Introduzione alla Blockchain e alle Criptovalute

Docente: Gian Luca Comandini

ATENEO IMPRESA

THE BLOCKCHAIN MANAGEMENT SCHOOL

11A EDIZIONE
Master Lab in Blockchain Technology & Management

Modulo I: Storia economica

- Storia della moneta
- Crisi del 2008
- Concetto di Trust
- Cronistoria di Bitcoin

Storia della moneta

- Economia del dono
- 8.000 a.C. – Baratto
- 5.000 a.C. – Pre-moneta (grano, tè, sale, bestiame)
- 2.000 a.C. – Metalli (anelli)
- 1.000 a.C. – Santuari marchiano gli anelli per certificarne valore
- 700 a.C. – Prima moneta in Lidia con Re Creso (elektron)
- 330 a.C. – Re Dario di Persia fa raffigurare il suo volto

11A EDIZIONE
ATENEO IMPRESA

Storia della moneta

- 1200 – Templi e santuari diventano banche (i Templari)
- 1500 – Moneta di carta chiamata «note di banco» (banconote)
- 1800 – Sistema Aureo
- 1950 – Carta di credito (diners)
- 2000 – SisalPay, AmazonPay, ApplePay, ecc
- 2009 – Bitcoin
- 2020 – Central Bank Digital Currency (CBDC)

11A EDIZIONE
ATENEO IMPRESA

Crisi del 2008

EVENTI:

- Grande Depressione (1929)
- Grande Recessione (2008)

CAUSE:

- Politiche FED post-crisi (2001)
- Speculazione finanziaria (2001-2006)
- Crollo immobiliare (2007)
- Mutui subprime (2008)
- Titoli «tossici»
- Malafede agenzie di rating

11A EDIZIONE
ATENEO IMPRESA

Crisi del 2008

- Lehman Brothers accumula 600Mld di debiti
- La più grande bancarotta della storia (26000 dipendenti)
- Molte altre banche falliscono, i PIL di molti paesi crollano
- Dopo oltre 15 anni ancora paghiamo la più grande falla del capitalismo finanziario

11A EDIZIONE
ATENEO IMPRESA

Concetto di Trust

- Fin dal baratto l'Uomo non si è mai fidato
- Nella storia non si è mai risolto il problema della fiducia
- Uno strumento per essere moneta deve avere 3 funzioni:
  - Mezzo di pagamento
  - Unità di conto
  - Riserva di valore
- Differenza tra valore intrinseco/estrinseco

11A EDIZIONE
ATENEO IMPRESA

Concetto di Trust

- 15 settembre 2008 – Lehman Brothers
- 31 ottobre 2008 - Bitcoin

La tecnologia blockchain ed il bitcoin nascono come precisa risposta e reazione alla crisi di fiducia nei confronti delle banche.
Chi l'ha inventata sapeva che avremmo avuto urgentemente bisogno di un nuovo sistema decentralizzato di scambio di valore e fiducia.
Oggi, i sistemi che utilizziamo quotidianamente vanno verso la decentralizzazione (social network, politica, fintech, sanità, ecc.)

11A EDIZIONE
ATENEO IMPRESA

Cronistoria

- 15 settembre 2008 – Crack Lehman Brothers
- 31 ottobre 2008 – «Bitcoin p2p e-cash paper»
- 3 gennaio 2009 – SN lancia Bitcoin. Nel primo blocco, messaggio: «Il Cancelliere sta per salvare per la seconda volta le banche» (titolo del The Times)
- 12 gennaio 2009 – SN invia 10 btc a Hal Finney. Prima transazione al mondo
- 18 maggio 2010 – Pizza day, primo acquisto in bitcoin (10.000btc)
- 12 dicembre 2010 – Assange accetta bitcoin, SN parla di «calcio a nido di vespe»

10A EDIZIONE
ATENEO IMPRESA

Cronistoria

- Febbraio 2011 – 1btc = 1$
- Aprile 2011 – SN sparisce per sempre
- Novembre 2013 – 1btc = 1.000$
- Novembre 2017 – 1btc = 10.000$
- Dicembre 2017 – 1btc = 20.000$
- Febbraio 2021 - 1btc = 50.000$
- Novembre 2021 – 1btc = 69.000$

10A EDIZIONE
ATENEO IMPRESA

Modulo II: Bitcoin

- Chi è Satoshi Nakamoto
- Protocollo Bitcoin
- White Paper Bitcoin

Satoshi Nakamoto

- Una o più persone?
- 31 ottobre 2008: pubblica il primo messaggio (Satoshi's paper)
- Aprile 2011: sparisce nel nulla per dedicarsi a "cose più importanti"
- Ad oggi detiene oltre 1 milione di btc
- Non ha mai usato i suoi btc
- Deve avere competenze in settori quali: informatica, crittografia, economia, ecc...
- Slang britannico/accademico
- Fuso orario americano

Alcune ipotesi

- *Craig Wright*, australiano, da sempre sostiene di essere SN e di averne le prove ma non è mai riuscito a dimostrarlo del tutto. Da molti è considerato un ciarlatano.
- *Dave Kleiman*, un programmatore deceduto nel 2013. Il fratello ha riconosciuto in lui SN e sostiene che Craig Wright abbia rubato il progetto a Dave dopo la morte. È una delle ipotesi più probabili, riconosciuta anche da un tribunale.
- *Cypherpunks*, una comunità di cryptoanarchici. I due esponenti di spicco, Hal *Finney e Nick Szabo* avevano teorizzato Bitcoin molti anni prima e sono vicini di casa del «falso» Satoshi Nakamoto.

