Validating a New Block

在有節點找個新塊後，會立刻廣播到網路，每個節點都會獨立檢查侯選塊。

Assembling and Selecting Chains of Blocks

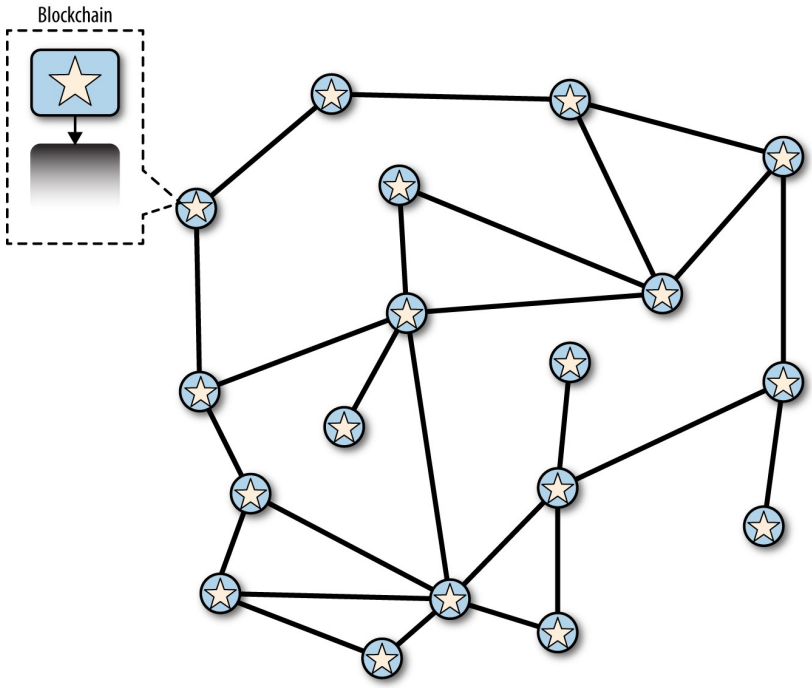
節點會選擇最長鏈作為主鏈，並將其實鏈視為支鏈。

最長鏈指得不是有最多區塊的鏈，而是有最多 PoW 的支鏈。

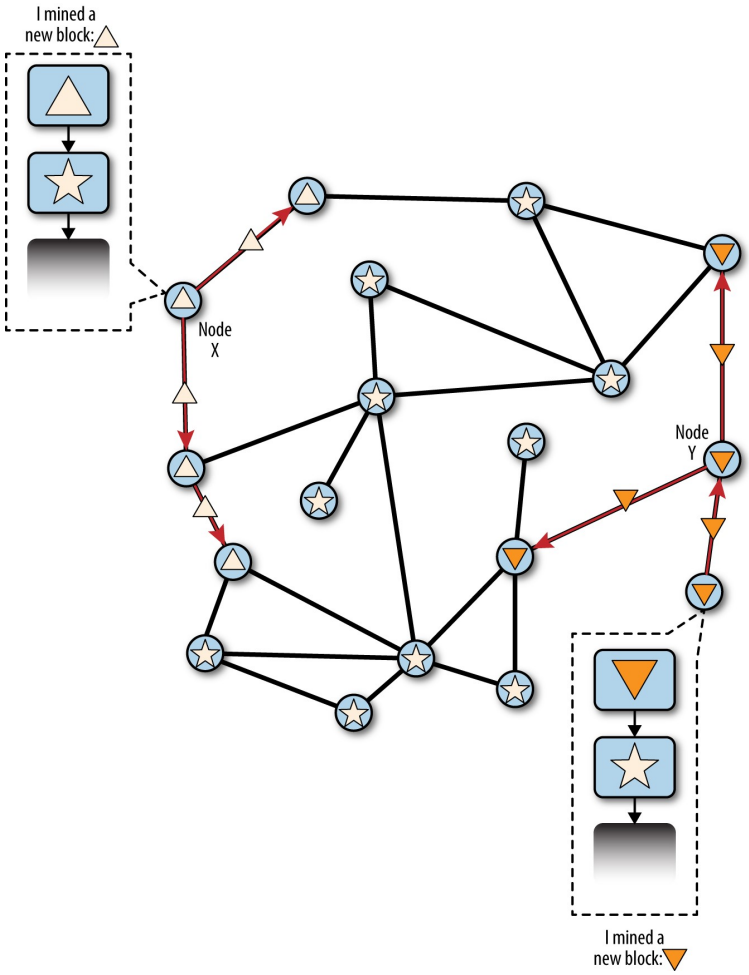
Blockchian Forks (not Hard or Soft)

