

## CONSENSO DI NAKAMOTO

Il consenso di Nakamoto viene impilato in blockchain:

- permissionless
- aperti

e in quei sistemi dove i preferite -allego  
AVAILABILITY over consistency (AP).

In diretta contrapposizione al consenso  
PBFT (Practical Byzantine Fault Tolerant) il  
quale viene impilato in blockchain:

- permissioned
- chiusi

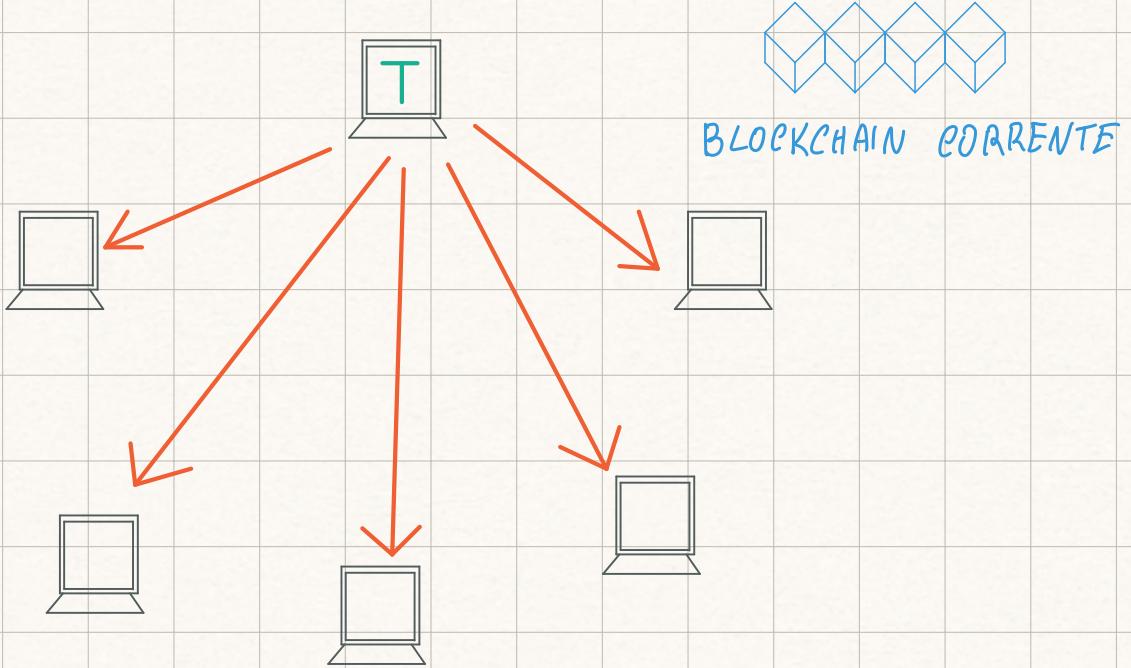
e in quei sistemi dove i preferito avere  
CONSISTENCY over availability (CP).