Protocollo Bitcoin

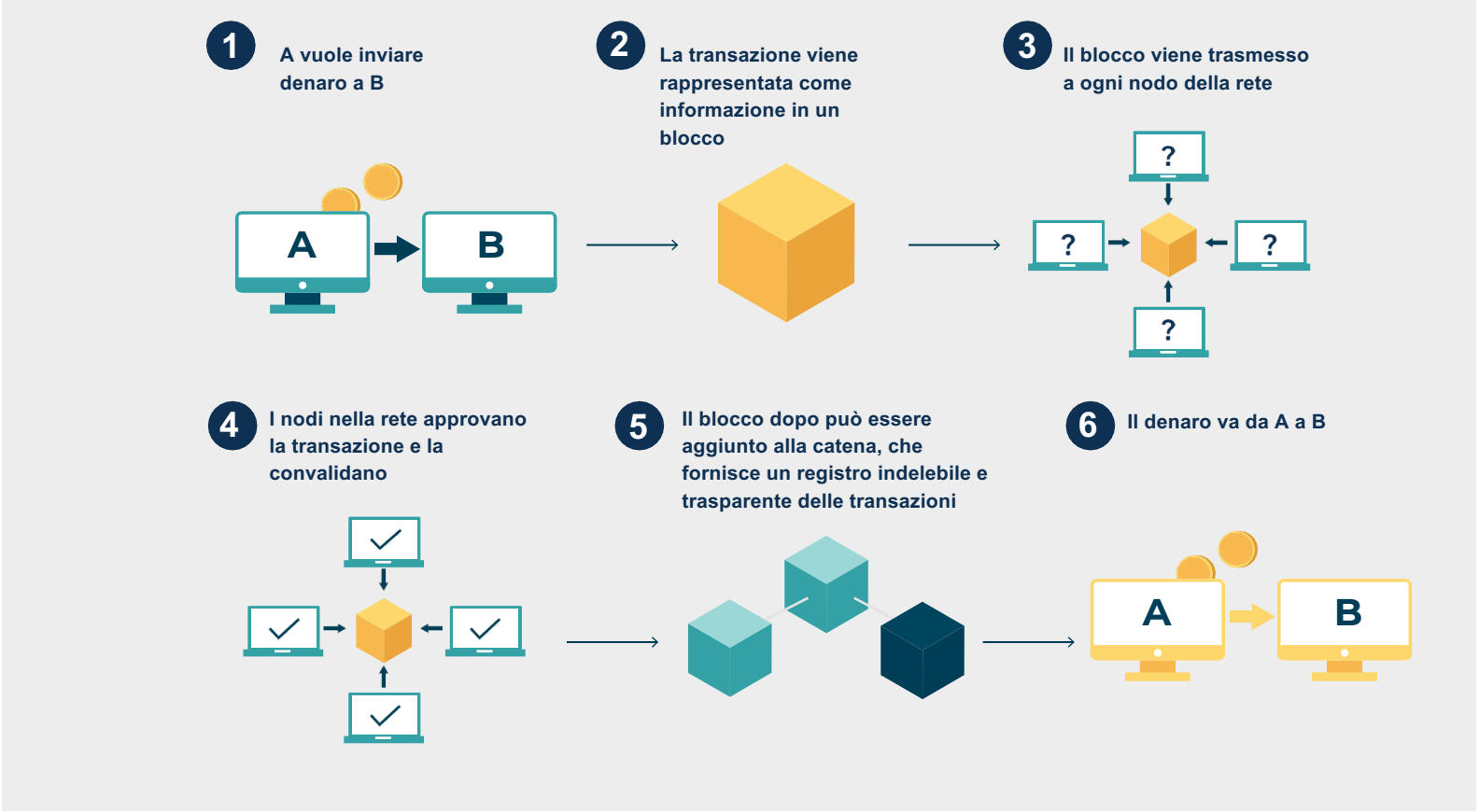
- Il Bitcoin è un protocollo crittografico che permette l'allocazione ed il trasferimento di proprietà di file. Ad oggi questo protocollo viene utilizzato per scambiare principalmente la propria criptovaluta, definita appunto bitcoin.

- Nel 2140 circa, finita l'emissione, sarà una moneta ininflazionabile.

- La moneta bitcoin utilizza la tecnologia Blockchain e sfrutta complessi algoritmi crittografici per gestire gli aspetti funzionali come generazione di moneta e verifica delle transazioni.

11A EDIZIONE
ATENEO IMPRESA

Come funziona Bitcoin?



11A EDIZIONE
ATENEO IMPRESA

Caratteristiche

- Decentralizzazione: indipendente da governi e banche
- Velocità: libertà di pagamento nel tempo e nello spazio
- Proprietà reale: è di chi lo possiede
- Sicurezza: basato su crittografia, impossibile falsificarlo
- Economicità: costi molto bassi
- Deflazione: aumenta di valore nel tempo
- Trasparenza: tracciabile in eterno
- Anti-truffa: no double spending

