UNIVERSITY of HAWAI'I®
MAUI COLLEGE

Module 2 – Introduction to Cryptocurrencies

Debasis Bhattacharya, JD, DBA
University of Hawaii Maui College
debasisb@Hawaii.edu
@uhmcabit
maui.hawaii.edu/cybersecurity

Currencies - Online Transactions

- Physical cash
  - Non-traceable (well, mostly!)
  - Secure (mostly)
  - Low inflation
- Fiat Currency – legal tender whose value is backed by a government
  - Note that since 1971, the US$ has no backing with gold!
  - Cryptocurrencies are not fiat currencies!
- Physical currencies can’t be used online directly

➢Electronic credit or debit transactions

- ◆Bank sees all transactions
- ◆Merchants can track/profile customers
- ◆Cryptocurrencies are not associated with any bank or regulatory agency!

Bitcoin

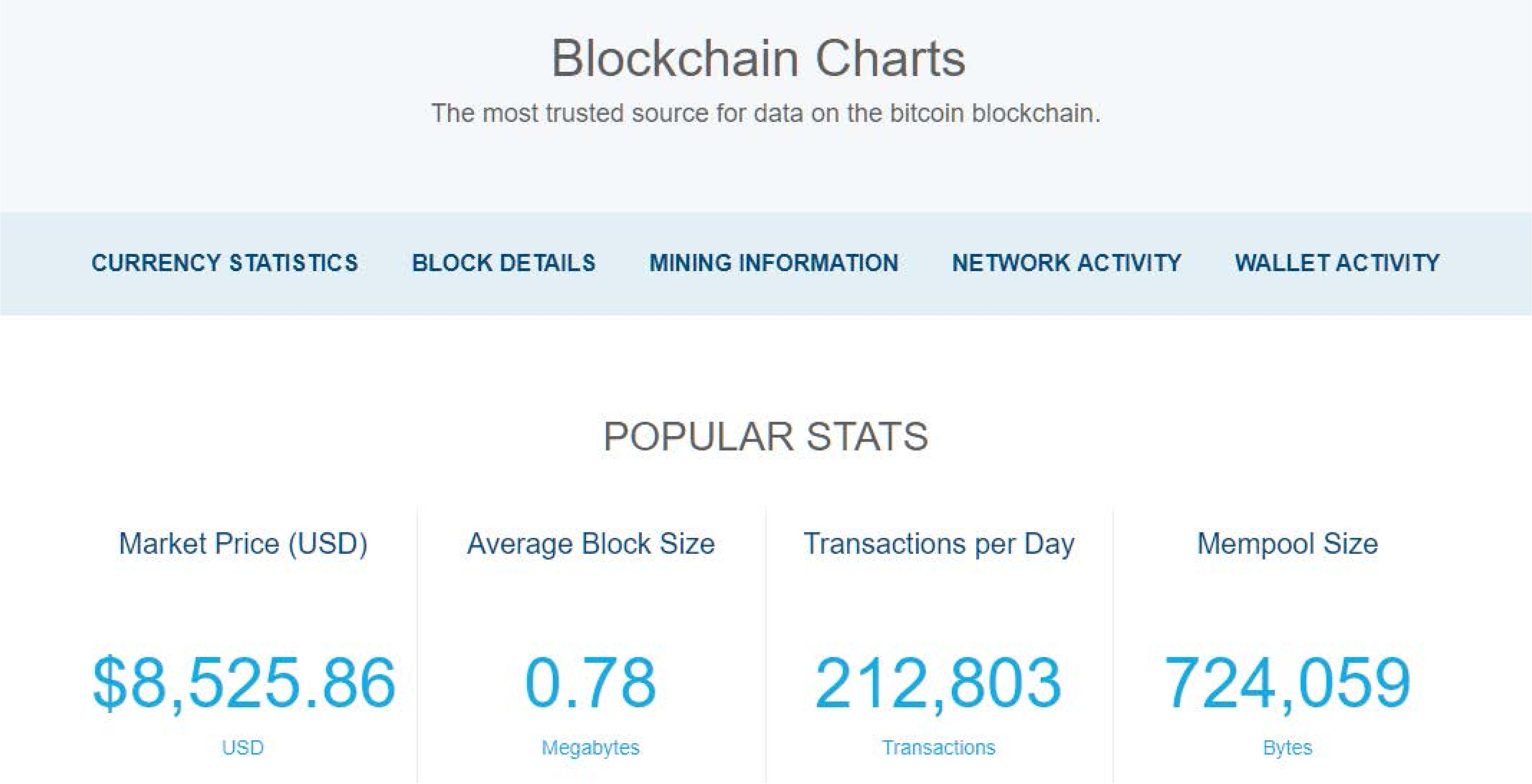
- A distributed, decentralized digital currency system
- Released by Satoshi Nakamoto 2008
- Effectively a bank run by an ad hoc network
    - Digital checks
    - A distributed transaction log

Size of the BitCoin Economy

- Number of BitCoins in circulation ~17 million (April 8, 2018)
- Total number of BitCoins generated cannot exceed 21 million.
  - Around 4 million left to be mined!
- Average price of a Bitcoin:
  - $8,522 in May 15, 2018
  - $7,149 in April 8, 2018
  - $18,000 in December, 2017
  - $3,867 on September 25, 2017;
  - $2,350 on June 27, 2017

  □ Price has been very unstable and speculative.
- Currently, 244,157 tx/day or ~170 tx/minute.
  (In contrast, Visa transaction 200,000 per minute!)

