivano aumenti del prezzo dell'ordine di grandezza del 20x, 100x ed in pochi giorni potevano anche perdere il doppio di tutto il valore guadagnato
- Altri token invece si basavano su truffe e venivano rilasciati sul mercato con il solo scopo di raccogliere più denaro possibile, per poi «scappare con il bottino» senza mai di fatto realizzare il progetto

Le Stablecoins

- Le stable-coins, sono dei token «ancorati» ad una specifica valuta o asset fisico (dollaro, oro)
- Gli Smart-Contracts e gli organismi di governance che ne regolano l'emissione fanno sì che la domanda e l'offerta sul mercato siano sempre bilanciate in maniera tale che il cambio con l'asset fisico di riferimento sia sempre 1:1 (o comunque estremamente vicino)
- Le stable-coins sono utilizzate principalmente come valute di scambio sugli Exchanges sia centralizzati che Decentralizzati ed hanno rappresentato uno strumento fondamentale per la creazione degli attuali meccanismi di finanza decentralizzata nel mondo dell crypto-valute

Thether USD (USDT)

- Thether USD (USDT) è la stable-coin attualmente più capitalizzata del mondo crypto, e con i volumi di scambio più alti su tutti gli Exchanges
- Il suo valore di mercato è ancorato al valore del dollaro statunitense, per cui su tutti gli exchanges $1 \text{ USD} = 1 \text{ USDT}$ (a meno di lievi fluttuazioni)
- Ogni USDT in circolazione corrisponde ad un dollaro custodito nelle riserve dell'azienda Thether Operations, responsabile della governance e del mantenimento dello sviluppo del token

USD Coin (USDC)

- Anche USD Coin (USDC) è una stable coin «ancorata» al dollaro statunitense ed è sviluppata e governata dall'azienda Circle, che ne detiene anche le riserve in oro corrispondenti
- Insieme a USDT è la stable-coin più utilizzata sugli exchanges e non solo