

Criptovalute: Cosa sono e come funzionano

Prof. Marino Miculan

Dipartimento di Scienze Matematiche, Informatiche e Fisiche
Università di Udine



Bitcoin mania



Fino al 31 dicembre,
€ 4.000
di riconoscimento
su tutti i modelli
Mercedes-Benz,
se permessi un'auto
dono da EU1 a EU4.

Scopri l'offerta
su [Mercedes.it](#)

FINANZA & MERCATI

IN PRIMO PIANO AZIONI OBBLIGAZIONI FONDI A TUTTI TASSI A VALUTE MONETARIE PREMI FINANZA PERSONALE STRUMENTI LETTERA AL DIRIGENTE

Home DOSSIER

Criptovalute: bitcoin e le altre

Bitcoin a briglia sciolta, «no» delle grandi banche al futuro
L'Ue è stata delle grandi banche, ma le monete virtuali
di Ylio Lupo

PIMCO
BANCHE E CREDITO
NEL CRISTIANO MARCHETTINI

SCOPRI DI PIÙ

Fino al 31 dicembre,
€ 4.000
di riconoscimento
su tutti i modelli
Mercedes-Benz,
se permessi un'auto
dono da EU1 a EU4.

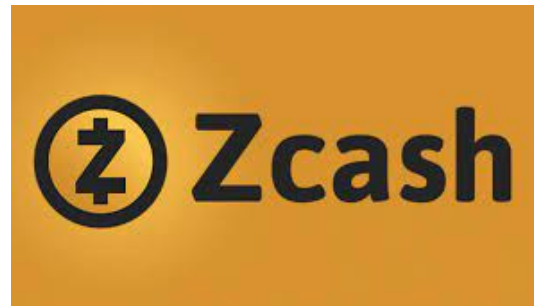
Scopri l'offerta
su [Mercedes.it](#)

<https://news.bitcoin.com/>
<https://trends.google.it/trends/explore?date=today%205-y&q=bitcoin>

