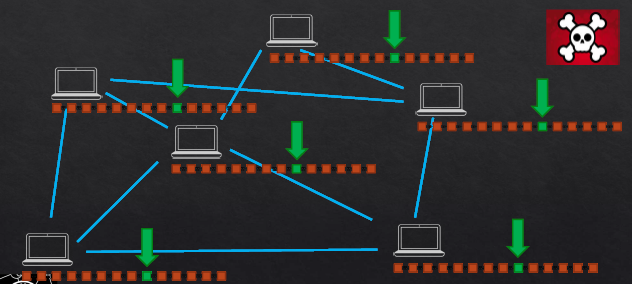
**4 – Redes P2P Distribuídas e Mecanismo de Consenso**

**Rede P2P:** No Blockchain, uma rede peer-to-peer ou P2P é uma rede distribuída e descentralizada (não há uma autoridade central) de computadores na qual cada um dos nós da rede funciona tanto como cliente quanto servidor do Blockchain e todos possuem igualmente a mesma autoridade sobre a rede, sendo que esses computadores estão ligados par a par.

**Mecanismo de Consenso:** Por meio da rede P2P cada computador pode verificar como está a cadeia de blocos dos outros computadores a quais ele está ligado, e se está de acordo com a dele, ou em Consenso com ele, uma rede é completamente atualizada quando todos os computadores participam do acordo entrando em Consenso. O Mecanismo de Consenso também está por trás da validação da adição de um bloco à rede, nesse caso existem dois principais Algoritmos de Consenso: Proof-of-Worf e Proof-of-Stake, utilizados no Bitcoin e Etherum respectivamente, mas de forma resumida, há uma disputa entre os computadores (mineradores) para quem consegue ser o primeiro a validar um bloco adicionando-o à rede.

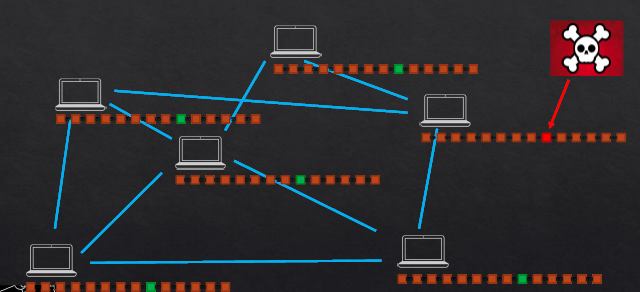


Veja que cada computador tem a cadeia de blocos do Blockchain idêntica) pois ela é constantemente atualizada por meio do Mecanismo de Consenso, fazendo com que todos fiquem com a mesma cadeia.

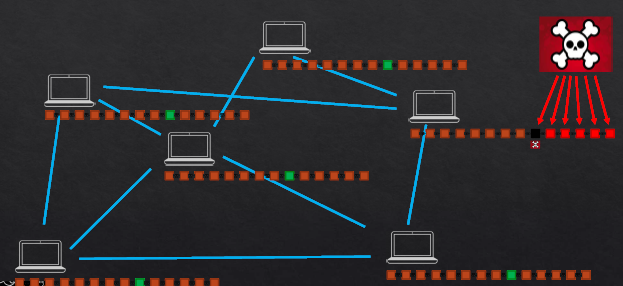
Logo, já vimos que cada computador pode se comportar como um servidor, armazenando essa cadeia de blocos, contudo eles também podem adicionar blocos a essa cadeia, por exemplo quando um computador adicionar um novo bloco nessa cadeia na próxima atualização todos os outros computadores ficaram com a cadeia anterior + esse novo bloco.

Voltemos ao nosso exemplo da aula passada, digamos que em algum momento adicionamos um bloco que contém a nossa escritura, e então essa nova cadeia foi atualizada na rede.

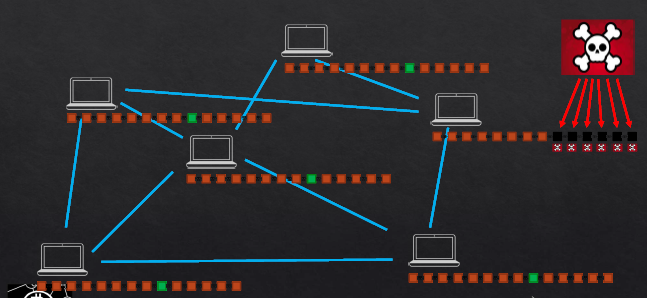
Depois de um tempo, varios outros blocos foram inseridos na cadeia da rede, e um hacker deseja fraudar minha escritura:



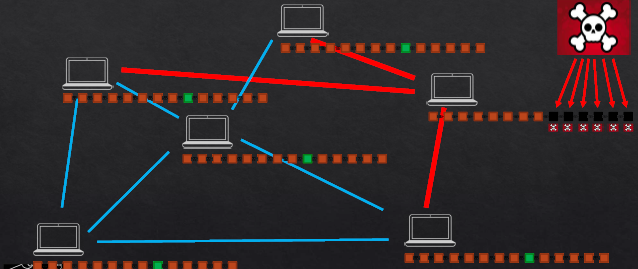
Vimos que ao modificar um bloco da cadeia, ele teria que alterar o hash de todos os blocos subsequentes da cadeia:



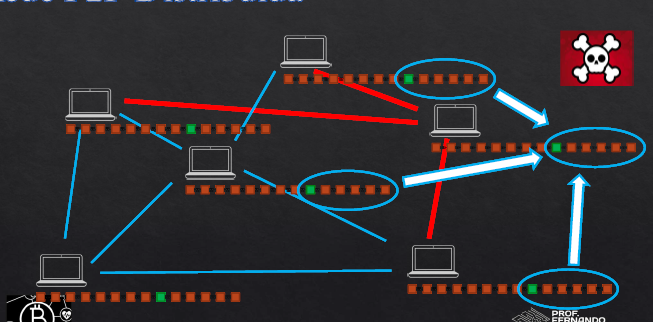
Digamos que o processamento do computador do hacker seja tão bom que ele consiga fazer essa modificação antes da atualização da rede:



Contudo, os blocos que estão fazendo par com ele verificarão que há um conflito na cadeia desse computador com relação às deles:



E sendo a cadeia fraudulenta uma minoria na rede, a rede entrará em consenso, e na próxima atualização, a cadeia correta da rede será sobrescrita, apagando da rede blockchain a fraude que o hacker tentou fazer.



Logo, a única maneira de um hacker conseguir fraudar essa transação seria apenas se ele hackeasse a maioria dos computadores da rede, logo na atualização a cadeia sobreposta seria a que ele criou. Mas note que isso é extremamente difícil supondo que haja muitos computadores.

Veja portanto, que isso aumenta ainda mais a segurança do blockchain.

Mais fontes:

<https://www.criptofacil.com/o-que-e-mecanismo-de-consenso/>

<https://www.criptofacil.com/o-que-e-e-como-funciona-o-proof-of-work/>

<https://pt.wikipedia.org/wiki/Peer-to-peer>

