

Bitcoin, Cryptocurrencies, and Blockchain Technology

Dr. Gina C. Pieters

Trinity University-Department of Economics, San Antonio, Texas, USA

University College London-Centre for Blockchain Technology, London, UK

Dallas Chapter of the National Association for Business Economics

March 16, 2018

My Interest as an International Economist:

The underlying technology (Blockchain) is fascinating. Allows us to connect the world in a way that we could not previously. Has implications for

- Financial Contagion
 - i.e. The Global Crash of 2008
- Global financial risk-sharing
 - Global asset reduces investment ties to domestic stock market
 - Entrepreneurship funding
- Criminal Activity
 - Money Laundering and Payment
 - Asylum-seekers/refugee wealth
- Monetary Policy

(Notice that getting-rich-quick is not on this list)

A few preliminaries

- Yes, I have purchased Bitcoin (and Ethereum, and Litecoin, and many more).
- Yes, I currently hold some (fractions) of Bitcoin (and Ethereum, and Litecoin, and many more)
- Yes, I buy/sell on Coinbase. And GDAX. And Kraken. And Bittrex. And a few more exchanges.

I am studying the system of cryptocurrencies. I need to understand how it works, not just how it is reported to work.

- No, I will not give you investment advice.
- No, I will not evaluate your ICO.
- No, I will not tell you whether your business needs to invest in/buy blockchain.

Layout

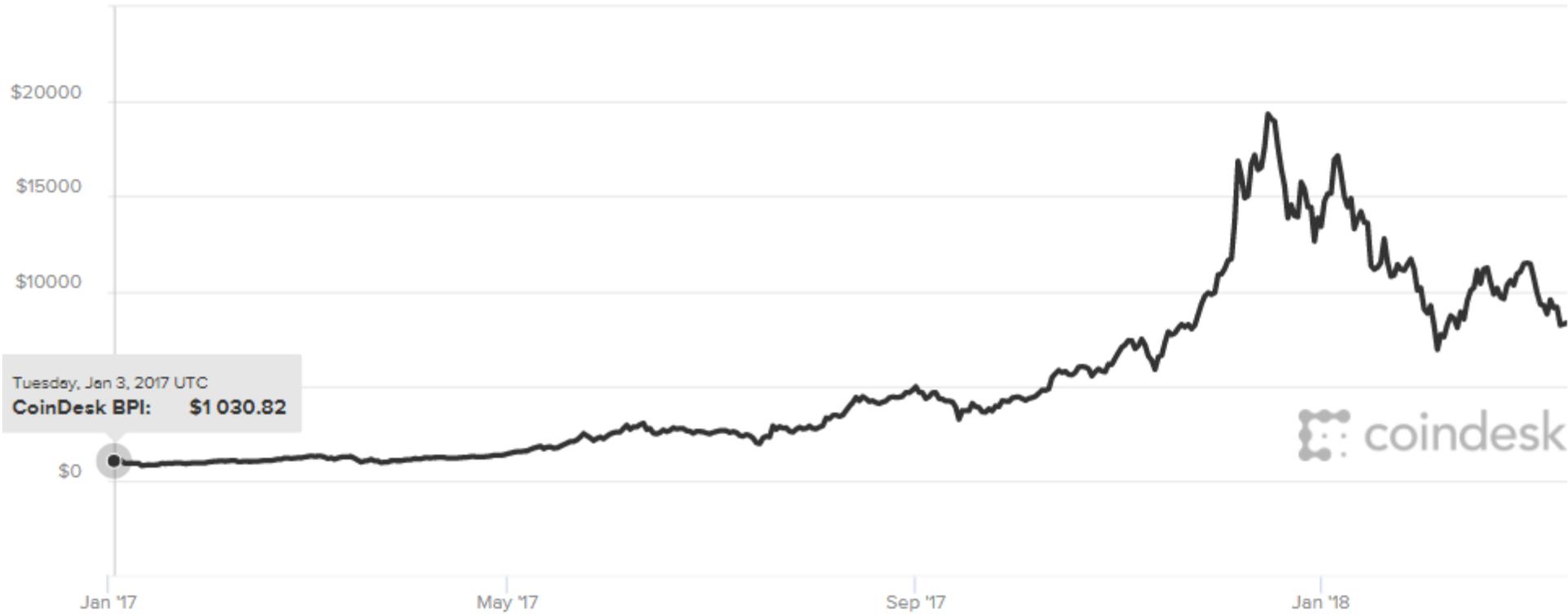
1. A Sense of Scale (and Hype)
2. The History of Digital Currencies
3. The Technology (Blockchain)
4. Cryptocurrencies
5. ICO's

Bitcoin (USD) Price

Closing Price OHLC

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

2017-01-01 to Mar 16, 2018 [Export](#)



\$8,314.97 ▲ 0.70%

Today's Open	\$8,256.99	Change	▲ \$57.98
Today's High	\$8,329.93	Market Cap	\$0.141T
Today's Low	\$8,256.99	Supply	16,921,313

