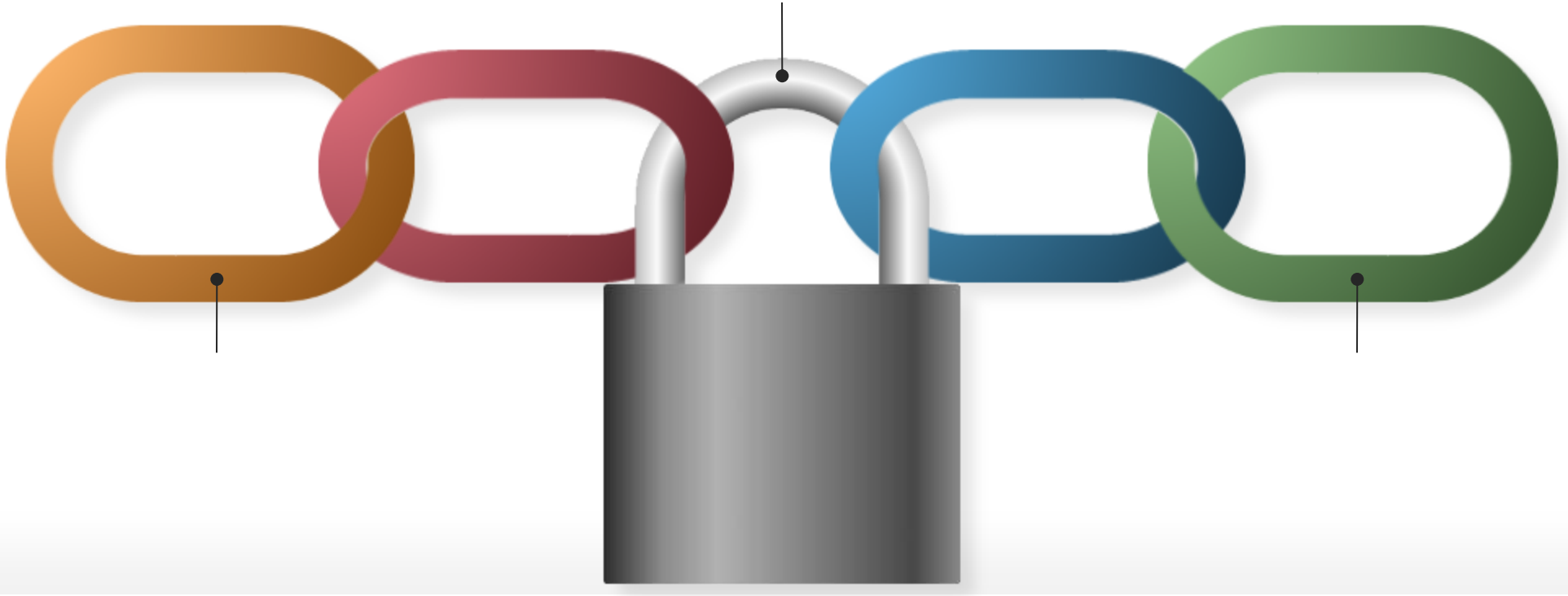
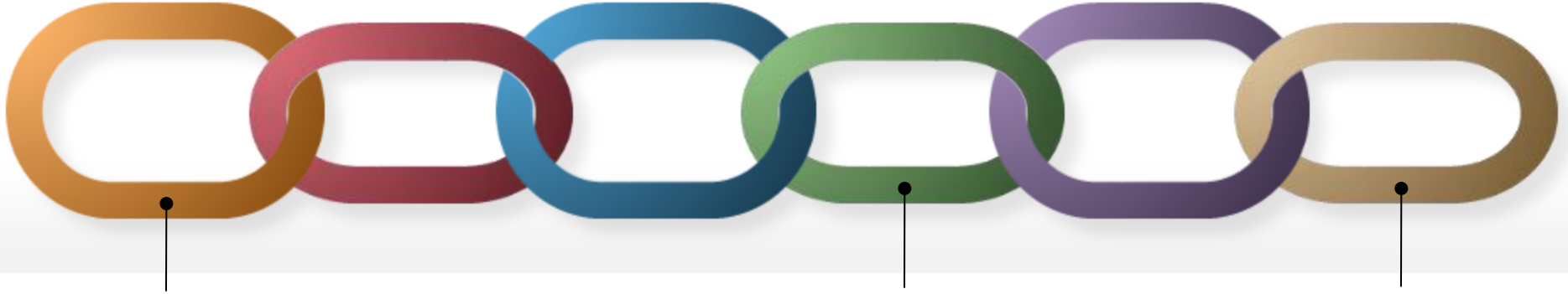


Sicurezza nelle Blockchain Pubbliche: Il Problema del Consenso

Ivan Visconti

Coordinatore CifrisChain

Università di Salerno



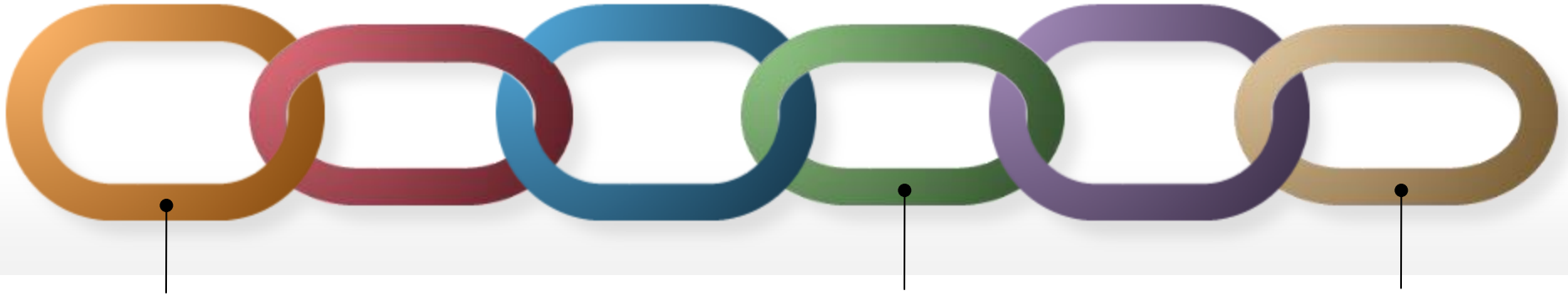
Prof. di Informatica (DIEM, Univ. di Salerno)

visconti@unisa.it

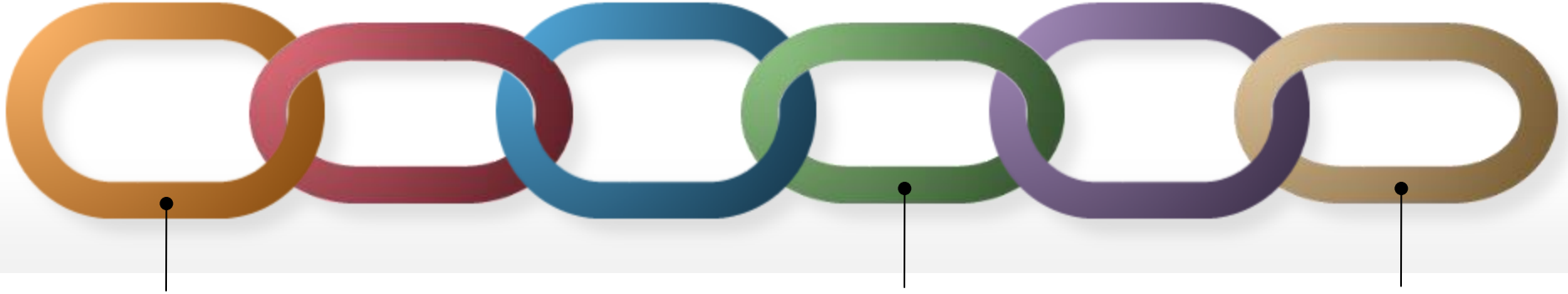
Temi di Ricerca: Zero-Knowledge Proofs e Blockchain Technology

