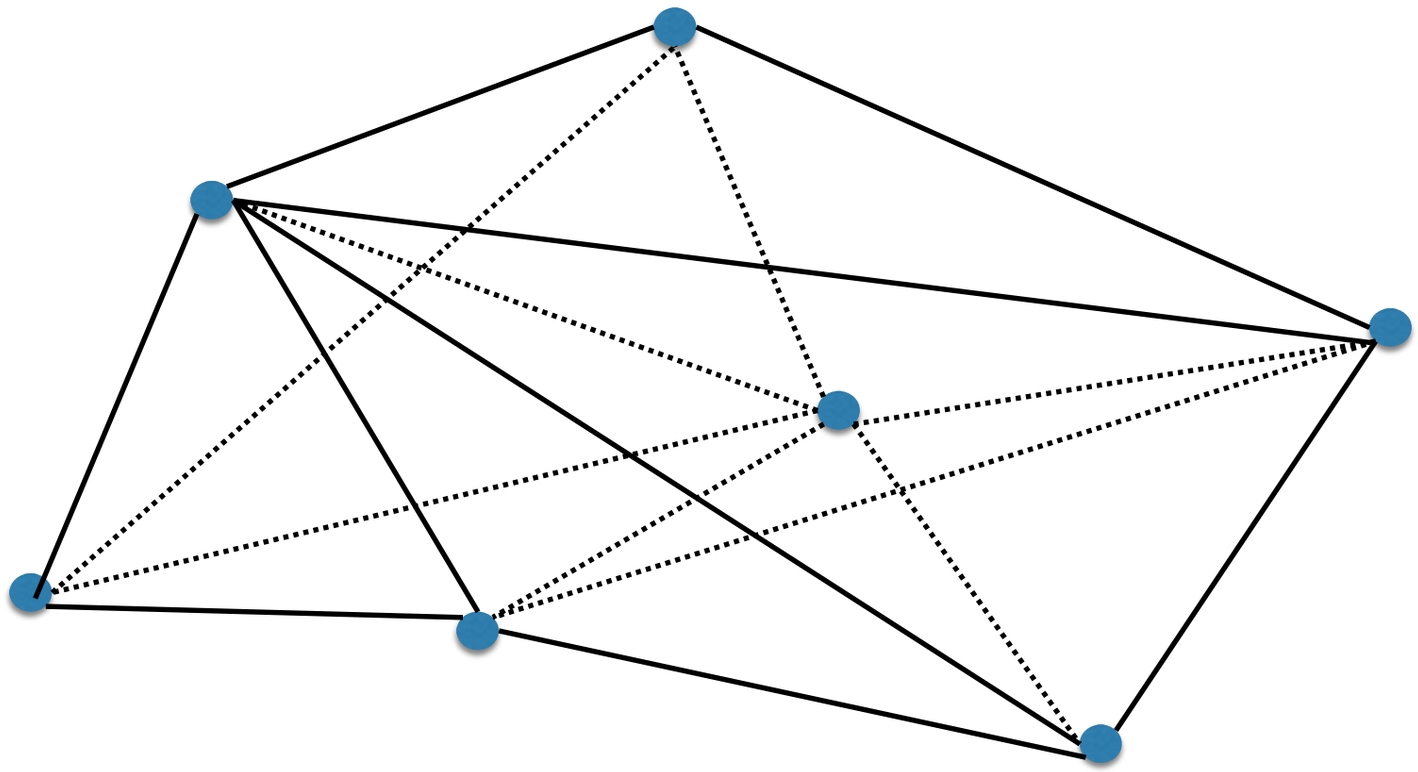
Multichain: rooted blockchain off-the-shelf platform

https://www.multichain.com/

Dott. Paolo Santancini

Blockchain Architect - paolo.santancini@gmail.com

Rooted: ciascun nodo è gerarchicamente dipendente ad altri nodi sulla base di ruoli ben definiti. La rappresentazione della loro distribuzione è data da un grafo (G) non orientato e connesso.



Ruoli: ciascun nodo ha uno o più ruoli.
Ogni nodo è contraddistinto dal suo indirizzo pubblico.

- *Admin*: definisce i permessi di tutti i nodi;
- *Mine*: partecipa al processo del consenso;
- *Activate*: gestisce i permessi a basso rischio dei nodi;
- *Create, Issue*: crea oggetti (asset, etc..);
- *Connect*: abilita la connessione alla blockchain;
- *Send*, Receive: movimenta transazioni all'interno della blockchain.

Mining: consiste nel numero di blocchi che può essere creato da uno stesso nodo con ruolo «mine», all'interno di una determinata finestra temporale.

Mining-diversity: parametro blockchain $(0 \leq x \leq 1)$

<u>Mining-diversity</u>: coefficiente legato alle probabilità Pr(F) e Pr(C). La prima è relativa al congelamento dell'intero processo di mining per malfuzionamento di determinati miners, la seconda riguarda il loro funzionamento malizioso. Sono espresse come distribuzione binomiale cumulativa:

$$Pr(F) = Pr(Bin(miners, 1-f) \leq (spacing-1))$$

$$Pr(C) = Pr(Bin(miners, 1-c) \leq (miners-spacing))$$

c = probabilità indipendente di ciascun miner relativa al verificarsi di un atteggiamento malizioso (colluso)
spacing = numero di nodi con lo stesso stato (*effettivamente operanti* = *miners*mining-diversity*)
miners = numero di nodi con ruolo «mine»

<u>All'aumentare del valore del mining-diversity diminuisce il valore di Pr(F) o di Pr(C) (grado di tolleranza).</u>