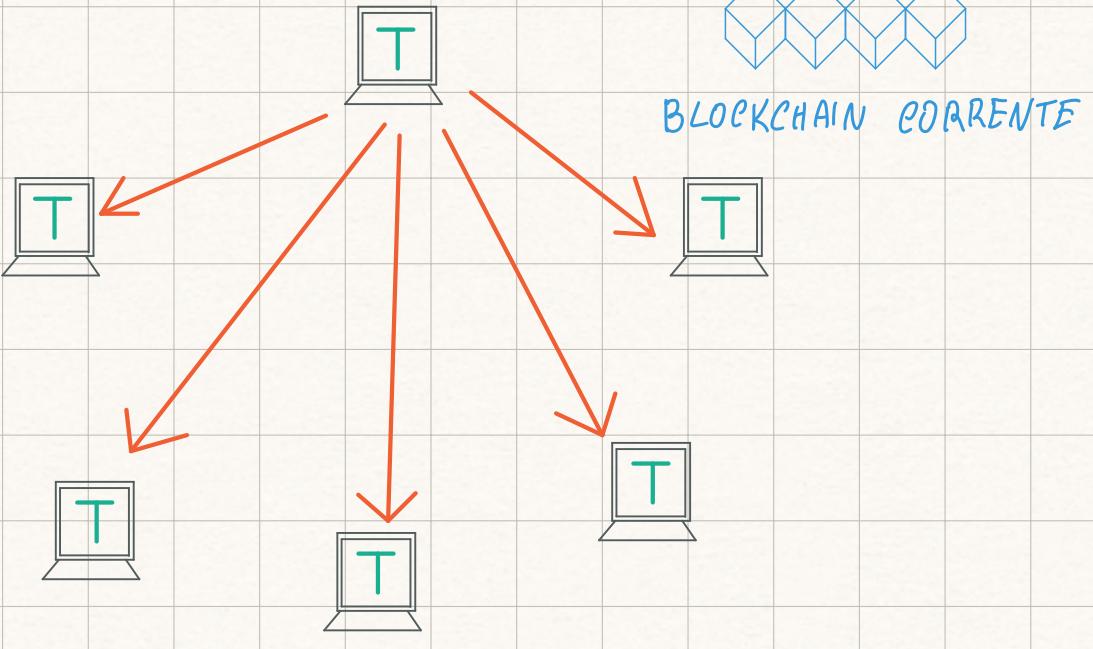
Satoshi Nakamoto (?)

## CONSENSO DI NAICAMOTO

1. Una nuova transazione T viene generata da un nodo e viene inviata in Broadcast a tutti gli altri nodi.

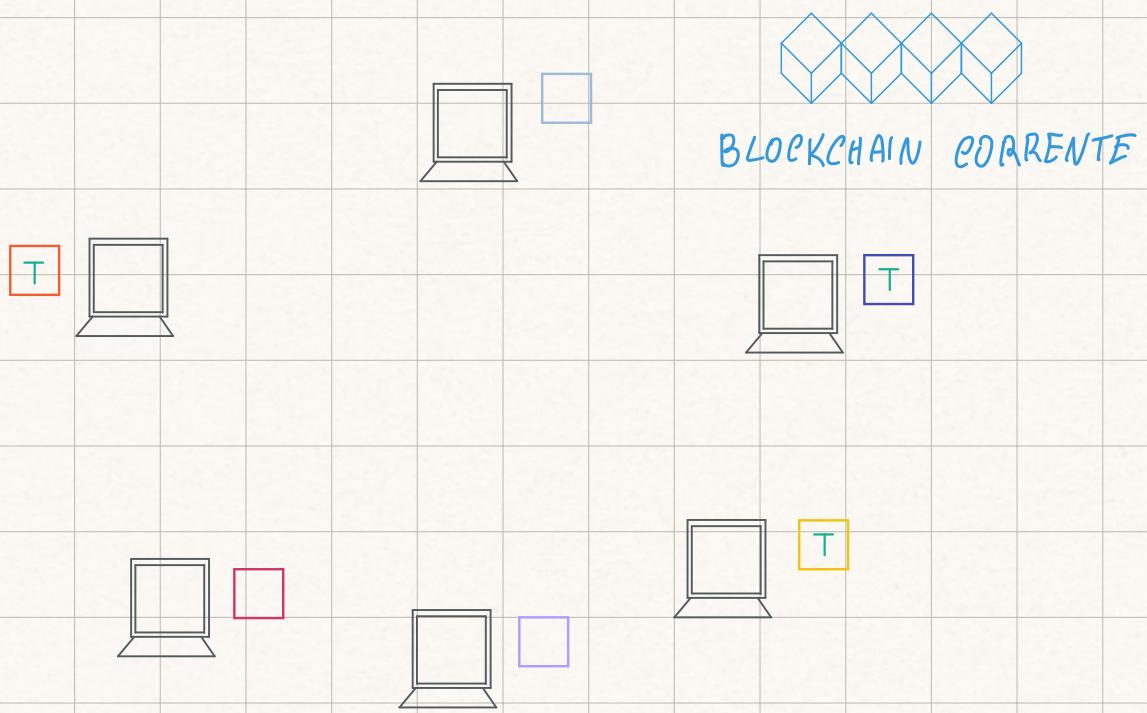


2. I nodi ricevono T e decidono se includere T nel blocco che stanno creando oppure no. Un blocco è considerato "pieno" quando ha 500 transazioni al suo interno.