E molte altre criptovalute e blockchain



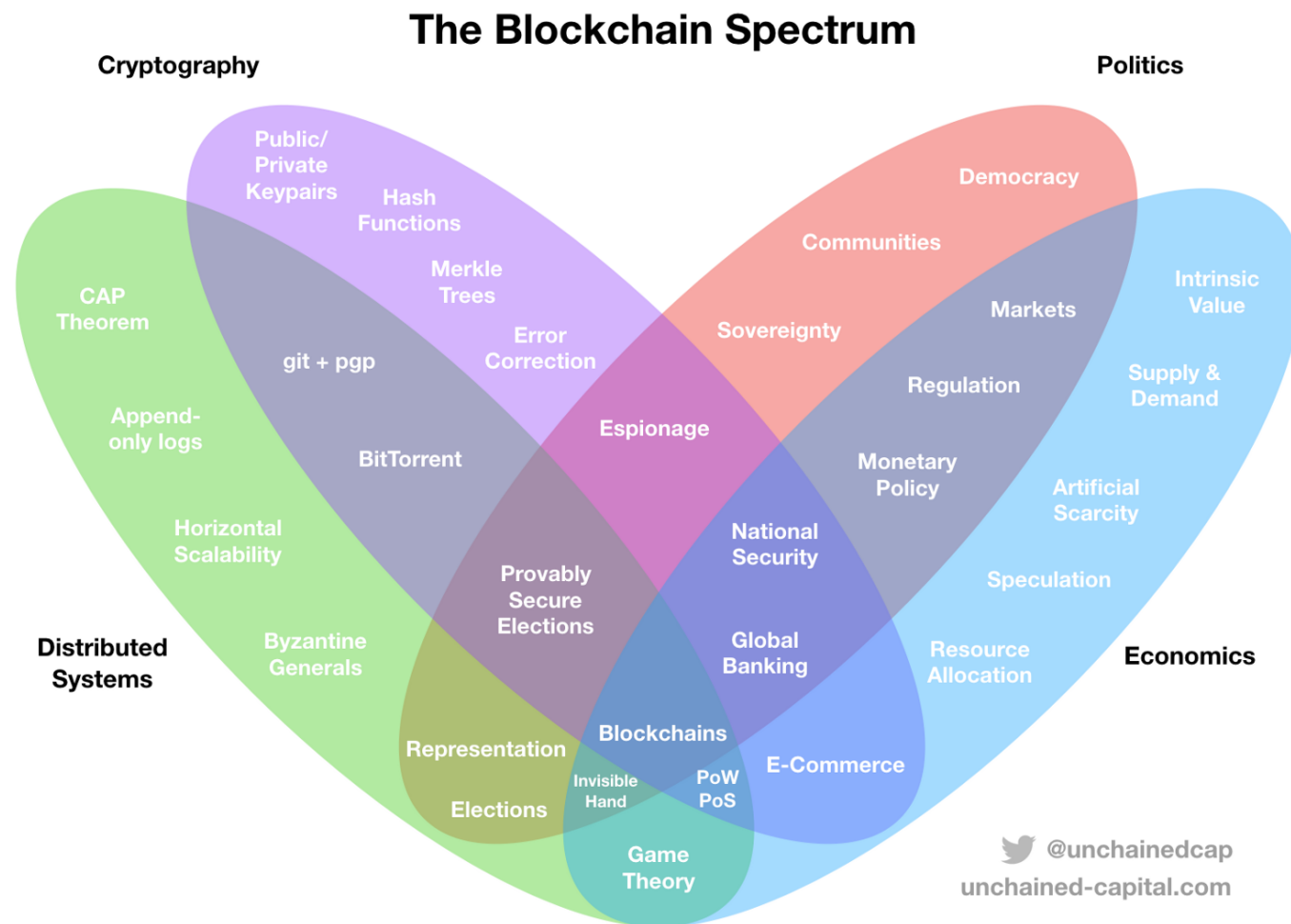
Algorand™



Non Fungible Tokens

Ma... cos'è la Blockchain??

- Coinvolge
 - Crittografia
 - Reti di computer e trasmissione dati
 - Teoria dei giochi
 - Teoria economica e monetaria
- Ma soprattutto, un cambiamento di paradigma culturale: **potrebbe sostituire qualsiasi autorità centrale con un equivalente decentralizzato peer-to-peer crittograficamente sicuro**