這裡的 fork 的指得是自然情況下因為網路延遲而產生的分岔。

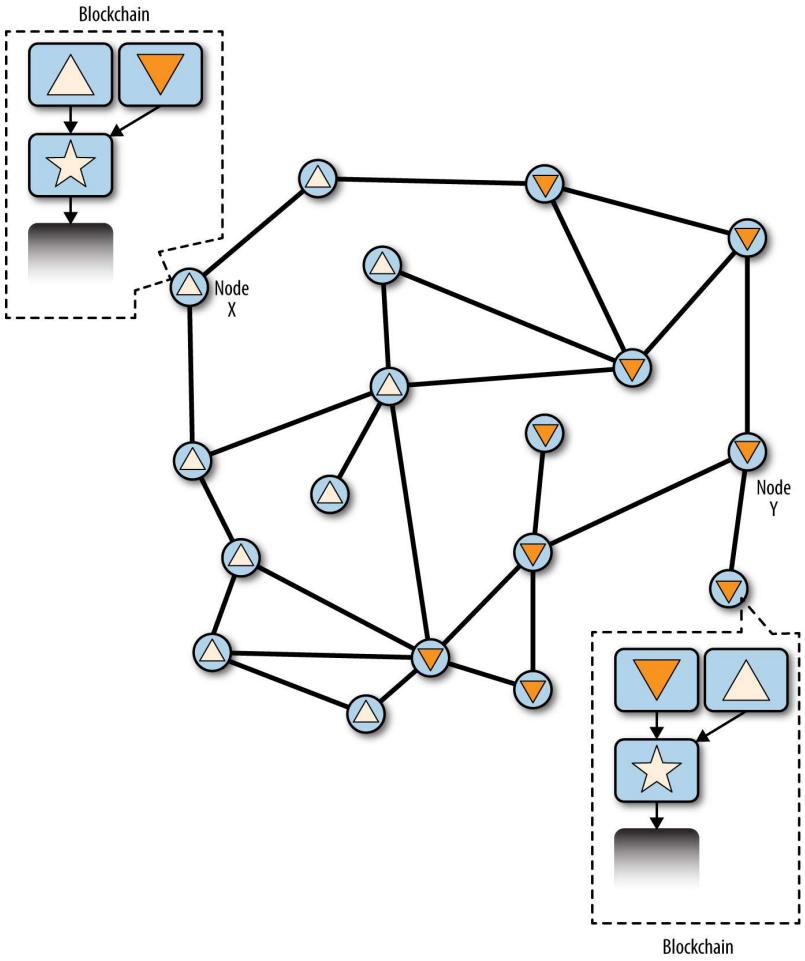
以下圖示 forks 整合的過程：



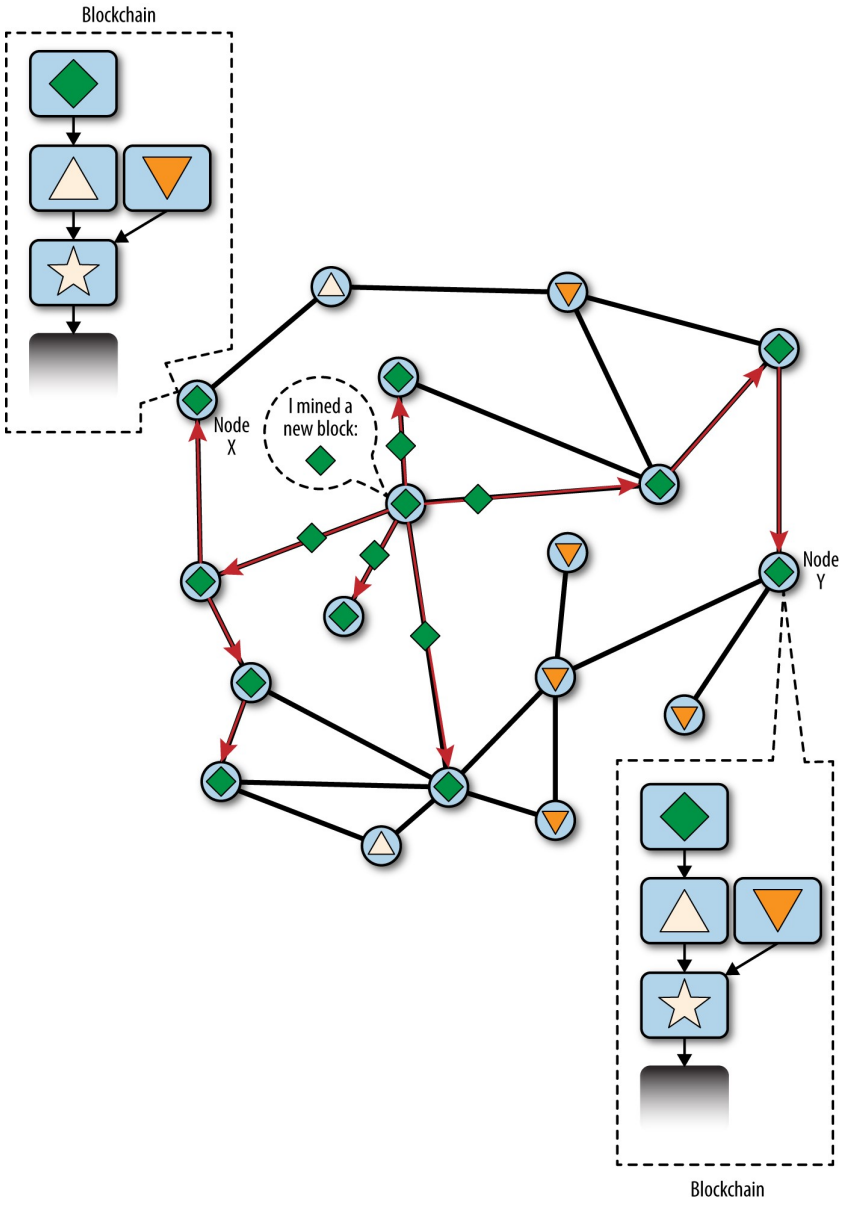
一、在還沒分裂前



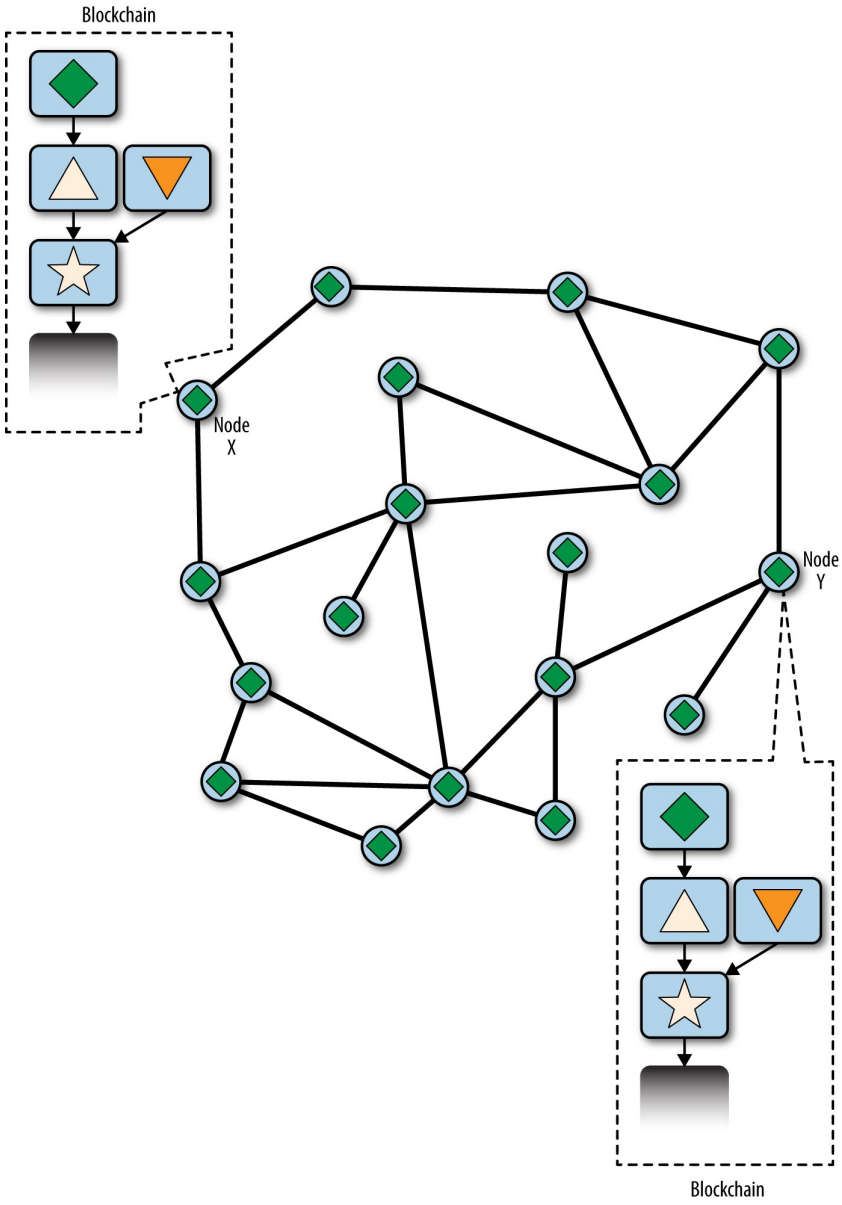
二、同時有不同節點挖到不同的新塊並廣播。



