

Bitcoin: P2P Digital Currency

Marco Mantilacci

Cristiano Santoni



Università degli Studi di Perugia

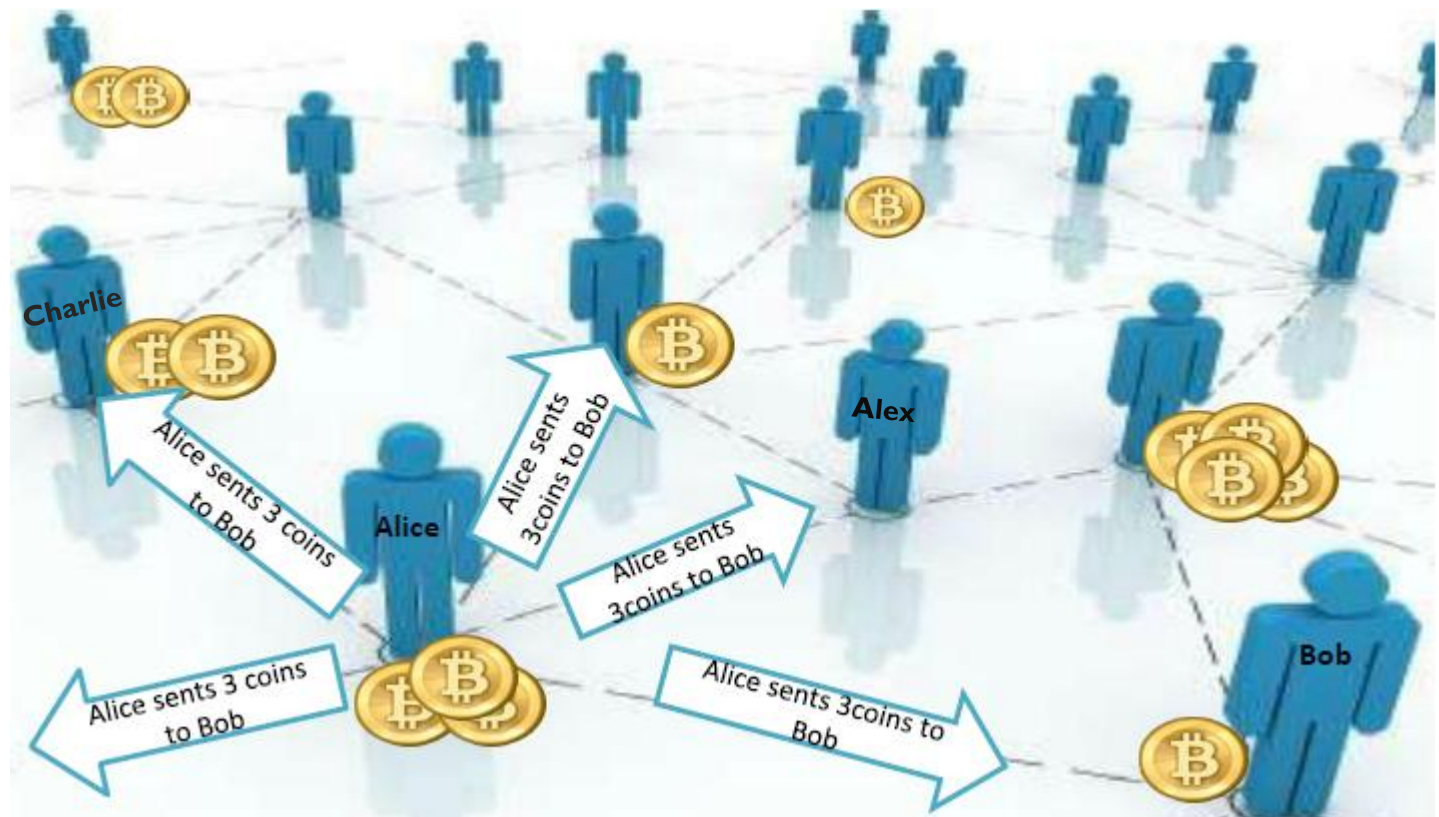
Introduzione

Attualmente i pagamenti in modalità elettronica vengono per lo più effettuati mediante carta di credito. Vediamo un esempio nello schema seguente :



Bitcoin

La rete Bitcoin non prevede la presenza di intermediari fidati come le banche, ma essa è basata su una rete peer-to-peer in cui tutti i nodi contribuiscono a mantenere “onesto” il sistema.



bitcoin

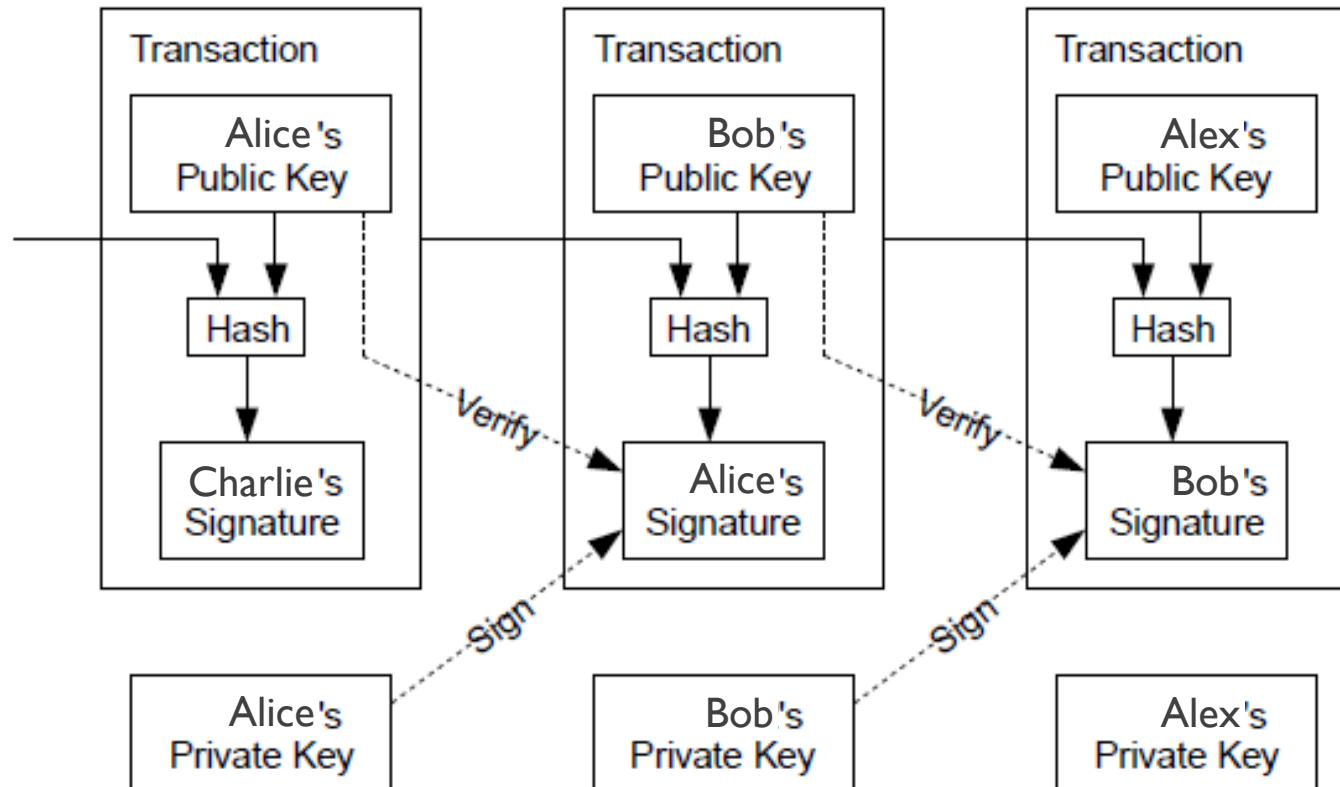
I bitcoin (BTC) sono l'unità monetaria fondamentale del sistema, essi sono rappresentati da una catena di firme digitali che vengono scambiati tra gli utenti al fine di effettuare pagamenti.

