BITCOIN TO BLOCKCHAIN: FROM CYPHERPUNKS TO JP MORGAN CHASE

Gloria Zhao
Aparna Krishnan

LECTURE OVERVIEW

1. PRE BITCOIN
2. EARLY BITCOIN: SCANDALS, HACKS, ILLEGAL ACTIVITY
3. SCALABILITY DEBATES AND ETHEREUM
4. ENTERPRISE BLOCKCHAIN
5. PRIVACY-CENTRIC ALTCOINS, AND PRESENT DAY

1 PRE BITCOIN: LIBERTARIAN DREAMS

LIBERTARIAN DREAMS

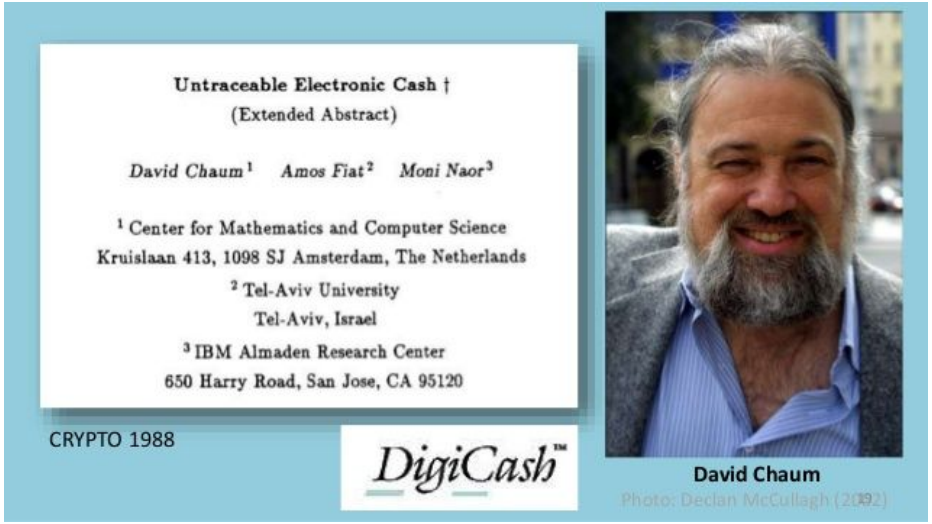
CYPHERPUNKS AND CRYPTO-ANARCHISTS

- **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"*

EARLY ATTEMPTS AT CRYPTOCURRENCY

DIGICASH AND HASHCASH

- **DigiCash**: “Blind signatures” public key cryptography
  - Failed due to centralization
- **HashCash:** Coins are minted by expending resources instead of by a central bank
  - Solve puzzle using cryptographic hash function



