Dipartimento di Matematica e Informatica
Università degli Studi di Cagliari

BLOCKCHAIN PUBBLICHE E PERMISSIONED: STATO DELL'ARTE E SVILUPPI RECENTI

Michele Marchesi

marchesi@unica.it

Blockchain permissioned, DEFI e loro applicazioni

Online, 24 Febbraio 2021

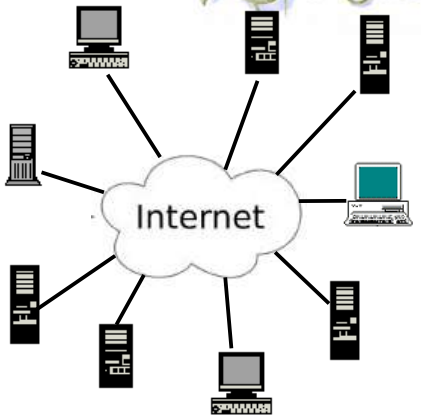
La blockchain: breve storia

- ✓ 2008-2009: Bitcoin, una moneta digitale:
  - basata su Internet
  - ***pubblica***: chiunque può parteciparvi
  - senza un'autorità centrale: funziona anche senza dare fiducia a tutti i partecipanti
- ✓ 2014-2015: Ethereum:
  - gli Smart Contract: **programmi eseguiti sulla blockchain**
  - la blockchain diviene un **calcolatore universale**
- ✓ 2015: Hyperledger:
  - la blockchain può essere usata anche privatamente
  - blockchain ***permissioned*** a invito
  - DLT: digital ledger technology

Le basi matematiche e informatiche

- ✓ Le basi matematiche (crittografiche) della tecnologia blockchain e DLT sono:
  - la crittografia asimmetrica: *il possesso della chiave privata **dimostra la proprietà** della chiave pubblica associata, e dell'**address** da questa ricavato*
  - le proprietà delle funzioni “hash”: *l'impronta digitale (“hash”) di un documento è unica, e cambia completamente anche dopo minime modifiche*
- ✓ Le basi informatiche sono:
  - la rete Internet: *senza Internet, la DLT non avrebbe senso!*
  - l'architettura peer-to-peer: *i nodi (computer) governano la rete in modo **decentralizzato***
  - il software open source: *chiunque può scaricare e usare il software di nodo, e collegarsi a una blockchain pubblica, o con altri attivarne una permissioned*

L'architettura informatica



- ✓ Una rete di nodi, composti da:
  - computer con adeguata potenza, RAM e disco,
  - collegati a Internet, con adeguata banda,
  - con software di gestione, tipicamente open source.
- ✓ La rete è P2P: nessun nodo la governa
- ✓ Nelle blockchain *permissioned* l'accesso può essere governato a livello di permessi di sistema
- ✓ Chiunque (autorizzato) può inviare *transazioni* e/o *query* alla blockchain, inviandole a un nodo qualunque

E' facile violare la crittografia?

- ✓ Bitcoin usa chiavi e impronte a 256 bit (circa 77 cifre decimali)
- ✓ L'unico modo noto per violarle è **provare tutte le combinazioni** sino a trovare quella giusta
- ✓ In linea di principio, la crittografia assimmetrica potrebbe **forse** essere violata da **computer quantistici**. Tuttavia:
  - Se fosse violata, cadrebbero tutte le applicazioni Internet in sicurezza (password, e-banking, firma digitale, ecc.)
  - Esistono nuovi algoritmi quantum-resistant

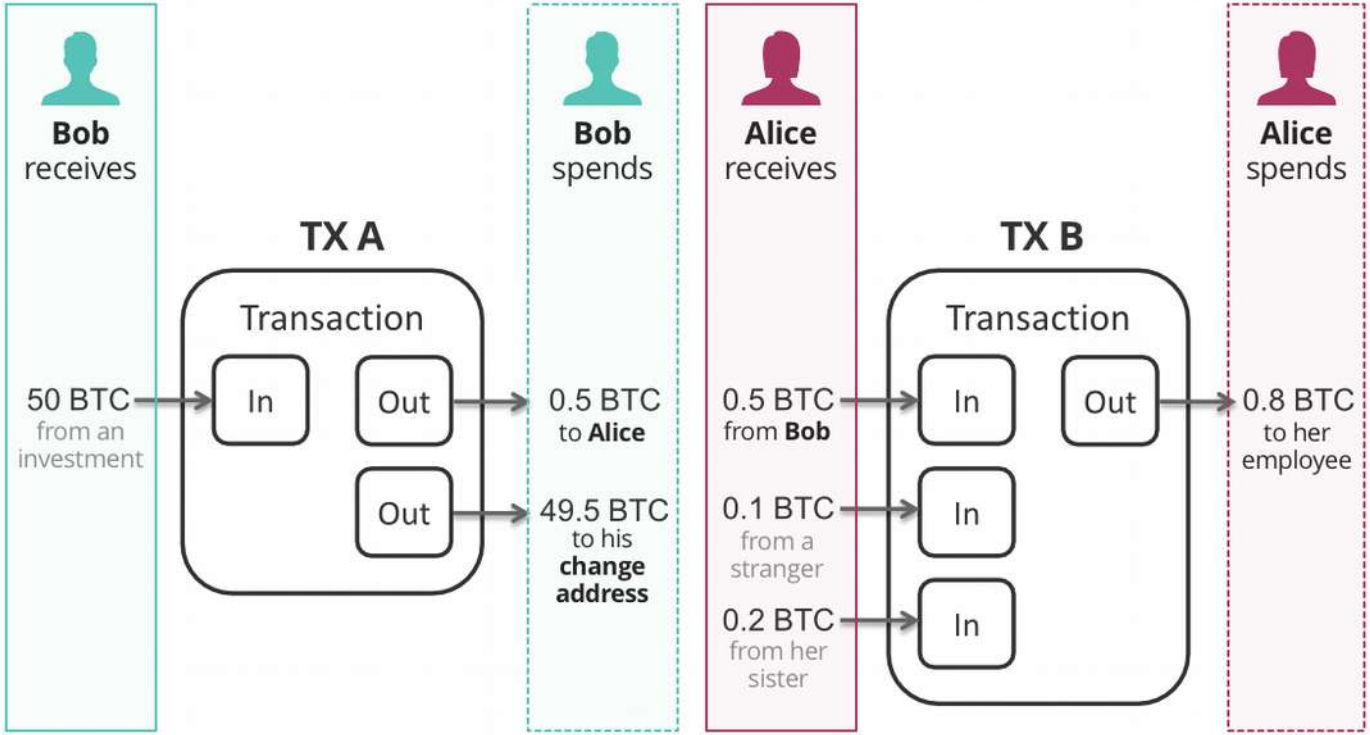
Violare la crittografia per tentativi (approccio *a forza bruta*)

- ✓ Poniamo di avere un sistema con **1000 CPU** in **ogni metro quadrato** delle terre emerse (150 milioni di Km2), capaci ciascuno di fare **mille miliardi** di tentativi al secondo.
- ✓ Il numero di computazioni **pari all'età della terra** (circa 10 miliardi di anni) richieste per provare tutti i numeri di 77 cifre è di circa 10 seguito da 30 zeri!
- ✓ Se avessimo un tale sistema di calcolo **per ogni stella di tutte le galassie conosciute** (mille miliardi di galassie, ciascuna con mille milardi di stelle), la probabilità di trovare la chiave in 10 miliardi di anni sarebbe ancora di circa **uno su un milione!**

L'idea originale

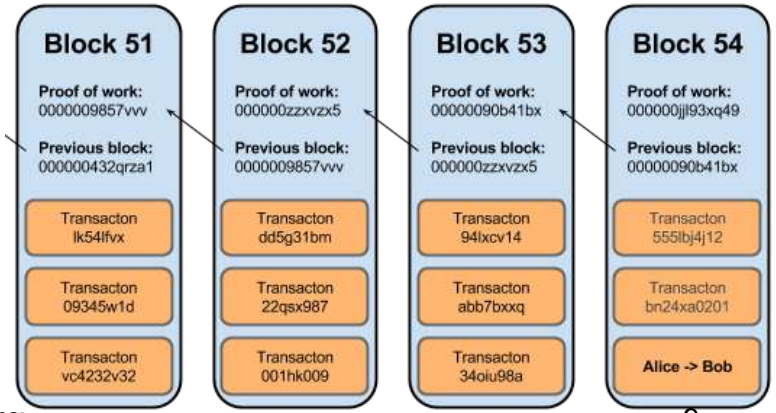
- ✓ La moneta è una registrazione in un registro pubblico (Blockchain), condiviso su Internet da migliaia di nodi e gestito in modo peer to peer
  - Chiunque può collegarsi alla rete con un nuovo nodo, usando software open source
- ✓ I trasferimenti di moneta (transazioni) sono comunicati alla rete P2P dai nodi
- ✓ Ogni trasferimento di moneta ha un **indirizzo pubblico** (derivato da una chiave crittografica pubblica):
  - tutti sanno quanta moneta è stata trasferita a un dato indirizzo
- ✓ Il proprietario, anonimo, possiede la chiave privata associata
  - Solo usando tale chiave privata si può trasferire (**una sola volta!**) la moneta verso un altro indirizzo pubblico, in modo **irrevocabile**