Bitcoins – All Charts as of Sunday May 15, 2018

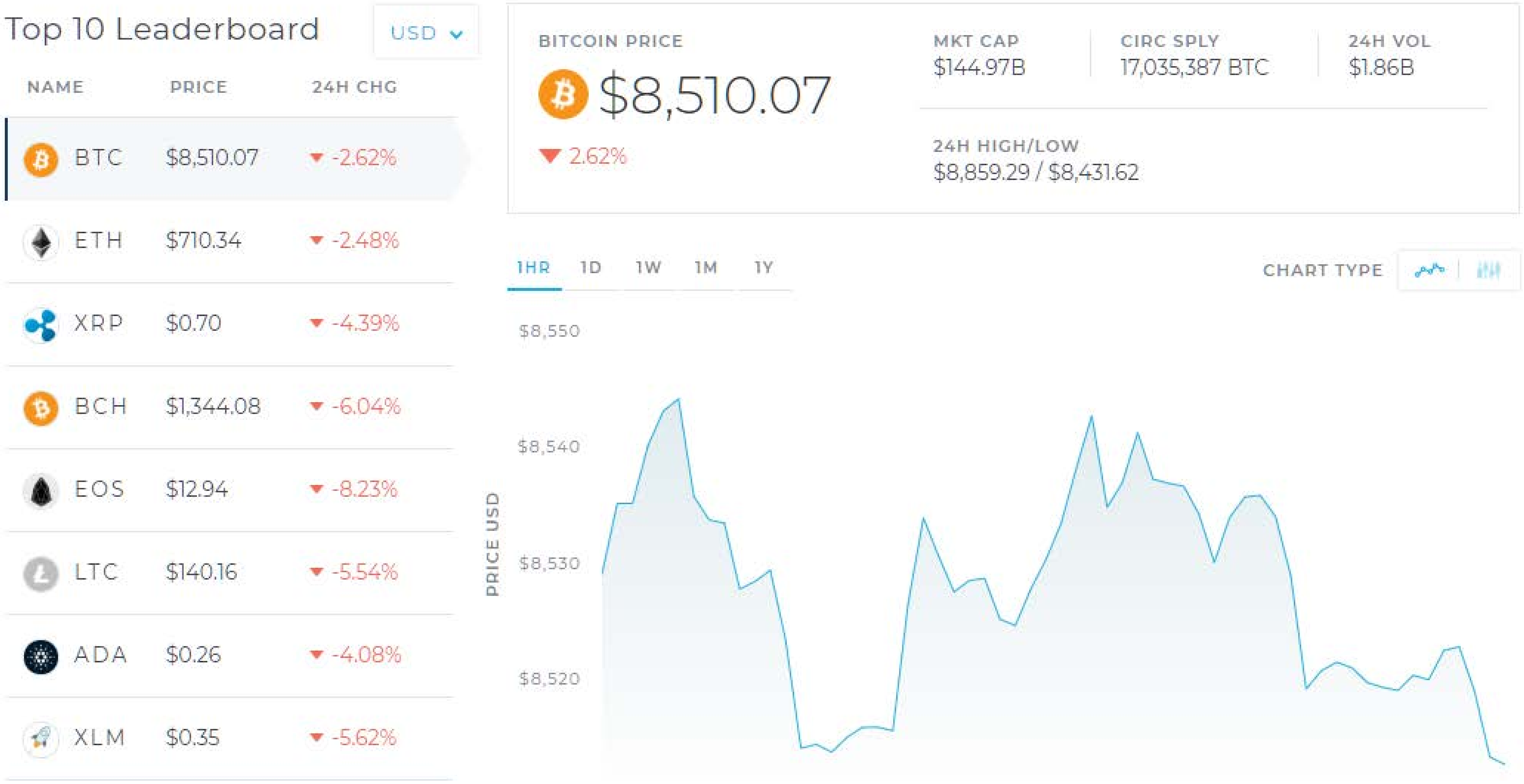


Blockchain Charts

The most trusted source for data on the bitcoin blockchain.

POPULAR STATS

Market Price (USD)	Average Block Size	Transactions per Day	Mempool Size
$8,525.86	0.78	212,803	724,059
USD	Megabytes	Transactions	Bytes



Top 10 Leaderboard

USD

NAME	PRICE	24H CHG
BTC	$8,510.07	▼ -2.62%
ETH	$710.34	▼ -2.48%
XRP	$0.70	▼ -4.39%
BCH	$1,344.08	▼ -6.04%
EOS	$12.94	▼ -8.23%
LTC	$140.16	▼ -5.54%
ADA	$0.26	▼ -4.08%
XLM	$0.35	▼ -5.62%

BITCOIN PRICE
$8,510.07
▼ 2.62%

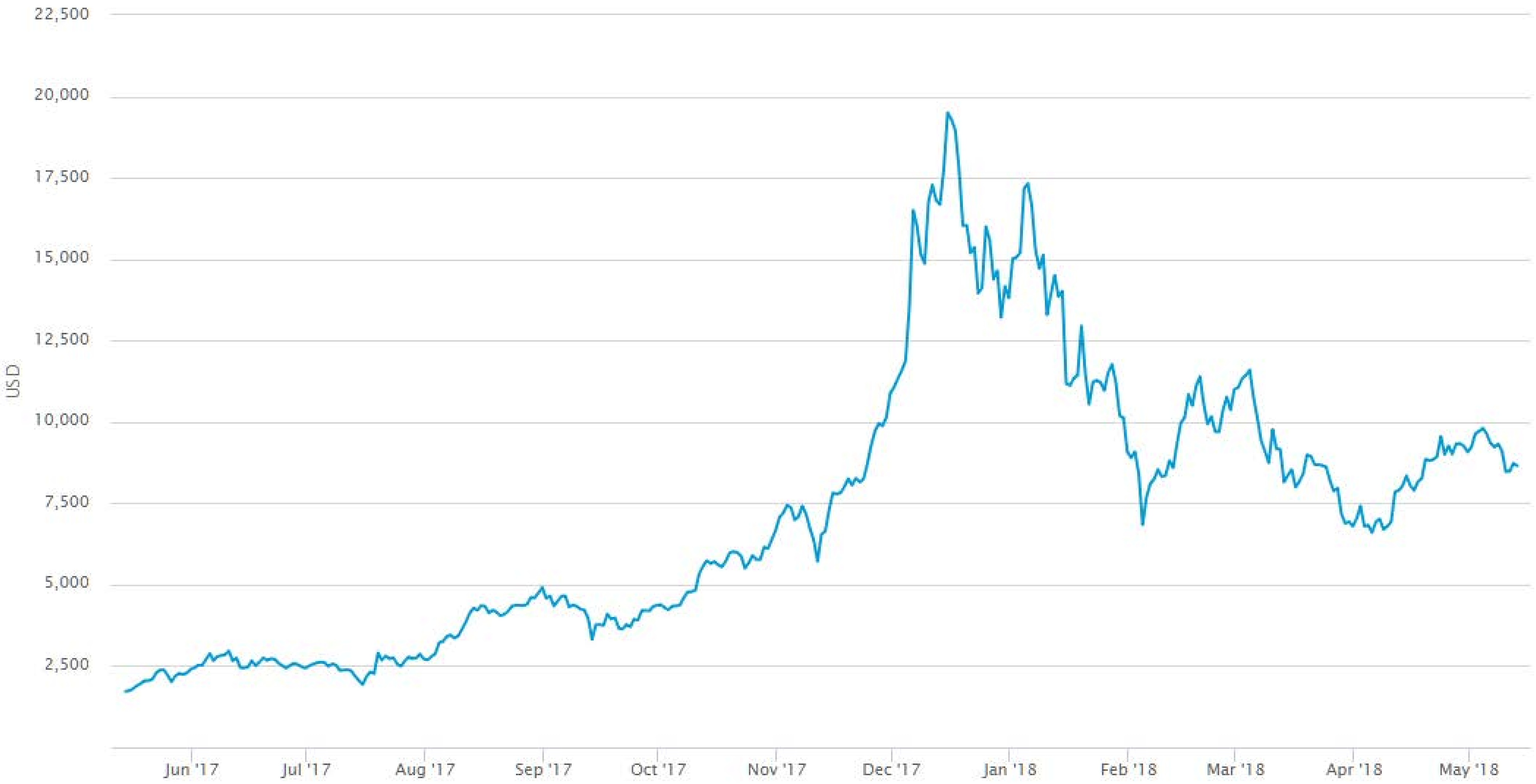
MKT CAP
$144.97B

CIRC SPLY
17,035,387 BTC

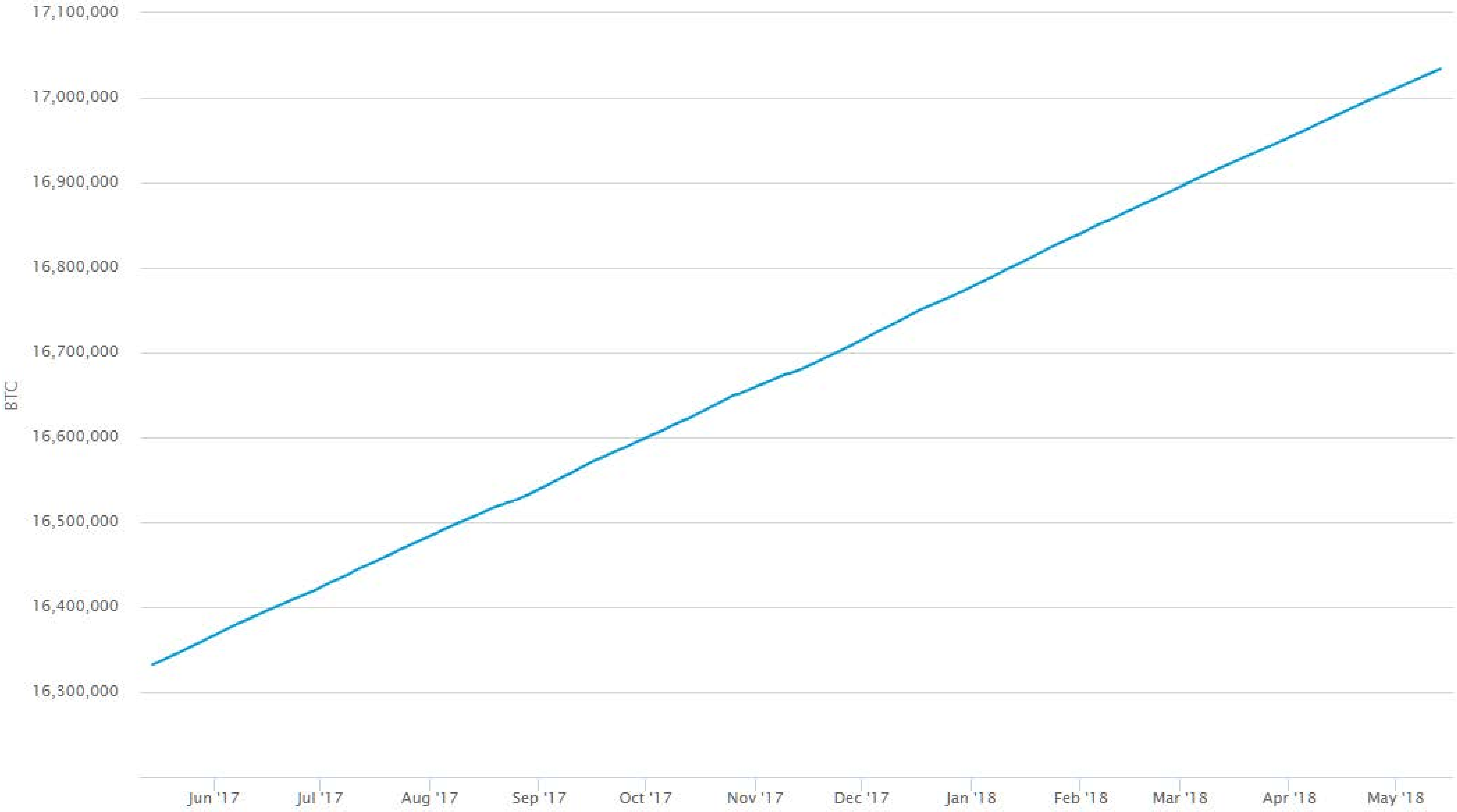