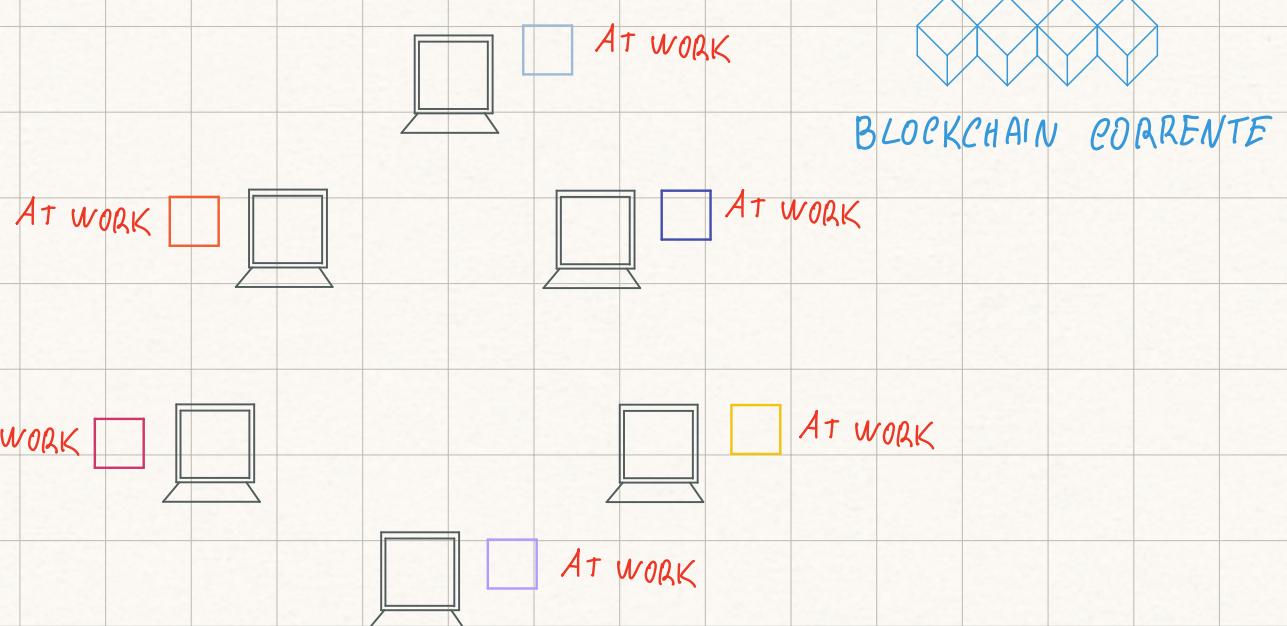


I nodi prima di inserire la transazione nel proprio blocco, controllano se la transazione è valida.

