Blockchain & Smart Contracts

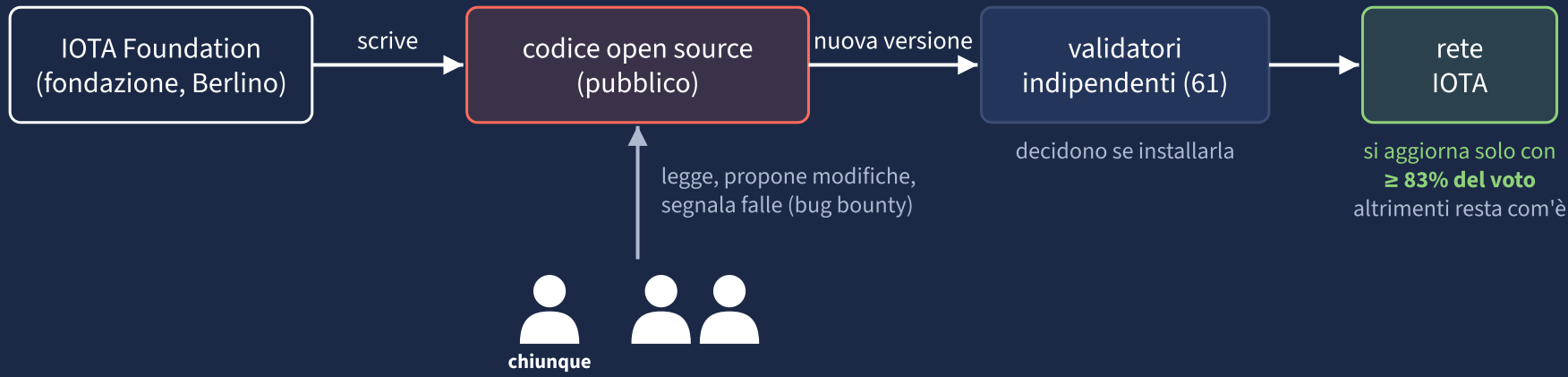
Sem. Blockchain e Smart Contract: aspetti giuridici e tecnologici · Università di Bologna, novembre 2026

Mirko Zichichi
mirko.zichichi@iota.org

IOTA

Chi sono

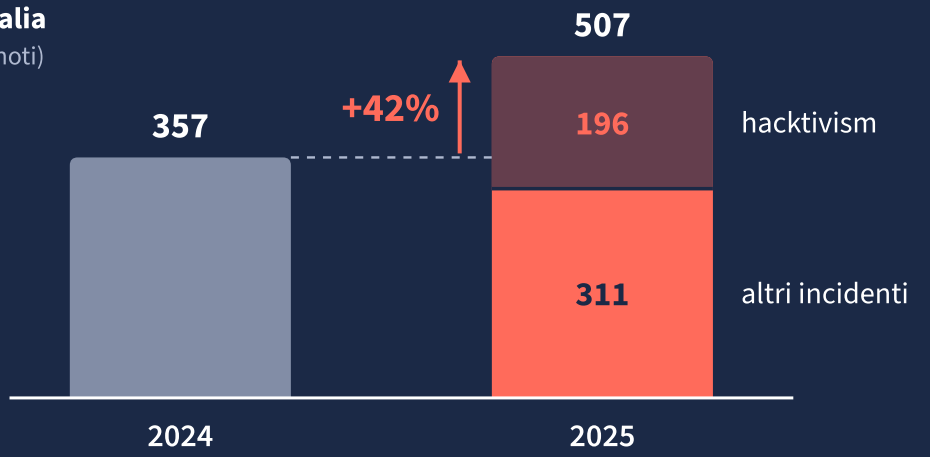
Mirko Zichichi, mirkozichichi.me: Engineering Team Lead alla IOTA Foundation, dottorato in Law, Science and Technology.



la fondazione scrive il software, ma non comanda la rete

L’Italia nel mirino: i numeri

Incidenti gravi in Italia
fonte: Clusit (incidenti noti)



senza hacktivism
+12%
(in entrambi gli anni)

E il 2026? Nei primi nove mesi il CSIRT Italia dell'ACN ha gestito più eventi che in tutto il 2025 (2.729, di cui 615 incidenti).

Rapporto Clusit 2026 (17 marzo 2026); Relazione annuale ACN 2025; Operational Summary ACN 2026.

Clusit: Associazione italiana per la sicurezza informatica
ACN: Agenzia per la cybersicurezza nazionale; **CSIRT** (Computer Security Incident Response Team): la sua squadra di risposta agli incidenti

Le cinque proprietà, con i fatti di quest’anno

Riservatezza

solo chi è autorizzato legge

uno spyware legge le chat di un giornalista

Integrità

nessuno modifica senza permesso

qualcuno cambia da remoto la temperatura dei frigoriferi

Disponibilità

il servizio c'è quando serve

il sito della Farnesina sommerso di richieste

Autenticità

sai con chi stai parlando

la voce clonata di un ministro chiede soldi

Non ripudio

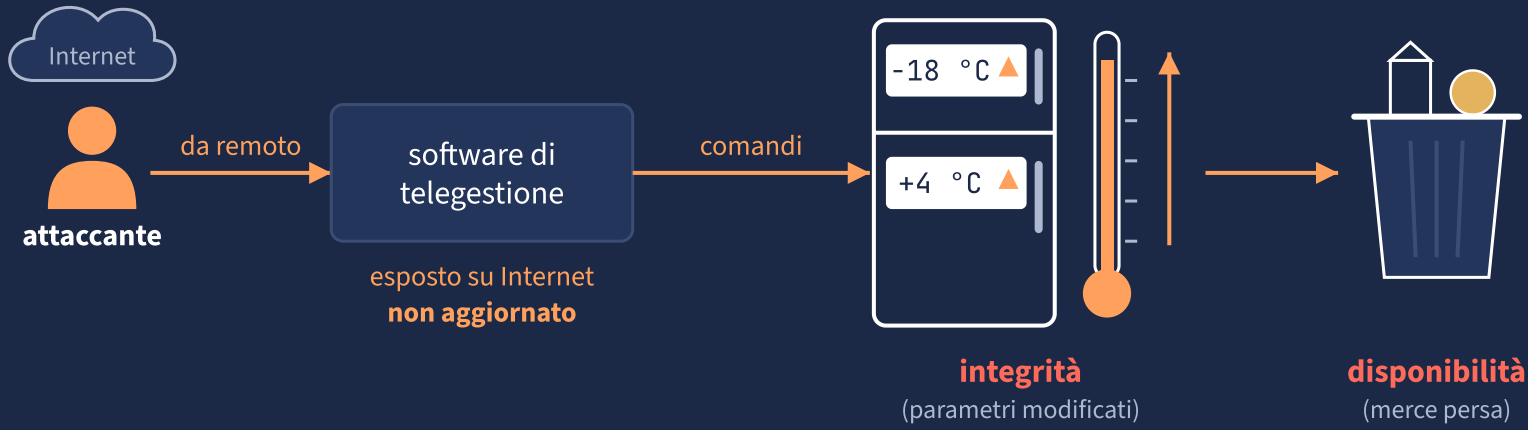
chi ha firmato non può negarlo

un bonifico firmato con la tua chiave è tuo: non puoi dire «non sono stato io»

Le prime quattro le vediamo violate nelle notizie; la quinta è quella su cui si regge una blockchain.

2 novembre 2026: i frigoriferi dei supermercati

Alle 4 del mattino qualcuno alza da remoto la temperatura dei frigoriferi in oltre 20 supermercati, da Palermo a Trapani.

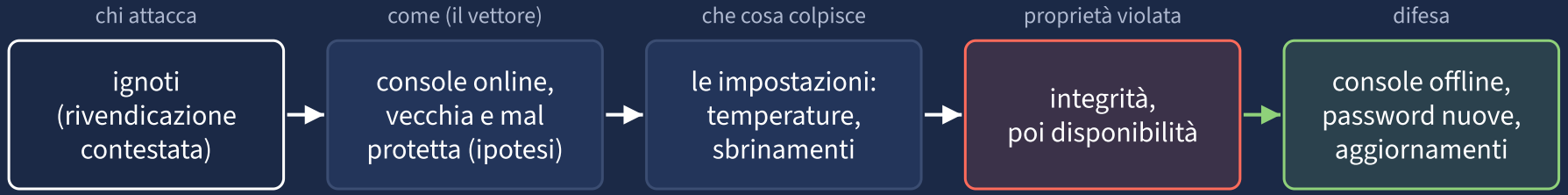


In Europa oltre 100 supermercati colpiti; la rivendicazione filorussa è **contestata** da esperti e ACN.

Il Post, 3 e 6 novembre 2026; bollettino ACN per la filiera del freddo.

Frigoriferi: perché ha funzionato

- Colpiti almeno 4 Coop del Gruppo Radenza e alcuni Decò; casi anche in Toscana e in provincia di Trento
- In Francia, a ottobre, circa 700 supermercati: impianti vecchi, console raggiungibili da Internet, password deboli



Un dato alterato diventa un danno fisico. Ogni apparecchio connesso fa parte del sistema: se nessuno lo aggiorna, diventa la porta d'ingresso.

Il Post, 3 e 6 novembre 2026; Cybersecurity360 sul bollettino ACN.

Un anno di attacchi: proviamo a classificarli

Per ogni notizia: quale proprietà della sicurezza è stata violata? Cliccate su una scheda.

2 nov 2026 ✓ confermato

Frigoriferi manomessi nei supermercati, da Palermo a Trapani

Temperature alzate da remoto in oltre 20 punti vendita in Sicilia e in altre regioni,…

Violate: integrità disponibilità

art. 14 Cyber Resilience Act — Il Post, 3/11/2026

8 ott 2026 ✓ confermato

Attacco al sito della Farnesina

Un attacco DDoS, attribuito dalla stampa al gruppo filorusso NoName057(16), viene…

Violate: disponibilità

d.lgs. 138/2024, art. 25 — Open, 8/10/2026

4 feb 2026 ✓ confermato

Milano-Cortina: attacchi ai siti dei Giochi

Il governo dichiara sventati attacchi di origine russa a sedi diplomatiche e a siti legati alle…

Violate: disponibilità

L. 90/2024 (cybersicurezza) — The Record, 5/2/20…

5 mar 2026 ✓ confermato

Spyware Paragon: le procure confermano

Le procure di Roma e Napoli trovano tracce di malware sui telefoni di due attivisti e del…

Violate: riservatezza integrità

art. 615-ter c.p. (accesso abusi… — Internazion…

feb 2025 ✓ confermato

La voce clonata del ministro Crosetto

Con una voce ricreata al computer, truffatori ottengono da un imprenditore circa 980.000 …

Violate: autenticità

artt. 640 e 494 c.p. — Il Post, 11/2/2025

29 ott 2026 ✓ confermato

Binance: rubati 6,3 miliardi di dollari in criptovalute

Tutto parte da un falso colloquio di lavoro: un malware, le credenziali degli ingegneri, poi g…

Violate: riservatezza integrità

Reg. (UE) 2023/1114, art. 75 — Il Post, 3/11/2026

8 ottobre 2026: il sito della Farnesina

- Il sito del ministero degli Esteri riceve un’ondata di richieste: le difese la respingono «senza provocare disservizi»
- Arriva dopo dure parole di Mosca contro il ministro Tajani; la stampa lo attribuisce a NoName057(16)

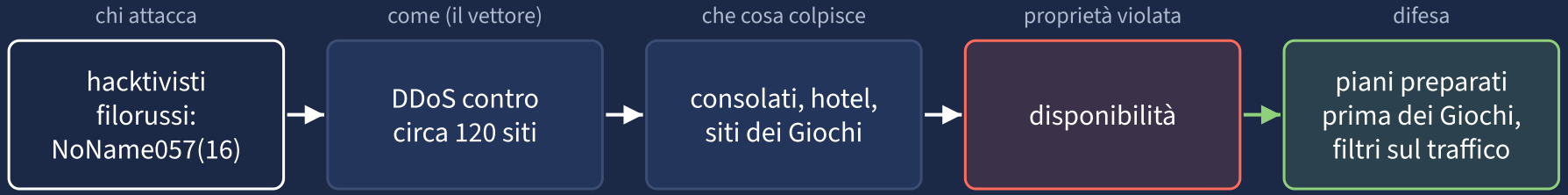


Un **DDoS** (*Distributed Denial of Service*) non entra nei sistemi e non ruba dati: li rende irraggiungibili. Non lo ferma la crittografia, ma la capacità di assorbirlo.

Open, 8 ottobre 2026.

Milano-Cortina, febbraio 2026: gli attacchi ai Giochi

- Alla vigilia dei Giochi il governo dichiara sventati attacchi di «origine russa» a sedi diplomatiche all'estero e a siti delle Olimpiadi, tra cui hotel di Cortina
- NoName057(16) rivendica: «support for Ukrainian terrorists is punished with our DDoS attacks»

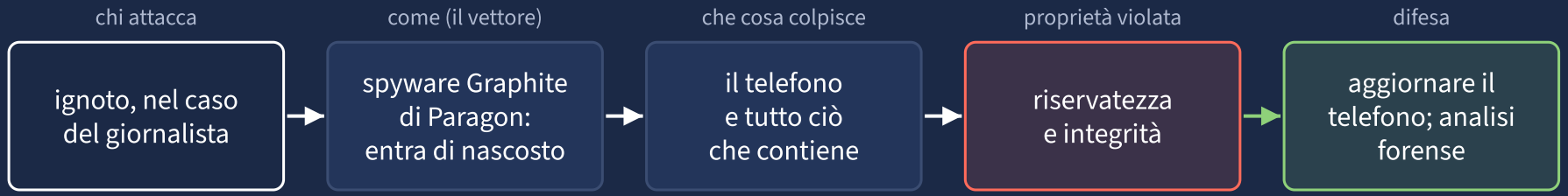


Hacktivism: attacchi per una causa politica, che cercano visibilità più che denaro. In Italia, nel 2025, 196 incidenti gravi su 507 (Clusit).

Attribuire un attacco è difficile: né la dichiarazione di un governo né una rivendicazione sono prove tecniche.

Paragon: lo spyware nel telefono

- Marzo 2026: le procure di Roma e Napoli trovano tracce di malware su tre telefoni: gli attivisti Luca Casarini e Giuseppe Caccia e il giornalista Francesco Cancellato (Fanpage)
- Per Casarini e Caccia le operazioni risultano dell'intelligence italiana; per Cancellato no: chi lo ha spiato resta ignoto

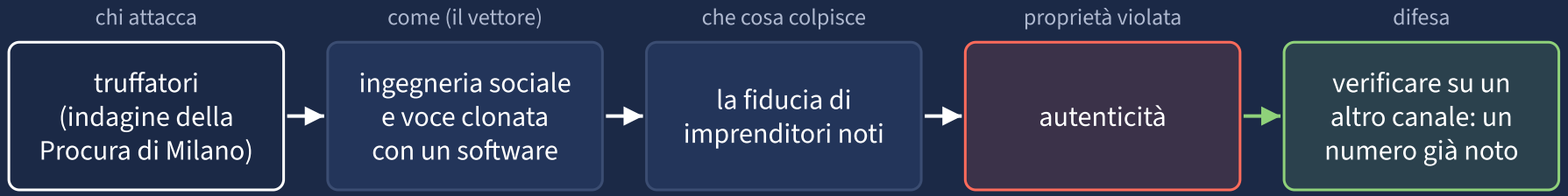


La cifratura *end-to-end* protegge il messaggio in viaggio, non il telefono: chi controlla il dispositivo legge prima che il messaggio sia cifrato.

Nota congiunta delle procure, 5 marzo 2026; Internazionale, 12 marzo 2026.

La voce clonata del ministro Crosetto

- Febbraio 2025: truffatori si fingono lo staff del ministro della Difesa e, almeno una volta, Crosetto stesso, con la voce riprodotta da un software
- Chiedono a imprenditori soldi per un falso riscatto di giornalisti rapiti: Massimo Moratti versa circa 980.000 € su un conto olandese, poi bloccati dalla Procura di Milano

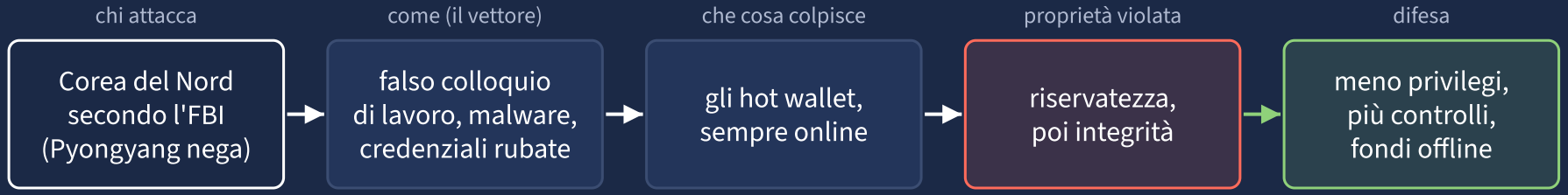


Autorità e urgenza (un ministro, un rapimento) sono le leve classiche dell'ingegneria sociale: spingono a saltare i controlli.

