UNIVERSITÀ DEGLI STUDI DI UDINE

Criptovalute per tutti: Cosa sono e come funzionano

Prof. Marino Miculan
Dipartimento di Scienze Matematiche, Informatiche e Fisiche
Università di Udine

Bitcoin mania


BUSINESS & FINANCE

Bitcoin Trades Full Speed Ahead

Uber Fires Over 20 In Wake Of Probe

$2,967


THE WALL STREET JOURNAL.

THURSDAY, NOVEMBER 30, 2017 – VOL. CCLXX NO. 128

Bitcoin's rise this year dwarfs other major episodes in recent decades.

Bitcoin Mania: Even Grandma Is In

Lauer's Firing Puts N In Turn


TECHNOLOGY: AMAZON AND SOFTBANK BILLIONAIRES BATTLE IN INDIA B4

BUSINESS & FINANCE

Bitcoin Price Jumps Past $4,000

$1.3B

Liberty Global

Cable Guy

Milano Finanza

Bitcoin ($): consolidamento laterale sotto i 60.000$


24 ORE FINANZA & MERCATI

Criptovalute: bitcoin e le altre

Bitcoin a briglia sciolta, «no» delle grandi banche al future

https://news.bitcoin.com/

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

E molte altre criptovalute e blockchain

Algorand™

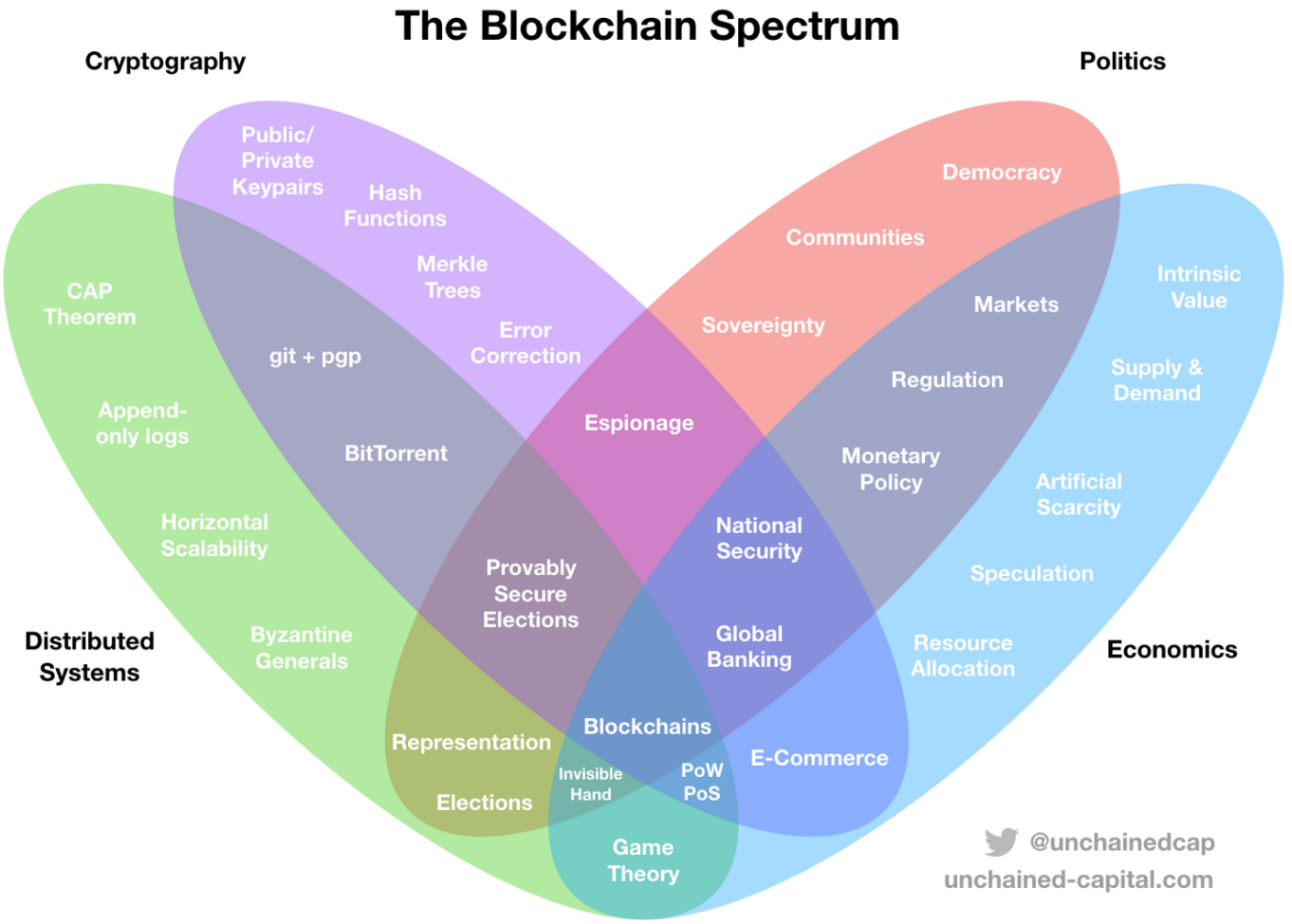
Zcash

IOTA

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 di elaborazione con un equivalente decentralizzato peer-to-peer crittograficamente sicuro**

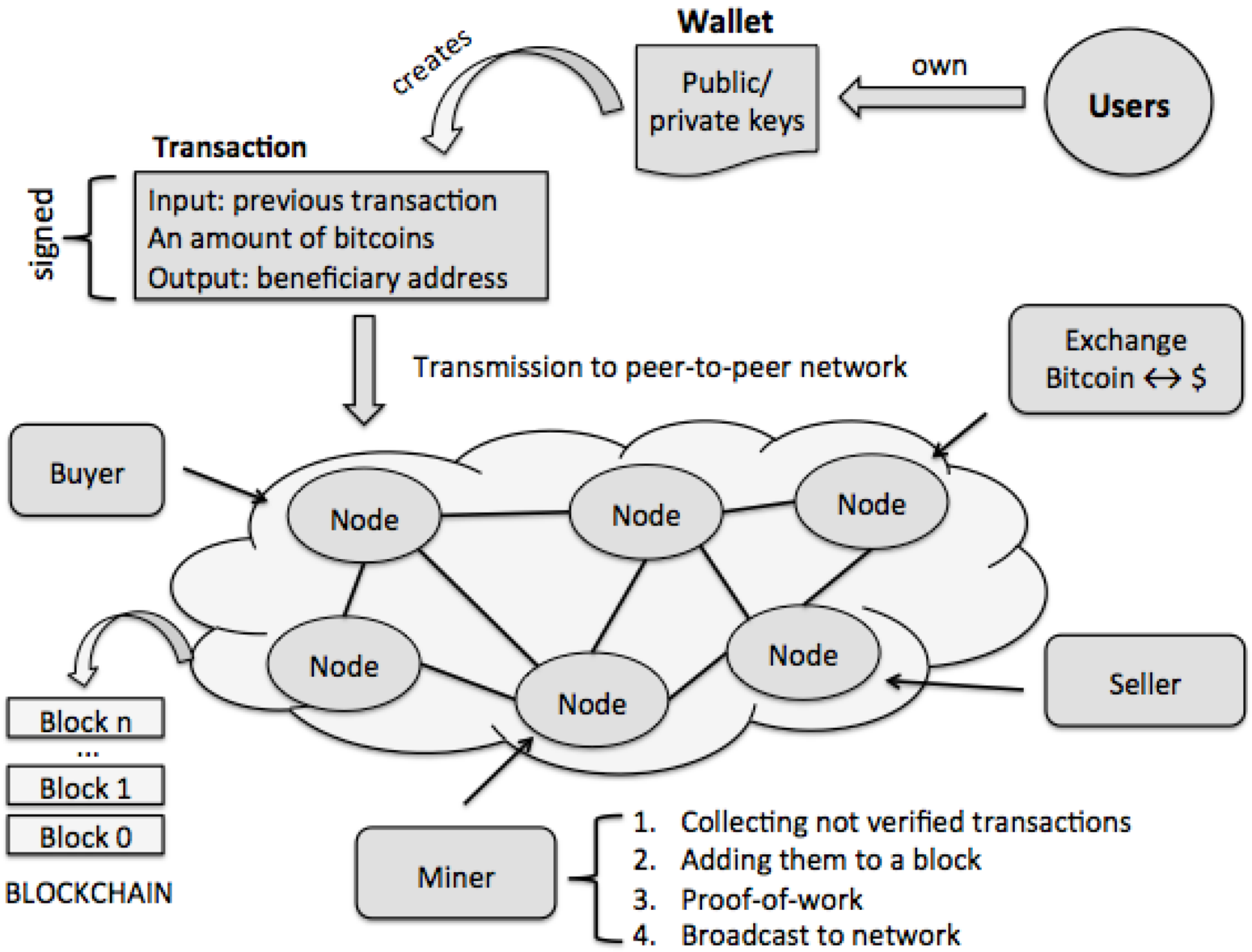


Cos'è Bitcoin? Concetti di base

- **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, operando **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?

