SOCIAL NETWORKS Nov 12 2015

LECTURE #17

BTC: Bit-Coins ฿

- 2008.
  Satoshi NAKAMOTO: { Widely presumed to be a pseudonym.

- 2009 (January)
  Became fully operational.

- 2009 – present
  All the transactions ever carried out in the Bit-Coin system
  ⇒ Available openly on the internet (in an anonymous way.)

฿: Bitcoins ≡ A decentralized electronic CRYPTO-currency system using PEER-TO-PEER networking.

(1) Enable payments between parties without relying on mutual trust.

(2) DIGITAL COINS

Issued and transferred by the bitcoin network.

(3) Total BTC = 14,088,575 (early 2015)
Market Cap = 3.2 B $ (us).

(4) No centralized Issuing Authority
- No backing by Reserve.
- No intrinsic value
- Circulating money.

(5) The BTC network is programmed to increase the money supply in a slowly increasing geometric series.

→ Until the number of BTC's reaches an upper limit of 21 million.

(6) Exchange rate fluctuates.
$ 1,240 = 1 BTC (December 2013)
$ 0.01 = 1 BTC.

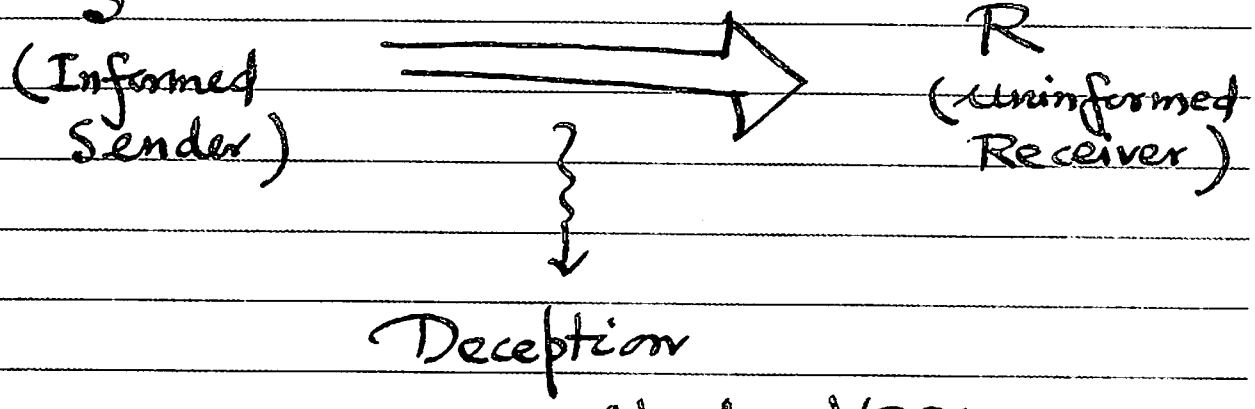
Key Objects.

1) Bit Coin Wallet. } Senders
2) Bit Coin Addresses (≥1) } - Receivers.
3) Bit Coin - Block chains } Recommenders
4) Bit Coin - Miners } - Verifiers.

↳ They solve increasingly difficult proof-of-work problems to be rewarded with BTC's (Satoshis).

Signaling Game

Information Asymmetry.



Deception

Needs VERIFIERS

V

a) Local Properties
(Propositional Logic Rules)

{Crypto System}
RSA.

b) Global Properties
(Modal Logic Rules)

{Costly Signaling,
{Distributed Computation
- No Collusion.

Verifying Global Properties:

BLOCK CHAIN (https://blockchain.info/)

- Distributed File System
  Resilient / Fault Tolerant

- Peer-to-Peer Network.
  No central Authority

- Issues: Consistency & Fault Tolerance
  CAP Theorem
  (Consistency, Availability, Partition Resistance)
  Byzantine General Problem
  (Malicious Collusion)
  Ripple Payment System

Main Ingredients:

(1) Bit-Coin Miners
(2) Time stamps
(3) Costly Signaling

Verify Global Properties:

a) Create a block chain

$\langle m_1, u_1 \rangle, \langle m_2, u_2 \rangle \cdots \langle m_n, u_n \rangle$

time stamps

$u_1 \leq u_2 \leq \cdots \leq u_n$.

Messages

$m_1, m_2, \cdots, m_n$

$\exists!$ message $(Vr_s, \cdot, \cdot, H(m_i, u_i))$ $\forall s$

Summary BTC.

$S \rightarrow R$

$(Vr_S, Vr_R, Trans(S \rightarrow R) = Y // Y \leq X @ u,$

$BTC\_W(S,u) = X @ u, u)_{Sg_S}$

Authentication

Local Property $Y \leq X$

$X = Deposit_S[0..u]$

$- Withdraw_S[0..u]$

GLOBAL PROPERTY

No-Double Spending

$\forall_{u_1 \leq u_2} \quad Dep_S[0..u_1] \triangleleft Dep_S[0..u_2]$

$\vee \quad WD_S[0..u_1] \triangleleft WD_S[0..u_2]$

Monotonicity of Trans.

+ Proof-of-Work.