Una voce o un numero di telefono non provano l'identità: si imitano. Serve qualcosa che l'impostore non può copiare, come una chiave (Capo II).

Binance, 29 ottobre 2026: il furto più grande

- In circa quattro ore escono dagli *hot wallet* del più grande exchange di criptovalute circa 6,3 miliardi di dollari
- Era cominciato a settembre: un ingegnere, contattato su un sito di annunci, scarica il «compito» di un falso colloquio, con un malware che l'antivirus non riconosce
- Per l'FBI è stata la Corea del Nord, che smentisce; 2,85 miliardi sono stati congelati, il resto Binance lo copre con fondi propri



Anche qui l'anello debole è una persona (Capo I). E chi controlla chiavi e permessi di un wallet ne controlla i fondi: lo riprendiamo nel Capo V.

Il Post, 3 novembre 2026; CoinDesk, 3 novembre 2026; FBI, 31 ottobre 2026.

FBI: Federal Bureau of Investigation, la polizia federale statunitense

Sei notizie, cinque proprietà



Il percorso di oggi

I Sicurezza informatica

II Concetti di base: hash e firma

III Sistemi distribuiti e blockchain

IV Creare una transazione

V Smart contract

VI Tokenomics e monete digitali

Capo I

Sicurezza informatica

Cosa vogliamo proteggere, da chi, e perché non basta mai

La sicurezza informatica

Proteggere le risorse informatiche da accessi, usi, alterazioni o distruzioni non autorizzati.

Sicurezza fisica

protegge i dispositivi e i locali



porte blindate, allarmi, casseforti

Sicurezza logica

protegge le informazioni



crittografia, password, firma elettronica

Non esistono sistemi sicuri

per chi vuole violare il sistema:

tempo necessario

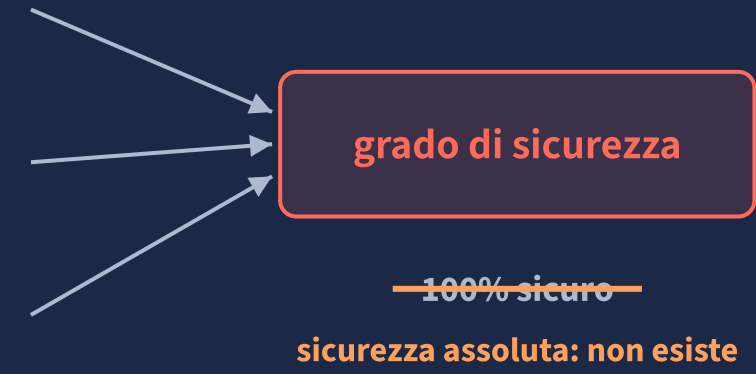
più è lungo, più è sicuro

investimento necessario

più è alto, più è sicuro

probabilità di successo

più è bassa, più è sicuro



- Più un sistema è complesso, più punti deboli ha: togliere tutto ciò che non serve (*Keep It Simple, Stupid*)
- Un sistema sicuro oggi può non esserlo domani: va aggiornato

Kerckhoffs: tutto pubblico, tranne la chiave

> *"Un sistema crittografico deve essere sicuro anche se tutto, tranne la chiave, è di pubblico dominio."* *A. Kerckhoffs, 1883*

il progetto (l'algoritmo)



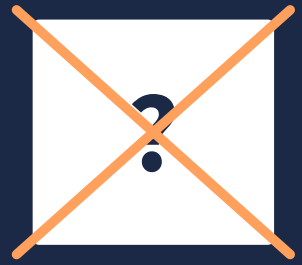
pubblico: lo vedono tutti, anche Eve

la chiave



solo la chiave è segreta

il contrario: progetto segreto



«security by obscurity»

prima o poi trapela



Auguste Kerckhoffs (1835–1903)

È la regola delle blockchain: il codice di Bitcoin, Ethereum e IOTA è pubblico; i fondi li protegge solo la chiave privata.

L’anello umano: le password

Le più usate in Italia

1. admin
2. password
3. 123456
4. Password
5. 12345678
6. 123456789
7. 12345
8. Napoli1926
9. 123stella
10. perlanera

NordPass, edizione 2025 (violazioni pubbliche tra settembre 2024 e settembre 2025).

Quasi **un utente su tre** usa una delle 10.000 password più comuni.

Un attaccante le prova tutte in una frazione di secondo.

M. Burnett, *10,000 Top Passwords*, 2011, su 6,5 milioni di credenziali trapelate.

Proviamo: che password usi?

Prova una password

`juventus1897`

La password non lascia questo computer: il calcolo avviene nel browser.

Caratteri usati: ✓ **minuscole** (26) – maiuscole (26) ✓ **cifre** (10) – simboli (33)

Alfabeto e lunghezza	36 simboli possibili, 12 caratteri
Combinazioni	$36^{12} \approx 4{,}74 \times 10^{18}$
Forza bruta, caso peggiore	**15 anni** a 10^{10} tentativi al secondo
Password molto diffuse	✕ **parola della lista + numeri**

> ✕ **Parola comune + numeri: un attacco a dizionario la prova presto.**

Anche i dati personali aiutano: con nome, data di nascita e una password trapelata altrove si indovina in 100 tentativi la password di oltre il 73% degli utenti (Wang et al., ACM CCS 2016).

ACM CCS: la conferenza sulla sicurezza informatica dell'Association for Computing Machinery

L’attacco a dizionario

Invece di provare tutte le combinazioni, si provano prima le password più diffuse.

Account **`avv.bianchi`** hash della password rubato dal database: `a941a4c4fd…f6c223`

L'attaccante calcola l'hash di ogni parola del dizionario e lo confronta con l'hash rubato.

Tentativi: **20** su 64 parole del dizionario

```
tentativo 16: 000000 → 91b4d1… ✗
tentativo 17: qwerty123 → daaad6… ✗
tentativo 18: zaq12wsx → e3e93b… ✗
tentativo 19: dragon → a9c43b… ✗
tentativo 20: sunshine → a941a4… ✓
✓ trovata: sunshine (tentativo 20)
```

Difese (NIST, 2025): rifiutare le password comuni o già trapelate, limitare i tentativi, almeno 15 caratteri.

NIST: National Institute of Standards and Technology, l'ente federale statunitense che scrive gli standard di sicurezza

Phishing: la password te la consegnano

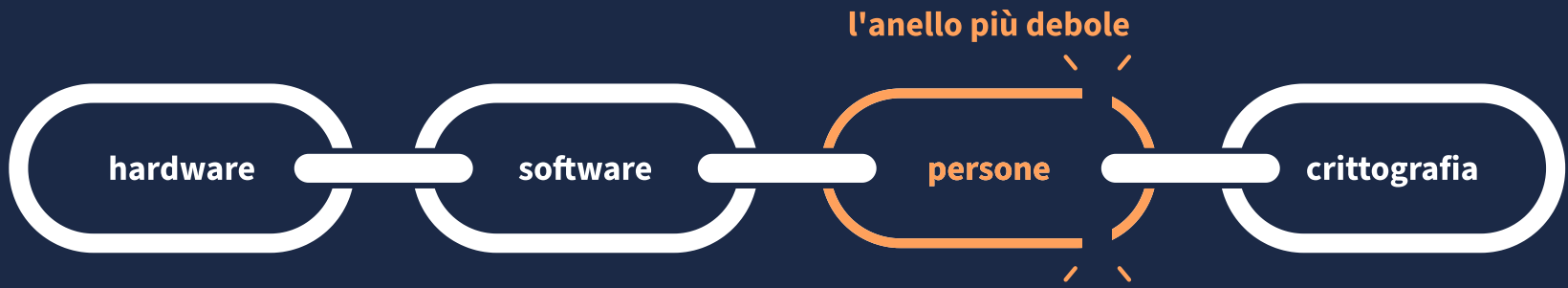


L'esca non è solo un'email: nel caso Crosetto era una voce al telefono.

Video: una scena di phishing dalla serie *Mr. Robot*, youtube.com/watch?v=JMYEr4Bgey4

L’anello più debole

> *"Security is a chain; it's only as secure as the weakest link."* *B. Schneier, Secrets and Lies, 2000*



la sicurezza è una catena: forte quanto l'anello più debole

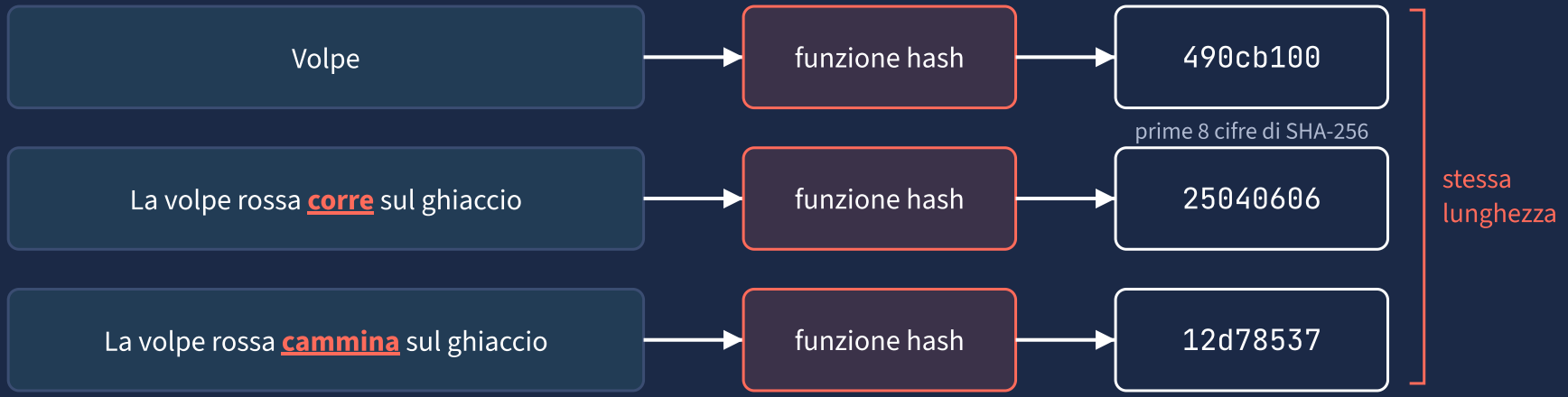
Spesso l'anello debole è una persona: le regole vanno pensate per persone vere, sotto pressione.

Capo II

Concetti di base

Integrità e non ripudio: le due proprietà su cui si regge una blockchain

Hash: l’impronta che rivela ogni modifica



lunghezza fissa, nessuna somiglianza

basta cambiare una parola e l'uscita cambia del tutto

Integrità: cambia una lettera, cambia tutta l'impronta. Chi conserva l'impronta si accorge di qualsiasi modifica.

Nella blockchain ogni blocco contiene l'impronta del precedente: la storia non si può riscrivere di nascosto.

SHA-256: Secure Hash Algorithm, con impronte di 256 bit

Proviamo: moat o maot?

Testo A

moat

`edf1eb932299d2c1e3c973f57e454fbdf5aceeed86bae113708c69d9adc737f4`

Testo B

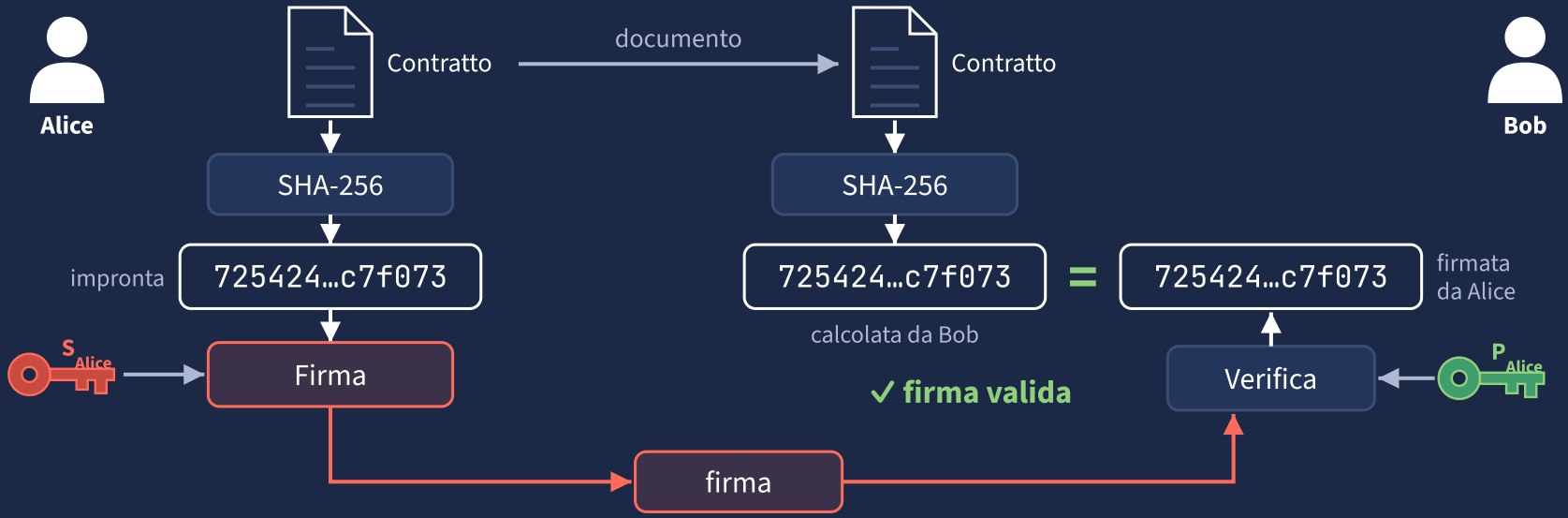
maot

`b075b42502 5fab0e0d45a491b5ddb4d42b6c 872f5a2c5f69e32996f9 e90b8f0b`

Bit diversi: **141** su 256 (55%)

Due lettere scambiate: cambia circa metà dei 256 bit.

Firma: chi ha firmato non può negarlo



Non ripudio: solo chi ha la chiave privata produce quella firma; chiunque la verifica con la chiave pubblica.

Firma: una modifica si vede



La firma resta legata a **quel** documento: una transazione firmata non si può ritoccare.

Proviamo: firmare e verificare

Alice firma

Documento di Alice

Alice paga 5 a Bob

1. Alice calcola l'impronta (SHA-256)

Impronta: `be4ae55aa9f1f82be73ff885d60ea2fb97280da4d03997d80c5a972e8780cfa6`

2. Alice firma con la sua chiave privata

Firma: `38974f2b80b36f…20c6f3`

Bob verifica

Documento ricevuto da Bob

Alice paga 5 a Bob

Chiave pubblica di Alice: `0476868a…6373`

Modifica una parola in transito

3. Bob verifica con la chiave pubblica di Alice

✓ **firma valida: documento integro, firmato da Alice**

Se in transito «5» diventa «6»: ✕ **firma non valida: documento alterato o firmatario diverso**

Integrità e non ripudio insieme: ecco perché una blockchain non ha bisogno di un notaio.