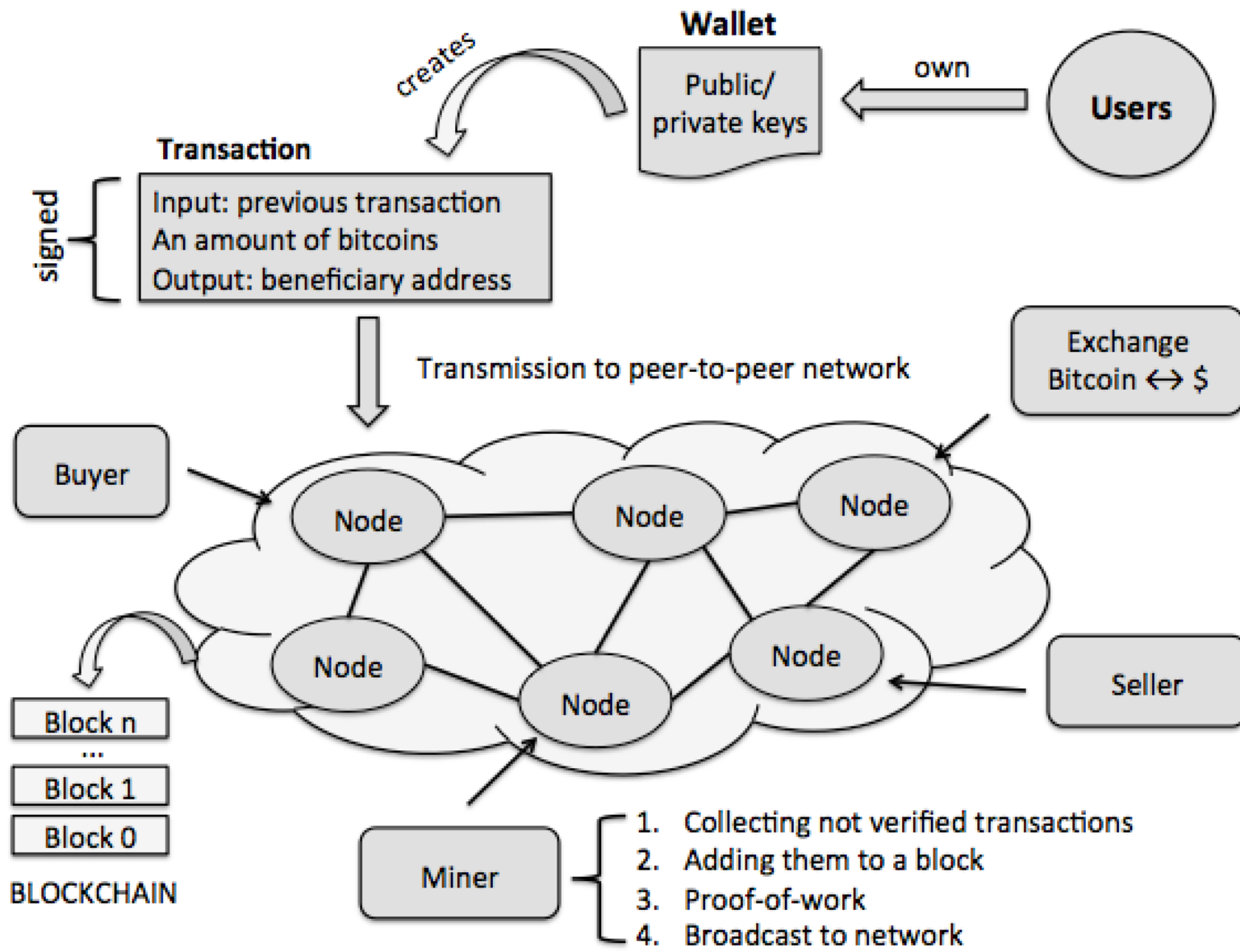
Cos'è Bitcoin? Concetti di base

- **Criptovaluta:** deriva la fiducia da:
 - NON dagli statuti a corso legale (come le valute fiat)
 - NON dalle proprietà chimiche/fisiche
 - Ma dalle **proprietà matematiche** che ne regolano la generazione di unità di valuta e verificano le transazioni, **indipendentemente** da una banca centrale



Cos'è Blockchain, in una diapositiva

- **Transazioni:** trasferimenti di bitcoin dagli indirizzi di input agli indirizzi di output
- **Blocchi:** raccolta di transazioni con timestamp
- **Miner:** agente che convalida le transazioni e le mette in blocchi
- **Blockchain:** l'intera serie di blocchi "incatenati" insieme
- I miner competono per aggiungere blocchi, il "vincitore" viene compensato con bitcoin



Transazioni e scambio di proprietà



Transazioni: trasferimenti di cosa?

- Nella moneta fiat, la transazione è lo scambio di oggetti fisici (monete, banconote, ...): la proprietà del valore corrisponde alla proprietà dell'oggetto fisico
- Ma i bitcoin esistono solo virtualmente. Nessun oggetto fisico da scambiare
- Invece: **una transazione è un accordo comune e condiviso sul cambio di proprietà**
- I Bitcoin non vengono "spostati". Cambiano solo le loro proprietà!
- La proprietà può essere divisa tra diversi partecipanti o unita

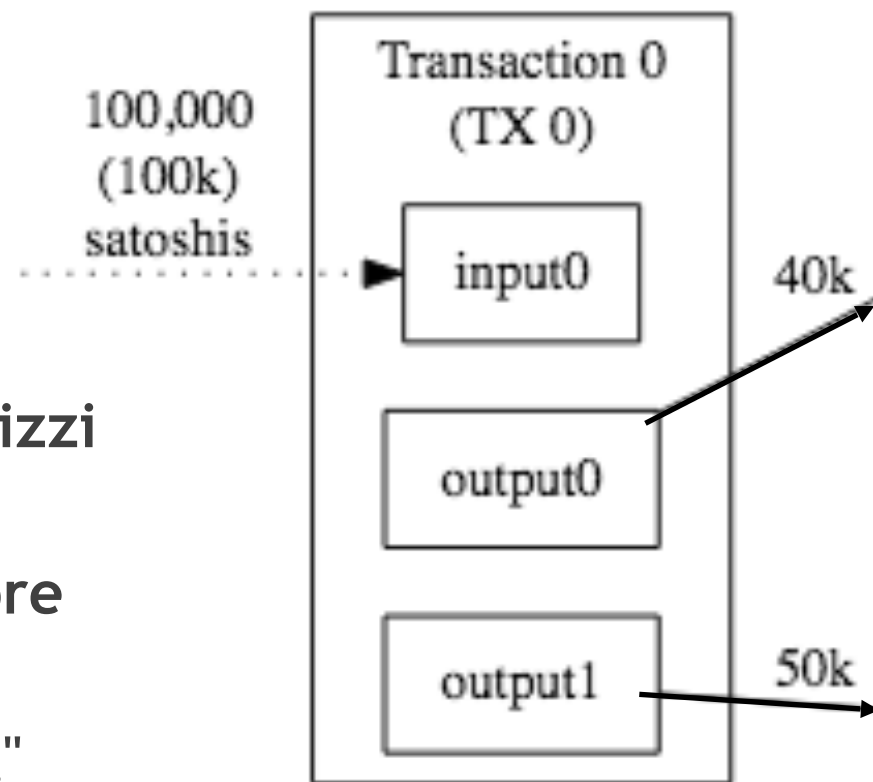
Un'analogia: pietre Rai (isole Yap, XV secolo)

