BLOCKCHAIN AT BERKELEY

BITCOIN TO BLOCKCHAIN HISTORY

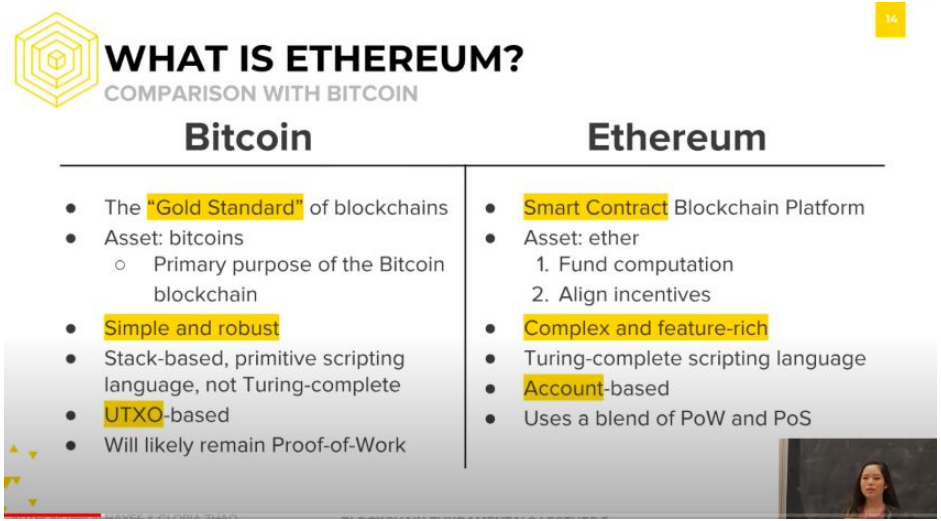
FROM CYPHERPUNKS TO JP MORGAN CHASE

DARYA KAVIANI
ERIKA BADALYAN

REMINDERS FOR FUTURE LECTURERS

Ethereum does not use a blend of PoS and PoW. Rather, Ethereum is still on PoW. However, Ethereum 2.0 uses PoS

Please disregard previous lecture slides that state Ethereum is a blend of PoS and PoW



Also fact check fact check! If you don't know the answer to a question just don't answer the question and pretend that question does not exist...or let someone else answer it

Table of Contents

PRE-BITCOIN: LIBERTARIAN DREAMS

Pre-Bitcoin: Libertarian Dreams

Obstruction of Privacy as Means of Oppression

1917 - during WWI the DOJ creates a special “N**** Subversion” section devoted to spying on Black Americans

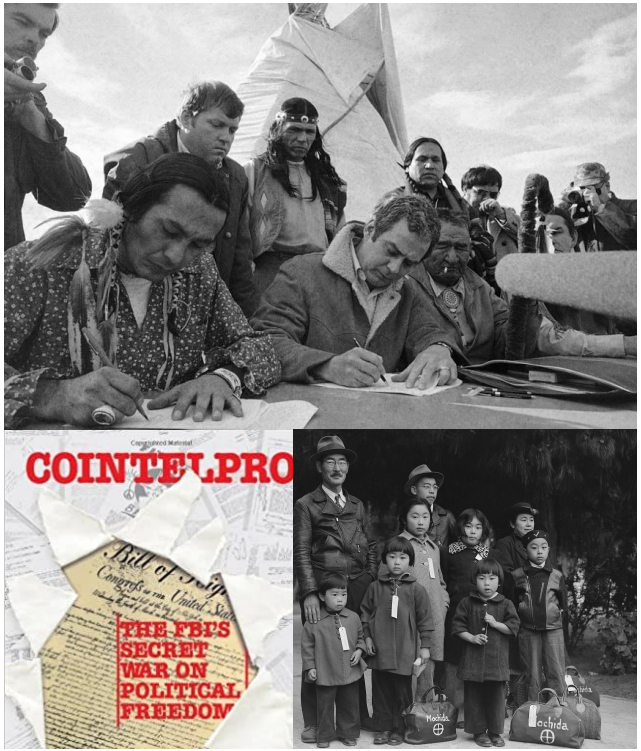
1942 - during WWII, the FBI gathers info on enemy aliens leading to the internment of 110,000 Japanese Americans

1956 - The FBI begins COINTELPRO to disrupt and discredit black civil rights groups leading to the assassination or imprisonment of key leaders

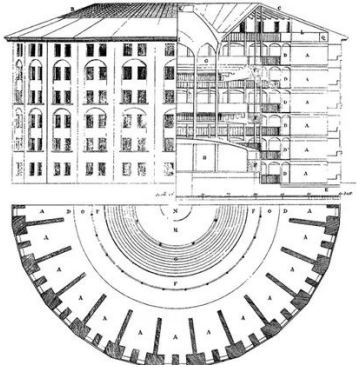
1961 - The FBI targets 12 leaders of the Puerto Rican independence movement for surveillance

1973 - After years of surveilling the American Indian Movement, the FBI sends 200 heavily armed agents to stop the protest at Wounded Knee.

1985 - Of the 33,120 pages of information on 600 Muslim entities in the U.S. by FBI’s Operation Vulgar, there have been no convictions.



Michel Foucault's Panopticon

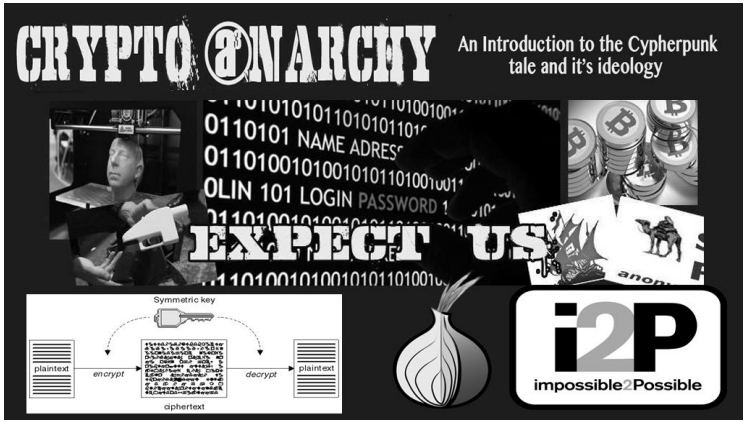


The Panopticon is constructed such that "the prisoner is seen without ever seeing and that the guards see everything without ever being seen." As a result of constantly being watched, prisoners "change their own behavior—their paranoia becomes as effective a tool of control as actual surveillance. They become silent, docile, alienated."