24H VOL
$1.86B

24H HIGH/LOW
$8,859.29 / $8,431.62

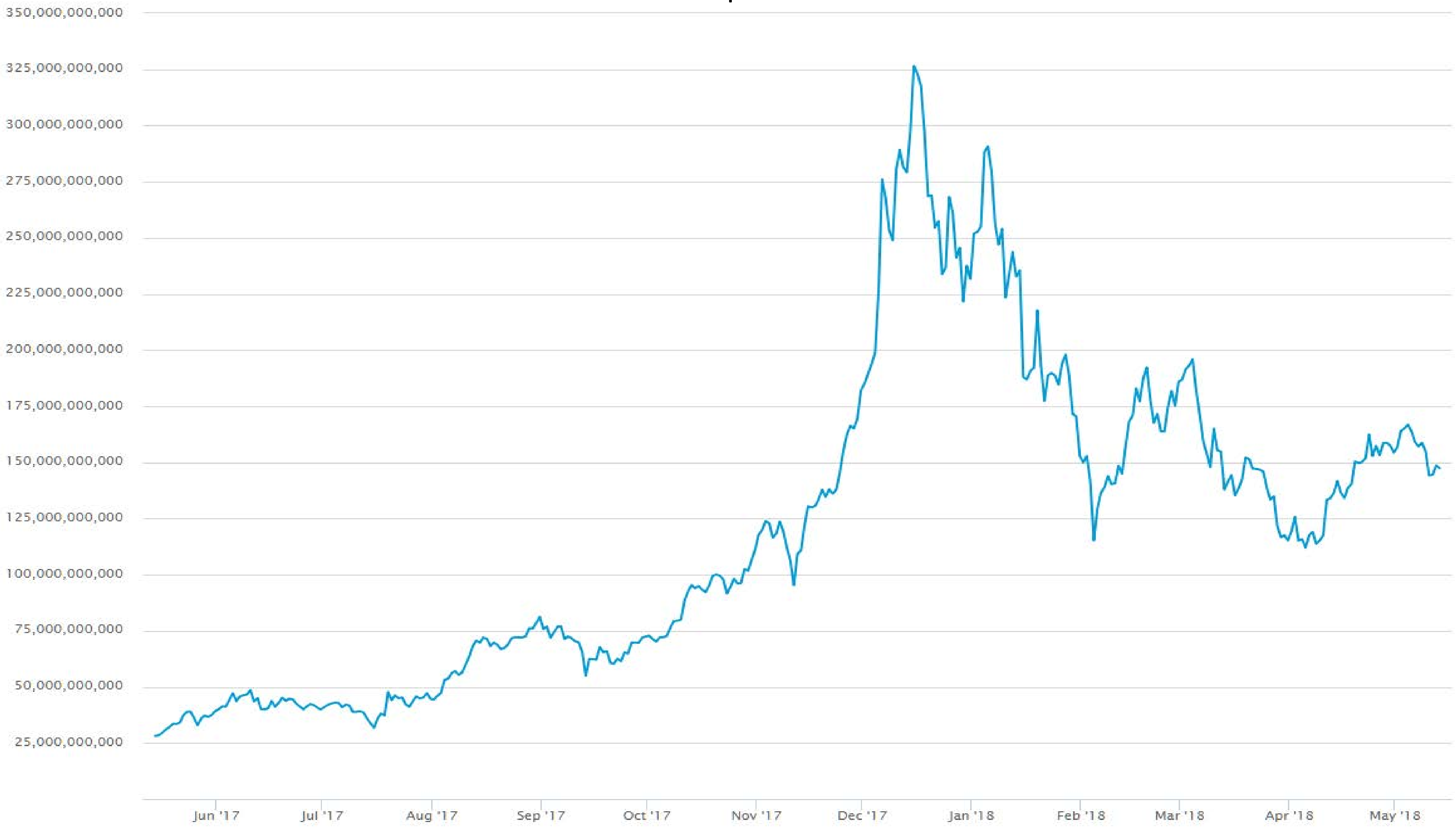
Bitcoins – Average price since June 2017

