CS 168: Blockchain and Cryptocurrencies

Projects and Research Directions

Prof. Tom Austin
San José State University

Project

- 1-2 people (including you)
- Must include implementation
- Open ended
- Interested in extending to thesis/ independent study?
  - See me to discuss options

Possible Projects

- Extend SpartanGold (SG) with features missing from Bitcoin.
- Port SG to different language.
- Take idea from research and implement.

Option: Add BTC Features to SG

- Merkle tree to store transactions
- Variable proof-of-work
- Fixed block size
- Wallet following BIP-32/BIP-39/BIP-44
- Add Bitcoin Script
  - Or something similar

Option: Port SpartanGold

- Re-implement SpartanGold in different language
- Popular languages for blockchain development:
  - Go, backed by Google
  - Rust, backed by Mozilla
- Goal: your client/miner should be able to interact with mine.

Option: Research

- Alternate consensus schemes
  - Proof-of-stake
  - Delegated proof-of-stake
  - *Useful* proof-of-work
  - Proof-of-storage
- Defense mechanisms
  - Non-outsourceable puzzles
  - Better anonymity designs

More research

- Smart contracts
- Increasing blockchain throughput
  - High-performance proof-of-stake
  - Bitcoin-NG
- Blockchain Governance
  - Tezos
- Blockchain-as-operating-system
  - EOS
- Non-Fungible Tokens

Decentralized App (Dapp)

- Writing an Ethereum Dapp is **not** enough by itself.
- If you write a Dapp implementing ideas from a research paper, that could work.

Grades

- We will negotiate a contract.
  - I will define implementation requirements for A, B, or C grade for YOUR project.
- Report required, graded separately from implementation.
- Presentation, also graded.

Paper discussion

Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten.

SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies.

In IEEE Symposium on Security and Privacy, pages 104–121. IEEE Computer Society, 2015.

Why are we reviewing this paper?

- Detailed analysis of cryptocurrency research
  - (as of 2015)
- Great starting point for your projects
- Underestimated some projects:
  - Ethereum (2nd by market cap today)

Organization of paper

1. Sales pitch to researchers
2. Overview of Bitcoin and its ecosystem
3. Bitcoin stability (and attacks)
4. Client-side security
5. Modifying Bitcoin (and altcoins)
6. Alternate consensus
7. Anonymity
8. Extending functionality

Plan for today

- Groups will meet individually to discuss questions
- Answer questions in Canvas **during class**
- We will join back together
- Representative from ONE group will summarize discussion

Discussion Question 1

One important goal of Bitcoin is **decentralization**.

How does Bitcoin attempt to achieve this?

What **challenges** have arisen to this decentralization?

What could be done to address these challenges?

Discussion Question 2

The paper discusses a variety of **attacks** against the network, some (currently) theoretical and some that have been observed in the wild.

What are some of these attacks, and what measures/incentives **defend** against these attacks? What attacks are **not** the actions of a **rational** actor?

Discussion Question 3

What are the problems with Bitcoin's **consensus** mechanism?

What **alternatives** are there? And what are the trade-offs in these designs?

Discussion Question 4

Bitcoin's **anonymity** guarantees are very weak. Why? How could a client's identity be revealed?

How have different altcoins attempted to address these problems?

Discussion Question 5

This paper discusses **uses** for Bitcoin besides financial transactions. What use cases have people found?

What **properties** of the blockchain are people relying on for these use cases?

Discussion Question 6

(You have more time on this question.)

At this point we have gone over many interesting directions that research could go.

What aspects do **you** find most interesting?
Why?