Quotes from Assia Boundoui's "The Feeling of Being Watched"

Cypherpunks and Crypto Anarchists

- **Cypherpunks and Crypto-anarchists**: libertarian groups concerned with privacy, and advocated cryptography as an important tool
- *"**Privacy** is the power to selectively reveal oneself to the world."*
- *"**Privacy** in an open society requires anonymous transaction systems."*



Cypherpunks and Crypto Anarchists

"Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

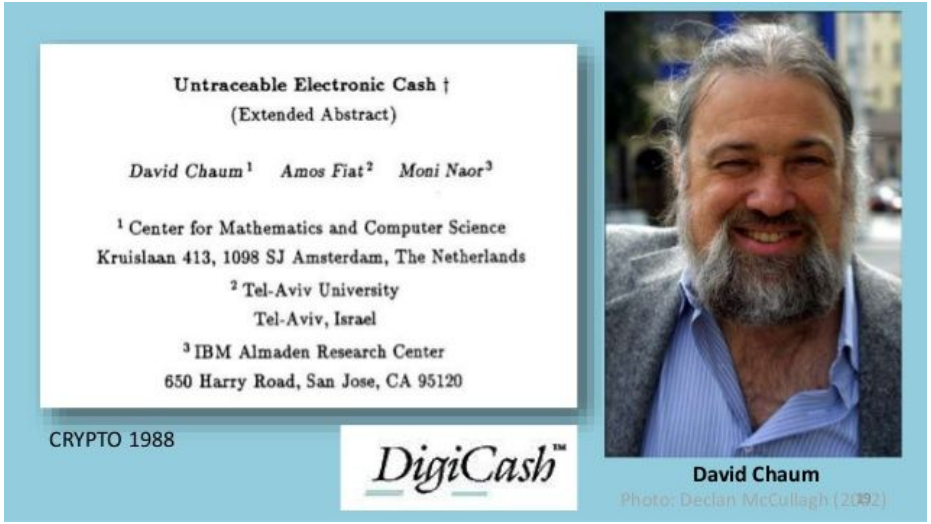
- *A Cypherpunk Manifesto (Eric Hughes, 90s)*

https://www.activism.net/cypherpunk/manifesto.html

Early Attempts at Cryptocurrency: **DigiCash**

DigiCash: "Blind signatures" public key cryptography

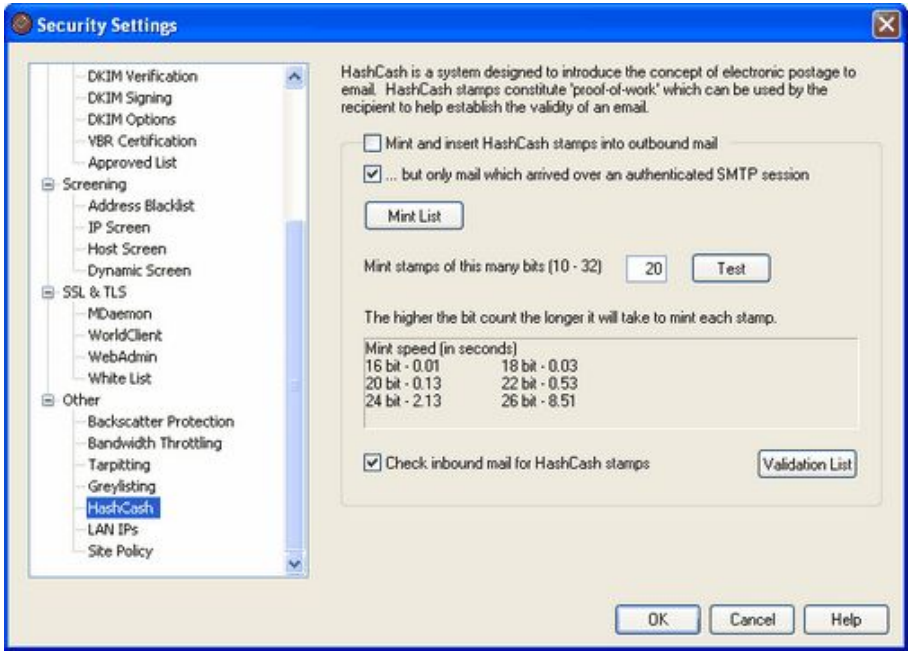
- David Chaum's company
- Allowed users to sign off on transactions without revealing anything about their identity
- Failed due to centralization



Early Attempts at Cryptocurrency: **HashCash**

HashCash: Coins are minted by expending resources instead of by a central bank

- Solve puzzle using a cryptographic hash function
- Originally designed as a mechanism to limit email spam



Early Attempts at Cryptocurrency: **B-Money**

B-MONEY: Introduced two protocols

- Practical way to enforce contractual agreements between anonymous actors
- Protocol in which every participant maintains an individual database of how much money belongs to each user

Satoshi Nakamoto

Anonymous creator of Bitcoin whitepaper: “electronic payment system based on cryptographic proof instead of trust.”