Indirizzi e transazioni



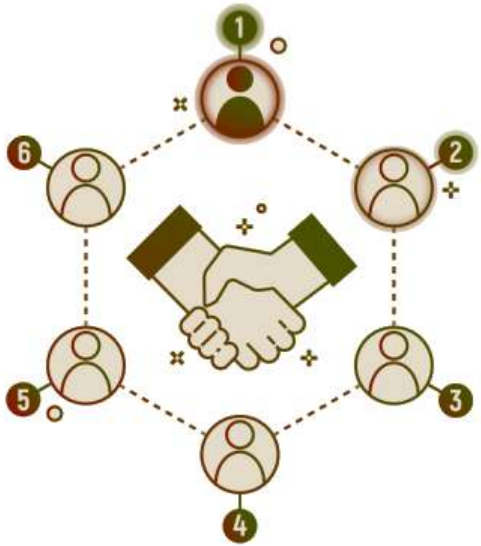
Transazioni e blocchi

- ✓ Le transazioni sono validate, aggregate in blocchi e registrate nella Blockchain
- ✓ La Blockchain è struttura “append only”, composta da una sequenza di blocchi, in cui ogni blocco contiene l’impronta hash del blocco precedente
  - In tal modo, la modifica a un blocco provocherebbe la modifica a catena di tutti i blocchi successivi, e ciò dà l'immutabilità
  - In DLT non blockchain, l'immutabilità delle transazioni è comunque garantita con altri mezzi
- ✓ Ogni nodo può inviare transazioni, quindi occorre un **meccanismo di consenso** per accettare le transazioni valide e inserirle nel DL
- ✓ Nelle blockchain pubbliche si usano tecniche di consenso complesse, lente e di costo volatile
- ✓ Nei DLT permissioned non ci sono questi problemi



Il problema del consenso

- ✓ **Ogni nodo** può creare e trasmettere transazioni verso la rete dei nodi
- ✓ Occorre che qualcuno **verifichi le transazioni**, crei i nuovi blocchi e li inserisca nella blockchain
- ✓ **I miner** fanno questo, gareggiando tra loro a risolvere un problema crittografico
- ✓ **Chiunque** può fare il miner (almeno in linea di principio)



L'attacco “Sybil”

- Se il sistema permette a chiunque di collegarsi anonimamente, un attaccante potrebbe eseguire un “Sybil Attack” (dal libro “Sybil”, sul disturbo dell’identità dissociativo, DID):
  - Genera molte identità differenti (anche migliaia o milioni)
  - Le collega tutte alla rete e ne prende il controllo

Proof of Work (PoW)

- ✓ L’attacco Sybil si evita rendendo **computazionalmente costoso** il lavoro di validazione dei blocchi
- ✓ Per validare un blocco, bisogna **“dimostrare di aver fatto del lavoro”** (PoW)
- ✓ In tal modo, mentre i miner “onesti” spendono qualcosa ma hanno la prospettiva di guadagnare di più, **un attacco massiccio costerebbe troppo**
- ✓ Sinora il sistema ha dimostrato di funzionare!

La creazione di valuta

- ✓ Il primo miner che riesce a validare il blocco corrente, lo inserisce nella Blockchain e guadagna una quantità fissata di criptovaluta, che in BTC si dimezza ogni quattro anni
- ✓ Tutti i nodi accettano il blocco validato, smettono di computare su di esso, e passano al blocco successivo
- ✓ In tal modo, si risolvono tre problemi:
  - L'attacco Sybil
  - La remunerazione del mining:
    critica nelle blockchain pubbliche!
  - La messa graduale in circolazione di nuova valuta

La rete dei miner

- ✓ Già nel 2014 la potenza di hash della rete Bitcoin era 300 volte superiore a quella di tutti i primi 500 supercomputer
- ✓ Il consumo attuale è di circa 8,5 GW: più della Svizzera, e meno del consumo degli asciugabiancheria in USA
- ✓ Il costo totale dell'hardware per il mining di Bitcoin è dell'ordine di 5-10 miliardi di US$
- ✓ Questo uso di risorse è la maggior debolezza dei Bitcoin
- ✓ Però, i miner si localizzano dove è disponibile energia a basso costo, che deve essere comunque consumata anche se non c'è un compratore
- ✓ Inoltre, man mano che il compenso in BTC dei miner diminuisce, il "punto di equilibrio" relativo al costo dell'energia diminuisce

