Blockchain

1. *What is Blockchain*?

   Blockchain is a Distributed Database.

   It is:

   - Append only
   - Transparent
   - Incorruptible (under mild assumptions)
   - Secure
   - Time-stamped
   - With Distributed Consensus

2. *Distributed Consensus*

Financial Arrangements

Barter

Simple enough: If A has b but wants a and B has a but wants b then the two can swap with each other. What is A has c and wants a, but B has a but wants b? We look for C who has b and wants c, and then we can arrange for an exchange.

The issue:

Getting the people to get together and arrange an exchange.

Solution:

1. Cash
2. Credit

Credit Make the transaction, be in debt until repayment after.

Cash Denominating some cash value to all goods, and using cash to buy and sell.

Cryptographic Hash Functions

Properties:

- Deterministic
- Efficient to compute
- Pre-image resistance
- Second pre-image resistance

- Collision resistance
- Small change in the input should modify hash extensively
- Fixed side output, for input of any size