Global Charts

Total Market Capitalization

Zoom 1d 7d 1m 3m 1y YTD ALL

From 2016-12-29 To Mar 15, 2018

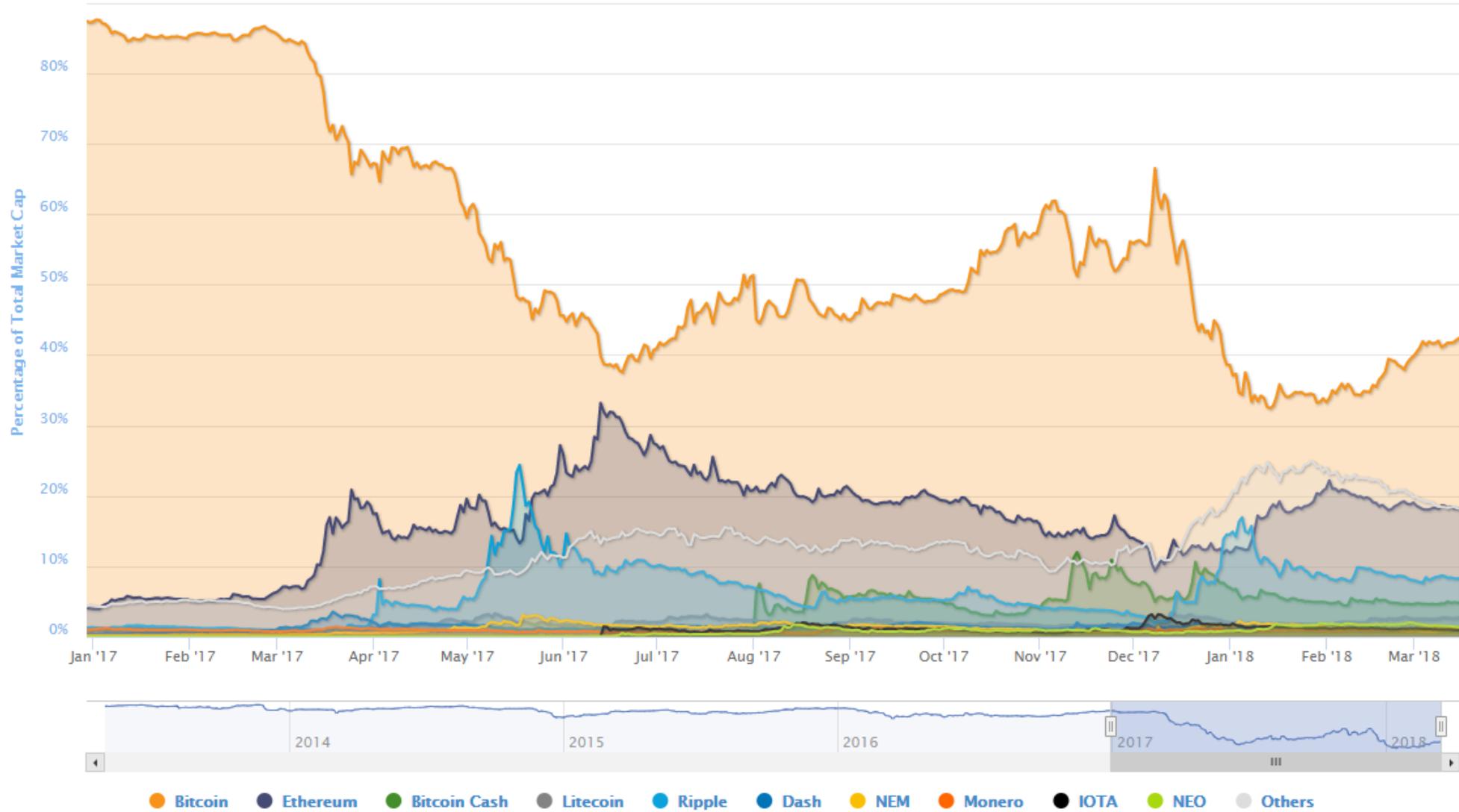


Source: coinmarketcap.com

Percentage of Total Market Capitalization (Dominance)

Zoom 1d 7d 1m 3m 1y YTD ALL

From 2016-12-29 To Mar 15, 2018



The History of Digital Currencies

- *Electronic money* is a broad term for any money, currency or asset not held in physical form---it can include representations of a sovereign currency or claims on a real-world good. (PayPal)
- *Digital currency* is a subset of electronic money that has no broadly accepted physical counterpart. (Online gaming: WoW gold, EVE Online ISK)
- *Virtual currency* is a subset of digital currency that is intentionally created, or predominately used, for purchasing both digital and non-digital goods in a non-contained economy. (Bitcoin)

Technical Challenge: With no physical equivalent, how do you verify ownership and validity of transactions to prevent "copy-and-paste" spending? (Counterfeiting)

The History of Digital Currencies

Solutions to Verification Problem

VISA, American Express, etc. (electronic money)

- Running total is associated with your account.