Una mining farm moderna

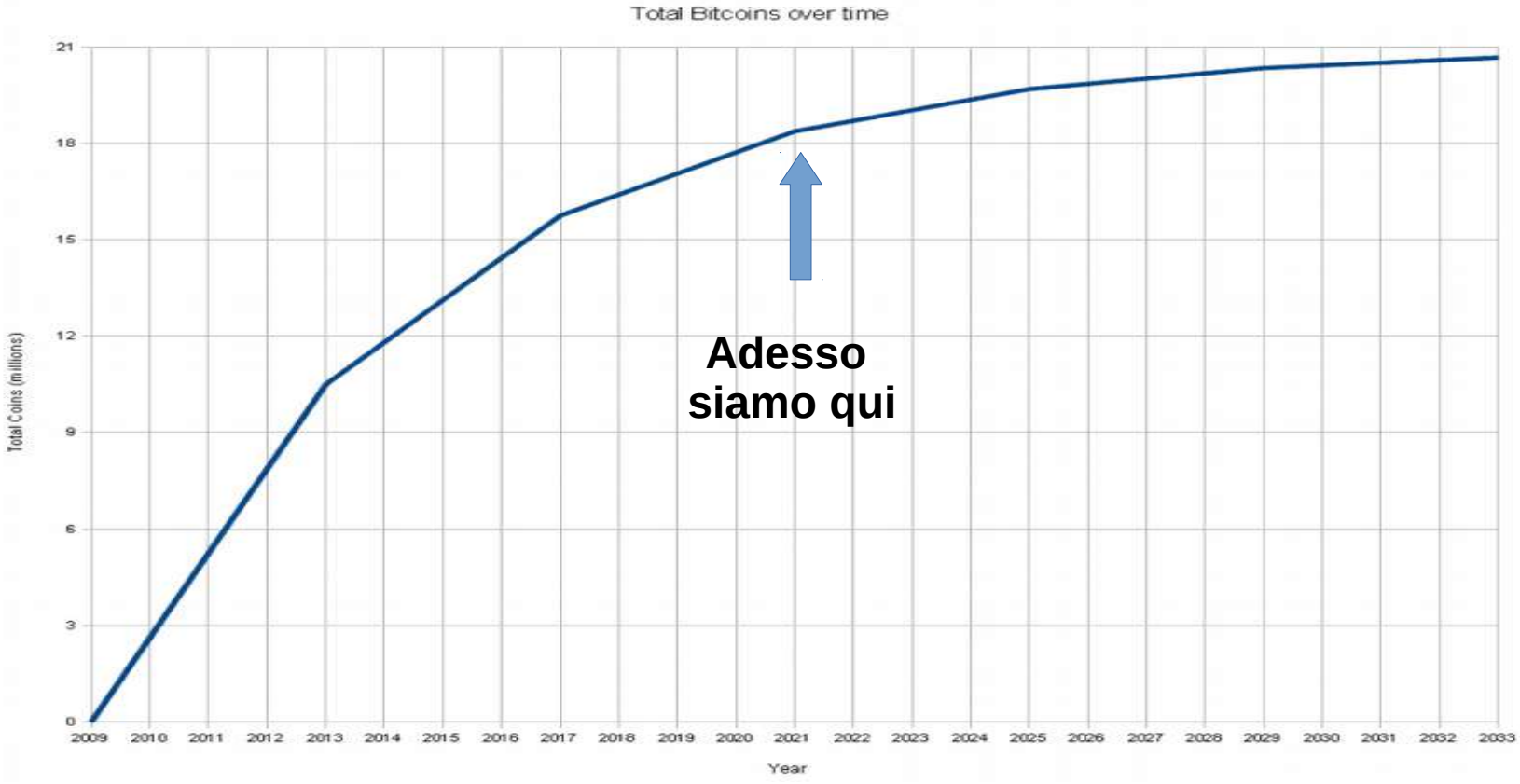
Bitcoin: un po’ di storia

- ✓ Nel gennaio 2009 Satoshi Nakamoto, pseudonimo di una persona o di un gruppo tuttora ignoto dà inizio alla rete P2P dei Bitcoin!
- ✓ All'inizio è un gioco crittografico, ma dopo poco, si inizia a dare un valore reale al Bitcoin
- ✓ Bitcoin inizia ad avere un valore:
  - Il 12/10/2009 sono comprati 5.050 BTC per 5,02 US$.
  - Maggio 2010: non trovano acquirenti di 10.000 BTC per 50 US$.
  - Il 22/5/2010 Laszlo Hanyecz compra due pizze della catena “Papa John's”, del valore di circa 25 US$, per 10.000 BTC.
  - Fast Forward: oggi un Bitcoin vale circa 50.000 US$!

Bitcoin: qualche numero al 02/2021

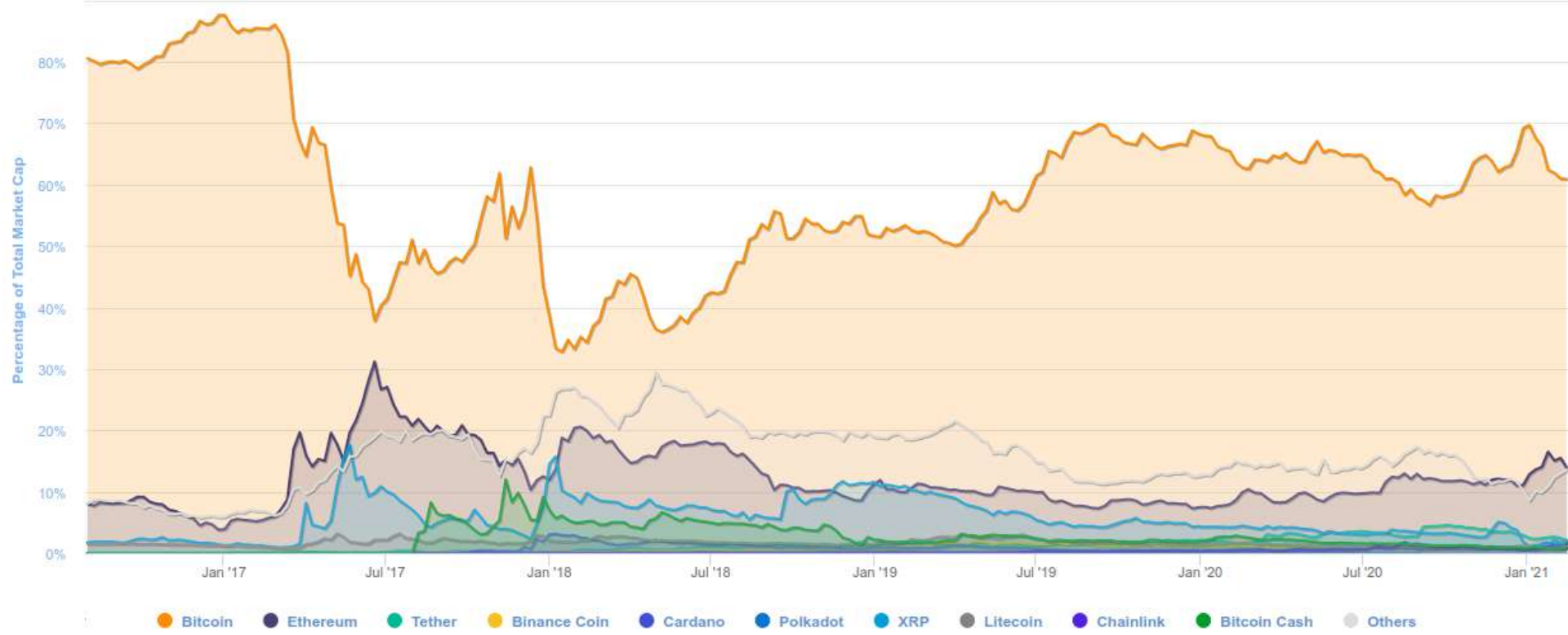
- Numero max. di transazioni per blocco: circa 2000, ogni 10’
- Transazioni giornaliere: circa 330.000
- BTC effettivamente scambiati ogni giorno: circa 150.000
- Dimensione della Blockchain: circa 670.000 blocchi, per circa 330 Gbyte

Numero totale di Bitcoin (milioni)

