# Nakamoto Consensus algorithm | Byzantine Generals secure algorithm

Decentralized Financial System | Bitcoin | Nakamoto Consensus | semiring $\mathbb{N}^{n}$-module

assemblage Wojciech Lawren

$$n\left\{\sum_{F_k=0}^{F_k<m}\frac{F_{\mathrm{k+1}}}{\varepsilon+F_k}=\|F_k\|^{\mathrm{v.1}}<\sum_{k=1}^{+\infty}\frac{f_{\mathrm{k+1}}}{\varepsilon+f_k}=\|C_k\|\to d(0,m)\wedge\int_{[1,\mathrm{k}\dot{-}\mathrm{m}]}f\delta k\right.$$

$$(D)\Omega\sim\left\{p_2p\supset N\supseteq n\mid k_k\colon N\mapsto n\veebar k_m\colon N\mapsto N_n\right\}\to\int_{[[1,N_n]_n]}H\delta k\sim O(N)$$

$$H_k:=N\left\{\int_{[1,\mathrm{k}]}\overset{x<X}{\underset{x=0}{\mathbf{for}}}\left(S_{256}(x\cdot k_k)<2^{224}\div D\right)\mathbf{exit}\,\delta k\rightrightarrows n\left\{\int_{[1,N_n]}\delta k_m\to[[1,N_n]_n]\right.\right.$$

*complete p2p-net space*

*sequence of seminorms associated to norm*

*Nakamoto Consensus*

*derived extension corollary sine qua non simulative limit*

- *ISO 31-11*
- *asymptotic*
- *pseudocode*

---

## Definition *ad hoc*

***p₂p* : peer-to-peer**

computer network : assert service without central coordination

**blockchain : *p₂p* immutable ledger**

network database : distributed across $p_2p$ nodes, rely on consensus

**consensus**

network algorithm : assert blockchain coherent transaction blocks : $O(n)$

**simulative limit**

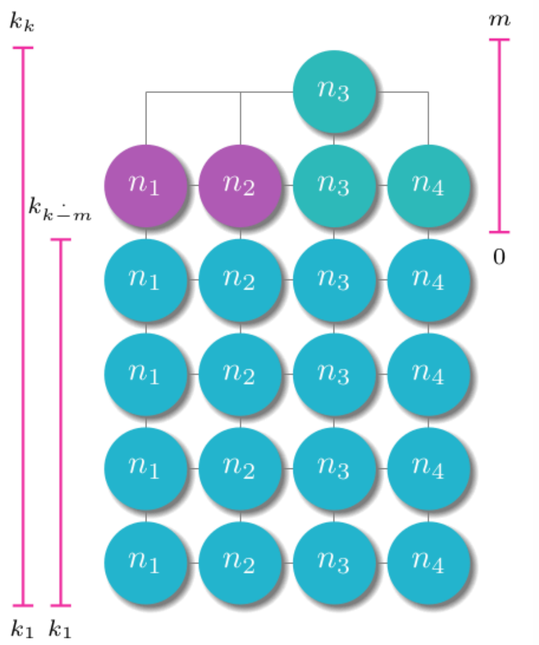
computational simulation : assert system aspect optimal limit

**PoW : proof of work**

algorithm : inverse of one way function : $O(n)$

**difficulty retarget**

reenforcement algorithm : constrain difficulty level to enforce block interval : $O(log\ k)$




## Metric space

$$\|f\|=\sum_{N=1}^{+\infty}2^{-N}\frac{\|f\|_{[-N,N]}}{1+\|f\|_{[-N,N]}}$$