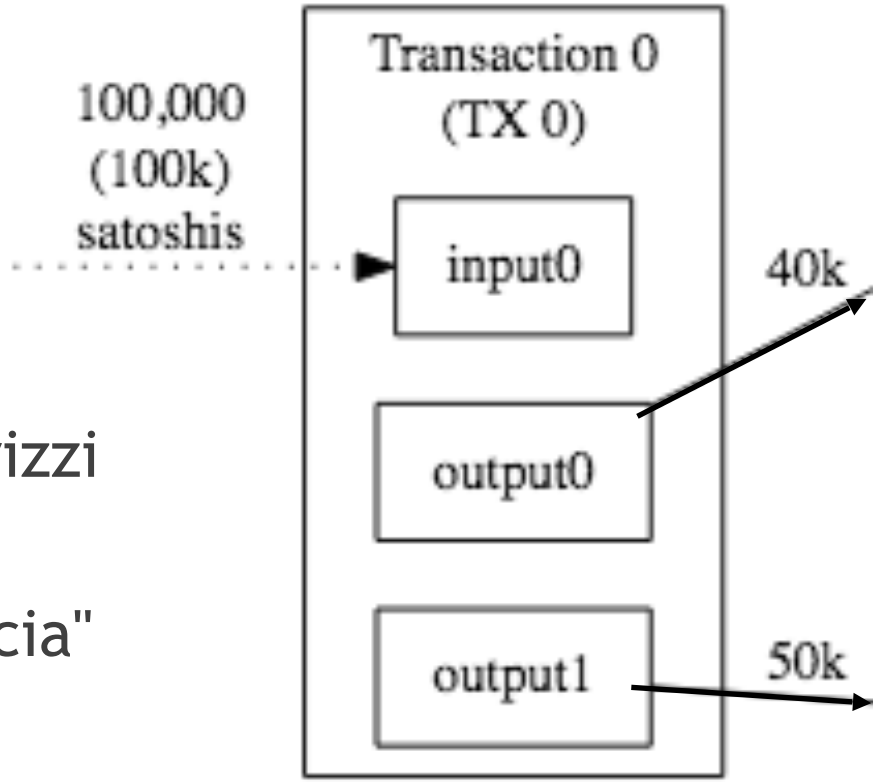
- Nella moneta fiat, la transazione è lo scambio di oggetti fisici (monete, banconote, …): la proprietà del valore corrisponde alla proprietà dell'oggetto fisico
- Ma i bitcoin esistono solo virtualmente. Nessun oggetto fisico da scambiare
- Invece: **una transazione è un accordo comune e condiviso sul 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" in mare, ma sono state comunque utilizzate nelle transazioni. Non è necessario l'accesso fisico alla pietra!
- Vedi https://youtu.be/J-ab9was1p0

