Lecture #13

BIT-COINS (BTC) €

May 7, 2013

2008
Satoshi Nakamoto (widely presumed to be a pseudonym)
→ Fully operational January 2009

All the transactions ever carried out in the Bitcoin system
→ Available on the internet (in an anonymous way)

BITCOINS = A decentralized electronic cash system using peer-to-peer networking
→ Enable payments between parties without relying on mutual trust.
→ Digital Coins: Issued and transferred by the bitcoin network.
→ Total Current Value = $100x10^6.

BITCOIN WALLET

BITCOIN ADDRESSES (≥ 1)

→ No centralized issuing authority (e.g. no backing by Reserve)
→ No intrinsic value.
The BTC network is programmed to increase the money supply in a slowly increasing geometric series. Until the number of Bitcoins reaches an upper limit of 21 million.

→ Bitcoin Miners.
Solve increasingly difficult proof-of-work problems to be awarded with BTC's.

→ Exchange rate: Fluctuates

$30 = 1 Bitcoin

↓

$0.01 = 1 Bitcoin.
Signaling Game (Information Asymmetry)

\[ \text{Informed} \quad \rightarrow \quad \text{Uninformed} \]

A \quad \text{Sender} \quad \downarrow \quad \text{Receiver}

\begin{align*}
\text{Deception} &\quad \simeq \quad \text{Local/Propositional Property} \\
\text{Verification} &\quad \simeq \quad \text{Global/Modal Properties}
\end{align*}

Non-Repudiation (Cryptography)

Costly Signaling [Proof of work]

Verifier

\[ \forall \]

2-player Game \quad \rightarrow \quad 3\text{-player Game} \]
A $\rightarrow$ Signing key (Private) $s_{A}$
Verification key (Public) $V_{A}$

A detects state (type) $s \in S$
Selects message $m \in M$
Time stamp $t \in T$
Sends $\left(\#A, m, \#B, H(s,t)\right)$ $\downarrow$
$\text{digest:}$

B (Verifier) can verify
1) A sent the message (using public key)

2) Local Property $f(s, m)$

3) Temporal Property $g(s, t)$

Verifier creates a chain
$\langle s_{i}, t_{i} \rangle, \langle s_{i}, t_{i} \rangle, \ldots, \langle s_{n}, t_{n} \rangle$
p. that $t_{1} \leq t_{2} \leq \ldots \leq t_{n}$

$= \text{message } \left(\#A, m, \#B, H(s_{i}, t_{i})\right)$ $\downarrow$

Proof-of-Work
Time Stamp:
BTC
BitCoins
A → B.

(#A, BTC-Wallet(A) = X, Transfer(A → B) = Y st. Y ≤ X, @ t ∈ T) sgtA

Authentication
Local Property: Y ≤ X

\[ X = \text{Deposits}_A[0..t] - \text{Withdrawal}_A[0..t] \]

Global Property: No Double Spending

\[ a \uparrow t_1 \leq t_2 \Rightarrow \text{Deposits}_A[0..t_2] - \text{Deposits}_A[0..t_1] \]

or

\[ \text{Withdrawal}_A[0..t_1] - \text{Withdrawal}_A[0..t_2] \]

Monotonicity of transactions.

Translating Work: