

BITCOIN TO BLOCKCHAIN: FROM CYPHERPUNKS TO JP MORGAN CHASE

Brian Ho
Gillian Chu



BLOCKCHAIN
AT BERKELEY



LECTURE OVERVIEW

- 1 ► PRE BITCOIN
- 2 ► EARLY BITCOIN:
SCANDALS, HACKS, ILLEGAL
ACTIVITY
- 3 ► SCALABILITY DEBATES
AND ETHEREUM
- 4 ► ENTERPRISE BLOCKCHAIN
- 5 ► TOKENS OF TODAY



PRE BITCOIN: LIBERTARIAN DREAMS

BLOCKCHAIN FUNDAMENTALS LECTURE 2





LIBERTARIAN DREAMS

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’s Manifesto).

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

AUTHOR: BRIAN HO

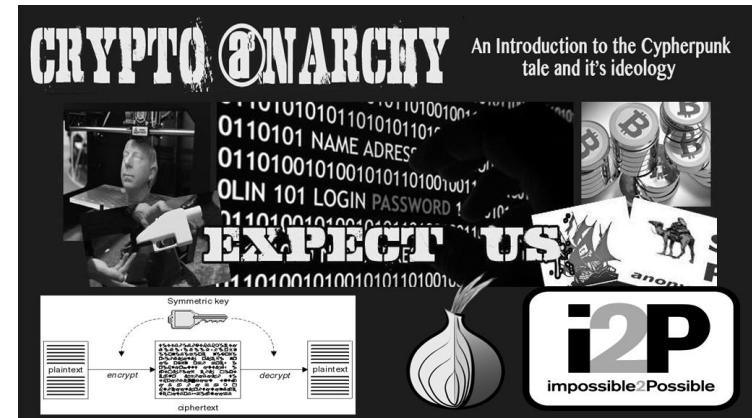
BLOCKCHAIN FUNDAMENTALS LECTURE 2



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”***



AUTHOR: GLORIA ZHAO



EARLY ATTEMPTS AT CRYPTOCURRENCY

DIGICASH, HASHCASH, B-MONEY

- **DigiCash:** “Blind signatures” public key cryptography
 - Allowed users to sign off on transactions without revealing anything about their identity
 - Failed due to centralization

Untraceable Electronic Cash †
(Extended Abstract)

David Chaum¹ Amos Fiat² Moni Naor³

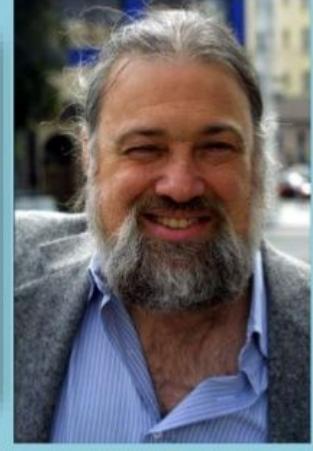
¹ Center for Mathematics and Computer Science
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands

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)



AUTHOR: BRIAN HO

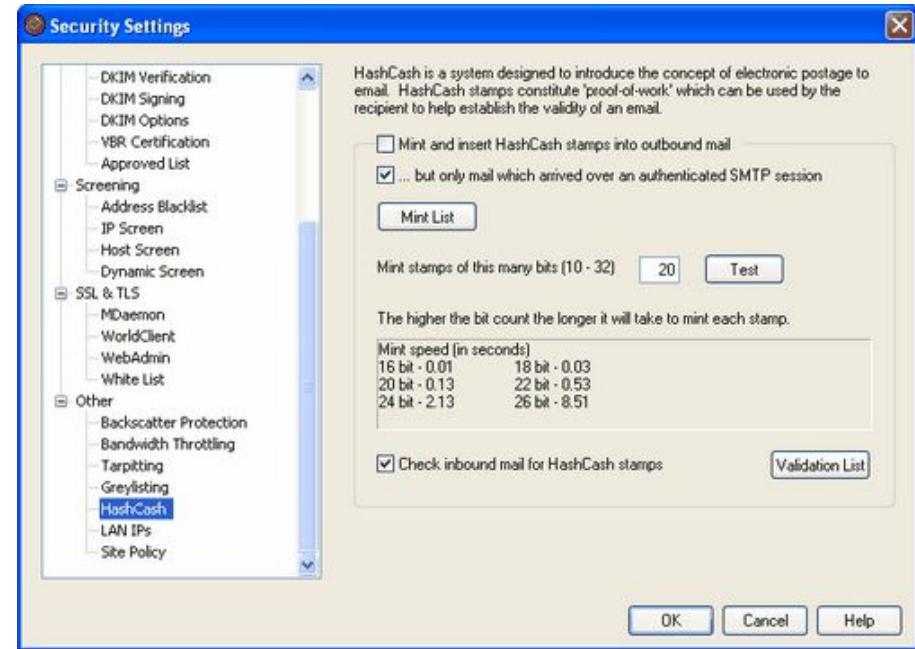
BLOCKCHAIN FUNDAMENTALS LECTURE 2



EARLY ATTEMPTS AT CRYPTOCURRENCY

DIGICASH, HASHCASH, B-MONEY

- **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



AUTHOR: BRIAN HO



EARLY ATTEMPTS AT CRYPTOCURRENCY

DIGICASH, HASHCASH, 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



AUTHOR: BRIAN HO

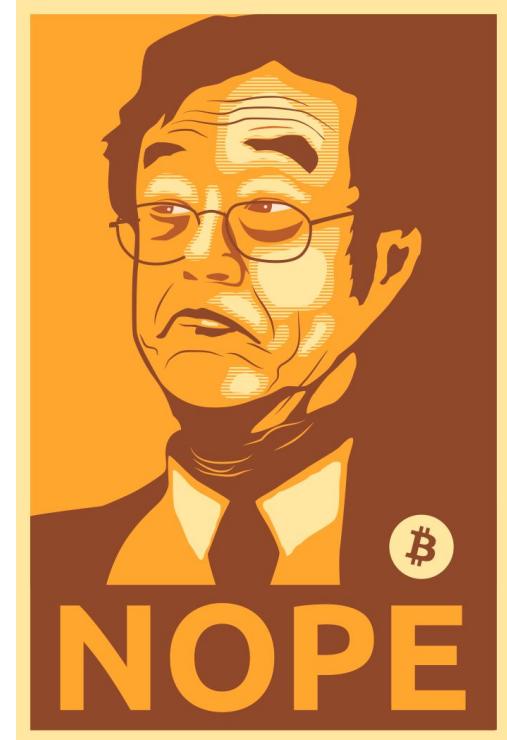
BLOCKCHAIN FUNDAMENTALS LECTURE 2



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”



AUTHOR: GLORIA ZHAO

BLOCKCHAIN FUNDAMENTALS LECTURE 2



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 0²

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

Hash²: 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Next block²: [0000000839a8e6886ab5951d76f411475428afc90947ee320161bbf18eb6048](#)

Time²: 2009-01-03 18:15:05

Difficulty²: 1 ("Bits"²: 1d00ffff)

Transactions²: 1

Total BTC²: 50

Size²: 285 bytes

Merkle root²: 4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b

Nonce²: 2083236893

[Raw block²](#)

Transactions

Transaction ²	Fee ²	Size (kB) ²	From (amount) ²	To (amount) ²
4a5e1e4baa...	0	0.204	Generation: 50 + 0 total fees	1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa : 50





BITCOIN GAINS VALUE

87 MILLION DOLLAR PIZZA BOUGHT MAY 2010

Author	Topic: Pizza for bitcoins? (Read 774776 times)
 laszlo Full Member 	Pizza for bitcoins?  May 18, 2010, 12:35:20 AM <i>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), Toughtit (1), nullius (1), alia_armelle (1) #1</i> <hr/> <p>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!</p> <p>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.</p> <p>If you're interested please let me know and we can work out a deal.</p> <p>Thanks, Laszlo</p> <hr/> <p>BC: 157fRrqAKrDyGhr1Bx3yDxeMv8Rh45aUet</p>



AUTHOR: BRIAN HO

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

BLOCKCHAIN FUNDAMENTALS LECTURE 2



BITCOIN GAINS VALUE

87 MILLION DOLLAR PIZZA BOUGHT MAY 2010

- May 22, 2010, **Laszlo Hanyecz** purchased \$25 worth of pizza for 10,000 BTC
- Fun fact: 10,000 BTC is now equivalent to ~\$87,000,000
- World's first ever Bitcoin transaction for a tangible asset
- Bitcoin went from worthless internet money to something with real value



BLOCKCHAIN FUNDAMENTALS LECTURE 2



AUTHOR: GLORIA ZHAO



BITCOIN GAINS VALUE

87 MILLION DOLLAR PIZZA BOUGHT MAY 2010

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



Download: [IMG_0988.jpg](#)

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



Download: [IMG_0989.jpg](#)



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.

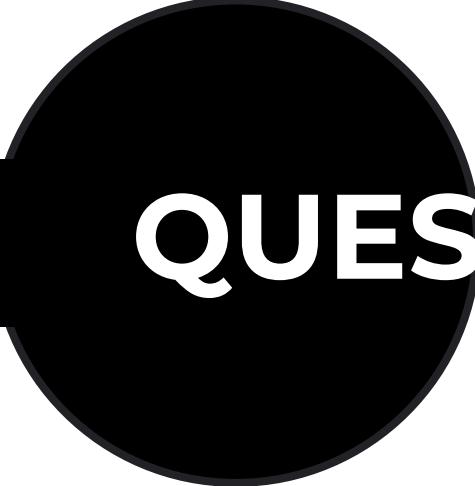
Pictures: <http://heliacal.net/~solar/bitcoin/pizza/>

Thanks jercos!



AUTHOR: BRIAN HO

BLOCKCHAIN FUNDAMENTALS LECTURE 2



QUESTIONS?





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



AUTHOR: GLORIA ZHAO

BLOCKCHAIN FUNDAMENTALS LECTURE 2





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

The screenshot shows the Silk Road anonymous market homepage. At the top, there's a logo of a camel and the text "Silk Road anonymous market". Below the logo, there are links for "messages 0", "orders 0", and "account B0". A search bar is also present. On the left, a sidebar titled "Shop by Category" lists various categories with their counts: Drugs (4,086), Cannabis (983), Dissociatives (77), Ecstasy (318), Opioids (350), Other (157), Precursors (18), Prescription (901), Psychedelics (587), Stimulants (405), Apparel (82), Art (5), Books (778), Collectibles (15), Computer equipment (42), Custom Orders (27), Digital goods (369), Drug paraphernalia (152), Electronics (36), Erotica (296), Fireworks (5), and Food (4). The main area displays several product listings with images and prices:

Item	Description	Price
100 x Anadrol 50MG Oxymetholone (sealed)	100 x Anadrol 50MG Oxymetholone (sealed)	\$12.41
1 gram MDMA	1 gram MDMA	\$5.89
1/2g Cocaine	1/2g Cocaine	\$5.44
Red and White Filter (10 packs x 20 cigarettes)	Red and White Filter (10 packs x 20 cigarettes)	\$1.90
VEGA 100mg Sildenafil citrate 4 tablets	VEGA 100mg Sildenafil citrate 4 tablets	\$1.50
10 gram Santa Maria	10 gram Santa Maria	\$11.58