Coordinatore di CifrisChain: oltre 100 iscritti

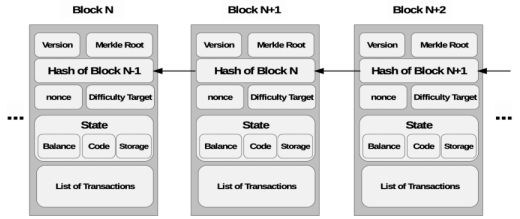
cifrischain@decifris.it



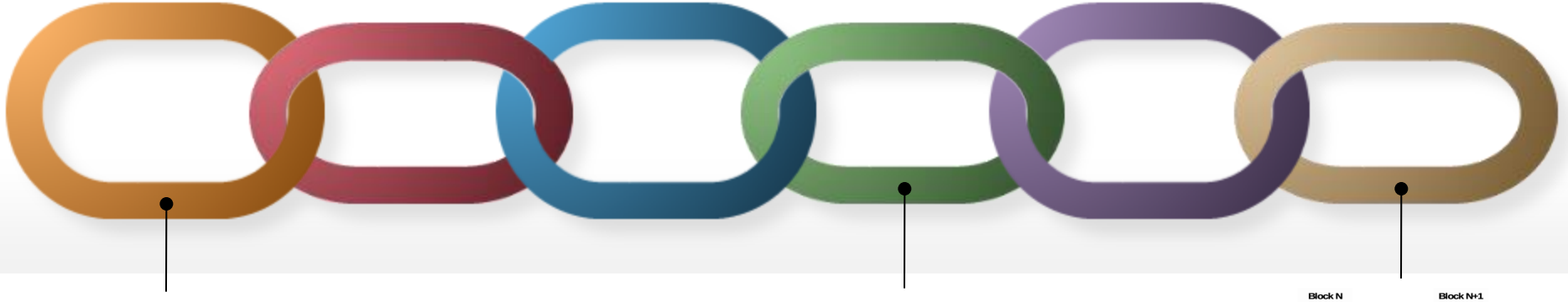
Blockchain? Che roba è?? Serve???



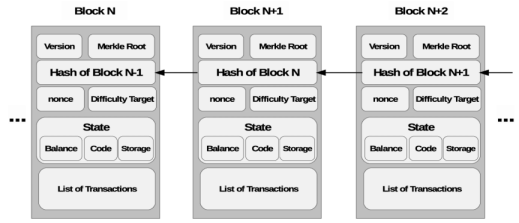
Blockchain? Che roba è?? Serve???



Una blockchain è una sequenza di blocchi collegati da una funzione hash crittografica che non può essere violata... blablabla... c'è la strategia nazionale, gli smart contract, le ICO, le crittovalute, miliardi di miliardi...



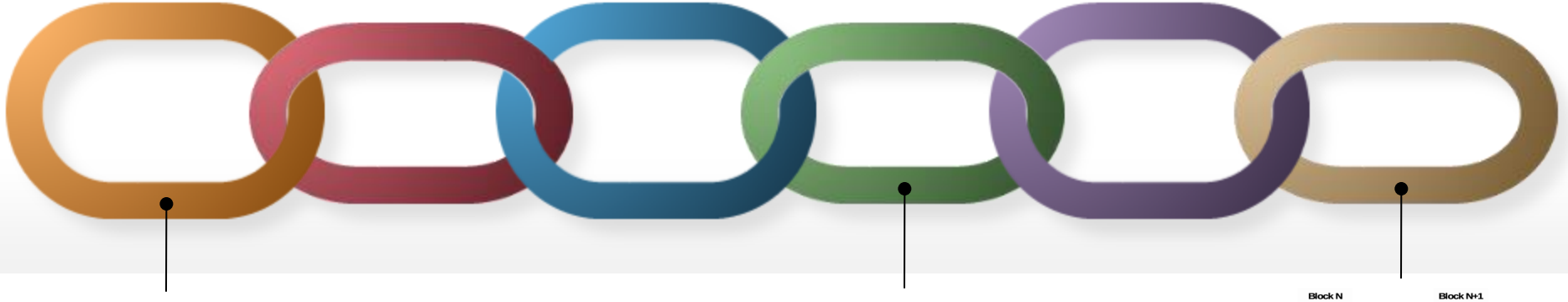
Blockchain? Che roba è?? Serve???

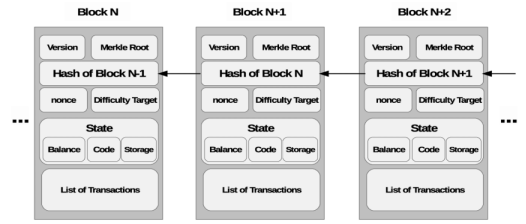


Una blockchain è una sequenza di blocchi collegati da una funzione hash crittografica che non può essere violata... blablabla... c'è la strategia nazionale, gli smart contract, le ICO, le crittovalute, miliardi di miliardi...

Serve! (non la capisco,
però spero di guadagnarci!)

Non serve! (non la capisco e la
boicotto perché non ci guadagno!)



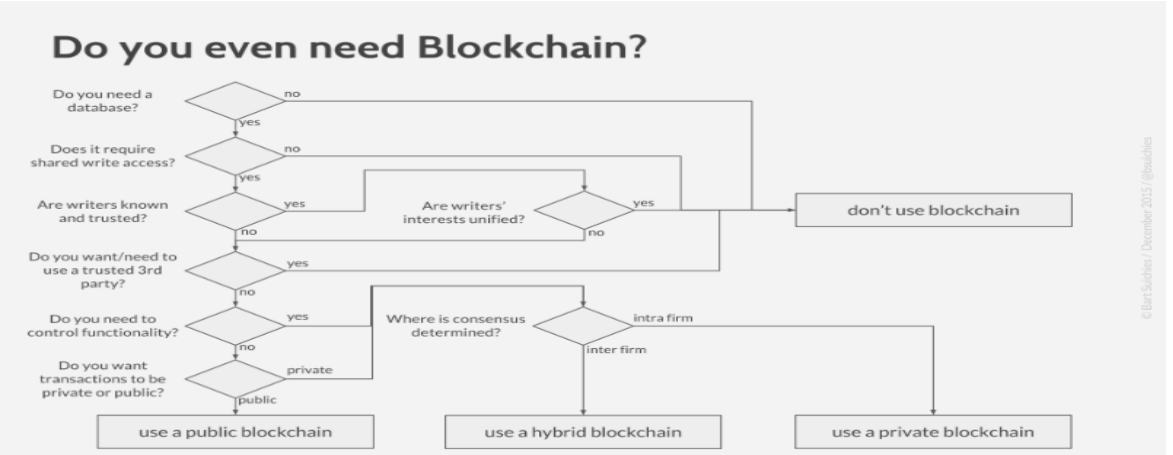


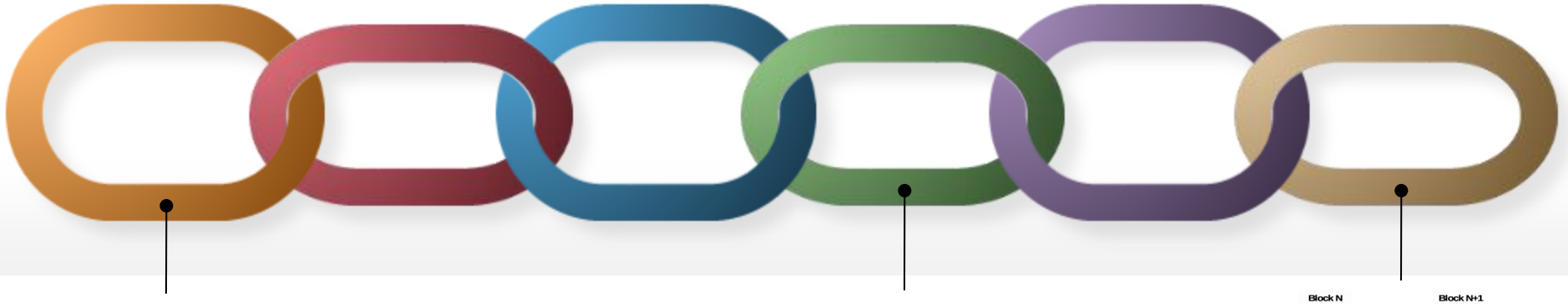
Blockchain? Che roba è?? Serve???

Una blockchain è una sequenza di blocchi collegati da una funzione hash crittografica che non può essere violata... blablabla... c'è la strategia nazionale, gli smart contract, le ICO, le crittovalute, miliardi di miliardi...

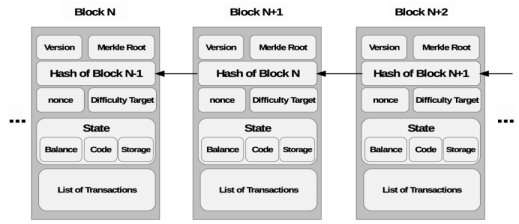
Serve! (non la capisco,
però spero di guadagnarci!)

Non serve! (non la capisco e la boicotto perché non ci guadagno!)





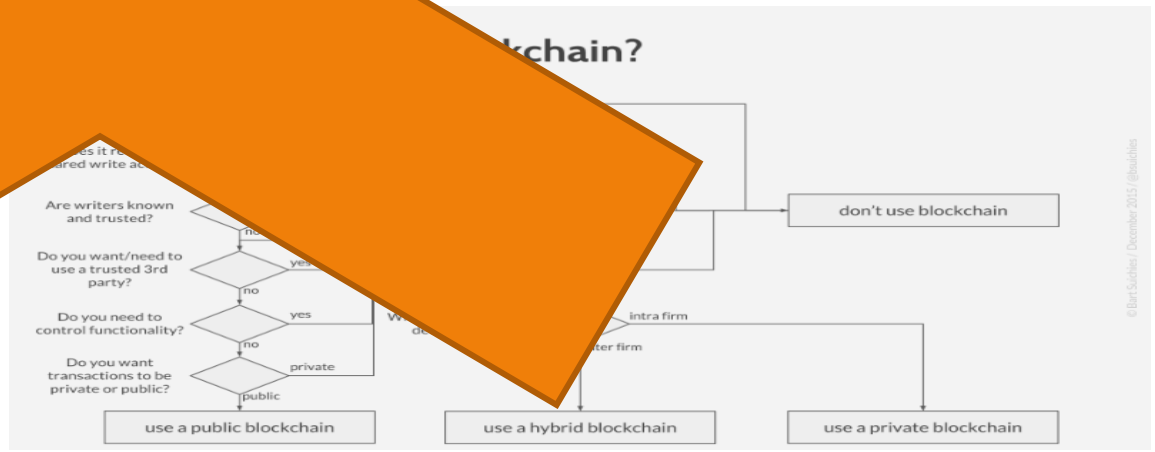
Blockchain? C roba è?? Serve??

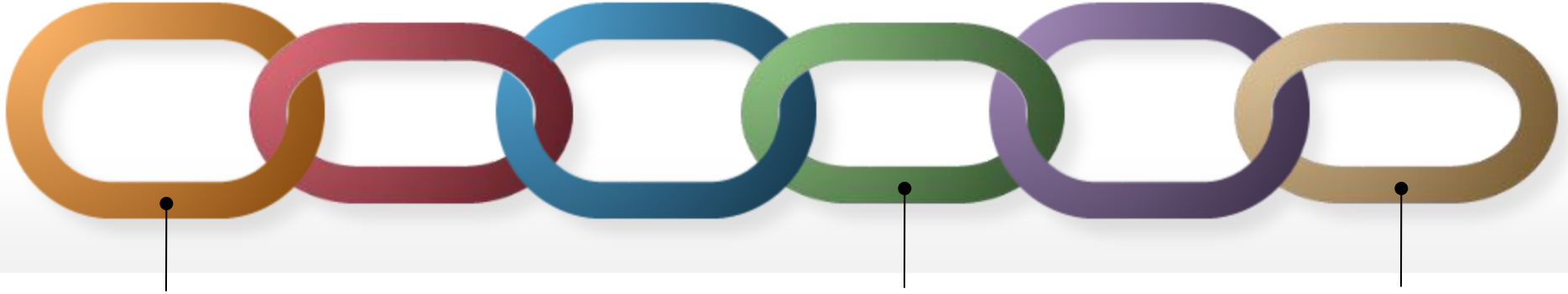


Una blockchain è u funzione hash crittografica che non pu e la strategia nazionale, gli smart contract, le ICO, le miliardi…

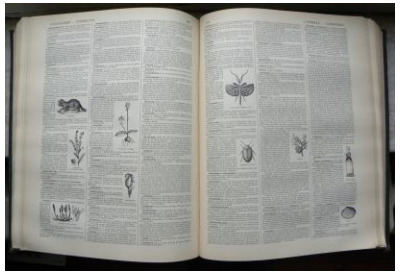
Serve! (non la capis però spero di gua

Non serve! (non la c e la boicotto perché non ci guadagno!)



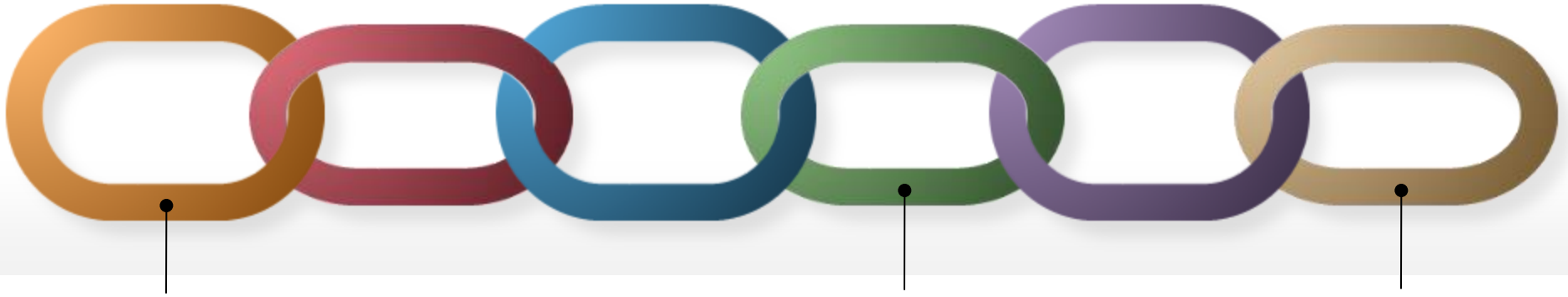


(una definizione informale di blockchain)

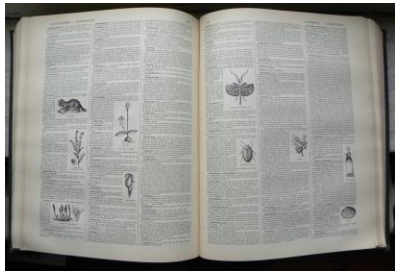


Una blockchain è una **piattaforma decentralizzata** che permette l'esecuzione di **smart contract** attraverso la validazione di transazioni che ne aggiornano lo stato

Tutte le transazioni sono **irreversibili** (immutabilità)



(una definizione informale di blockchain)



Una bl**entralizzata** che
perme**t** attraverso la
valida**z**nano lo stato

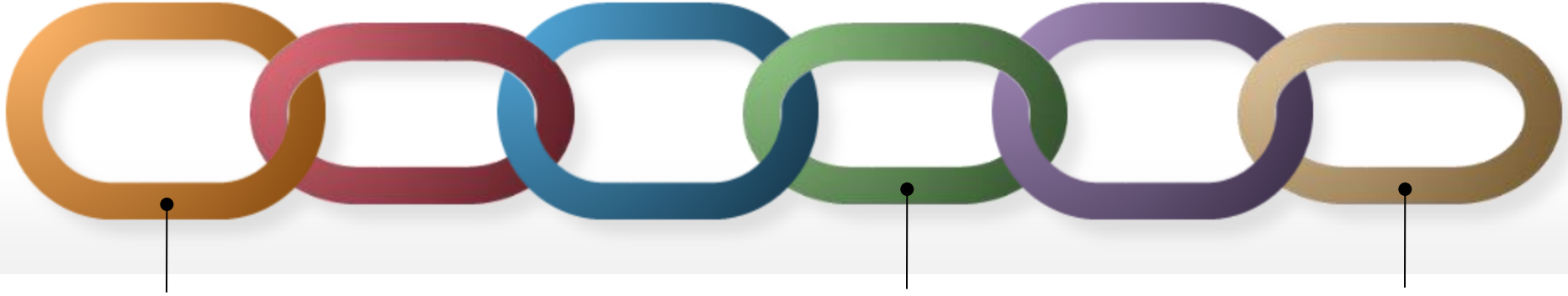
Tutte l**o**mmutabilità)

(una definizione informale di forno)

una cupola in materiale refrattario con una porta di accesso costantemente aperta, una cappa che raccorda il forno con un condotto di espulsione dei fumi ed un piano di cottura dove è possibile appoggiare ciò che deve essere sottoposto ad alte temperature

(una definizio informale di forno)

una cupola
porta di accesso
cappa che raccord
condotto di
espulsione dei
ra dove
è possibile a
io che
sottoposto ad
emperature

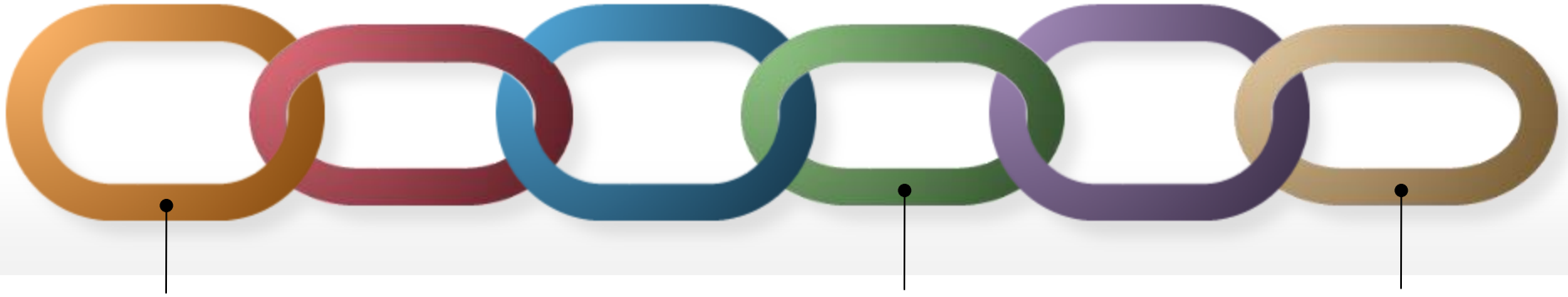


scop rte

A che pro?