Online gaming currency (simulated currencies)

- Value associated with user account. All transactions should only occur on within-game servers.

E-gold (early virtual currency)

- Founded in 1996. E-gold was a digitally traded currency backed by gold that could be traded for sovereign currencies, with the issuance and trading system managed by the company Gold & Silver Reserve.
 - Shut down in 2009 due to legal issues.

Bitcoin, Ethereum, etc. are *Decentralized Virtual Currencies*.

- Satoshi Nakamoto's breakthrough was the **blockchain**: a solution to the verification problem that did not require a single entity verifying transactions at its center.

The Technology: Blockchain Ledger

Imagine a giant Excel spreadsheet in the sky that everyone can read and write on, maintaining a history of all transactions (a ledger).

	A	B	C	D
1	Sender	Amount	Recipient	
2	A	10 BTC	B	
3	B	4.5 BTC	C	
4	C	3.5 BTC	D	
5	C	1 BTC	A	
6	etc	etc	etc	
7				

A jumble of unique numbers and letters: The “public key” that identifies your “wallet”.

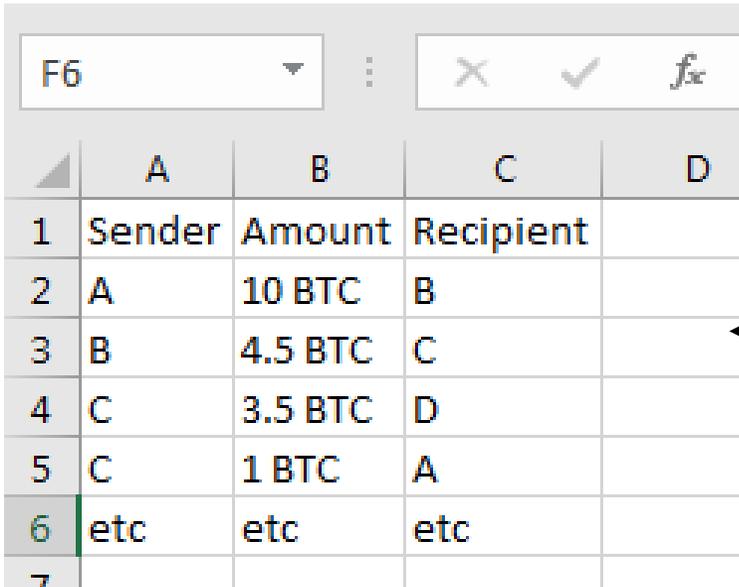
Every Bitcoin transaction is COMPLETELY PUBLIC. It’s only anonymous if your public key is not linked to your identity. (more on this later)

FYI: Ledgers are very ancient (and established) systems of recording transactions. This was not the innovation. It’s the “Giant-Speadsheet-In-The-Sky” part¹.

¹This visualization comes from Susan Athey, an economics professor at Stanford University.

The Technology: Blockchain Ledger

Imagine a giant Excel spreadsheet in the sky that everyone can read and write on, maintaining a history of all transactions (a ledger).



	A	B	C	D
1	Sender	Amount	Recipient	
2	A	10 BTC	B	
3	B	4.5 BTC	C	
4	C	3.5 BTC	D	
5	C	1 BTC	A	
6	etc	etc	etc	
7				

Assuming B began with 0 BTC, now has:

- +10 BTC (from A)
- -4.5 BTC (to C)
- =5.5 BTC

Assuming C began with 0 BTC, now has:

- +4.5 BTC (from B)
- -4.5 BTC (to A and D)
- =0 BTC

If everyone can “read” the ledger, then everyone can verify whether or not you have sufficient funds for a transaction...IF the ledger is correct.

The Technology: Blockchain

- If everyone can read it, then everyone can verify whether you have sufficient funds to engage in a transaction.
- But who gets to write entries in ledger? Why can't I make an entry and then delete it to return my money to myself?
- The full ledger is downloaded onto every computer that has signed up to verify and record Bitcoin transactions.
 - The Incentive to be a Bitcoin Ledger Keeper (Accountant): The first node to correctly compile the most recent block 10-minute batch of transactions is paid 12.5 newly created Bitcoin by the Bitcoin algorithm.
 - Must be compatible with past records (the chain of blocks---the Blockchain).
 - Must solve a cryptographic puzzle
 - The puzzle gets harder or easier to maintain the 10 minute solution time. This is part of what is called "Proof of Work".
 - These accountants are called "Miners".