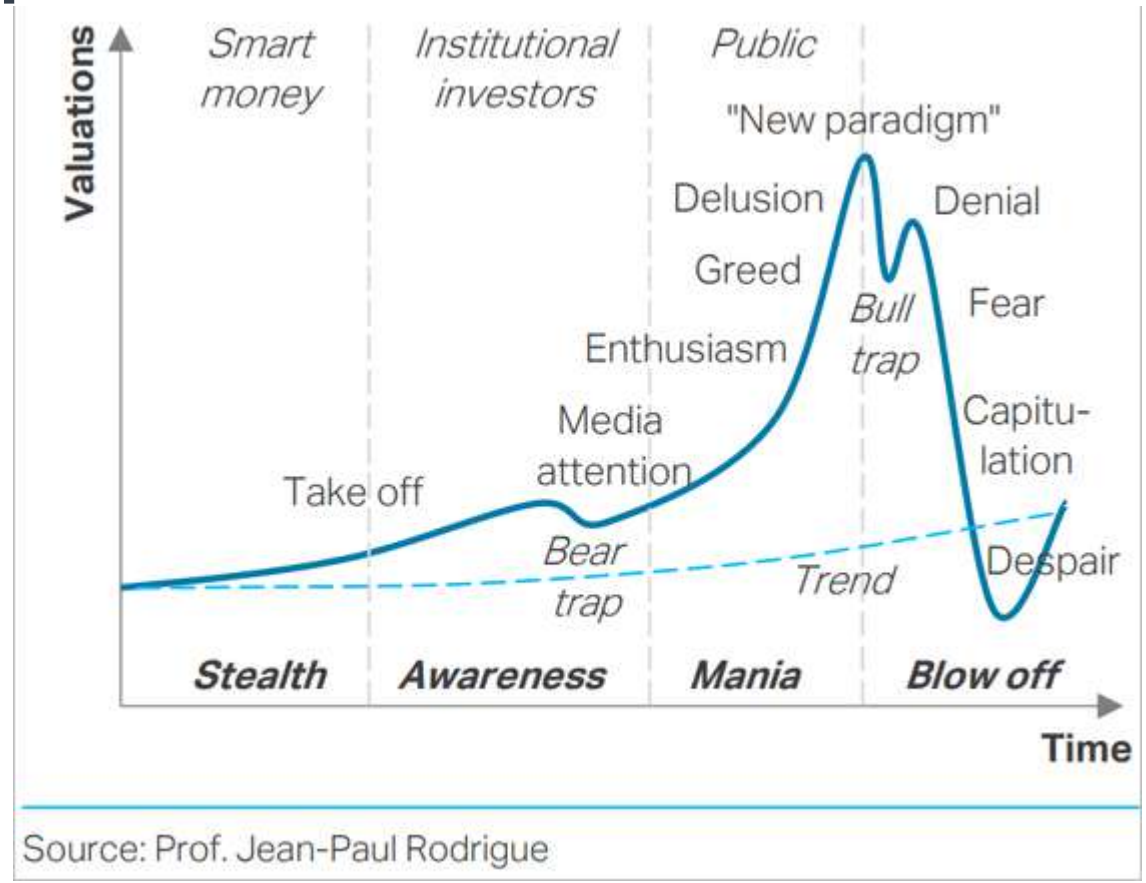


Bitcoin: prezzo in US$

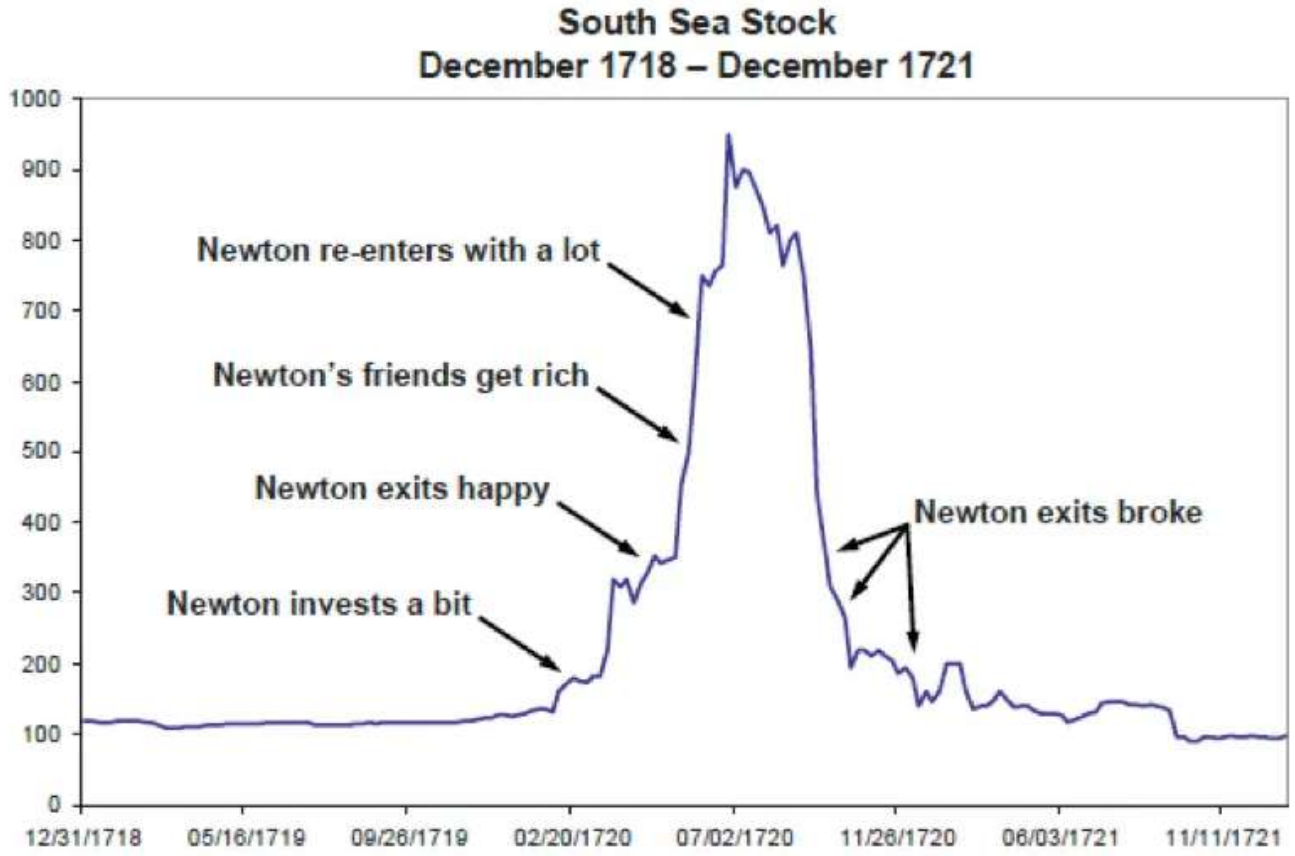
Bitcoin: capitalizzazione relativa



Il tipico ciclo di una “bolla”



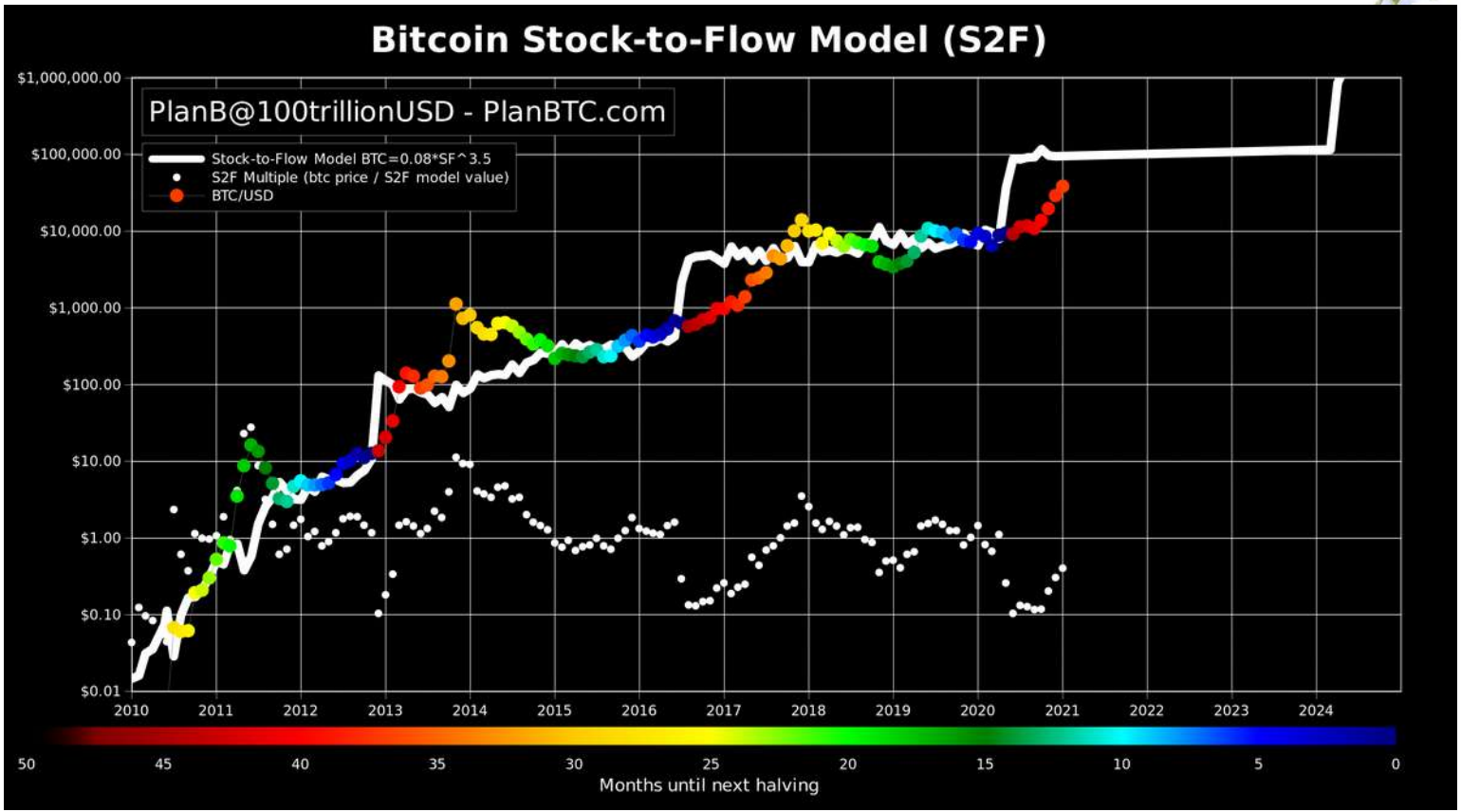
La bolla della “South Sea” e Newton



Bitcoin e criptovalute: sono una bolla?

- **Lo sono:**
  - Il BTC e le criptovalute **non hanno valore intrisico** (create dal nulla)
  - Non sono garantite da uno Stato o da una grande banca
  - Hanno crescite e cali da “bolla”
- **Non lo sono:**
  - **Hanno quantità limitata e rendimento zero**: non c'è effetto “Ponzi” (pagamento del rendimento con le quote dei nuovi entrati)
  - Non si basano su promesse di rendita futura (come South Sea)
  - Stanno entrando i grossi investitori

Bitcoin: modello stock-to-flow



Le 3 fasi di Bitcoin

- **Fase iniziale: sperimentazioni tra pochi “nerd”:**
  - la rete funziona e genera BTC
  - il valore è zero, ma piano piano aumenta
  - l'uso per scambiare beni e servizi è minimo
  - Questa fase è durata sino a circa il 2011

2 fase: Oro Digitale

- E’ la fase attuale
- Il valore dei BTC aumenta fortemente (ma poi precipita e poi si riprende...)
- Le persone comprano BTC per arricchirsi
- L'uso di scambio è ancora ridotto, ma crescente
- Fenomeno degli HODLER: “HODL” – “Hold on for dear life”
- Estrema volatilità!!