Una un computer *decentralizzato* che esegue *pubblicamente* programmi (smart contract)

il programma attende un input (transazione) per eseguire un'operazione

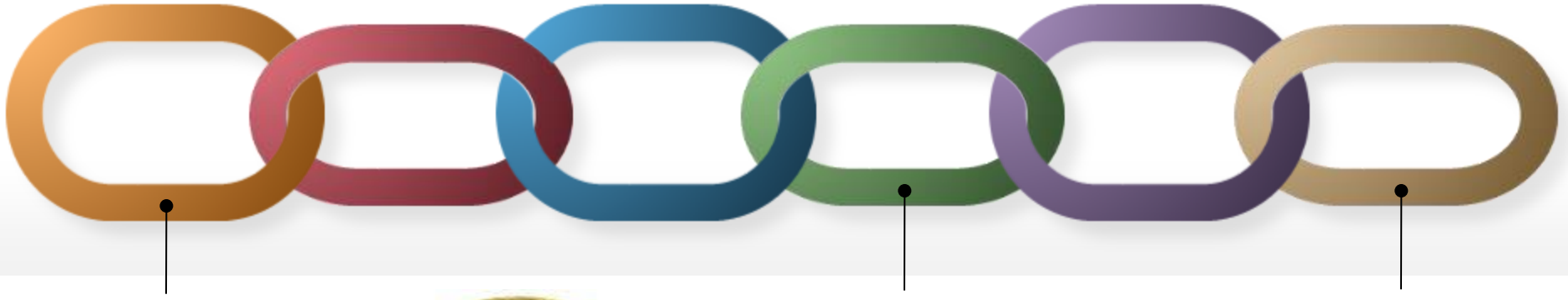


Resilienza e Trasparenza

Non sono ancora convinto.
A che servono questi programmi pubblicamente verificabili?

Il computer decentraliz
continua a funziona
correttamente anche
di attacchi su larga s

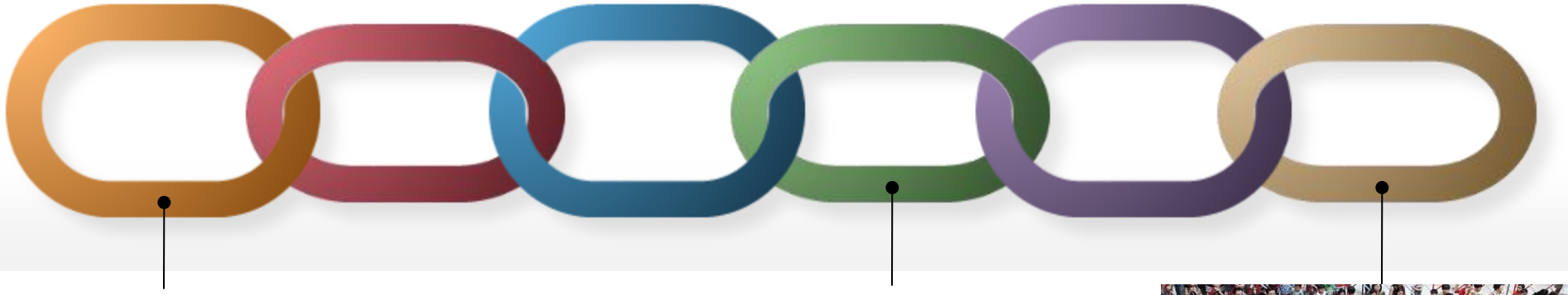
Tutti possono verificare la corre zza dello stato attuale dell'esecuzione di un programma (e dell'intero computer) grazie all'immutabilità



Bitcoin

Una blockchain con 2 programmi:
1) coniatura di monete (assegnate con una lotteria)
2) trasferimento di monete tra portafogli

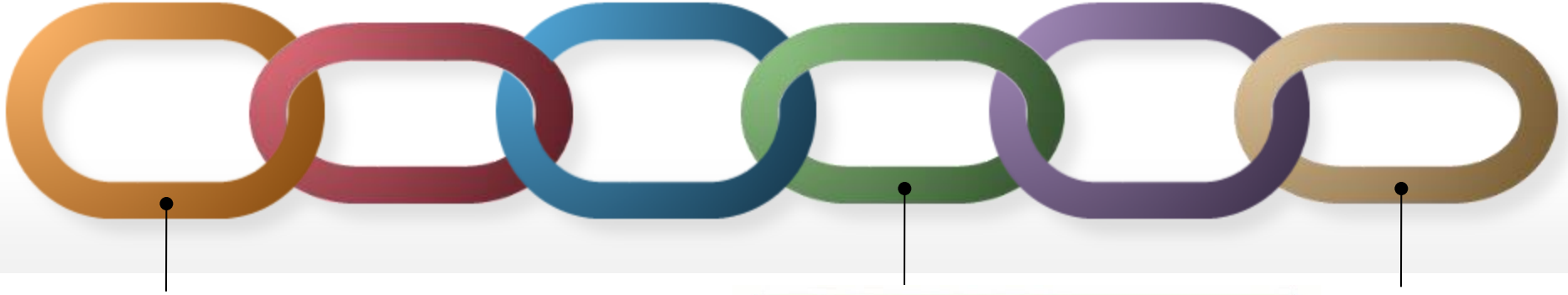
Nota: la trasparenza e la resilienza portano ad azioni impensabili in un mondo in cui di solito si agisce grazie alla fiducia in terze parti (notai, banche, foro di....)



Il fascino di Public Verifiability

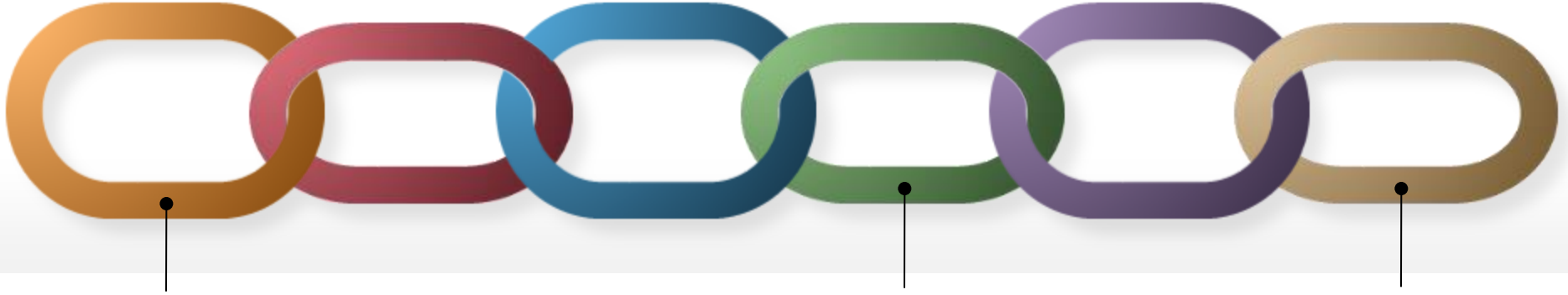
Tutti possono verificare lo stato attuale dell'esecuzione di uno smart contract a partire dalla sua creazione.
La **trasparenza** porta fiducia e partecipazione

per ogni bitcoin, è possibile verificare tutti i portafogli che lo hanno custodito dalla sua coniazione fino a quello corrente



In altre parole....