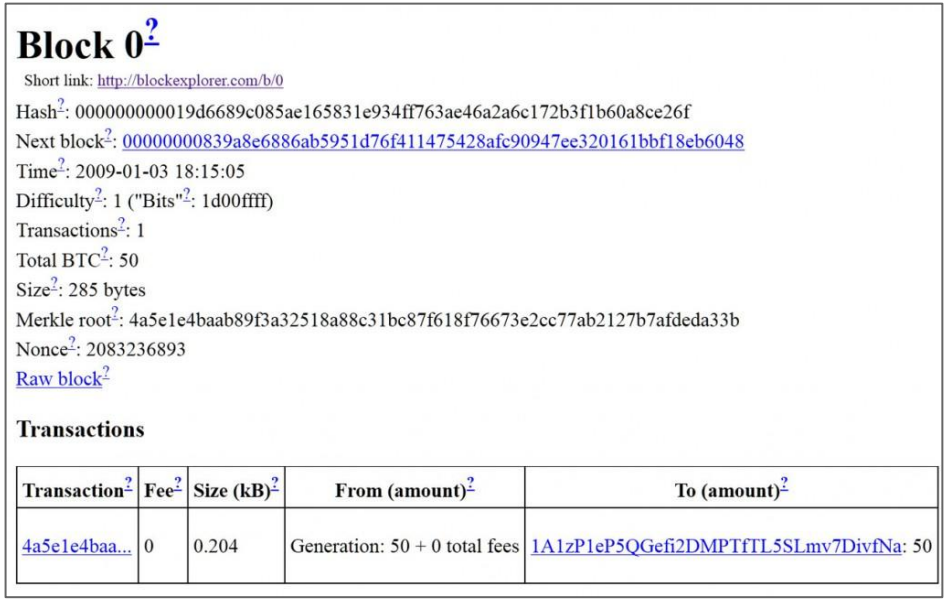
Bitcoin Whitepaper

2008 Launch

Proof of Work

Bitcoin: The First Cryptocurrency

- Genesis block mined January 3, 2009
- Coinbase of the genesis block references a story in *Times of London* involving the Chancellor bailing out banks - Bitcoin's libertarian roots
- First bitcoin transaction on Jan 12, 2009 with Hal Finney



Block 0

Short link: http://blockexplorer.com/b/0

Hash: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block: 00000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048

Time: 2009-01-03 18:15:05

Difficulty: 1 ("Bits": 1d00ffff)

Transactions: 1

Total BTC: 50

Size: 285 bytes

Merkle root: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

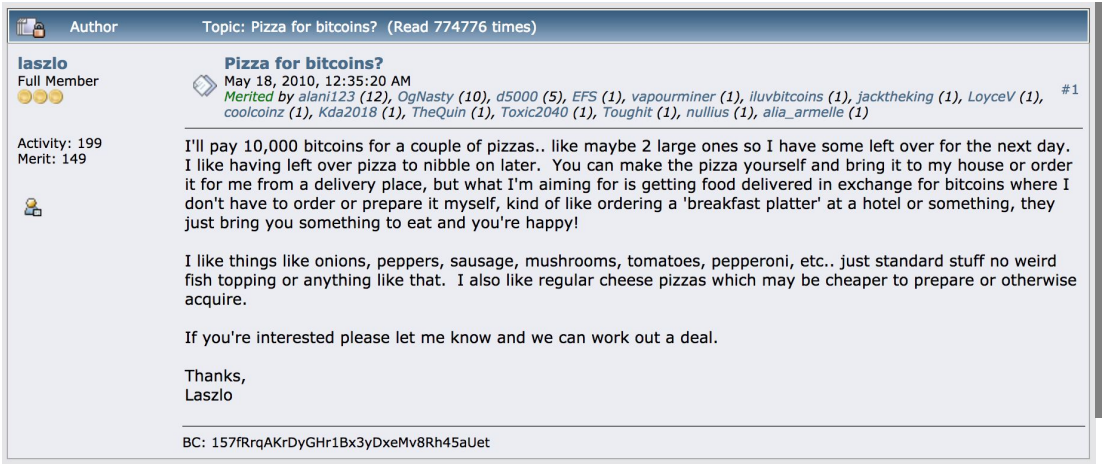
Nonce: 2083236893

Raw block

Transactions

Transaction	Fee	Size (kB)	From (amount)	To (amount)
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa: 50

Bitcoin Gains Value: Pizza Party



Author | Topic: Pizza for bitcoins? (Read 774776 times)

laszlo
Full Member

Activity: 199
Merit: 149

Pizza for bitcoins?
May 18, 2010, 12:35:20 AM #1
Merited by alani123 (12), OgNasty (10), d5000 (5), EFS (1), vapourminer (1), iluvbitcoins (1), jacktheking (1), LoyceV (1), coolcoinz (1), Kda2018 (1), TheQuin (1), Toxic2040 (1), Toughit (1), nullius (1), alia_armelle (1)

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

BC: 157fRrqAKrDyGHr1Bx3yDxeMv8Rh45aUet

5184x3456 (1/60) f/5.6 f(35)=78mm (flash) 2010-05-22 15:01:08 -0400
Download: IMG_0984.jpg

5184x3456 (1/60) f/5.6 f(35)=78mm (flash) 2010-05-22 15:01:22 -0400
Download: IMG_0985.jpg

5184x3456 (1/60) f/5.6 f(35)=78mm (flash) 2010-05-22 15:01:29 -0400
Download: IMG_0986.jpg

5184x3456 (1/60) f/5.6 f(35)=78mm (flash) 2010-05-22 15:01:56 -0400

5184x3456 (1/60) f/5.6 f(35)=78mm (flash) 2010-05-22 15:02:07 -0400

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!

https://bitcointalk.org/index.php?topic=137.0

- May 22, 2010, **Laszlo Hanyecz** purchased $25 worth of pizza for 10,000 BTC
- Fun fact: 10,000 BTC is now equivalent to ~$100,000,000
- World's first ever Bitcoin transaction for a tangible asset
- Bitcoin went from worthless internet money to something with real value

QUESTIONS?