3 fase: Vera moneta

- I BTC sono sempre più usati per pagare beni e servizi
- Il prezzo si stabilizza
- Siamo ancora lontani da questa fase:
  forse non ci arriveremo mai!
- Bitcoin non scala bene in termini di numero di transazioni
- Soluzione: transazioni off-chain (Lightning Network)

Criticità di Bitcoin

- Numero di transazioni per secondo molto basso: 3-4
- Dimensione della blockchain, che cresce sempre
- Concentrazione della potenza di mining in poche mani
- Concentrazione dei BTC: poche entità (***whales***) possiedono grandi quantità di BTC e possono speculare facilmente, senza controllo
- Il sistema è pensato solo per la gestione della valuta digitale

Chi è Satoshi Nakamoto?

- **Fatti:**
  - Satoshi Nakamoto (a dx.) è veramente un giapponese esperto di crittografia che vive negli USA, ma non ha nulla a che vedere col Bitcoin!
  - Satoshi Nakamoto (pseudonimo) ha pubblicato il “white paper” nel 2008 e nel 2009 ha fatto partire la rete Bitcoin
  - Ha detto di vivere in Giappone e di avere 37 anni
  - L’ora dei suoi post indica piuttosto la costa Ovest USA
  - Scrive in ottimo inglese
  - E molto probabile che abbia fatto il miner di oltre un milione di BTC, i cui address sono noti e non sono mai stati spesi
  - Gli ultimi messaggi risalgono a fine 2010, poi è scomparso

Chi è Satoshi Nakamoto? L'ipotesi Finney

- **Fatti:**
  - Hal Finney, nato nel 1956, è stato un grande esperto di crittografia, creatore insieme a Phil Zimmermann del PGP
  - Nel 2004 ha creato il primo sistema di PoW riusabile
  - E' stato coinvolto nel progetto Bitcoin sin dall'inizio
  - Ha effettuato la prima transazione di BTC con Nakamoto
  - Ha vissuto per vari anni vicino al Satoshi Nakamoto della pagina precedente, e probabilmente lo conosceva
  - Ha negato di essere SN, ma appunto SN è un'identità creata per preservare l'anonimità del vero autore di Bitcoin!
  - Nell'ottobre 2009 gli fu diagnosticata la SLA e nNel marzo 2013 era quasi totalmente paralizzato
  - E' morto il 28 agosto 2014

Chi è Satoshi Nakamoto? L'ipotesi Finney

- **Deduzioni:**
  - Hal Finney è sempre stato considerato tra i primi candidati a essere Satoshi Nakamoto
  - Finney:
    - Molto probabilmente conosceva un vero Satoshi Nakamoto
    - Ha mantenuto funzionante la rete BTC all'inizio
    - Ha iniziato a stare molto male proprio quando SN è scomparso (e se era veramente SN, non avrebbe più potuto mantenere il segreto)

  - Conclusione: ***La probabilità che Finney fosse Satoshi Nakamoto è piuttosto alta!***

Chi è Satoshi Nakamoto? L'ipotesi Wright

- Craig Steven Wright è un informatico australiano
- Si è occupato di Bitcoin molto presto, fondando nel 2011 con Dave Kleiman la W&K Info Defense Research LLC per effettuare mining e sviluppo sw su Bitcoin
- Nel 2015, *Wired* e *Gizmodo* conducono due inchieste parallele, sostenendo che Wright è Satoshi Nakamoto
- Nel 2016 Wright proclama di essere Satoshi, ma poi rinuncia a provarlo
- Wright fornisce la chiave di un address di SN, che però sembra essere un riuso di una chiave nota del 2009
- Nel 2017, insieme a Roger Ver, promuove un "Hard fork" ostile di Bitcoin, dando vita a "Bitcoin Cash" (BCH) e il gruppo cerca senza successo di far crollare il prezzo di BTC rispetto a BCH, per farlo diventare il "vero" Bitcoin
- Nel Novembre 2018 si separa da BCH, creando con un fork "Bitcoin Satoshi Value" (BSV)
- Nel 2019 dice che Bitcoin è stato un progetto da lui diretto, insieme a Finney e Kleiman
- Craig Wright è certamente stato coinvolto nel progetto Bitcoin sin dai primi tempi
- ***Nell'ambiente dei Bitcoiners è però scarsamento considerato: non esistono reali prove che sia Satoshi!***

Chi è Satoshi Nakamoto? L'ipotesi Le Roux

- **Fatti:**
  - Paul Solotshi Calder Le Roux è un informatico e criminale rodesiano
  - Nato nel 1972 e abbandonato dai genitori, è stato adottato a due anni dalla famiglia Le Roux, scappata dopo la cacciata dei bianchi dalla Rhodesia
  - Si interessa di programmazione, dimostrando grandi abilità
  - A 16 anni è arrestato per aver veduto materiale pornografico illegale
  - Si occupa di crittografia e sviluppa nel 1998 il programma E4M/TrueCrypt per gestire unità a disco crittografate virtuali su Windows e Linux
  - Nel 2004, fonda vari siti Web e call center per vendere medicinali online; è un'attività borderline che gli frutta molti soldi
  - Nel 2007 si "diversifica" nel traffico di armi e droga
  - E' a capo di una grande organizzazione, ben partizionata e occultata
  - Organizza l'omicidio di vari membri che lo avevano truffato o tradito

Chi è Satoshi Nakamoto? L'ipotesi Le Roux

- **Fatti:**
  - E' arrestato nel settembre 2012: è tuttora in carcere negli USA
  - Sembra che Craig Wright abbia chiesto protezione da Le Roux, perché teme di essere ucciso
- **Deduzioni:**
  - La curiosa somiglianza: Satoshi / Solotshi
  - Entrambi programmatori C++ ed esperti di crittografia e privacy
  - Entrambi diffidenti nei confronti dell'autorità
  - Entrambi consapevoli delle difficoltà con i sistemi di pagamento tradizionali, Le Roux a causa del suo racket di droga
  - Satoshi è scomparso all'inizio del 2011 per "passare ad altre cose", nel periodo in cui Le Roux stava passando da genio del software a capo a tempo pieno di una gang
  - ***La probabilità che SN sia Le Roux è comunque alquanto bassa!***

Chi è Satoshi Nakamoto? L'ipotesi Kleiman

- **Fatti:**
  - Dave Kleiman è stato un grande esperto di analisi forensi informatiche
  - Nato nel 1967 e adottato dai coniugi Kleiman, si arruola come tecnico nell'esercito USA, poi entra nella Polizia di Palm Beach
  - Nel 1995 resta paralizzato a causa di un incidente di moto
  - Si dedica a tempo pieno alle analisi forensi informatiche e viene considerato uno dei principali esperti mondiali, nonostante sia un autodidatta
  - Scrive libri, e scrive nelle mailing list di crittografia usate poi anche da SN
  - E' amico e co-autore di paper scientifici con Craig Steven Wright, con cui fonda nel 2011 la W&K Info Defense Research LLC
  - Viene ricoverato in ospedale nel 2010 per un'infezione da stafilococco resistente agli antibiotici, e lascierà l'ospedale solo per brevi periodi

Chi è Satoshi Nakamoto? L'ipotesi Kleiman

- **Fatti:**
  - Nel 2013 lascia l'ospedale e va a vivere da solo in condizioni da "barbone"
  - Muore in povertà il 26 aprile 2013; l'autopsia confermerebbe la morte naturale
- **Deduzioni:**
  - Era nel "giro" dei crittografi che collaborarono all'ideazione di Bitcoin nella mailing list Metzdowd di sicurezza informatica
  - Era molto focalizzato su privacy e sicurezza e teneva sempre con sé una chiavetta USB ad alta sicurezza
  - Aveva il profilo e le competenze giuste per essere SN
  - E' stato ricoverato in ospedale proprio quando SN è scomparso (e non avrebbe più potuto mantenere il segreto)
  - Recentemente, Ira Kleiman, fratello di Dave Kleiman, ha citato in giudizio Wright per la metà dei presunti Bitcoin di SN, del valore di 5 miliardi di dollari.
  - Conclusione: ***La probabilità che Kleiman fosse Satoshi Nakamoto è piuttosto alta!***

Chi è Satoshi Nakamoto?

Hal Finney?

Dave Kleiman?

Craig Wright?

Paul Le Roux?

Qualcun altro?