11A EDIZIONE
ATENEO IMPRESA

Dati

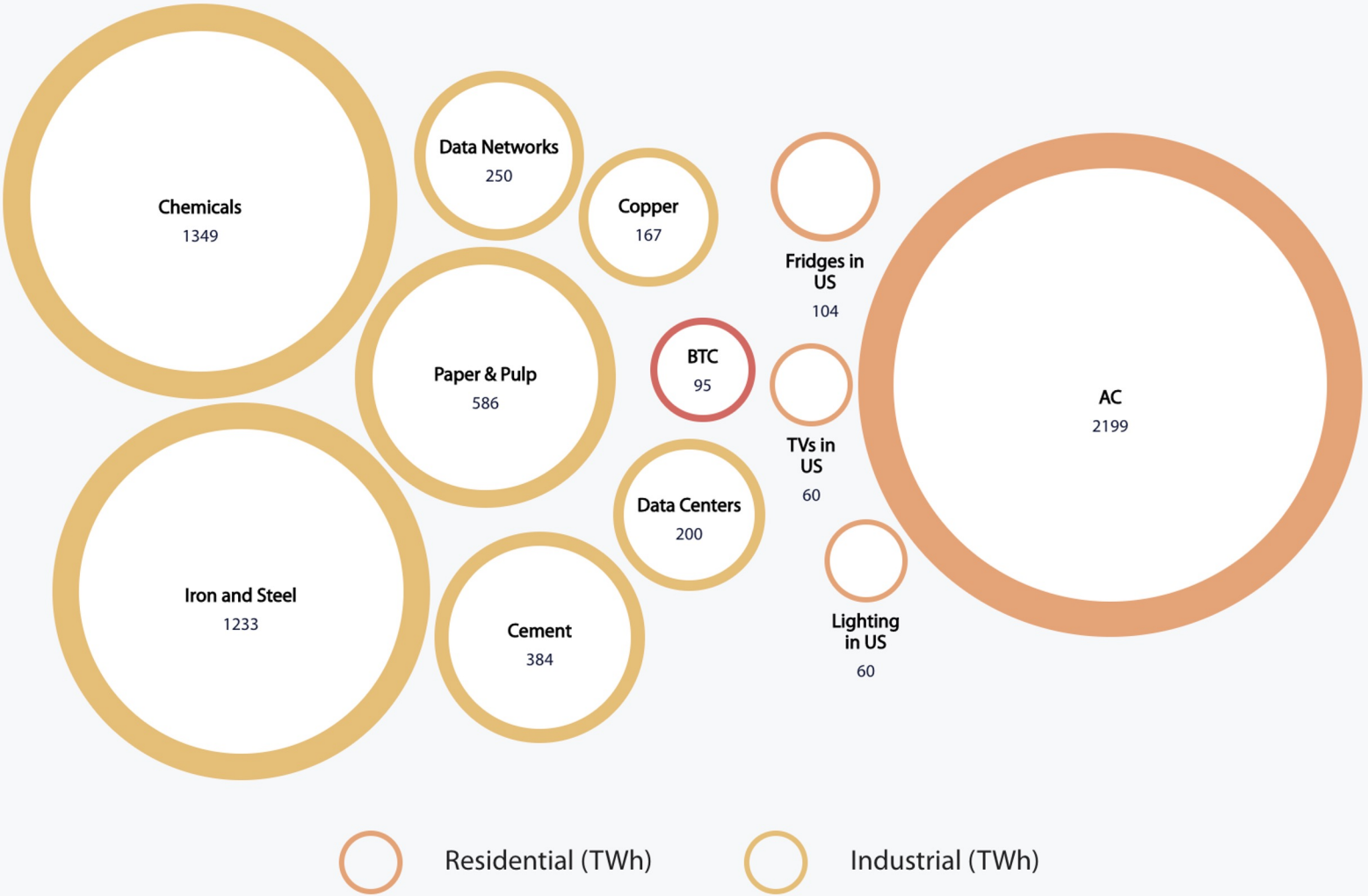
- La potenza computazionale dell'intera rete Bitcoin è 50.000 volte superiore dei 500 supercomputer più potenti al mondo messi insieme
- Potenza di calcolo: 270 Eh/s = 270.000.000.000.000.000.000 di hash al secondo
- Energia consumata: circa 95 TWh - Terawatt/ora, 0,15% del consumo mondiale di energia (Fonte: Cambridge Bitcoin Eletricity Consumption Index: https://ccaf.io/cbeci/index)
- Per il 39% Bitcoin utilizza energie rinnovabili

11A EDIZIONE
ATENEO IMPRESA

Dati

- Bitcoin in circolazione oggi: +19,3 Milioni
- Capitalizzazione di mercato: +400 mld
- Transazioni giornaliere: +250 mila
- Indirizzi unici usati: +600 mila
- Nel 1995 gli investimenti Internet furono 150 Mln, oggi gli investimenti in blockchain sono oltre 15 MLD
- 1/5 di tutti i bitcoin sono persi per sempre

11A EDIZIONE
ATENEO IMPRESA



11A EDIZIONE
ATENEO IMPRESA

Belgium

83.4

TWh per year

Finland

83.7

TWh per year

Bitcoin

95.4

TWh per year

Kazakhstan

96.6

TWh per year

Philippines

98.5

TWh per year

11A EDIZIONE

ATENEO IMPRESA

Mining

- Il Mining ha 3 ruoli fondamentali per il funzionamento di Bitcoin:
  1. Verifica le transazioni e convalida i blocchi
  2. Raccoglie le fee delle transazioni
  3. Evita la doppia spesa
- È un sistema distribuito di consensi sulle avvenute transazioni
- I miners competono per ottenere la ricompensa in bitcoin inviando alla rete una prova (proof of work) della risoluzione del difficile problema di calcolo
- Un altro miner deve accettare la proof of work, viene così inserito il blocco e la catena prosegue
- Il livello di difficoltà aumenta e diminuisce per validare un blocco ogni 10 minuti circa