- Le pietre Rai vengono scolpite e posizionate da qualche parte, poi mai spostate
- Il sistema monetario si basa su una storia orale e condivisa di proprietà
- L'acquisto di un oggetto con una pietra rai implica semplicemente concordare che la proprietà sia cambiata
- La transazione è registrata nella storia orale, condivisa con tutto il villaggio. Sharing is caring!
- Non è richiesto il movimento fisico della pietra
- In effetti, alcune pietre sono andate "perse", ma sono state comunque utilizzate nelle transazioni. Non è necessario l'accesso fisico alla pietra!
- Vedi <https://youtu.be/J-ab9was1p0>



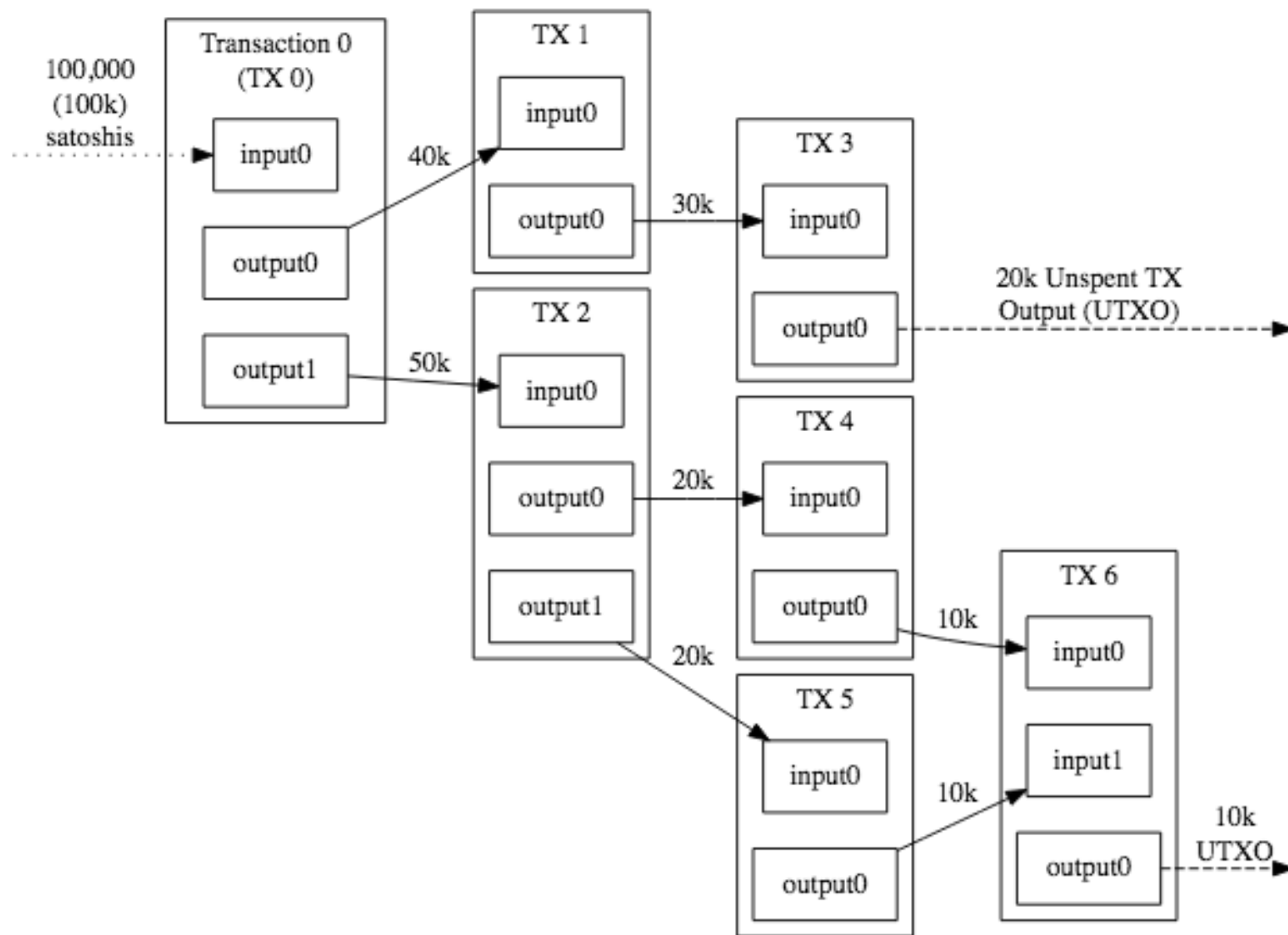
Transazioni Bitcoin: contabilità a tripla voce