三、整個網路產生了分岔。

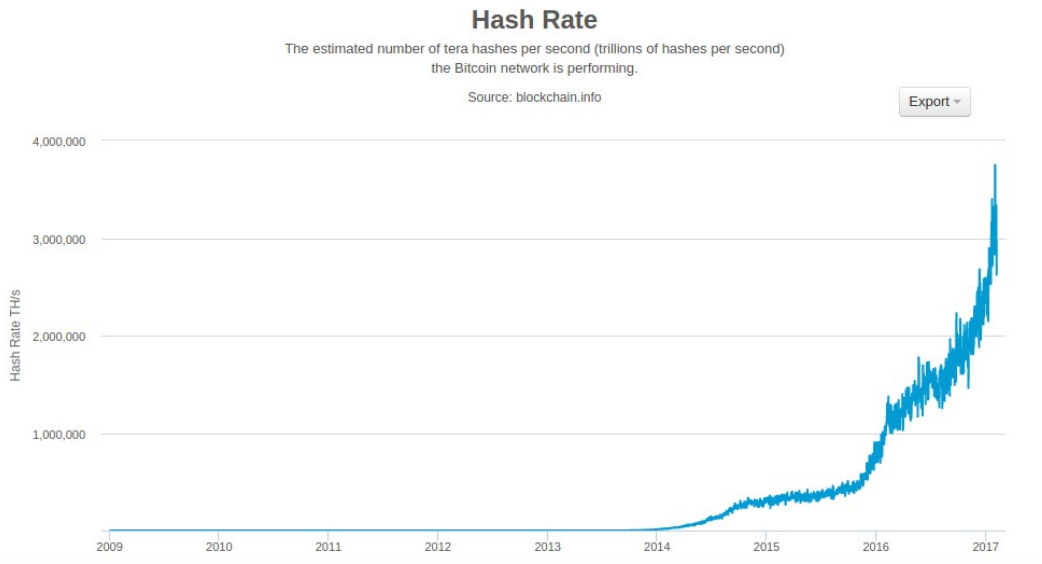


四、新一輪的挖礦開始，礦工並選擇他的父塊，進行投票。



五、網路又重新達到一致

Mining and the Hashing Race



Mining Pool

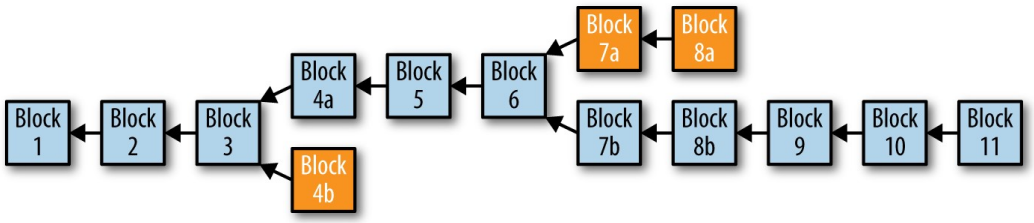
礦工為了要分散風險而加入礦池，但會有中心化的問題。

Consensus Attack

最有名的是 51%攻擊，原理是用強勢的算力再造一條新鏈取代掉原來已交易完的舊鏈，以達到雙花。

Hard Fork

出現在比特幣節點有部分的使用不相容的共識規則，導致產生出並行的兩條鏈。產生原因可能是軟體更新，或者是刻意分裂的。



Soft Fork

是相容於過去版本的更新，就算有節點不用新的規則，還是可以繼續運行不會產生分裂。但這樣的更新會有所限制，只有分寬舊有的規則，不用加上新的規則。