11A EDIZIONE
ATENEO IMPRESA

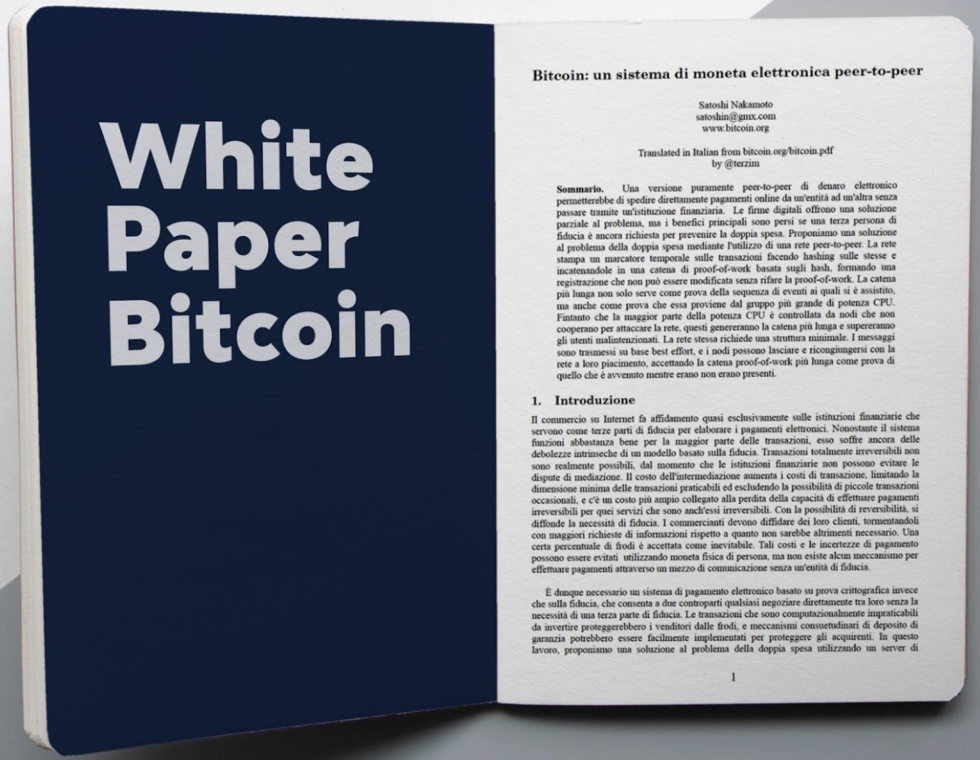
White Paper Bitcoin

- Dal documento iniziale di Bitcoin si notano uno slang britannico e alcuni modi di dire inglesi
- Il white paper è intitolato «Bitcoin p2p e-cash system» e spiega il funzionamento di Bitcoin
- Nulla di nuovo, il documento copia altre 5 tesi già esistenti e teorizzate molti anni prima da:

Wei Dai, *Adam Back*, *Hal Finney*, *Nick Szabo* e *Tim May*

11A EDIZIONE
ATENEO IMPRESA

White Paper Bitcoin



Bitcoin: un sistema di moneta elettronica peer-to-peer

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Translated in Italian from bitcoin.org/bitcoin.pdf
by @terzim

Sommario. Una versione puramente peer-to-peer di denaro elettronico permetterebbe di spedire direttamente pagamenti online da un'entità ad un'altra senza passare tramite un'istituzione finanziaria. Le firme digitali offrono una soluzione parziale al problema, ma i benefici principali sono persi se una terza persona di fiducia è ancora richiesta per prevenire la doppia spesa. Proponiamo una soluzione al problema della doppia spesa mediante l'utilizzo di una rete peer-to-peer. La rete stampa un marcatore temporale sulle transazioni facendo hashing sulle stesse e incatenandole in una catena di proof-of-work basata sugli hash, formando una registrazione che non può essere modificata senza rifare la proof-of-work. La catena più lunga non solo serve come prova della sequenza di eventi ai quali si è assistito, ma anche come prova che essa proviene dal gruppo più grande di potenza CPU. Fintanto che la maggior parte della potenza CPU è controllata da nodi che non cooperano per attaccare la rete, questi genereranno la catena più lunga e supereranno gli utenti malintenzionati. La rete stessa richiede una struttura minimale. I messaggi sono trasmessi su base best effort, e i nodi possono lasciare e ricongiungersi con la rete a loro piacimento, accettando la catena proof-of-work più lunga come prova di quello che è avvenuto mentre erano non erano presenti.

1. Introduzione

Il commercio su Internet fà affidamento quasi esclusivamente sulle istituzioni finanziarie che servono come terze parti di fiducia per elaborare i pagamenti elettronici. Nonostante il sistema funzioni abbastanza bene per la maggior parte delle transazioni, esso soffre ancora delle debolezze intrinseche di un modello basato sulla fiducia. Transazioni totalmente irreversibili non sono realmente possibili, dal momento che le istituzioni finanziarie non possono evitare le dispute di mediazione. Il costo dell'intermediazione aumenta i costi di transazione, limitando la dimensione minima delle transazioni praticabili ed escludendo la possibilità di piccole transazioni occasionali, e c'è un costo più ampio collegato alla perdita della capacità di effettuare pagamenti irreversibili per quei servizi che sono anch'essi irreversibili. Con la possibilità di reversibilità, si diffonde la necessità di fiducia. I commercianti devono diffidare dei loro clienti, tormentandoli con maggiori richieste di informazioni rispetto a quanto non sarebbe altrimenti necessario. Una certa percentuale di frodi è accettata come inevitabile. Tali costi e le incertezze di pagamento possono essere evitati utilizzando moneta fisica di persona, ma non esiste alcun meccanismo per effettuare pagamenti attraverso un mezzo di comunicazione senza un'entità di fiducia.

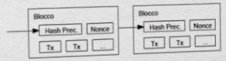
È dunque necessario un sistema di pagamento elettronico basato su prova crittografica invece che sulla fiducia, che consenta a due controparti qualsiasi negoziare direttamente tra loro senza la necessità di una terza parte di fiducia. Le transazioni che sono computazionalmente impraticabili da invertire proteggerebbero i venditori dalle frodi, e meccanismi consuetudinari di deposito di garanzia potrebbero essere facilmente implementati per proteggere gli acquirenti. In questo lavoro, proponiamo una soluzione al problema della doppia spesa utilizzando un server di

11A EDIZIONE
ATENEO IMPRESA

4. Proof-of-Work

Per implementare un server di marcatura temporale distribuito su base peer-to-peer, avremo bisogno di usare un sistema simile a quello di Hashcash di Adam Back [6], piuttosto che basarci sui messaggi di quotidiani o Usenet. La proof-of-work comporta la ricerca di un valore che, una volta sottoposto ad hash (ad esempio con SHA-256), restituisca un hash che inizia con un numero di zero bit. Il lavoro medio richiesto è esponenzialmente proporzionale al numero di zero bit richiesti e può essere verificato eseguendo un unico hash.

Per la nostra rete di marcatura temporale, implementiamo la proof-of-work incrementando un nonce nel blocco fino a quando è trovato un valore che dà all'hash del blocco gli zero bits necessari. Una volta che l'impegno della CPU è stato speso per soddisfare la proof-of-work, il blocco non può essere modificato senza rifare il lavoro. Poiché i blocchi successivi sono incatenati dopo di esso, il lavoro necessario per cambiare il blocco dovrebbe includere il rifacimento di tutti i blocchi successivi.



La proof-of-work risolve anche il problema della determinazione della rappresentatività in un sistema di decisioni prese a maggioranza. Se la maggioranza fosse basata sul principio "un indirizzo IP-un-voto", potrebbe essere sovvertita da chiunque fosse in grado di allocare molti IPs. La proof-of-work invece segue essenzialmente il principio "una CPU-un voto". La decisione di maggioranza è rappresentata dalla catena più lunga, su cui è stato speso il massimo sforzo di proof-of-work. Se la maggioranza di potenza della CPU è controllata da nodi onesti, la catena onesta crescerà più velocemente e supererà eventuali catene concorrenti. Per modificare un blocco passato, un utente malintenzionato dovrebbe rifare la proof-of-work del blocco e di tutti i blocchi successivi ad esso e poi raggiungere e superare il lavoro dei nodi onesti. Mostreremo in seguito che la probabilità che un utente malintenzionato raggiunga il lavoro dei nodi onesti diminuisce in modo esponenziale a mano a mano che vengono aggiunti blocchi successivi.

Per compensare l'aumento della velocità dell'hardware e il variare dell'interesse dei nodi operativi col tempo, la difficoltà della proof-of-work è determinata da una media mobile che ha come obiettivo la creazione di un numero medio di blocchi ogni ora. Se i blocchi vengono generati troppo velocemente, la difficoltà aumenta.

5. La Rete

I passi per far girare la rete sono i seguenti:

1) Le nuove transazioni sono trasmesse a tutti i nodi.
2) Ogni nodo immagazzina le nuove transazioni in un blocco.
3) Ogni nodo lavora per trovare una proof-of-work difficile per il suo blocco.
4) Quando un nodo trova un proof-of-work, trasmette il blocco a tutti gli altri nodi.
5) I nodi accettano il blocco solo se tutte le transazioni in esso sono valide e non sono già state spese.
6) I nodi esprimono l'accettazione del blocco mediante il tentativo di creare il prossimo blocco nella catena, utilizzando l'hash del blocco accettato come hash precedente.

I nodi considerano sempre come corretta la catena più lunga e continueranno a lavorare per allungarla. Se due nodi trasmettono diverse versioni del blocco successivo contemporaneamente, alcuni nodi possono ricevere l'una o l'altra prima. In tal caso, questi lavorano sul primo che hanno ricevuto, ma salvano l'altra ramificazione nel caso diventi più lunga. Questo impasse sarà risolto quando la proof-of-work successiva viene trovata e una delle ramificazioni diventa più lunga; i nodi che stavano lavorando sull'altra ramificazione a quel punto si sposteranno su quella più lunga.

Le trasmissioni delle nuove transazioni non devono necessariamente raggiungere tutti i nodi. Fintanto che raggiungono numerosi nodi, non ci vorrà molto affinché vengano inserite in un blocco. Le trasmissioni dei blocchi tollerano anche i messaggi troncati. Se un nodo non riceve un blocco, lo richiederà quando riceverà il blocco successivo e capirà di averne saltato uno.

6. L'Incentivo

Per convenzione, la prima transazione in un blocco è una transazione speciale che "conia" una nuova moneta di proprietà del creatore del blocco. Questo fornisce un incentivo ai nodi affinché sostengano la rete, e fornisce un modo per la distribuzione iniziale di monete in circolazione, dato che non vi è alcuna autorità centrale che possa emetterle. L'aggiunta costante di una data quantità di nuove monete è analoga al processo dei minatori d'oro, che spendono risorse per incrementare la quantità di oro in circolazione. Nel nostro caso, viene spesa potenza CPU e viene consumata energia elettrica.

L'incentivo può essere anche finanziato con costi di transazione. Se il valore di uscita di una transazione è inferiore al suo valore di ingresso, la differenza è una tassa di transazione che viene aggiunta al valore di incentivazione del blocco contenente la transazione. Nel momento in cui sia entrato in circolazione un ammontare predeterminato di monete, l'incentivo può migrare interamente ai costi di transazione e essere completamente privo di effetti inflazionari.

L'incentivo può contribuire ad incoraggiare i nodi a rimanere onesti. Se un utente malintenzionato fosse avidamente in grado di assemblare più potenza di CPU rispetto a tutti i nodi onesti, dovrebbe scegliere tra un utilizzo truffaldino (ritornando al mittente tutti i suoi pagamenti), o un utilizzo volto a coniare nuove monete. Dovrà necessariamente trovare più redditizio giocare secondo le regole, dato che tali regole lo favoriscono con più monete nuove di tutti gli altri messi insieme, piuttosto che minare la sicurezza del sistema e la validità della propria ricchezza.