SATOSHI NAKAMOTO

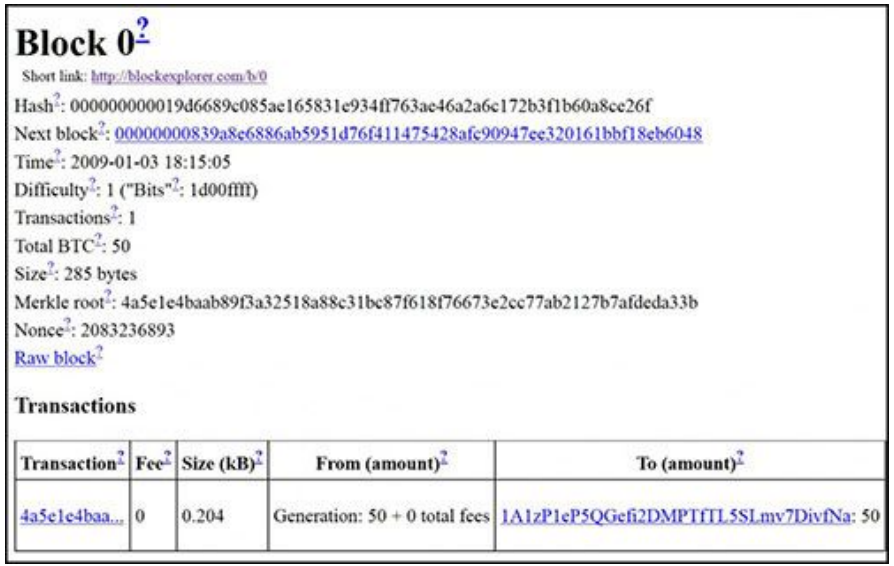
OCTOBER 2008: BITCOIN WHITEPAPER

- **Satoshi Nakamoto:** anonymous creator of Bitcoin, wrote the white paper
- Do we need trust? “electronic payment system based on cryptographic proof instead of trust”
- Solution to distributed consensus: Proof-of-Work, “one-CPU-one-vote”

BITCOIN: THE FIRST CRYPTOCURRENCY

GENESIS BLOCK MINED JAN 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

46 MILLION DOLLAR PIZZA BOUGHT MAY 2010

- May 21, 2010, **Laszlo Hanyecz** purchased $25 worth of pizza for 10,000 BTC
- Fun fact: 10,000 BTC is now equivalent to ~$46,000,000
- World's first ever Bitcoin transaction for a tangible asset
- Bitcoin went from worthless internet money to something with real value

2

EARLY BITCOIN: SCANDALS, HACKS, ILLEGAL ACTIVITY

BITCOIN THEFT

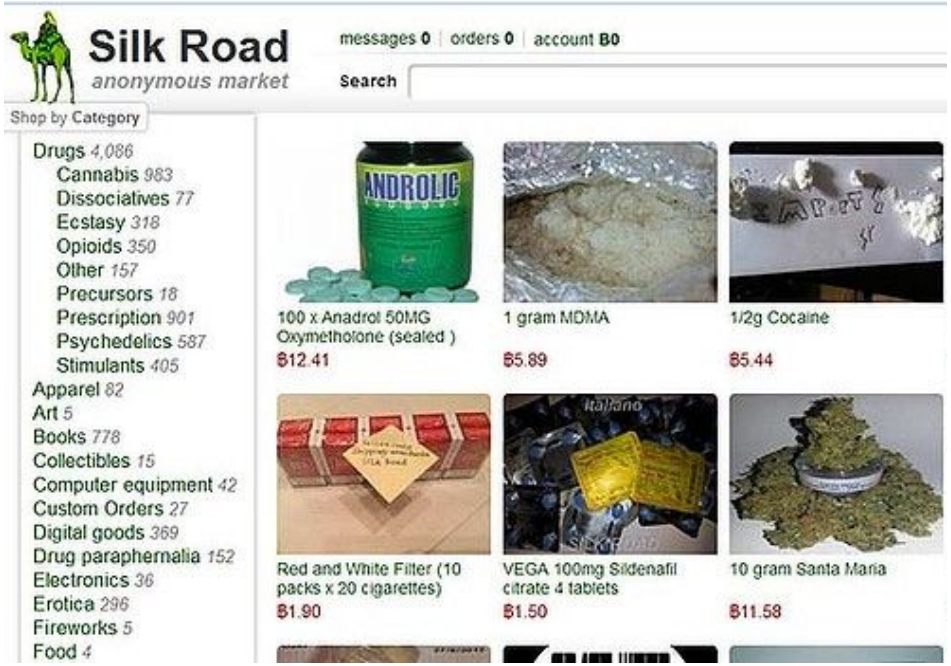
MT. GOX JULY 2010 - FEB 2014

- 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
- 2014: Mt. Gox loses 744,408 bitcoins in a theft that went unnoticed for years; Mt. Gox declares bankruptcy