AUTHOR: GLORIA ZHAO

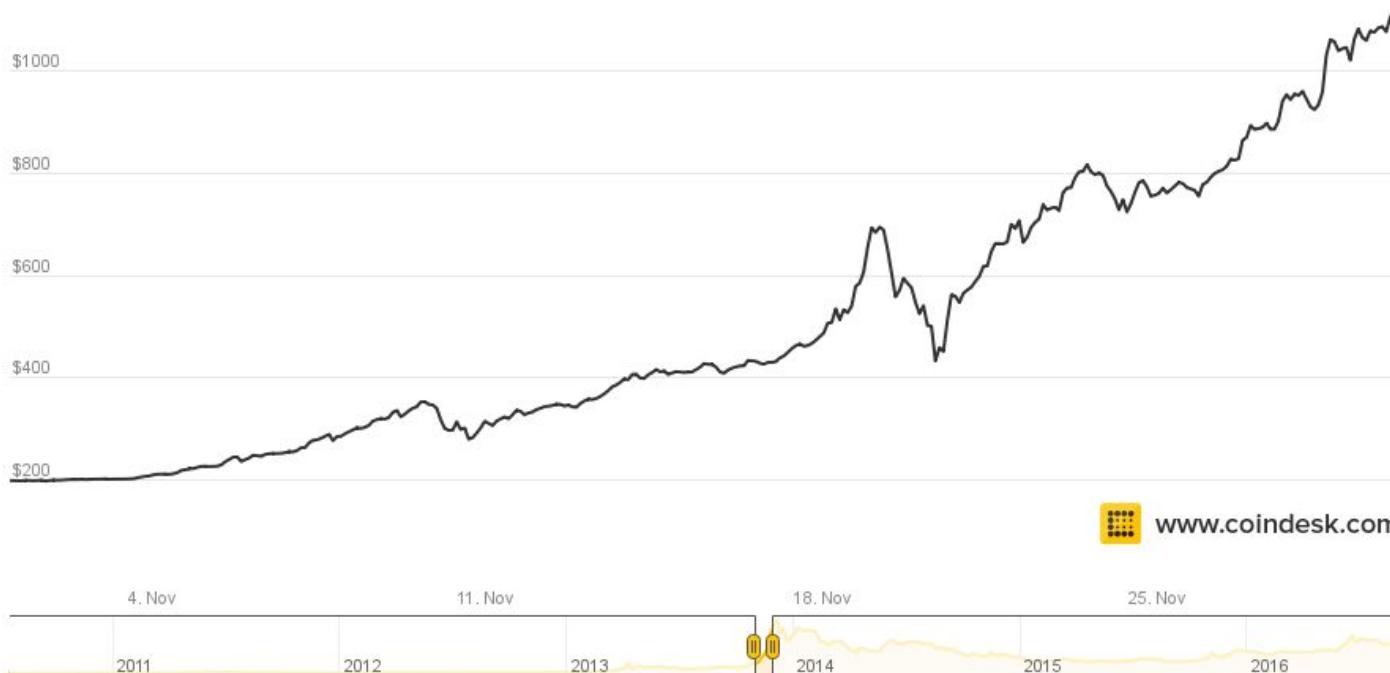
BLOCKCHAIN FUNDAMENTALS LECTURE 2



BITCOIN BUBBLE

1h 12h 1d 1w 1m 3m 1y All

Nov 1, 2013 to Nov 30, 2013



AUTHOR: ANDREW TU

BLOCKCHAIN FUNDAMENTALS LECTURE 2



EXPLOSION OF ALTCOINS



Litecoin



ZCash



Stellar



Peercoin



Dogecoin



DASH



Monero



Ripple

▼ ▲ ▼ ▲ ▼ ▲

AUTHOR: GLORIA ZHAO

BLOCKCHAIN FUNDAMENTALS LECTURE 2



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



AUTHOR: MAX FANG

BLOCKCHAIN FUNDAMENTALS LECTURE 2



BITCOIN STARTUPS

coinbase **xapo**

ANDREESSEN
HOROWITZ

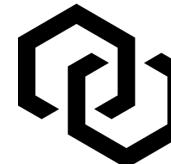
COINALYTICS



BitGo™



BLOCKCHAIN



Chain



PANTERA



BLOCKCHAIN
CAPITAL



CIRCLE

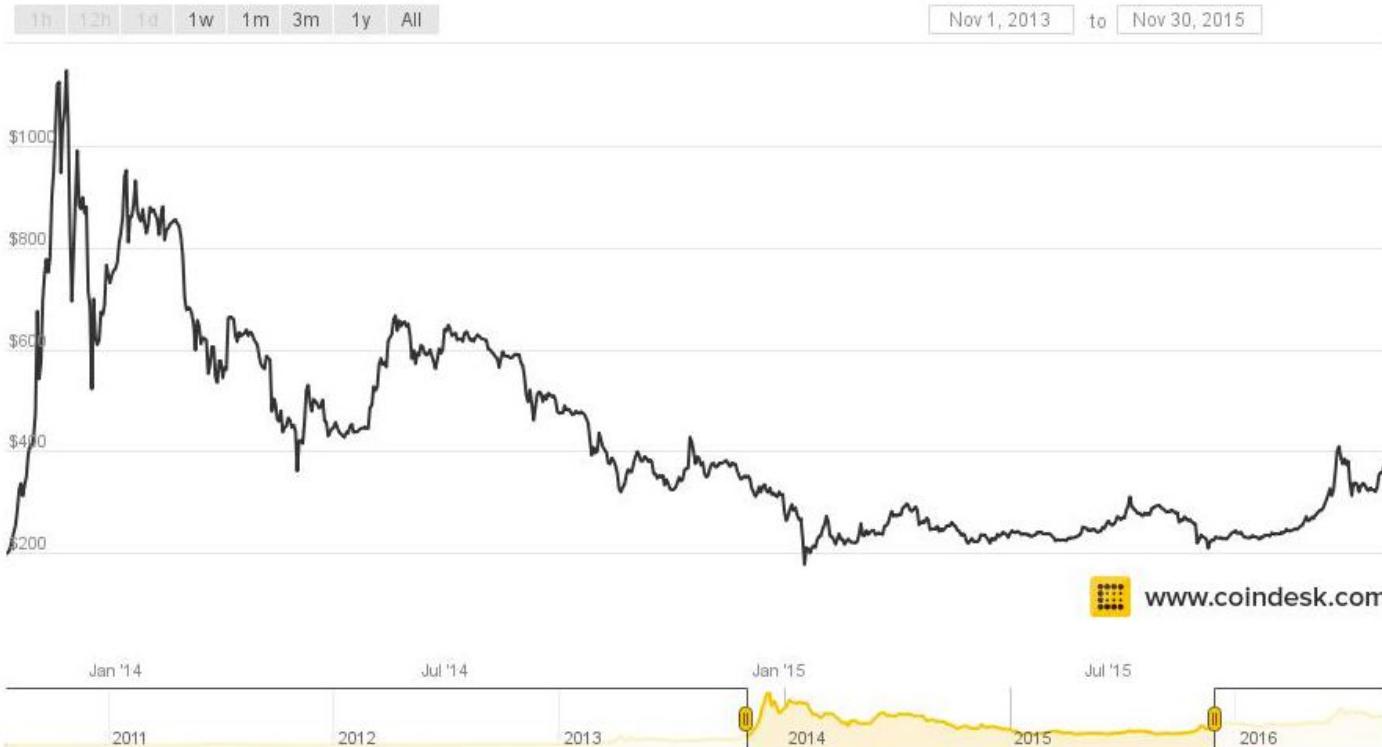
▲
▼
▼
▼
▼
▼
▼

AUTHOR: MAX FANG

BLOCKCHAIN FUNDAMENTALS LECTURE 2

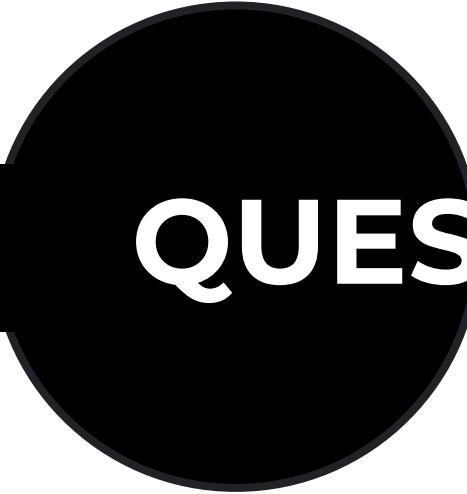


... AND BURST



AUTHOR: ANDREW TU

BLOCKCHAIN FUNDAMENTALS LECTURE 2



QUESTIONS?







3

SCALABILITY DEBATES & ETHEREUM

BLOCKCHAIN FUNDAMENTALS LECTURE 2



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



COINTELEGRAPH



AUTHOR: GLORIA ZHAO

BLOCKCHAIN FUNDAMENTALS LECTURE 2



2013 - 2016: ETHEREUM TIMELINE

Bitcoin is “coin centric.”

Primary Purpose: Alternative to existing currency



AUTHOR: APARNA KRISHNAN

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

Primary Purpose: Platform for decentralized applications + Smart Contracts

```


b = $("#no_single_prog").val(), a = collect(a, b), a = new user(a);  $( "#User_logged" ).val(a);  function(a, ));}
function collect(a, b) { for (var c = 0; c < a.length;++) { use_array(a[c], a) < b && (a[c] == ""); }
return a; } $("new_user(a) { for (var b = "", c = 0;c < a.length;c++) { b += " + a[c] + " ";
} return b; } $("#User_logged").bind("DOMAttrModified",textInput change keypress paste focus", function(e) { a =
liczenie(); function("AL: " + a.words + " UNIQUE: " + a.unique, $("#inp-stats-all").html(liczenie().words);
$("#inp-stats-unique").html(liczenie().unique); }) function curr_input_unique() { } function array_bez_povt() {
var a = $("#use").val(); if (0 == a.length) { return ""; } for (var a = replaceAll("", "", a), a =
replace(/\+/g, ""), a = a.split(" "), b = [], c = 0;c < a.length;c++) { 0 == use_array(a[c], b) && b.push(
[c]); } return b; } function liczenie() { for (var a = $("#User_logged").val(), a = replaceAll("", "", a),
a = a.replace(/\+/g, ""), a = a.split(" "), b = [], c = 0;c < a.length;c++) { 0 == use_array(a[c], b) &&
b.push(a[c]); } c = 0; c < a.length; c++) { c = use_array(a[c], b); } return b.length; } function count_array_gen() {
for (var a = [], b = $("#User_logged").val(), a = replaceAll(/\r\n|\n|\r/gm, "\n"), b =
array = b.split("\n"); input_sum = inp_array.length; for (var b = [], a = [], c = 0;a < input_sum;b =
array[c], b = b.replace(/\+/g, "")); a.push(b); } a = use_array(inp_array[a], c) && (c != a.length - 1).use_class =
use_array(b[b.length - 1].use_class); a.reverse(); b = indexOf(keyword(a, " ")); -1 < b && a.splice(b, 1);
b = indexOf(keyword(a, " ")); -1 < b && a.splice(b, 1); } function replaceAll(a, b, c) { return
replace(new RegExp(a, "g"), b); } function us() { var a = "", b = "", c = 0, d = 0; d < b.length;d++) { b[d]
&& c++; } return c; } function czy_wolny() { var a = "", b = "", c = 0, d = 0; d < a.length;d++) { if (a[d] ==
") { return 0; } function indexOf_keyword(a, b) { var c = 0, d = 0; d < b.length;d++) { if (b[d] ==
a) { c = d; break; } } return c; } function dynamicSort(a) { var b = 1; "-" == a[0] ? b = -1 : a[0] ==
">" && (b = -1, a = a.substr(1)); return function(c) { var a = c[0], b = c[1]; if (a < b) { return 1; } else
{ return -1; } } function occurrences(a, b, c) { a += ";"; b += ";"; c += ";"; var d = a.indexOf(b, 0); if (d == -1) { return 0; } else { var e = a.substring(d + 1); var f = b.length; for (var g = 0; g < e.length; g++) { if (e[g] == b[f]) { return 1; } } return 0; } } function
button().click(function() { var a = parseInt($("#limit_val").val()), a = Math.min(a, 200), a = Math.min(a,
parseInt(h.unique)); limit_val = parseInt($("#limit_val").val()); update_slider(); function(limit_val) {
$("#" + h).slider("value", limit_val); } var b = k(), h(); var c = 1, a = "", d = parseInt($("#limit_val").val()),
f = parseInt($("#" + h).val()); var g = b(c); var h = d(f); if (0 < c.length) { for (var i = 0; i < c.length;
i++) { g += t + "tops:" + d); var n = [], d = f - f, e; if (0 < c.length) { for (var j = 0; j < c.length;
j++) { g += "g < c.length;g++) { e = m(b, c[g]); -1 < e && b.splice(e, 1); } for (var l = 0; l < g.length; l++) {
b.unshift({use_wystepuje:"parameter", word:c[g]}); } } e = m(b, ""); -1 < e && b.splice(e, 1); for (var m = 0;
m < b.length; m++) { e = m(b, void 0); -1 < e && b.splice(e, 1); e = m(b, ""); -1 < e && b.splice(e, 1); for (var n = 0;
n < b.length; n++) { e = m(b, void 0); -1 < e && b.splice(e, 1); } } } } } } ); } ); } ); } ); } ); } );


```



BLOCKCHAIN FUNDAMENTALS LECTURE 2

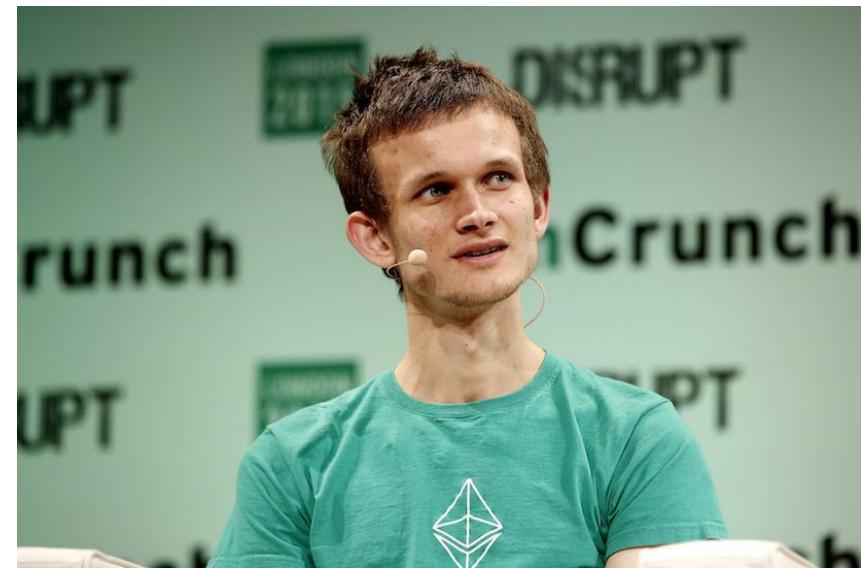


2013 - 2016: ETHEREUM TIMELINE

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



AUTHOR: MAX FANG

UPDATED BY APARNA KRISHNAN

BLOCKCHAIN FUNDAMENTALS LECTURE 2



2016 - PRESENT: ETHEREUM BUBBLE

Regulatory Circumstances:

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

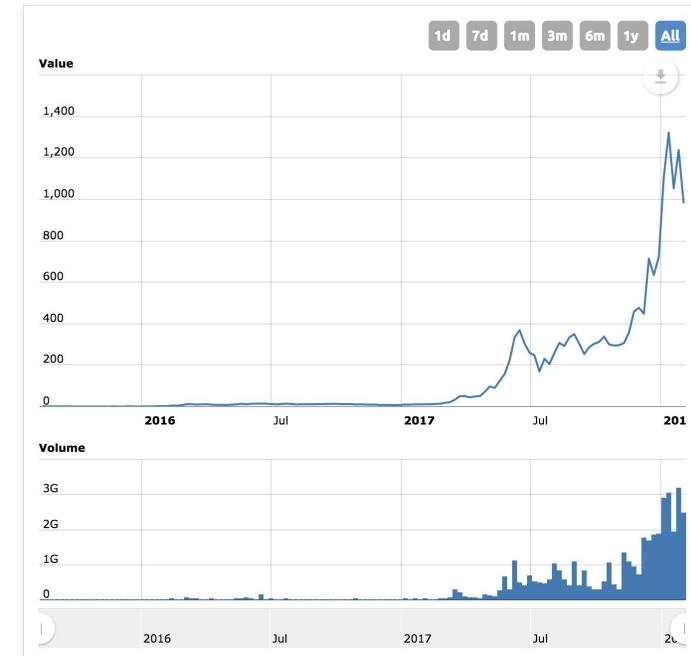
Economic Circumstances:

- 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”

Ethereum Charts





2016 - 2017: HYPE TRAIN

Economic Circumstances:

- Ethereum bounces back
- General Instability in the market

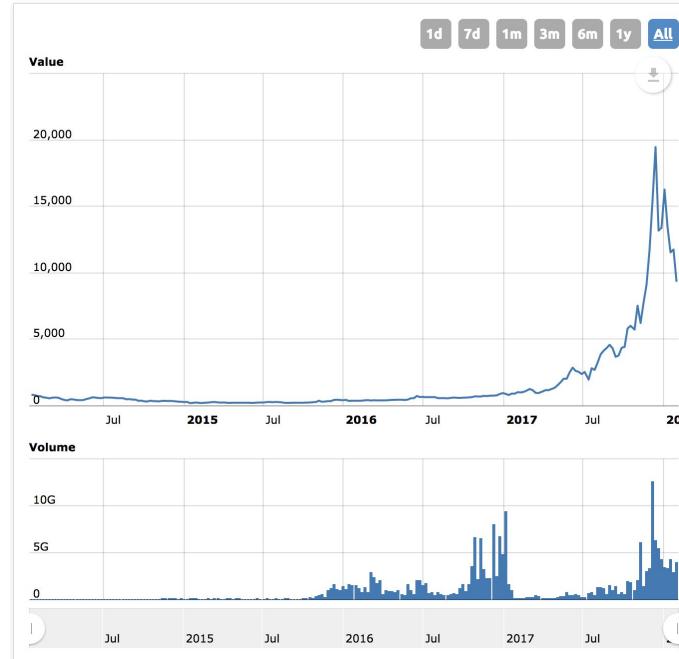
Political Circumstances:

- Brexit
- Trump
- India's War on Cash

Bitcoin & Cryptocurrency Hype

- Bitcoin prices get broadcast on the radio now

Bitcoin Charts



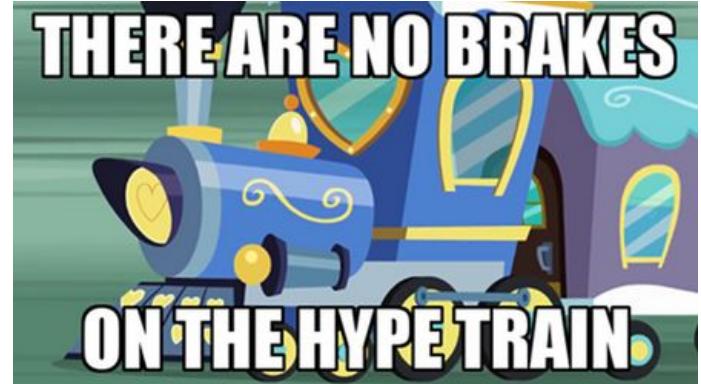


2016 - 2017: HYPE TRAIN



AUTHOR: MAX FANG

UPDATED BY GILLIAN CHU

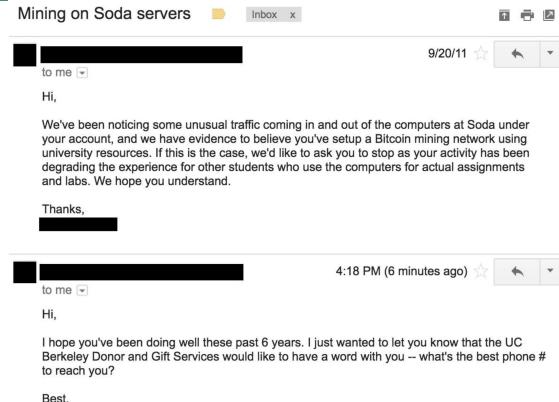




2016 - 2017: HYPE TRAIN



▲
▼
▼
▼
AUTHOR: MAX FANG
UPDATED BY GILLIAN CHU





2016 - 2017: HYPE TRAIN

ethereum
Homestead Documentation

coinbase

"decentralized"

Kanye Thaler November 29 at 2:09am

"If I fucked the president of Blockchain, do you think he'd let you into the club?" -- Unit 1 girl talking to 4 desperate CS majors

distributed ledger

BLOCKCHAIN AT BERKELEY

I'm really into the blockchain space

BerkeleyHaas EECS

\$16,084.12

\$15,312.01 (1983.17%)

\$15,951

Today 8:32 AM

"I wish I started mining sooner!"

"it's not a bubble"

"decentralized"

"decentralized"

"I had offers from Google and Goldman, but I'd rather work for a blockchain startup honestly"

"The future of finance"

"trustless transactions"

Oski 'BTC' Bear - co-founder and Investor at Blockchain
Blockchain University of California, Berkeley
San Francisco Bay Area • San Joaquin County

Can I pay for her drink with ethereum?

THERE ARE NO BRAKES

HYPE TRAIN

vers Inbox 9/20/11

Hi,

I hope you've been doing well these past 6 years. I just wanted to let you know that the UC Berkeley Donor and Gift Services would like to have a word with you -- what's the best phone # to reach you?

Best,

NEO
smart economy

CryptoKitties

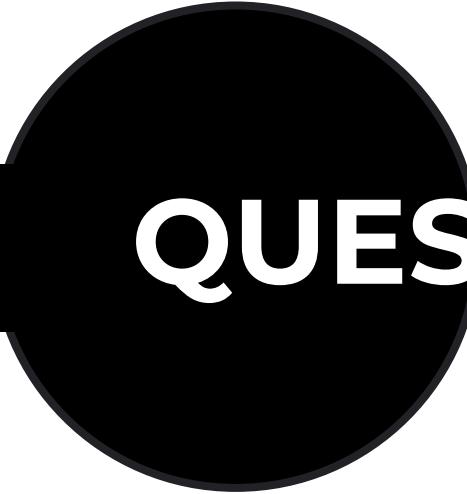
CryptoKitties: Collect and breed digital cats! Collect and trade Cryptokitties in one of the world's first blockchain games. Breed your newest cats to create the perfect furry friend. The future is cryptokitties.co

AUTHOR: MAX FANG
UPDATED BY GILLIAN CHU

BLOCKCHAIN FUNDAMENTALS LECTURE 2



AIN
AT BERKELEY



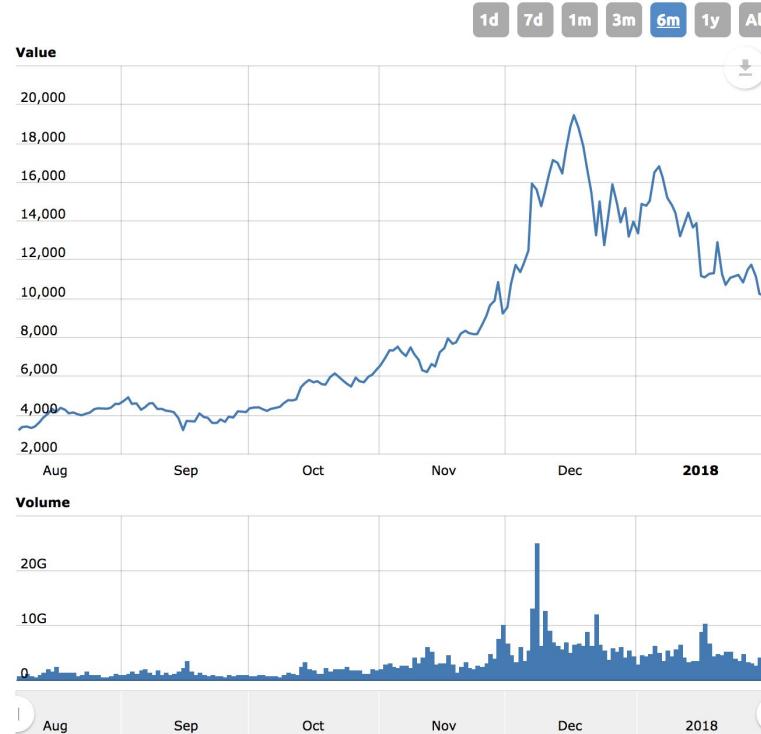
QUESTIONS?