- Una transazione ha tre componenti fondamentali:
 - Un identificatore di transazione univoco
 - Un elenco di indirizzi di input
 - Un elenco di indirizzi di output
- Significato: "la proprietà di questi bitcoin viene trasferita da questi indirizzi di input a questi indirizzi di output, in base a queste azioni"
- La transazione è firmata digitalmente dal possessore degli indirizzi di input
- Potrebbero esserci degli avanzi, intesi come "mancia" per i minatori (commissioni di transazione)
- (1 satoshi = 10^{-8} BTC; 1000 satoshi = 0,43 €)



Transazioni

- Le transazioni sono raccolte in **blocchi**, e registrate **per sempre**
- In ogni momento, le uscite TX non spese sono dove si trova la (proprietà del) denaro
- Circa 1.350.000.000 di TX, finora ([vedi qui](#))
- **Tutte le transazioni sono aperte all'ispezione di tutti!**





Transaction View information about a bitcoin transaction

447cb6623db32b5f28c94ac10551802075f053208fe995204a145197e2904bb9

3Nxwenay9Z8Lc9JBiywExpnEFilp6Afp8v (44,000 BTC - Output)



3LrLWTSdd69oZVVQ6dtWaAAaBLn7N3rRjz - (Spent)	333.33328889 BTC
3QkXtcSWJA9w77eCujnMBKDWFe7F7zwxTg - (Spent)	333.33328889 BTC
3Qd7hXZoZ1iyXZznrbdUwUQBxHmujdqhJ - (Spent)	333.33328889 BTC
3ECJwvx9VgftcUuEJMVNvmWnTGVmK179L - (Spent)	333.33328889 BTC
3BuQmbmdce3e31GEovq5SgowLdfMgJzLDE - (Spent)	333.33328889 BTC
3NwKLjJjzXSnBFQWokXRgBG3JeuF3bsnfE - (Spent)	333.33328889 BTC
3GEaT8ZXELcjMSFvGro6eZcC5S1LSLZuN - (Spent)	333.33328889 BTC
35DVAzDtZDKAU94kFT9sxoscnuLCTxgwYc - (Spent)	333.33328889 BTC
3Nxwenay9Z8Lc9JBiywExpnEFilp6Afp8v - (Unspent)	38,000 BTC
35mwqShnStDro6uEB4bmsgbyBo8en6Byfm - (Spent)	333.33328889 BTC
39pvSqfNcUosc8RGVWxyzKM3ny96a3uSkW - (Spent)	333.33328889 BTC
39QNJsgQg5JnBXAtbF8ezkDn72VqWdPZPJ - (Spent)	333.33328889 BTC
3L9qAGBQLbXkFAB2GpijnJXPScSVjuiJio - (Spent)	333.33328889 BTC
37WSkANPVUQ8uukt8hv671CejRtBtQ4tJ - (Spent)	333.33328887 BTC
3EEwPZZ6pYRJStCz9RBoVYPRnoWyGWEka - (Spent)	333.33328889 BTC
3C4ABC7iPcAAKBh6SJXfvUSDBew3abCtw3 - (Spent)	333.33328889 BTC
3HpQozfTzoXAsHf87m2mwJXUQ14LVtLgK4 - (Spent)	333.33328889 BTC
337RfngTLRTpU7RT9sKWQWDdmfcdmWnugi - (Spent)	333.33328889 BTC
3P2eoKr3vAeZhJcTzon3VFkv5r7DqSXW9G - (Spent)	333.33328889 BTC

43,999.9992 BTC

Summary	
Size	1055 (bytes)
Received Time	2016-08-30 11:45:03
Included In Blocks	427512 (2016-08-30 11:51:09 + 6 minutes)
Confirmations	854 Confirmations
Relayed by IP	5.39.93.85 (whois)
Visualize	View Tree Chart

Inputs and Outputs	
Total Input	44,000 BTC
Total Output	43,999.9992 BTC
Fees	0.0008 BTC
Estimated BTC Transacted	333.33328887 BTC
Scripts	Hide scripts & coinbase

44.000 bitcoin (circa 1885 M€) divisi tra diverse destinazioni, alla tasa di 0,0008 BTC (=34 €)

Gli output che sono stati spesi, sono stati utilizzati come input in transazioni successive

