University of Virginia **cs4501: Cryptocurrency Cafe** March 16, 2015

Class 16: Alternate Cryptocurrencies

Project Proposals

Project Proposals are due **Thursday, 19 March** (11:59pm). Send your proposal by email to evans@virginia.edu with subject line `Project Proposal`. Your email should contain at least:

1. Title of your Proposal - a short title that should get across what you are doing.
2. Team members list - a list of everyone on your team. You should `cc:` all the team members in the email so I have one email to reply-all to that will reach your full tem.
3. Motivation - explanation of why your project topic is worthwhile.
4. Project Plan - what you plan to do.
5. First deliverable - description of what you will have ready to submit for the first deadline, **Sunday, 5 April** (note that you will be presenting about your project in class on **Wednesday, 1 April**).

If you are looking for teammates for your project, or searching for a project idea, come to my office hours after class today if possible.

Alternate Cryptocurrencies

How can decentralized cryptocurrencies be different from bitcoin?

Variations:

- Economics: deflationary vs. inflationary
- Proof-of-work: possible advantages of other proof-of-work mechanisms
- Consensus mechanism: majority of computing power vs. alternatives
- Scripting language for transactions: simpler vs. more powerful and expressive
- Parameters: speed of blocks, size of transactions

Dogecoin!

What is a *key derivation function*?

Why is SHA-256 is horrible key derivation function today?

Colin Percival, *Stronger Key Derivation via Sequential Memory-Hard Functions*, 2009. presentation slides including XKCD 538.

What is a *memory-hard* algorithm?

Is a memory-hard algorithm better for a cryptocurrency proof-of-work than a compute-intensive one like SHA-256?

Andrew Miller, Ari Juels, Elaine Shi, Bryan Parno, and Jonathan Katz. *Permacoin: Repurposing Bitcoin Work for Data Preservation*. IEEE Security and Privacy ("Oakland") 2014.

Interesting Video If you're still looking for ideas for your project still, this video may give you some good ideas: *What Satoshi Didn't Know*, Gavin Anderson, DevCore Boston 2015. (This talk gets into the history of bitcoin and lots of issues with flaws in its design, and raises some interesting possibilities for future work - e.g., are there ways to use old unspent transactions to solve network problems without spending them?)