CS 168: Blockchain and Cryptocurrencies

Ethereum Introduction

Prof. Tom Austin
San José State University

Some Brief Ethereum Facts

- Number 2 cryptocurrency by market cap.
  - **Not** why we are studying it
- Core developers
  - Vitalik Buterin (creator)
  - Gavin Wood
- Block 0 mined July 30, 2015

Ethereum Prehistory: Mastercoin

- Protocol layer on top of Bitcoin
- Focused on financial contracts
  - Two-party contracts with enforced terms
- October 2013: Vitalik suggested a more flexible scripting language
  - More limited vision
  - Not Turing-complete

December 2013: Ethereum Proposal

- The name "Ethereum" first appears in print
- Transaction fees for different actions included
  - Computational steps paid for in ether (this concept changed later)
  - Once fees exhausted, processing stops
- *Contracts* became accounts in their own right

More History

- Gavin Wood joins project
  - Designs the Ethereum Virtual Machine (EVM).
  - Writes "The Yellow Paper" in 2014.
- Gas model changes
  - Miners explicitly vote on gas price.
  - Previous approaches allowed them to implicitly do this anyway.

Account Types

- *Externally owned accounts* (EOAs)
  - Equivalent to accounts in Bitcoin
  - Have a private key
- Contract accounts
  - Have contract code
  - No private key
    - Cannot initiate transactions
  - Can react to transactions and call other contracts
  - Contain data

Common Features with Bitcoin

- Digital currency
  - Called *ether* (ETH)
    - **Not** "ethereum"
  - Smallest unit: *wei*
- ~~Proof-of-work blockchain~~
  - ~~Ethash — designed to be ASIC-resistant~~
  - ~~Much quicker: 14-15 second block time~~
  - ~~Plans to move to *proof-of-stake* (Casper)~~
- Peer-to-peer network

Differences from Bitcoin

- Turing-complete virtual machine
  - Almost…
  - Brings up a lot of security issues
- Gas
  - Prevents denial-of-service attacks
  - Transactions specify
    - ETH earmarked for gas
    - gas-rate
- Uses account balances rather than UTXOs
  - Nonces are therefore required for transactions
- Less conservative development culture
  - "Move fast and break things"
  - More frequent *hard-forks*
  - Expect changes
- ***Finally proof-of-stake!***

Lab, Part 1

Create Ethereum MetaMask wallet.

Details in Canvas.

Decentralized Applications (DApps)

- Also referred to as dApps, Dapps, and ĐApps
  - Đ is the Old-English letter 'Eth'
- Written in a smart contract language
  - Solidity is the most prevalent

Review Test Faucet Contract in Remix IDE

(in-class)

Suggested Reading

- The Beige Paper
  - https://github.com/chronaeon/beigepaper/blob/master/beigepaper.pdf
  - Less formal version of the Yellow Paper (https://ethereum.github.io/yellowpaper/paper.pdf)
- *Mastering Ethereum,* by Andreas M. Antonopoulos and Gavin Wood. https://github.com/ethereumbook/ethereumbook
  - Many of the examples from today taken from this book

Lab, Part 2

Write your own Faucet contract.

Details in Canvas.