11A EDIZIONE
ATENEO IMPRESA

White Paper Bitcoin

10. Privacy

Il modello bancario tradizionale consegue un certo livello di privacy limitando l'accesso alle informazioni alle parti coinvolte e alla terza controparte fiduciaria. La necessità di annunciare pubblicamente tutte le transazioni preclude tale metodo, ma la privacy può essere ancora mantenuta rompendo il flusso di informazioni in un altro luogo: ovvero mantenendo anonime le chiavi pubbliche. Il pubblico può vedere che qualcuno sta inviando un certo importo a qualcun altro, ma senza informazioni che colleganо la transazione ad un utente specifico. Questo è simile

al livello delle informazioni rilasciate dai mercati azionari, dove il tempo e la dimensione dei singoli scambi - il "nastro" - è reso pubblico, ma senza che si riveli l'identità delle controparti.

Come ulteriore schermo protettivo, una nuova coppia di chiavi deve essere utilizzata per ogni singola transazione, in modo da impedire che essa sia ricondotta ad un singolo proprietario. Qualche collegamento è ancora inevitabile nelle transazioni multi-input, che necessariamente rivelano che i loro input erano di proprietà dello stesso individuo. Il rischio è che, se il proprietario di una chiave fosse rivelato, si possa risalire ad altre transazioni effettuate dallo stesso.

11A EDIZIONE
ATENEO IMPRESA

11A EDIZIONE
ATENEO
IMPRESA

Modulo III: Blockchain

- Crittografia di base
- Tecnologia Blockchain
- Smart Contract
- Altre applicazioni

Crittografia

- Forme primitive di crittografia: antichi spartani, ebrei e Cifrario di Giulio Cesare

- Due elementi:
  1) Algoritmo, la regola con cui si nasconde qualcosa;
  2) Chiave, il parametro che permette di avere accesso a ciò che si nasconde

- Da cifratura simmetrica si passa a cifratura asimmetrica

- Bitcoin utilizza algoritmo SHA-256 che restituisce un digest di 64 caratteri

11A EDIZIONE
ATENEO IMPRESA

Funzione Hash

- Algoritmo matematico che trasforma qualsiasi stringa di informazioni (come un testo in un codice alfanumerico di lunghezza arbitraria

- È irreversibile ed univoco, dalla stessa informazione uscirà sempre lo stesso codice (hash) ma dal codice non si può risalire all'informazione

- Serve dunque come doppia verifica

11A EDIZIONE
ATENEO IMPRESA

Cifratura asimmetrica

Chiave pubblica A

Chiave privata A

Chiave pubblica B

Chiave privata B

11A EDIZIONE
ATENEO IMPRESA

Blockchain

La Blockchain è un database (o libro mastro) decentralizzato, criptato, condiviso e distribuito tra più nodi di una rete. Chiunque può leggerlo, ma può essere modificato solo con il consenso di tutti i partecipanti. La crittografia e la decentralizzazione garantiscono immutabilità, incorruttibilità e trasparenza.
Un nuovo PARADIGMA!

“Catena di blocchi”: ogni blocco contiene tutte le transazioni e lo storico di ogni transazione. Tutti i blocchi sono incatenati tra loro grazie alla crittografia. Ciò rende le transazioni immodificabili.
Vediamo come funziona: https://youtu.be/vqLiAb7a3sU

Tipologie di accesso

	Chiuso	Aperto
Centralizzato	**Blockchain private o permissioned**: l'accesso al network e le attività di controllo e validazione sono limitati ad un ristretto gruppo di partecipanti che seguono delle specifiche linee guida (Governance della Blockchain). E' una blockchain adatta per applicazioni aziendali e/o organizzazioni che necessitano di garantire l'autenticazione dei partecipanti e dei nodi stessi della Blockchain.	
Distribuito	**Blockchain Ibride**: l'accesso al network è riservato ad un numero ristretto di partecipanti che sono riconosciuti ed autenticati. La validazione è affidata a tutti i nodi e tutti concorrono alla sicurezza complessiva della Blockchain.	**Blockchain permissionless**: l'accesso al network è totalmente libero per chiunque intenda partecipare. Il controllo è distribuito e riguarda tutti i partecipanti. Tutti possono accedere e tutti sono chiamati a validare le transazioni.

Tipologie di blockchain

Vi sono 3 tipologie di blockchain:

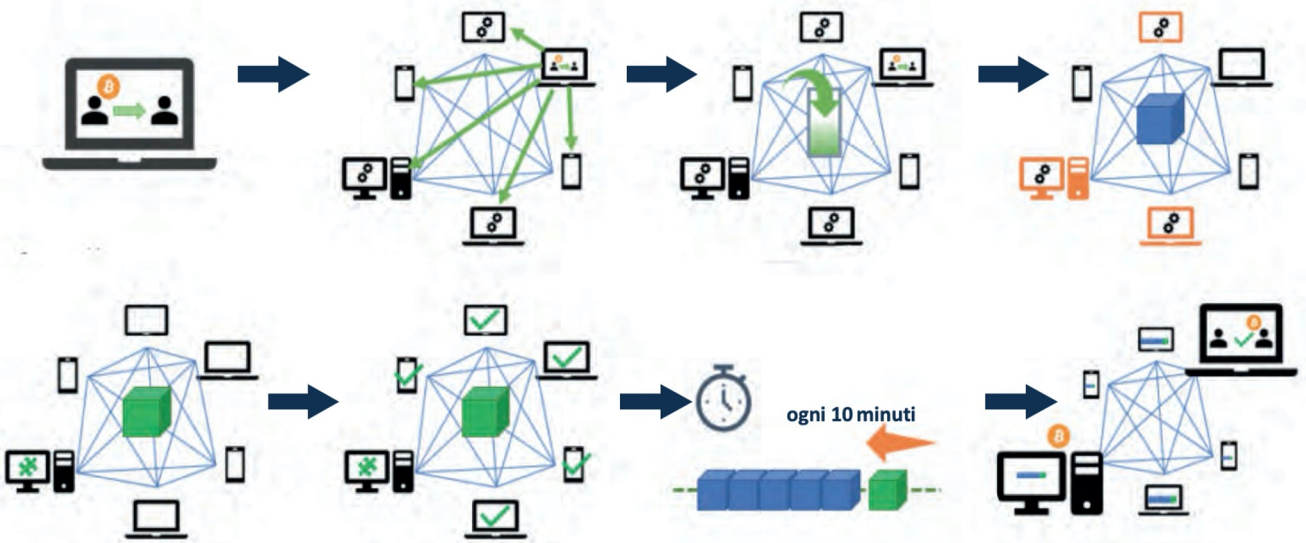
1. **Permissionless**: non serve autorizzazione, chiunque ne può prendere parte, totalmente decentralizzate (ad esempio Bitcoin ed Ethereum).
2. **Permissioned**: introducono il concetto di governance centralizzata, vi è un consorzio o autorità centrale a decidere chi può accedervi (ad esempio Libra, Ripple e Hyperledger).
3. **Ibride:** l'accesso è limitato ad un gruppo ristretto di partecipanti, riconosciuti e autenticati. Tutti concorrono alla validazione e alla sicurezza della rete (ad esempio Bankchain).

