LECTURE # 11 APRIL 28 2015

2008 BIT-COINS (BTC) ฿

Satoshi NAKAMOTO. { Widely presumed to be a pseudonym.

Became fully operational in January 2009

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

฿itcoins ≡ 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
Market Cap = 3.2 Billion $
(4) No centralized Issueing Authority
(No backing by Reserve; No intrinsic value)

<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

$1240 ≡ 1 BTC (December 2013)

$0.01 ≡ 1 BTC.

Some Objects:

1) BITCOIN WALLET
2) BITCOIN - ADRESSES. (≥1)

} Sender-Receivers

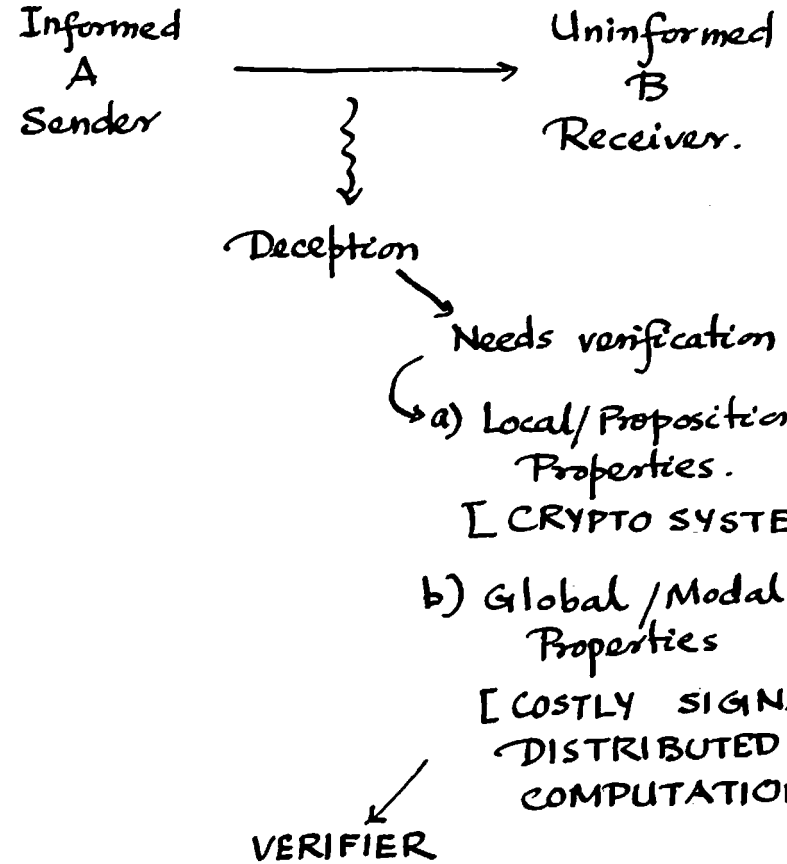
3) BITCOIN - BLOCKCHAINS
4) BITCOIN MINERS

} Recommender-Verifier.

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

SIGNALING GAME

Information Asymmetry.



Three-player

Sender-Receiver-Verifier Game.

PUBLIC KEY CRYPTO SYSTEM

Asymmetric Cryptography:

2 separate keys. { Public / Verification key Vr_A
Private / Signing key Sg_A

Vr_A & Sg_A are mathematically linked while they are computationally asymmetric.

ONE WAY FUNCTION.

<1> Mathematical Underpinning:

Algebraic Problem { a) Integer Factorization
b) Discrete Logorithm
c) Elliptic Curves.
d) Lattice Theory.

Closely related to ideal membership.

<2> It is computationally easy for a user A to generate { Vr_A Sg_A

<3> It is "hard" to derive Sg_A from Vr_A.

(a) Anyone can verify A's identity

(b) No one (with conventional computational resources) can assume/steal A's Identity.

<c> A can have many persistent heteronyms (anonymity/pseudonymity).

<d> A's identity can be linked to his genetic identity (e.g. whole-genome)

<e> No secure key-exchange is necessary.

<4> Public key Encryption:

$(\text{message})|_{Vr_A} \xrightarrow[CT]{}$ Send to A.

Only A can decode the message

$(C.T)|_{Sg_A} = (\text{message})_{Vr_A \circ Sg_A}$

Cypher Text

$= \text{message}.$

Verifies A's identity.

(Also anyone can send A a secret over open channel.).

<5> Private key Signature.

$(\text{message})|_{Sg_A} \xrightarrow[ST]{}$ Sent by A.

Only A could have encoded/signed the message.