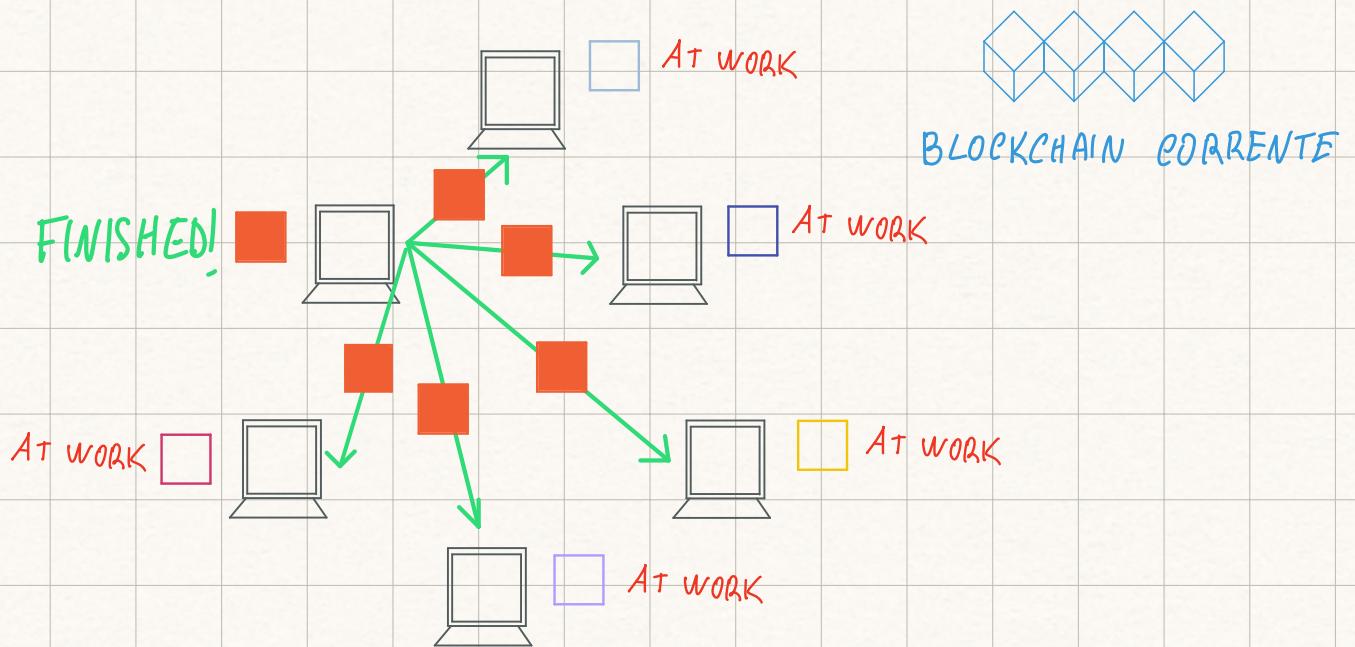
Questo controllo è effettuato in automatico, seguendo circa 20 regole per decidere se una transazione è valida oppure no.



3. I nodi, una volta preparato il blocco con il numero sufficienti di transazioni (500, per il peso di 1MB), vanno alla ricerca della PoW per il proprio blocco.