Block #513709

Summary	
Number Of Transactions	884
Output Total	10,522.48211423 BTC
Estimated Transaction Volume	916.60769833 BTC
Transaction Fees	0.05491949 BTC
Height	513709 (Main Chain)
Timestamp	2018-03-16 00:56:44

Viewable version of Bitcoin's Blockchain
Source: <https://blockchain.info/>

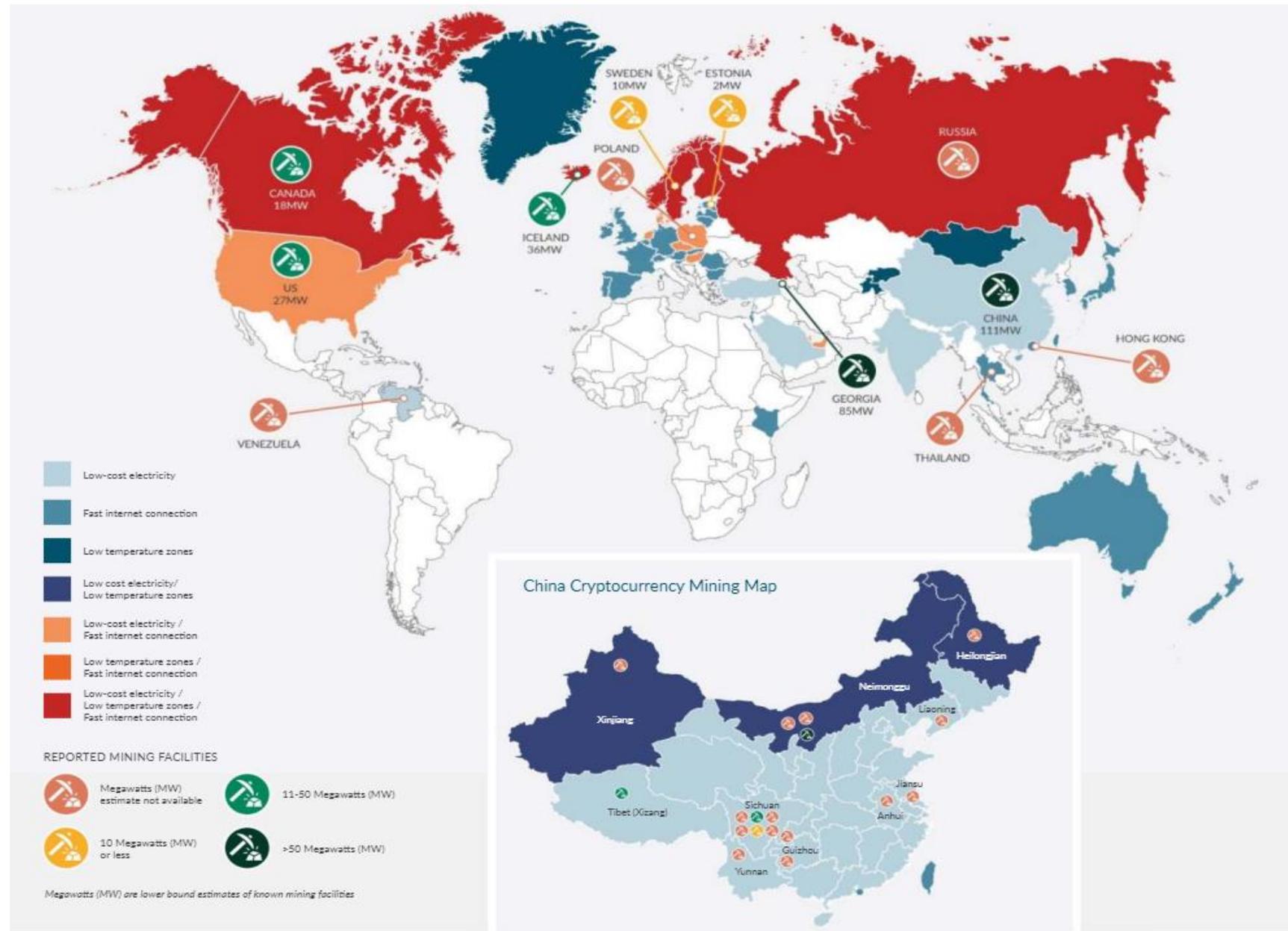
- Received Time
- Relayed By
- Difficulty
- Bits
- Size
- Weight
- Version
- Nonce

Transactions

09a514e9e282fa8f1a60b8df9883eecd5811bcac9ed27023736203839e2b600		2018-03-16 00:56:44
No Inputs (Newly Generated Coins)	 1AM2fYfpY3ZeMeCKXmN66haoWxvB89pJUx Unable to decode output address 3G7y14BudP2a4kjPAuecg4iUKM84GgPPWb	12.4293703 BTC 0 BTC 0.12554919 BTC
		12.55491949 BTC
b76ad255fcdfd8d04ae023517e102058ce13a3bb5e5b0b7a01a529b20db8ece3		2018-03-16 00:55:50
1FKkMKGGWSrpC8JfekZ7Rfv1qkeALRAWXf	 14wf6zooiid2KgXjvY9gpmbzr7wgdwUhfYm	0.14078278 BTC
		0.14078278 BTC
c14f13b29c3c5a6308f59353468a55d2c2812f7b060b0f93c57a513e92d0ad87		2018-03-16 00:54:01
1Q7GqKEYdDPK5vSn1WYhmsm5sntOxLHtt	 1CniTZeA13AnfKTWNiRvzm5uaeCFH8VwG	0.01235509 BTC

Anyone, anywhere in the world, can be miner, you just need to download the software.

