BLOCKCHAIN

È una tecnologia politica:

- DECENTRALIZZATA / DISINTERMEDIATA
- AUTONOMA
- TRASPARENTE
- RESPONSABILITÀ INDIVIDUALE
- SOVRANITÀ DELL'INDIVIDUO
- è un sistema distribuito
- che usa la crittografia
- per garantire consenso
- verso token
- con un valore economico o sociale

COMPONENTI DELLA BC

BLOCCHI:

Sono formati da:

- id
- timestamp
- insieme di dati

ogni blocco ha un hash che lo identifica e ne certifica l'info

FUNZIONE DI HASH:

dati di len arbitraria ⟶ stringa len fissa (digest)

Una funzione di hash deve essere:

- Deterministica
- Caotica
- Minimizzare le collisioni

CHAINS:

I blocchi sono concatenati cronologicamente e l'hash del

blocco i dipende da quello del blocco i-1

CONSENSO:

In un sistema distribuito alcuni nodi possono essere corrotti o malevoli

- POW: i miner lavorano per risolvere un problema difficile da risolvere ma facile da verificare, risolvibile solo con la forza bruta, in modo che la potenza computazionale conti
  Trovare il nonce, ovvero un numero che, aggiunto all' hash dell'intestazione corrente, dia un hash che inizia con n zeri (difficoltà)
  La difficoltà viene costantemente calibrata per garantire un blocco x 10 min
- POS: i validatori accumulano criptovaluta non spendibile
  Viene estratto casualmente un validatore con probabilità proporzionale allo stake.
  In caso di falsificazione lo stake viene trattenuto

TRANSAZIONI:

Interazioni tra due utenti sulla bc
Ogni blocco contiene un determinato numero di transazioni
Per eseguire una transazione bisogna pagare una fee che va al miner/validatore del blocco

FIRMA DIGITALE:

Certifica le transazioni con crittografia asimmetrica
- la transazione é certificata con una chiave privata
- la transazione puó essere verificata con una chiave pubblica

P2P NETWORK:

la bc é una rete p2p distribuita e decentralizzata
- ogni nuovo blocco é condiviso con tutti i nodi
- il blocco deve essere accettato da tutti i nodi, iniziando la creazione di un nuovo blocco

CRIPTOVALUTE

Valuta digitale garantita dalla crittografia

WALLET:

il w3 fa un trade-off tra trasparenza e privacy, il contenuto dei

wallet é pubblico

WALLET CRITTOGRAFICO: contiene le chiavi private per accedere agli asset e firmare le transazioni

Ogni wallet ha un address univoco derivato dalla public Key.

L'address può essere nominato con un servizio simile al DNS

Quando il wallet viene creato viene generata una seed phrase

TIPI DI WALLET:

- HOT (online):
  - web based
  - desktop
  - mobile
- COLD (offline):
  - hardware
  - paper
- CUSTODIAL: le chiave privata é in mano a terzi.
  User Friendly ma meno sicuro
- NON CUSTODIAL: la chiave privata é gestita dall'utente.
  Più responsabilità ma più sicuro
- SINGLE SIGNATURE: il wallet ha una sola chiave private
- MULTI SIGNATURE: il wallet ha più chiavi private. Servono tutte per firmare una transazione

TOKEN

Unità di valore quantificabile, memorizzata e scambiata sulla bc

- FUNGIBILI: criptovalute
  - Interscambiabili con token dello stesso tipo
  - Divisibili
  - Trasferibili
- NON FUNGIBILI:
  - Non interscambiabili
  - Non divisibili
  - Trasferibili

- SEMI-FUNGIBILI: token multi-standard. FT con una fornitura limitata
- SOULBOUND: token non trasferibili

APPLICAZIONI:

- FT:
  - DeFi
  - staking
  - stablecoins
  - exchange
- NFT:
  - Arte digitale
  - pfp
  - metaverso decentralizzato
- SBT:
  - credenziali personali

METODI DI VOTAZIONE

Funzione che mappa il credito di un individuo nel suo potere di voto

$$V = F(T)$$

- UNA PERSONA UN VOTO: $V = 1$
- UN TOKEN UN VOTO: $V = T$

Il primo è democratico, ma ignora le differenze tra gli individui

Il secondo è meritocratico, ma crea plutocrazia

Un compromesso è il voto quadratico: $V = \sqrt{T}$

dove n voti richiedono n^2 crediti. Inoltre: $\sum \sqrt{x_i} \geq \sqrt{\sum x_i}$

Il VQ è vulnerabile al sybil attack, attraverso il quale un utente malevolo può creare diverse identità false per incrementare il suo potere, e alle coalizioni pre-esistenti.

