Social Networks  Nov 12 2015

Lecture #17

BTC: Bit-Coin B

$ 2008.
Satoshi NAKAMOTO: Widely presumed to be a pseudonym.

0 2009 (January)
Became fully operational.

0 2009 - present
All the transactions ever carried out in the Bit-Coin system
⇒ Available openly on the internet (in an anonymous way)

B: Bitcoins = A decentralized electronic

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

3. No centralized issuing authority
   - No backing by reserve.
   - No intrinsic value
   - Circulating money.

4. 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.

5. Exchange rate fluctuates:
   - $1,240 = 1 BTC (December 2013)
   - $0.01 = 1 BTC.
Key Objects.

1) Bit Coin Wallet → Senders
2) Bit Coin Addresses (21) → 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.

S  \rightarrow  R

(Informed Sender)  \rightarrow  (Informed Receiver)

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
\[
\langle m_1, u_1 \rangle, \langle m_2, u_2 \rangle \ldots \langle m_n, u_n \rangle
\]

time stamps
\[
u_1 \leq u_2 \leq \ldots \leq u_n.
\]

Messages
\[
m_1, m_2, \ldots, m_n
\]

\[\exists! \text{ message } (v_{r_5}, \ldots, H(m_i, u_i))\]
Summary BTC.

\[ S \rightarrow R \]

\[(V_{s}, W_{R}) \text{ Trans } (S \rightarrow R) = Y / Y_{s} x @ u, \]

\[ BTC \_ W(s, u) = x @ u, u \]

Authentication

Local Property \( Y \leq X \)

\[ X = \text{Deposits}_{S}[0..n] \]

- Withdraws_{S}[0..n]

Global Property

No Double Spending

\[ \forall u, s_{u} \text{ Deps}_{S}[0..u] < \text{Dep}_{S}[0..u] \]

\[ \forall \text{ WDs}_{S}[0..u] < \text{ WDs}_{S}[0..u] \]

Monotonicity of Trans.

+ Proof of Work.