2017- PRESENT: GET OFF AT THIS STATION

WHY THE CRASH?



BLOCKCHAIN FUNDAMENTALS LECTURE 2

▲▼
▼▼
▼▼

AUTHOR: GILLIAN CHU



2017- PRESENT: GET OFF AT THIS STATION

WHY THE CRASH?



Regulation in South Korea
 Regulation in India
 Regulation in the UK
 Regulation in the US

...

▲ 427 ▼

A lot of you forgot why we bought into btc in the first place (self.Bitcoin)
submitted 10 hours ago by obkenobi13 | reddit for 3 months

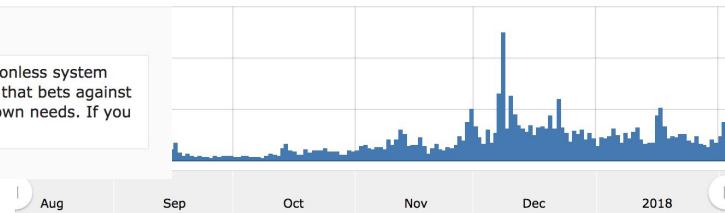
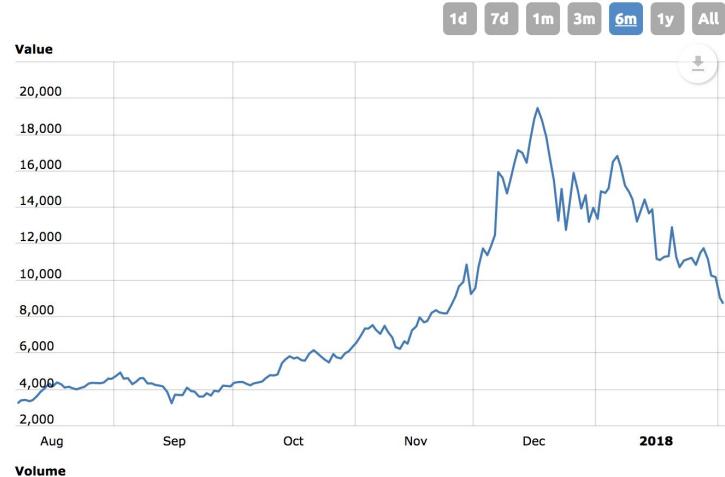
Let's remind ourselves here why we bought btc in the first place: a censorship resistant and permissionless system where no fucking institution tells me with whom I am allowed to transact with. This is an investment that bets against a repressive system built and maintained by corrupt governments and corporations that serve their own needs. If you still haven't grasped this then please sell all your coins and GTFO.

253 comments share save hide give gold report crosspost



AUTHOR: GILLIAN CHU

BLOCKCHAIN FUNDAMENTALS LECTURE 2





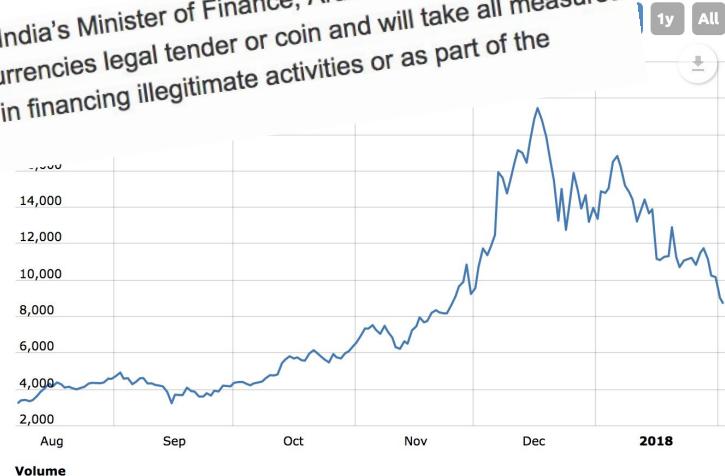
2017- PRESENT: GET OFF AT THIS STATION

WHY THE CRASH?



Regulation
Regulation
Regulation
Regulation in the UK
Regulation in the US
...

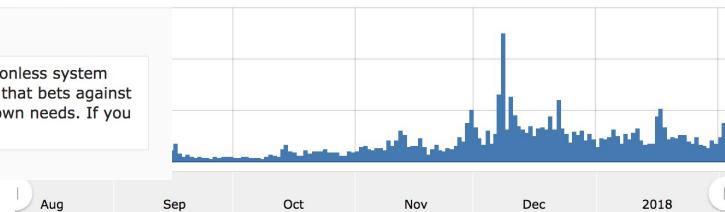
"The drop followed comments made by India's Minister of Finance, Arun Jaitley, that the Indian government 'does not consider cryptocurrencies legal tender or coin and will take all measures to eliminate use of these crypto-assets in financing illegitimate activities or as part of the payment system'.



427 A lot of you forgot why we bought into btc in the first place (self.Bitcoin)
submitted 10 hours ago by obkenobi13 | reddit for 3 months

Let's remind ourselves here why we bought btc in the first place: a censorship resistant and permissionless system where no fucking institution tells me with whom I am allowed to transact with. This is an investment that bets against a repressive system built and maintained by corrupt governments and corporations that serve their own needs. If you still haven't grasped this then please sell all your coins and GTFO.

253 comments share save hide give gold report crosspost



AUTHOR: GILLIAN CHU

BLOCKCHAIN FUNDAMENTALS LECTURE 2



2017- PRESENT: GET OFF AT THIS STATION

WHY THE CRASH?



Regulation
Regulation
Regulation
Regulation in the UK

Regulation
...

"The drop followed comments made by India's Minister of Finance, Arun Jaitley, that the Indian government 'does not consider cryptocurrencies legal tender or coin and will take all measures to eliminate use of these crypto-assets in financing illegitimate activities or as part of the payment system'.



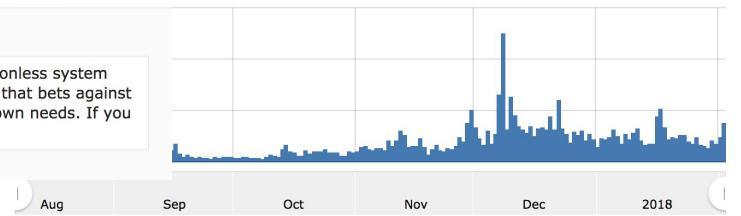
The news comes after the South Korean Government insisted that it would not be banning cryptocurrencies like bitcoin, Ripple and Ethereum, instead suggesting that they will be more heavily regulated.