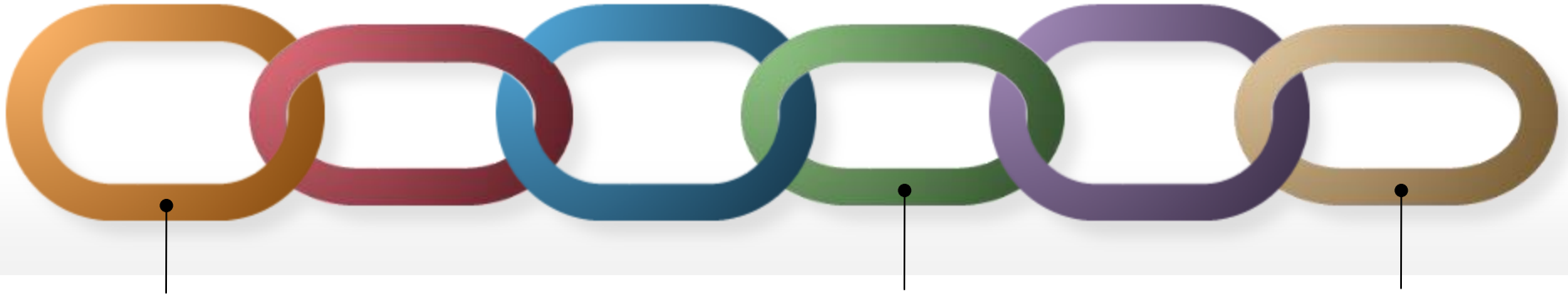
La tecnologia blockchain è un dirompente strumento per l'anticontraffazione

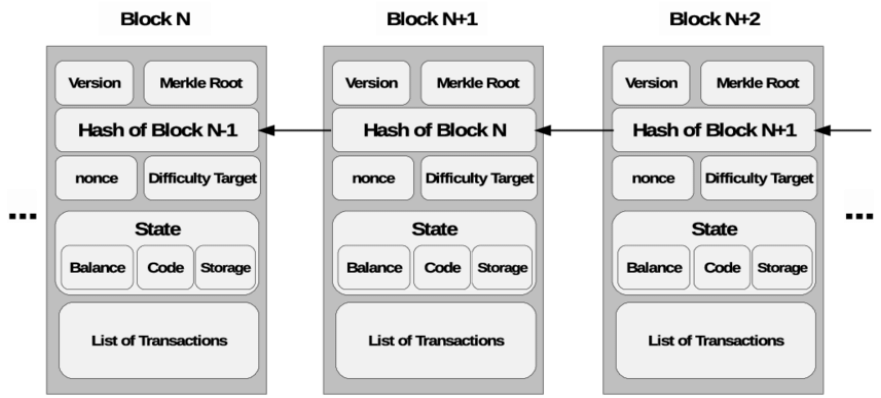


se

Perché si chiama blockchain?

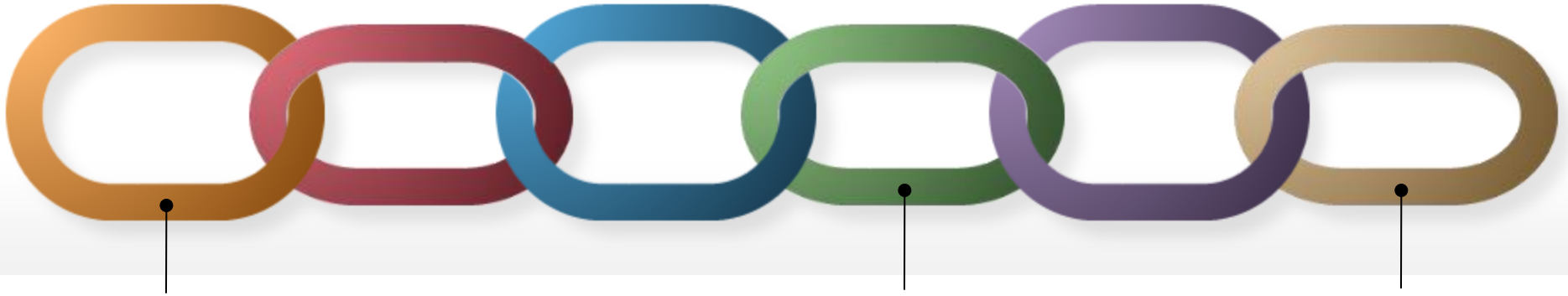
Una blockchain è un computer *decentralizzato* che esegue programmi (smart contract)



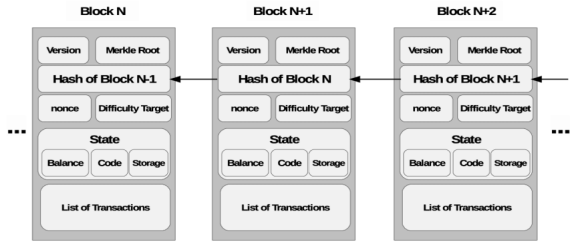


Blockchain

è lo strumento utilizzato da Satoshi Nakamoto per costruire Bitcoin, la prima blockchain/cryptocurrency

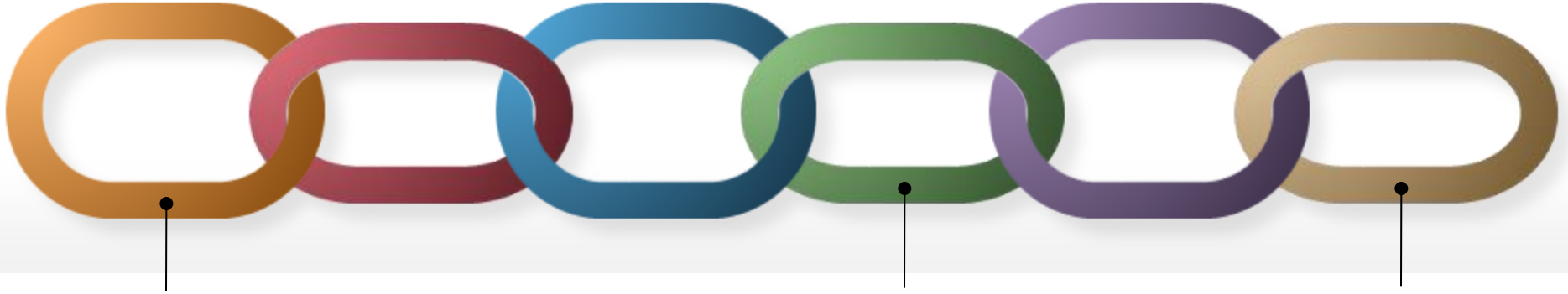


E’ facile da costruire una blockchain?

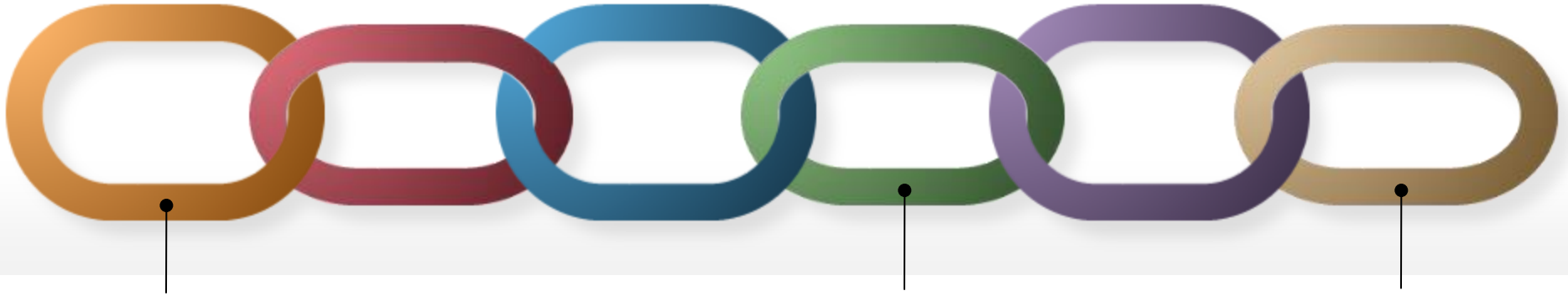


La sequenza di blocchi (o qualunque altra tecnica) identifica le operazioni del computer decentralizzato

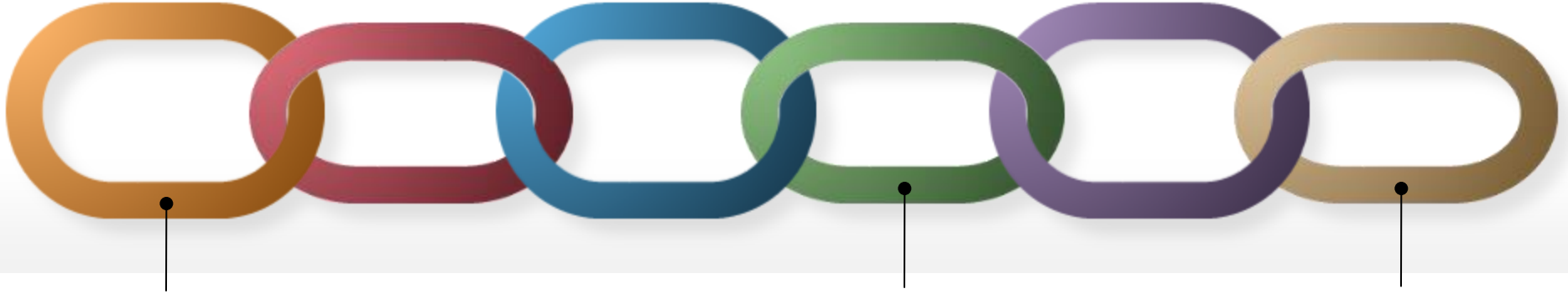
C’è il problema di stabilire il prossimo blocco, cioè quali sono le prossime cose che farà il computer:
Problema del Consenso



