Blockchains

Dist. Comp.

Spatial Security: Impossible for adversary to be 'everywhere'

Cryptography

Computational Security: Impossible for adv. to quickly solve 'hard' problems with non-negligible prob.

Game Theory

Uncertainty based Security: Impossible for adv. to 'know' everything

Problem: To decentralize 'trust' → requires agreement

Fundamental Technique:

① Tamper resistant chain of info (append only)
② Monopoly is avoided (randomness)
③ Adding to 'longest' ~~correct~~ chain is rewarded
④ Appending elsewhere is penalized.

'Correct' chain (of info) is agreed upon

Ex: DNA

Append only chain, no time travel

Random mutations, hormonal chemistry

Survival of the fittest