$(ST)|_{Vr_A} = (\text{message})_{Sg_A \circ Vr_A}$

$= \text{message}.$

Authenticates A's action.

(Anyone can verify A's action.)

NOTE BOOK

Example RSA (Rivest - Shamir - Adleman).

<1> Choose 2 distinct prime numbers, p, q, $p \neq q$.

<2> Compute $n = pq$

$$\varphi(n) = \varphi(p)\,\varphi(q) = (p-1)(q-1)$$

Euler's totient fn.

<3> Choose e, s.t. $\gcd(e, \varphi(n)) = 1$

$$d \cdot e + c\varphi(n) = 1$$

$$\therefore d \cdot e \equiv 1 \pmod{\varphi(n)}$$

$$d \equiv e^{-1} \pmod{\varphi(n)}$$

<4> $Vr = e$ ← Public

$Sg = d$ ← Private

<5> m = message → $m|_{Vr} = c \equiv m^e \pmod{n}$

Polynomial in $\log |e|$

Repeated Squaring.

<6> $m \equiv c^d \pmod{n}$

→ $c|_{Sg} = m$ recovered in polytime if one knows d or $\varphi(n) = n - p - q + 1$ or p, q (factorization of n)

Uses Fermat's little thm: p = prime, $p \nmid a$ $\Rightarrow a^{p-1} \equiv 1 \bmod p$.

$ed + k\varphi(n) = 1$

$\Leftrightarrow \quad ed - 1 = k(p-1)(q-1)$

$m^{ed} = m^{ed-1} \cdot m$

$= \left(m^{(p-1)}\right)^{c(q-1)} m \equiv m \pmod{p}$

similarly

$m^{ed} \equiv m \pmod{q}$

$\therefore (m^e)^d \equiv m \pmod{pq}$

SIGNALING GAME

⟨1⟩ $A \rightarrow$ { Private Signing key Sg_A ; Public Verifying key Vr_A.

⟨2⟩ A detects

(a) type/state $s \in S$ (e.g. $y =$ BTC wallet)

(b) message $m \in M$ (e.g. transfer x BTC to B $\wedge\, y - x \geq 0$)

(c) time stamp t

⟨3⟩ A Sends an augmented message.

$C \equiv \left(Vr_A, Vr_B, m, \#S, t\right)\Big|_{Sg_A}$

($\#S$: digest)

<4> B verifies

(a) A sent the message

$C|_{Vr_A} \Longrightarrow Vr_A, Vr_B$, etc...

(b) Local Properties:

m is consistent with s.

(A sent the message

$y_A \geq x_{A \to B}$

A's wallet has BTC to pay B)

$\boxed{\mathcal{F}(s,m)}$

(c) Global Properties:

$s_{t_1}, s_{t_2}, \ldots$ etc.

satisfy certain state transition properties.

(A did not double-spend)

$\mathcal{G}(s,t)$.

(d) B performs an action consistent with $\underline{m}$

A gets utility $U_A(s,m,a)$

(e.g. receives a good)

B gets utility $U_B(s,m,a)$

$y_B \leftarrow y_B + x_{A \to B}$.

Verifying the global properties.

Create a Blockchain

$\langle s_1, t_1 \rangle, \langle s_2, t_2 \rangle, \cdots, \langle s_n, t_n \rangle$

such that

$t_1 \leq t_2 \leq \cdots \leq t_n$

$\wedge \quad \exists$ message $(Wr_A, \cdot, \cdot, tl(s_i, t_i))|_{Sig_A}$.

Ingredients.

(a) BitCoin Miners.
(b) Costly Signaling (Proof-of-Work)
(c) Timestamp.

Blockchain (https://blockchain.info/)

→ a) Distributed File-System
b) Peer-to-Peer Network
c) Fault-Tolerance
{CAP
{Byzantine General Bob}

◊ Ripple Payment

SUMMARY. BTC.

$$A \longrightarrow B$$

$$(\forall r_A,\ BTC\text{-}W(A) = X,\ Trans(A \to B) = Y \ // \ Y \leq X \ @ \ t \in T)_{Sig_A}.$$

Authentication:

Local Property $Y \leq X$

$X = Deposit_A[0..t] - Withdraw_A[0..t]$

Global Property

NO DOUBLE SPENDING

$$\forall t_1 \leq t_2 \quad Dep_A[0..t_1] \lhd Dep_A[0..t_2]$$

$$\forall WD_A[0..t_1] \lhd WD[0..t_2]$$

(Monotonicity of transactions)

+ PROOF-OF-WORK