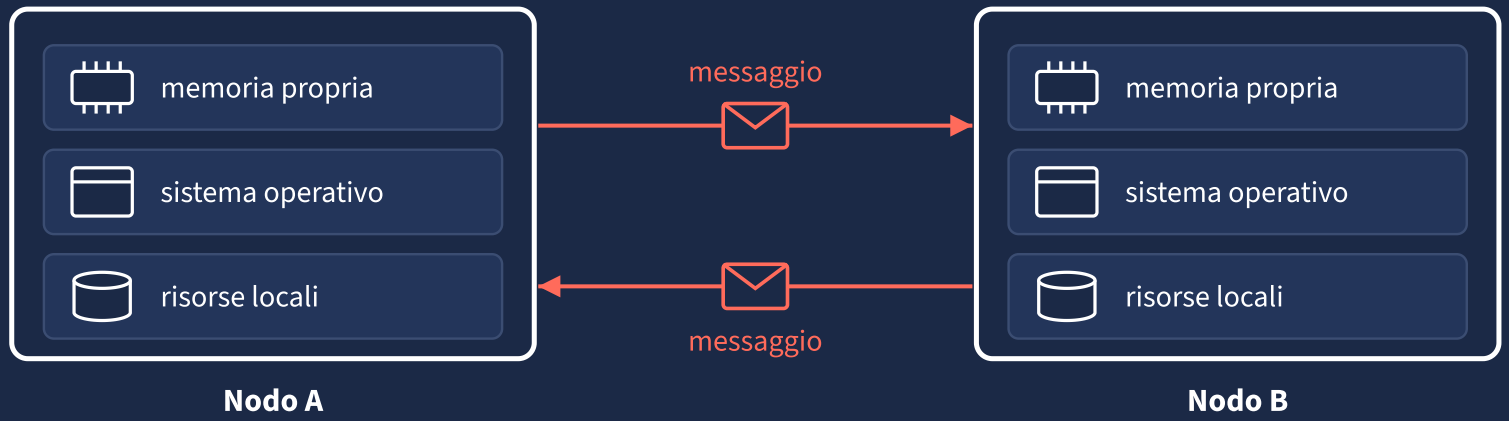
Capo III

Introduzione ai sistemi distribuiti

Dal server unico al registro condiviso

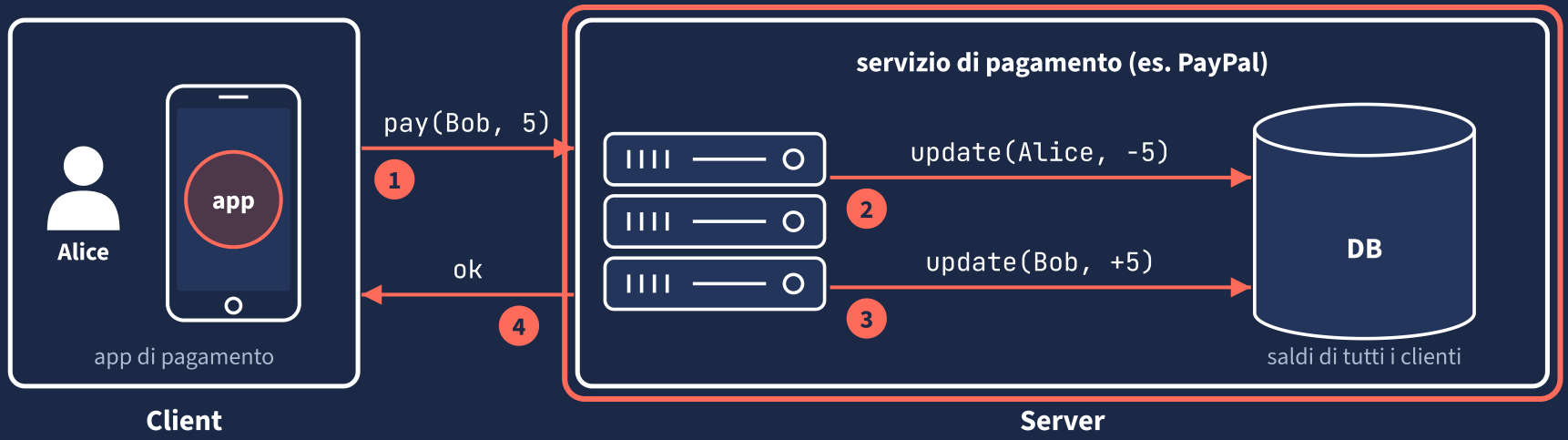
Sistema distribuito: nodi che si parlano

Computer diversi che collaborano scambiandosi **solo** messaggi: nessuna memoria in comune, e ognuno può guastarsi o mentire.



nessuna memoria condivisa: comunicano solo con messaggi

Client/server: Alice paga Bob 5 euro



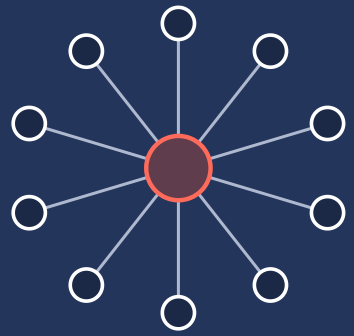
un'unica società custodisce il registro: punto unico di fiducia e di guasto

Il registro dei saldi è di una sola società: va creduta, e se si ferma, si ferma tutto.

DB: database, l'archivio dei dati

Peer to peer: nessuno al centro

Centralizzato



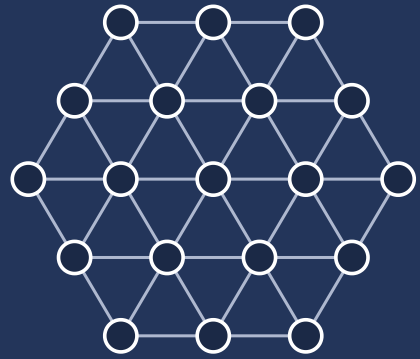
un nodo si occupa di tutto

Decentralizzato



il carico è distribuito
su più sotto-nodi

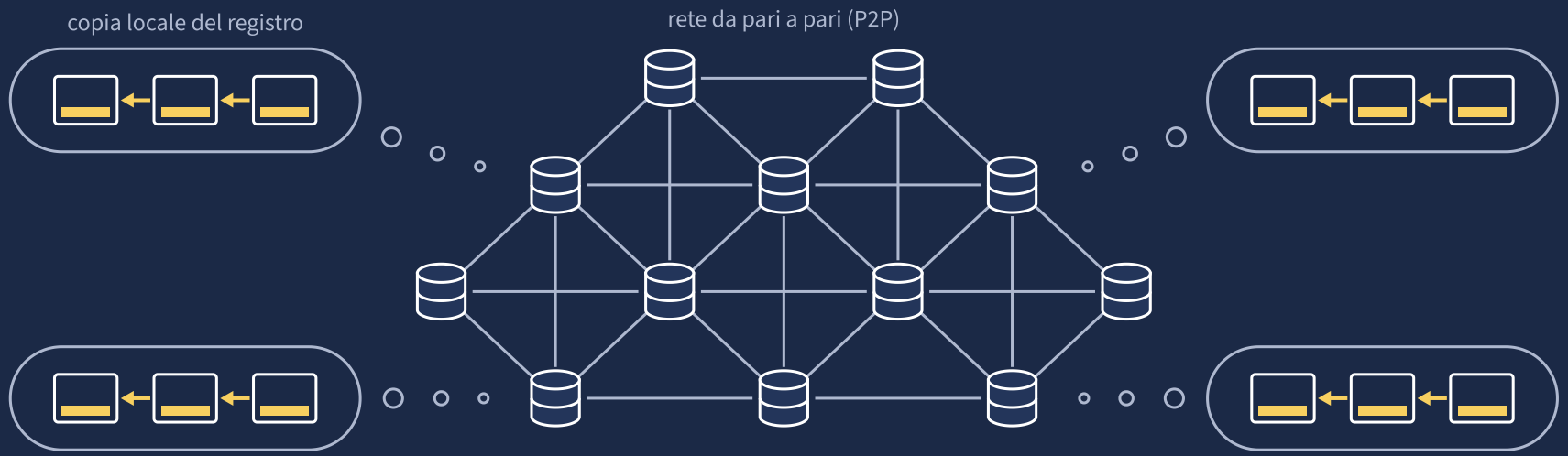
Distribuito (P2P)



tutti i nodi sono pari

Nel *peer to peer* ogni nodo è client e server insieme: non c'è un centro da attaccare o da corrompere.

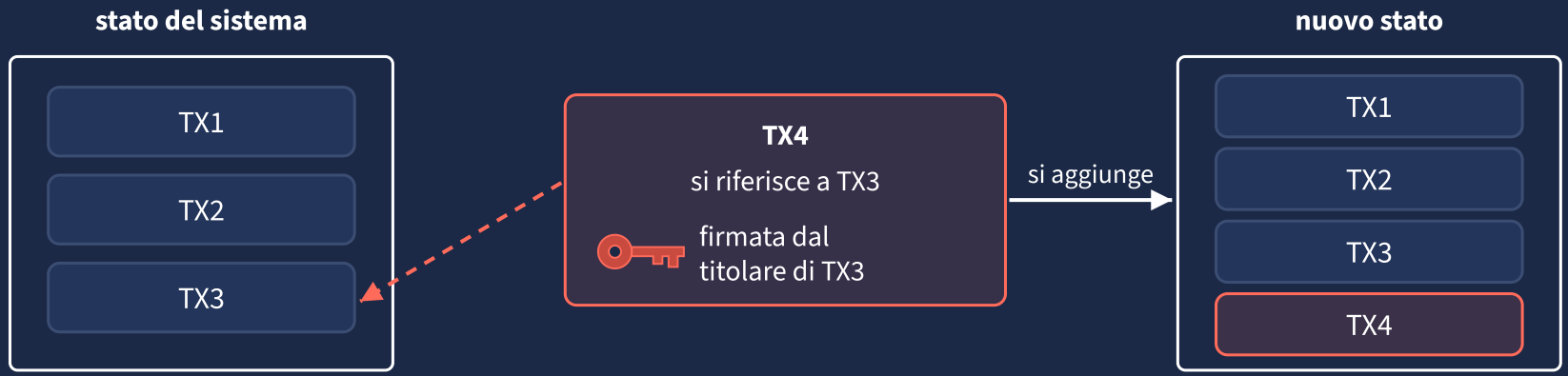
Blockchain: tante copie dello stesso registro



ogni nodo aggiorna la sua copia con lo stesso meccanismo di consenso

Ogni nodo tiene una copia del registro e la aggiorna con le stesse regole: è una *Distributed Ledger Technology* (DLT) a blocchi.

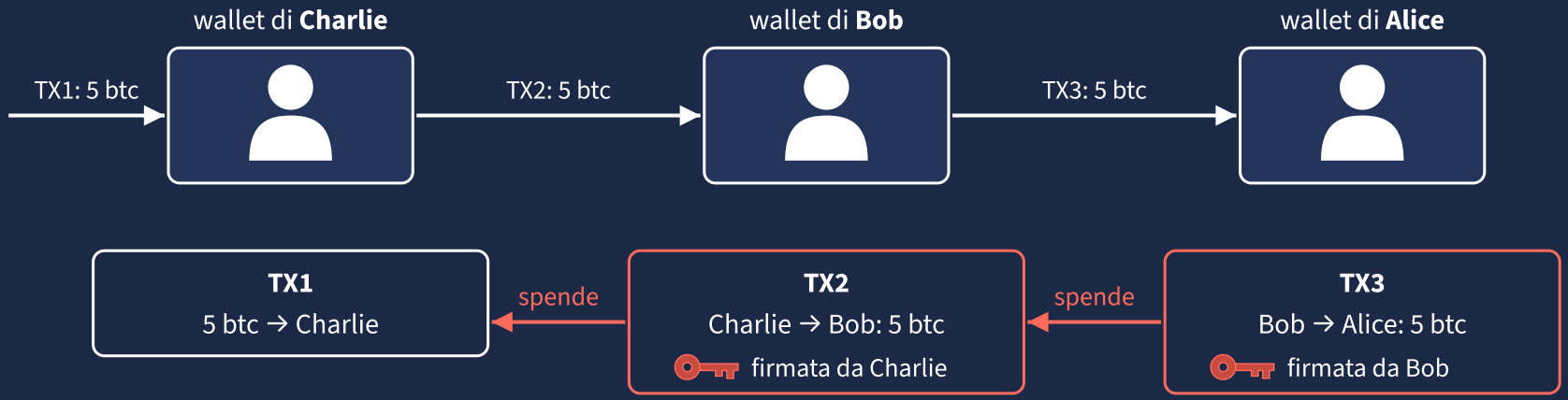
Transazioni



Il registro conserva lo stato; una transazione è l'operazione firmata che lo cambia.

TX: abbreviazione di «transazione»

Transazioni: un esempio



una moneta è una catena di firme: ogni transazione spende la precedente

Transazioni vere

12 gennaio 2009 · blocco 170

Satoshi Nakamoto manda **10 BTC** a Hal Finney

La prima transazione tra due persone. Gli altri 40 BTC della moneta tornano a Satoshi come resto.

22 maggio 2010 · blocco 57.043

Laszlo Hanyecz paga **10.000 BTC** per due pizze

Per pagare unisce 131 «monete» ricevute prima: in Bitcoin i fondi sono come banconote, si spendono intere e si riceve il resto.

Sono ancora lì, leggibili da chiunque: il registro non dimentica e non si corregge.

Dati da mempool.space: transazioni f4184fc5… e a1075db5….

BTC: bitcoin, l'unità della moneta

Blocchi veri

Blocco 0 · 3 gennaio 2009

`0000000000`19d6689c…e26f

«The Times 03/Jan/2009 Chancellor on brink of second bailout for banks»

Il titolo del giornale scritto da Satoshi Nakamoto dentro il primo blocco: una data certa, e un messaggio.

Blocco 840.000

impronta	`00000000000000000000`320283……
prec.	172014…94ab
ora	20/4/2024 00:09 UTC
transazioni	3.050

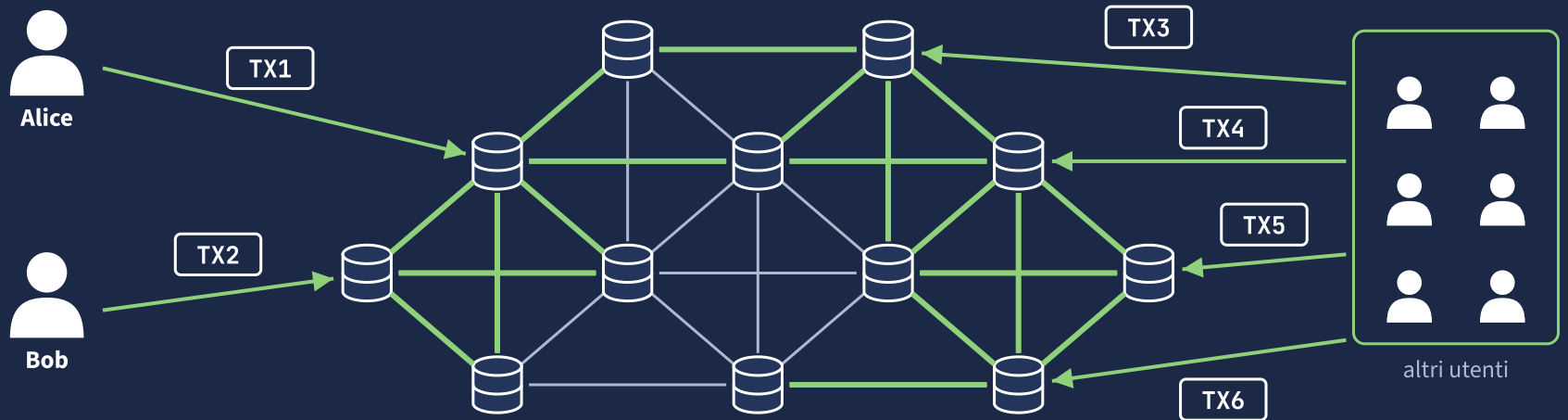
Blocco 840.001

impronta	`00000000000000000000`1b48a7……
prec.	320283…83a5
ora	20/4/2024 00:10 UTC
transazioni	2.823

Ogni blocco scrive l'impronta del precedente: cambiare il blocco 840.000 cambierebbe la sua impronta e romperebbe il legame con il 840.001. Le impronte iniziano con 19 zeri: è la prova del lavoro fatto per trovarle.

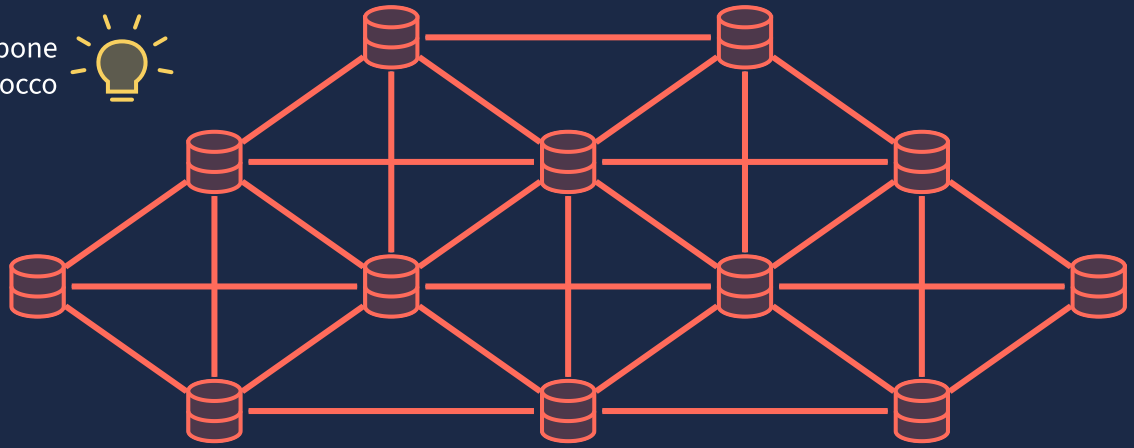
UTC: tempo coordinato universale, l'ora di riferimento mondiale

Registro distribuito: inserimento delle transazioni



Registro distribuito: propagazione di un blocco

un nodo propone
un nuovo blocco



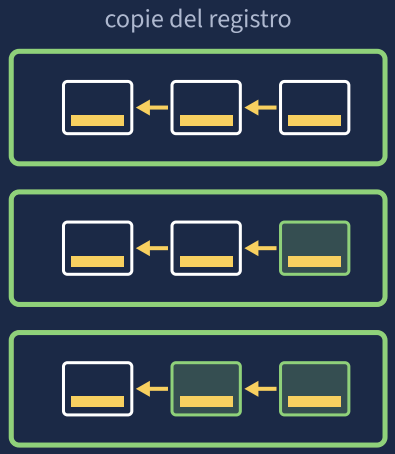
1° passaggio
ai vicini

2° passaggio
ai vicini dei vicini

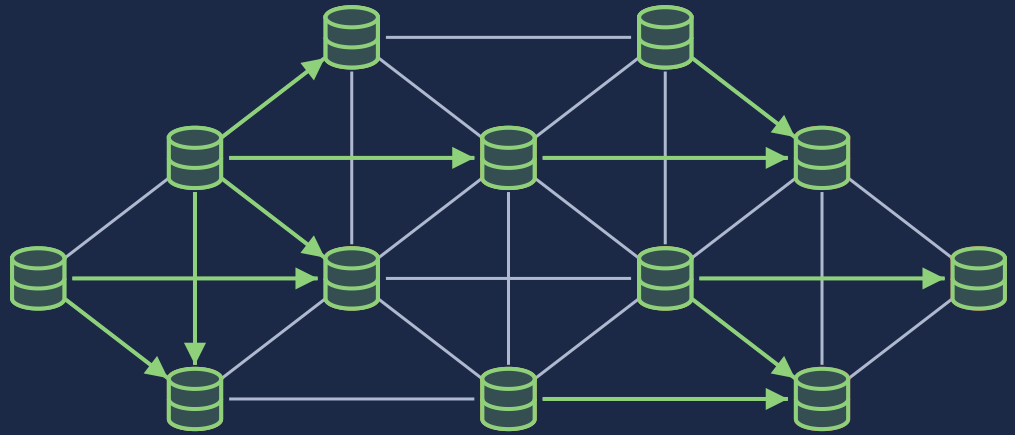
3° passaggio
tutta la rete

ogni nodo controlla il blocco e lo passa ai vicini

Registro distribuito: sincronizzazione

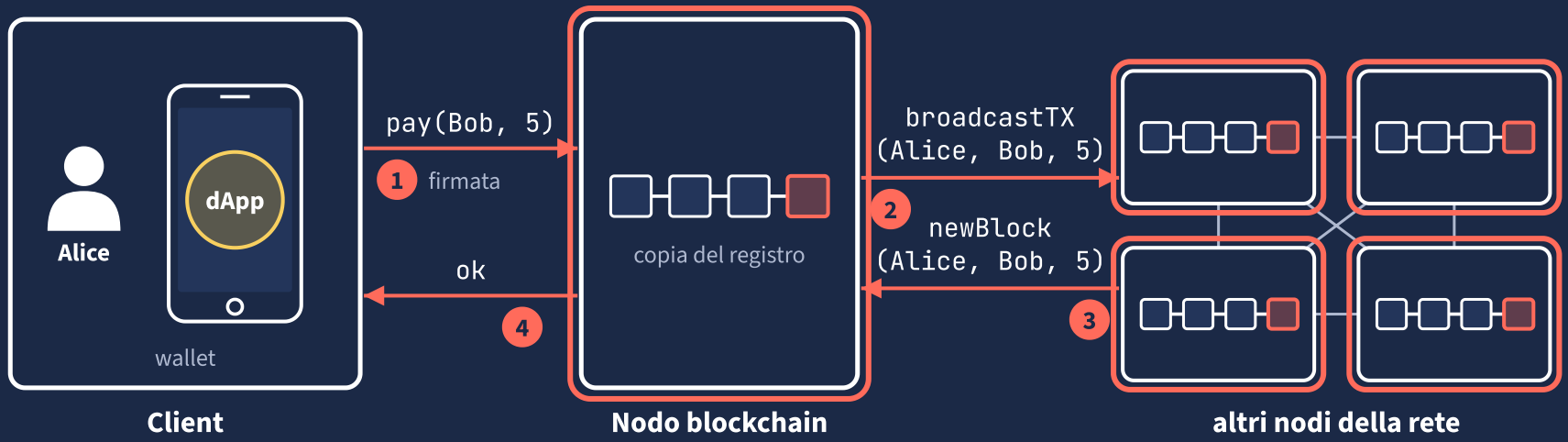


chi è indietro chiede e riceve i blocchi mancanti



✓ **tutti i nodi hanno lo stesso registro**

Alice paga Bob 5 bitcoin



nessuna società custodisce da sola il registro: ogni nodo ne ha una copia

Rispetto al pagamento con PayPal: nessuna società custodisce il registro, e per cambiarlo serve il consenso della rete.

Chi decide qual è il registro giusto?



Il generale 1 sente «attacca» e «ritirata».
Chi mente? Non può saperlo.

La regola Lamport, Shostak, Pease (1982)
con messaggi «orali» (non firmati)

$$n \geq 3f + 1$$

n = generali · f = traditori

più di ⅔ devono essere leali

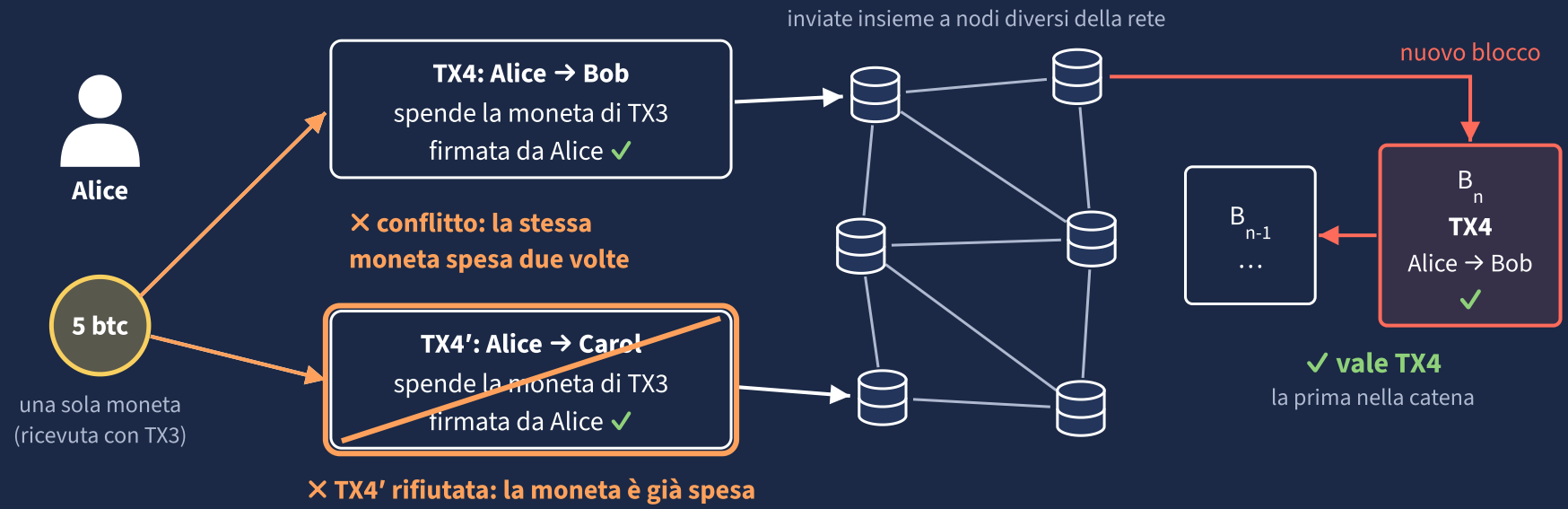
1 traditore: con 3 generali no, con 4 sì

Nella blockchain

validatori = generali
blocchi e voti = messaggi
nodi guasti o disonesti = traditori

Senza un capo, i nodi devono mettersi d'accordo anche se alcuni mentono o sono spenti: è il problema del consenso.

Double spending: perché un bitcoin non si copia



Un file si copia; una moneta no. Prima di Bitcoin serviva una banca a tenere i conti: qui è la rete a decidere quale pagamento è venuto prima.

La catena più lunga vince

- Se due blocchi arrivano insieme, la rete per un attimo si divide in due rami
- I miner continuano sul ramo che vedono per primo: vince quello che si allunga di più
- Per questo un pagamento si considera sicuro dopo qualche blocco in più (**conferme**)

Come aspettare che un assegno sia incassato: gli exchange accreditano i bitcoin solo dopo alcune conferme.

Perché serve la Proof of Work?

- Senza un capo, chi ha il diritto di scrivere il prossimo blocco?
- Votare per account non funziona: chiunque ne crea un milione, gratis
- Allora si fa una **gara che costa fatica**: una lotteria i cui biglietti si comprano con calcoli, cioè con elettricità
- Chi vuole riscrivere la storia deve rifare tutta quella fatica, più in fretta di tutti gli altri insieme

La *Proof of Stake* cambia il biglietto: non elettricità, ma una cauzione in moneta che si perde se si imbroglia (Ethereum dal 2022, IOTA).

Il gioco dei miner

Regola: vince chi trova per primo un'impronta che inizia con `0`

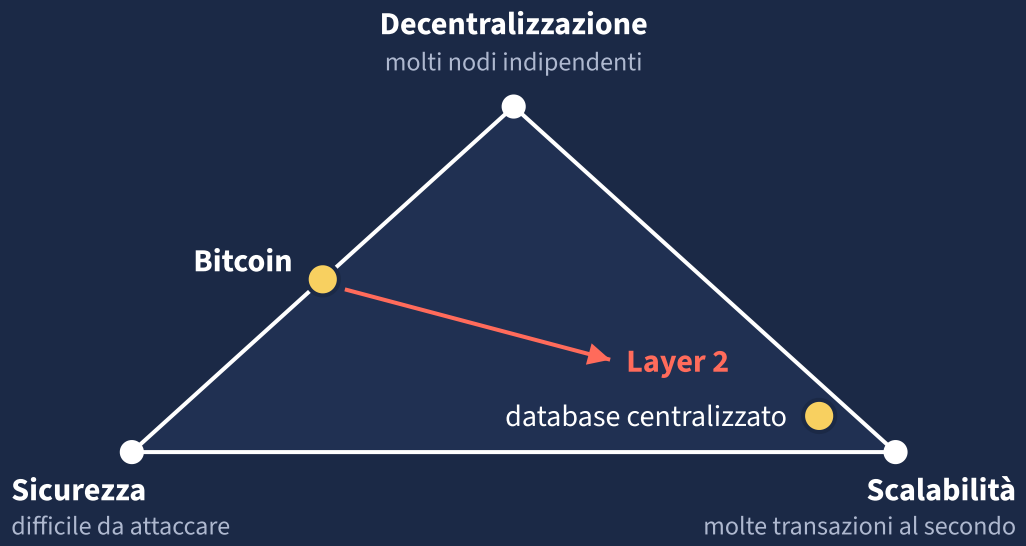
Nuova gara: blocco successivo | Ricomincia

blocco 0 `0000000000…` ← **blocco 1 · Dario** `0ed95925f0…` ← **blocco 2 · Carla** `06751bead8…` ← **blocco 3 · Carla** `00b1a98d51…` ← **blocco 4?** in gara

Miner	Potenza	Tentativi di questo turno (impronte)	Blocchi vinti
Anna	1	`69c6b4`	0
Bruno	2	`a700d5` `5c09f0`	0
Carla	3	`70974b` `00b1a9`	2
Dario	6	`fb765e` `31364e` `c4db17` `13ff51` `dfdb17` `676c5d`	1

Carla trova `00b1a98d51…` al turno 1: aggiunge il blocco 3 e incassa 3,125 BTC. Gli altri lo controllano con un solo calcolo ✓ e ripartono da lì.

Il trilemma della blockchain



Due su tre

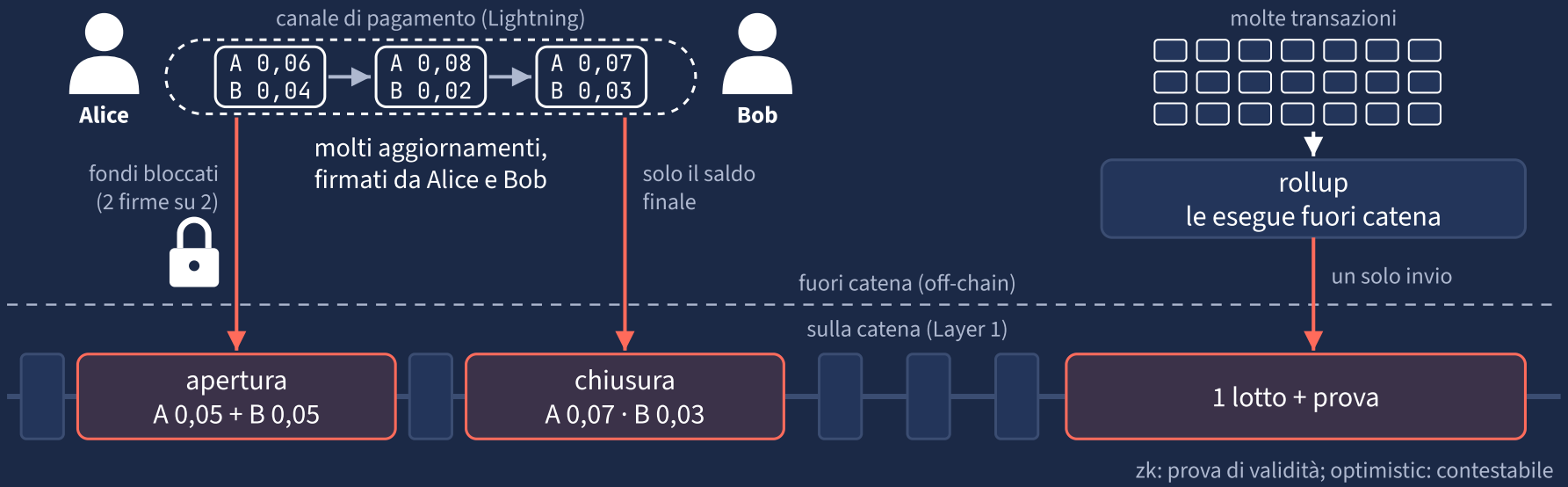
un progetto ottiene bene
al massimo **due proprietà su tre**
(V. Buterin)

Bitcoin: decentralizzato e sicuro,
ma poche transazioni al secondo

database centralizzato: veloce,
ma ci si fida di un solo gestore

Layer 2: le transazioni escono
dalla catena, che resta garante

Layer 2: meno transazioni sulla catena



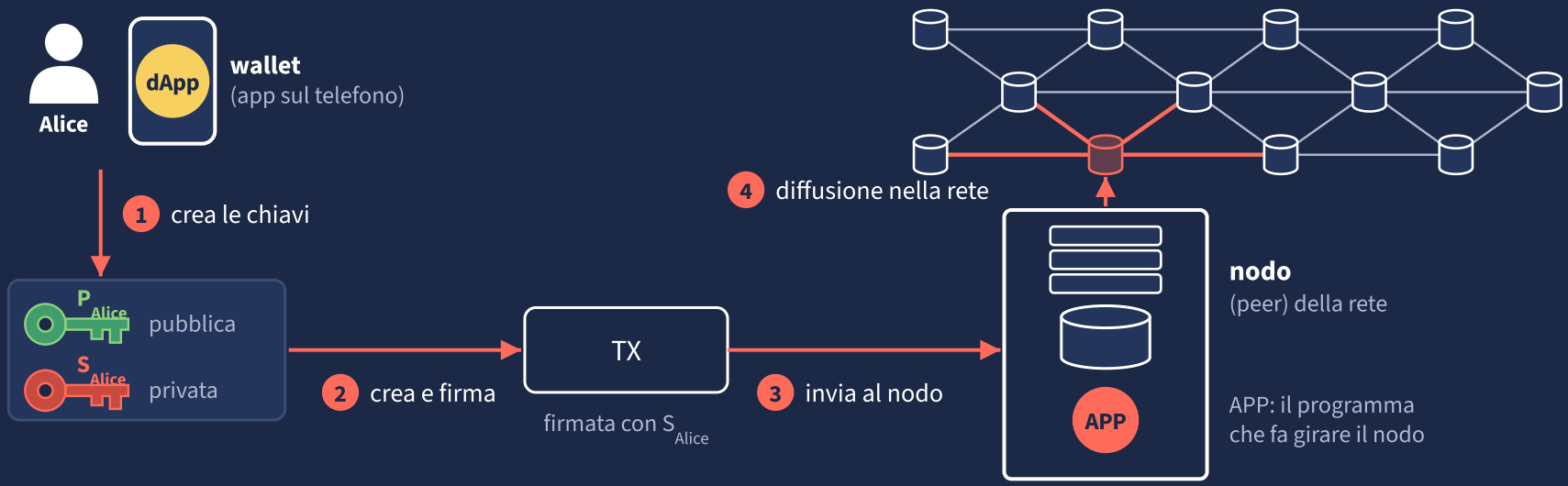
zk: prova di validità; optimistic: contestabile

Capo IV

Parte interattiva: creare una transazione

Chiavi, firma, invio: poi tocca a voi, dal telefono

Come nasce una transazione



1° Le chiavi nel wallet



Nessuno vi assegna un conto: il wallet se lo calcola da solo, offline, in un millisecondo.