- ***Se uno scrittore avesse creato la trama per un giallo, non avrebbe potuto far meglio!***

Tornando alla blockchain, riassumendo:

- ✓ DLT, inclusa la blockchain, è un registro pubblico di tutte le transazioni, reso immutabile usando le funzioni hash
- ✓ Non è soggetta a un'autorità centrale
- ✓ E' replicata su tutti i nodi di una rete P2P, ed è un “database” cui si può solo appendere informazione, ma non cancellarla: le transazioni sono irrevocabili e non alterabili
- ✓ Riceve in continuazione nuove transazioni, validate tramite crittografia asimmetrica
- ✓ Gli utenti sono identificati da un address, a sua volta ricavato da una chiave pubblica, la cui chiave privata è posseduta solo dall’utente ed è sicura
- ✓ La blockchain richiede un meccanismo di consenso per decidere quali transazioni e quali blocchi sono accettati
- ✓ **E' in sostanza un meccanismo per ingenerare fiducia, senza dover dare fiducia a tutti i nodi, o a un gestore centralizzato!**

Caratteristiche chiave delle blockchain

- ✓ **Distribuzione**: le informazioni sono memorizzate su più nodi, dando resilienza e sicurezza
- ✓ **Tracciabilità**: tutte le transazioni sono tracciabili in ogni parte, e se ne può conoscere con certezza la provenienza
- ✓ **Decentralizzazione**: le transazioni sono gestite senza un'autorità centrale di gestione
- ✓ **Trasparenza**: i contenuti sono accessibili e verificabili da tutti
- ✓ **Immutabilità**: i dati accettati non sono più modificabili in alcun modo
- ✓ **Programmabilità**: si possono programmare azioni complesse (Smart Contracts), anch'esse totalmente verificabili
- ✓ **Low-cost**: open source, poca manutenzione e costi di gestione bassi

Utilizzo delle blockchain *pubbliche*

- ✓ Uso principale: **gestione di criptovalute**
- ✓ Registrazione di informazioni **immutabili e con data certa**:
  - informazione **limitata**, ma può essere l'hash di un documento di dimensioni qualsiasi
  - chiunque potrà poi accedere a questa informazione
  - utilizzabile anche per "ancoraggio" periodico di "sidechain" e altri database
- ✓ Esecuzione di **Smart Contracts** (per lo più gestiscono **token DeFi**):
  - gestione dei Token: criptovalute di secondo livello, e dei Decentralized Exchange (DEX)
  - applicazioni di gioco, scommesse, certificazione di proprietà e di provenienza, ...
- ✓ Massimo livello di immutabilità e autorevolezza, e quindi di **fiducia**
- ✓ **Nessun costo di infrastruttura**, ma **costi di utilizzo non predicibili**
- ✓ Tempi di risposta lenti, problemi di scalabilità

Costo medio di una transazione (US$)

Le blockchain *permissioned*

- ✓ DLT gestiti da un numero ridotto di **organizzazioni interessate**
  - Devono comunque essere gestiti da una rete di nodi:
    DLT con un solo gestore sono ridicole!
  - Per essere credibili, devono avere almeno 7-10 nodi **indipendenti**
  - Così è molto improbabile che possano essere "sequestrate"
- ✓ Gestire un nodo è molto semplice e poco costoso
  - Si usano "motori" di blockchain pubbliche o software open source apposito
  - Richiedono amministrazione della gestione dei permessi di accesso al sistema
  - Gestione dei controlli di esecuzione anche entro gli smart contract

Le blockchain *permissioned*

- ✓ Hanno livelli di accesso graduabili, possono mantenere la riservatezza dei dati e soddisfare i requisiti GDPR
- ✓ Non hanno problemi di velocità, scalabilità e volatilità dei costi: scalano attivando nuove blockchain!
- ✓ Possono però avere problemi di **fiducia**, in dipendenza dalla loro gestione
- ✓ Sono la scelta obbligata di quasi tutte le applicazioni industriali di Dapp, per la loro controllabilità, efficienza e costo

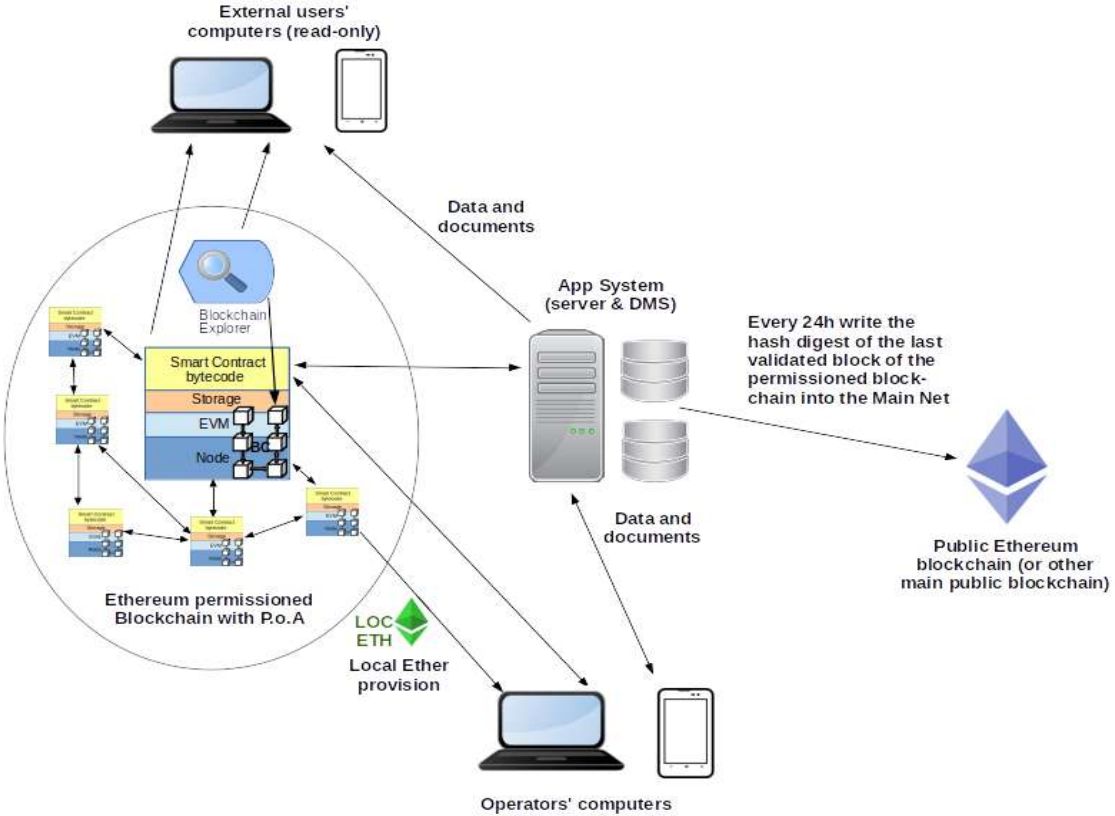
Quando usare una blockchain permissioned?

- ✓ Ha senso utilizzare una blockchain permissioned quando **il sistema di interesse coinvolge più organizzazioni**
- ✓ Però **nessuna di queste, e nessuna organizzazione esterna, può prendersi carico della sua gestione**. Ciò può avvenire:
  - perché nessuno vuole o può gestire il sistema
  - perché alcuni partecipanti non vogliono dare la gestione a uno di essi,
  - per problemi di costo legati all'uso di una blockchain pubblica o di un provider esterno
- ✓ Preliminarmente, è necessario un **contratto chiaro** per determinare obblighi e diritti dei partecipanti, inclusi:
  - tempi e procedure per ritirarsi
  - procedure per la gestione dei nodi e dei permessi di accesso a vari livelli
  - procedure per l'aggiunta e la cancellazione di nuovi nodi

Un'architettura permissioned che dà quasi la stessa fiducia di una blockchain pubblica

- ✓ Una blockchain permissioned, per **avere i vantaggi** di una blockchain pubblica **senza averne gli svantaggi**, dovrebbe avere le seguenti caratteristiche:
  - software gestione nodi open source e diffuso, in modo da trovare facilmente competenze
  - i nodi devono essere **pubblicamente accessibili da Internet**, per offrire servizi, eventualmente previa autenticazione;
  - i tempi di validazione delle transazioni devono essere rapidi (dell'ordine di 1" o meno)
  - l'hash dell'ultimo blocco della blockchain permissioned **viene scritto periodicamente** (ad es. ogni 24 ore) entro una **blockchain pubblica**: in modo da garantire l'inalterabilità di tutte le transazioni effettuate, **con la stessa forza della blockchain pubblica usata**;
  - uno o più nodi **esternamente accessibili** della blockchain permissioned fanno girare un **explorer**, programma che consente a chiunque (eventualmente previa autorizzazione) di esaminarne il contenuto: in tal modo **il livello di trasparenza diviene uguale a quello di una blockchain pubblica**.

