Oltre i Bitcoin: il Web 3.0

Relatore: Lucio Crusca

Linux Day 2017
Software Libero Pinerolo
https://softwareliberopinerolo.org

Agenda

- Bitcoin
  - La blockchain
  - Raggiungere il consenso
  - Evoluzione del mining
  - Limiti tecnologici
- Ethereum
  - Dalla valuta al software: Smart Contracts
  - Ecosostenibilità
  - Il Web 3.0

Bitcoin – La blockchain

- Moneta
  - Strumento di pagamento
  - Unità di misura del valore dei beni
  - Le fiat hanno non valore intrinseco
  - Permettono però di acquistare beni
  - Sono di fatto un numero presso una banca
  - Io non mi fido di chiunque, ma mi fido della banca
  - Lo stesso vale per gli altri

Bitcoin – La blockchain

- Alice e Bob si fidano reciprocamente
- Alice ha 100 monete fiat, Bob ne ha 70
- Il PC di Alice memorizza il suo saldo e quello di Bob
- Il PC di Bob memorizza il suo saldo e quello di Alice
- Alice vende a Bob un bene che costa 20 monete
- I due PC salvano la transazione
- I due PC aggiornano i rispettivi wallet (120, 50)
- Alice e Bob non hanno più bisogno di una banca

Bitcoin - La blockchain

- Carol vuole acquistare da Bob
- Alice e Bob non si fidano di Carol
- Si affidano tutti e tre ad David, notoriamente onesto
- David non è una banca: è un algoritmo
- Alice, Bob e Carol installano il software che implementa “David”, cioè Bitcoin
- La blockchain è l’insieme di transazioni
- La crittografia permette l’anonimato dei wallet
- wallet anonimo ≠ proprietario anonimo

Bitcoin – Il consenso

- E se Eve modifica il software sul suo PC?
- Alice, Bob e Carol sono d’accordo sulla blockchain
- Eve sostiene che le transazioni siano differenti
- Eve è in minoranza e viene esclusa
- Ogni transazione ha un costo computazionale alto
- Anche quelle false
- Non conviene fare i furbi
- È possibile raggiungere il consenso solo fra onesti

Bitcoin – I limiti tecnologici

- La blockchain contiene solo transazioni
- Calcolare una transazione è faticoso per il PC
- Computer veloci, progettati ad hoc e costosi (ASIC)
- Serve molta energia elettrica
- Conviene solo a chi può fare economia di scala
- Il mining è appannaggio di pochi
- La rete esiste grazie a pochi privati facoltosi
- La moneta stessa è in mano a pochi

Ethereum

- Stesso principio della blockchain di Bitcoin
- Non contiene transazioni, ma “cose da fare”
- Le “cose da fare” si chiamano “Smart Contracts”
- È una blockchain programmabile
- Il linguaggio di programmazione è Turing Completo
- Si chiama Solidity, con il quale si fanno dApp
- L’esecuzione delle dApp è distribuita su tutti i nodi

Smart Contracts

- L’esecuzione richiede molta memoria RAM
- Controproducente produrre ASIC
- Una scheda video decente costa meno
- Qualsiasi PC può diventare un nodo della rete
- La rete non è più in mano a pochi facoltosi
- L’esecuzione ha comunque un costo
- La valuta Ether serve a pagare l’esecuzione
- L’unità di misura di tale costo è il “gas”

Il Web 3.0

- Le dApp non possono essere interrotte
- I risultati delle dApp non possono essere censurati
- L’unico modo è censurare l’intera rete
- Censura non realistica per nazioni democratiche
- Esistono già dApp per “passare alla storia”
- Molte altre devono ancora essere sviluppate
- Lo sviluppo delle dApp avviene per crowdfunding
- Il contributo non è a fondo perduto
- Si acquistano token (o coin) dello sviluppatore (ICO)

Il Web 3.0

- I token possono essere rivenduti
- Il costo dei token è controllato dal mercato
- I token possono essere usati per eseguire la dApp
- La valuta è sempre l’Ether
- I token sono essi stessi moneta di scambio
- Simili alle azioni
- Non danno la proprietà sulla società emittente

Il Web 3.0

- Esempio: Horizon State
- È una dApp che serve a votare online
- I voti espressi non sono modificabili, né censurabili
- Sono anonimi, allo stesso modo dei wallet
- Sono verificabili, grazie alla crittografia
- Sono unici, sempre grazie alla crittografia

Il Web 3.0

- Votare costa token, i token costano Ether
- Gli Ether forniscono il gas per conteggiare i voti
- I token possono essere acquistati da uno stato
- E ceduti agli aventi diritto di voto
- Oppure acquistati da SLiP
- E ceduti ai soci per votare il prossimo direttivo
- Cambia solo la quantità, quindi il costo totale
- Il cittadino vota comunque gratis
- Lo stato risparmia e i brogli sono impossibili

Il Web 3.0

- Altre dApp possono essere l’equivalente della PEC
- Un blog non censurabile
- Una testata giornalistica non censurabile
- Un social network non censurabile
- Un motore di ricerca assolutamente imparziale
- Un browser… no quello esiste già...
- ...ed è sufficiente per usare il Web 3.0

Il Web 3.0 oggi

- Esistono diversi software per il wallet
- MetaMask è probabilmente il più semplice
- Avere un wallet non significa essere un nodo
- Gli Ether si acquistano pagando in valuta
- Gli Ether si acquistano presso un Exchange
- Rinkeby Test Network per provare gratis
- Esistono wallet hardware (Ledger)
- Gli Ether si possono rivendere e convertire in valuta

Ecosostenibilità

- La rete Ethereum richiede potenza di calcolo
- I miners consumano energia in cambio di numeri
- Come può essere ecocompatibile?
  - Di per sé non lo lo è, né mira ad esserlo
- Si evolverà verso consumi sempre minori (PoS)
  - Byzantium è il primo passo (16/10/2017)
- Ethereum non è un prodotto fine a sé stesso
- Le dApp faranno risparmiare energia
- Le dApp permetteranno controlli ora irrealizzabili

Ecosostenibilità

- Immaginiamo una dApp per pannelli solari (BCDC ?)
- Posso produrre energia e venderla al vicino di casa
- La transazione può essere automatica...
- … e controllata dinamicamente dalla dApp
  - Quando il vicino ha bisogno di energia, la dApp seleziona per lui il pannello solare più vicino al momento non usato dal proprietario, ed acquista da lì l'energia
- Non serve più trasferire l'energia alla centrale
- Si minimizza lo spreco
- Potrebbe non servire più neppure la centrale...

Il Web 3.0 domani

- Farà sparire l’attuale Web 2.0? No...
- … così come oggi il Web degli anni 90 esiste ancora
- Farà sparire Google? No...
- … così come oggi lycos.com esiste ancora
- Farà sparire Facebook? No…
- … così come oggi Usenet esiste ancora
- Sarà davvero Ethereum?
- Fra 5 anni lo sapremo

Riferimenti

- https://it.wikipedia.org/wiki/Ethereum
- https://www.ethereum.org
- Perché Ethereum sta superando Bitcoin: https://venturebeat.com/2017/06/11/why-ethereum-is-outpacing-bitcoin/
- Perché chiamano Ethereum il Web 3.0: https://www.reddit.com/r/ethereum/comments/68b9y3/why_is_ethereum_beimg_called_web_30/
- dApps directory: https://www.stateofthedapps.com/
- Horizon State: https://horizonstate.com/
- The Immortals: https://www.stateofthedapps.com/dapps/the-immortals
- BCDC: https://www.bcdc.online/

Ieri Bitcoin, oggi Ethereum, domani il Web 3.0