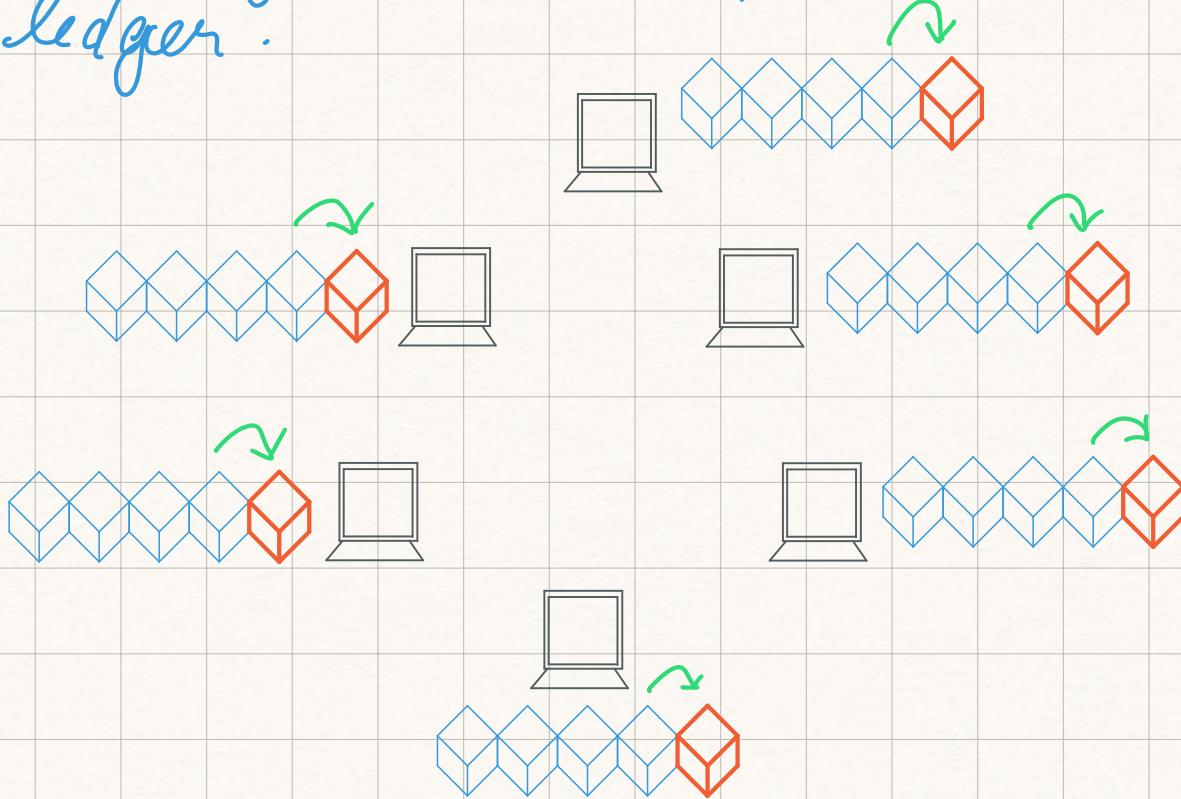
4. Ci sarai un modo ogni minuto che atterrerà la PoW. Il modo che l'ha trovata, invia il blocco in gossiping a tutti gli altri nodi.



5. Ogni nodo, alla ricezione del blocco, eseguirà:

- che tutte le transazioni sono valide
- che le transazioni non sono relative ad un bene già speso
- che la PoW è valida. Per controllare ciò il nodo calcola di nuovo l'hash del blocco usando la moneta fornita come PoW, verificando che l'hash risultato sia effettivamente più piccolo del valore hash target.

6. Se i nodi fanno tutto a buon fine, il blocco viene aggiunto alla copia locale del ledger.



# POW & ONESTÀ

La PoW è l'esito della ricerca di una monce da parte di un minatore, per poter validare il proprio blocco di transazioni. La difficoltà della ricerca della PoW viene regolata ogni due settimane per far sì che venga minato 1 blocco al minuto. Questa regolazione della difficoltà è necessaria in quanto sempre più macchine sono in grado di effettuare computazioni esponenziali. La PoW è un meccanismo che serve a:

- **SCORAGGIARE**: Gli modi maliziosi devono spendere molta patenza di calcolo e quindi molte risorse economiche in HW ed energia elettrica. Non alla portata di tutti.

- **RENDERE MATEMATICAMENTE IMPOSSIBILE**:

memorizzare di un blocco, in quanto quest'è comprensibile a dover calcolare di nuovo l'hash di tutti i blocchi precedenti, ovvero a doverli ricalcolare una nuova PoW fino al generis block. La PoW rende anche quasi impossibile l'attacco del 51% in quanto ci'

dovebbe avere una maggioranza di nodi maliziosi in grado di effettuare computazioni esponenziali, e questo è quasi impossibile.

## REWARD

Oltre all' "intimidazione" della PoW, viene utilizzato anche un meccanismo di REWARD per ricompensare i Miner che hanno esibito con successo una PoW. La reward serve a due scopi:

- incentivare i nodi a rimanere onesti
- permettere un'immagine costante di nuova valuta all'interno del sistema.

## ATTACCHI & FORK

La propagazione e l'accettazione di un blocco da parte di un nodo, abbiamo visto essere un problema di consensus. Sappiamo però che in un sistema olistribuito asincrono, nè anche un solo nodo fallisce non è garantito che il consenso è raggiungibile. Per questo

motiv i son stati rilasciati: vincoli di raggiungimento del consenso, alla possibilità che possa esistere un sottogruppo di modi disponibili, al patto che i modi restanti rimangano in maggioranza.