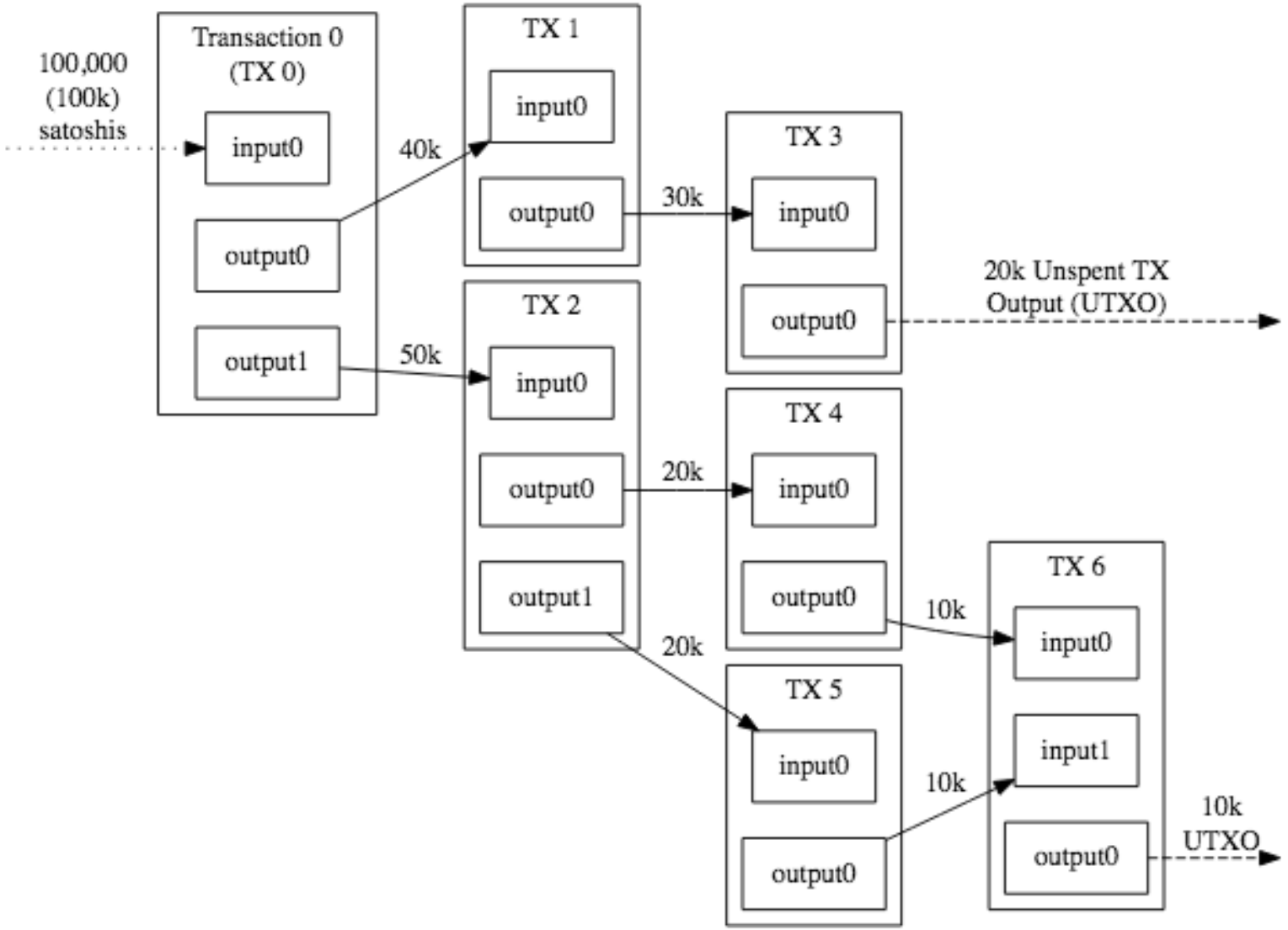
Transazioni Bitcoin: contabilità a tripla voce

- 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"
- Potrebbero esserci degli avanzi, intesi come "mancia" per i minatori (commissioni di transazione)
- (Un satoshi è un centomilionesimo di un bitcoin. 1 satoshi = 10^{-8} BTC; 1000 satoshi = 0,43 €)



Transazioni

- Le transazioni formano un grafico aciclico diretto (DAG)
- 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 1.200.000.000 di TX, finora (vedi qui)
- **Tutte le transazioni sono aperte all'ispezione di tutti!**



Triple-Entry Bookkeeping (Transaction-To-Transaction Payments) As Used By Bitcoin

Transaction View information about a bitcoin transaction

447cb6623db32b5f28c94ac10551802075f053208fe995204a145197e2904bb9

3Nxwenay9Z8Lc9JBiywExpnEFiLp6Afp8v (44,000 BTC - Output)	3LrLWTSdd69oZVVQ6dtWaAAaBLn7N3rRjz - (Spent)	333.33328889 BTC
	3QkXtcSWJA9w77eCujnMBKDWFe7F7zwxTg - (Spent)	333.33328889 BTC
	3Qd7hXZoZ1iyXZznrbdUwUQBxHMmujdqhJ - (Spent)	333.33328889 BTC
	3ECJwvx9VgfotcUuEJMVNvmWnTGVMk179L - (Spent)	333.33328889 BTC
	3BuQmbmdce3e31GEovq5SgowLdfMgJzLDE - (Spent)	333.33328889 BTC
	3NwKLjJjzXSnBFQWokXRgBG3JeuF3bsnfE - (Spent)	333.33328889 BTC
	3GEaT8ZRXELcjMSFvGro6eZcC5S1LSLZuN - (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
	37WSkANPVUQ8uuktf8hv671CejRtBtQ4tJ - (Spent)	333.33328887 BTC
	3EEwPZZ6pYRJSotCz9RBoVYPRnoWyGWEka - (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 tassa 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