Al fine di evitare l'inflazione di questa moneta è stato fissato a 21 milioni il tetto massimo di BTC in circolazione. Nel caso in cui questa moneta subisse un andamento deflazionistico, è possibile dividere i BTC fino all'ottava cifra decimale (0.01 μ BTC) al fine di permettere pagamenti di valore "ordinario" anche in tale situazione.



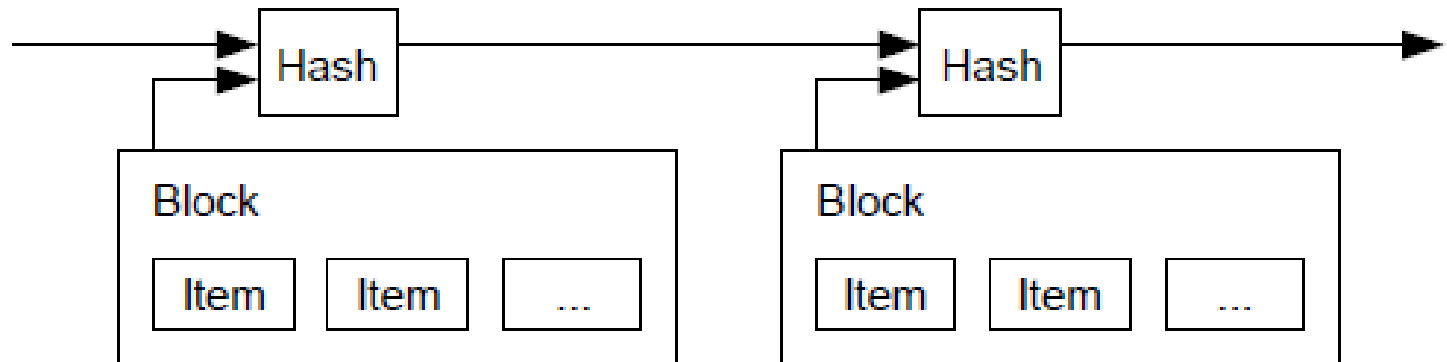
Transazioni

Le transazioni sono gli elementi che rappresentano gli scambi di somme tra gli utenti Bitcoin. Inoltre le transazioni riguardanti uno stesso “gettone”, messe in catena, vanno anche a comporre il bitcoin stesso.



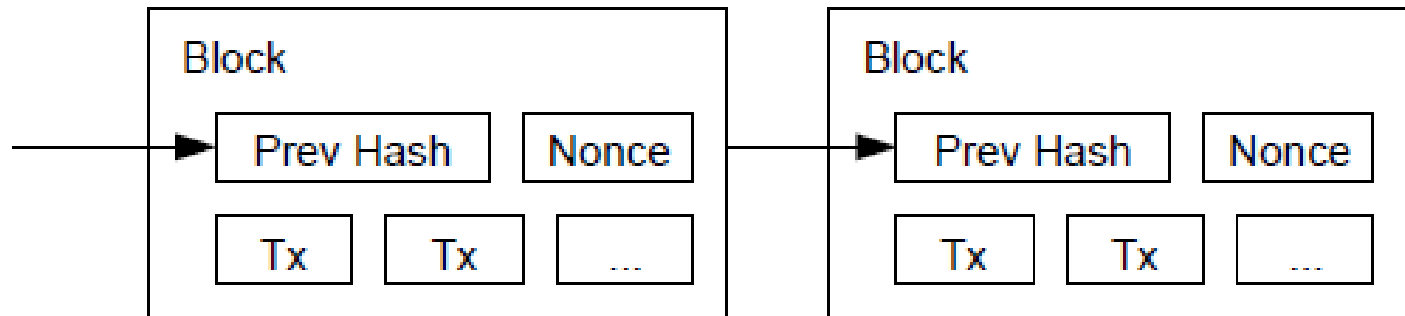
Timestamp Server

Al fine di evitare il double-spending, viene utilizzato un timestamp server. Tale server (distribuito - costituito dai nodi della rete) non fa altro che calcolare l'hash di un blocco di transazioni (soddisfando la proof-of-work). Le transazioni presenti in quel blocco vengono quindi pubblicamente accettate e non sarà più possibile per i precedenti possessori spendere i bitcoin contenuti in esse.