1. Viene richiesta una nuova transazione

2. La transazione viene inviata a tutti i nodi

3. I miners la aggiungono alla lista delle transazioni da elaborare

4. I miners provano a creare un nuovo blocco valido



5. Il primo miner che riesce a trovare un blocco valido lo invia agli altri nodi della rete

6. Il blocco viene validato ossia viene verificato che il "puzzle" sia effettivamente risolto

7. Il blocco viene aggiunto alla main blockchain che viene inviata a tutti i nodi della rete

8. La transazione è effettuata (il miner che ha risolto il "puzzle" viene ricompensato con i nuovi bitcoin)

I blocchi

Cos'è un blocco? Un file che contiene una serie di informazioni:

1. Numero del blocco
2. Hash univoco
3. Timestamp
4. Transazioni
5. Ecc

Ogni blocco contiene al proprio interno il codice hash del blocco precedente.

Ciò rende impossibile modificare transazioni o informazioni passate

11A EDIZIONE
ATENEO IMPRESA

Nel 1400 già esisteva?

Nel 1400 nell'Isola di Yap (Micronesia) gli abitanti iniziarono ad utilizzare i sassi come moneta.

Per evitare furti, adottarono un ingegnoso sistema: ogni abitante teneva un registro pubblico in cui annotare le proprietà e gli scambi di ogni pietra.
Quindi solo il reale proprietario del sasso poteva spenderlo anche senza doverlo portare con sé. Era una forma primitiva di blockchain.

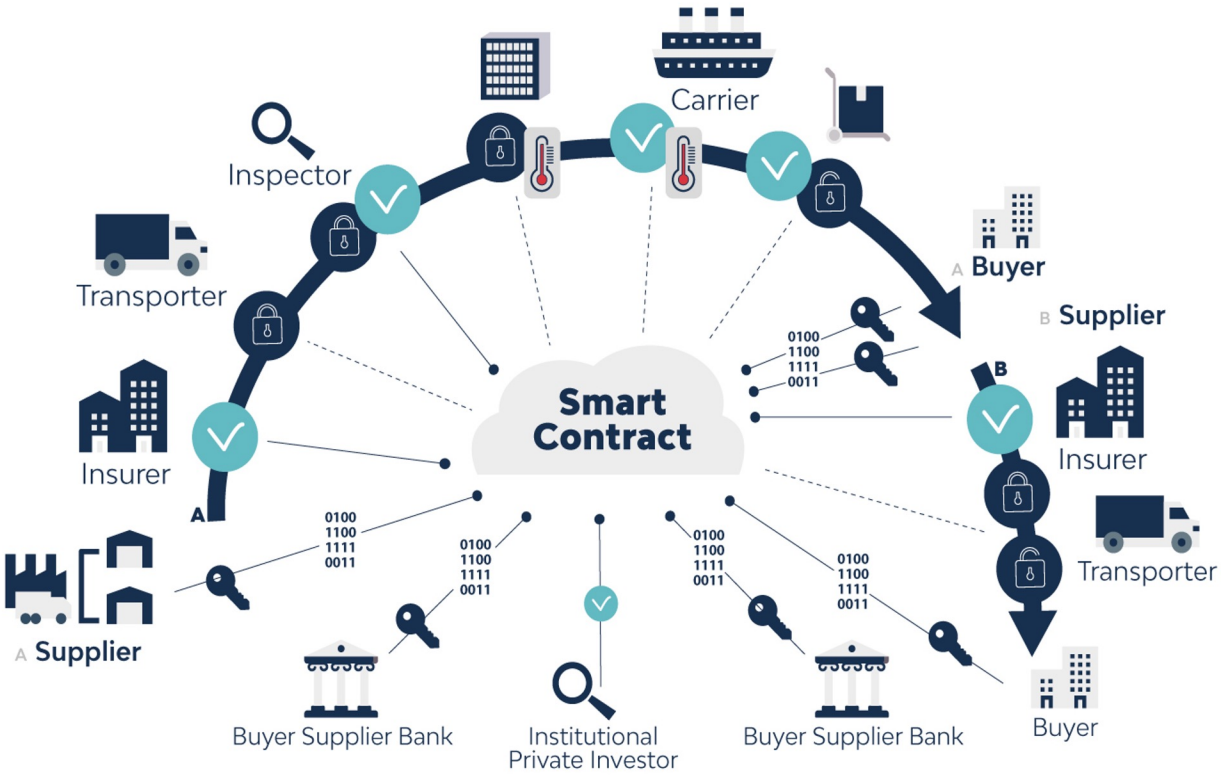
11A EDIZIONE
ATENEO IMPRESA

Smart Contract

Uno Smart Contract è la trasposizione in codice di un contratto, in modo da verificare in automatico l'avverarsi di determinate condizioni e, conseguentemente, di eseguire in automatico le azioni previste e pre-accordate.