L'output non speso è un indirizzo in cui ci sono 38.000 BTC

Identità in Bitcoin: *pseudonimato*, non anonimato

- Tutte le transazioni sono visibili a tutti
- Per preservare la privacy, non possiamo utilizzare dati personali (come e-mail)
- Soluzione Bitcoin: usa **pseudonimi**
 - Un utente possiede alcuni indirizzi univoci, ma questi indirizzi non forniscono alcuna informazione diretta sul proprietario: non possiamo recuperare la sua identità da un indirizzo
 - Gli indirizzi non sono emessi da alcuna autorità: **ogni utente può generare tutti gli indirizzi** (praticamente casuali) di cui ha bisogno
 - Non conosciamo le identità dietro questi indirizzi (a meno che il proprietario non decida di renderli pubblici)

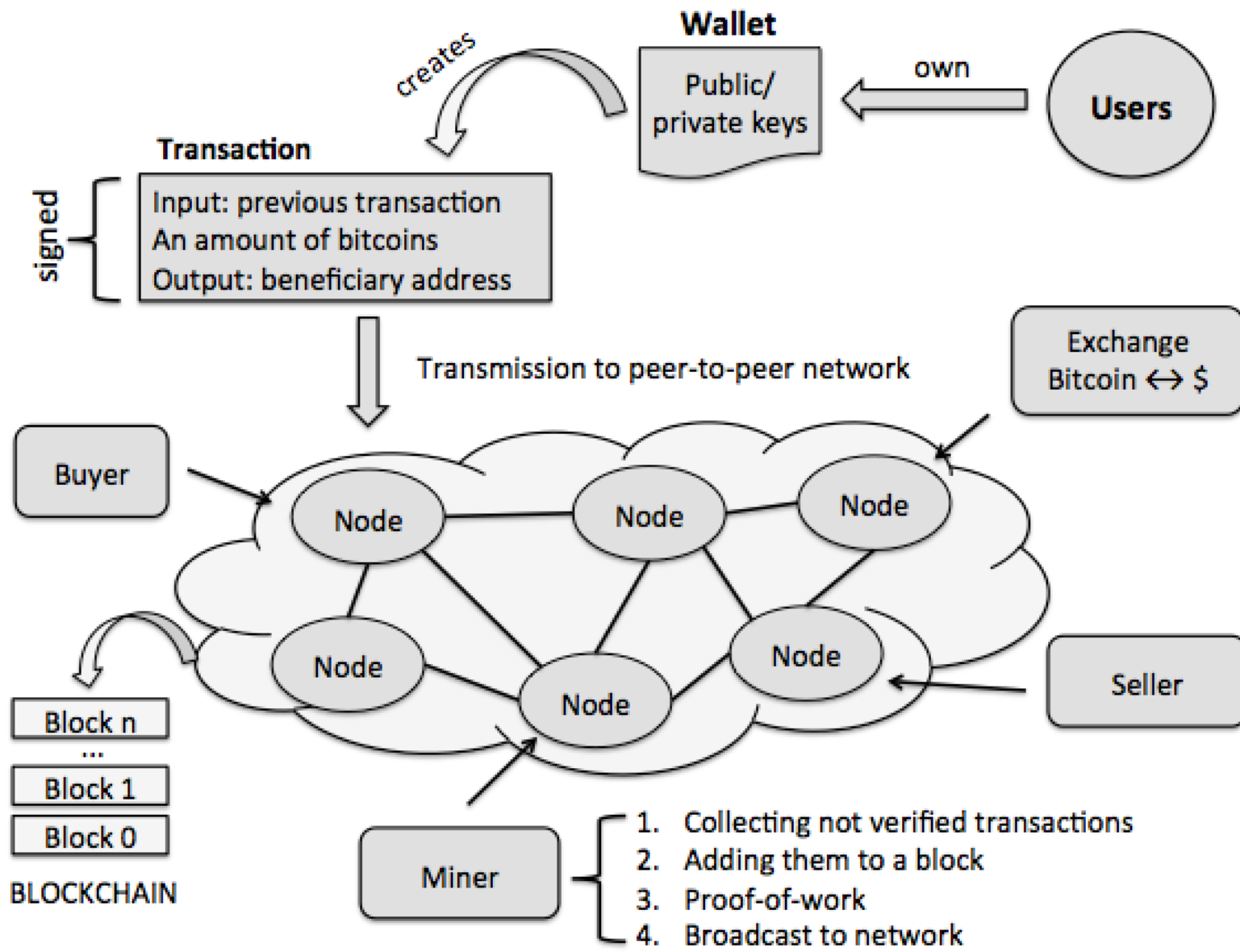


Il libro mastro distribuito (Distributed Ledger)