Il Problema del Consenso

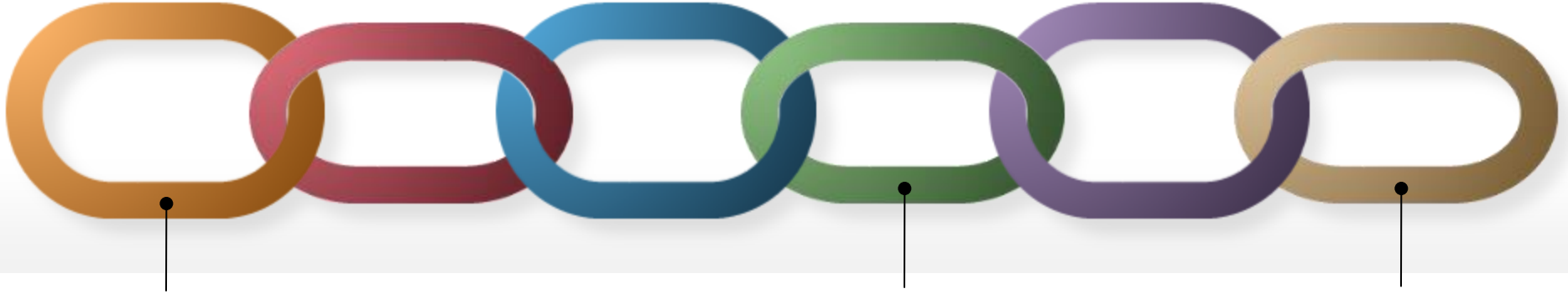


Il Problema del Consenso: tutto risolto negli anni 80



Il Problema del Consenso: tutto risolto negli anni 80

Maggioranza onesta?
c'è un modo veloce per metterci d'accordo
(ma se siamo in troppi diventa lentissimo)



Il Problema del Consenso: tutto risolto negli anni 80

Maggioranza onesta?
c'è un modo veloce per metterci d'accordo
(ma se siamo in troppi diventa lentissimo)

Maggioranza disonesta?
non c'è speranza

Quindi senza identificazione è impossibile

con un po’ di elementari
clonazioni gli imbroglioni
raggiungono facilmente
la maggioranza

gli accademici si sono gongolati
per 25 anni e poi…

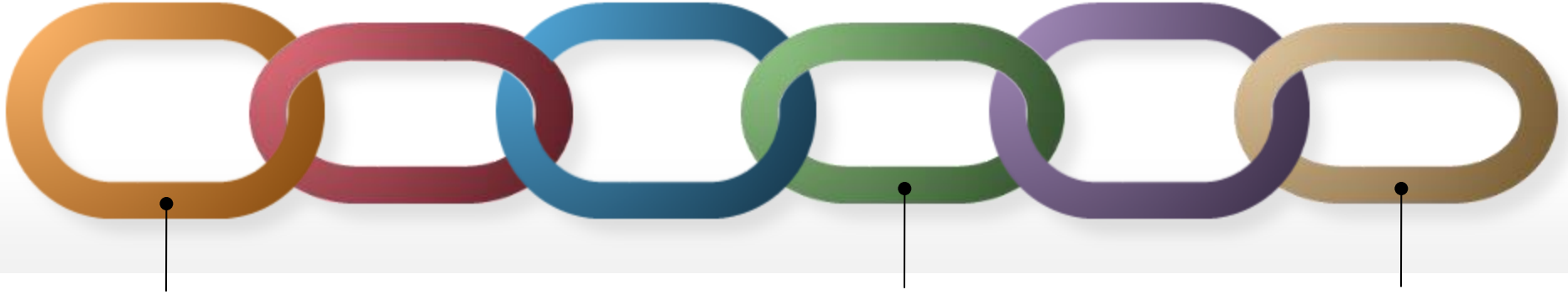
L'idea geniale di Nakamoto

da una persona ➔ un voto

L'idea geniale di Nakamoto

da una persona ➔ un voto

a una "computazione" ==> un biglietto (stile gratta e vinci)

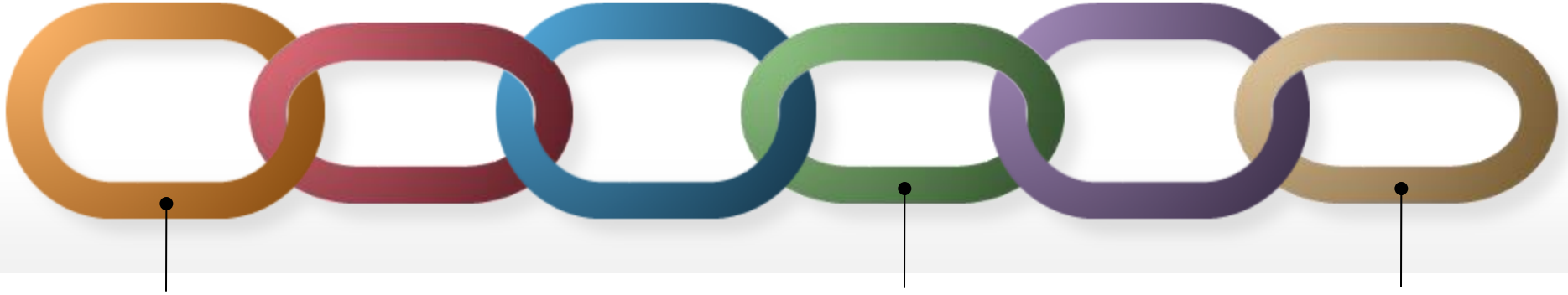


L'idea geniale di Nakamoto

da una persona ➔ un voto

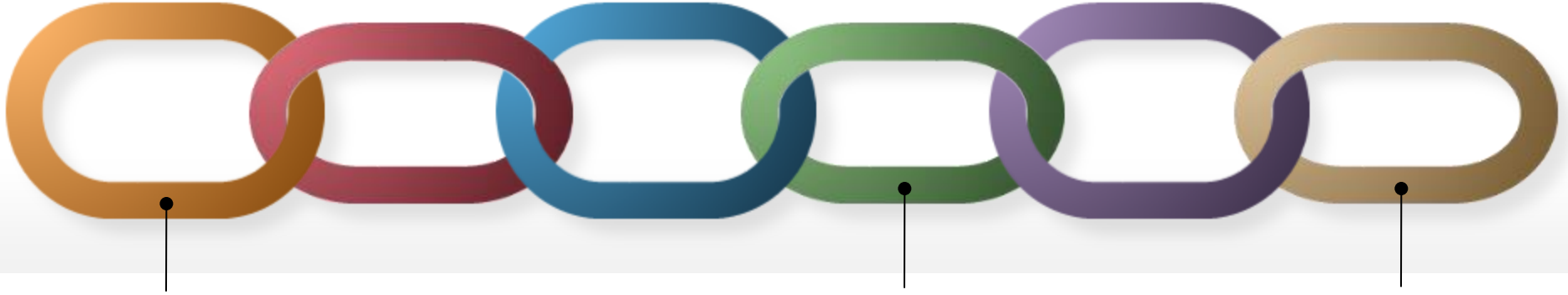
a una "computazione" ==> un biglietto (stile gratta e vinci)

non parli con nessuno, fai dei calcoli (**proof of work, PoW**) e se vinci lo annunci… EUREKA! veloce e robusto!
il premio attira potenza di calcolo onesta > malevola