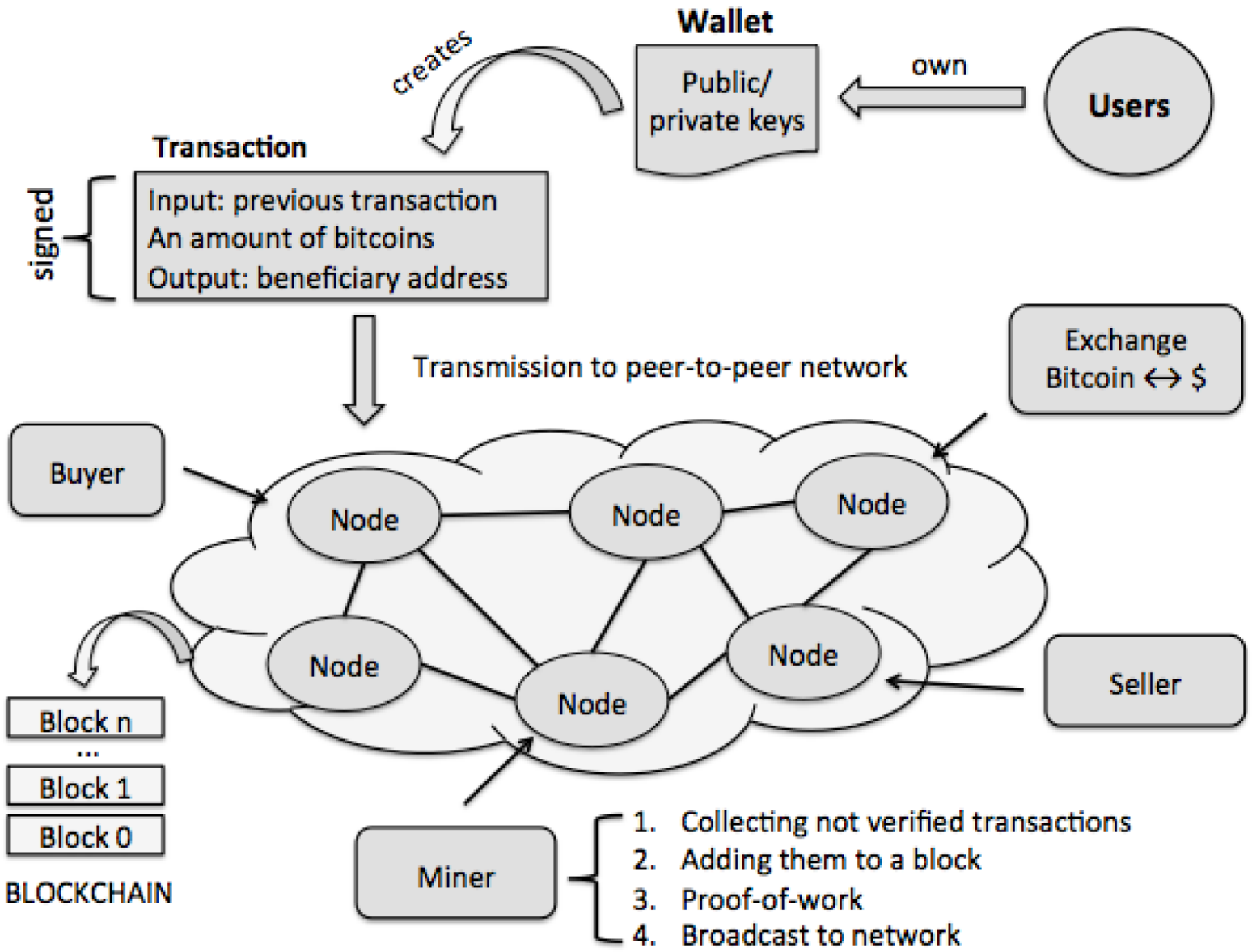
Identità in Bitcoin: *pseudonimato*, non anonimato