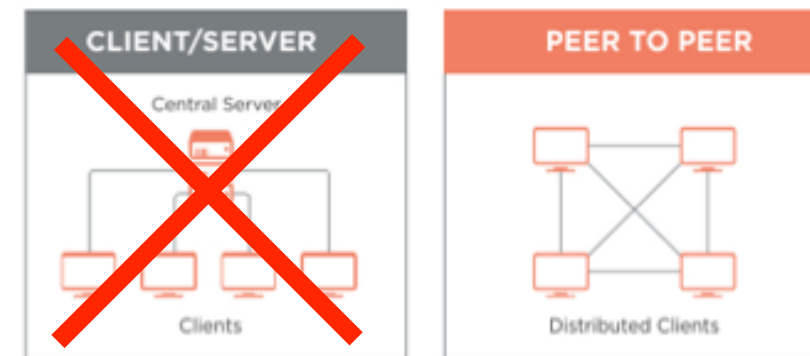
Cos'è Blockchain, in una diapositiva

- **Transazioni:** trasferimenti di bitcoin dagli indirizzi di input agli indirizzi di output
- **Blocchi:** raccolta di transazioni con timestamp
- **Miner:** agente che convalida le transazioni e le mette in blocchi
- **Blockchain:** l'intera serie di blocchi "incatenati" insieme
- I miner competono per aggiungere blocchi, il "vincitore" viene compensato con bitcoin



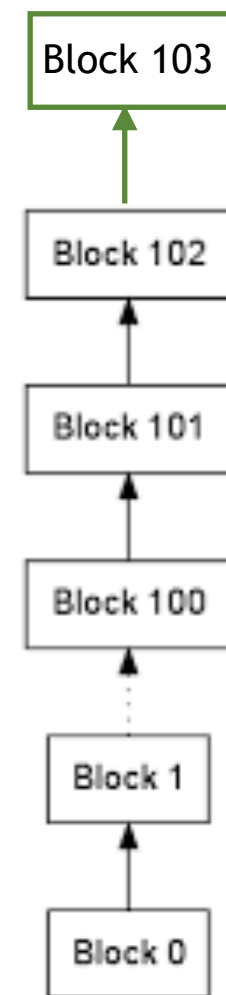
Il libro mastro distribuito (distributed ledger)

- Dove conserviamo queste transazioni?
- Abbiamo bisogno di un **libro mastro permanente**
 - Risolto in un sistema **veramente distribuito**
 - Sicurezza crittografica
 - Incentivi economici sinergici
- **Non supportato da alcuna autorità centrale** (governo o organizzazione)
 - Nessuna necessità di intermediari di fiducia
 - Nessuna Banca Centrale per l'emissione di denaro
 - Alta ridondanza, disponibilità, scalabilità
 - Massima responsabilità dei singoli!



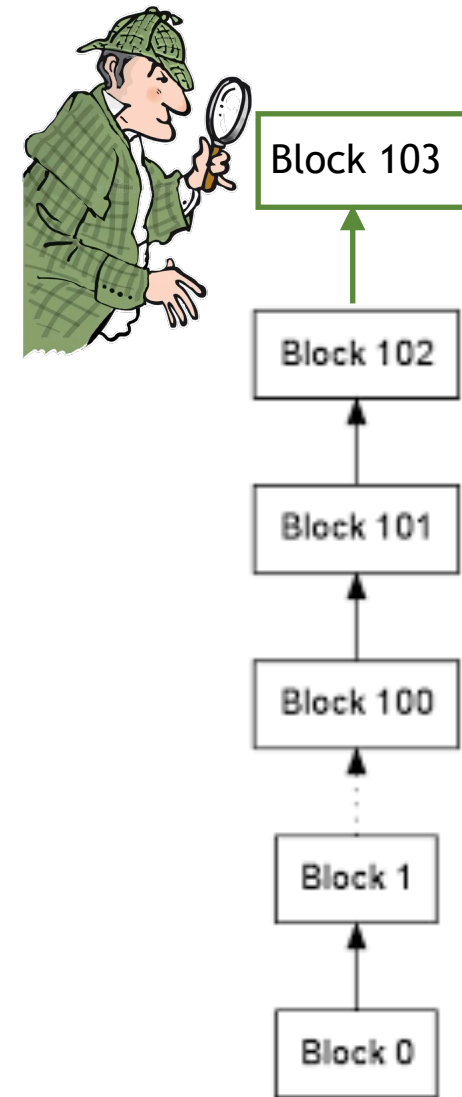
Verifica delle transazioni in un sistema Proof-of-Work

- La validazione delle transazioni è fatta dai *miner*.
- Chiunque può, in linea di principio, diventare miner
- Mario è un miner: il suo lavoro è convalidare le transazioni
 1. Raccoglie un po' di transazioni in sospeso
(tra queste, anche il suo premio)
 2. Controlla le transazioni rispetto alla sua copia della blockchain per assicurarti che siano legittime
 3. Cerca la soluzione ad un dato puzzle matematico (in Bitcoin, questo si chiama *mining*, e prende molto tempo e energia)
 4. Solo dopo aver trovato la soluzione (*proof-of-work*), può aggiungere il blocco alla propria blockchain e annunciarlo alla rete, assieme alla soluzione trovata.