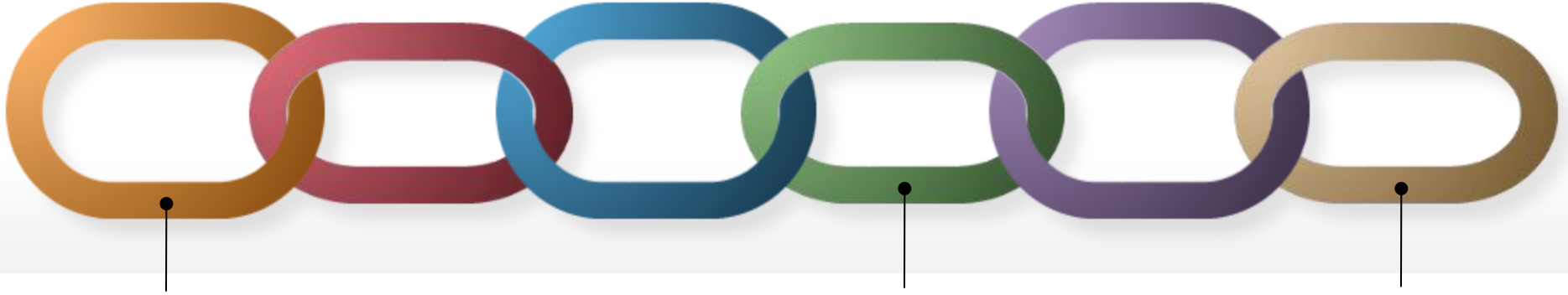
Dove siamo nel 2019 rispetto a Proof of Work

- validato su carta
  (dimostrato essere matematicamente corretto
  su assunzioni ragionevoli di rete e computazionali)



Dove siamo nel 2019 rispetto a Proof of Work

- validato su carta
  (dimostrato essere matematicamente corretto
  su assunzioni ragionevoli di rete e computazionali)
- validato in pratica

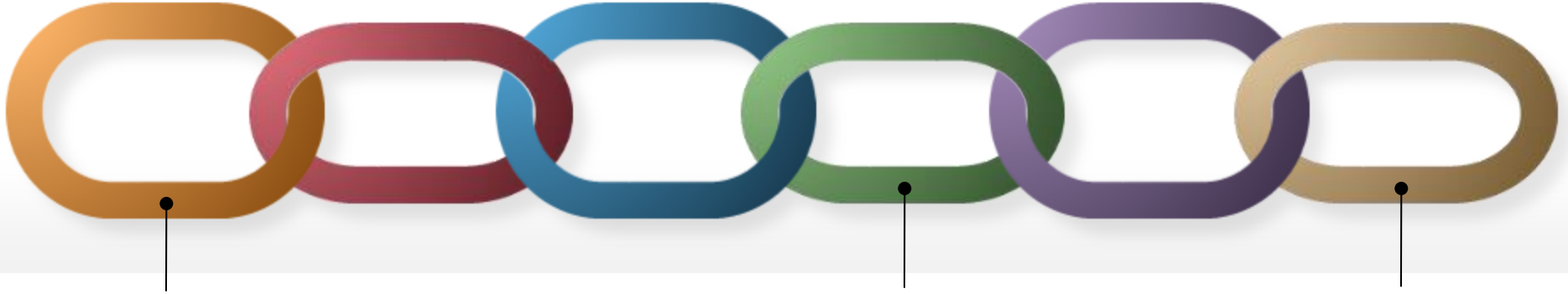


Dove siamo nel 2019 rispetto a Proof of Work

- validato su carta
  (dimostrato essere matematicamente corretto
  su assunzioni ragionevoli di rete e computazionali)
- validato in pratica

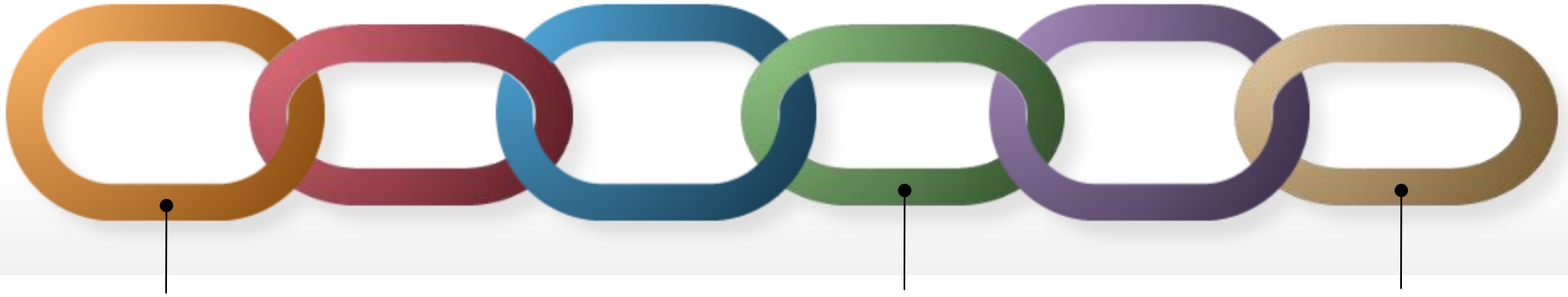
Problema

Bitcoin consuma più energia elettrica dell'Irlanda



Alternative più sostenibili?

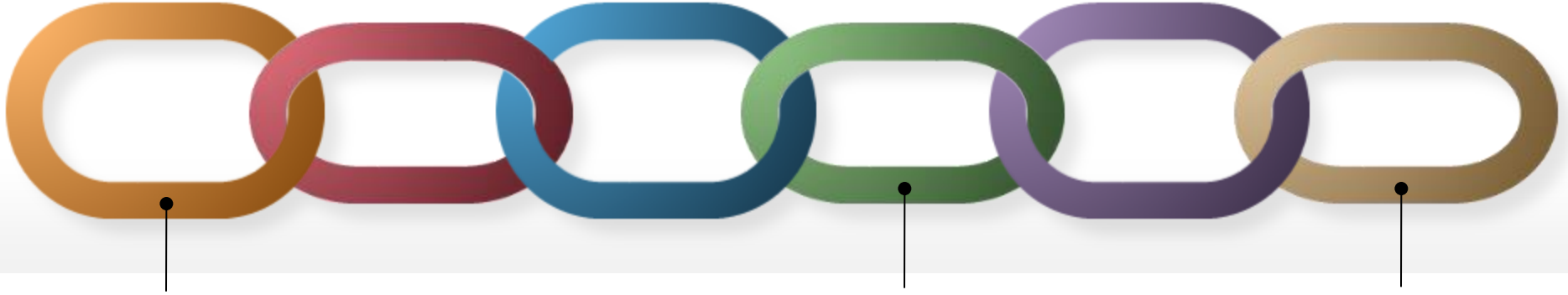
Molti puntano su *Proof of Stake*



Alternative più sostenibili?

Molti puntano su *Proof of Stake*

Una "moneta" ==> un biglietto

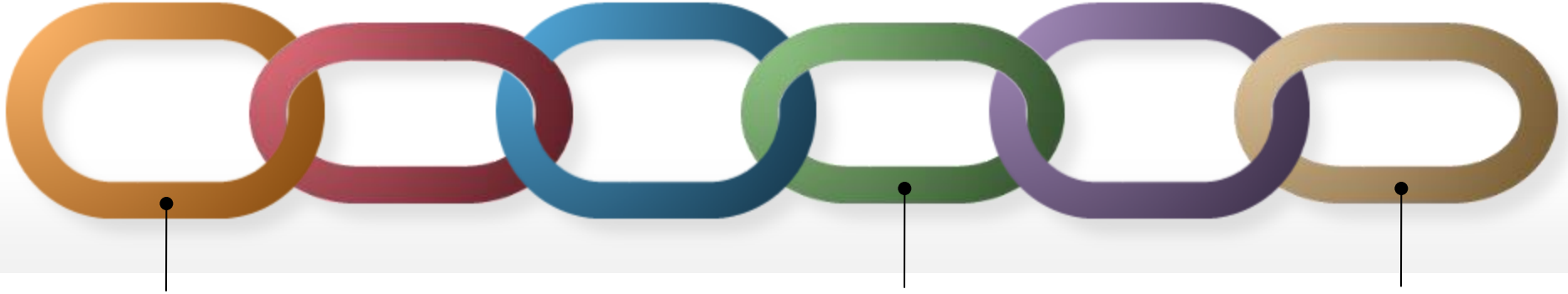


Alternative più sostenibili?

