389C: Bitcoin and Other Cryptocurrencies

The Intersection of Technology and the Economy

Syllabus (topics)

- Syllabus week + Intro to Bitcoin
- Blockchain Structure
- Proof-of-Work and Mining
- Wallets and Transactions
- Anonymity
- Politics and Regulation
- Cryptocurrency Market and ICOs
- Bitcoin as Platform
- Altcoins (focus on Ethereum), Proof-of-Stake
- Ethereum Contracts & Ethereum as a Platform

Syllabus (class structure)

- Lecture
  - Informational, usually covering slides (which will be posted on Piazza)
- Quizzes
  - These will be on in-class slides or readings that we have assigned
- Projects
  - Simplified implementations of cryptocurrency technology
  - Mostly in Java

Syllabus (Exams)

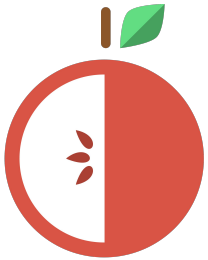
- One midterm
  - High level
  - Concept-based, not code-based
  - Multiple Choice
  - Short Answer
- One final project
  - Ethereum smart contract
  - More details on this later

Syllabus (people)

- Dr. Jonathan Katz
  - jkatz@cs.umd.edu
  - Website
- Cameron Payton
  - cpayton@umd.edu
  - Facebook
- John Kos
  - jkos@terpmail.umd.edu
  - Facebook
- Office Hours TBD
  - Will be announced via Piazza and syllabus modification
- Piazza

Feedback

- We will occasionally solicit feedback from everyone in class
  - Extremely important! Why?
- Google Form



Let’s begin!

What is cryptocurrency?

- “A cryptocurrency is a digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency.” - Wikipedia
- What does this mean?

What is cryptocurrency?

- Uses cryptography
- Controlled creation of coins
- Can be bought and sold for fiat currencies
  - Fiat Currency - any currency issued by a central government (i.e., USD, GBP, EUR, etc.)
- Cannot be held in a physical format
  - Wallets can be physical, coins themselves cannot be
- Can pay for items with them
  - Markets such as South Korea actually accept Bitcoin at retail stores throughout the country
  - Wikipedia accepts bitcoin donations!
  - Subway (yes, **the** Subway), Overstock, Namecheap, Steam, Expedia, and more accept bitcoin!

overstock.com®

Non-slip Rug Pad on Overstock.com invoice ID 201637783.

$28.74 USD
0.00597066 BTC

USE COINBASE WALLET | USE BITCOIN ADDRESS

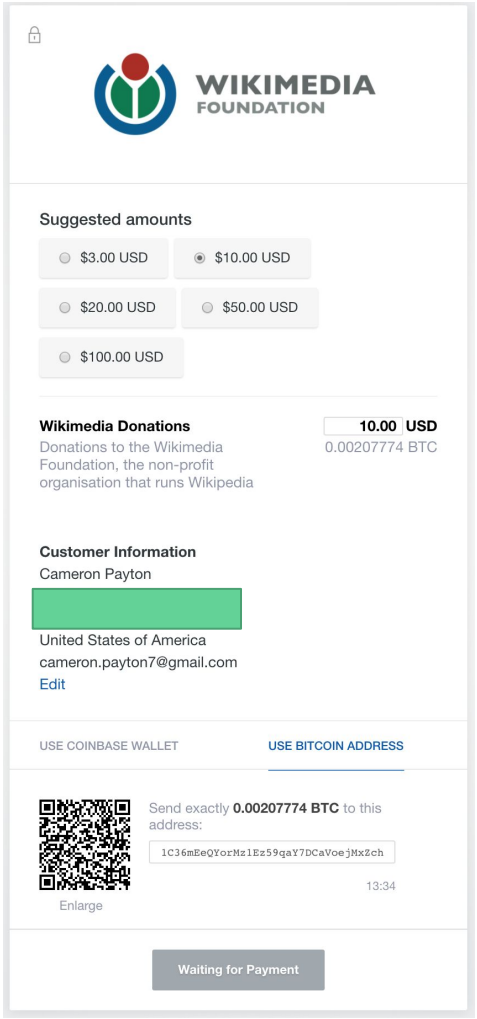
Enlarge

Send exactly **0.00597066 BTC** to this address:

`161rxCJENhR5rqvS1iumumk8r11tVKq7xM`

14:44

Waiting for Payment


WIKIMEDIA
FOUNDATION
Suggested amounts
$3.00 USD
$10.00 USD
$20.00 USD
$50.00 USD
$100.00 USD
Wikimedia Donations
Donations to the Wikimedia Foundation, the non-profit organisation that runs Wikipedia
10.00 USD
0.00207774 BTC
Customer Information
Cameron Payton
United States of America
cameron.payton7@gmail.com
Edit
USE COINBASE WALLET
USE BITCOIN ADDRESS
Send exactly 0.00207774 BTC to this address:
1C36mEeQYorMz1Ez59qaY7DCaVoejMxZch
13:34
Enlarge
Waiting for Payment

How is cryptography used?

- Mathematically complex hash functions (SHA-256, SCRYPT, etc.)
- Gives way to hash-based data structures
  - Keeps coins and transactions secure
  - Prevents fraud and modification
  - Helps with anonymity
- Cryptography is the cornerstone of all cryptocurrency technology (hence the name **crypto**currency)
  - How does the advent of quantum computing affect this?

How is coin creation controlled?

- Decentralization
- Usually (but not always) through some form of mining
  - Bitcoin vs. Ripple
- In turn, this:
  - Prevents counterfeit coins
  - Prevents oversupply
  - (Sort of) controls inflation
- Number of coins created may or may not have an absolute cap
  - Bitcoin has a cap of ~21 million coins

Reading for next week

- Bitcoin Whitepaper
  - Satoshi Nakamoto
  - Can be found on class repo or here
- Satoshi Nakamoto
  - Anonymous person (or possibly group of people) who created bitcoin, the first (and most popular) cryptocurrency
  - Owns ~1 million bitcoin (approx. 5% of all bitcoins)
  - Fun fact: Many people say Satoshi cannot actually cash in on these coins ever (why?)

Summary

- We’ve talked a lot about general cryptocurrency today
- This class will focus mainly on bitcoin
- Towards the end of the semester, we will also cover a few altcoin
    - This will mostly focus on Ethereum

Parting Notes

- Github
- Feedback Form
- Slides can be found at ter.ps/389CFall18w1
- Will post these slides on piazza