

Blockchain & Money



Class 6

September 25, 2018

Class 6 Overview

- Review of Course Projects
- Smart Contracts
- Blockchain Design with Smart Contracts
- DApps and Token Sales
- Legal Issues of Smart Contracts
- Conclusions

Requirements

- Class Participation 30%
- Two Individual Write-ups (15% x 2) 30%
 - Critical Business Reasoning about Class Topic
 - Due prior to Class: 1st by 10th Class; 2nd by 23rd Class
- Group Research Paper 40%
 - Serious effort on Use Case
 - Organize Groups (3 or 4) by 8th Class (10/2)
 - Choose area for Use Cases by 12th Class (10/18)
 - Topics outside of Finance with pre-approval

Class 6 (9/25): Study Questions

- What are smart contracts? How do they compare to traditional contracts? What are tokens?
- What are smart contract platforms such as Ethereum? What generally distinguishes them from Bitcoin?
- What are decentralized applications (DApps)? What has been the usage and why haven't any DApps yet received wide consumer adoption?

Class 6 (9/25): Readings

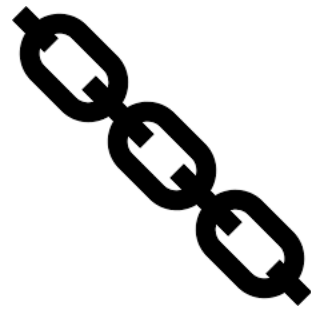
Required

- *'Smart Contracts: 12 Use Cases for Business & Beyond'* Chamber of Digital Commerce
- *'State of the Dapps: 5 Observations from Usage Data'* McCann
- *'Ethereum Competitors: Guide to the Alternative Smart Contract Platforms'* Blockonomi

Optional

- *'Smart Contracts: Building Blocks for Digital Markets'* Szabo
- *'A Next-Generation Smart Contract and Decentralized Application Platform'* Ethereum
- *'Blockchain Technology as a Regulatory Technology'* De Filippi & Hassan

Smart Contracts



- “A set of promises,
- specified in digital form,
- including protocols
- within which the parties perform on these promises.”

Nick Szabo, 1996

However

- Smart Contracts may not be **‘Smart’**
- Smart Contracts may not be **‘Contracts’**

Bitcoin – Technical Features

Ethereum?

- Cryptography & Timestamped Logs

- Cryptographic Hash Functions
- Timestamped Append-only Logs (Blocks)
- Block Headers & Merkle Trees
- Asymmetric Cryptography & Digital Signatures
- Addresses

Yes



- Decentralized Network Consensus

- Proof of Work
- Native Currency
- Network

Yes



- Transaction Script & UTXO

- Transaction Inputs & Outputs
- Unspent Transaction Output (UTXO) set
- Script language




No





State Transitions
Account Based
7 languages

Bitcoin vs Ethereum Design

- | | |
|------------------------------|---|
| • Founder: Satoshi Nakamoto | Vatalik Buterin |
| • Genesis: January 2009 | July 2015 |
| • Code: Non Turing (Script) | Turing Complete (Solidity, Serpent, LLL or Mutan) |
| • Ledger: UTXO – Transaction | State - Account Based |
| • Merkle Trees: Transactions | Transactions, State, Storage, Receipts (w/nonces) |
| • Block Time: 10 minutes | 14 seconds |
| • Consensus: Proof of Work | Proof of Work |
| • Hash Function: SHA 256 | Ethash |

Bitcoin vs Ethereum Design

- Currency: Bitcoin  ETH
- Mining: ASIC  GPU
- Hashrate: 54 Exahash/S  260 Terahash/S

- Pre-sale: None  ICO & prerelease of 72 m ETH
- Rewards: 12.5 BTC/block  3 ETH/block
- Monetary Policy: 1/2s every 210,000 blocks (4 yrs)  Fixed, but changes by updates (was 5/block; proposal to 2)
- Fees: Voluntary  Needed & market based

Smart Contract Platforms

- Ethereum (2015) - \$22 b current market value
- EOS (2018) - \$5 b – completed \$4.2 b year long ICO in July
- NEO (2016) – \$1.1 b - China; delegated BFT; supports wider range of code
- Ethereum Classic (2016) – \$1.1 b - Created from the ‘DAO’ hard fork
- LISK (2016) – \$360 m - code in Java; uses side chains
- Stratis (2017) - \$150 m

Smart Contract Potential Use Cases





















Digital Chamber of Commerce (12/16)

- Digital Identity
 - Securities
 - Derivatives
 - Mortgages
 - Supply Chain
 - Clinical Trials
- Records
 - Trade Finance
 - Financial Data
 - Land Title
 - Auto Insurance
 - Cancer Research

Decentralized Applications (dApps)

- Applications run on a Decentralized Blockchain Network
- Generally have a Native Token & Run as a Smart Contract on top of a Platform

Rankings by Popular Categories [View all >](#)

Games >	Users (24hr)	Gambling >	Users (24hr)	Exchanges >	Users (24hr)	Finance >	Users (24hr)
 CryptoKitties	410	 333 ETH	1,588	 IDEX	1,428	 OmiseGO	373
 Etheremon	313	 Fomo3D	1,251	 ForkDelta	825	 Simple Token	44
 Blockchain Cuties	254	 PoWH 3D	591	 Bancor	315	 minereum	24
 My Crypto Heroes	185	 Infiniti Money	274	 Etheremon	313	 WINGS DAO	19
 Gods Unchained	150	 FREECELL	205	 localethereum	185	 Accelerator	19

© State of the DApps. All rights reserved. This content is excluded from our Creative Commons license. For more information, see <https://ocw.mit.edu/help/faq-fair-use/>

Initial Coin Offerings – Crowdfunding for Investment & Consumption

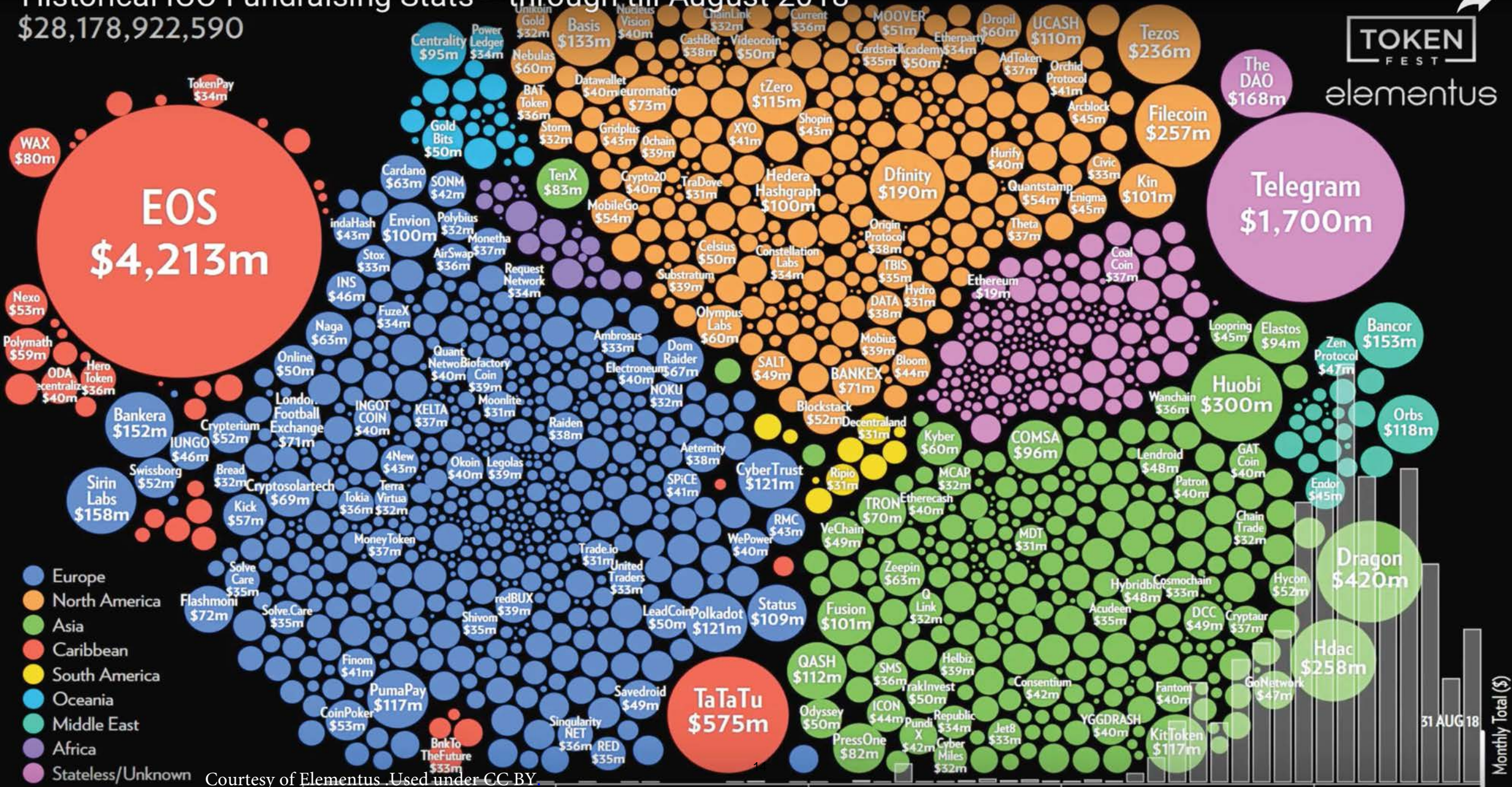
- Proceeds used to build networks
- Tokens usually issued prior to being functional
- Development, while open source, is largely centralized
- Promoters allocate themselves ‘premined’ tokens
- Tokens are fungible & transferable
- Scarcity is fostered with preset ‘Monetary policy’
- Purchasers anticipate profits through appreciation

Historical ICO Fundraising Stats -- through till August 2018

\$28,178,922,590



elementus



Courtesy of Elementus. Used under CC BY.

Monthly Total (\$)

31 AUG 18

Legal Issues – Smart Contracts

Guest Lecturer – Larry Lessig



- Harvard Professor of Law and Leadership
- Founder of Stanford Law’s Center for Internet and Society
- Clerked for Justice Antonin Scalia and for Appeals Court Judge Richard Posner
- Numerous Awards, including Free Software Foundation’s Freedom Award, Fastcase 50 Award and named one of Scientific American’s Top 50 Visionaries
- Author of 8 books, including:
 - **‘Code and Other Laws of Cyberspace’**
 - **Code/architecture** – physical or technical constraints
 - **Market** – economic forces
 - **Law** – explicit mandates by government
 - **Norms** – social conventions

Class 7 (9/27): Study Questions

- How critical are the technical and commercial challenges – scalability, efficiency, privacy, security, interoperability – of current blockchain technology?
- What are the possible tradeoffs of decentralization, scalability and security? What are tradeoffs of consensus software updates, governance and so-called ‘hard forks’?
- What might current work – Layer 2 applications, zero-knowledge proofs, alternative consensus algorithms – do to address current commercial challenges?

Class 7 (9/27): Readings

Required

- *'Geneva Report'* Chapter 2 (pages 9 – 16); Casey, Crane, Gensler, Johnson, and Narula
- *'On the Scalability of Blockchains'* The Control
- *'Transaction Speeds: How do Cryptocurrencies Speeds Stack up to Visa or PayPal?'*
How Much.net
- *'Layer 2 / the Lightning Network'* Digital Currency Initiative
- *'Top 8 Privacy Coins'* Invest in Blockchain

Optional

- *'On Sharding Blockchains'* Ethereum Wiki
- *'zkLedger: Privacy-Preserving Auditing for Distributed Ledgers'* Narula, Vasquez & Virza

Conclusions

- Nakamoto's P2P Money →
Buterin's Ethereum P2P Computing
- Smart Contracts & DApps Provide:
 - Decentralized Computing &
 - Self Executing Commitments
- Token Sales for Proposed DApps have Spawned new form of Crowdfunding – Initial Coin Offerings (ICOs)
- Amongst 1000's of Proposals & Offerings, Few DApps have yet Gained Wide Consumer Adoption
- Smart Contracts and DApps, though, have real Potential to bring Change



MIT OpenCourseWare
<https://ocw.mit.edu/>

15.S12 Blockchain and Money
Fall 2018

For information about citing these materials or our Terms of Use, visit: <https://ocw.mit.edu/terms>.