Molti puntano su *Proof of Stake*

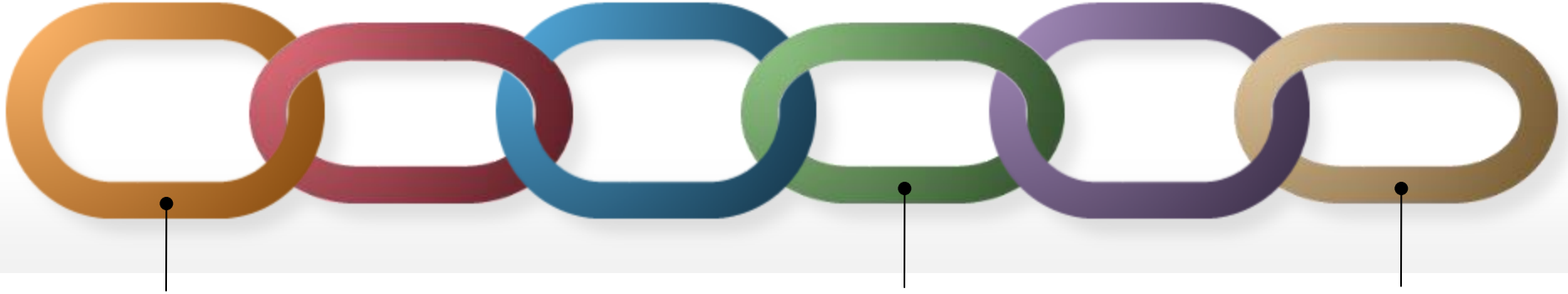
Una "moneta" ==> un biglietto

Il computer decentralizzato è affidabile purché la ricchezza dei "corrotti" resti minoritaria nella rete



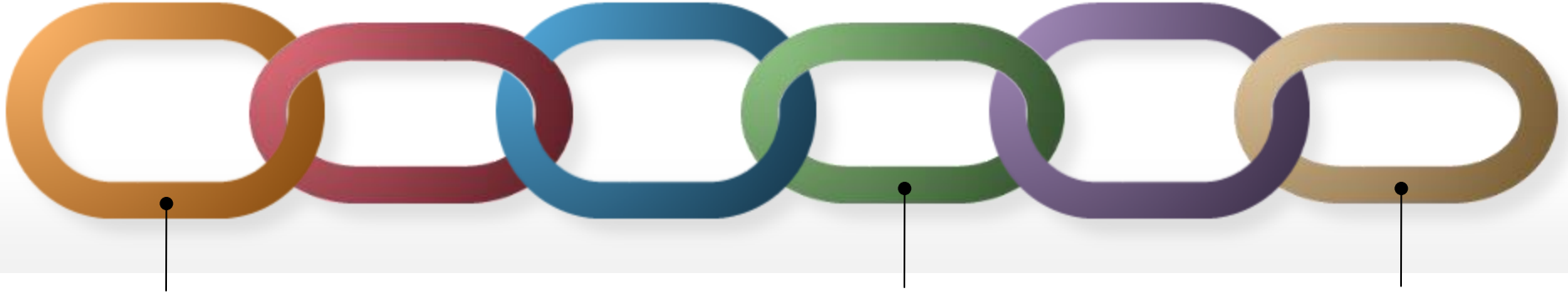
Dove siamo nel 2019 rispetto a Proof of Stake

- parzialmente validato su carta
  (dimostrato essere matematicamente corretto
  ma su assunzioni di rete e finanziarie meno limpide)



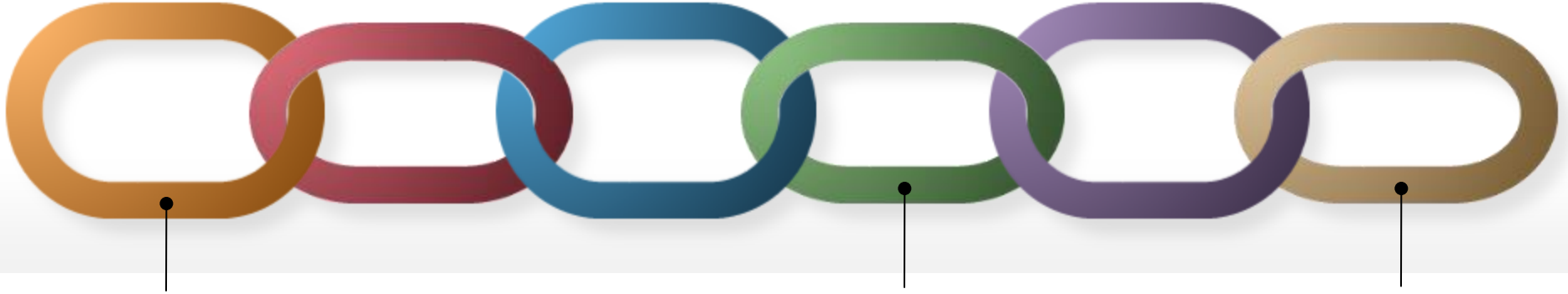
Dove siamo nel 2019 rispetto a Proof of Stake

- parzialmente validato su carta
  (dimostrato essere matematicamente corretto
  ma su assunzioni di rete e finanziarie meno limpide)
- nel tempo diverse falle (non applicabili a proof of work) e pezze (es. long range attack, nothing at stake, attack of the clones, problemi di privacy)



Dove siamo nel 2019 rispetto a Proof of Stake

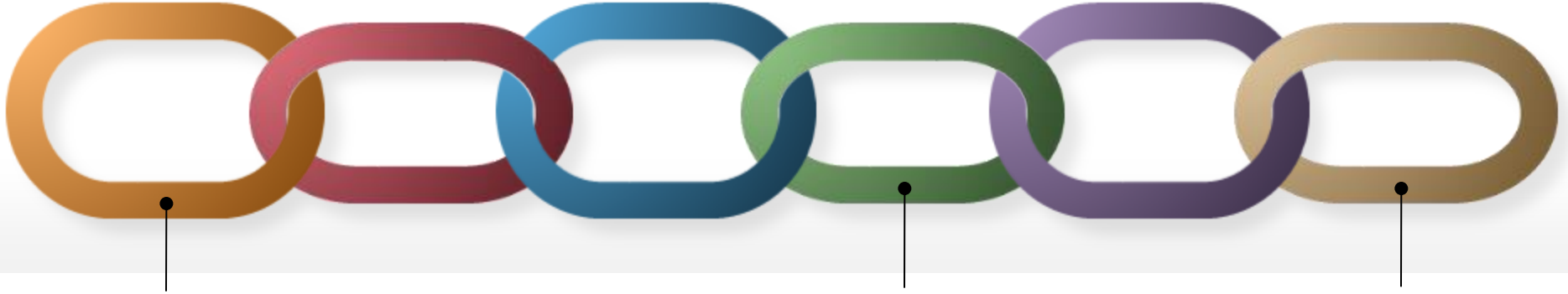
- parzialmente validato su carta
  (dimostrato essere matematicamente corretto
  ma su assunzioni di rete e finanziarie meno limpide)
- nel tempo diverse falle (non applicabili a proof of work) e pezze (es. long range attack, nothing at stake, attack of the clones, problemi di privacy)
- non ampiamente validato in pratica



Dove siamo nel 2019 rispetto a Proof of Stake

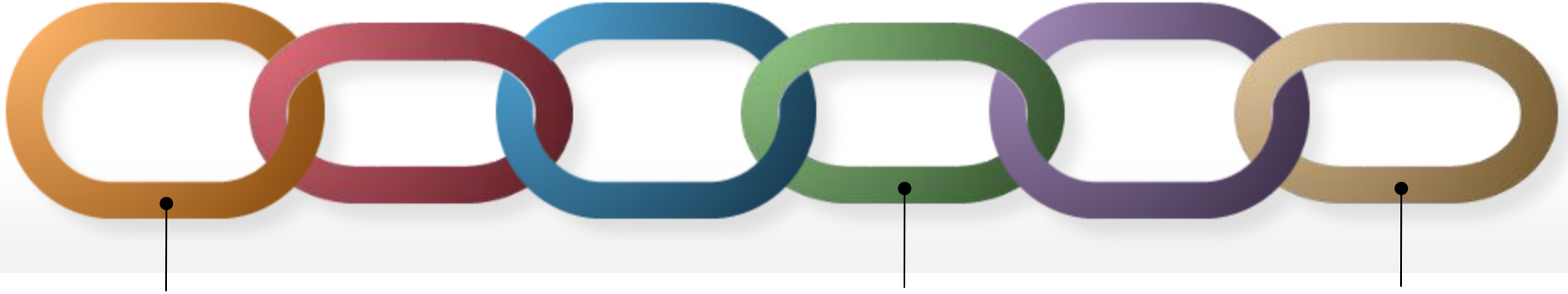
- parzialmente validato su carta
  (dimostrato essere matematicamente corretto
  ma su assunzioni di rete e finanziarie meno limpide)
- nel tempo diverse falle (non applicabili a proof of work) e pezze (es. long range attack, nothing at stake, attack of the clones, problemi di privacy)
- non ampiamente validato in pratica
- grandi e promettenti investimenti in questa direzione

(Cardano, Dfinity, Ethreum, Filecoin, Algorand, Concordium, Snow White…)



Conclusioni

La tecnologia blockchain se compresa ed utilizzata propriamente in sinergia con altre tecnologie offre un'alternativa credibile e trasparente a tanti processi oggi contaminati dalla contraffazione e dall'inaffidabilità.



Vi ringrazio per il tempo dedicatomi