HOWEVER you only get paid if you are the FIRST to complete the block: a computing power arms race.



Live Map:
<https://bitnodes.earn.com/nodes/live-map/>

Source: Global Cryptocurrency Benchmarking Study, University of Cambridge

Cryptocurrencies

- Thus far: Blockchain is a way of storing, recording, and viewing data that doesn't require a centralized transaction verifier or record keeper.
- Bitcoin is the oldest cryptocurrency: a virtual money with transactions recorded on a decentralized blockchain.
- Digital money recorded to a decentralized blockchain is not owned by any individual or company; and can be spent anywhere: a "Global Currency"
 - There is an active, but technical, debate about whether a centralized blockchain is a "true blockchain" or a "glorified database".
- Examples of other popular cryptocurrencies
 - Ethereum (ETH): Designed for dApps (Decentralized Applications). Can use Ethereum's blockchain to launch your own crypto. Not the same as Ethereum Classic (ETC).
 - Ripple (XRP): Designed for bank-to-bank transfers.
 - Litecoin (LTC), Bitcoin Cash (BCH), Decentralized Cash (DASH): Variants of BTC, different blockchain programming.

Cryptocurrencies

- Many buy Bitcoin or similar cryptocurrencies on intermediate markets called exchanges. This is not necessary but is easy.
- Coinmarketcap.com lists 9,386 exchanges; and 1,564 cryptocurrencies.
- Purchases occur 24/7 using a variety of currencies using blockchain. (The blockchain never closes)
- Exchanges are tied to a physical location.
- Effectively impossible to restrict access to exchanges (online only, no global regulatory system)
 - Using an exchange can link your identity to your account number, causes interesting price premiums around the world. [Pieters and Vivanco, 2017]

Example of an Exchange: ANXBTC

(no longer accessible/not an endorsement)

BUY/SELL

Please enter the transaction amount below

Available Funds	
USD	0
BTC	0

BUY BTC SELL BTC

Amount

QUOTE PRICE

QUICK TIPS

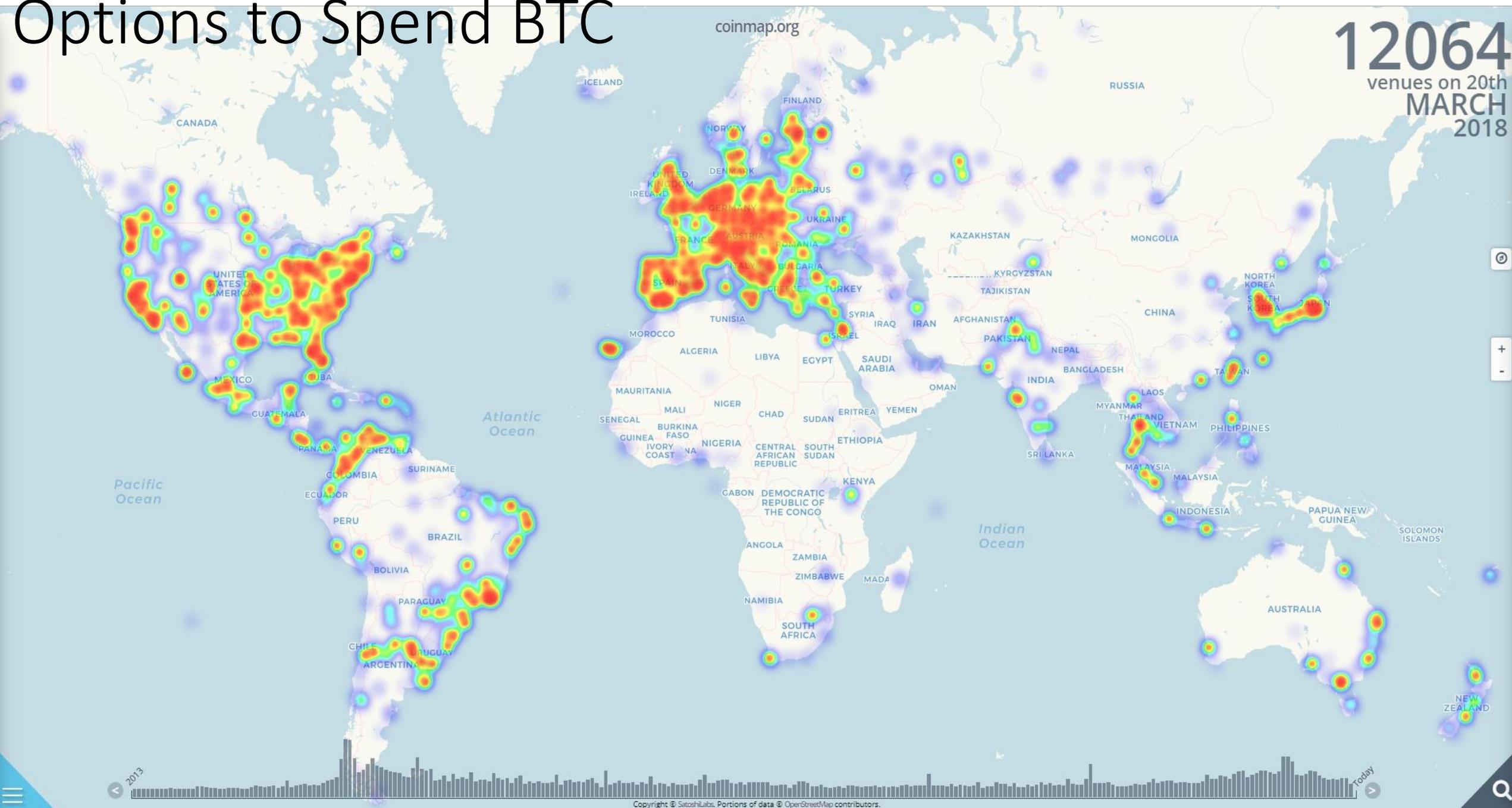
Buying and selling Bitcoins is easy! Once you have your account set up, you can start buying or selling Bitcoins. More instructions are available at [\[link\]](#)