Proof-of-work (POW)

Si tratta di un'operazione computazionalmente complessa, ma di semplice verifica (data una soluzione), che permette di difendere il sistema dal double-spending. Nel sistema Bitcoin la POW consiste nel calcolare un nonce che aggiunto al blocco di transazioni dia come risultato del calcolo dell'hash un valore con un certo numero di zeri all'inizio



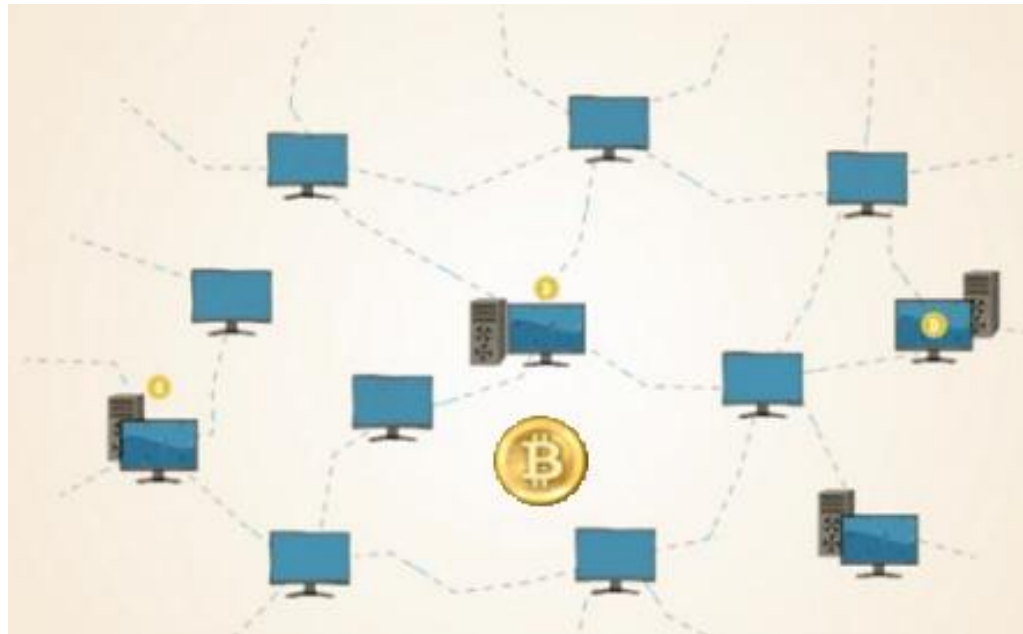
$\text{Hash}(\text{Block}) = 00\dots0XXXXXXXXXXXXXXXXXX$

Richiesti dalla POW

Bitcoin Network

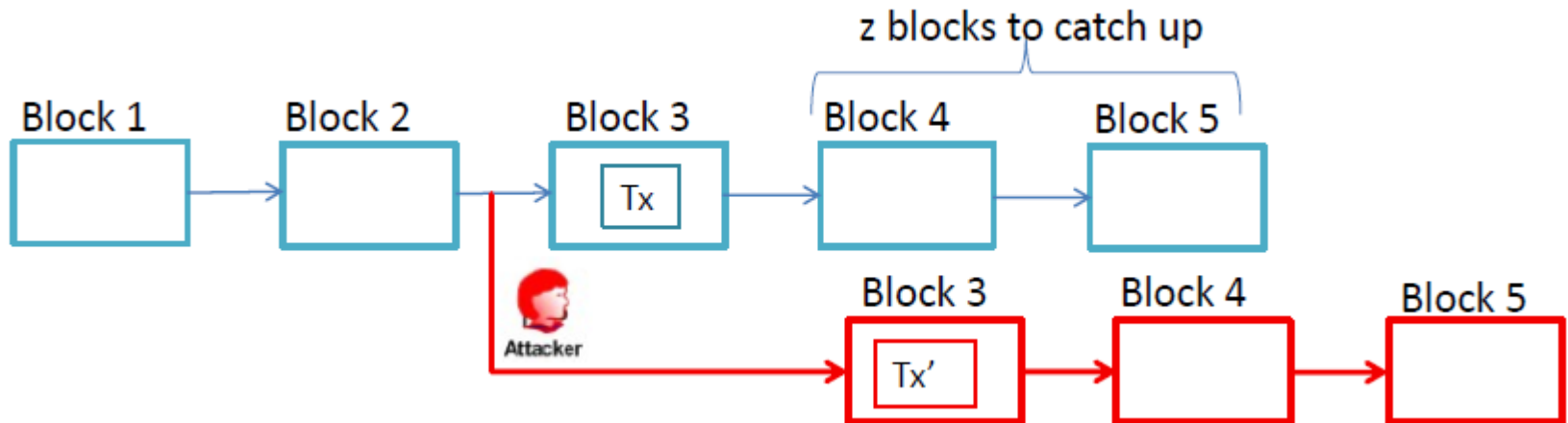
La rete Bitcoin funziona secondo i seguenti passi:

1. Le nuove transazioni vengono annunciate a tutti i nodi
2. Ogni nodo colleziona le transazioni all'interno di un blocco
3. Ogni nodo cerca di trovare la soluzione alla POW per il proprio blocco
4. Quando un nodo trova la soluzione, la invia in broadcast insieme al blocco a tutti i nodi
5. I nodi, dopo aver verificato la correttezza della soluzione alla POW, accettano come valido il blocco solo se tutte le transazioni in esso sono valide (non utilizzano bitcoin già spesi)
6. I nodi esprimono l'accettazione del blocco iniziando a lavorare alla ricerca della soluzione per la POW utilizzando l'hash del blocco come input.



Double-Spending

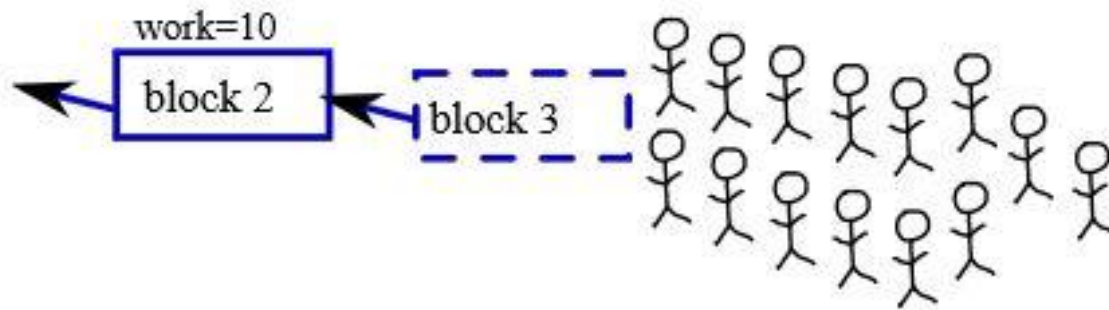
Un attaccante non può creare nuovi bitcoin o rubare monete che non siano mai appartenute a lui. L'unica che può fare è cercare di modificare le transazioni eseguite da lui stesso.



Al fine di portare a termine tale attacco, l'attaccante dovrà non solo modificare il blocco contenente la transazione in questione, ma anche ricalcolare la proof-of-work per tutti i blocchi successivi.

Chain split 1/8

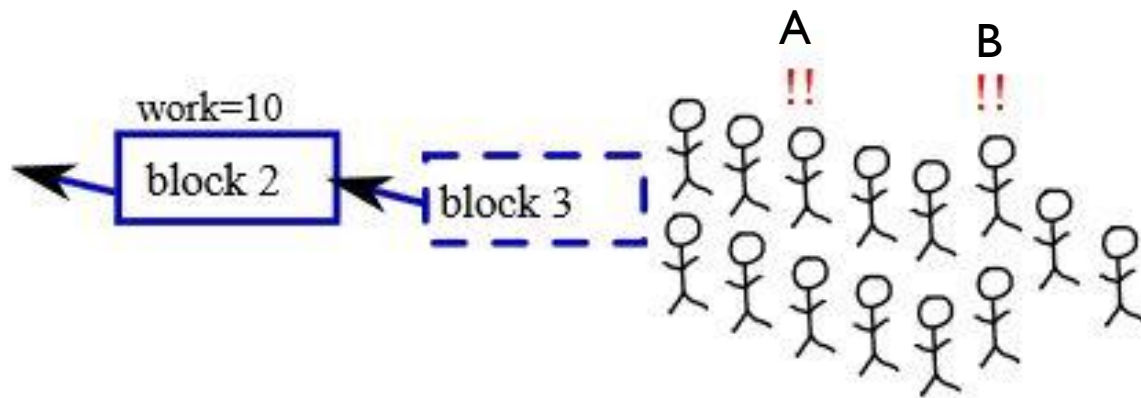
Un numero di nodi miners lavorano sulla convalida del blocco 3 (POW + controllo transazioni)



Chain split 2/8

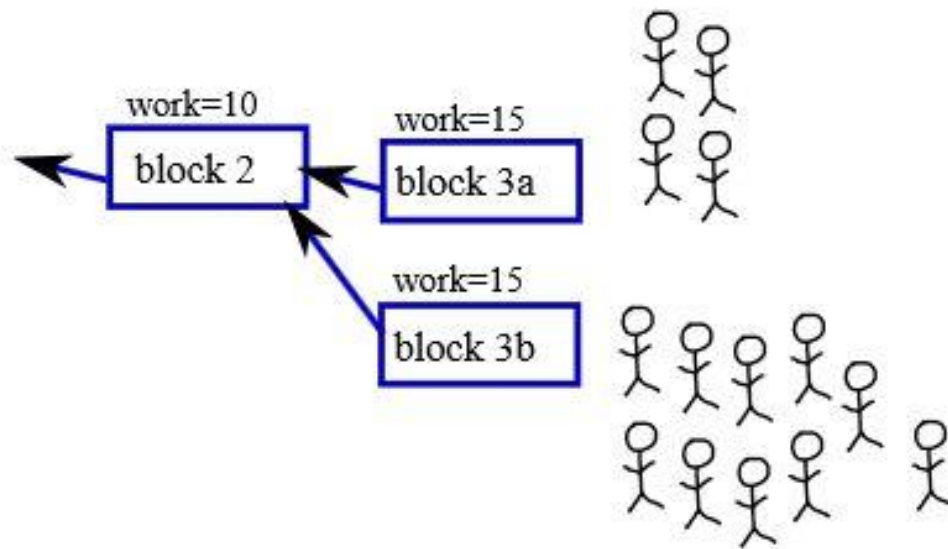
Problema -----> due nodi possono reclamare simultaneamente la convalida di un blocco!!!!