EARLY BITCOIN: SCANDALS, HACKS, ILLEGAL ACTIVITY

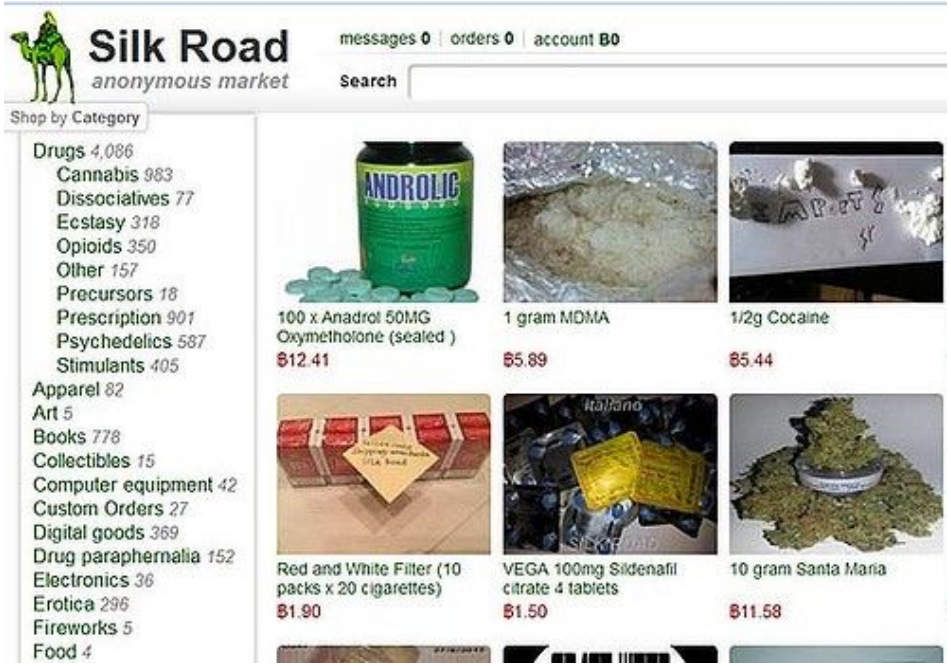
Bitcoin Theft

- 2010: **Jed McCaleb** creates Mt. Gox, the biggest online bitcoin exchange
- 2011: Mt. Gox suffers a significant breach of security that resulted in fraudulent trading
- 2014: Mt. Gox is handling 70% of transactions across the entire internet
- 2014: Mt. Gox loses 744,408 bitcoins in a theft that went unnoticed for years; Mt. Gox declares bankruptcy

Mt. Gox July 2010 - Feb 2014

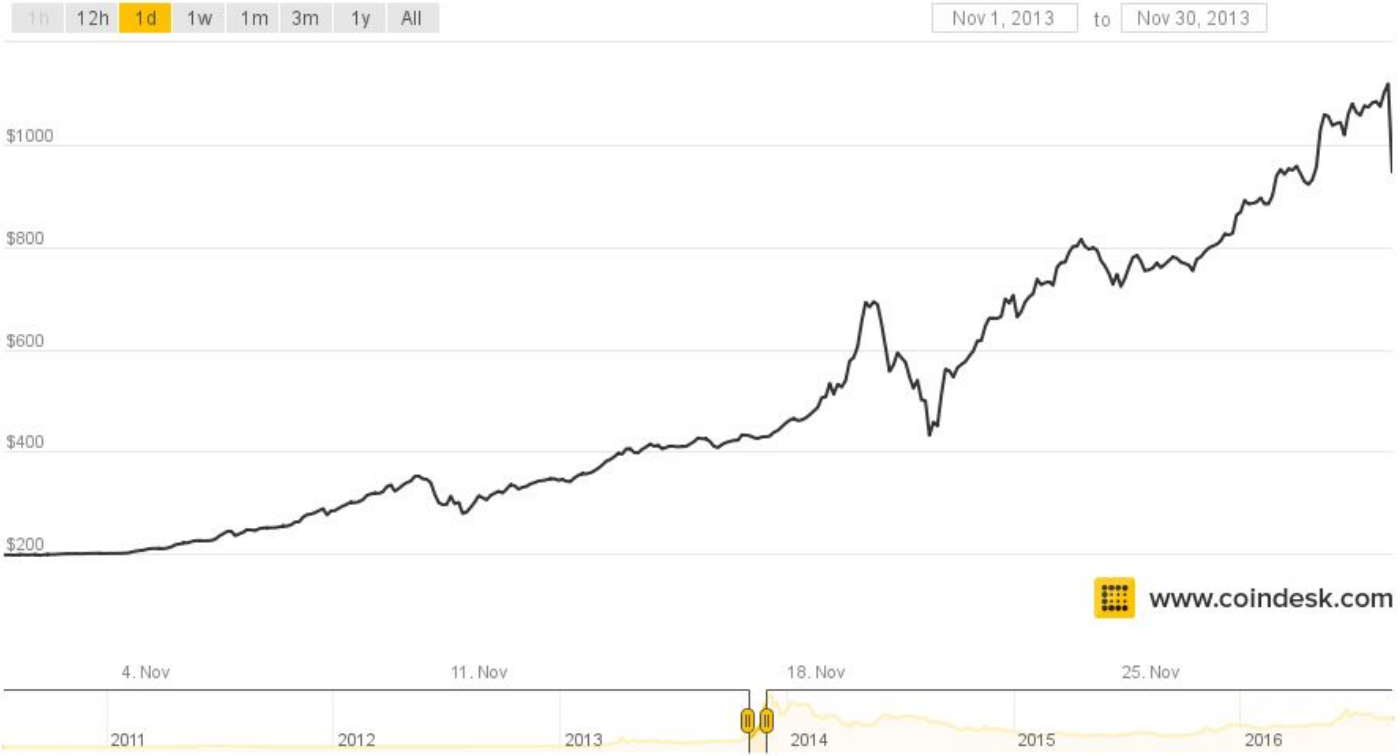
Bitcoin Drug Scandal

- Feb 2011: **Silk Road** opens as the anonymous “eBay of Drugs”, using **Tor** and **Bitcoin**
- Drugs and illegal market goods become the use case for Bitcoin
- Oct 2013: the FBI shut down Silk Road, seizing $3.5m in bitcoin
- **Ross Ulbricht** “Dread Pirate Roberts” is serving a life sentence



Silk Road Feb 2011 — Oct 2013

Bitcoin Bubble



Bitcoin Headlines

2014 Headlines

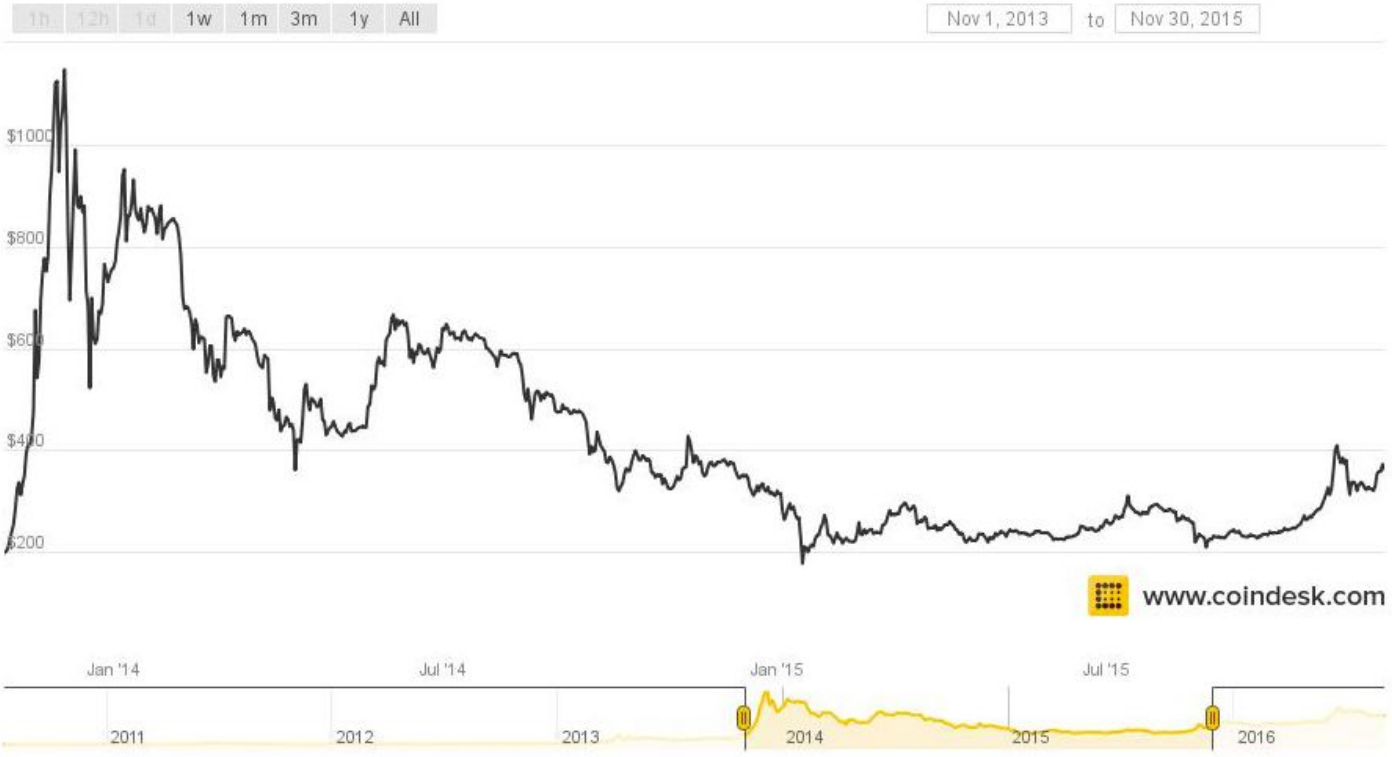
- February 2014: Mt. Gox Allegedly Loses $350 Million in Bitcoin (744,400 BTC)
- March 2014: Bitcoin Inventor Satoshi Nakamoto 'Found' in California
- 2014 Sep. Tim Draper: Bitcoin's Price Still Headed to $10k

Merchant Acceptance

- 2014 Jan. Porn.com accepts Bitcoin
- 2014 Jan. Overstock.com Becomes First Major Retailer to Accept Bitcoins
- 2014 Apr. New Colorado Marijuana Vending Machines Will Accept Bitcoin
- 2014 Sep. PayPal partners with and Coinbase, BitPay
- (2014 Oct.) "Whoever said that bitcoin couldn't buy you things? ... Shitexpress is a service that mails a tupperware container of horse manure with a personalised message on your behalf." - CoinDesk

Bitcoin Startups

...And Burst


1h 12h 1d 1w 1m 3m 1y All
Nov 1, 2013 to Nov 30, 2015
$1000
$800
$600
$400
$200
www.coindesk.com
Jan '14
Jul '14
Jan '15
Jul '15
2011
2012
2013
2014
2015
2016

QUESTIONS?

THE RISE OF ETHEREUM

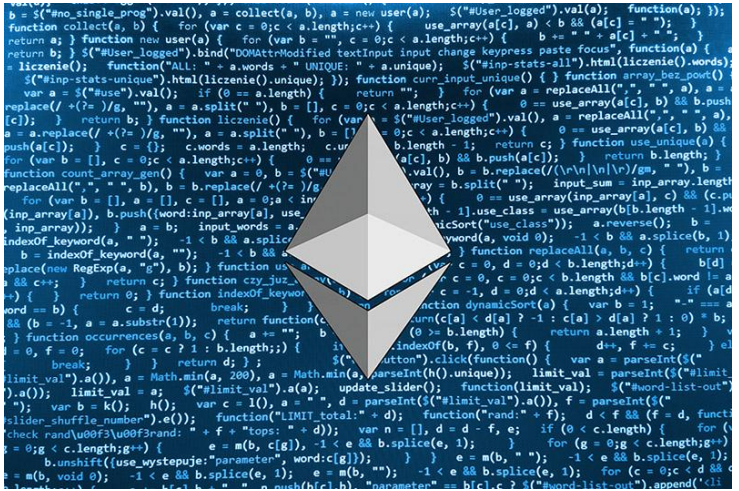
The Rise of Ethereum

Bitcoin is “coin centric.”

Primary Purpose: Alternative to existing currency

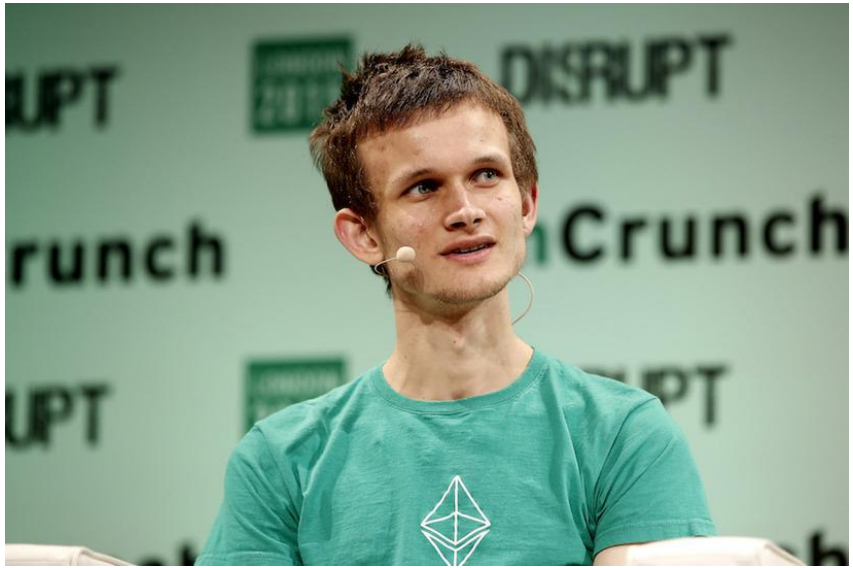
Ethereum is a Turing-complete protocol that uses its coin ether as “fuel”.

Primary Purpose: Platform for decentralized applications + Smart Contracts



2013 - 2016: Ethereum Timeline

- **Late 2013:** Ethereum described in whitepaper by Vitalik Buterin
- **July and August 2014:** Ethereum crowdsale
- **July 30th 2015:** Ethereum blockchain launched
- **May 2016:** Value of Ethereum tokens worth more than $1 billion
- **July 2016:** TheDAO rise and hack



2016 Onwards: Rise of Ethereum

Regulatory Circumstances:

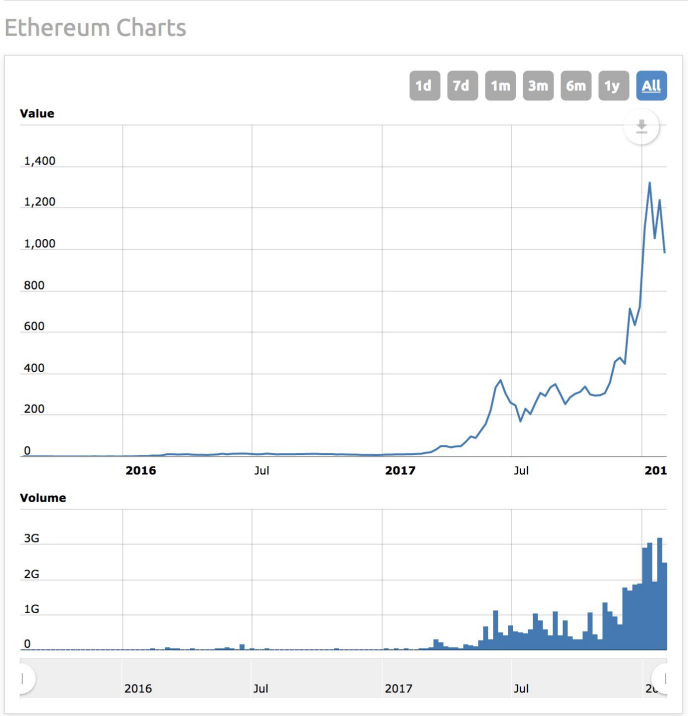
- Speculation about how the Securities and Exchange Commision would rule on the DAO fiasco, reversal of tokens values

Economic Circumstances:

- Exchange Traded Funds ruling
- ICOs (Initial Coin Offerings)
- Venture Capital funding for crypto companies

Other factors:

- People don't want to miss out on the "next Bitcoin"



Ethereum Hype Train

Ethereum DApps

CryptoKitties

DAI

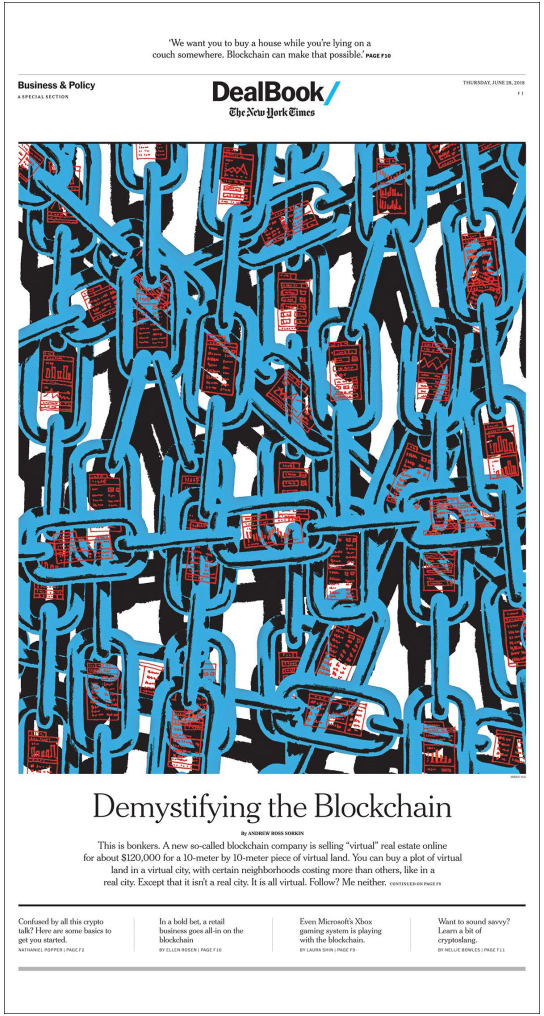
Brave

QUESTIONS?