Options to Spend BTC

coinmap.org

12064

venues on 20th
MARCH
2018



Options to Withdraw Cash

(i) To Bank Account

WITHDRAW FUNDS

Bank Account Bank Wire Coinbase Account **BTC Address**

AMOUNT (MAX) DESTINATION
0.00 BTC BTC address

Enter a BTC address and the amount you wish to transfer from your GDAX trading account. BTC transfers are free and fast.

Two Factor Code
000000 [Get Code](#)

Enter the verification code generated by the Google Authenticator or Authy app. Alternatively, click [Get Code](#) to have the code sent to your phone via SMS.

[Withdraw funds](#)

YOUR LIMITS

Daily Withdrawal Limit Used
\$0 of \$10,000

[Apply](#) for higher withdrawal limits

PROCESSING TIME

BTC network transfers are fast and free

(iii) On location

Sell bitcoins for cash near Moscow, RU

Buyer	Distance	Location	Price/BTC	Limits	
iPresident (1000+; 97%)	0 km	Moscow, Russia	166956.80 RUB	Any amount	Sell
AlfaCash-in (3000+; 100%)	0 km	Moscow, Russia	145807.43 RUB	150000 - 100000000 RUB	Sell
shgn (3000+; 100%)	0 km	Moscow, Russia	159215.00 RUB	10000 - 100000 RUB	Sell
salamgorjestan (3000+; 99%)	1.5 km	Moscow, Russia	169496.38 RUB	650000 - 6500000 RUB	Sell
slonopay (21; 100%)	1.5 km	Moscow, Russia	165168.16 RUB	50000 - 400000 RUB	Sell

[Show more on map for selling bitcoins for cash](#)

(ii) To A Prepaid Card

bitpay

Accept Bitcoin Wallet **Card** Help Log In Activate [Order](#)

Load dollars using any bitcoin wallet, spend anywhere

The BitPay Card is one of the fastest, easiest ways to turn your bitcoin into dollars. Apply now in under 2 minutes.

[Order Now](#) [How it works](#)

bitpay

4000 1234 5678 9010

VALID THRU 01/21

SATOSHI NAKAMOTO

VISA

Initial Coin Offerings (ICO's)

Blockchain has the potential to speed up transactions, decrease vulnerability to record manipulation.

- FinTech
- Healthcare

- ICO: Initial Coin Offering. Creating a new coin (altcoin).
 - New spin on blockchain technology
 - New application of blockchain technology
 - New business idea
 - NEW.