- **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)

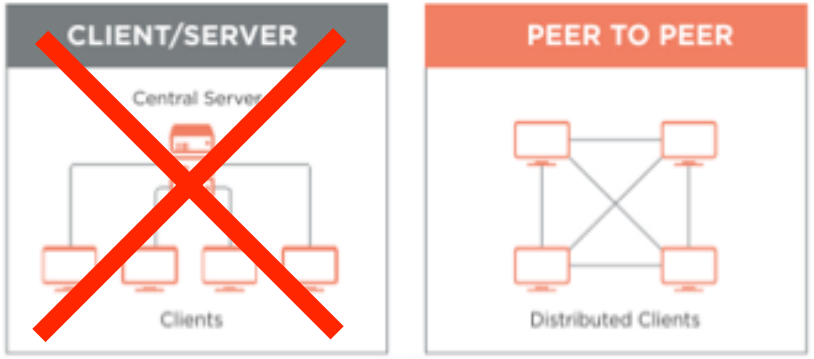
Cos'è Blockchain, in una diapositiva

- **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)

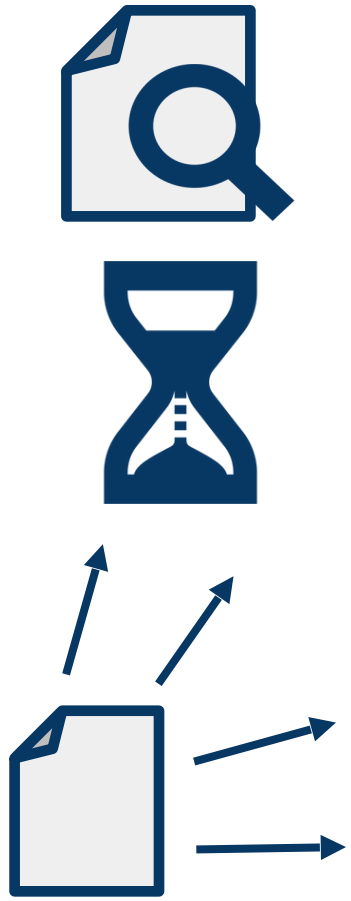
- Dove conserviamo queste transazioni?
- Abbiamo bisogno di un **libro mastro permanente**
  - Risolto in un sistema veramente distribuito
  - Sicurezza crittografica
  - Incentivi economici sinergici
- Non supportato da alcuna autorità centrale (governo o organizzazione)
  - Nessuna necessità di intermediari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



Verifica delle transazioni in un sistema Proof-of-Work

Dave è un miner: il suo lavoro è convalidare le transazioni

1. Raccoglie un po' di transazioni in sospeso (dal *mempool*)
2. Controlla le transazioni rispetto alla sua copia della blockchain per assicurarti che siano legittime
3. Cerca la soluzione ad un dato puzzle matematico (proof-of-work).
   - In Bitcoin, questo si chiama *mining,* e prende molto tempo e energia.
4. Solo dopo aver trovato la soluzione, può annunciarla alla rete, insieme al blocco delle transazioni verificate (tra queste, anche il suo premio).



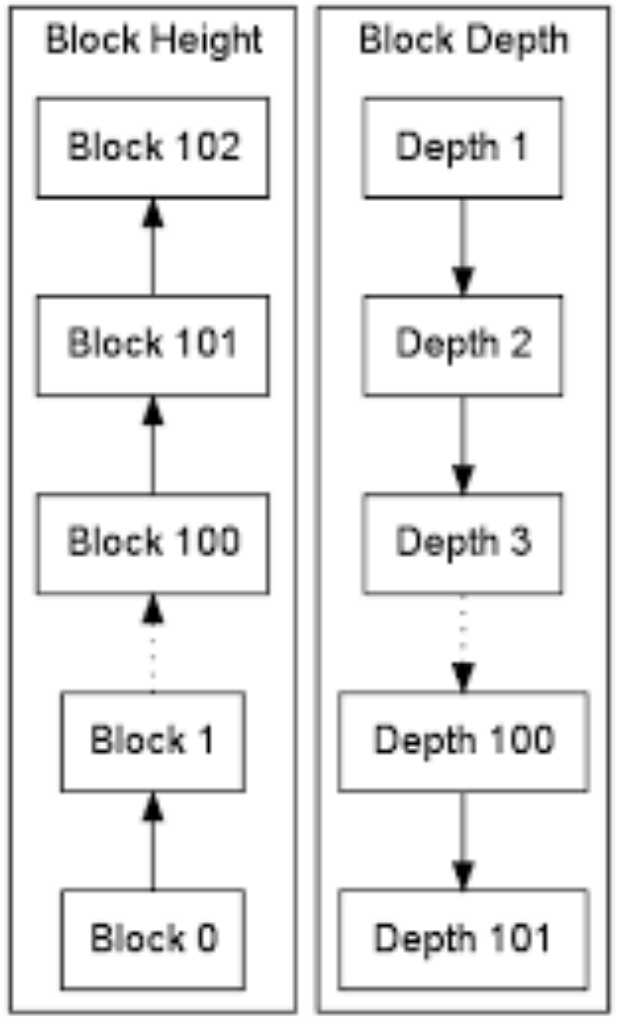
Tutti gli altri nodi, quando ricevono un blocco:

