University of Virginia **cs4501: Cryptocurrency Cafe** January 28, 2015

Class 5: DigiCash

Schedule

Project 1 is due **Friday, 30 January** (11:59pm).

Upcoming office hours: Thursday 4-5pm (Dave, Rice 507); Friday (Nick, noon-2pm in Hackcville).

Cryptographic Hash Functions

A *cryptographic hash function*, $H(x)$, must satisfy these two properties:

- **one-way** (preimage resistance): given h= $H(x)$ it is hard to find preimage x.
- **strong collision-resistance**: hard to find any pair x and y where $H(x) = H(y)$

If we use SHA-256 for H, how many 258-bit messages would be expected to hash to a given value x?

Signing Message Digests

Sign: Sign(m) = $E(KR_A, H(m))$

Given KU_A, m, and S, how does Bob verify that S is a valid signature from Alice for m?

A bitcoin address for public key K is RIPEMD160(SHA256(K)) where both RIPEMD160 and SHA256 are cryptographic hash functions.

Is this more or less secure than just using K?

Suppose someone finds a way to find collisions for RIPEMD160. How serious of a risk would this pose to bitcoin?

Suppose someone finds a way to find preimages for RIPEMD160. How serious of a risk would this pose to bitcoin?

Untraceable Electronic Cash

High Trust Bank must be trusty!

David Chaum, Amos Fiat, and Moni Naor. *Untraceable Electronic Cash*. CRYPTO 1988.

Simple RSA Signatures
Public Key = (e, n) Private Key = d

Identity: $M^{de} = M \mod n$

Sign(m) = $m^d \mod n$

Blind Signatures Alice picks random k in $[1, n)$
$t = mk^e \mod n$
Sends t to signer.

Signer returns t^d.

$t^d = (mk^e mod n)^d \mod n \quad = m^d k^{ed} \mod n \quad = m^d k \mod n$

Dividing by k gives Sign(m) = $m^d \mod n$.

What should a signer know before signing a random-looking string?

Cut-and-Choose

Suppose Alice sends 256 copies and the Bank checks 255 of them. What is the probability Alice can cheat without getting caught?

What should the maximimum bill size be to prevent cheating?

Identity Strings

I = "alice@alice.org" M_i = "Bill #[r_i] : Bear's Turns Bank owes the holder of this message $100."
+ identity strings: $I_1 = (h(I_{1L}), h(I_{1R})), ..., I_n = (h(I_{nL}), h(I_{nR}))$
where h is a one-way hash function and each $I_{iL} \oplus I_{iR} = I$ (but I_{iL} is choosen randomly).

To spend a bill, the reciever chooses either L or R for each pair for spender to open.

What is the probability Alice can spend a bill twice without revealing her identity?

Before Bitcoin: The Rise and Fall of DigiCash

> *By all accounts Chaum was a charismatic leader with an interesting management style, but he refused to compromise his artistic vision in any area against the best advice of his employees. He was suspicious of everyone and 'paranoid' with a habit of suddenly changing his mind without warning. At one time, Microsoft had offered DigiCash $180 million to allow them to preinstall Ecash software on Windows computers and the deal was on the verge of completion, but Chaum suddenly decided that his product was worth more and the deal collapsed. If the deal had gone through, cryptocurrency would now be as ubiquitous as Internet Explorer.*