I nodi A e B reclamano la convalida simultanea del blocco 3

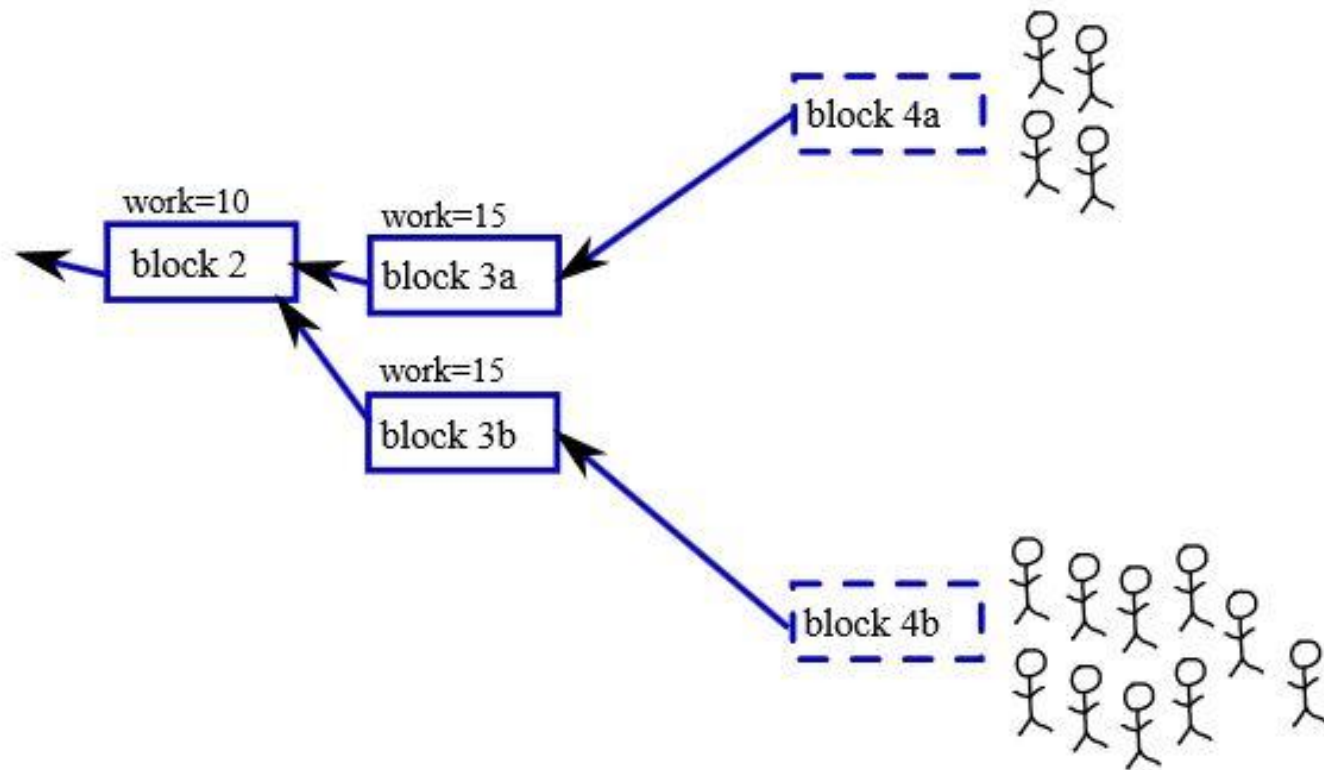


Chain split 3/8

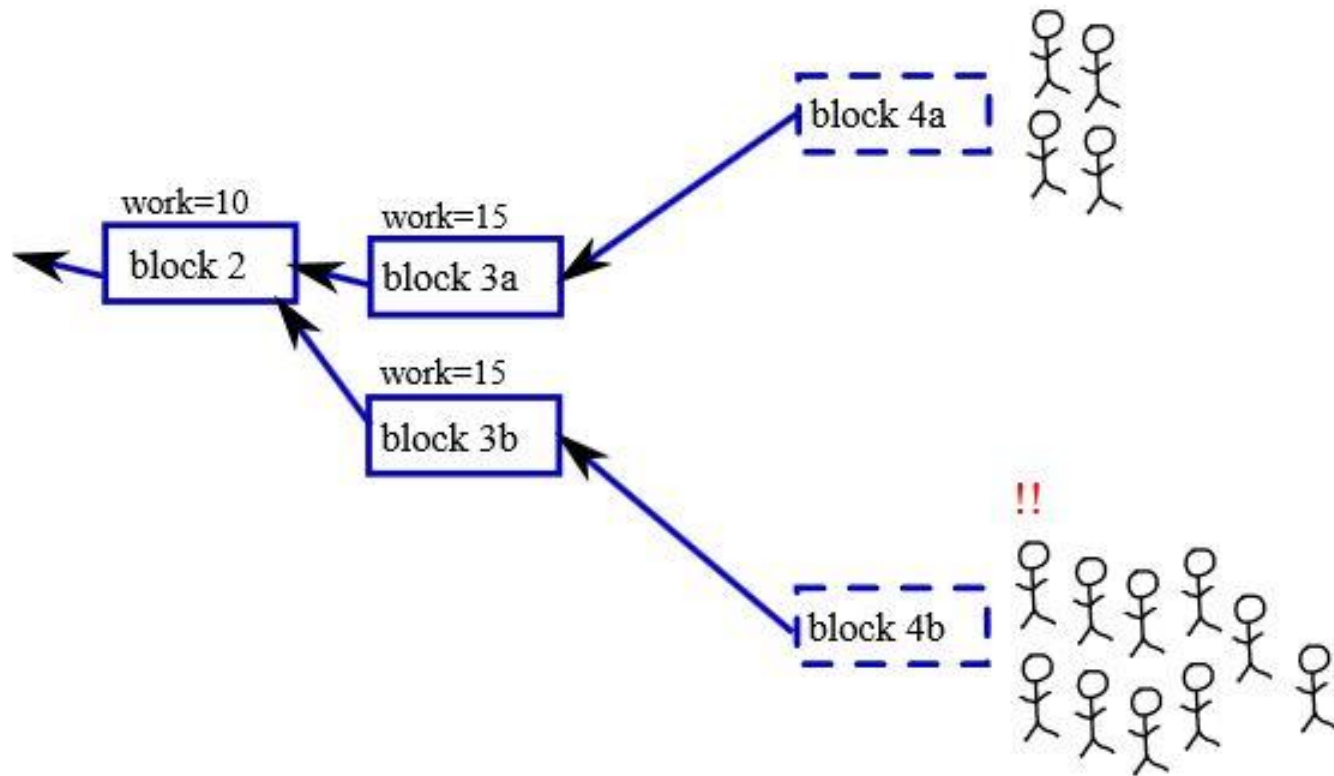
Alcuni riceveranno prima il blocco 3-a altri il 3-b ---> CHAIN SPLIT!



