Lecture #13

pp 90

May 7 2013

BIT-COINS (BTC) ₿

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 = 100×10^6.

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~~ 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

↕

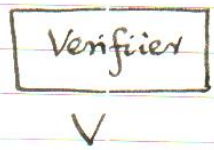
$0.01 ≡ 1 Bitcoin.

pp 92

Signaling Game (Information Asymmetry.

Non-Repudiation. (Cryptography)

Costly Signaling [Proof of work]



2-player Game ⟶ 3 player Game.

pp93

A → { Signing key (Private) Sg_A
Verification key (Public) Vr_A.

A detects state (type) $s \in S$.
Selects message $m \in M$
time stamp $t \in T$
Sends $(\#A, m, \#B, H(s,t))\big|_{Sg_A}$
↓
digest.

B (≠ Verifier) can verify
1) A sent the message (using public key)
2) Local Property
$\mathcal{F}(s,m)$
3) Temporal Property
$\mathcal{G}(s,t)$

Verifier
Creates a chain
$\langle s_1, t_1\rangle, \langle s_2, t_2\rangle \cdots \langle s_n, t_n\rangle$
s.t. that $t_1 \leq t_2 \leq \cdots \leq t_n$
$\exists_{message}\ (\#A, \cdot, \#\cdot, H(s_i,t_i))\big|_{Sg_A}$

Proof-of-Work
Time Stamp.

pp94

BTC.

Bit Coins.

$A \longrightarrow B$.

$(\#A,\ BTC\_Wallet(A) = X\ ,\ Transfer(A \to B) : Y$
s.t. $Y \leq X, @t \in T)_{sg_A}$

Authentication

Local Property $Y \leq X$

$X = Deposits_A[0..t] - Withdrawal_A[0..t]$

Global Property No Double Spending

a $\forall t_1 \leq t_2$ $Deposits_A[0..t_1] \lhd Deposits_A[0..t_2]$
or $Withdrawal_A[0..t_1] \lhd Withdrawal_A[0..t_2]$

Monotonicity of transactions.

Proof-of-Work.