I metodi di votazione devono prevedere un metodo per verificare l'identità, in modo da impedire votazioni multiple e/o bottate

QUADRATIC FUNDING

Metodo ottimale per finanziare opere pubbliche in una comunità democratica

I beni pubblici sono caratterizzati da rivalità e escludibilità

	ESCLUDIBILE	NON ESCLUDIBILE
RIVALITÀ	BENI PRIVATI soldi, macchine, vestiti...	BENI COMUNI risorse naturali...
NON RIVALITÀ	BENI "CLUB" cinema, spotify...	BENI PUBBLICI infrastrutture, aria...

Tre attori

- Beneficiario: chi propone il progetto e cerca fondi per finanziarlo
- Piccoli donatori: persone comuni che scelgono a quale progetto contribuire con piccole donazioni individuali
- Grandi donatori: contribuiscono ad una matching pool che va ad integrare i fondi dei piccoli donatori

Il QF tiene conto sia del contributo individuale che del numero di donatori

Fondo per il proj p: $Q(p) = \left(\sum \sqrt{c_i(p)}\right)^2$ $F(p) = MP \cdot \frac{Q(p)}{Q}$

DAO

- Decentralizzata: le decisioni sono prese dalla collettività
- Governance: il potere di voto è proporzionato ai token posseduti
- Tesoreria: pool di token gestita collettivamente
- Autonoma: le regole sono scritte in uno smart contract sulla bc

Limitazioni:

- Attacchi: le proprietà (decentraliz., consenso..) delle DAO comportano dei rischi
- Efficienza: in alcuni casi, completa decentraliz. e autonomia sono impossibili. La centraliz. permette efficienza ma non libera partecipazione
- Educazione: le DAO devono educare di più gli utenti rispetto ad un sistema

centraliz. I possessori di token possono avere background differenti
- Astensione: non tutti gli utenti sono interessati a votare, attribuendo più potere a chi è più attivo

BTC HALVING

Satoshi Nakamoto decise che dovranno esistere al massimo 21M BTC
Inizialmente il reward per ogni blocco minato era 50 BTC
I reward rimangono invariati per 210k blocchi (~4 anni) dopodiché vengono dimezzati
L'unità minima di BTC è 10^{-8} BTC (1 satoshi), per 32 halving
L'halving aumenta la competizione tra i miner, eliminando i meno produttivi.
Diminuisce la disponibilità, aumentandone il valore

GAS E FEES

La bc di ETH può essere vista come una macchina virtuale (EVM) che esegue le funzioni dello smart contract in cambio di fees che vanno a pagare i validatori
Le fees dipendono da:
- complessità dell'operazione
- priorità dell'operazione
- congestione del sistema

L'unità di misura del costo delle operazioni è il gas, espresso in gwei (10^9 wei). 10^9 gwei fanno 1 ETH
La base fee è impostata dal protocollo e viene pagata per ogni unità di gas. La base fee viene bruciata, creando un meccanismo deflazionistico (solo se il block reward < burned fee)
La priority fee, pagata sempre per ogni unità di gas, va al validatore

SMART CONTRACTS

È uno script che:
- viene eseguito sulla bc
- una volta fatto il deploy sulla bc, non può essere modificato
- fa esattamente ciò che gli viene detto

PRO
- decentralizzato: ogni blocco detiene la stessa copia dello sc, nella

stesso stato

- automatizzato: viene eseguito automaticamente quando si verificano determinate condizioni
- deterministico: lo stesso input avrá lo stesso outcome
- immutabile
- trasparente: ogni utente puó visualizzarlo prima di accettarlo

CONS

- bugs: la trasparenza permette ai malintenzionati di trovare bug
- compatibilitá: un cambio della piattaforma puó causare contrasti tra sc
- irl: come fa a sapere lo sc degli eventi irl?

STABLECOINS

crypto che sono "pegged" ad un asset esterno

Fiat-collateralized: sono sostenute da una valuta Fiat (USDT, USDC)

Crypto-collateralized: sono sostenute da un'altra criptovaluta. Data l'alta volatilitá viene fatta un over-collateralization in modo da coprire perdite (DAI)

Algoritmiche: non hanno una valuta collaterale. Un algoritmo funziona come una banca centrale, mintando coins quando é sopra il valore di peg e bruciandole quando é sotto

CENTRAL BANK DIGITAL CURRENCY

Sono valute digitali rilasciate da una banca centrale e solitamente sono la versione digitale di una fiat giá esistente

I trasferimenti sono istantanei e a basso costo.

A differenza delle crypto, sono tracciabili, centralizzate e valide solamente sotto determinate giurisdizioni

ZERO KNOWLEDGE PROOFS

Provare che un'affermazione é vera senza rivelare il perché

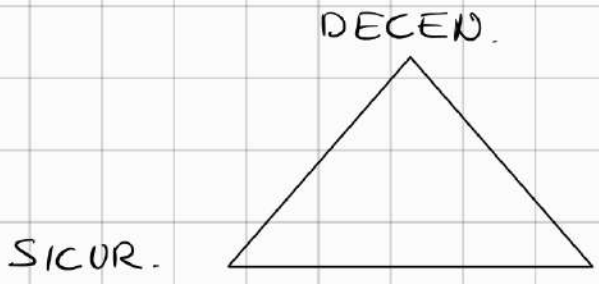
La prova di un teorema contiene piú info del fatto che sia solo vero

INTERATTIVA: richiede l'interazione tra il prover e il verifier, di conseguenza non é verificabile indipendentemente

NON INTERATTIVA: il prover e il verifier scambiano una chiave segreta condivisa generata casualmente per generare e verificare le prove

Richiede solo un giro di comunicazione interattiva

SCALING A BLOCKCHAIN



BC TRILEMMA: solo 2/3

BTC e ETH sono decen. e sicure ma non scalabili

SCALABILITÀ: aumentare velocità e intensità delle transazioni

SCALING ON-CHAIN: richiedono la modifica del protocollo (layer 1)

- sharding: Un sottoinsieme di validatori è responsabile di uno o più shard. Non è mai stato implementato

SCALING OFF-CHAIN: implementati separatamente dal layer 1

ROLLUP: delegare la computazione al layer 2

le transazioni vengono eseguite su una chain parallela che comprime i dati di output e fa un rollup sulla bc principale

Come avviene la verifica? Dipende dall'implementazione dello sc

- ROLLUP OTTIMISTICI: i rollup vengono assunti corretti. Se il rollup è incorretto il sistema deve riconoscerlo, recuperare lo stato e penalizzare il validatore, implementando un risolutore delle controversie in grado di verificare le prove di frode mandate dagli utenti

  Se il sistema entra in dispute resolution mode, la transazione viene rieseguita sul layer 1
- ZK ROLLUP: ogni batch sul layer 1 contiene una prova di validità che permette di verificare la correttezza di uno statement senza rivelarlo

Quello ottimistico introduce ritardi, quello ZK è più complesso

METODO DI ELO

s_{ij} è il punteggio nella partita di i contro j, $s_{ij} \in \{1, 0.5, 0\}$

μ_{ij} è il punteggio atteso nella partita di i contro j, $\mu_{ij} = \frac{1}{1+10^{-(r_i - r_j)/c}}$

Dopo la partita $r_i = r_i + K(s_{ij} - \mu_{ij})$

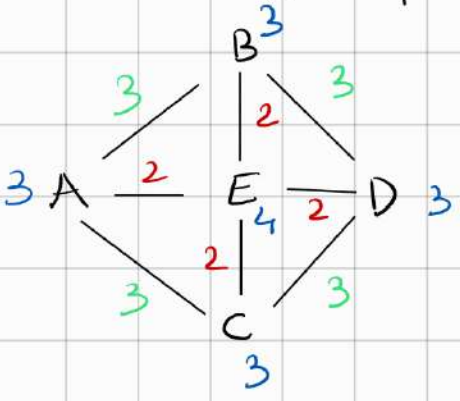
GRAFI REGOLARI E REGOLARIZZABILI

Un grafo è regolare:

- non diretto non pesato, se $\exists$ un $r > 0$ t.c. ogni nodo ha grado r
- diretto non pesato, se $\exists$ un $r > 0$ t.c. ogni nodo ha grado in/out r

Un grafo è regolarizzabile:

- non diretto non pesato, se ogni arco può essere pesato con interi positivi in modo che ogni nodo abbia grado pesato pari a $r > 0$
- diretto non pesato, se ogni arco può essere pesato con interi positivi in modo che ogni nodo abbia grado pesato in/out pari a $r > 0$



- non è regolare
- è regolarizzabile

MISURE DI CENTRALITÁ

GRADO:

$$x = eA \quad x_i = \sum a_{ki} \qquad x = eA^T \quad x_i = \sum a_{ik}$$

CLOSENESS: misura quanto un nodo è vicino agli altri

$$c_i = \left(\frac{1}{n-1}\sum_{i \neq j} d_{ij}\right)^{-1} = \frac{n-1}{\sum_{i \neq j} d_{ij}}$$

BETWENNESS: misura quanto un vertice si trova nei cammini tra le altre coppie di vertici

$$b_i = \sum_{\substack{s \neq t \\ s \neq i \\ t \neq i}} \frac{n'_{st}}{n_{st}}$$

n'_{st} è il numero di cammini minimi tra s e t che comprendono i

n_{st} è il numero di cammini geodesici tra s e t

AUTOVETTORE: un nodo è importante se è collegato a nodi importanti

$$x_i = \frac{1}{\lambda}\sum a_{ki} x_k, \quad \lambda \neq 0 \qquad \lambda x = xA$$

λ

il vettore delle centralità è l'autovettore destro di A e λ è l'autovalore massimo associato

Se A è irriducibile (fortemente connesso) x è unico e positivo

METODO DELLE POTENZE:

$\forall K \geq 1$

calcola: $x^K = x^{(K-1)} A$

normalizza: $x^K = x^K / m(x^K)$

- x^K converge all'autovettore dominante di A
- $m(x^K)$ converge all'autovalore dominante di A

Se $|\lambda_1| > |\lambda_2|$, il rateo di convergenza è $(\lambda_1/\lambda_2)^K \to 0$

KATZ: l'autovettore funziona solo se il grafo è connesso nei DAG è nulla per ogni nodo. Viene data della centralità

$x_i = \alpha \sum a_{ki} x_k + \beta$, $x_i = \alpha x A + \beta$

PAGERANK: un nodo con alta centralità dà alta centralità anche alle sue connessioni

1) link ricevuti
2) centralità dei linkers
3) propensione al link dei linkers

$$x_i = \alpha \sum \frac{a_{ki}}{d_k} x_k + \beta \qquad x = \alpha x D^{-1} A + \beta$$

HITS: divide i nodi in hub (collegamenti a autorità) e autorità (contengono le info utili)

$$x_i = \alpha \sum a_{ki} y_k \qquad y_i = \beta \sum a_{ik} x_k$$

$$x = \alpha A y \qquad y = \beta A^T x$$

$$\lambda x = x A^T A \qquad \lambda y = y A A^T$$

MISURE DI POTERE

A volte essere centrali non ha molta utilità.

Un nodo è potente se è collegato a nodi meno potenti

$$X_i = \sum \frac{a_{ki}}{x_k}$$

- più alto il grado, maggiore il potere
- minore il potere dei vicini, maggiore il potere

PERTURBAZIONE

Se A non è regolarizzabile si può perturbare completamente o diagonalmente

$$A_\varepsilon^F = A + \varepsilon \bar{E} \qquad A_\varepsilon^D = A + \varepsilon \bar{I}$$

RETI SEGNATE

BILANCIAMENTO STRUTTURALE:

- l'amico del mio amico é mio amico
- l'amico del mio nemico é mio nemico
- il nemico del mio amico é mio nemico
- il nemico del mio nemico é mio amico

TRIANGOLI:

- BILANCIATO: se contiene un numero pari di segni negativi
- SBILANCIATO: se contiene un numero dispari di segni negativi

Un grafo é bilanciato se tutti i suoi triangoli sono bilanciati e gode della proprietá di mutuo antagonismo, ovvero che é possibile dividere i nodi in due fazioni contrapposte.