Immaginiamo ad esempio la macchinetta del caffè, un'auto o una casa a rate, un treno che arriva in ritardo, ecc.

Ambiti applicativi di uno *Smart Contract*



11A EDIZIONE

ATENEO IMPRESA

Alcuni casi applicativi

- Finanziamenti trasparenti ai partiti
- Tasse
- Charity
- Assicurazioni
- Notaio
- Sanità
- Diritti d’autore

Modulo IV: Criptovalute

- Cosa sono
- Requisiti
- Casi studio

Criptovaluta

- Per la prima volta una moneta è sottratta all'emissione e al controllo di un ente centrale
- E' una rappresentazione digitale di valore basata su crittografia, che utilizza un registro decentralizzato denominato «blockchain» per memorizzare tutte le informazioni sulle transazioni effettuate
- Esistono più di 10.000 criptovalute nel mondo

11A EDIZIONE
ATENEO IMPRESA

Requisiti

Secondo *Jan Lansky* una criptovaluta è un sistema che soddisfa 6 condizioni:

1 - Il sistema non richiede un'autorità centrale, il suo stato è mantenuto attraverso un consenso distribuito

2 - Il sistema mantiene un controllo delle unità di criptovaluta e della loro proprietà

3 - Il sistema determina se possono essere create nuove unità di criptovaluta. Se tali unità si possono creare, il sistema definisce la loro origine e come determinare il loro possessore

11A EDIZIONE
ATENEO IMPRESA

Requisiti

4 - La proprietà di una criptovaluta può essere provata solo crittograficamente

5 - Il sistema consente di eseguire transazioni nelle quali avviene un cambio di proprietà delle unità crittografiche. La conferma della transazione può essere rilasciata solo da un ente che può provare la proprietà delle criptovalute oggetto della transazione

6 - Se vengono date simultaneamente due diverse istruzioni per il cambio di proprietà delle stesse unità crittografiche, il sistema esegue al massimo una delle due.

Alcune criptovalute

- Bitcoin
- Ethereum
- Tether
- Bnb
- Cardano
- Solana
- Iota
- Algorand
- Polygon
- Polkadot
- Uniswap
- Eos
- Stellar
- Monero

11A EDIZIONE
ATENEO IMPRESA

Today's Cryptocurrency Prices by Market Cap

Highlights

The global crypto market cap is **$826.08B**, a ▲ 0.37% increase over the last day. Read More

Trending

More >

1	STEPN GMT	▼ 0.38%
2	Bitcoin BTC	▲ 0.09%
3	Shiba Inu SHIB	▲ 0.52%

Recently Added

More >

1	Onigiri Neko ONIGI	$0.007977
2	Pusuke Inu PUSUKE	$0.0000004298
3	METAFASTEST METAF	$0.3982

nity Accounts

More > Top Commu

on @Qtum_Foundation + Follow

+ Follow

PlayDapp_IO + Follow

CoinMarketC

2023 #CI

2023 CMC

Jan 6

Watchlist | Portfolio | Cryptocurrencies | Categories | DeFi | NFT | Metaverse | Polkadot | BNB Chain | Solana | Avalanche | Show rows 100 | Filters | Customize

#	Name	Price	24h Volume	1h %	24h %	7d %	Market Cap	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$16,954.08	$8,324,742,532 491,301 BTC	▼ 0.04%	▲ 0.12%	▲ 2.28%	$326,471,294,305	19,256,206 BTC	
2	Ethereum ETH	$1,266.55	$2,842,145,384 2,246,703 ETH	▼ 0.18%	▲ 0.32%	▲ 5.71%	$154,992,264,841	122,373,866 ETH	
3	Tether USDT	$0.9999	$12,105,596,519 12,106,629,112 USDT	▲ 0.00%	▲ 0.01%	▲ 0.03%	$66,268,279,243	66,272,490,385 USDT	
4	USD Coin USDC	$1.00	$1,523,596,074 1,523,629,313 USDC	▲ 0.01%	▲ 0.01%	▼ 0.01%	$43,925,517,919	43,923,254,230 USDC	

11A EDIZIONE
ATENEO IMPRESA

Fonti per documentarsi

Instagram: @Giallucoma

Facebook: GIAN LUCA COMANDINI

Twitter: GLComandini

Info: www.bitcoin.org

News: www.cointelegraph.com (@cointelegraphit)

Community Facebook “Bitcoin Italia”

Imprese: www.actafintech.com

Libro: «Da Zero alla Luna» di G.L.Comandini

Master: www.theblockchainmanagementschool.it

Bonus per iniziare: https://bit.ly/3XeHQvv

11A EDIZIONE
ATENEO IMPRESA

11° Master Lab in
Blockchain Technology &
Management

ATENEO
IMPRESA

Gian Luca Comandini

Email: g.comandini@actafintech.com

Instagram: @Giallucoma

Twitter: @GLComandini

ATENEO IMPRESA

THE BLOCKCHAIN MANAGEMENT SCHOOL

T. 06 54912353 - 06 549121
M. 351 8203944
info@ateneoimpresa.it
segreteria@ateneoimpresa.it

TBMS | CANALI UFFICIALI

Facebook

@theblockchainmanagementschool.it

Sito Web

theblockchainmanagementschool.it

Linkedin

The Blockchain Management School | Ateneo Impresa