ECDSA: Elliptic Curve Digital Signature Algorithm, la firma su curve ellittiche; **Keccak-256** e **BLAKE2b-256** sono funzioni hash

Un indirizzo vero

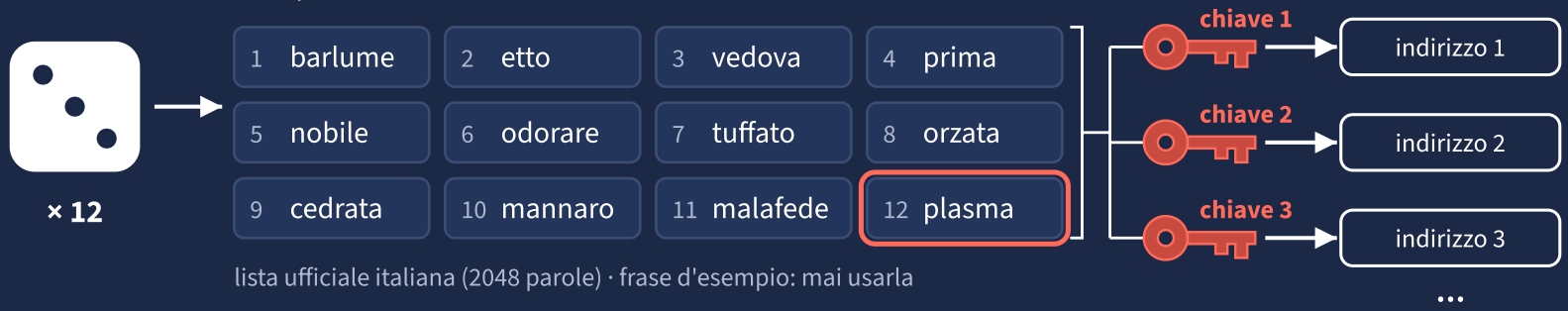
`1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa`

- Il 3 gennaio 2009 riceve i **50 BTC** del primo blocco: per una particolarità del codice, non si potranno mai spendere
- Da allora migliaia di persone gli hanno mandato bitcoin in omaggio: **57,7 BTC**, in 67.479 transazioni, mai toccati
- Chi c’è dietro? Nessuno lo sa: l’indirizzo è uno pseudonimo

mempool.space, indirizzo 1A1zP1eP…DivfNa, dati del 10 novembre 2026.

La seed phrase

un dado con 2048 facce, lanciato 12 volte



lista ufficiale italiana (2048 parole) · frase d'esempio: mai usarla

l'ultima parola contiene anche un controllo,
come l'ultima lettera del codice fiscale

una parola sbagliata (quasi sempre) si scopre subito:
«orzata» scritta «orzo» → **✕ frase non valida**

su qualsiasi wallet, le 12 parole
ridanno tutte le chiavi e gli indirizzi

chi ha le 12 parole ha i fondi
$2048^{12} \approx 5{,}4 \times 10^{39}$ combinazioni:
indovinarle è impossibile

Proviamo: dodici parole

Genera 128 bit a caso

Solo una dimostrazione: una frase mostrata in aula non va mai usata.

1 **abaco** 00000000000	2 **abaco** 00000000000	3 **abaco** 00000000000	4 **abaco** 00000000000
5 **abaco** 00000000000	6 **abaco** 00000000000	7 **abaco** 00000000000	8 **abaco** 00000000000
9 **abaco** 00000000000	10 **abaco** 00000000000	11 **abaco** 00000000000	12 **abete** 00000000**0011**

12 × 11 = 132 bit: **128 casuali** + **4 di controllo** (dall'impronta SHA-256). Una parola sbagliata quasi sempre rompe il controllo. Combinazioni possibili: $2^{128} \approx 3{,}4 \times 10^{38}$.

Nella stampa: il vettore di prova ufficiale, 128 bit a zero.

2° La transazione: una vera, sul contratto della classe

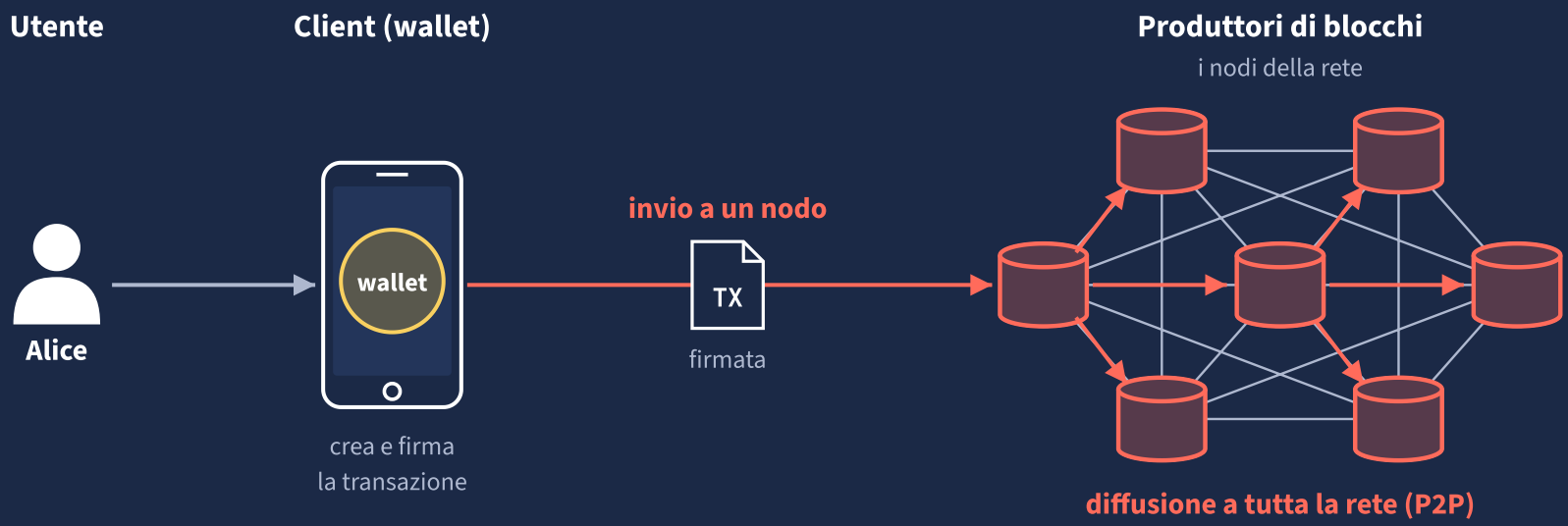
```
sender: "0x6677605b…8f734a97b7e3"     # chi firma (un telefono in prova)
transaction:
  MoveCall: aula::iscriviti           # la funzione dello smart contract
  arguments: [Rubinetto, "bruno-p6z4"]
gasData:
  price: 1000                         # NANOS per unità di gas
  budget: 8338400                     # massimo che si accetta di pagare
txSignatures: ["ANGLNreIjnwYIS/kkZ2k…"]  # firma Ed25519 + chiave pubblica
```

Costo: calcolo 0,001 IOTA (bruciati) + spazio 0,0085 IOTA − rimborso 0,0032 IOTA = **0,0064 IOTA**.

Lo spazio sul registro si paga come una cauzione: chi cancella i dati se la riprende.

NANOS: l'unità più piccola, un miliardesimo di IOTA

3° Invio al nodo e 4° diffusione nella rete



Tocca a voi: prendete il telefono

mirkozichichi.me/slides/
smartcontractgiur2026/aula

1. Il telefono crea il vostro **wallet**: una coppia di chiavi e un indirizzo
2. Chiedete token di prova al **faucet**: servono per il gas
3. **Iscrivetevi** con un soprannome: lo smart contract vi dà 10 AULA
4. **Inviate** qualche AULA a un compagno, scegliendolo per nome

Rete di prova di IOTA (devnet): token senza valore. Il soprannome resta pubblico sulla blockchain.

La lavagna: i vostri token in tempo reale

In aula questa lavagna si collega allo smart contract sulla rete di prova devnet di IOTA e mostra, in tempo reale, gli iscritti, gli AULA in circolazione e gli ultimi invii.

Capo V

Introduzione agli smart contract

Programmi che nessuno può fermare da solo

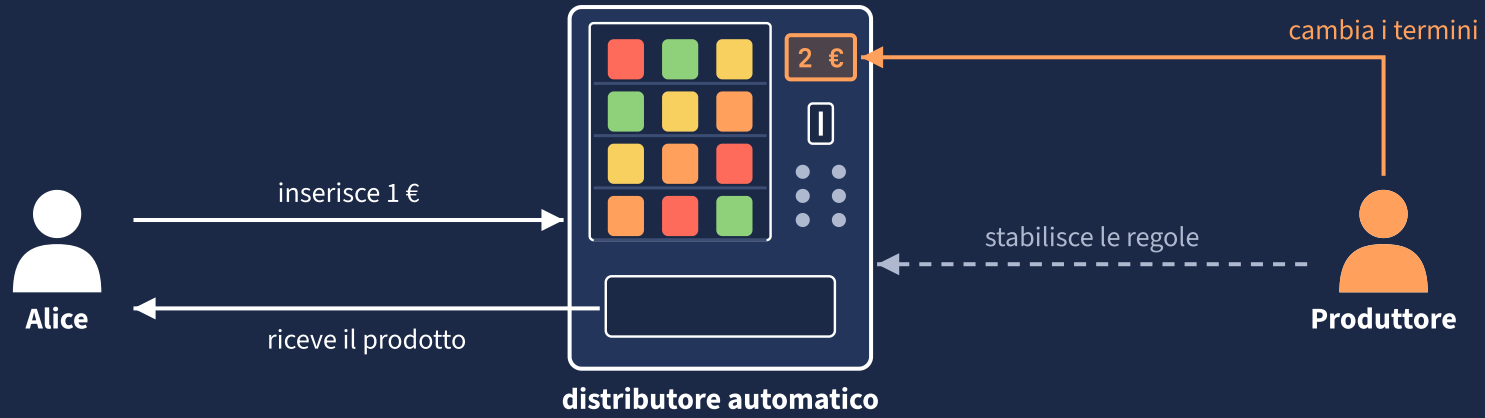
Smart contract: un programma eseguito da tutti i nodi

> *"A smart contract is a computerized transaction protocol that executes the terms of a contract."* N. Szabo, 1994

- Il codice e i suoi dati stanno sulla blockchain, visibili a tutti; ogni nodo lo esegue e ottiene lo stesso risultato
- Il contratto della classe: 208 righe di Move, pubblicate oggi sulla devnet con una sola transazione

Da quel momento il contratto risponde a chiunque, a qualsiasi ora: anche se io spengo il computer.

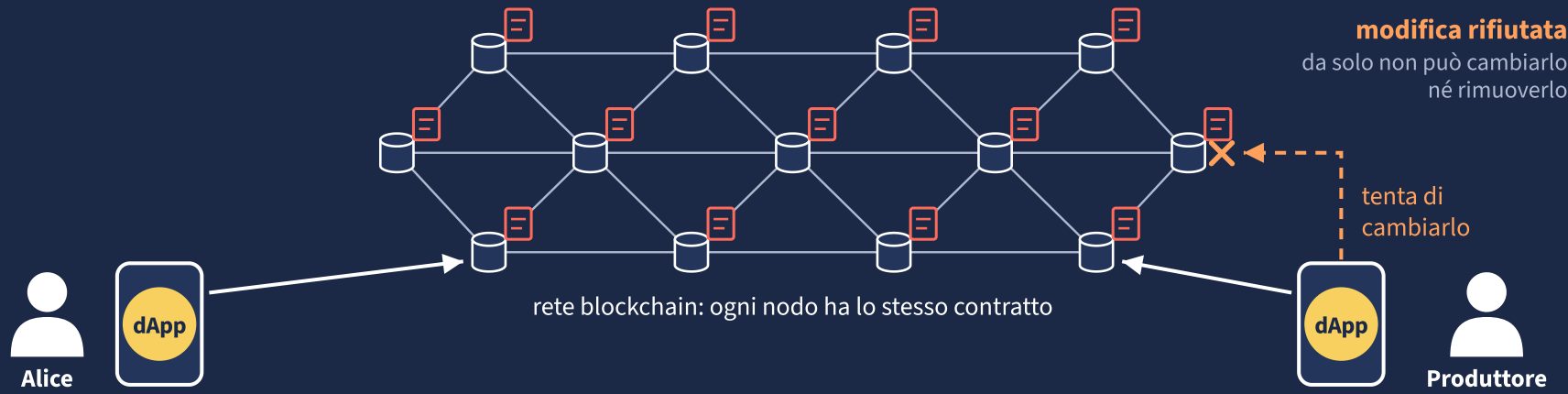
Il distributore automatico



la certezza dell'esecuzione dipende dalla fiducia nel produttore

... e potrebbe ingannare l'acquirente

Fiducia senza intermediario

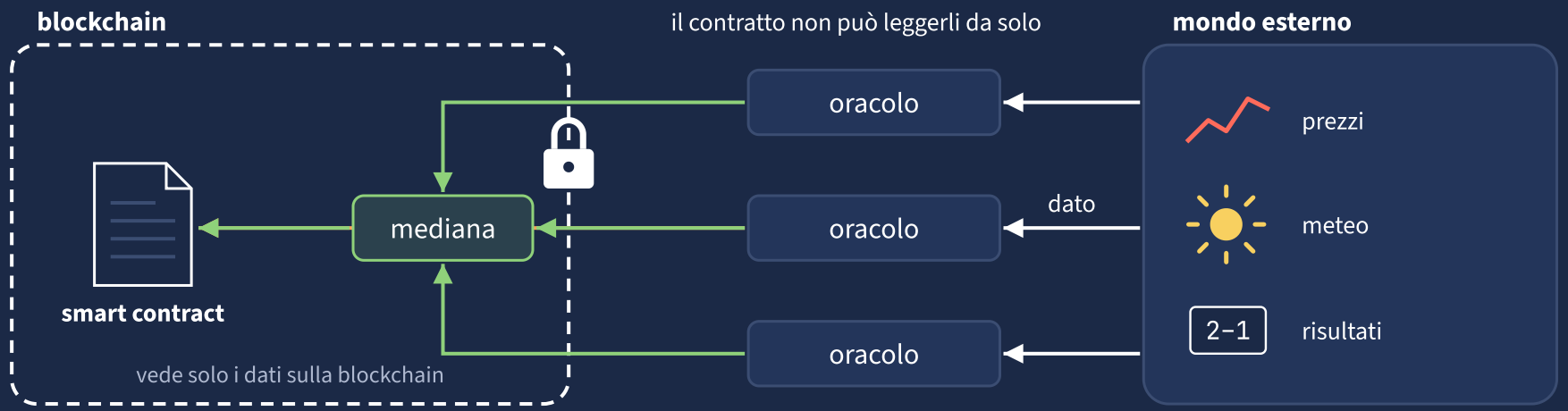


codice aperto (open source) + accordo di più di ⅔ dei validatori

→ nessuna deviazione tecnica dall'accordo iniziale

Codice pubblico, più di due terzi dei validatori onesti, nessuno che possa cambiarlo da solo: allora il contratto non devia dall'accordo.

Il problema dell'oracolo



un solo oracolo: il contratto è affidabile quanto lui (se sbaglia o mente, il contratto esegue lo stesso)

più oracoli indipendenti, valori aggregati: un errore isolato non basta

Il contratto è affidabile quanto i dati che riceve dal mondo esterno.

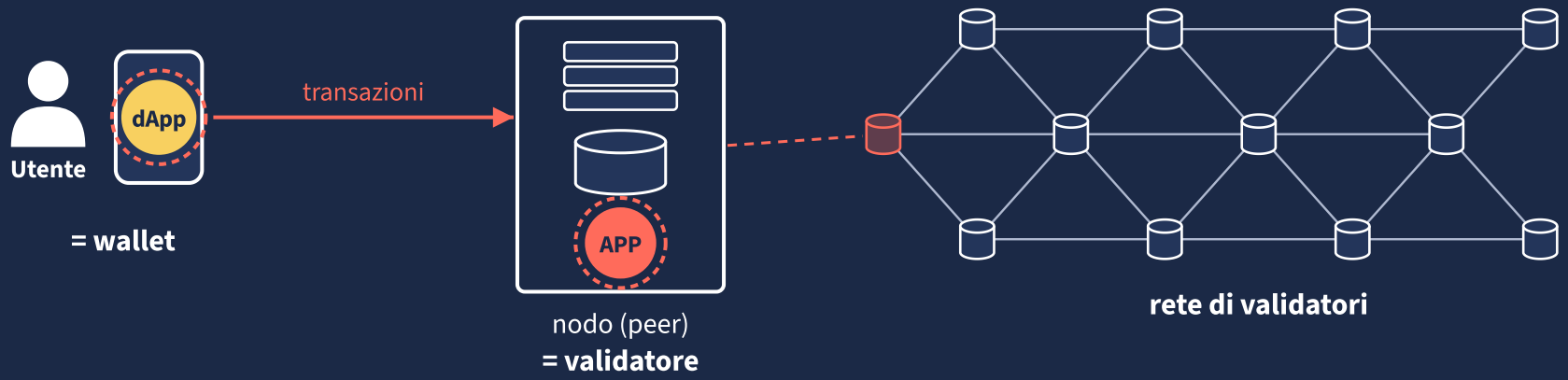
Che cos’è una piattaforma per smart contract

Una piattaforma per smart contract è fatta di:

- un network di **validatori** (i nodi della blockchain)
- un algoritmo di **consenso** (Proof of Work, Proof of Stake)
- un **registro condiviso** (la blockchain)
- un sistema di **indirizzi** (account e wallet)
- un **computer decentralizzato** (la macchina virtuale)
- un **linguaggio** per scrivere i contratti (Move)
- una **struttura economica** (criptovalute e token)

Da qui in poi, in alto a destra, vedete a quale di queste parti siamo arrivati.

I validatori: chi fa girare la rete

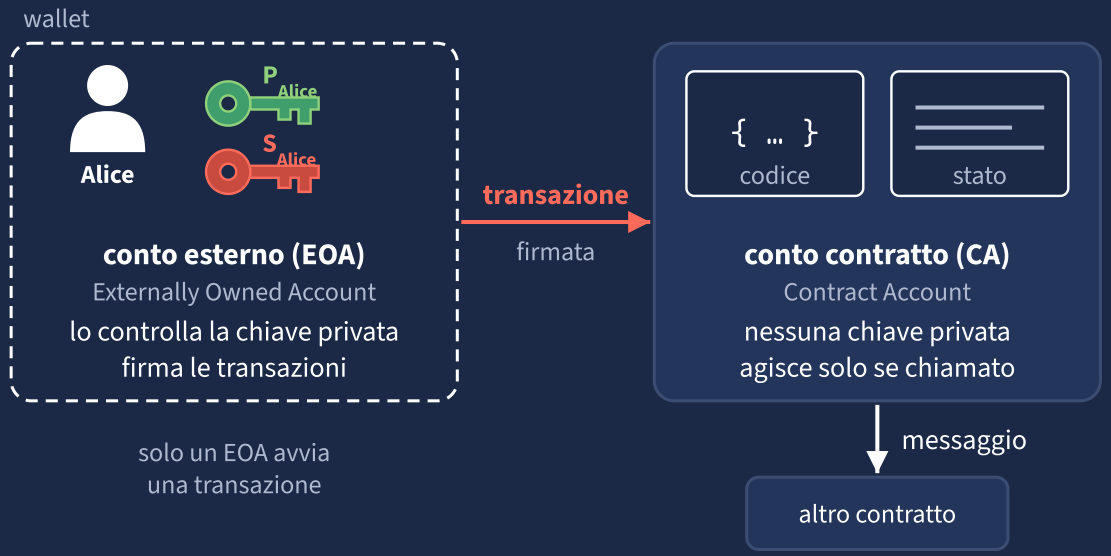


dApp **dApp** = interfaccia per gli utenti

APP **APP** = interfaccia dei nodi

- **IOTA**: rete attiva dal 5 maggio 2025, software open source; a novembre 2026 la fanno girare **61 validatori**
- Una nuova versione del protocollo parte solo quando l'ha installata più dell'83% del potere di voto: la v39 è attiva dal 5 novembre 2026

Wallet e account



solo un EOA avvia una transazione

EIP-7702

Ethereum, aggiornamento Pectra, 7 maggio 2025



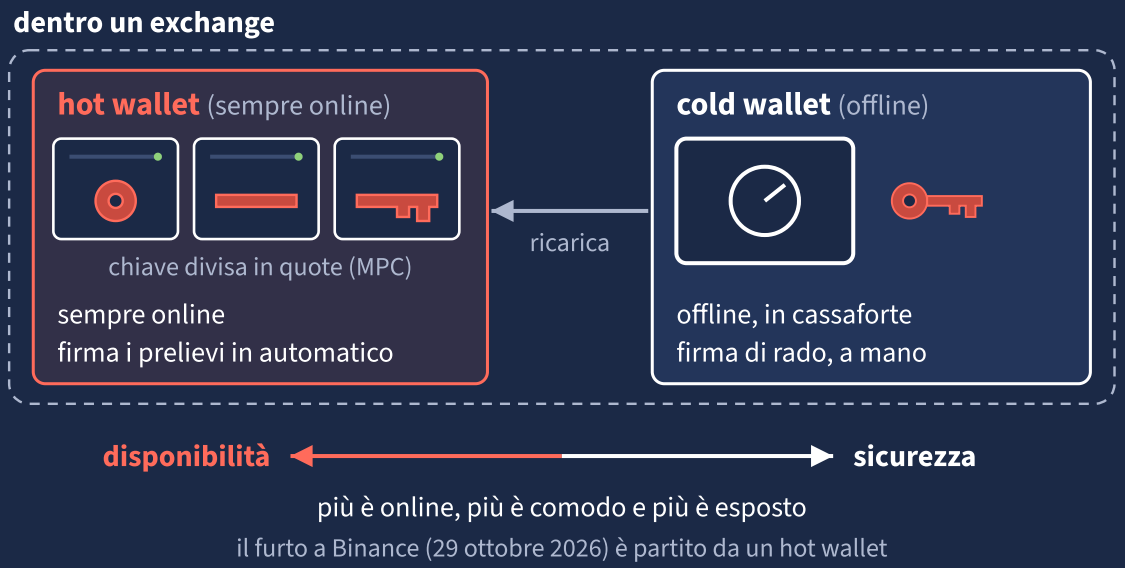
l'EOA esegue quel codice come se fosse un contratto

chi può autorizzare la delega decide che cosa fa il conto

29 ottobre 2026, Binance: gli attaccanti ottengono permessi di esecuzione su un hot wallet tramite EIP-7702

EIP: Ethereum Improvement Proposal, una modifica proposta (e poi adottata) al protocollo di Ethereum

Binance, rivisto: dove stanno le chiavi



e i tuoi fondi?

custodia
fondi lasciati sull'exchange

tu

le chiavi sono sue:
tu vedi un saldo
nel suo registro

autocustodia
il tuo wallet, la tua chiave

tu

copia di riserva:
12–24 parole
(seed phrase)

«not your keys, not your coins»

Su un exchange le chiavi non sono vostre: «not your keys, not your coins».

Binance, 29 ottobre 2026: il percorso dell'attacco

giugno
un ingegnere installa un pacchetto software manomesso
PC sostituito, ma il team dei wallet resta esposto

→

settembre
un altro ingegnere viene contattato per un lavoro: video con finti HR e CEO
il «compito di prova» contiene un malware
zero-day (mai visto prima)

→

20 ottobre
con uno strumento interno di IA raggiungono i PC di due ingegneri dei wallet

→

29 ottobre
con credenziali rubate lanciano uno script; con **EIP-7702 comandano un hot wallet**
20:05 UTC: escono i fondi
00:10 UTC (30/10): bloccati
rubati ≈ 6,3 miliardi di $



≈ 2,85 miliardi di $ congelati
in gran parte stablecoin, bloccate dai loro emittenti (Tether, Circle)
una funzione del loro contratto

bitcoin: non congelabili
nessun emittente: nessuno può bloccarli, una volta usciti
recuperarli è quasi impossibile

- Su Ethereum gli aggressori hanno ottenuto, con **EIP-7702**, il diritto di eseguire codice per conto di un hot wallet
- La delega è registrata sulla blockchain: per revocarla serviva la stessa firma collettiva (MPC), e quindi tempo

HR: risorse umane; **IA**: intelligenza artificiale

Il precedente: Bybit, febbraio 2025

- **21 febbraio 2025**: dal cold wallet multifirma di Bybit escono circa **1,5 miliardi di dollari**
- Gli aggressori avevano manomesso l'interfaccia web di Safe{Wallet}, usata per firmare
- I tre firmatari hanno approvato una transazione che **sembrava** legittima e sostituiva il codice del wallet
- L'FBI attribuisce l'attacco alla Corea del Nord (TraderTraitor)

Si firma ciò che lo schermo mostra: se lo schermo mente, la firma è valida lo stesso.

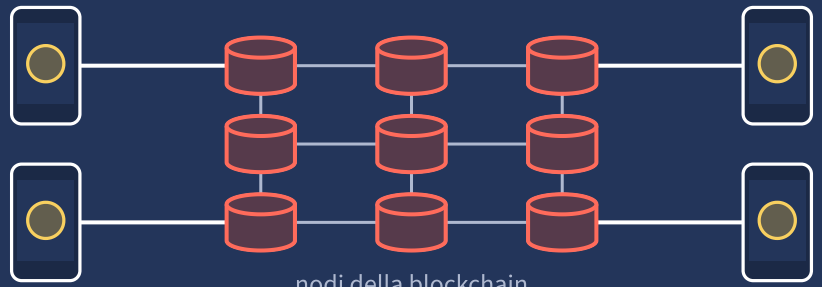
Computazione decentralizzata

App tradizionali



richieste elaborate da **uno o pochi server**

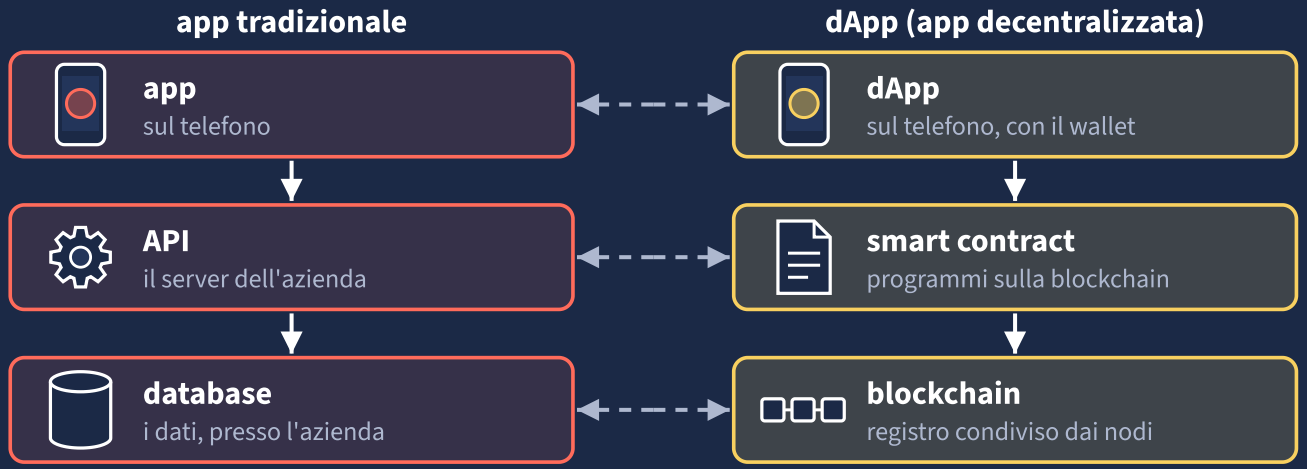
dApp (app decentralizzate)



richieste elaborate da **tutti i nodi**

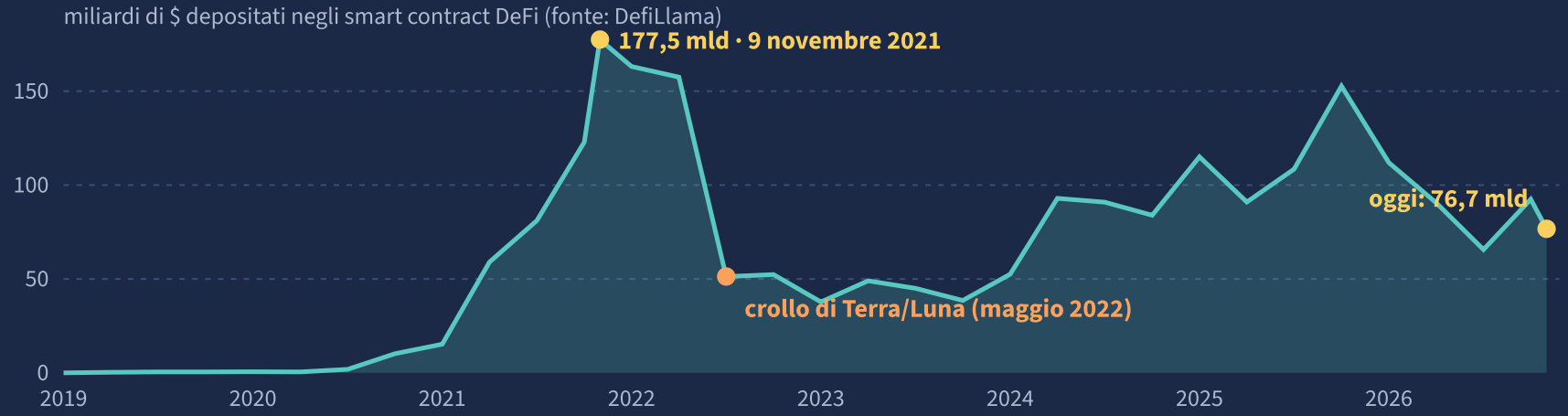
ISP: Internet Service Provider, il fornitore di accesso a Internet

Applicazioni decentralizzate (dApp)



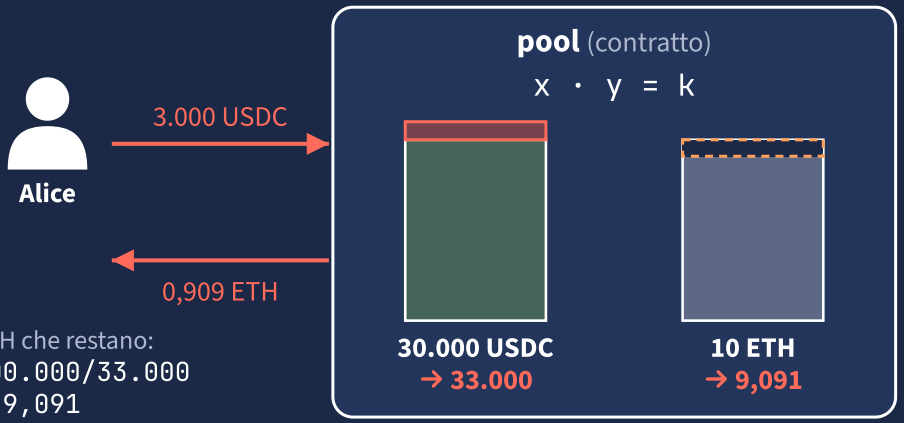
come un'app parla con il suo server,
la dApp parla con gli smart contract sulla blockchain (ad es. IOTA)

La finanza decentralizzata (DeFi)



- Scambi senza intermediario: **Uniswap**, dove il prezzo lo fa una formula
- Prestiti senza banca: **Aave**, 11,8 miliardi prestati, sempre con garanzia superiore al prestito

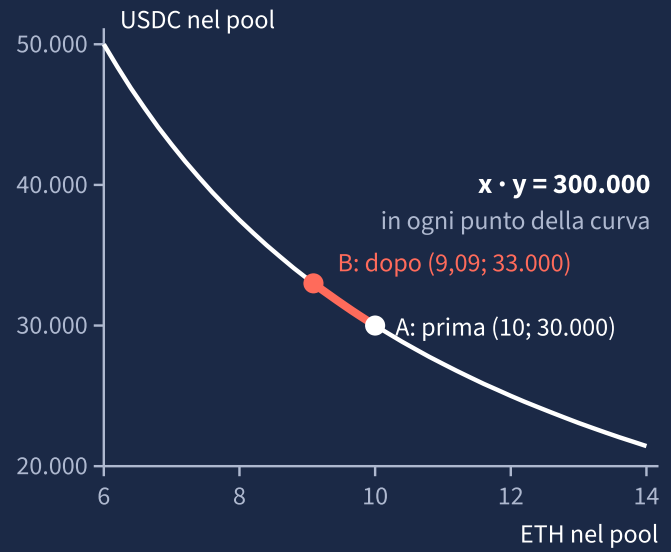
Uno scambio senza banco: x · y = k



ETH che restano:
`300.000/33.000`
`= 9,091`

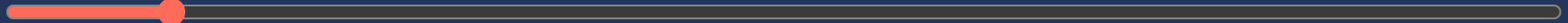
prezzo medio 3.300
+10% (slippage); con
300 USDC solo +1%

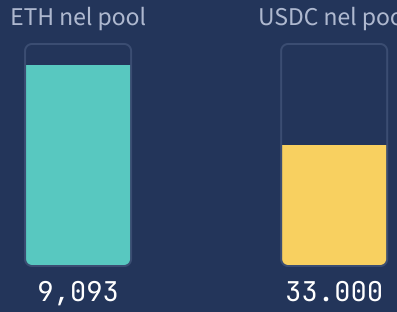
prezzo: 30.000 / 10 = 3.000 USDC per ETH
lo 0,3% di ogni scambio va ai fornitori di liquidità
nuovo prezzo: 33.000 / 9,091 = 3.630



Proviamo: comprare da un pool

Paghi **3000 USDC** per comprare ETH dal pool

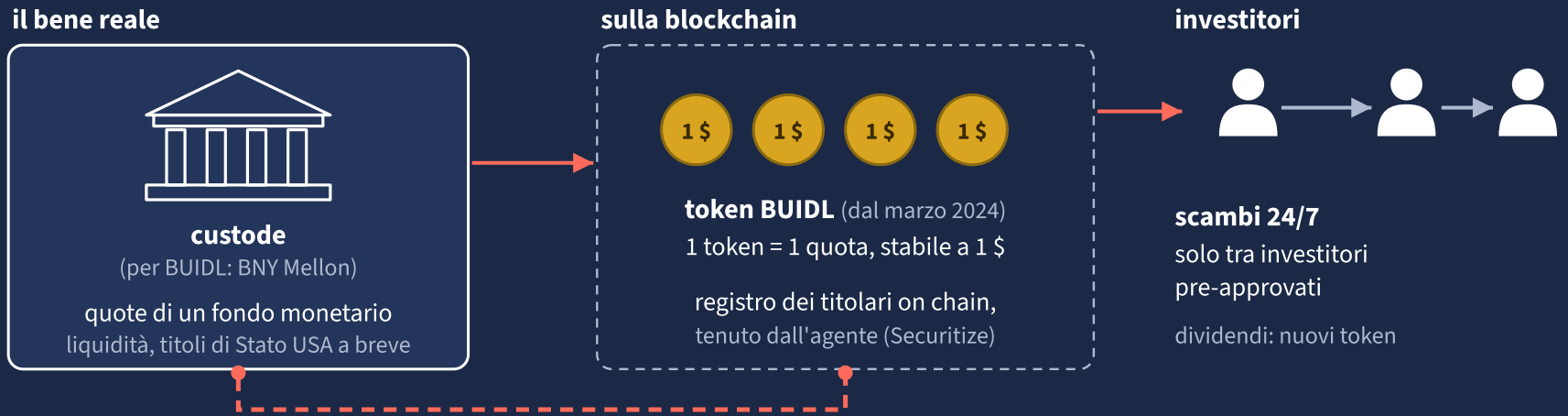




Ricevi	**0,907 ETH**
Prezzo prima dello scambio	3000 USDC per ETH
Prezzo medio che hai pagato	3309 **(+10,3%)**
Prezzo nel pool dopo	3629

Nessun banco e nessun ordine: il prezzo lo fa la formula x · y = k. Lo 0,3% resta a chi ha messo i fondi nel pool.

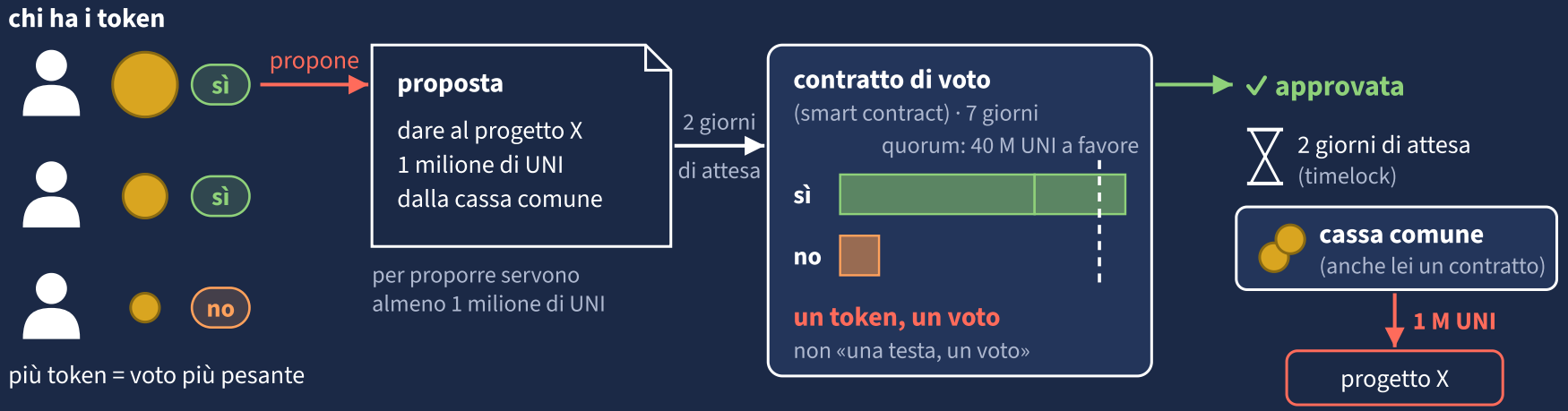
Tokenizzazione: titoli e fondi sulla blockchain



- **40 miliardi di dollari** di attività reali in token; 14 miliardi sono titoli di Stato USA (10/11/2026)
- **Italia**: CDP, primo *digital bond* (2024); **BCE**: Pontes, per regolarli in euro di banca centrale (2026)

BUIDL: il fondo tokenizzato di BlackRock; **BNY**: la banca depositaria (BNY Mellon)
CDP: Cassa Depositi e Prestiti; **BCE**: Banca centrale europea

Che cos'è una DAO



esempio reale: Uniswap (token UNI)

è il contratto a pagare: nessun consiglio, nessuna banca

DAO: Decentralized Autonomous Organization, organizzazione autonoma decentralizzata; **UNI**: il token di Uniswap

The DAO, 2016: «il codice è legge»?

The DAO (contratto, 2016)

```
ritira():
  1. invia gli ether
  2. azzera il saldo
```

l'errore: prima paga, poi aggiorna

invia ether

ritira() di nuovo

… molte volte

attaccante (contratto)

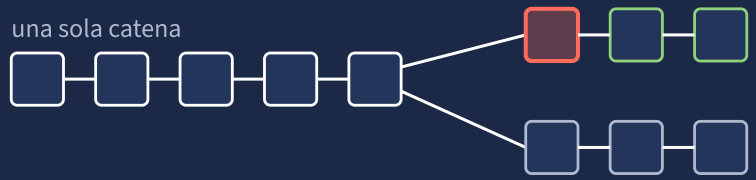
```
quando riceve:
  chiama ritira()
```

il saldo non è ancora azzerato: paga ancora

≈ 3,6 milioni di ether

in una «child DAO» dell'attaccante

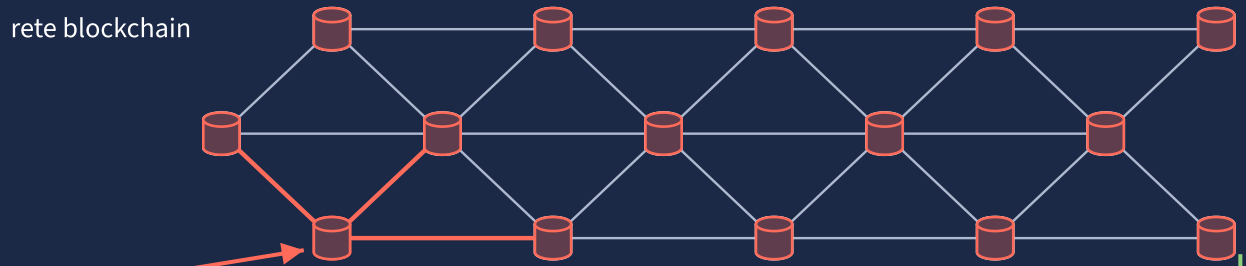
17 giugno 2016



Ethereum (ETH)
il fork sposta i fondi della DAO in un contratto di rimborso

Ethereum Classic (ETC)
chi rifiuta il fork resta sulla catena di prima, invariata

Esempio: un voto in uno smart contract






```
execute(
  SmartContractAddress: VotingContract,
  methodToExecute: vote,
  parameters: challengeID, true)
```

«esegui il metodo vote del contratto: voto favorevole (true)»

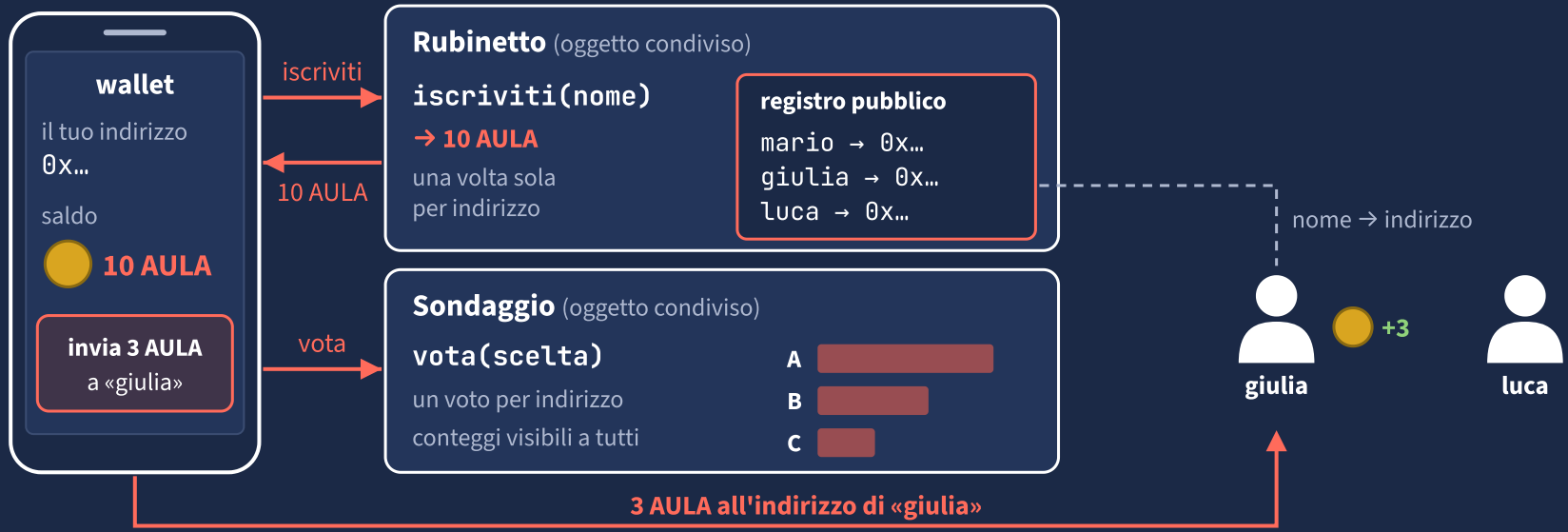
stato di VotingContract	
favorevoli	12 → **13**
contrari	7

Il voto, nel contratto della classe

```
public fun vota(sondaggio: &mut Sondaggio, scelta: u64, ctx: &TxContext) {
    assert!(sondaggio.aperto, EChiuso);
    assert!(scelta < sondaggio.opzioni.length(), ESceltaNonValida);
    let chi = ctx.sender();
    assert!(!sondaggio.votanti.contains(chi), EGiaVotato);
    sondaggio.votanti.add(chi, scelta);
    let conteggio = &mut sondaggio.voti[scelta];
    *conteggio = *conteggio + 1;
}
```

Le regole sono nel codice: sondaggio aperto, scelta valida, un voto per indirizzo.

Il contratto della classe, tutto intero



Votate dal telefono

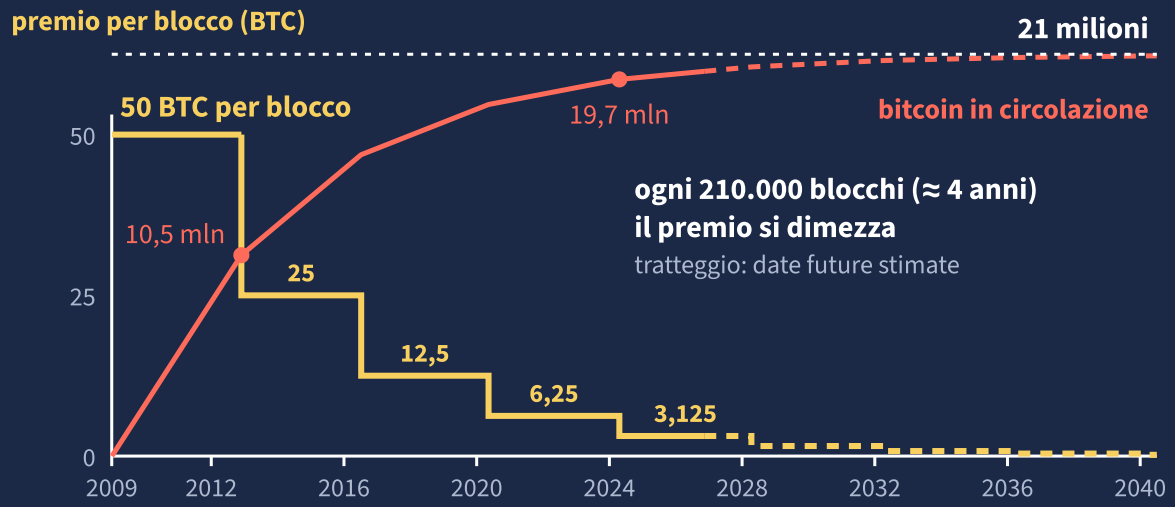
In aula questa lavagna si collega allo smart contract sulla rete di prova devnet di IOTA e mostra, in tempo reale, i voti.

Capo VI

Tokenomics e monete digitali

Chi crea la moneta, chi la garantisce, chi la può bloccare

Bitcoin: una moneta a offerta fissa



ogni 210.000 blocchi (≈ 4 anni)
il premio si dimezza
tratteggio: date future stimate

Perché 21 milioni?

$210.000 \times 50 \times (1 + ½ + ¼ + \ldots)$

$= 210.000 \times 50 \times 2$

$= 21.000.000$

in realtà 20.999.999,9769:
premi arrotondati al satoshi

Chi fa rispettare la politica monetaria di Bitcoin?

Blocco

blocco 975.328 (oggi)

Il miner si paga **6,25 BTC**

Premio previsto dal protocollo a questa altezza: **3,125 BTC** (50 dimezzato 4 volte)

+ commissioni delle transazioni nel blocco: **0,02 BTC** = massimo **3,145 BTC**

✕ nodo 1 ✕ nodo 2 ✕ nodo 3 ✕ nodo 4 ✕ nodo 5

Ogni nodo rifiuta il blocco: «coinbase pays too much». Il miner ha fatto il lavoro per niente.

Nessuna banca centrale: ogni nodo rifà il conto, e un miner che si paga troppo vede il suo blocco rifiutato.

Proviamo: il dimezzamento

Epoca: **4** (dopo 4 dimezzamenti), dal blocco 840.000, 20 apr 2024

Premio per blocco	Bitcoin emessi a fine epoca	Del totale finale
3,125 BTC	**20.343.750**	**96,88%**

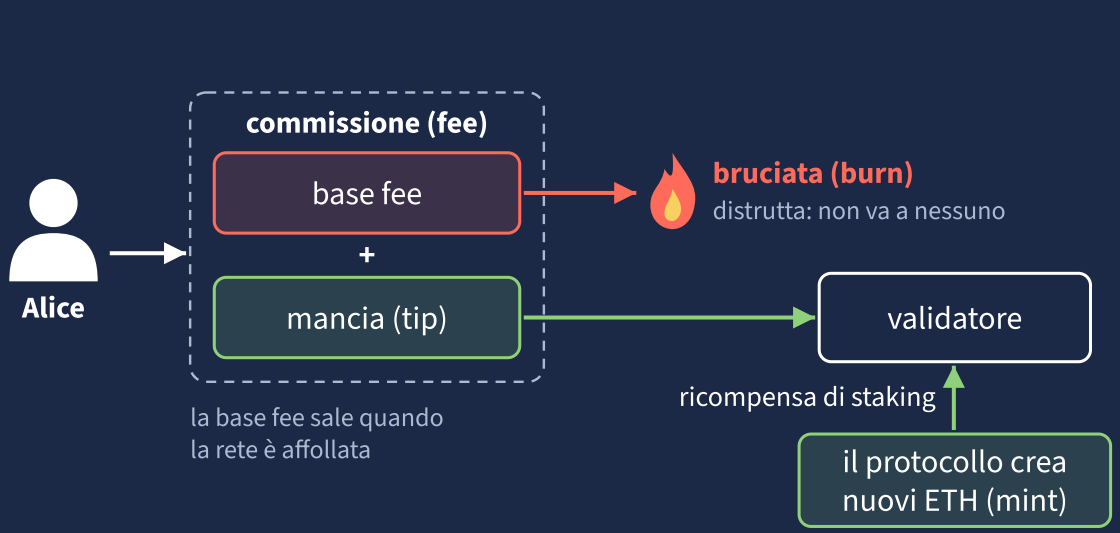
Totale finale: **20.999.999,9769** BTC, raggiunto intorno al 2140. Nessuno può cambiarlo senza il consenso della rete.