CAMMINI:

- un cammino é positivo se ha un numero pari di segni meno
- un cammino é negativo se ha un numero dispari di segni meno

Un grafo é bilanciato se tutti i suoi cicli sono positivi

WALK INDEX: misura il numero di cicli positivi penalizzando i piú lunghi

$$W = \sum \frac{A^S}{S!}$$

SIMILARITÁ

Due nodi sono simili se condividono molti vicini

Associare ogni nodo i alla riga i di A (un vettore di lunghezza n), la similarità tra i e j é una funzione che calcola la distanza tra i vettori

SIMILARITÁ DEL COSENO: coseno dell'angolo tra due vettori

$$\sigma_{ij} = \cos(A_i, A_j) = \frac{A_i \cdot A_j}{\|A_i\| \cdot \|A_j\|}$$

0 vettori ortogonali, 1 vettori paralleli

COEFFICIENTE DI CORRELAZIONE DI PEARSON:

$$\sigma_{ij} = \frac{\text{cov}(A_i, A_j)}{} \in [-1, 1]$$

$sd(A_i)$ $sd(A_j)$

NETWORK MODELS

Metodo per generare reti artificialmente

RANDOM MODEL (Erdös-Rényi):

1) vengono posizionati n nodi
2) per ogni coppia di nodi viene aggiunto un'arco con probabilità p

PREFERENTIAL ATTACHMENT (Barabasi-Albert):

1) gli n nodi vengono posizionati uno alla volta
2) ogni nodo viene connesso a quelli esistenti con m archi. La probabilità di connessione è proporzionata al grado del nodo scelto

CONNETTIVITÁ E RESILIENZA

COMPONENTE CONNESSA: insieme massimo di nodi nel quale ogni coppia è connessa da un cammino

COMPONENTE GIGANTE: è tipicamente presente nelle reti reali e copre la maggior parte del grafo. Sia il random che pa model ne generano una

K-COMPONENTE: insieme massimo di vertici dove ogni nodo è raggiungibile da almeno K cammini nodo-indipendenti

CONNETTIVITÁ: numero di cammini nodo-indipendenti che collegano due nodi. Può essere usato per misurare la forza di connessione tra due nodi

ROBUSTEZZA: l'insieme minimo di nodi da rimuovere per disconnettere due vertici è chiamato minimum cut set e la sua dimensione coincide con la loro connettività.
Una K-componente rimane connessa fino alla rimozione di K-1 nodi
Più alto è K, maggiore è la robustezza della rete

COMPONENTE FORTEMENTE CONNESSA: insieme di nodi dove ogni coppia è connessa da un cammino diretto.
Definisce una out-component e una in-component

PERCOLAZIONE: rimuovere nodi dalla rete seguendo una determinata strategia per testarne la robustezza

PICCOLO MONDO

EFFETTO DEL PICCOLO MONDO: proprietà globale, nella maggior parte delle

reti la distanza geodesica media è bassa, comparata al numero di nodi

La lunghezza dei cammini scala con il $\log n$. Facendo una visita in ampiezza il numero di nodi incontrati aumenta esponenzialmente con la distanza dalla sorgente

Inoltre le distanze sono distribuite normalmente, quindi la distanza media stima la distanza tipica della rete

SCALE-FREE NETWORKS

In molte reti reali la distribuzione dei gradi è asimmetrica

POWER LAWS: tipo di distribuzione a coda lunga

$p_k = Ck^{-\alpha}$, $2 \leq \alpha \leq 3$ è tipico per le reti

RETI SCALE-FREE: reti che seguono una distribuzione power law, non hanno una scala caratteristica dei gradi, ovvero che la distribuzione dei gradi non ha un valore medio attorno al quale la maggior parte dei nodi si concentra, a differenza delle reti random, dove tutti i nodi hanno ~grado uguale

- HUB: nodi altamente connessi che mantengono la connettività della rete
- ROBUSTEZZA: la rete è robusta alla rimozione casuale e vulnerabile sugli hub

ASSORTATIVITÁ

OMOFILIA: tendenza ad associarsi con chi condivide caratteristiche simili

- CARATTERISTICHE ENUMERATIVE: finite e non ordinate (sesso, nazionalità...)

  Viene assegnata ai nodi in base alle loro caratteristiche

  Una rete è assortativa se gli archi collegano principalmente nodi con le stesse caratteristiche

  Si usa la modularità

- CARATTERISTICHE SCALARI: continue e ordinabili: (età, altezza ...)