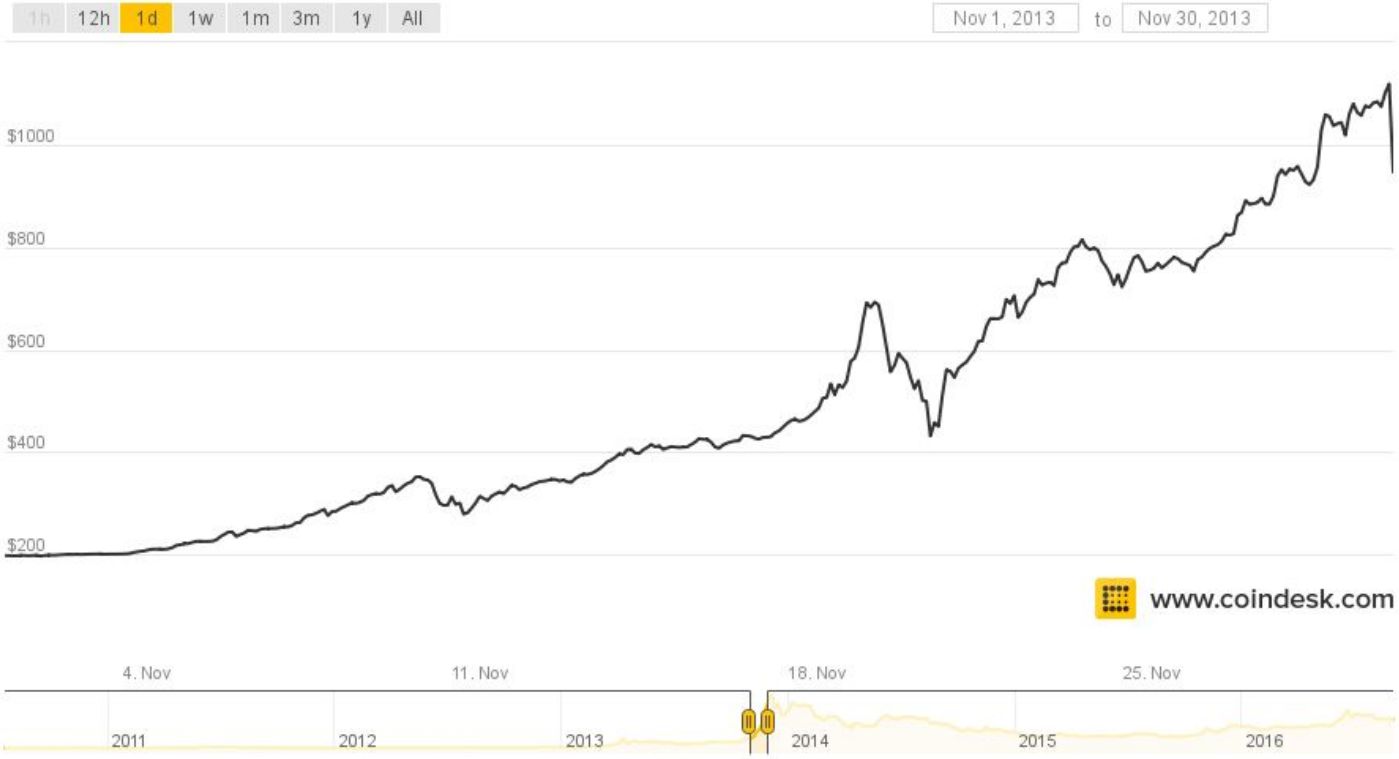
BITCOIN DRUG SCANDAL

SILK ROAD FEB 2011 - OCT 2013

- Feb 2011: **Silk Road** opens as the anonymous “eBay of Drugs”, using Tor and Bitcoin
- Drugs and black 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