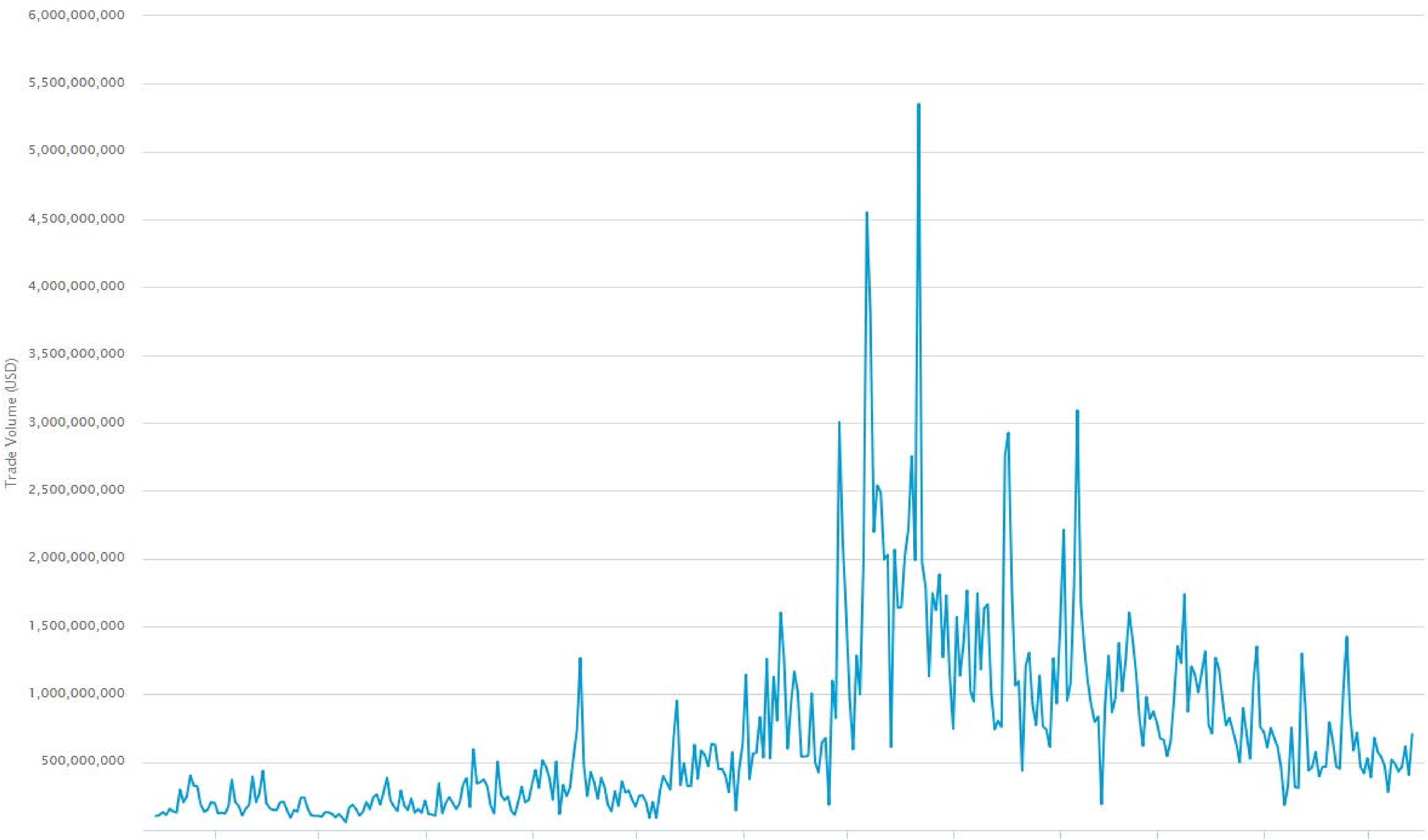


Bitcoins in Circulation – May 2018



Market Capitalization





USD Exchange Trade Volume

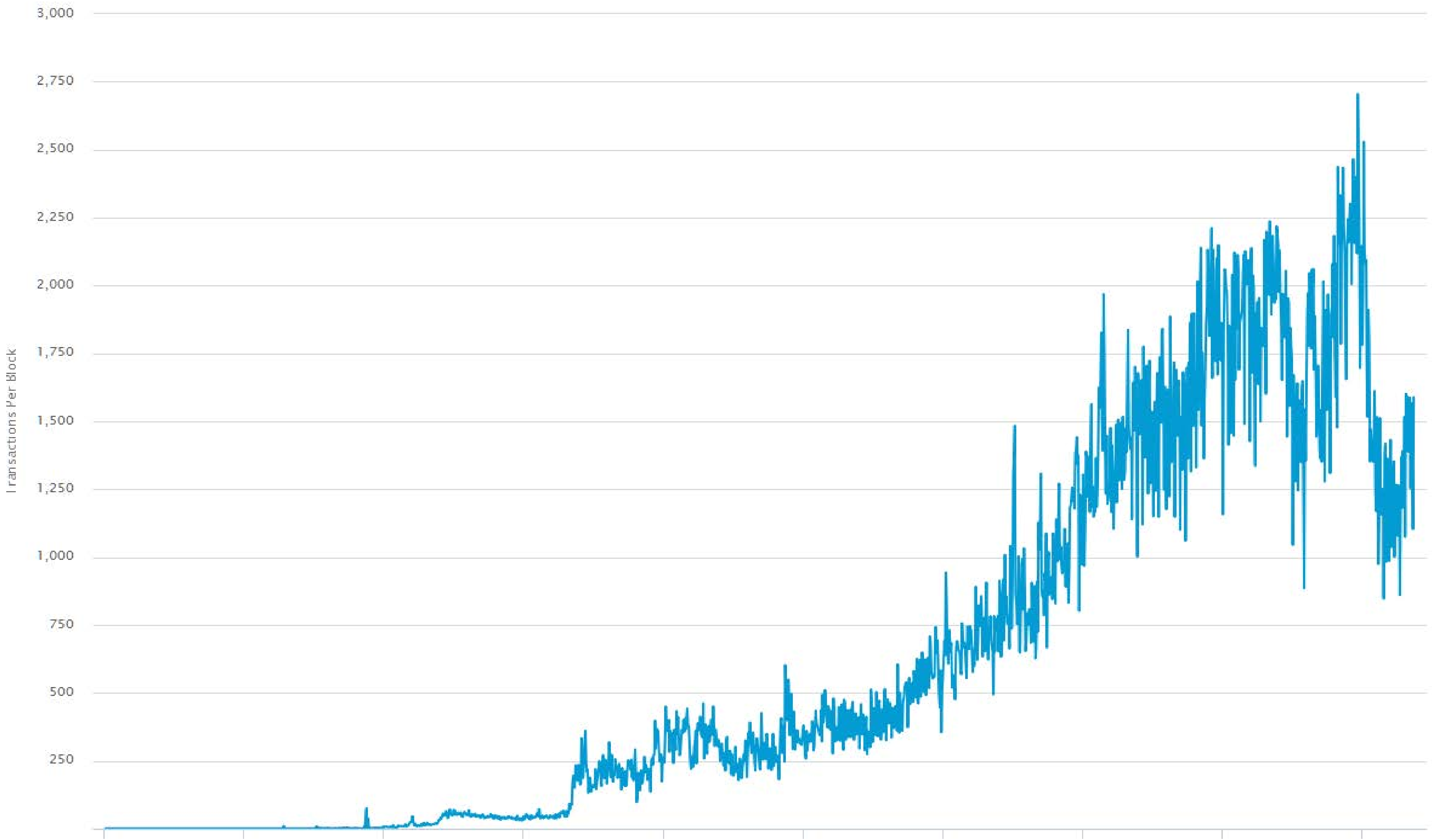
The total USD value of trading volume on major bitcoin exchanges.

