Trust

- Intuitively obvious concept
- Difficult to rigorously define
- Different kinds of trust:
  - I trust a doctor on my health
  - I trust a communication link on data integrity
  - I trust that a friend will return the money I lent her

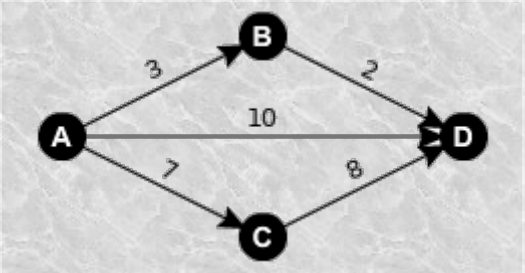
We need this concept (along with the concept of reputation) for ambitious projects such as decentralized search

Decentralized Trust Network

- We try to create a network of economic decentralized trust between equal entities.
- A directly trusts B a value V:
- A has put value V in a box that either A or B and nobody else can open (e.g. using a 1/2 multisig).
- A (indirectly) trusts B a value V:
- There is at least one trust path from A to B which carries a value V. (Intuitive definition)

DTr(A,D) = 10

Tr(A,D) = 19



More on trust

Why risk my money?

- You can replenish it by stealing from somebody that trusts you – honest/passive strategy
- Alice (indirectly) trusts Bob a value V if Bob goes away with all the money entrusted to him, everyone else follows the passive strategy and Alice loses value V in the worst case.
- You already trust a potential seller, so why read reviews?
- Obviate the need for star or review based ranking

Interesting results

- If we consider each direct trust as a weighted edge in a graph, we get:

$$\text{Trust}(A,B) = \text{MaxFlow}(A \rightarrow B)$$

- When we want to buy from a seller there is a way to recalculate direct trust such that the risk of losing money from the seller is maintained before and after giving him the money.

Closing comments

- User is freed from reading dubious reviews and judging a seller's quality through stars, instead he must risk losing money by explicitly trusting it to his friends.
- There are still some privacy considerations involving calculation of max flow.
- The infrastructure is non Sybil-attackable.
- This is still a work in progress.

Questions?

https://github.com/OrfeasLitos/DecentralizedTrustNetwork