BITCOIN BUBBLE



EXPLOSION OF ALTCOINS

Litecoin

ZCash

Ripple

Peercoin

PIVX

DASH

Monero

Dogecoin

BITCOIN HEADLINES

POPULARITY GROWS, MERCHANT BEGIN TO ACCEPT BITCOIN

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

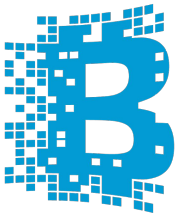
coinbase

xapo

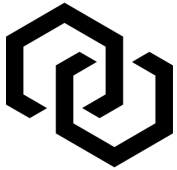
ANDREESSEN HOROWITZ

COINALYTICS

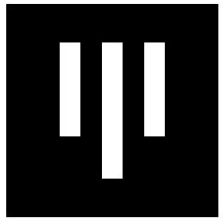
BitGo™



BLOCKCHAIN



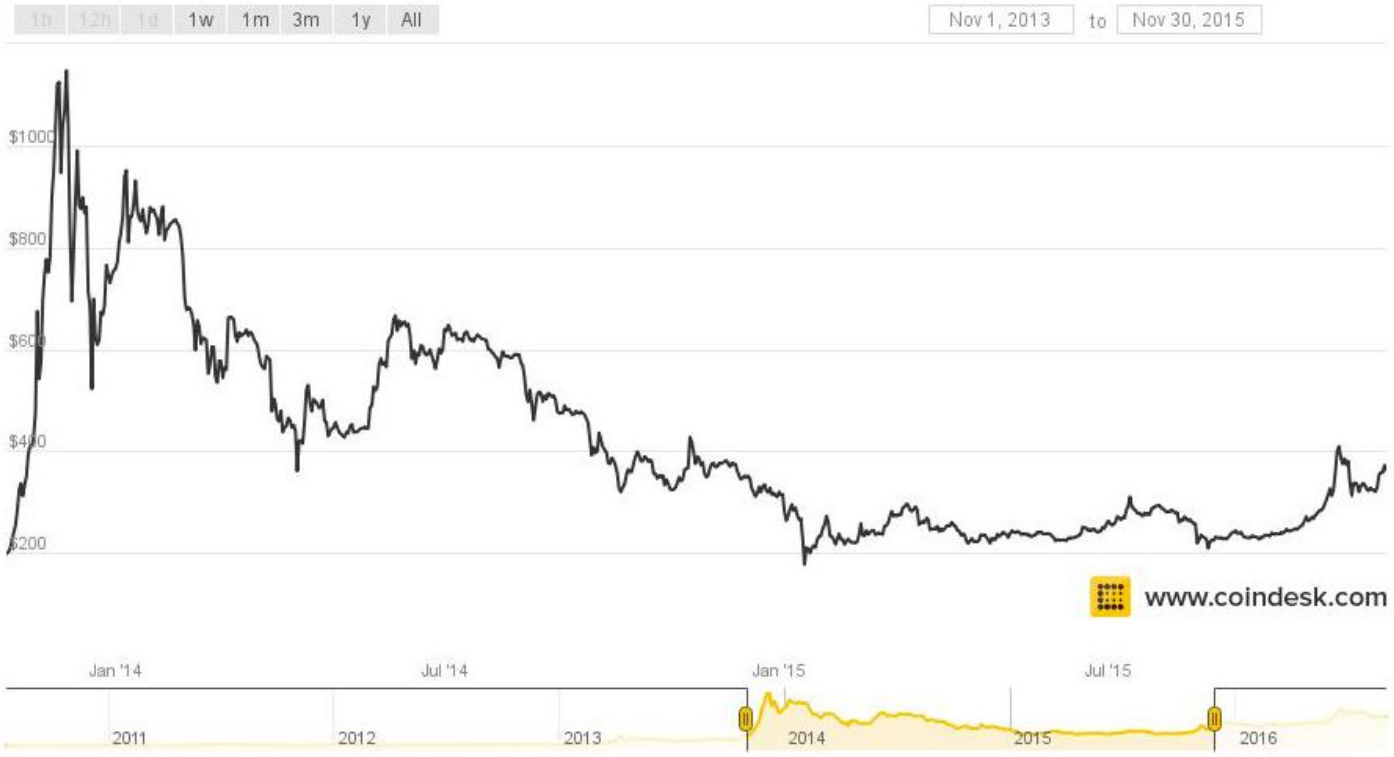
Chain



PANTERA

BLOCKCHAIN CAPITAL

… 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

3 SCALABILITY DEBATES & ETHEREUM

