University of Virginia **cs4501: Cryptocurrency Cabal** November 16, 2015

Class 23: Before (and Beyond) Bitcoin

Schedule

Starting Wednesday and every following class: Be prepared to give an elevator pitch for your project. Your pitch should be no more than 2 minutes long. You may use visuals as long as you can obtain them by (quickly) entering a URL in a web browser. Your pitch should get across in a convincing and engaging way: (1) the purpose of your project (what problem are you solving), (2) what you are actually doing, and (3) why we should care.

Monday, 23 November (8:29pm): Project Progress Reports. Send an email to ccc-staff@cs.virginia.edu, cc-ing all members of your project team. The email should have a subject line, `Project:` *Title*, with your project title. Its body should contain at least this information:

1. A link to the website for your project (this could be a github page if you want). That site should have a front page that describes your project, lists the team members, and provides more information about your project.
2. A short paragraph explaining how your project has changed since the preliminary proposal email. This should explain if the goals of your project have changed and why.
3. A description of what progress you have made on your project.
4. A description of what you plan to do to complete your project, and your plans for doing this. If you have a multi-person team, this should include an explanation of how your team is working together and who is doing what.
5. (optional) Any questions you have for us.

Notes

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.

$$\begin{aligned} t^d &= (mk^e mod n)^d \mod n \\ &= m^d k^{ed} \mod n \\ &= m^d k \mod n \end{aligned}$$

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?

> *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.* (Before Bitcoin: The Rise and Fall of DigiCash)