ENTERPRISE BLOCKCHAIN: INTEREST FROM BANKS

Banks and Blockchain

- Rise of interest in "private blockchains" or "permissioned ledgers."
  - Not open
  - Not trustless
  - No economic incentives like in Bitcoin
  - Separate "blockchain" from "Bitcoin"
- Con:
  - Glorified public key cryptography
- Benefit:
  - More compliant



'We want you to buy a house while you're lying on a couch somewhere. Blockchain can make that possible.' PAGE F10

Business & Policy
A SPECIAL SECTION

DealBook
The New York Times

THURSDAY, JUNE 28, 2018
F 1

Demystifying the Blockchain

By ANDREW ROSS SORKIN

This is bonkers. A new so-called blockchain company is selling "virtual" real estate online for about $120,000 for a 10-meter by 10-meter piece of virtual land. You can buy a plot of virtual land in a virtual city, with certain neighborhoods costing more than others, like in a real city. Except that it isn't a real city. It is all virtual. Follow? Me neither. CONTINUED ON PAGE F9

Confused by all this crypto talk? Here are some basics to get you started.
NATHANIEL POPPER | PAGE F2

In a bold bet, a retail business goes all-in on the blockchain
BY ELLEN ROSEN | PAGE F10

Even Microsoft's Xbox gaming system is playing with the blockchain.
BY LAURA SHIN | PAGE F9

Want to sound savvy? Learn a bit of cryptoslang.
BY NELLIE BOWLES | PAGE F11

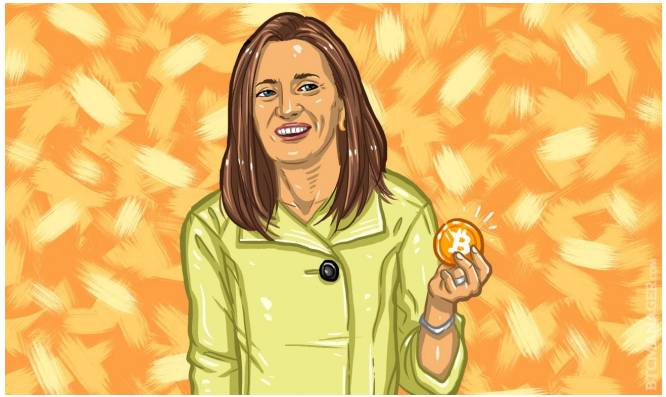
Private Blockchain Initiatives

Chain

IBM

Digital Asset

HYPERLEDGER PROJECT



Dimon on Bitcoin/Blockchain

Jan 2014: "It's a terrible store of value. It could be replicated over and over."

Oct 2014: "[Bitcoin developers] are going to try and eat our lunch. And that's fine. That's called competition, and we'll be competing."

Nov 2015: "Virtual currency, where it's called a bitcoin vs. a U.S. dollar, that's going to be stopped. … No government will ever support a virtual currency that goes around borders and doesn't have the same controls. It's not going to happen."

http://www.businessinsider.com/jp-morgans-jamie-dimon-on-bitcoin-2014-1

Dimon Quotes on Bitcoin/Blockchain

Oct 2017: “Bitcoin is a “fraud” that won’t end well. If you’re stupid enough to buy [bitcoin], you’ll pay the price for it one day. The blockchain is a technology which is a good technology. We actually use it… God bless the blockchain."

JP Morgan Unveils Quorum

Feb 2019: JPMorgan claimed it is the first US bank to create and successfully test a digital coin representing a fiat currency (JPM Coin)

- An internal ledger for banks
- A fungible digital token that represents USD held by JPM

QUESTIONS?

BLOCKCHAIN COMMUNITY & POLITICS

Community

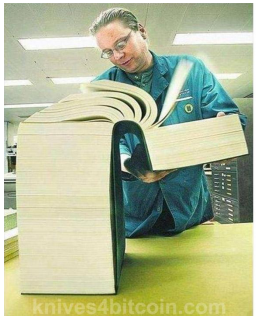
bitcointalk.org

slack

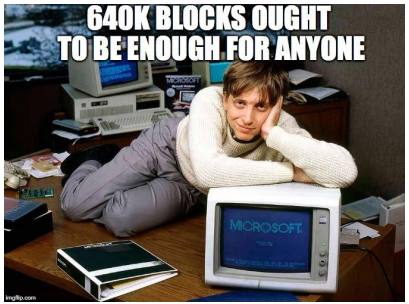
Controversial Topics

In the blockchain community, we have different ways to come to consensus about changes that happen. We have the most trouble agreeing on:

- Block Size?
- Confirmation Times?
- Centralization in third party companies?



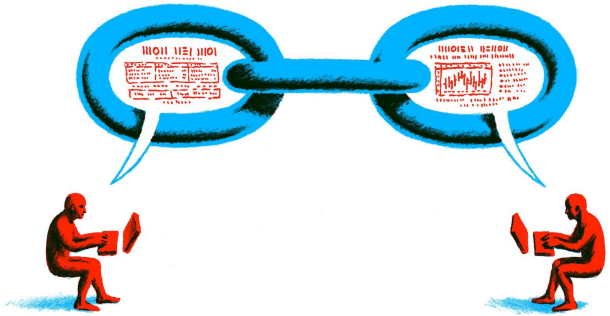
The Bitcoin block size debate is now available in this convenient paperback



QUESTIONS?

WHERE ARE WE NOW

Federal Interest Amidst Voter Suppression



FEDERAL DEVELOPMENTS

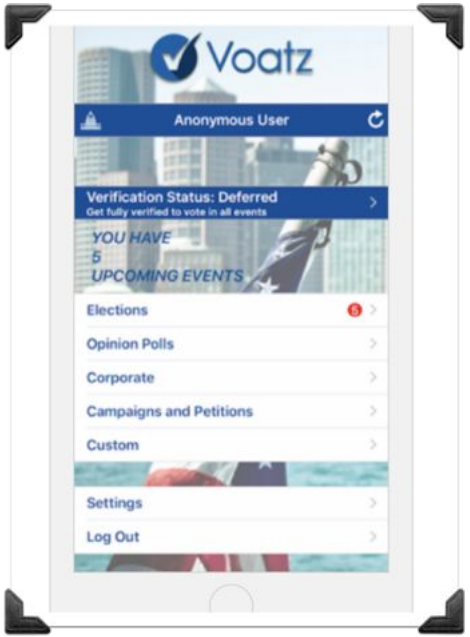
Blockchain

- **USPS applies for Blockchain-based patent for secure voting.** On August 13, a patent filed by the US Postal Service was published. The patent, entitled "Secure Voting System," enables confirmation of voter identity with respect to mail-in votes, separates voter identification and votes assure anonymity, and uses "the security of blockchain" to store the votes on a distributed ledger in a blockchain.