Source: blockchain.info

Average Number Of Transactions Per Block

The average number of transactions per block.

Source: blockchain.info



BitCoin: Challenges

- Creation of a virtual coin/note
    - How is it created in the first place?
    - How do you prevent inflation? (What prevents anyone from creating lots of coins?)
- Validation
    - Is the coin legit? (proof-of-work)
    - How do you prevent a coin from double-spending?
- Buyer and Seller protection in online transactions
    - Buyer pays, but the seller doesn’t deliver
    - Seller delivers, buyer pays, but the buyer makes a claim.
- Trust on third-parties
    - Rely on “proof of work” instead of trust
    - Verifiable by everyone – blockchain is visible to all
    - No central bank or clearing house

Security in Bitcoin

- Authentication
  - Am I paying the right person? Not some other impersonator?
- Integrity
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability
  - Can I make a transaction anytime I want?
- Confidentiality
  - Are my transactions private? Anonymous?

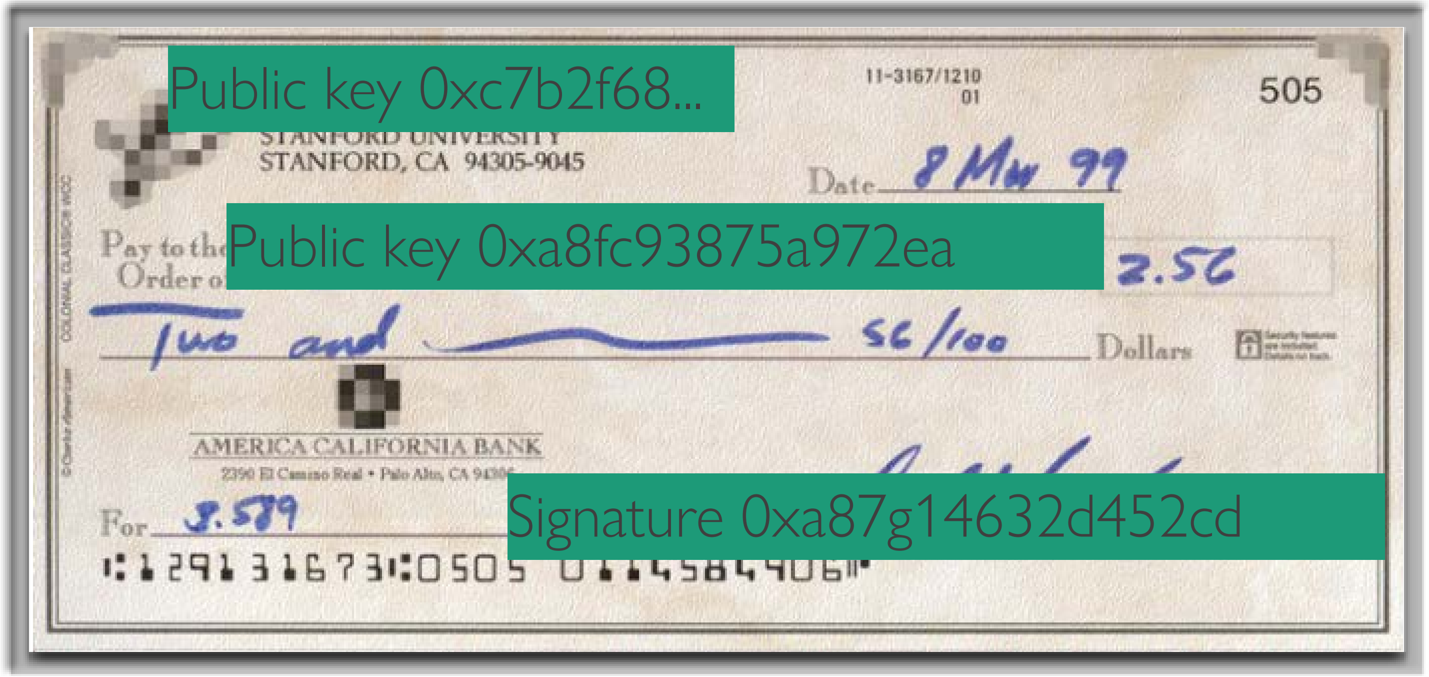
Security in Bitcoin

- Authentication → Public Key Crypto: Digital Signatures
  - Am I paying the right person? Not some other impersonator?
- Integrity → Digital Signatures and Cryptographic Hash
  - Is the coin double-spent?
  - Can an attacker reverse or change transactions?
- Availability→ Broadcast messages to the P2P network
  - Can I make a transaction anytime I want?
- Confidentiality→ Pseudonymity
  - Are my transactions private? Anonymous?