  La rete è assortativa se nodi con valori simili hanno più collegamenti

  Si usa la covarianza $cov(X,Y) = E[(X - E[X])(Y - E[Y])]$

- GRADO: è una caratteristica scalare

MOTIFS

Sono pattern strutturali delle reti che possono fornire informazioni

TRANSITIVITÁ: implica che se x è collegato a y e y a z, allora x è

collegato a z

TRANS. PARZIALE: se x è collegato a Y e Y a Z, non è garantito che ci sia il collegamento tra x e Z, ma è molto probabile

COEFFICIENTE DI TRANSITIVITÁ: misura il rateo di triadi chiuse

RECIPROCITÁ: frequenza dei loop di lunghezza due nei grafi diretti

$$R = \frac{1}{m} \sum_{ij} A_{ij} A_{ji}$$

EPIDEMIE

La diffusione dipende da:

- tipo di patogeno
- struttura della rete
- rete dei contatti

Il processo di trasmissione da nodo a nodo è sufficientemente complesso da poter essere modellato come casuale

PROCESSO DI BRANCHING

1ª ONDATA) un soggetto contagia i suoi K incontri in modo indipendente con probabilità p

2ª ONDATA) i nuovi K infetti incontreranno altri K soggetti portando a K^2 i nuovi possibili contagi

nª ONDATA) si continua così, portando a K^n possibili contagi

NUMERO RIPRODUTTIVO BASE: numero atteso di nuovi casi per individuo

$$R_0 = p \cdot K$$

- Se $R_0 < 1$, il contagio termina dopo un numero finito di ondate
- Se $R_0 > 1$, il contagio persiste con probabilità maggiore di 0

MODELLO SIR: un individuo passa attraverso tre stati:

- SUSCETTIBILE
- INFETTO
- RIMOSSO

Il contatto è rappresentato con un grafo diretto. Viene introdotta la variabile tempo. Inizialmente, alcuni nodi sono nello stato I, gli altri nello stato S. Ogni nodo $\in$ I ha probabilità p di infettare i suoi

vicini $\in S$. Dopo un certo tempo il nodo $\in I$ non è più infetto e quindi passa allo stato R

$\beta_T = \ln \frac{\langle K^2 \rangle - \langle K \rangle}{\langle K^2 \rangle - 2\langle K \rangle} > 0$ le reti scale-free hanno $\langle K^2 \rangle$ alto quindi sono più vulnerabili alle epidemie

MODELLO SIS: non c'è rimozione, passata l'infezione si è di nuovo suscettibili

Inizialmente alcuni nodi sono nello stato I, tutti gli altri in S.
Ogni nodo $\in I$ ha una probabilità p di infettare i suoi vicini $\in S$.
Dopo un certo tempo i nodi $\in I$ passano allo stato S.
L'epidemie SIS possono durare per molto tempo. Su grafo finito, un fallimento del contagio per un certo numero di passi può portare al termine dell'epidemia

EPIDEMIE SIRS: quando l'infezione passa il nodo è rimosso per un certo tempo, per poi tornare suscettibile

Dal punto di viste della scienza delle reti è meglio vaccinare gli hub (super spredders) anziché i vulnerabili. Non conoscendo completamente la rete dei contatti (caratteristiche globali) non è possibile identificare gli hubs, ma solo stimarli attraverso caratteristiche locali (vicini, grado ...)

VACCINAZIONE PER CONOSCENZA: si sceglie un campione delle popolazione e gli si fa scegliere un conoscente e lo si vaccina. Secondo il paradosso degli amici, si ha molta più probabilità di immunizzare un hub

DIMOSTRAZIONE PARADOSSO DEGLI AMICI

Numero medio di amici: $\mu_1 = \frac{1}{n}\sum K_i = \langle K \rangle$

Numero medio di amici di amici: $\mu_2 = \frac{1}{\sum K_i}\sum a_{ij} K_j = \frac{1}{\sum K_i}\sum K_j \sum a_{ij}$

$= \frac{1}{\sum K_i}\sum K_j^2 = \langle K^2 \rangle$

$\sigma^2 = E((x - E(x))^2) = E(x^2 - 2xE(x) + E(x)^2)$

$= E(x^2) - 2E(x)E(x) + E(x)^2$

$\sigma^2 = E(x^2) - E(x)^2$

Usando la formula della varianza:

$\mu_2 - \mu_1 = \frac{\langle K^2 \rangle}{\langle K \rangle} - \langle K \rangle = \frac{\langle K^2 \rangle - \langle K \rangle^2}{\langle K \rangle} = \frac{\sigma^2}{\langle K \rangle}$

I nodi con più connessioni hanno più probabilità di svilupparne di nuove