L'architettura permissioned con Ethereum, o Hyperledger Besu



La Blockchain come avvocato (gli Smart Contract)

- ✓ Uno Smart Contract è un programma, che gira su un supporto sicuro (trusted) ed è a sua volta trasparente e sicuro
- ✓ Poiché l'esecuzione di un programma software è deterministica e immutabile (a parità di input e di stato), **il codice può essere considerato un contratto**
- ✓ I contraenti **si obbligano ad accettare il risultato delle sue elaborazioni**
- ✓ Su una blockchain, uno Smart Contract prende input da fonti sicure, **identificate dalle firme digitali dei partecipanti**
- ✓ In output:
  - può trasferire token che rappresentano beni o servizi reali
  - può attivare altri contratti
  - può registrare informazioni o collegarsi (indirettamente) a sistemi esterni

La Blockchain come avvocato (gli Smart Contract)

- ✓ Una volta che le clausole contrattuali sono correttamente inserite nel codice di uno Smart Contract, e questo è accettato dai contraenti, gli effetti non sono più legati alla loro volontà o all'azione di intermediari
- ✓ La Blockchain **fornisce tutte le garanzie**, senza la necessità di un'autorità centrale!
- ✓ Il "Decreto Semplificazioni" DL 135/2018, art. 8 ter, pubblicato in G.U. il 12/2/2019 dà esplicitamente valore legale alle registrazioni su registri distribuiti e agli Smart Contract (SC), che "...*soddisfano il requisito della forma scritta previa identificazione informatica delle parti interessate…"*
- ✓ Inoltre, **il codice stesso degli SC è ispezionabile da tutti**, e **garantito immutabile** una volta installato nella blockchain:
  - **questa è una situazione nuova, senza precedenti nell'informatica!**

Usi della Blockchain

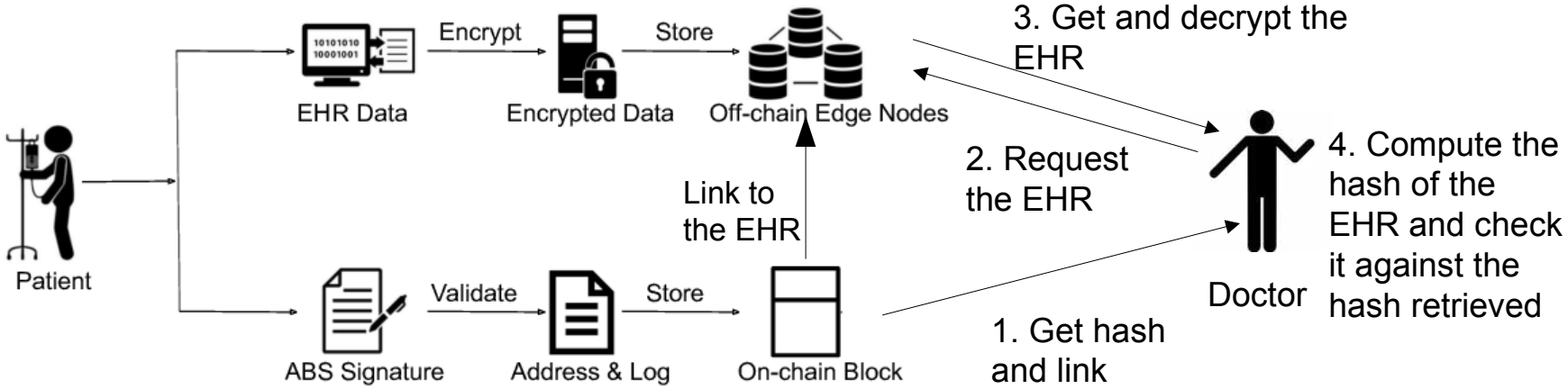
- ✓ Uso principale: gestione di criptovalute
- ✓ Altri usi:
  - Registrazione di informazioni immutabili e con data certa:
    - tale informazione è limitata, ma può essere l'hash di un documento di dimensioni qualsiasi
    - chiunque potrà poi accedere a questa informazione
    - si possono anche "ancorare" periodicamente DLT permissioned
  - Eseguire Smart Contracts (inclusi i Token)

La Blockchain come notaio

- In quasi tutte le Blockchain, è possibile registrare informazioni generiche (sequenze di bit)
- Si possono registrare:
  - direttamente dati (**devono essere pochi**)
  - la **“firma hash”** e il link di documenti mantenuti off-chain
- Una volta accettata in un blocco, l’informazione resta nella Blockchain, **per sempre**
- Strumento di immutabilità e trasparenza di documenti
- Tale notarizzazione ha ormai valore di legge

Notarizzazione di dati sensibili

- ✓ “Off-chain data storage” pattern:



Ancora notarizzazione

- L’assegnazione di data e integrità certa a quantità anche massive di documenti e a costi molto ridotti si può applicare a:
  - Documenti contrattuali e di gestione di una filiera
  - Documenti su cui si voglia rivendicare il diritto d’autore
  - Documenti relativi alla sicurezza sul lavoro
  - Certificazioni di formazione e valutazione di esami e test del personale
  - Log informatici di accesso ai sistemi, e impronte digitali di applicativi software e firmware
- La vera rivoluzione è comunque quella relativa agli Smart Contract e alle loro funzionalita!

15 blockchain trends in 2021: Expect the unexpected

1 Le dimensioni del mercato globale della blockchain cresceranno esponenzialmente

- La tecnologia blockchain è esplosa in popolarità quest'anno. Le aziende di moltissimi settori hanno mostrato un crescente interesse ad adottare questa tecnologia per migliorare i processi aziendali.
- La pandemia COVID-19 ha accelerato la spinta alla trasformazione digitale in molte aree.
- Si prevede che le dimensioni del mercato globale della blockchain aumenteranno da 3,0 miliardi di USD nel 2020 a 39,7 miliardi di USD entro il 2025, con un tasso di crescita annuale composto del 67,3% nel periodo 2020-2025.
- "Si stima che il prossimo anno almeno il 25% di Forbes Global 2000 utilizzerà la blockchain come base per la fiducia digitale su larga scala."

2. Il Covid-19 accelererà la transizione blockchain

- Riorientamento dei vari progetti blockchain.
- Sino al 90% dei progetti blockchain richiederà la sostituzione entro un anno, perché la maggior parte sta ignorando caratteristiche chiave come tokenizzazione, gli SC e il consenso decentralizzato.
- La pandemia ha favorito approcci più realistici e pragmatici alle iniziative blockchain.
- I progetti blockchain con chiari vantaggi dovrebbero procedere il prossimo anno a un ritmo ancora più veloce.
- C'è stato anche un aumento del numero di aziende interessate a partecipare a reti che aiutano specificamente ad affrontare alcuni dei problemi della catena di approvvigionamento che la pandemia ha sollevato.

3. I progetti strategici a lungo termine verranno sospesi

- La volatilità e l'incertezza innescate da COVID-19 hanno portato molte aziende a ritirarsi da alcuni dei loro progetti DLT più a lungo termine.
- Molti altri progetti strategici a lungo termine sono stati rallentati.
- I budget per progetti puramente sperimentali e di ricerca e sviluppo, gestiti separatamente dall'azienda, stanno diventando più difficili da ottenere e quest'anno sono stati tagliati.
- E questo farà sì che un numero ancora maggiore di questi progetti venga sospeso.

4. Le aziende devono accelerare la loro trasformazione digitale

- La trasformazione digitale non è più una scelta per le aziende: è essenziale per la sopravvivenza.
- A causa della maggiore tensione che la pandemia COVID-19 ha imposto sulle attività quotidiane, le aziende hanno un disperato bisogno di accelerare il loro processo di trasformazione digitale per emergere più forti di prima.
- È molto probabile che la tecnologia blockchain apporti i cambiamenti più trasformativi e radicali nel modo in cui funzionano le aziende, negli anni a venire.
- Molte industrie stanno quindi esaminando intensamente la blockchain come uno strumento utile per diventare ancora più digitali.