Bitcoin oggi

- **73.150 dollari** il 10 novembre 2026: −42% dal massimo di 126.080 (6 ottobre 2025)
- Dal gennaio 2024 negli USA si compra anche in Borsa, con un ETF: quello di BlackRock ne custodisce per 59,5 miliardi di dollari
- In Italia: Intesa Sanpaolo ha comprato 11 bitcoin nel gennaio 2025, «un test»
- **El Salvador** ha fatto marcia indietro: dal 2025 accettarli è facoltativo

ETF: Exchange-Traded Fund, fondo quotato in Borsa (quello di BlackRock si chiama IBIT)

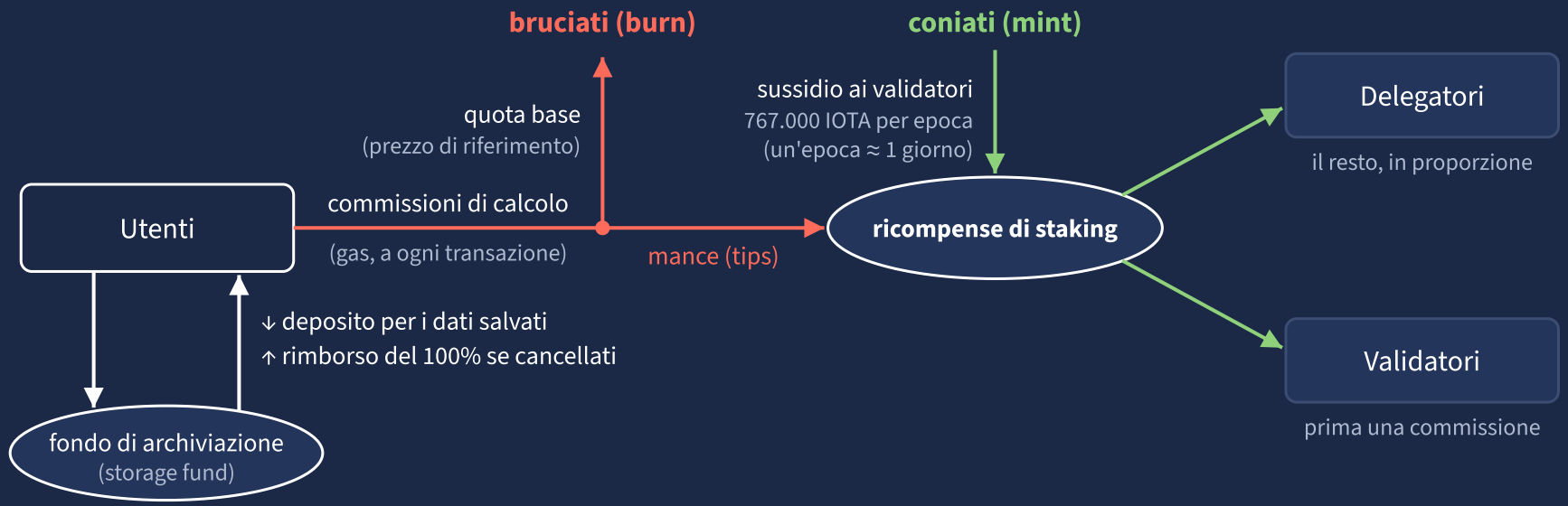
Ethereum: si crea e si brucia



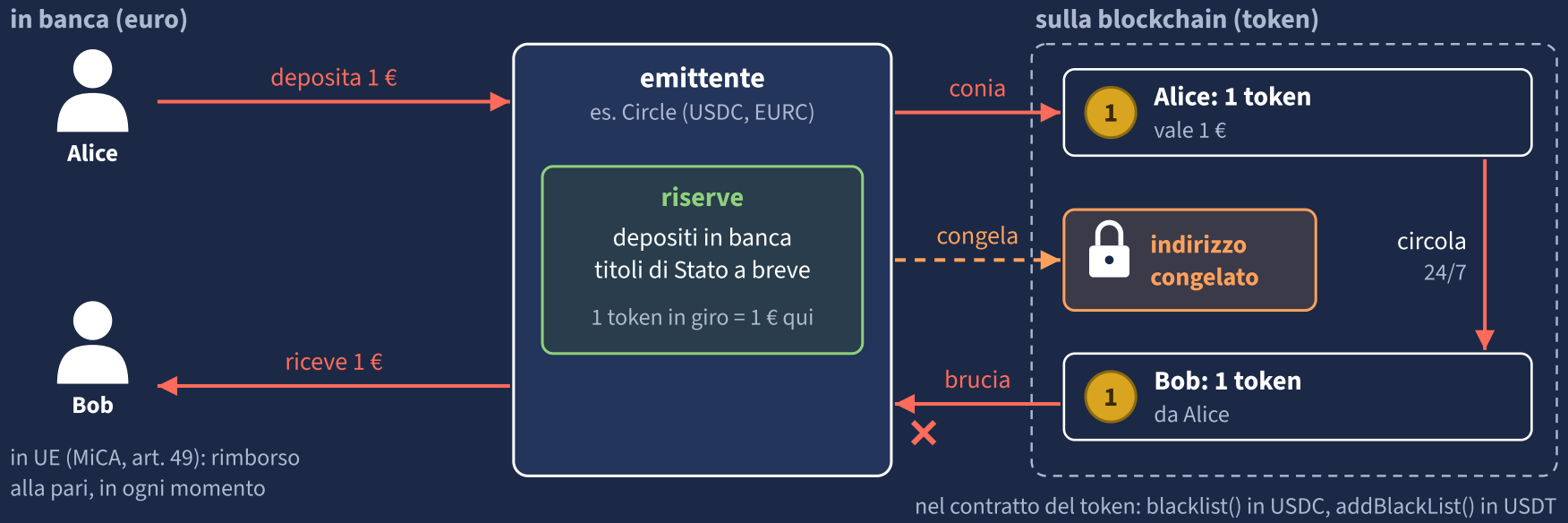


ETH: ether, la moneta di Ethereum

IOTA: le commissioni si bruciano, i validatori si pagano a ogni epoca



Stablecoin: un dollaro sulla blockchain



In circolazione: **294 miliardi di dollari**. USDT (Tether) il 60%, USDC (Circle) il 24%; in euro appena lo 0,3%.

MiCA: Markets in Crypto-Assets, il regolamento UE sulle cripto-attività (Reg. (UE) 2023/1114)

Proviamo: chi può bloccare una stablecoin?

USDC (Circle) USDT (Tether) Il contratto del token, sulla blockchain, ha funzioni che solo l'emittente può chiamare.

Titolare	Saldo
Alice	500
Bob	300
Mallory (ha ricevuto fondi rubati)	0 bloccato
Offerta totale	800

Utenti

Mallory invia 100 a Bob

Bob invia 100 a Mallory

Tether (emittente)

Blocca Mallory

Azzera il saldo bloccato

✓ Tether azzera il saldo di Mallory: −1000 dall'offerta (destroyBlackFunds)

✕ Mallory → Bob: rifiutato, Mallory è bloccato

✓ Tether blocca Mallory (addBlackList)

La sera del furto a Binance: Tether ha bloccato più di 1,5 miliardi, Circle più di 800 milioni. I bitcoin rubati, nessuno ha potuto fermarli.

MiCA e GENIUS Act: la legge entra nel codice

- **UE, MiCA**: rimborso «in qualsiasi momento e al valore nominale» (art. 49), niente interessi (art. 50), almeno il 30% dei fondi su conti bancari separati (art. 54)
- Circle è istituto di moneta elettronica autorizzato in Francia dal 1° luglio 2024: USDC ed EURC sono conformi; USDT no, e per l'ESMA gli intermediari UE non devono più offrirlo
- **USA, GENIUS Act**: può emettere solo chi ha «the technological capability to comply… with the terms of any lawful order» (Sec. 4(a)(6)(B))
- Cioè ordini di «seize, freeze, burn, or prevent the transfer» (Sec. 2(16)): la funzione di blocco diventa un obbligo di legge

GENIUS Act: la legge USA sulle stablecoin (Guiding and Establishing National Innovation for U.S. Stablecoins, Public Law 119-27, 18 luglio 2025)
ESMA: Autorità europea degli strumenti finanziari e dei mercati

Tre monete digitali, tre garanti

bitcoin
cripto-attività

chi la emette
nessuno: nasce col mining

quanta ce n'è
meno di 21 milioni, per codice

valore
libero: oscilla

nessuno la può congelare

stablecoin
es. USDC, USDT, EURC

chi la emette
un'impresa (es. Circle, Tether)

quanta ce n'è
quanto ha in riserva

valore
agganciato a 1 $ o 1 €

l'emittente può congelare un indirizzo

euro digitale
CBDC · non ancora emesso

chi la emette
la BCE (Eurosistema)

quanta ce n'è
tetto per persona, da fissare

valore
è euro: come il contante

legge UE in trattativa; prima emissione possibile nel 2029

chi garantisce?

nessuno: codice e rete	l'emittente, con le riserve	la banca centrale

CBDC: Central Bank Digital Currency, moneta digitale di banca centrale

L’euro digitale: come funzionerebbe

- **Offline**, da telefono a telefono, come il contante: «only the payer and the payee would know» (BCE)
- **Limite di detenzione** (art. 16 della proposta): la cifra non c’è; la BCE ha simulato da 500 a 3.000 €, «illustrative»
- **Waterfall** (art. 13): se il saldo non basta si attinge al conto in banca; l’eccedenza torna in banca da sola
- «L’euro digitale **non è moneta programmabile**» (art. 24): ammessi però i pagamenti condizionati, come il pagamento alla consegna

La legge è ancora in negoziato; se arriva, pilota dal 2027 con 36 prestatori (7 italiani) e prima emissione possibile nel 2029.

Grazie!

IOTA

Mirko Zichichi · mirko.zichichi@iota.org · mirkozichichi.me

Le slide interattive: **mirkozichichi.me/slides/smartcontractgiur2026**

Allegato A

Appendice

Per approfondire: testi, norme, strumenti e un glossario

Per approfondire: blockchain e consenso (Capi II–IV)

- **S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*** (2008): nove pagine, il testo fondativo. bitcoin.org/bitcoin.pdf
- **L. Lamport, R. Shostak, M. Pease, *The Byzantine Generals Problem*** (1982). lamport.azurewebsites.net/pubs/byz.pdf
- **Ethereum, la documentazione per sviluppatori**: transazioni, conti, gas, Proof of Stake. ethereum.org/developers/docs
- **BIP-39**, le frasi di recupero, con la lista di parole italiana. github.com/bitcoin/bips/blob/master/bip-0039.mediawiki
- **IOTA, documentazione**: oggetti, Move, consenso, tokenomics. docs.iota.org
- **Esploratore della rete IOTA**: per vedere le transazioni fatte in aula. explorer.iota.org
- **Mempool.space**: i blocchi di Bitcoin in tempo reale. mempool.space

Per approfondire: smart contract e cripto-attività (Capi V–VI)

- **N. Szabo, *Smart Contracts*** (1994) e ***The Idea of Smart Contracts*** (1997). fon.hum.uva.nl/…/smart.contracts.html
- **The Move Book**: il linguaggio Move, abilità e risorse. move-book.com
- **MiCA, Reg. (UE) 2023/1114** sui mercati delle cripto-attività. eur-lex.europa.eu/eli/reg/2023/1114/oj
- **D.lgs. 5 settembre 2024, n. 129**: l'attuazione italiana di MiCA. normattiva.it
- **Art. 8-ter, d.l. 135/2018**: tecnologie a registro distribuito e smart contract. normattiva.it
- **ESMA, rapporto sul MEV** (luglio 2025) e parere sulle stablecoin non conformi (ottobre 2026). esma.europa.eu
- **BCE, l'euro digitale**: stato del progetto. ecb.europa.eu/euro/digital_euro
- **Uniswap v2, whitepaper** (2020): la formula $x \cdot y = k$. uniswap.org/whitepaper.pdf
- **Dati aperti**: DeFi e stablecoin su defillama.com, titoli tokenizzati su rwa.xyz

Le notizie citate in apertura

- **Rapporto Clusit 2026**, presentazione del 17 marzo 2026. securitysummit.it
- **ACN, Relazione annuale 2025** (sintesi). puntosicuro.it
- **Frigoriferi dei supermercati**, Il Post, 3 novembre 2026. ilpost.it
- **Una settimana di attacchi hacker e allarmi bomba**, Il Post, 9 novembre 2026. ilpost.it
- **Farnesina e Milano-Cortina**: Open, 8 ottobre 2026, open.online; The Record, 5 febbraio 2026, therecord.media
- **Caso Paragon**, Internazionale, 12 marzo 2026. internazionale.it
- **La voce clonata del ministro Crosetto**, Il Post, 11 febbraio 2025. ilpost.it
- **Il furto a Binance**: Il Post, 3 novembre 2026, ilpost.it; CoinDesk, 3 novembre 2026, coindesk.com
- **Normativa**: l. 90/2024, d.lgs. 138/2024 (NIS2), Cyber Resilience Act

Il contratto della classe

- **Codice sorgente** del pacchetto Move usato in aula (moneta AULA e sondaggio), con i test: cartella `aula/move` del sito, nel repository pubblico github.com/miker83z/mirkozichichi
- **L'app per il telefono**: mirkozichichi.me/slides/smartcontractgiur2026/aula
- **Rete di prova IOTA** (devnet): i token non hanno valore e la rete può essere azzerata; il faucet chiede un captcha. faucet.devnet.iota.cafe
- **Per programmare**: l'IOTA CLI e un'introduzione a Move. docs.iota.org/developer/getting-started

Glossario (1/3)

Termine	Traduzione o originale	In breve
Funzione hash	*hash function*	trasforma qualsiasi dato in un'impronta di lunghezza fissa
Firma (elettronica)	*digital signature*	prova, con la chiave privata, chi ha approvato un dato
Sistema distribuito	*distributed system*	computer che collaborano scambiandosi messaggi
Da pari a pari	*peer to peer (P2P)*	rete senza centro: ogni nodo è client e server
Registro distribuito	*distributed ledger (DLT)*	registro replicato tra molti nodi che si accordano tra loro
Blocco	*block*	pacchetto di transazioni con l'impronta del blocco precedente
Consenso	*consensus*	la regola con cui i nodi si accordano sullo stesso registro
Proof of Work (PoW)	*prova di lavoro*	chi risolve un puzzle di calcolo propone il blocco
Proof of Stake (PoS)	*prova di partecipazione*	i validatori impegnano una quota e votano i blocchi
Double spending	*doppia spesa*	spendere due volte la stessa moneta

Glossario (2/3)

Termine	Traduzione o originale	In breve
Conferma	*confirmation*	blocco aggiunto dopo quello che contiene un pagamento
Wallet	*portafoglio*	programma che custodisce le chiavi e firma le transazioni
Seed phrase	*frase di recupero (BIP-39)*	12 o 24 parole da cui si ricalcolano tutte le chiavi
Hot / cold wallet	*portafoglio caldo / freddo*	chiavi sempre online / chiavi offline
Faucet	*faucet*	servizio che regala token di prova
Gas	*gas*	unità di misura (e prezzo) del calcolo di una transazione
Smart contract	*smart contract*	programma eseguito da tutti i nodi di una blockchain
Applicazione decentralizzata	*dApp*	interfaccia che usa smart contract invece di un server
Oracolo	*oracle*	servizio che porta dati esterni sulla blockchain
Validatore	*validator*	nodo che vota i blocchi nella Proof of Stake

Glossario (3/3)

Termine	Traduzione o originale	In breve
Token	*token*	unità di valore o di diritto gestita da uno smart contract
NFT	*non-fungible token*	token unico, che rappresenta un bene o un diritto
Stablecoin	*stablecoin*	token ancorato a una valuta, emesso da un privato
Token di moneta elettronica	*e-money token (EMT)*	stablecoin ancorata a una sola valuta ufficiale (MiCA)
Token collegato ad attività	*asset-referenced token (ART)*	token ancorato ad altri valori o a più valute (MiCA)
Finanza decentralizzata	*DeFi*	scambi e prestiti tramite smart contract, senza intermediari
DAO	*decentralized autonomous organization*	organizzazione che decide con voti registrati in un contratto
Tokenizzazione	*tokenization*	rappresentare un bene reale (titolo, fondo) con un token
Layer 2	*livello 2*	sistema che esegue transazioni fuori dalla catena principale
Euro digitale	*digital euro (CBDC)*	moneta digitale emessa dalla banca centrale

Crediti

- **Contenuti**: edizione interattiva, novembre 2026, delle slide del seminario "Blockchain e Smart Contract: aspetti giuridici e tecnologici", Università di Bologna; il Capo I riprende la lezione "Introduzione alla Crittografia" (con prof. Stefano Ferretti)
- **Immagini**: ritratto di Auguste Kerckhoffs, pubblico dominio (Wikimedia Commons); logo IOTA della IOTA Foundation
- **Le dimostrazioni** girano nel browser; solo la lavagna e l'app della classe, quando le si usa, parlano con i server pubblici della rete di prova IOTA

Versione interattiva delle slide:
mirkozichichi.me/slides/smartcontractgiur2026