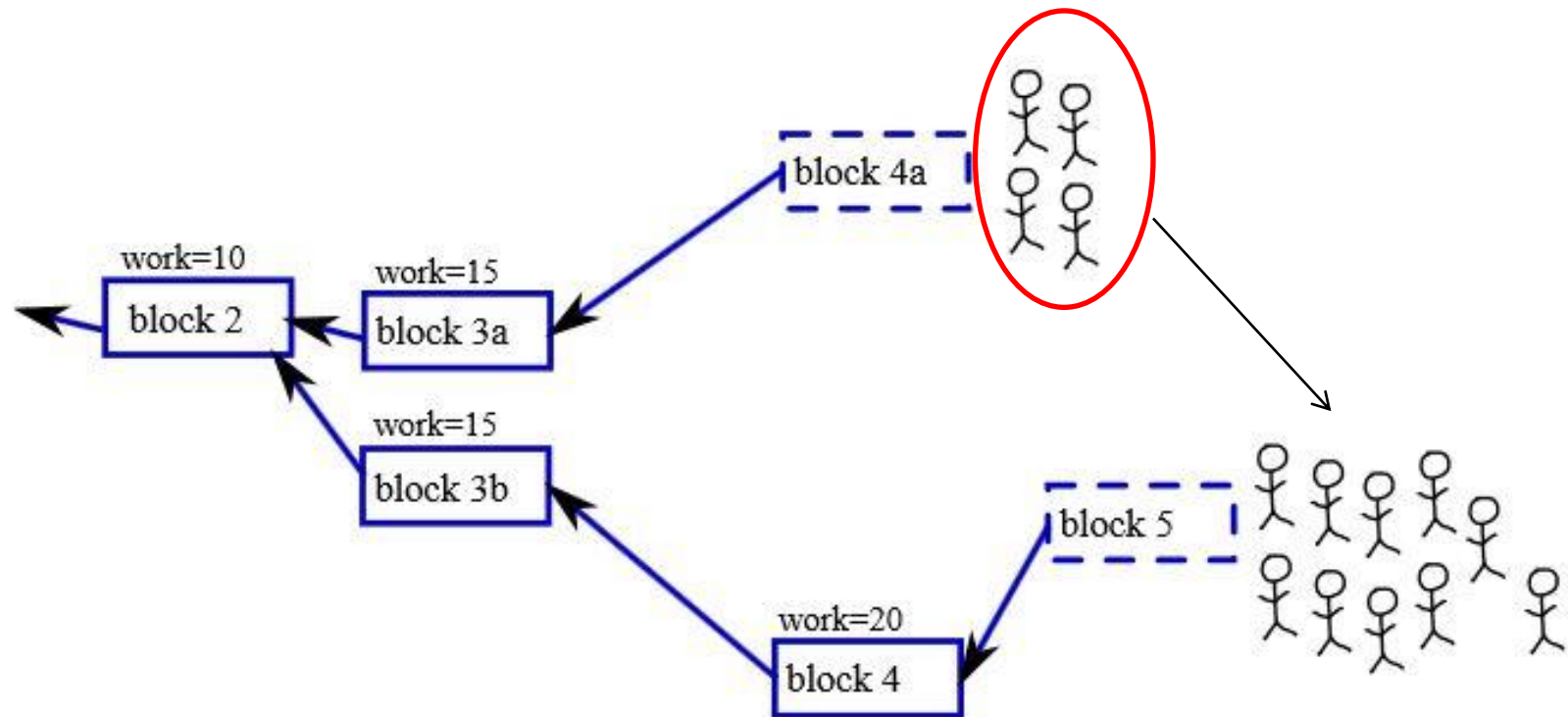
Chain split 4/8



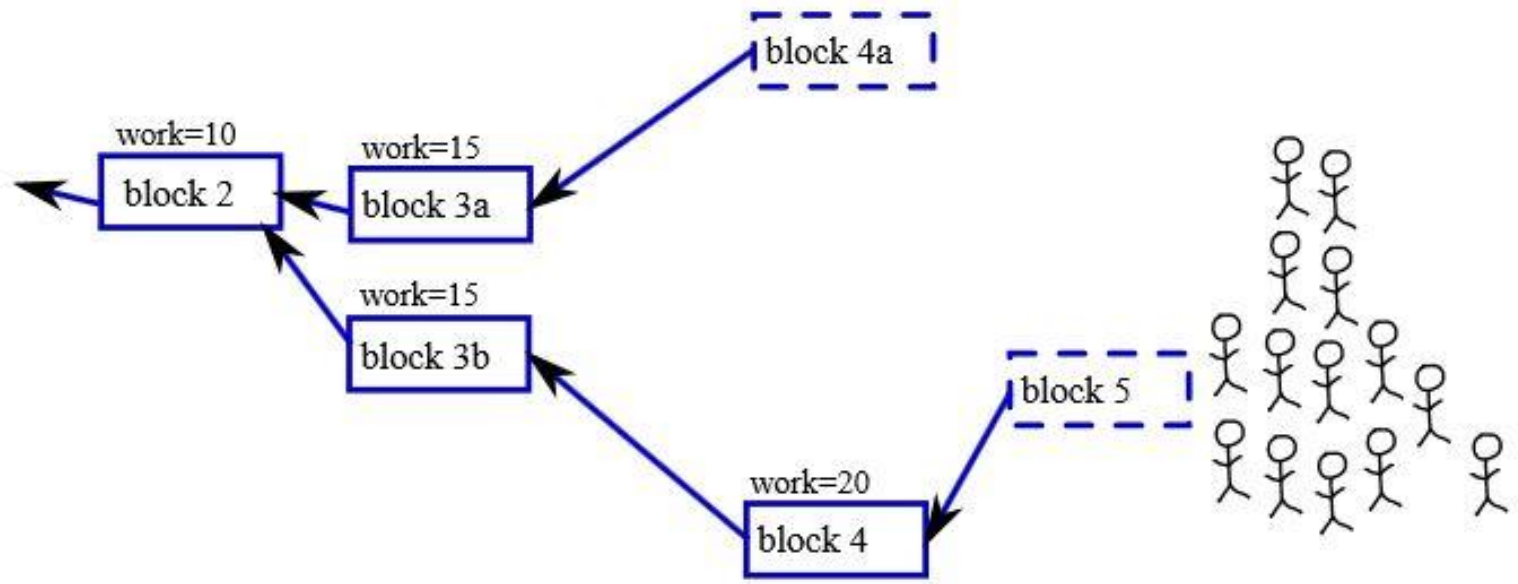
Chain split 5/8



Chain split 6/8

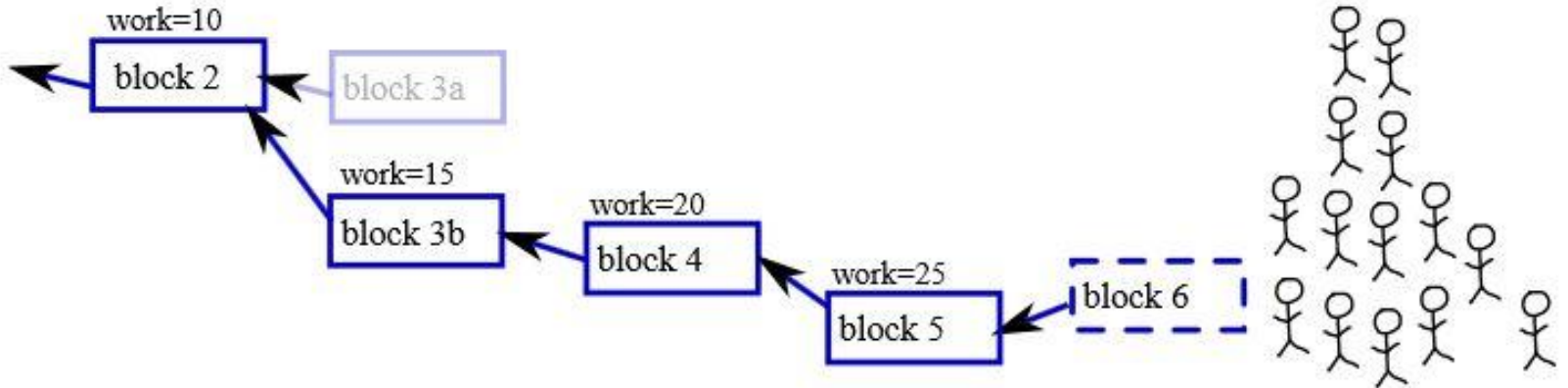


Chain split 7/8



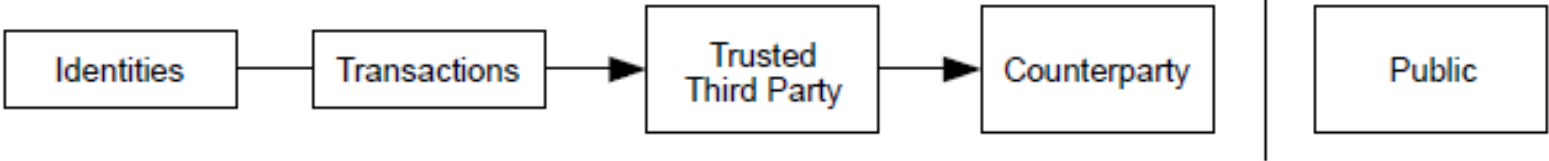
Chain split 8/8

Viene cancellata la catena generata a partire dal blocco 3 A

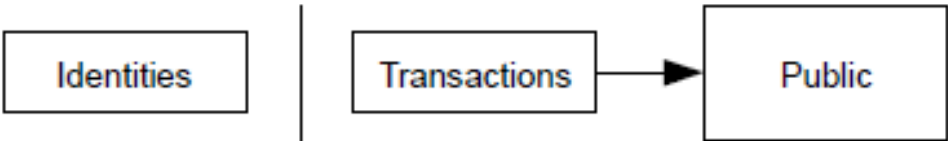


Privacy

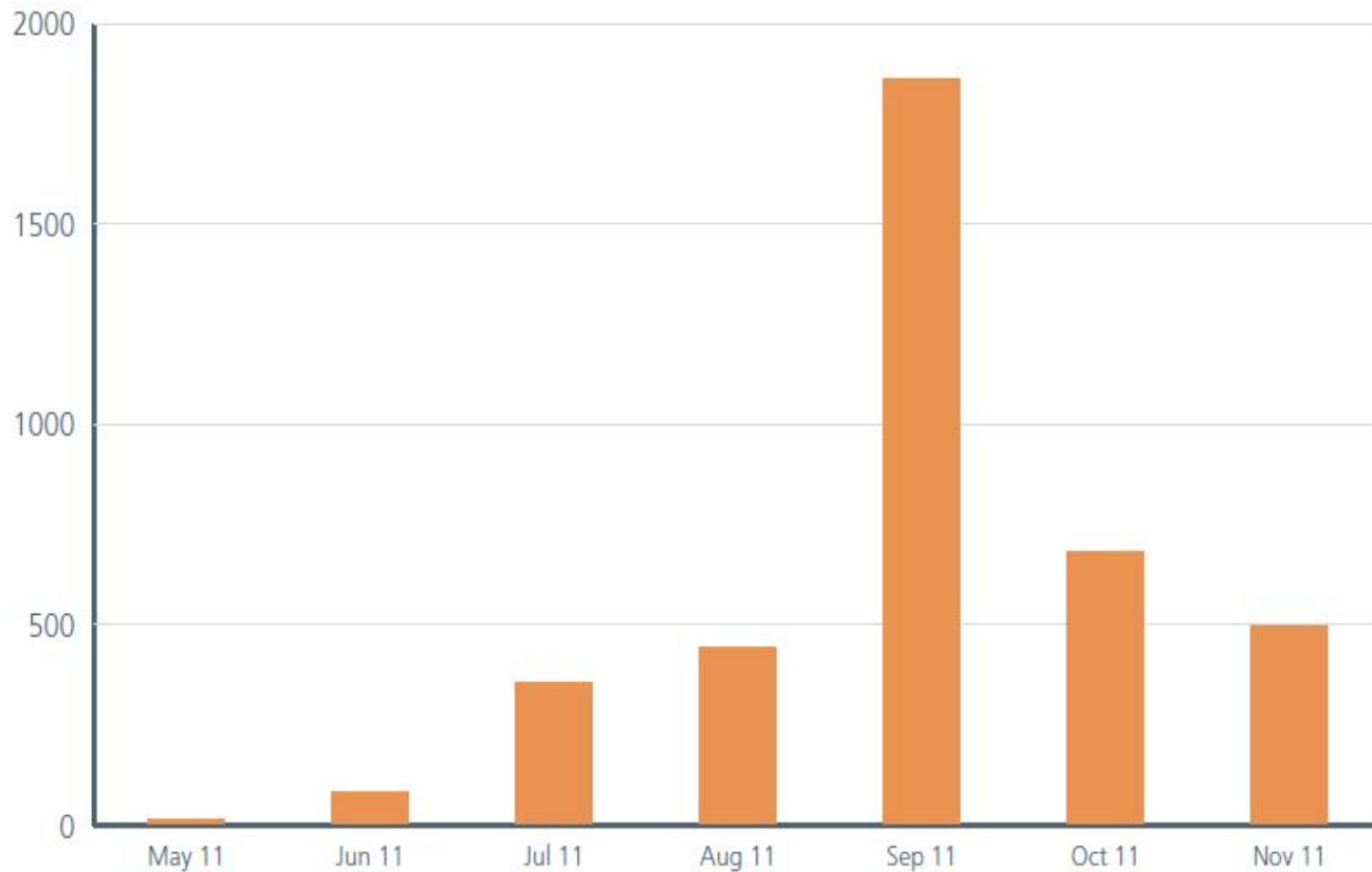
Traditional Privacy Model



New Privacy Model



Numero furti BTC



Furto del Portamonete

- Non tutti gli user sono informatici;
- Wallet.dat non è criptato di default;
- Codice maligno disegnato per “rubare” i portamonete;
- Non mettere tutti i tuoi soldi nello stesso portamonete: domandare a “Allinvain” che ha perso 50.000 BTC da un singolo wallet.dat file!
- en.bitcoin.it/wiki/Securing_your_wallet