BITCOIN STRUGGLES TO SCALE

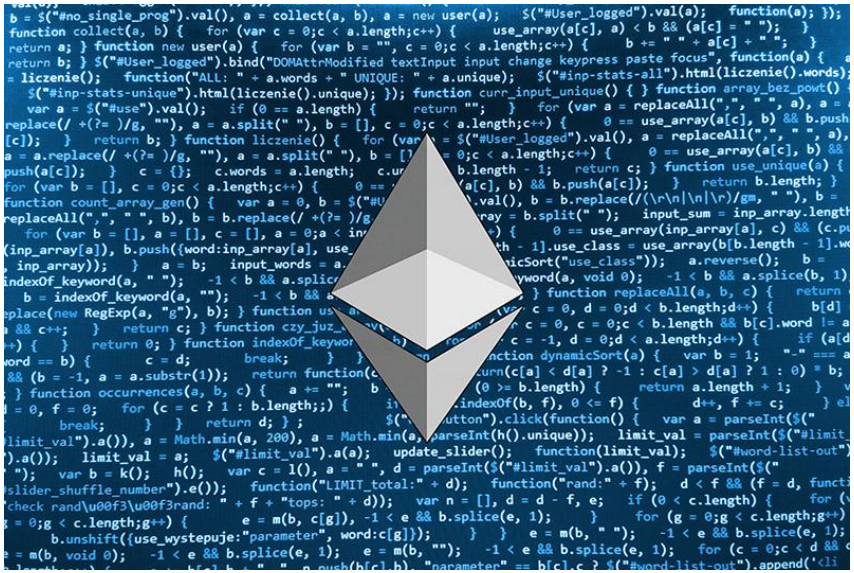
BLOCK SIZE DEBATE 2015

- Bitcoin blocks are created every 10 minutes and can only hold 1 MB of transactions
- 2015: blocks begin to run out of space, transactions go unconfirmed
- **Block Size Debate** raises questions about decentralized governance

2013 - 2016: ETHEREUM TIMELINE

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

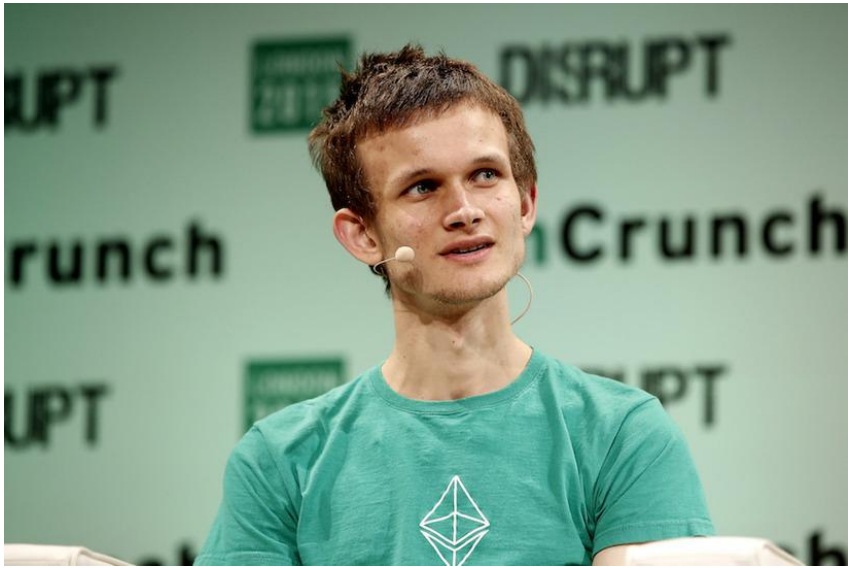


2013 - 2016: ETHEREUM TIMELINE

ETHEREUM BLOWS UP IN MULTIPLE WAYS

History

- 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 - PRESENT: ETHEREUM BUBBLE