5. A livello globale, il 30% dei progetti entrerà in produzione.

- Si prevede che un numero crescente di progetti basati su blockchain passerà alla fase di produzione.
- Ciò anche per l'accelerazione indotta dalla pandemia e l'avvio di progetti che possono portare "benefici misurabili in un breve lasso di tempo".
- Secondo Gartner, oltre il 40% delle aziende intervistate ha almeno un progetto pilota di blockchain in esecuzione.
- Prevedono che il 30% dei progetti globali entrerà in produzione, in parte a causa dell'impatto della pandemia COVID-19.
- La maggior parte delle reti che passano dal progetto pilota alla produzione verranno quindi eseguite su piattaforme blockchain aziendali private.

6. Le blockchain private (permissioned) domineranno

- Le blockchain permissioned diventeranno il principale contributore alla crescita del mercato blockchain, e saranno il mercato di maggiori dimensioni nel 2021.
- Le soluzioni blockchain aziendali saranno sviluppate su misura in base alle esigenze di business di un'azienda.
- La blockchain privata offre maggiori opportunità alle aziende in termini di utilizzo della tecnologia blockchain per casi d'uso business-to-business.
- Offrono maggiore efficienza, privacy, affidabilità e trasparenza, mentre la sicurezza viene fornita a una blockchain privata utilizzando chiavi private note solo alle persone autorizzate nell'organizzazione.

7. I progressi più rapidi saranno fatti dalla Cina

- La Cina sta guidando il gioco globale della blockchain e continuerà questo ruolo nel 2021.
- La Blockchain sta portando la Cina a un livello, che è ben oltre quello attuale di altri attori del mercato globale.
- La rete nazionale di servizi basati su Blockchain sostenuta dallo stato, mira a rendere la blockchain parte integrante dell'infrastruttura digitale del paese.
- L'ulteriore ambizione della Cina è fornire un'infrastruttura pubblica globale tramite questa rete.
- Inoltre, mentre altri attori come l'Europa stanno pensando di lanciare la propria valuta digitale, la Cina è quasi pronta per emettere il Crypto Yuan.

8. Il settore bancario e finanziario dominerà il mercato

- Tra tutte le industrie colpite dalla pandemia COVID-19, il settore finanziario è un'area che è stata particolarmente colpita.
- Il calo dei profitti e la contrazione dei margini hanno costretto le banche ad adattarsi e soddisfare sempre più le esigenze dei loro clienti in un mondo digitale in crescita.
- L'adozione della tecnologia fintech e blockchain, consente loro di semplificare e modernizzare le loro operazioni.
- III settore bancario e finanziario dovrebbe mostrare una crescita esponenziale nell'adozione della blockchain nei prossimi anni.
- Di conseguenza, questo settore sarà il più rilevante nel mercato globale della blockchain nei prossimi anni.

9. Crescente offerta di DLT da parte di istituzioni finanziarie non tradizionali

- Un'altra tendenza che vedremo durante il 2021, e innescata anche da COVID-19, sarà l'aumento del numero di istituzioni finanziarie non tradizionali.
- Sarà attivato da un numero crescente di aziende, ma anche di consumatori, che usano transazioni e servizi finanziari online basati su blockchain.
- Questi gruppi hanno parecchie opzioni non bancarie fornite da istituzioni che vanno da istituti di credito non bancari, a banche basate su criptovalute, a servizi finanziari completamente decentralizzati (DEFI).

10. Di grande tendenza: DEFI...

- Accanto a una forte accelerazione nell'accettazione della tokenizzazione, ovvero dell'archiviazione digitale di asset su blockchain, un'altra grande tendenza del 2021 e oltre sarà la DEFI: servizi finanziari decentralizzati.
- Con DEFI, la blockchain potrebbe essere utilizzata per casi d'uso finanziari fino ad ora carenti.
- Questa forma alternativa di finanziamento si inserisce perfettamente nella “fintechizzazione” dell'economia.
- Quest'anno il valore totale dei servizi finanziari decentralizzati (basati su criptovalute) ha registrato una crescita impressionante e ha superato i 10 miliardi di dollari. Si prevede un'ulteriore accelerazione nel 2021 e oltre.

11. … e ZKP (Zero Knowledge Proof)

- Un'altra tendenza importante del 2021 è l'arrivo delle ZKP.
- Le ZKP sono necessarie per affrontare le sfide legate alla privacy che attualmente stanno frenando i progetti blockchain.
- Le ZKP basate su blockchain consentono alle aziende con diversi sistemi di conservazione dei dati di essere "sincronizzate" in modo verificabile record per record senza condividere informazioni sensibili.
- Stanno arrivando sempre più soluzioni per implementare le ZKP.
- La grande sfida rimane tuttavia la complessità: le ZKP sono molto più complesse da sviluppare rispetto alla codifica di uno SC senza privacy, ma per motivi di sicurezza ci si aspetta che le aziende passino dallo sviluppo di DApp allo sviluppo di ZApp.

12. Le criptovalute possono raggiungere nuovi massimi di prezzo

- Il 2020 si è dimostrato un buon anno per tutte lle criptovalute e le aspettative sono che il 2021 sia un anno ancora migliore per Bitcoin e le altre criptovalute.
- Esse sono di interesse per gli investitori che cercano nuovi beni rifugio, per la pandemia COVID-19.
- Essendo largamente insensibile a fattori politici grazie alla sua natura decentralizzata, Bitcoin ha dimostrato di essere una "preziosa forma di oro digitale", qualificandosi come uno dei migliori investimenti mondiali.
- Tuttavia, con l'enorme volatilità dei prezzi delle criptovalute, ci si può aspettare di tutto.

13. Le frodi stanno aumentando

- Sebbene il 2020 sia un ottimo anno per gli investimenti in criptovalute, il rovescio della medaglia è un deciso aumento delle frodi crittografiche.
- Gli scambi globali di criptovalute hanno subito attacchi di alto profilo, mentre gli attacchi verso le società di finanza decentralizzata (DeFi) hanno rappresentato oltre il 20% del volume totale di truffe nel 2020.
- Le aspettative sono che ciò continuerà nel 2021.
- Potremmo vedere vari tipi di frodi, compresi false piattaforme di investimento crittografico, truffe di falsi portafogli crittografici, nuove forme di malware che prendono di mira le criptovalute meno conosciute.

14. Il numero di progetti CBDC aumenterà

- Molte banche centrali in tutto il mondo stanno esplorando il possibile lancio della propria valuta digitale della banca centrale (CBDC).
- Secondo un recente rapporto BRI, l'80% delle banche centrali di tutto il mondo sta studiando i pro e i contro di una simile valuta.
- Questo processo si intensificherà ulteriormente nel 2021, guidato dalla diminuzione dell'uso del contante, dalla digitalizzazione dell'economia, dall'arrivo di valute digitali private come Libra/Diem.
- La Cina ha già eseguito dozzine di esperimenti con cittadini e aziende, ed è pronta per un lancio a livello mondiale.
- La BCE prenderà una decisione sul progetto dell'euro digitale a metà del 2021.

15. I governi vareranno regolamenti più severi su valute digitali e FinTech

- L'ultima tendenza del 2021 e oltre è che i governi intensificheranno la loro ricerca di una regolamentazione sempre più rigorosa.
- La crescente digitalizzazione dell'economia innescata dalla pandemia è un fattore strettamente monitorato dai regolatori di tutto il mondo.
- Il settore bancario digitale, le criptovalute e la blockchain saranno probabilmente i principali soggetti della regolamentazione.
- Poiché un numero crescente di transazioni finanziarie avviene al di fuori dei meccanismi tradizionali, questioni come la DEFI non possono più essere ignorate dalle autorità di regolamentazione.

Alcune fonti

- Prezzi di criptovalute e token: https://coinmarketcap.com/
- Informazioni su cripto e blockchain:
  https://coindesk.com/
  https://cointelegraph.com/
  https://blockchain.news/
- Articolo su Forbes:
  https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50/
- Explorer di Bitcoin: https://explorer.bitcoin.com/btc
- Explorer di Ethereum: https://etherscan.io/
- Sito Agile Group: www.agile-group.org/

Alcune fonti

- Prezzi di criptovalute e token: https://coinmarketcap.com/
- Informazioni su cripto e blockchain:
  https://coindesk.com/
  https://cointelegraph.com/
  https://blockchain.news/
  https://blog.nyctale.io/
- Articolo su Forbes:
  https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50/
- Explorer di Bitcoin: https://explorer.bitcoin.com/btc
- Explorer di Ethereum: https://etherscan.io/
- Sito Agile Group: www.agile-group.org/

Grazie dell'attenzione!

Domande?