1. Controllano che le transazioni siano legittime e Dave ha effettivamente trovato una soluzione per il puzzle.
2. Se tutto va bene, aggiunge il blocco alla blockchain

Dave ottiene una ricompensa (quindi Proof-of-work è una "gara")

Validated blocks = the Blockchain

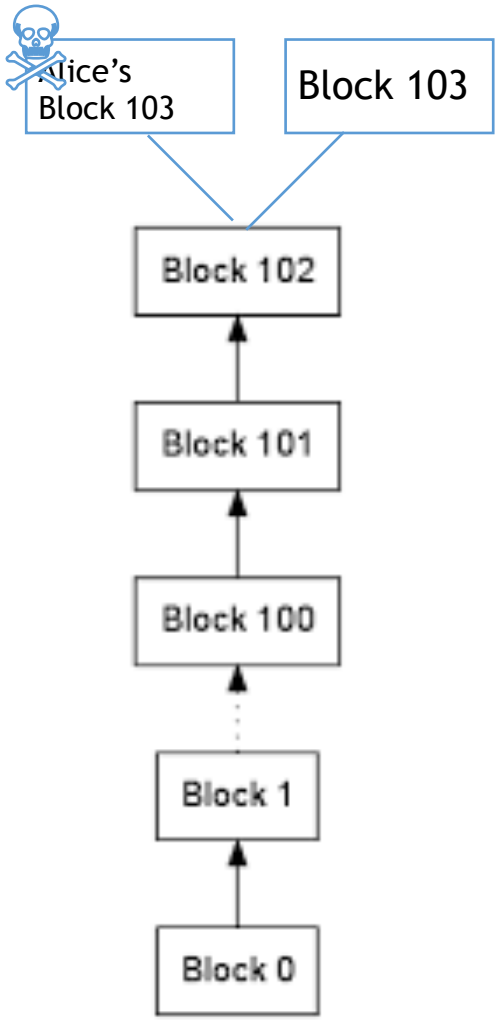
- Each time a valid block is found by some miner, it is broadcast to the whole network, and each node add it to its copy of the ledger
- Each block references a previous block, hence the whole set of blocks is called blockchain
  - Each block has height and depth (confirmations)
    - The deeper is a block, the more confirmation it has got
  - Currently 825k blocks…and counting
- Not all nodes are involved in mining: most nodes just wait for the others to solve the puzzle and announce the block
  - These nodes just keep a local copy of the blockchain.



Block Height Compared To Block Depth

Perché la prova del lavoro impedisce gli attacchi??

- Supponiamo che un gruppo disonesto di minatori (la banda di Alice) cerchi di annunciare un nuovo blocco, forse contenente alcuni dati 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 collettiva messa nella ricerca!
- 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