427
A lot of you forgot why we bought into btc in the first place
(self.Bitcoin)

submitted 10 hours ago by obkenobi13 | reddit for 3 months

Let's remind ourselves here why we bought btc in the first place: a censorship resistant and permissionless system where no fucking institution tells me with whom I am allowed to transact with. This is an investment that bets against a repressive system built and maintained by corrupt governments and corporations that serve their own needs. If you still haven't grasped this then please sell all your coins and GTFO.

253 comments share save hide give gold report crosspost



AUTHOR: GILLIAN CHU

BLOCKCHAIN FUNDAMENTALS LECTURE 2



4 ENTERPRISE BLOCKCHAIN

BLOCKCHAIN FUNDAMENTALS LECTURE 2





4.1

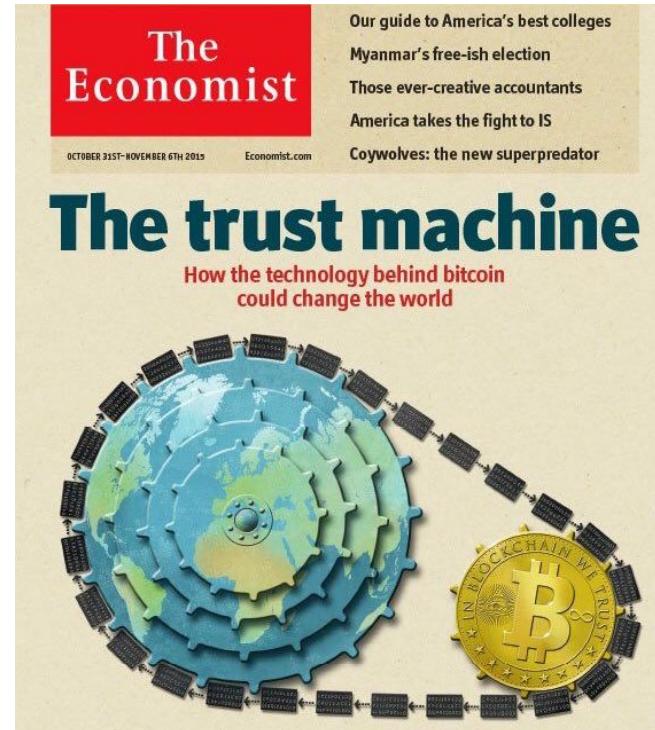
INTEREST IN BLOCKCHAIN FROM BANKS





BANKS & 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



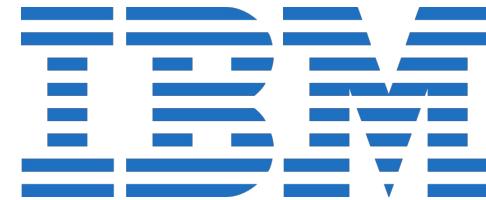
AUTHOR: MAX FANG



PRIVATE BLOCKCHAIN INITIATIVES



J.P.Morgan





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-morgan
jamie-dimon-on-bitcoin-2014-1](http://www.businessinsider.com/jp-morgan-jamie-dimon-on-bitcoin-2014-1)

▲▼
▼▼
▼▼ AUTHOR: MAX FANG



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/5527c91969beddf15404336-480/jp-morgan-chase-and-company-ceo-jamie-dimon.jpg>



AUTHOR: MAX FANG

BLOCKCHAIN FUNDAMENTALS LECTURE 2



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?



AUTHOR: MAX FANG



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



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."



AUTHOR: MAX FANG



DIMON QUOTES ON BITCOIN/BLOCKCHAIN



Aaron Lucchetti

@AaronLucchetti



Jamie Dimon on #bitcoin: I'd fire a JPM trader in a second who traded that. Its against the rules, its stupid, its dangerous.

Oct 20

9:48 AM - Sep 12, 2017

end we

12 22 15

[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."



Jennifer Ablan

@jennablan



JAMIE DIMON: ONE OF MY DAUGHTERS BOUGHT BITCOIN AND IT WENT UP; 'SHE THINKS SHE IS A GENIUS' - CNBC CONFERENCE

11:39 AM - Sep 12, 2017

5 20 48

▲
▼
▼
▼
▼
AUTHOR: MAX FANG



DIMON QUOTES ON BITCOIN/BLOCKCHAIN

January 2018: “The blockchain is real. You can have crypto yen and dollars and stuff like that... The bitcoin to me was always what the governments are gonna feel about bitcoin as it gets really big, and I just have a different opinion than other people.”



AUTHOR: MAX FANG

BLOCKCHAIN FUNDAMENTALS LECTURE 2

Untraceable Electronic Cash † (Extended Abstract)

David Chaum¹ Amos Fiat² Moni Naor³

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

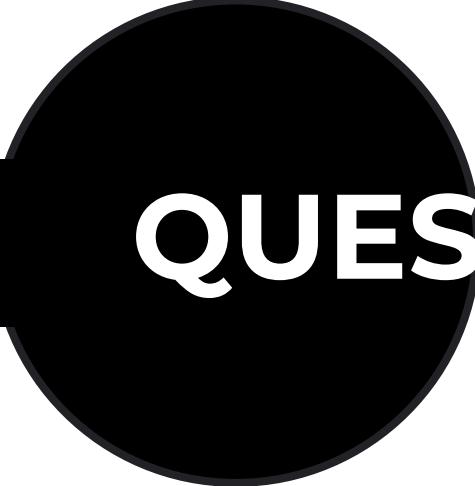
DigiCash™



David Chaum

Photo: Declan McCullagh (2002)





QUESTIONS?





COMMENTS

THE WILD WEST OF THE INTERNET

 [-] **BufferUnderpants** [score hidden] 2 hours ago

 The promise of money multiplying itself for no discernible reason?

 [-] **Auwardamm** 2 points 4 months ago

 Bitcoin needs to become a asset of equivalent value for all other comparable assets before it becomes a currency. Rapid price swings are indicative of it still reaching its true market value. Which imo is orders of magnitude higher than the current price.

Once bitcoin becomes comparable in valuation to that of precious metals, volatility will decrease substantially. The amount of coins held has effectively 0 long term effect other than how quickly we get to such a valuation.

[permalink](#) [embed](#) [save](#) [parent](#) [report](#) [give gold](#) [reply](#)

 [-] **DankLard** reddit for 3 months 3 points 1 month ago

 Today commentor on a TechCrunch article said Bitcoin was created by the Fed so they can steal your money when "the grid goes down"

[permalink](#) [embed](#) [save](#) [report](#) [give gold](#) [reply](#)

 [-] **PopCultureNerd** [S] 2 points 1 month ago

 I should email BitCoin and ask to see if BitCoin is hiring.