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"

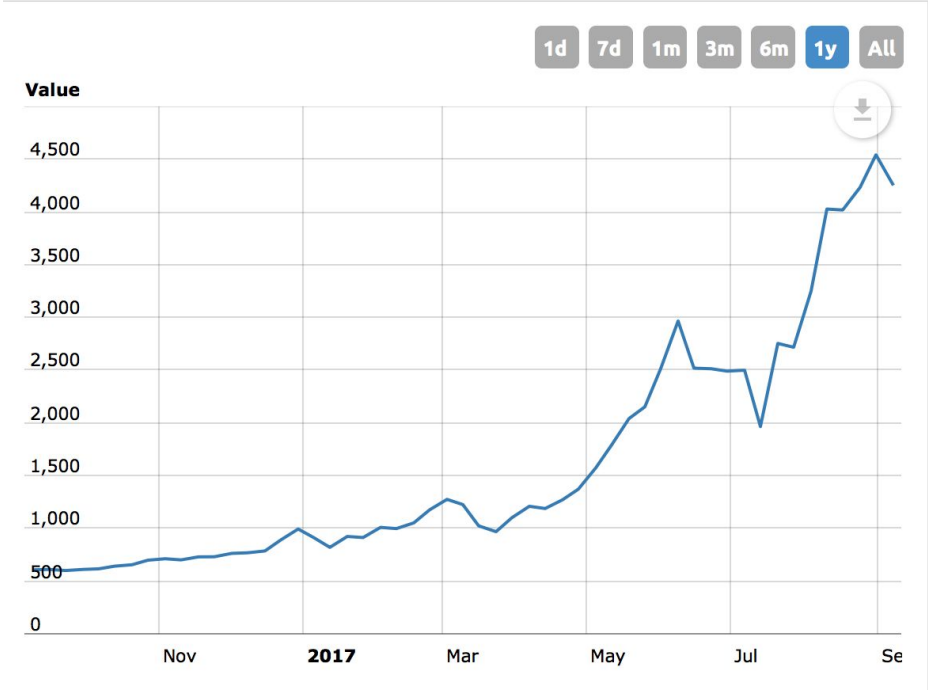
2016 - PRESENT: BITCOIN BOUNCES BACK

Economic Circumstances:

- Ethereum bounces back
- Circumventing Capital Controls
- General Instability in the market

Political Circumstances:

- Brexit
- Trump
- India's War on Cash

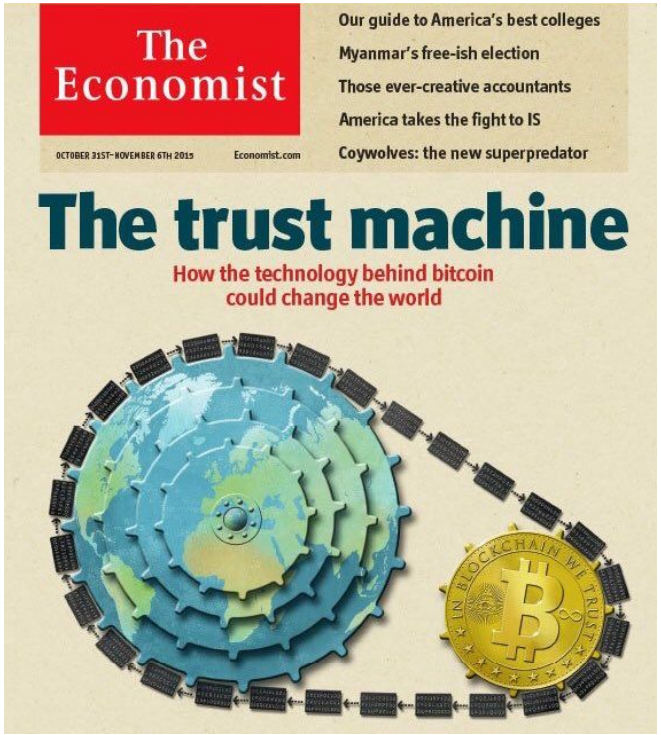


4 ENTERPRISE BLOCKCHAIN

4.1 INTEREST IN BLOCKCHAIN FROM BANKS

INTEREST IN BLOCKCHAIN FROM BANKS

- 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



PRIVATE BLOCKCHAIN INITIATIVES

Chain

R3

Digital Asset

HYPERLEDGER PROJECT

J.P.Morgan

IBM

DIMON QUOTES ON BITCOIN/BLOCKCHAIN

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

People still don't understand Bitcoin

"It's a terrible store of value." CNBC

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

DIMON QUOTES ON BITCOIN/BLOCKCHAIN

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." Conceding legitimacy to Bitcoin

http://static6.businessinsider.com/image/5527c91969beddfd15404336-480/jp-morgan-chase-and-company-ceo-jamie-dimon.jpg

DIMON QUOTES ON BITCOIN/BLOCKCHAIN

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.”

Bankers hate the lack of control. Perhaps threatened?

http://fortune.com/2015/11/04/jamie-dimon-virtual-currency-bitcoin/

DIMON QUOTES ON BITCOIN/BLOCKCHAIN

February 2016: “The Blockchain is a technology, which we’ve been studying … and yes it’s real. It could probably reduce the cost of real application in certain things. … If it proves to be cheap and secure it will be adopted for a whole bunch of stuff."
Separate "blockchain" from "Bitcoin"

Untraceable Electronic Cash †

(Extended Abstract)

David Chaum[1] *Amos Fiat*[2] *Moni Naor*[3]

[1] Center for Mathematics and Computer Science
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

[2] Tel-Aviv University
Tel-Aviv, Israel

[3] IBM Almaden Research Center
650 Harry Road, San Jose, CA 95120

CRYPTO 1988

DigiCash™

David Chaum

Photo: Declan McCullagh (2002)


JPMORGAN CHASE&Co

4.2 BITCOIN COMMUNITY AND POLITICS

COMMUNITY

WHERE DOES THE COMMUNITY EXIST?

bitcointalk.org

slack

Vitalik Buterin @VitalikButerin · Aug 12

PoW provides nothing remotely like "very good protection" in the case of high network latency.

2 3 15

Peter Todd @petertoddbtc · Aug 12

Wait, so why do you think Bitcoin has the two week difficulty adjustment period, and specifically, the 4x limit on diff drops?

4 6 38

BLOCKCHAIN AT BERKELEY

October 2nd, 3rd
http://cesc.io/

BLOCKCHAIN
AT BERKELEY

POLITICS

- Internal politics
- Right-wing extremism?
- Libertarianism

GEMINI coinx ChainPay
bitpay coinbase SNAPCARD
trucoin bitsquare Coinkite

BITMAIN
NTMINER
BTCChina BitFury

5

2017 THE YEAR OF ICOs

ICOs
THE HYPE

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

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

Bancor

Filecoin

References

- Venture funding
  - http://www.coindesk.com/bitcoin-venture-capital/
  - https://letstalkpayments.com/high-profile-investments-bitcoin-2013/
  - http://www.coindesk.com/venture-capital-funding-bitcoin-startups-triples-2014/
- News:
  - http://www.coindesk.com/6-weird-wonderful-bitcoin-events-2014/
  - http://www.coindesk.com/7-biggest-crypto-scandals-2014/
  - http://www.coindesk.com/year-headlines-coindesks-top-news-stories-2014/