Blockchain

Bitcoin è una moneta non fiduciaria:

- Non ha una terza parte centrale che può "censurare"
- Non ha costi di verifica
- Facilità di transizioni
- Mantenere le proprietà nel tempo
- Quantità limitata
- Non contraffabile
- Offerta controllata (dipende dal mercato che è libero)

È quindi:

- Riserva di valore
- Mezzo di scambio
- Unità di conto

Il mining è finalizzato come CERTIFICA di bitcoin e delle transizioni, non nella produzione, è stato aggiunto il guadagno per incentivare l'attività, quando saranno prodotti tutti i bitcoin bisognerà guadagnare in altro modo.

Caratteristiche Blockchain

È un protocollo, un database che contiene tutti i file che vengono trasferiti nellea rete.

Ha la funzione di registro pubblico delle transizioni certificate

Preserva da duplicazioni e falsificazioni.

È distribuita per tutti gli utenti.

Mining

Premia il primo miner che risolve la Proof of Work (reward), ha spesa in fatto di energia elettrica e utilizzo di hardware performanti.
Il reward si "regola" ogni 2 settimane in base al valore di mercato del bitcoin e alla difficoltà di compilazione.

Truffare la rete

Immaginando che la rete stia lavorando al blocco 91, se un miner sta lavorando al 60, prima di "attaccare il 91" dovrei chiudere tutti i calcoli tra il 60 e il 91, devo quindi andare contro corrente rispetto tutta la rete con costi e tempi elevati.
Se ho risorse elevate di conviene di più aiutare la rete facendo mining che attaccando la rete, quindi non ha senso attaccare bitcoin a scopo remurativo.

Altre cripto valute

Sono fattibili in quanto bitcoin è open source, degli esempi di altri cripto-valute sono:

- LiteCoin

- Smart contract: è specializzato nei contratti (se metto dei soldi in una scatola, ti saranno asseganti se faccio un'attività X). Devo scrivere il contratto in linguaggio di programmazione, non facile quindi. Il contratto NON È REVERSIBILE.