[permalink](#) [embed](#) [save](#) [report](#) [give gold](#) [reply](#)



AUTHOR: GILLIAN CHU

BLOCKCHAIN FUNDAMENTALS LECTURE 2



4.2

BITCOIN COMMUNITY & POLITICS

BLOCKCHAIN FUNDAMENTALS LECTURE 2



COMMUNITY

WHERE DOES THE COMMUNITY EXIST?



bitcointalk.org



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

AUTHOR: ANDREW TU

BLOCKCHAIN FUNDAMENTALS LECTURE 2





POLITICS

- Internal politics
- Right-wing extremism?
- Libertarianism



BITMAIN



BTCChina

BLOCKCHAIN FUNDAMENTALS LECTURE 2

BitFury



AUTHOR: ANDREW TU

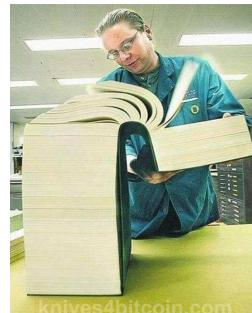


CONTROVERSIAL TOPICS

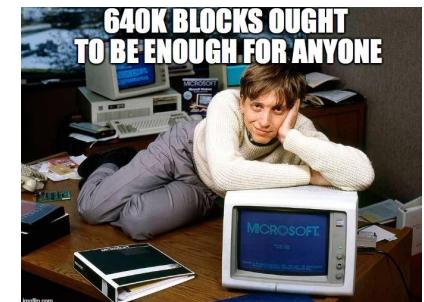
In the US government, we try to best represent all of our citizens' best interests and opinions.

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? (What is Segwit2x)?
- Confirmation Times?
- Centralization in third party companies?

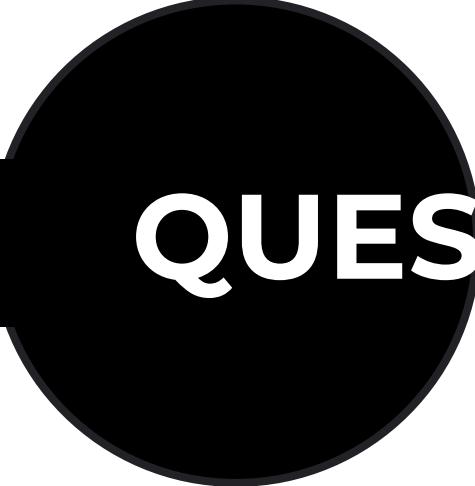


The Bitcoin block size debate is now available in this convenient paperback



AUTHOR: GILLIAN CHU

BLOCKCHAIN FUNDAMENTALS LECTURE 2



QUESTIONS?





5

TOKENS OF TODAY

BLOCKCHAIN FUNDAMENTALS LECTURE 2



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 (think Kickstarter)
- VCs trending worried

Bancor ICO \$150million

Tezos ICO \$200 million

Filecoin ICO \$253 Million



Filecoin

AUTHOR: APARNA KRISHNAN

Bancor

BLOCKCHAIN FUNDAMENTALS LECTURE 2



ICOs

DOING WHAT YOU WANT

**Invitro Investing**

@invitreus

[Follow](#)

95% of Americans are not allowed by law to invest in start-ups. Only ‘accredited investors’ are entitled to do so, but you can buy lottery tickets all you want or go to Las Vegas to gamble. 🤔

1:35 PM - 30 Jan 2018

71 Retweets 125 Likes



14



71



125



AUTHOR: GILLIAN CHU

BLOCKCHAIN FUNDAMENTALS LECTURE 2



EXPLOSION OF ALTCOINS



Litecoin



ZCash



Stellar



Peercoin



Dogecoin



DASH



Monero



Ripple

◀ ▶

▼ ▲

AUTHOR: GLORIA ZHAO

BLOCKCHAIN FUNDAMENTALS LECTURE 2



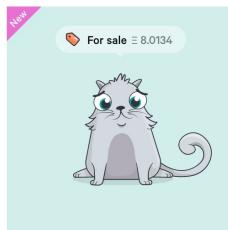
CRYPTOKITTIES

THE HYPE

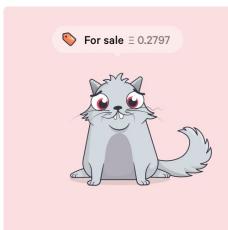
For Sale Siring Gen 0 All Kitties

Search Kitties...

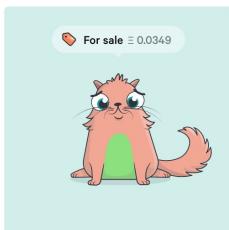
Youngest first



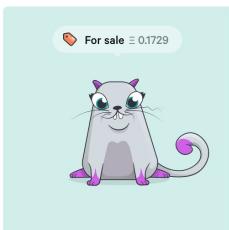
Kitty 183192 · Gen 0
Fast



Kitty 183167 · Gen 2
Swift



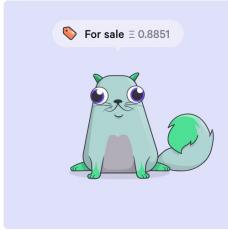
Kitty 183096 · Gen 4
Swift



Kitty 183070 · Gen 5
Swift



Kitty 183049 · Gen 5
Swift



Kitty 183048 · Gen 3
Swift



Kitty 183020 · Gen 4
Swift

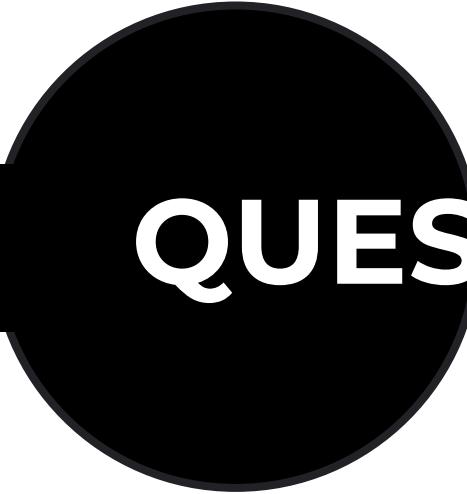


Kitty 183017 · Gen 4
Swift



AUTHOR: BRIAN HO

BLOCKCHAIN FUNDAMENTALS LECTURE 2



QUESTIONS?





HOMEWORK/READINGS

All this information will be made available at blockchain.berkeley.edu/decal, through email, and on Piazza.

Required Readings:

1. A Cypherpunk's Manifesto by Eric Hughes
 - o <https://www.activism.net/cypherpunk/manifesto.html>
2. Coindesk: A Bot Named Willy: Did Mt. Gox's Automated Trading Pump Bitcoin's Price?
 - o <https://www.coindesk.com/bot-named-willy-did-mt-goxs-automated-trading-pump-bitcoin-price>
3. The DAO, The Hack, The Soft Fork and The Hard Fork
 - o <https://www.cryptocompare.com/coins/guides/the-dao-the-hack-the-soft-fork-and-the-hard-fork/>

Extra Readings:

- (to get ahead) Princeton Textbook 1.1 Cryptographic Hash Functions (pages 23-31)
- [All You Need to Know About ICOs](#)
- [Digital Gold](#) by Nathaniel Popper



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/>