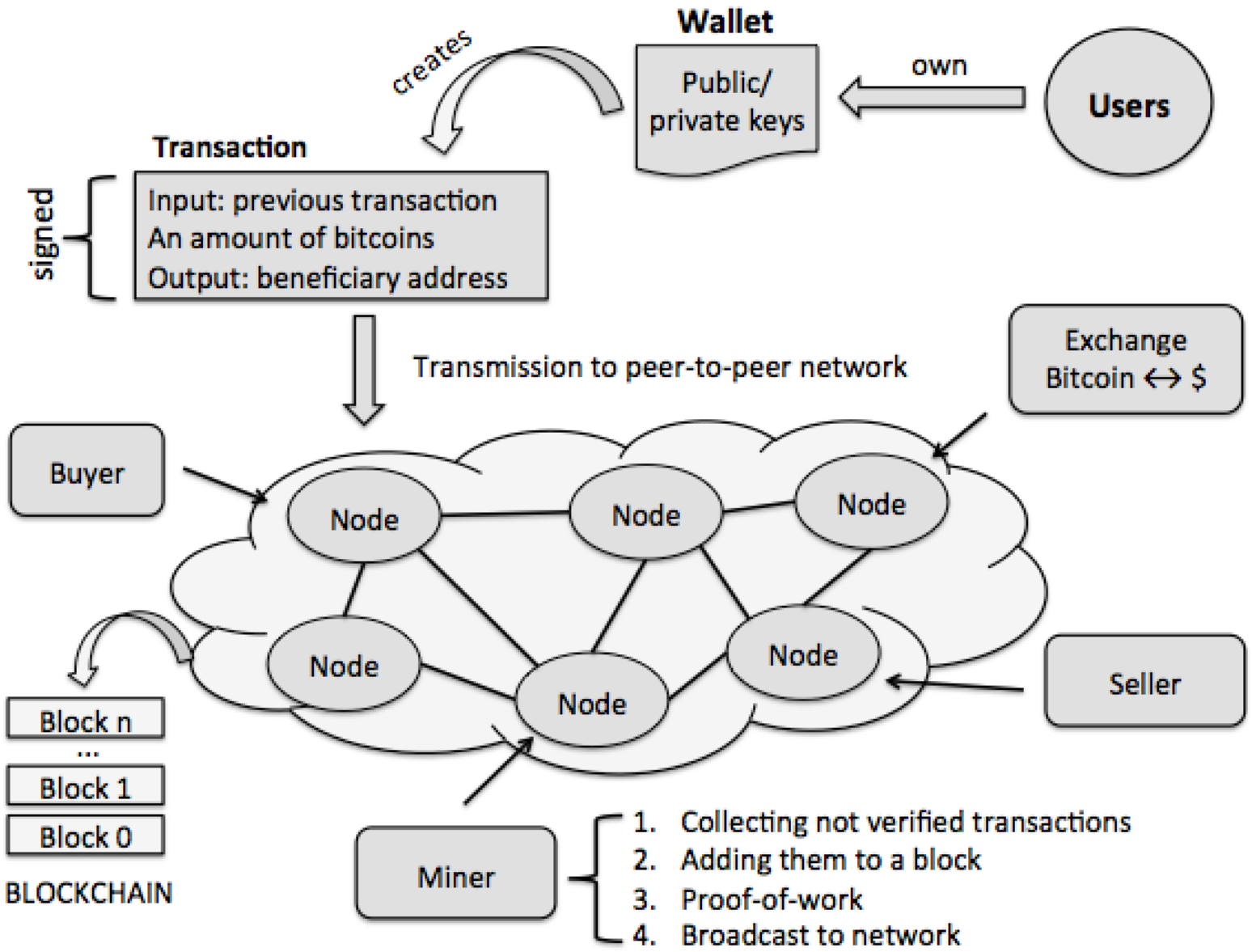
- Quindi, alla fine la blockchain conterrà solo blocchi estratti dalla **maggioranza computazionale** della rete

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.

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



Altri usi della tecnologia Blockchain

- Registri
- 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*

ethereum.org

- I **contratti** sono i principali elementi costitutivi di Ethereum.
- Un contratto è un programma per computer che vive all'interno della rete Ethereum distribuita e ha il proprio bilancio ether, memoria e codice.
- Scritto in linguaggi immediatamente familiari a qualsiasi programmatore (ad esempio, Solidity)
- Ogni volta che invii una transazione a un contratto, esegue il suo codice, che può memorizzare dati, inviare transazioni e interagire con altri contratti.
- I contratti sono mantenuti dalla rete, senza alcuna proprietà o controllo centrale.
- I contratti sono alimentati da Ether, il criptofuel di Ethereum.
- Applicazioni infinite!
- In particolare, token non fungibili: NFT può rappresentare un oggetto digitale unico, scambiabile ma non intercambiabile

Grazie per l'attenzione

marino.miculan@uniud.it