Back to BitCoin

- Validation
  - Is the coin legit? (proof-of-work) → Use of Cryptographic Hashes
  - How do you prevent a coin from double-spending? → Broadcast to all nodes
- Creation of a virtual coin/note
  - How is it created in the first place? → Provide incentives for miners, earn bitcoins after work!
  - How do you prevent inflation? (What prevents anyone from creating lots of coins?) → Limit the creation rate of the BitCoins. Right now, 12.5 coins to miners

Bitcoin Transactions



Public key 0xc7b2f68...

STANFORD UNIVERSITY
STANFORD, CA 94305-9045

11-3167/1210
01

505

Date 8 Mar 99

Pay to the Order of Public key 0xa8fc93875a972ea

2.56

Two and 56/100 Dollars

AMERICA CALIFORNIA BANK
2390 El Camino Real • Palo Alto, CA 9430

For 8.589

Signature 0xa87g14632d452cd

Bitcoin Network

- Each P2P node runs the following algorithm:
  - New transactions are broadcast to all nodes.
  - Each node (miners) collects new transactions into a block.
  - Each node works on finding a proof-of-work for its block. (Hard to do. Probabilistic. The one to finish early will probably win.)
  - When a node finds a proof-of-work, it broadcasts the block to all nodes.
  - Nodes accept the block only if all transactions in it are valid (digital signature checking) and not already spent (check all the transactions).
  - Nodes express their acceptance by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Practical Limitation

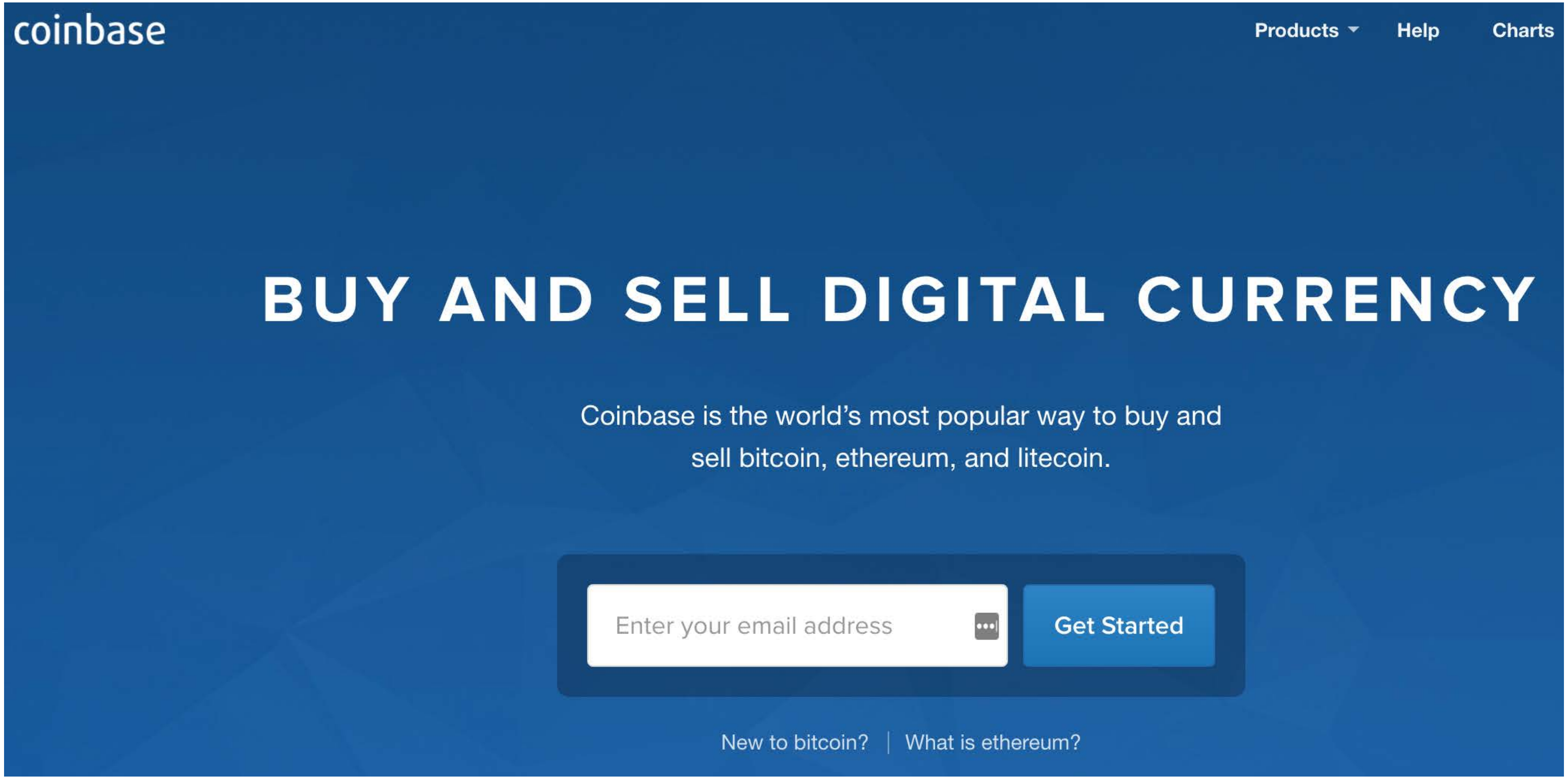
- At least 10 mins to verify a transaction.
  - Agree to pay
  - Wait for one block (10 mins) for the transaction to go through.
  - But, for a large transaction ($$$) wait longer, around 60 minutes. Because if you wait longer it becomes more secure.
  - For large $$$, you wait for six blocks (1 hour).