Questo rende l'attacco del 51% possibile in teoria.

### FORK:

Una Fork è una incrinatura del ledger locale al modo in quale, da un certo punto nel tempo, i dati spariscono (eventual consistency). Essa è generata:

- per caso: in caso due mining, dopo aver trasmesso la POW per il proprio blocco, inviano il blocco agli altri nodi, ma accadeva che alcuni nodi ricevessero un blocco e gli altri, l'altro blocco. Quando viene generato il blocco successivo, questo farà riferimento soltanto ad uno dei due blocchi precedenti. - Questo permetterà la rimozione della FORK e di raggiungere consistenza

- in modo malizioso: si cerca di generare -apporta una Bifurcazione- affinché i nodi onesti si portino sul ramo malizioso. Diversi modi per fare ciò:

- SELFISH MINING: un gruppo di nodi maliziosi tengono per sé i blocchi validati: creando così un ramo malizioso parallelo. Questo ramo viene pubblicato strategicamente quando esso supera in lunghezza il ramo principale.

Un altro possibile attacco è l'attacco Elline.

Questo attacco consiste nell'oscurare porzioni di reti in modo da rendere gruppi di nodi onesti impossibilitati a partecipare al consensus. In questo modo i nodi maliziosi limitano il potere onesto.

# Proof of Stack

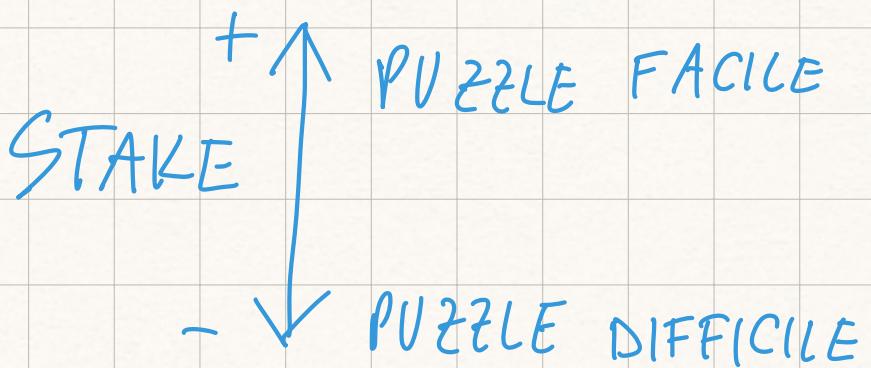
LIMITAZIONE PROOF OF WORK:

- GRANDE SPRECO DI ENERGIA E RISORSE

Proof of Stack risolve questo problema in questo modo:

1. Nella PoW, in base alla capacità di calcolo di un Miner, esso era in grado di risolvere l'enigma crittografico prima degli altri e preparare un nuovo blocco oppure no. Quindi la possibilità per un Miner di preparare un nuovo blocco era direttamente proporzionale alla sua capacità di calcolo. Nel PoS, invece che giudicare tale chance di preparare un blocco dalla capacità di calcolo, viene usato un altro parametro. Lo **STAKE**, il quale è un indicatore del portafoglio del miner.

2. Più è alto lo STAKE, più facile è l'enigma crittografico da risolvere.



Questo evita competizioni e riduce il scommesso energetico. Inoltre uno STAKE è impossibile da falsificare e quindi è più sicuro rispetto ad considerare il potere computazionale che potrebbe comunque essere attuato.

L'attacco del 51% è possibile ma questo significherebbe che i nodi maliziosi dovrebbero detenere il 51% della quantità di Criptovaluta e questo è davvero molto poco verosimile.

3. Questo può significare che non ci sono più ricompense per la validazione dei blocchi; bensì: mineri prendono una commissione le transazioni che validano.

*num*

Il problema del POS è che da una influenza  
proporzionata alle persone che sono già  
ricche.