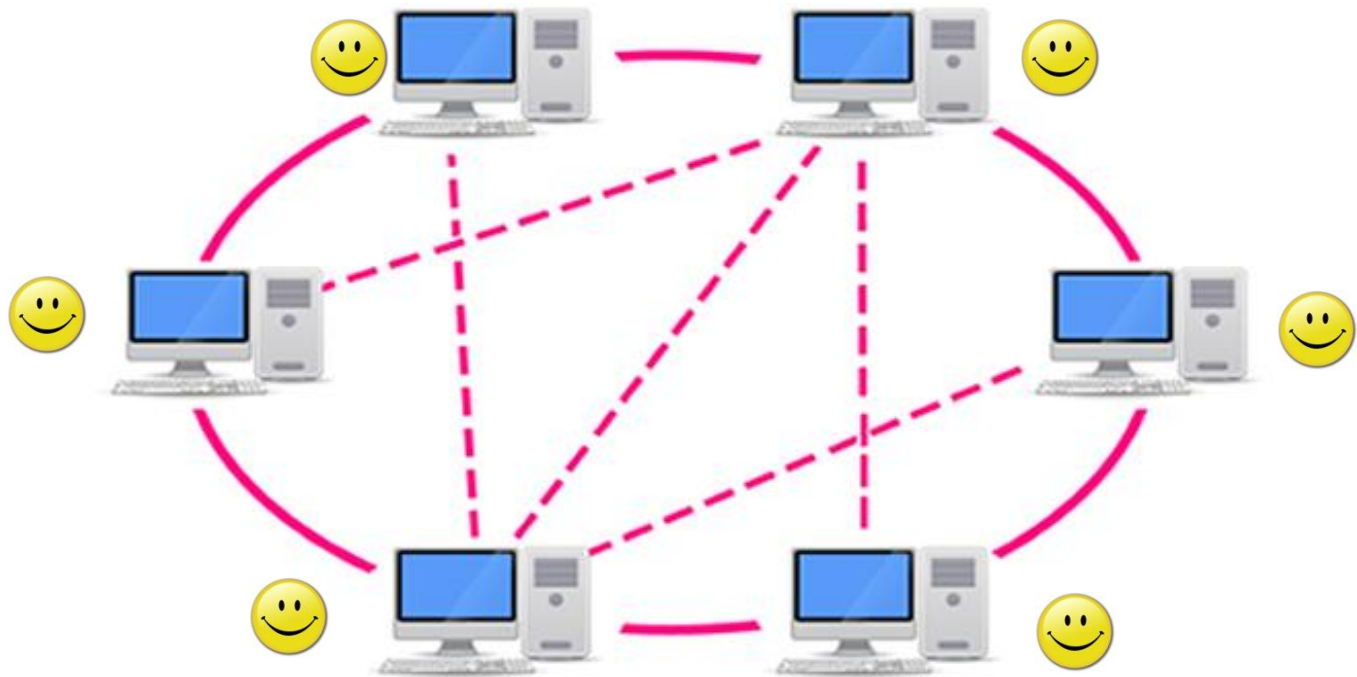
DOS Attack

- impedire il funzionamento dei servizi di rete proposti;
- Es. sovraccarico della rete bitcoin con l'invio di milioni di piccole transazioni tra alcuni dei miei accounts:

A ---> B ---> C ---> A ---> B ---> C ...

- DOS più elaborati sono in grado di causare il blocco della rete?!
- DDOS (denial of service distribuito).

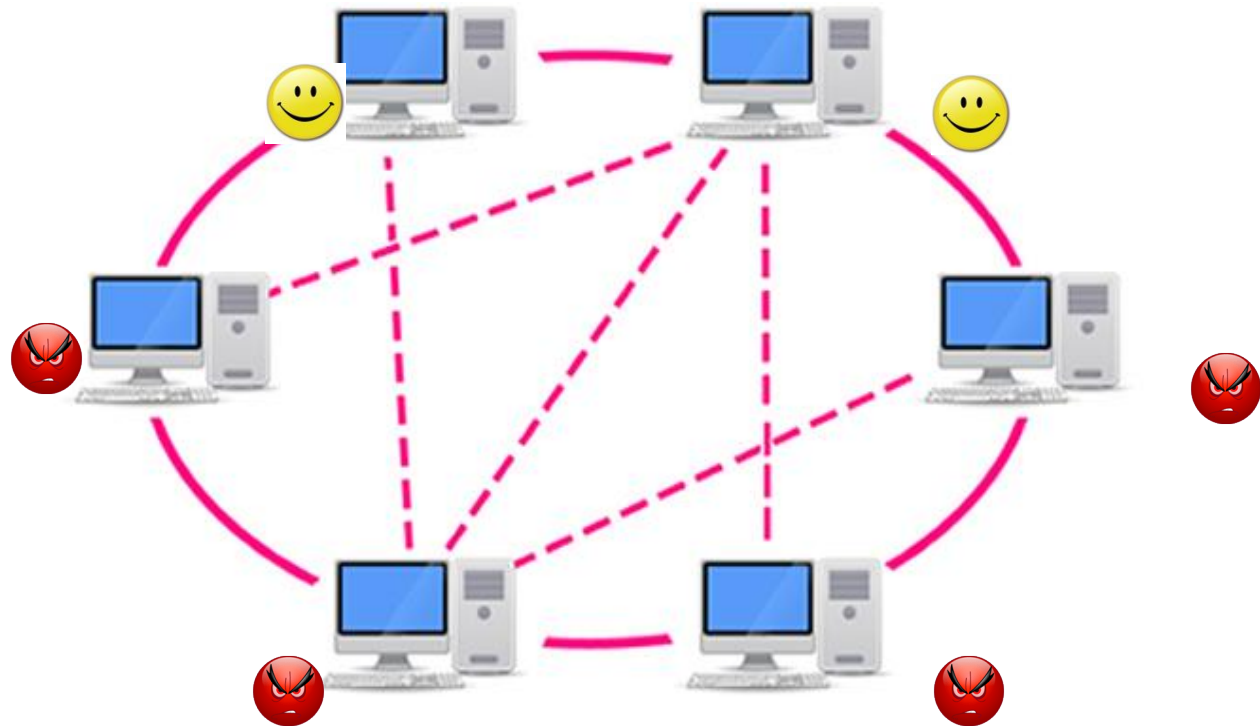
Cancer Nodes



Bitcoin p2p network formata da soli 6 nodi.

Obiettivo attacco ---> Ottenere il controllo della rete!

Cancer Nodes



Numero alto di nodi “corrotti” --->

L'attaccante può influenzare il comportamento della rete!

Es. Negazione transazioni, controllo dei blocchi, double-spending...

Questo tipo di attacco richiede disponibilità di risorse elevatissime!

Violazione degli algoritmi crittografici

- ECDSA (Elliptic Curve Digital Signature Algorithm) per la firma digitale e SHA-256 per il calcolo dell'hash attualmente ci garantiscono la sicurezza;
- Scenario futuro: aumento della potenza di calcolo (Es. Computer quantistici) ----> dovremo rivedere tutti gli algoritmi crittografici compresi quelli alla base della sicurezza di internet!

Conclusioni

- Centralizzazione vs Decentralizzazione;
- Robusto livello di sicurezza;
- Privacy garantita;
- Nessun intermediario, costi irrilevanti!
- Conferma transazioni non istantanea;
- Non viola nessun accordo governativo o finanziario;
- Il suo Futuro??? Dipenderà da quanti soggetti lo accetteranno in cambio di cose e servizi utili!

Fonti

- - Bitcoin: A Peer-to-Peer Electronic Cash System -
<http://bitcoin.org/bitcoin.pdf>
- Bitcoin wiki -
<https://en.bitcoin.it/wiki/Category:Technical>
- Wikipedia: Bitcoin -
<http://en.wikipedia.org/wiki/Bitcoin>
- Wikipedia: Electronic Money -
http://en.wikipedia.org/wiki/Electronic_money
- SURVEY OF ELECTRONIC PAYMENT METHODS AND SYSTEMS -
http://doc.utwente.nl/18925/1/survey_havinga.pdf