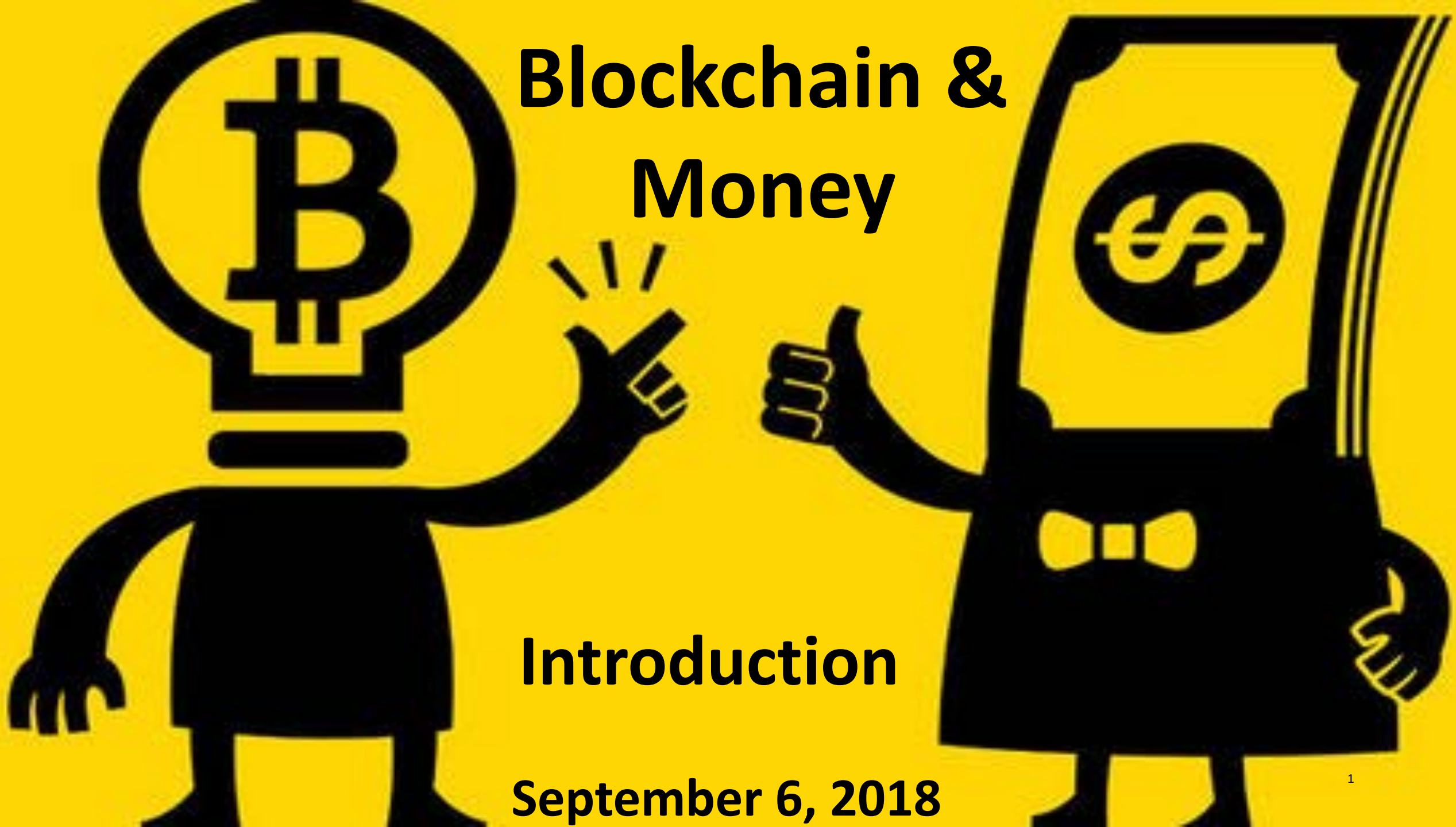
Blockchain & Money



Introduction

September 6, 2018

Intro Class: Study Questions

- What is blockchain technology and why might it be a catalyst for change for the financial sector?

- What you as a student wish to learn from this course, ‘Blockchain and Money’?

Note: This course has been selected by The MIT Golub Center for Finance and Policy for recording.

Intro Class: Readings

- ‘*How blockchain can solve the payments riddle*’ Gensler
- ‘*The blockchain catalyst for change*’ Vox

The Internet: Layers of open protocols

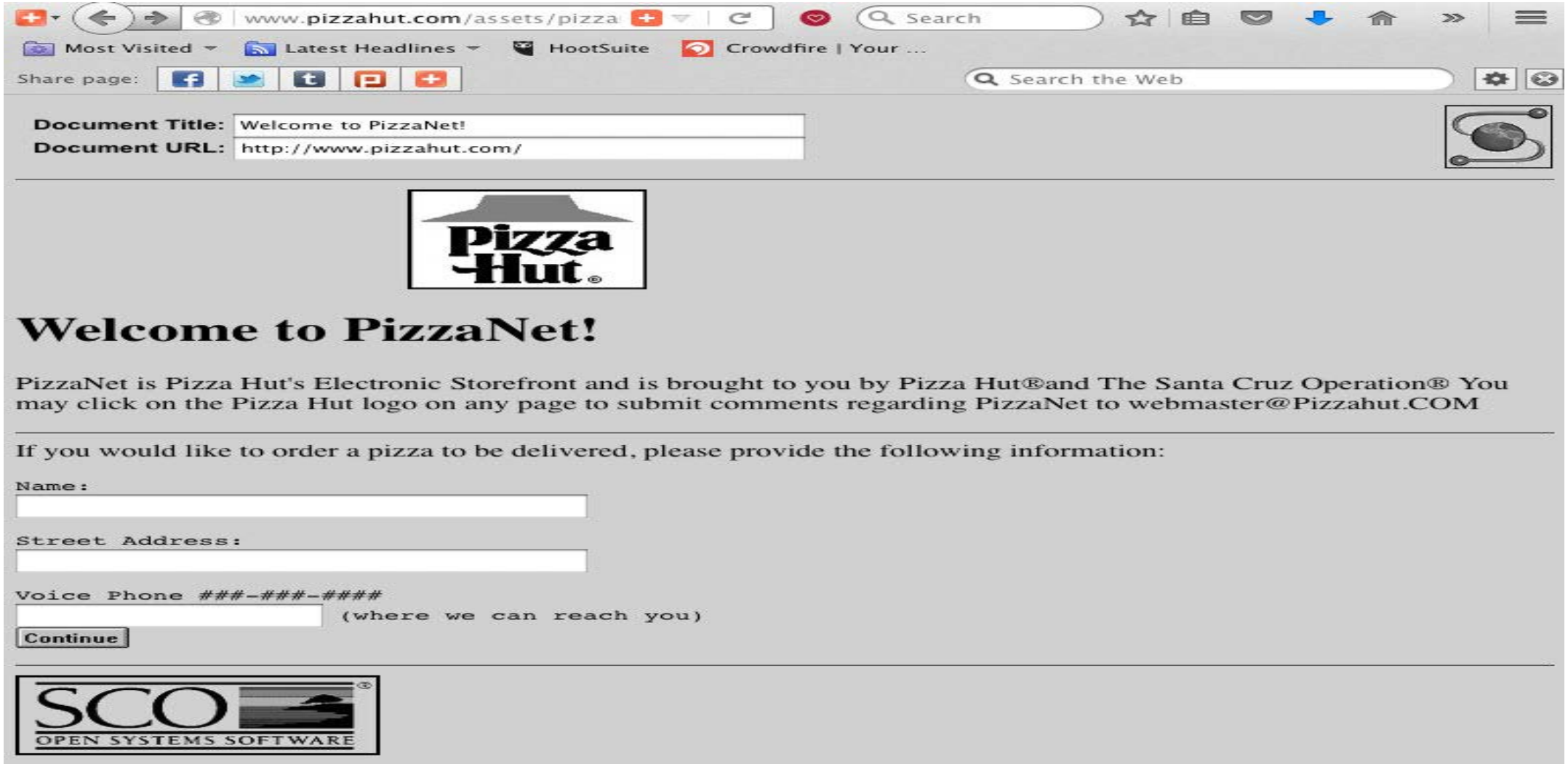
HTTP- 1990

TCP/IP - 1974

Ethernet - 1974

‘*The Net*’ opening scene 1995 Sandra Bullock

First online sale: Pizza Hut in 1994



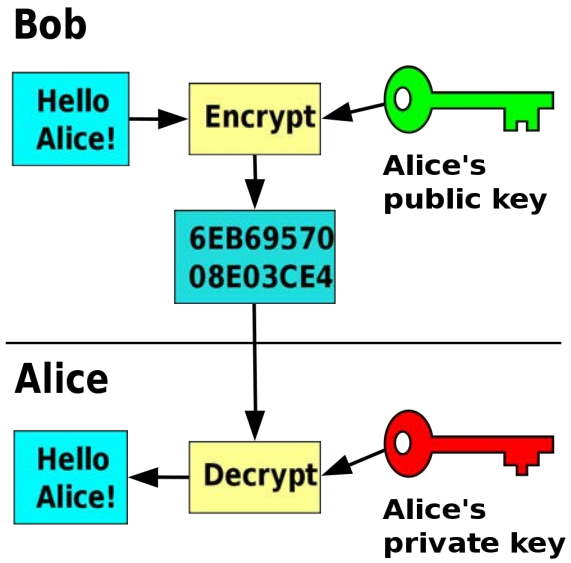
But money changed hands with delivery

Cryptography:

Communications in the presence of adversaries

Scytale Cipher
Ancient Times

Enigma Machine
1920s - WWII



Asymmetric Cryptography
1976 to today

Image by CIA and in the public domain via Wikimedia Commons.

Image is in the public domain via Wikipedia.

Early Cryptographic Digital Currencies Failed

- DigiCash (David Chaum) – 1989
- Mondex (National Westminster Bank) - 1993
- CyberCash (Lynch, Melton, Crocker & Wilson) – 1994

The Internet: Cryptographic protocols

SSL / TLS – 1996

HTTP- 1990

TCP/IP - 1974

Ethernet - 1974

Further Cryptographic Digital Currencies Failed

- DigiCash (David Chaum) – 1989
- Mondex (National Westminster Bank) - 1993
- CyberCash (Lynch, Melton, Crocker & Wilson) – 1994
- E-gold (Gold & Silver Reserve) – 1996
- Hashcash (Adam Back) – 1997
- Bit Gold (Nick Szabo) – 1998
- B-Money (Wei Dai) - 1998
- Lucre (Ben Laurie) – 1999

Digital Payments Innovation, though, Continued

2003

2007

The Riddle Remained

How to move value
peer-to-peer
without any
trusted central intermediary

Bitcoin: A Peer-to-Peer Electronic Cash System

- From: Satoshi Nakamoto <satoshi <at> vistomail.com>
  Subject: Bitcoin P2P e-cash paper
  Newsgroups: gmane.comp.encryption.general
  Date: Friday 31st October 2008 18:10:00 UTC

- “I've been working on a new electronic cash system that's fully peer-to-peer, with no trusted third party.”

A new layer?: Programmable transactions

SSL / TLS - 1996

HTTP- 1990

TCP/IP - 1974

Ethernet - 1974

???

PayPal 1998

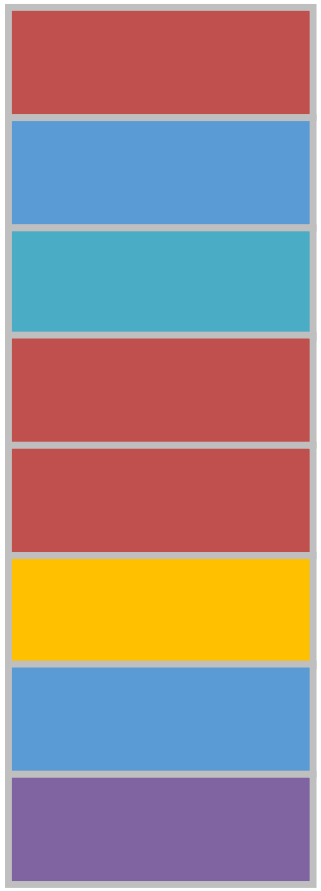
amazon 1995

CISCO 1984

3com 1979

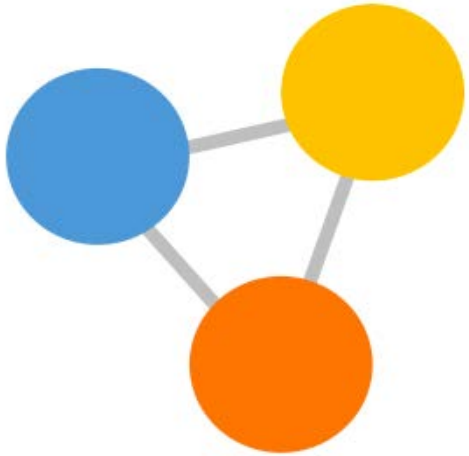
What is a blockchain?

timestamped
append-only log



auditable database

consensus protocol



Secured via cryptography

- Hash functions for **tamper resistance** and **integrity**
- Digital signatures for **consent**
- Consensus for **agreement**

Addresses '**cost of trust**' (Byzantine Generals problem)

- Permissioned
- Permissionless

Pizza for bitcoins?

May 18, 2010, 12:35:20 AM

- “I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but *what I'm aiming for is getting food delivered in exchange for bitcoins* where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

- I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

- If you're interested please let me know and we can work out a deal.

- Thanks,
  Laszlo”

Re: Pizza for bitcoins?

May 21, 2010, 07:06:58 PM

- “So nobody wants to buy me pizza? Is the bitcoin amount I'm offering too low?”

Re: Pizza for bitcoins?

May 22, 2010, 07:17:26 PM

- “I just want to report that I successfully traded 10,000 bitcoins for pizza.

  Pictures: http://heliacal.net/~solar/bitcoin/pizza/

  Thanks jercos!”

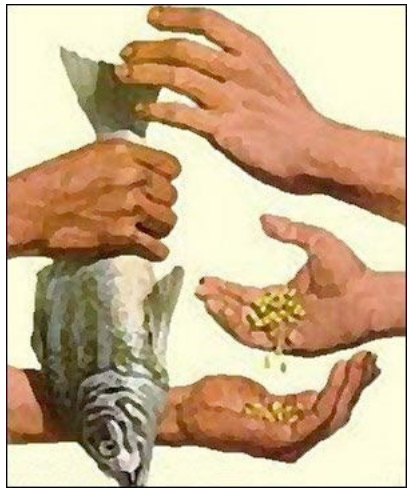
Medium of Exchange: 10,000 Bitcoins for 2 Pizzas

- Value:
  - May 22, 2010 - $41
    - $20.50 per pizza
  - September 5, 2018 - $66 million
    - $33 million per pizza

Blockchain Technology

- Verifiably moves ‘data’ on a decentralized network
- The ‘data’ can represent value or computer code
- Thus it goes directly to the plumbing of the financial sector and money
- Broad adoption rests on addressing technical, commercial and public policy hurdles
- It can be a catalyst for change in the world of finance and money

What is the Role of Money?



Medium of Exchange

Store of Value

Unit of Account

What is the Role of Finance?

Moving, Allocating & Pricing:

Money

Risk

Throughout the Economy

Financial Sector Challenges => Blockchain Potential Opportunities

- Repeated crises and instability
- Fiat currency instabilities associated with unsound policies
- Centralized intermediaries' concentrate risks & economic rents
- Central Bank legacy payment systems
- Clearing & settlement costs & counterparty risks
- Financial inclusion

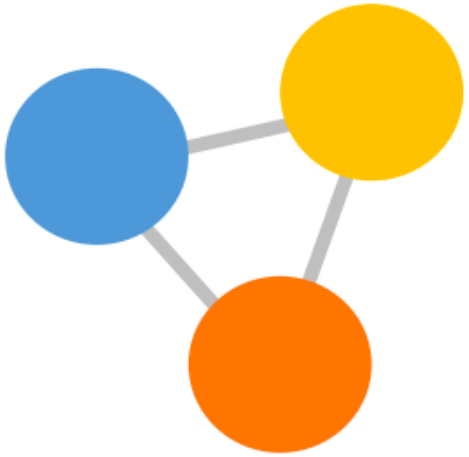
- Payment system costs: **½ - 1 %** of Global GDP
- Financial sector costs: **7 ½ %** of U.S. GDP

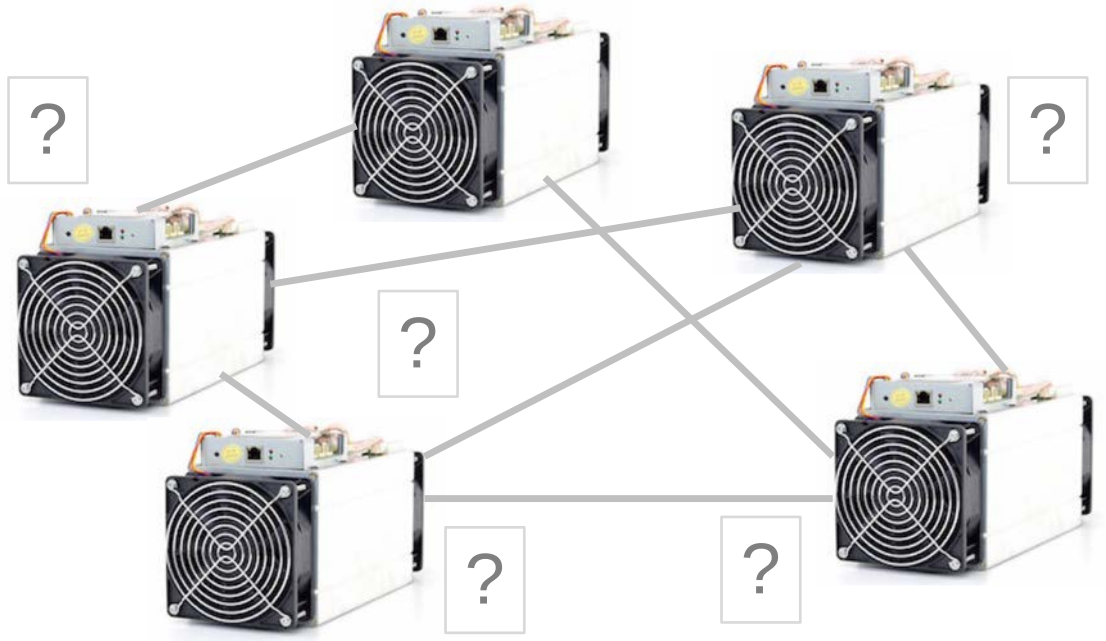
Financial Sector Issues with Blockchain Technology

- Performance, Scalability, & Efficiency
- Privacy & Security
- Interoperability
- Governance
- Commercial Use Cases
- Public Policy & Legal Frameworks

Financial Sector Favors

permissioned blockchains vs. permissionless blockchains

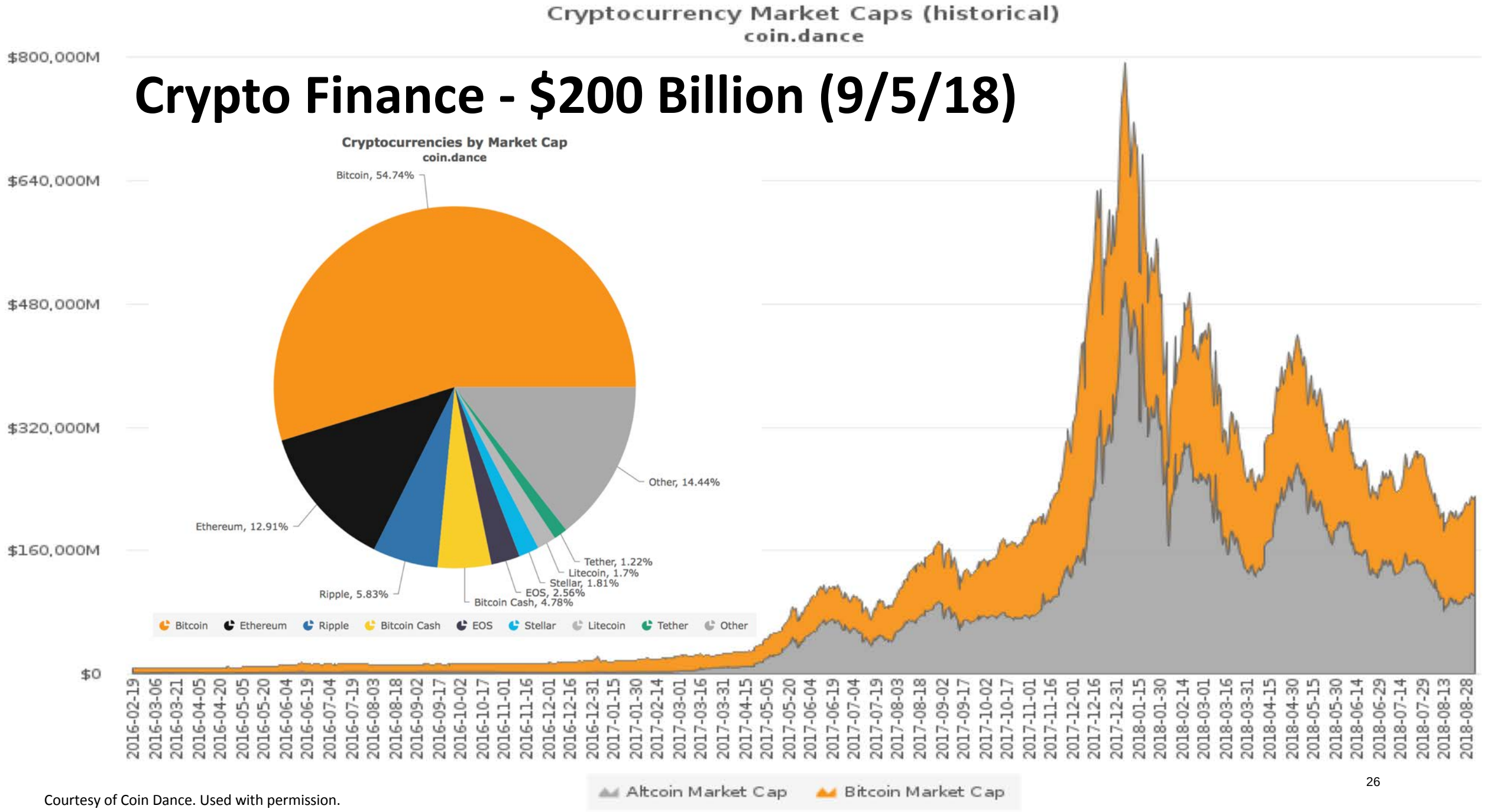




- Known set of participants
- No proof-of-work or mining
- No need for a native currency
- Distributed database technology

- Unknown participants
- Security based on incentives;
- Native currency
- Crypto-economics

Crypto Finance - $200 Billion (9/5/18)



Courtesy of Coin Dance. Used with permission.

Yet Modest in Relation to Global Capital Markets

- Global Equity Markets:
    - $80 Trillion
- Global Debt & Bond Markets:
    - $250 Trillion
- Global Holdings of Gold:
    - $7 Trillion

Public Policy Framework

- Guarding against Illicit Activity

- Financial Stability

- Protecting the Investing Public

The Duck Test

“When I see a bird that walks like a duck and swims like a duck and quacks like a duck, I call that bird a duck.”

James Whitcomb Riley, poet

Incumbents Eying Crypto Finance

- Crypto's market cap, trading volume, volatility and spreads are drawing attention
- So has Coinbase's 20 million accounts, about as many as Fidelity Investments, twice Charles Schwab and nearly as many as Vanguard
- Startups more willing to beg for forgiveness while incumbents often need ask for permission
- Incumbents interested to serve customer interest; gain a share of profits; & protect their franchises
  - Exchanges – CME; Eurex; Intercontinental Exchange; Nasdaq
  - Asset Managers – Fidelity
  - Investment Banks – Goldman Sachs

Financial Sector Potential Use Cases

- **Payment Systems -** Cross border, Large interbank, & Retail
- **Central Bank Digital Currency & Private Sector Stable Value Tokens**
- **Secondary Market Trading** – Crypto-exchanges & custody
- **Venture Capital -** Crowdfunding through Initial Coin Offerings
- **Clearing, Settlement and Processing –** Securities & Derivatives
- **Trade Finance & Supply Chain -** Digitizing paper-based processes
- **Digital IDs and Data Reporting**

Blockchain & Money 15.S12

- For those wishing to explore:
  - Blockchain technology fundamentals
  - Blockchain technology economics &
  - Potential use to change the world of money and finance
- For those who wish to gain critical reasoning skills:
  - Understanding the ‘ground truths’ of blockchain technology &
  - Separate rigorous analysis from mere assertion and hype

Four Forces – Larry Lessig
‘Code and Other Laws of Cyberspace’

- **Code/architecture** – physical or technical constraints
- **Market** – economic forces
- **Law** – explicit mandates by government
- **Norms** – social conventions

We will Explore a Range of Perspectives

MINIMALIST → → → MAXIMALIST

Bitcoin Minimalist

Smart Contract Minimalist

Blockchain Minimalist

Bitcoin Maximalist

Smart Contract Maximalist

Blockchain Maximalist

But Anchor  our Discussion in the Middle

Requirements

- Class Participation 30%
- Two Individual Write-ups (15% x 2) 30%
- Group Research Paper 40%

Act 1: Blockchain & Money Fundamentals

- Class 2 (9/11): Money, Ledgers & Bitcoin
- Class 3 (9/13): Blockchain Basics & Cryptography
- Class 4 (9/18): Blockchain Basics & Consensus
- Class 5 (9/20): Blockchain Basics & Transactions, UTXO and Script Code
- Class 6 (9/25): Smart Contracts & DApps
- Class 7 (9/27): Technical Challenges
- Class 8 (10/2): Public Policy
- Class 9 (10/4): Permissioned Systems
- Class 10 (10/11): Financial System Challenges & Opportunities

Act 2: Blockchain & Use Case Economics

- Class 11 (10/16): Blockchain Economics
- Class 12 (10/18): Assessing Use Cases

Act 3: Financial Sector Use Cases

- Class 13 & 14 (10/30 & 11/1): Payments
- Class 15 & 16 (11/6 & 8): Central Banks & Commercial Banking
- Class 17 (11/13): Secondary Markets & Crypto-Exchanges
- Class 18 (11/15): A New Approach to Crypto-Exchanges & Payments
- Class 19 (11/20): Primary Markets, ICOs & Venture Capital
- Class 20 (11/27): Primary Markets, ICOs & Venture Capital
- Class 21 (11/29): Post Trade Clearing, Settlement & Processing
- Class 22 (12/4): Trade Finance & Supply Chain
- Class 23 (12/6): Digital ID

Further MIT Blockchain Opportunities

- Blockchain Seminar – Tuesday nights (5:30 – 7 pm)
  - Michelle Fiorenza

- Digital Currency Initiative – Working Groups & Projects

- Applied Blockchain (1.125) – Tuesday/Thursday (2:30 – 4 pm)

Class 2 (9/11): Study Questions

- What do the roles and characteristics of money mean historically and in today's digital economy?

- What is fiat currency, what are its ledgers and how it fits within the history of money?

- How does Bitcoin fit within the history of money, the emergence of the Internet and failed attempts of cryptographic payment systems?

Class 2 (9/11): Readings

- *'Conflict reigns over the history and origins of money'* Science News
- '*A Brief History of M*oney' IEEE Spectrum
- '*What is Money? An Artist's Make and Take*' Wall Street Journal video
- '*A Brief History of Ledgers*' LLFOURN, Medium
- '*Bitcoin and Cryptocurrency Technologies, Preface — The Long Road to Bitcoin*' Clark (pages 3 – 21)
- '*Bitcoin P2P e-cash paper*' Nakamoto (cover e-mail only)

Conclusions: Class 24 (12/11)

- Blockchain technology provides P2P alternative &
  address 'costs of trust'
- Financial sector has had challenges of resilience, costs and inclusion
- Fiat currency has had challenges & instabilities as well

- We already live in an electronic currency age
- Money is but a social & economic consensus

- Blockchain technology - along with crypto finance - can be a catalyst for change
- Though much that masquerades as fact is but mere assertion
- Broad adoption rests on addressing technical and commercial challenges
- Public confidence is built upon coming within public policy norms

- Now let's challenge each other, learn a lot and together explore Blockchain & Money
  (and have a bit of fun along the way)

15.S12 Blockchain and Money
Fall 2018