Where Are We Now

Mobile Voting

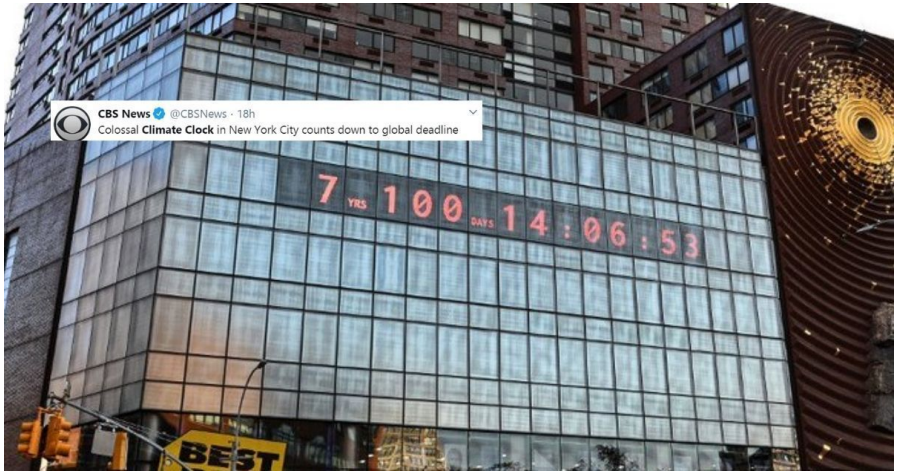
Voatz
Voting Redefined



- Voatz
  - Boston, MA Startup
  - blockchain-powered mobile voting application
  - two private-permissioned blockchains thru **HyperLedger**
    - The first is an “identity chain” and the second is the “voting chain.”

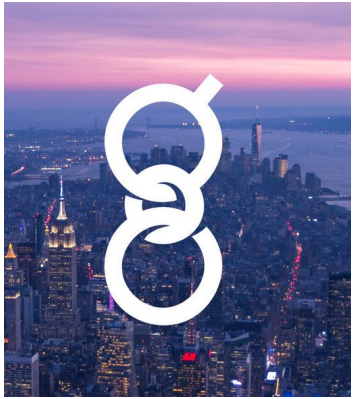
Where Are We Now

Climate Change



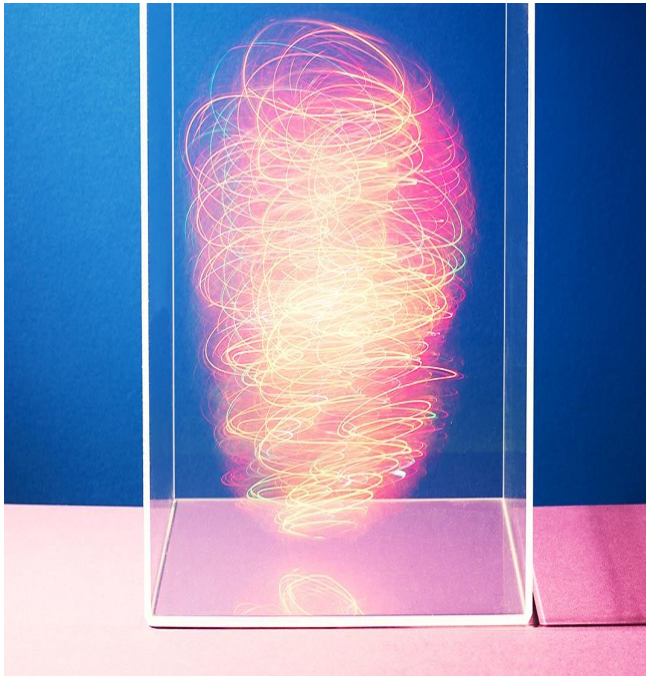
- Race against the clock to discover solutions to combat climate change
- Global Power and Energy Blockchain Conference and the Blockchain in Energy Forum are hard at work to find innovative solutions

ENERGY BLOCKCHAIN CONSORTIUM



Energy Innovations

- **Microgrid** set up on rooftop solar panels with blockchain ledger that records transactions
  - Microgrid: distributed energy generation, can function independently and provide power during natural disasters
  - Net Metering: residents can sell energy back to local utility
- **Swytch**: awards tokens to people and organizations that reduce their carbon footprint
  - e.g. generating renewable energy (companies), lowering energy usage (consumer)



Environmental Strides

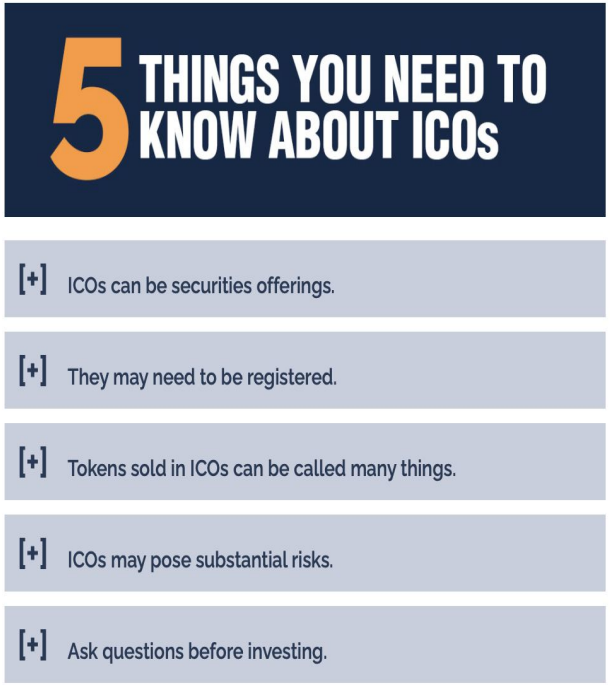
- **Carbon Credits** can be represented as tokens to be traded
  - Carbon Credit = prevention 1 metric ton of CO_2 release into atmosphere
  - Easily tradeable tokens allow for increased integrity of information and ease of measuring impact, transferring ownership rights, redemption
- **Veridium** tokenizes Carbon Credits, used in many carbon projects
- **RecycleToCoin**: rewards recyclers with cryptocurrency (BCDC tokens)

ICOS

ICOs - Initial Coin Offerings

- Way for people to invest Ether into startups of companies being built on top of Ethereum
- Permissionless, effortless way to invest in a good company (think Kickstarter)
- VCs are worried

Bancor ICO $150million
Tezos ICO $200 million
Filecoin ICO $253 Million



QUESTIONS?