**Cryptoeconomics**

Bitcoin is a fusion of several subfields of computer science and economics. It’s a pretty radical idea - radical enough that it has produced a whole new field of study, with a new term coined to describe its underlying principles - cryptoeconomics. Cryptoeconomics is the use of cryptography, distributed systems consensus algorithms and game theory to build incentive mechanisms for entities in a decentralised network to cooperate.

Key ideas:

**Cryptography**( **TODO: expand later**)

* use of public keys to send a secret message that can only be unlocked by the owner of the corresponding private key
* use private key to sign a message to prove that the message comes from you.

**Economics**

* How to devise an efficient system for people to trade goods and services
* Early trade consisted of barter system
  + we choose to give up something in exchange for gaining something else. The idea is that we give something up that is valuable to us(commodity X) to gain something else which we need (commodity Y). But even if we make this choice to give up X, we may not be able to make this trade for several reasons:
    - We may not be able to find someone who has that commodity Y available and willing to exchange it for commodity X
    - They may not want to do the exchange right now
    - Due to geographical constraints it may not be easily possible to do the exchange.

So, it is important to come up with a common unit of value exchange or a currency which all parties need to agree on to have a certain value and then they can price the commodity they have on offer wrt to this currency.

* So we need a currency that:
  + Is easy to exchange for anything else(easily portable, divisible into smaller units)
  + Is scare, because if there isn’t a scarcity of that currency, everyone could easily get as much of it as they need and then no one would be willing to give up anything in exchange for it - i.e. It won’t have any value as a unit of exchange. So scarcity of a currency is representative of the cost of the item we’re willing to exchange for it.
  + Doesn’t lose its value over time (is a stable unit of measure of value)
* Money comes to mind
  + What is money really and why do we need it? To pay for things. Why do we pay for things? Because otherwise we could have everything - but we can’t. In real life, we make choices because of the scarcity of things:
    - Ownership of items: diamond encrusted bluetooth set vs warm winter jacket
    - Time: Stable but boring job vs the poor PhD student life you know will enjoy

So money is a scarce resource which is a placeholder to represent the scarcity of all other resources in the world (goods/services/time.. pretty much everything) and is used as a intermediate means of exchange of these scarce resources for one another.

**Game Theory**

Game (zero-sum vs non zero sum - **TODO: expand)**

Nash equilibrium - defines the game state reached on following the course of action which offers the highest reward to all participants in the system in all scenarios - that is a rational actor cannot improve their outcome by making any other move.

The aim of crypto-economics - build a non-zero sum game with a Nash Equilibrium which is win-win for all players (should ideally be the aim of economics too, but sadly that isn’t always the case - power corrupts and absolute power corrupts absolutely)!<https://ncase.me/trust/>

Game theory can have positive incentives and negative incentives (In the case of bitcoin, positive incentives are created using block reward and transaction fees, and negative incentives are created using loss of block reward and the associated work done in PoW and loss of teh deposit in PoS **TODO:expand**)