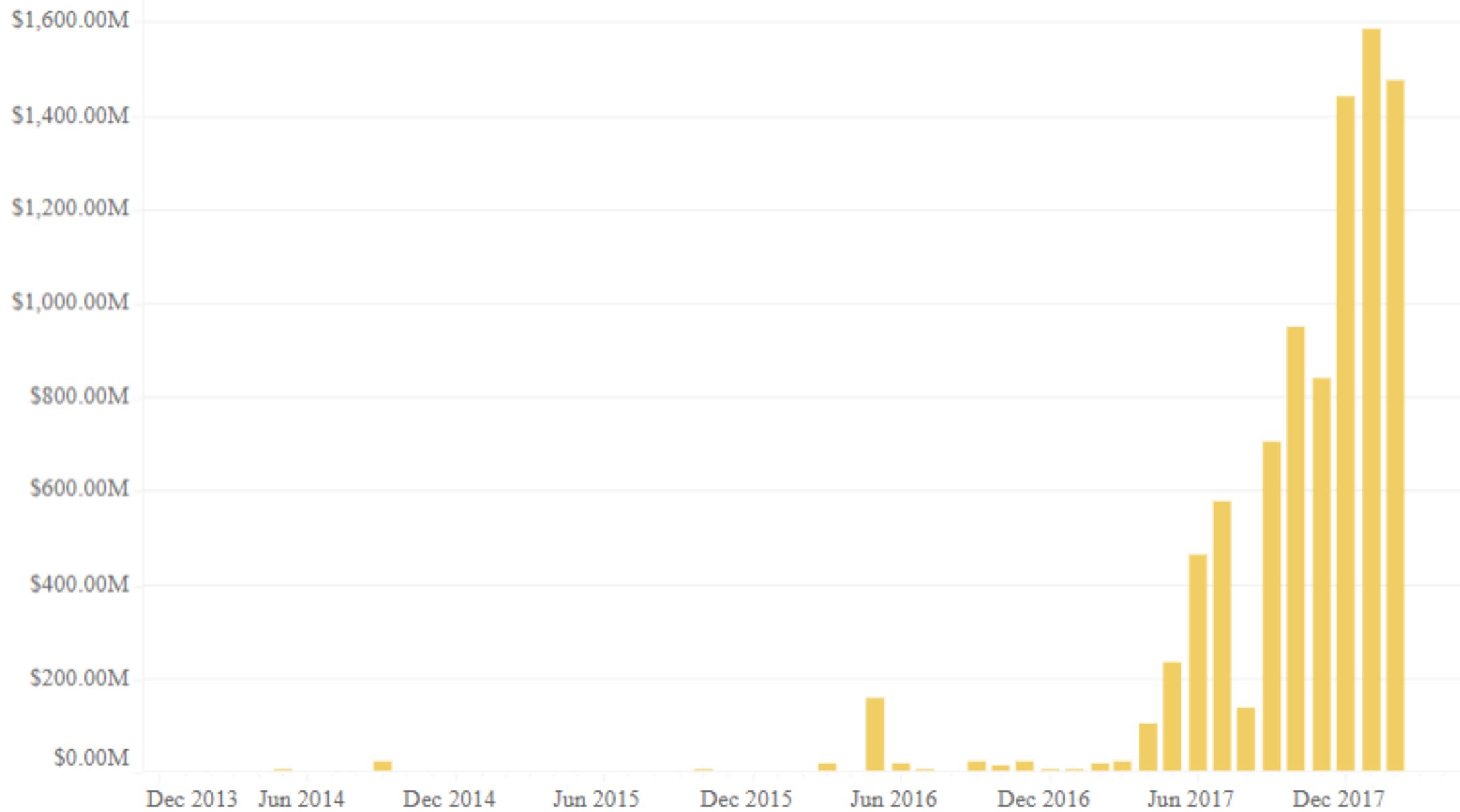
- Current state is somewhat like the Internet and web-pages in the late 90's/early 00's.

- Example: WhopperCoin: A cryptocurrency set up by Burger King in Russia. Each whopper purchase gives the consumer a coin, 1700 coins can be traded in for one whopper. (Yes, this is a customer loyalty program). (August 29, 2017)