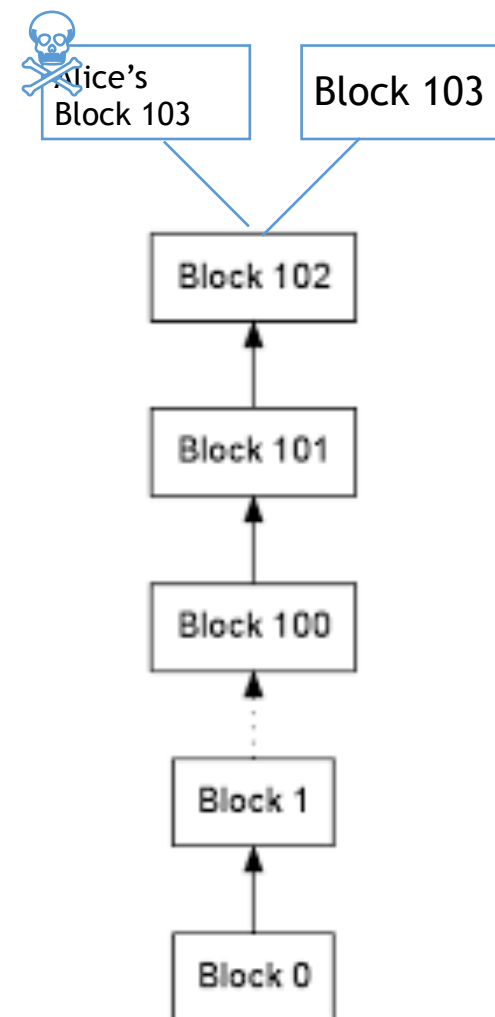
Verifica delle transazioni in un sistema Proof-of-Work

- Ogni altro nodo, quando riceve il blocco trovato da Mario:
 1. Controlla che le transazioni siano corrette e Mario abbia effettivamente trovato una soluzione per il puzzle
 2. Se tutto va bene, aggiunge il blocco alla sua copia della blockchain
 3. E adesso tutti i miner devono ricominciare dal nuovo blocco
- Quindi il mining è una gara: chi trova per primo il blocco, vince il premio (bitcoin nuovi + le commissioni)
- Più potenza di calcolo si impiega, più è probabile trovare per primi la soluzione (e guadagnare)



Perché la proof-of-work impedisce gli attacchi??

- Supponiamo che un gruppo disonesto di minatori (la banda di Alice) cerchi di annunciare un nuovo blocco, forse contenente alcune transazioni falsi, all'attuale blockchain
- Per raggiungere questo obiettivo, devono "vincere" la gara dei puzzle
- Ma la probabilità di essere i primi a risolvere il puzzle è proporzionale alla potenza computazionale impiegata!
- Se il 51% della potenza computazionale complessiva sulla rete è controllato da minatori onesti, **è più probabile che qualche nodo onesto vincerà la gara prima della banda di Alice**
- In questo caso, un blocco corretto verrà aggiunto alla blockchain invece di quello malevolo di Alice, e la banda di Alice deve ricominciare dal nuovo blocco!



L'accordo Satoshi: la maggioranza computazionale ha sempre ragione

- Quindi, alla fine la blockchain conterrà solo blocchi estratti dalla **maggioranza computazionale** della rete

**La verità è ciò che crede la maggioranza
(computazionale)**

- Un blocco (e le transazioni in esso contenuti) può essere ritrattato dopo che è stato annunciato perché è stata scoperta una catena più lunga, ma più vecchio è il blocco, più è improbabile che ciò accada
- In Bitcoin, la "profondità di conferma definitiva" è 6 (la probabilità di ritrattamento è ~ 0). Cioè, dopo circa 1 ora.

Altri usi della tecnologia Blockchain



Altri usi della tecnologia Blockchain

- Registri (anagrafi, catasto, PRA,...)
- Sistemi di registrazione autorevoli
- Servizi di directory
- Servizi di timestamping ("Prova di esistenza")
- Scambi di controparti
- Token non fungibili (NFT)
- Blockchain più espressive (ad es. Ethereum) consente applicazioni più generali, con gli *smart contracts*



Grazie per l'attenzione

marino.miculan@uniud.it