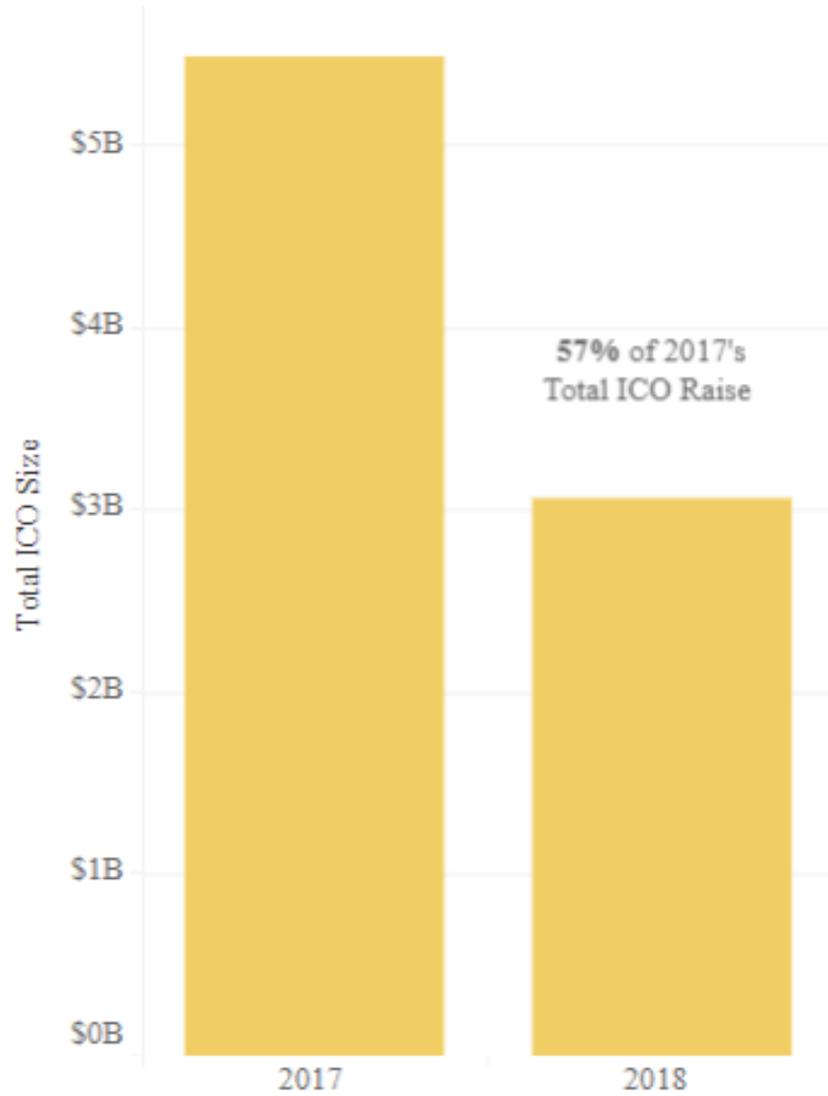
All-Time Cumulative ICO Funding



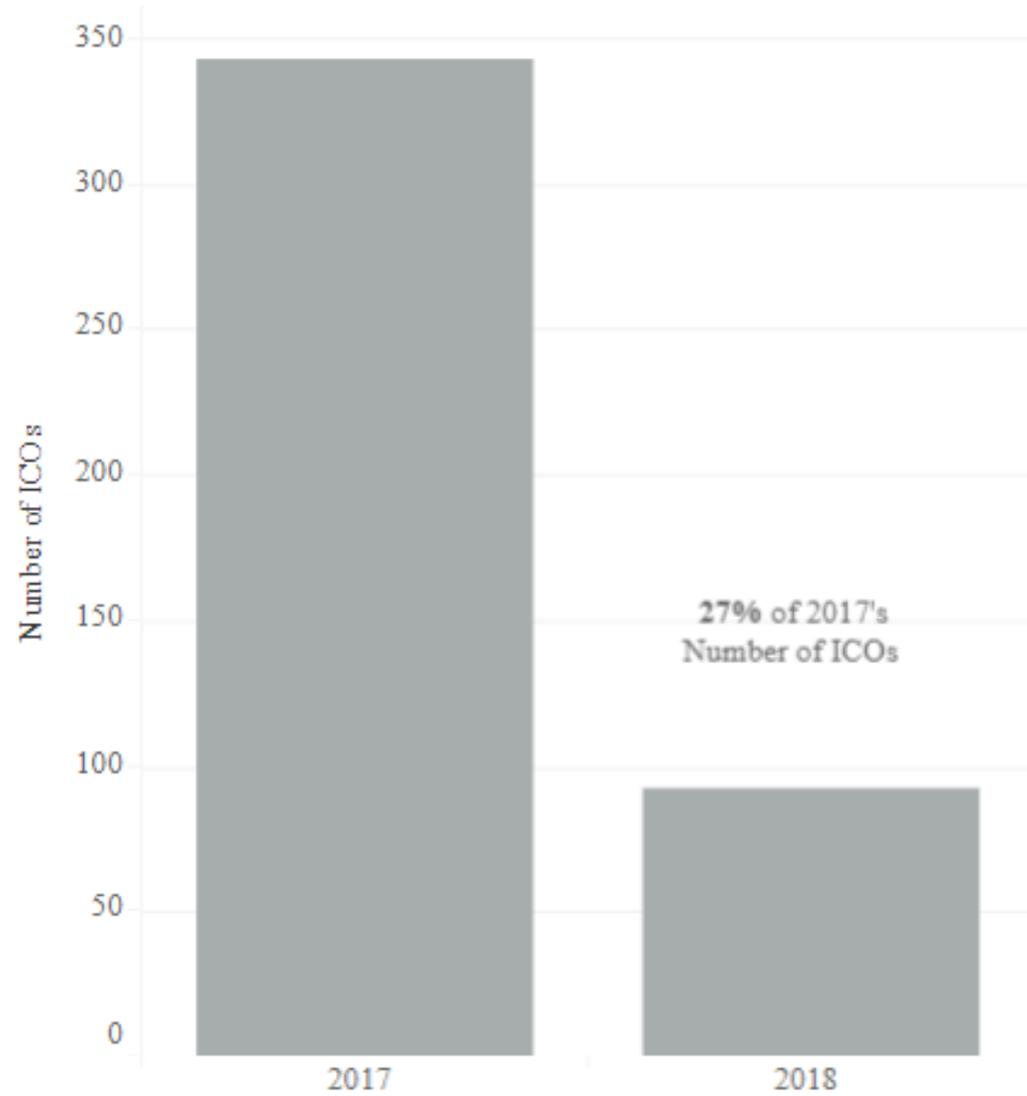
Monthly New ICO Funding



Total ICO Size



Number of ICOs



Thank you!

Contact Information

- Email: prof.pieters@gmail.com
- Website: www.ginapieters.com
- Twitter: @prof_pieters (crypto, international economics, and opinions)