BitCoin Economics

- Rate limiting on the creation of a new block
  - Adapt to the "network's capacity"
  - A block created every 10 mins (six blocks every hour)
    - How? Difficulty is adjusted every two weeks to keep the rate fixed as capacity/computing power increases
- N new Bitcoins per each new block: credited to the miner → incentives for miners
  - N was 50 initially. In 2013, N=25
  - Since 2016 N = 12.5, next half is June 2020 for N = 6.25.
  - Halved every 210,000 blocks (every four years)
  - Thus, the total number of BitCoins will not exceed 21 million. (After this miner takes a fee)

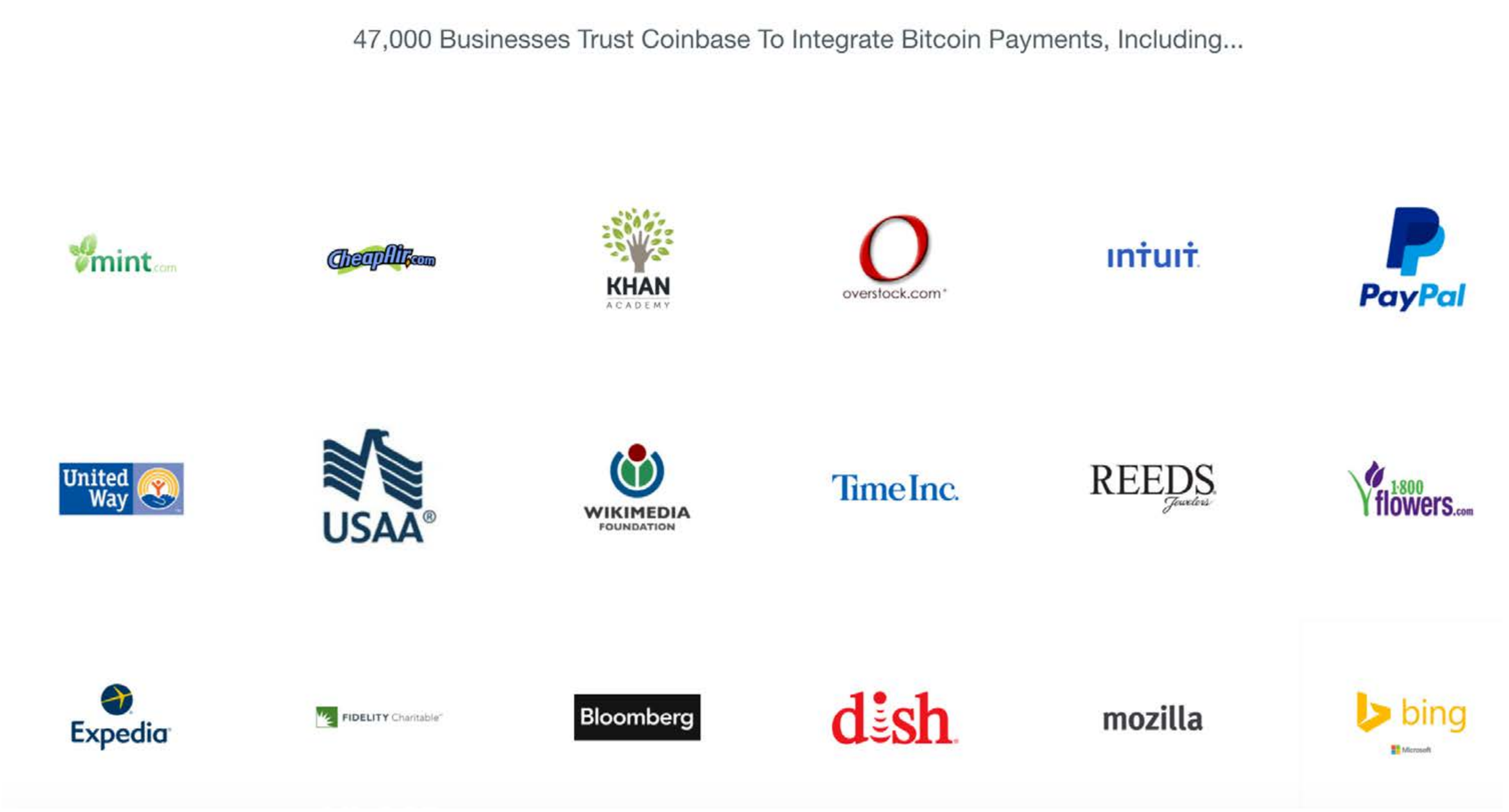
Privacy Implications

- No anonymity, only pseudonymity
- All transactions remain on the block chain– indefinitely!
- Retroactive data mining
  - Target used data mining on customer purchases to identify pregnant women and target ads at them
    (NYT 2012), ended up informing a woman's father that his teenage daughter was pregnant
  - Imagine what credit card companies could do with the data

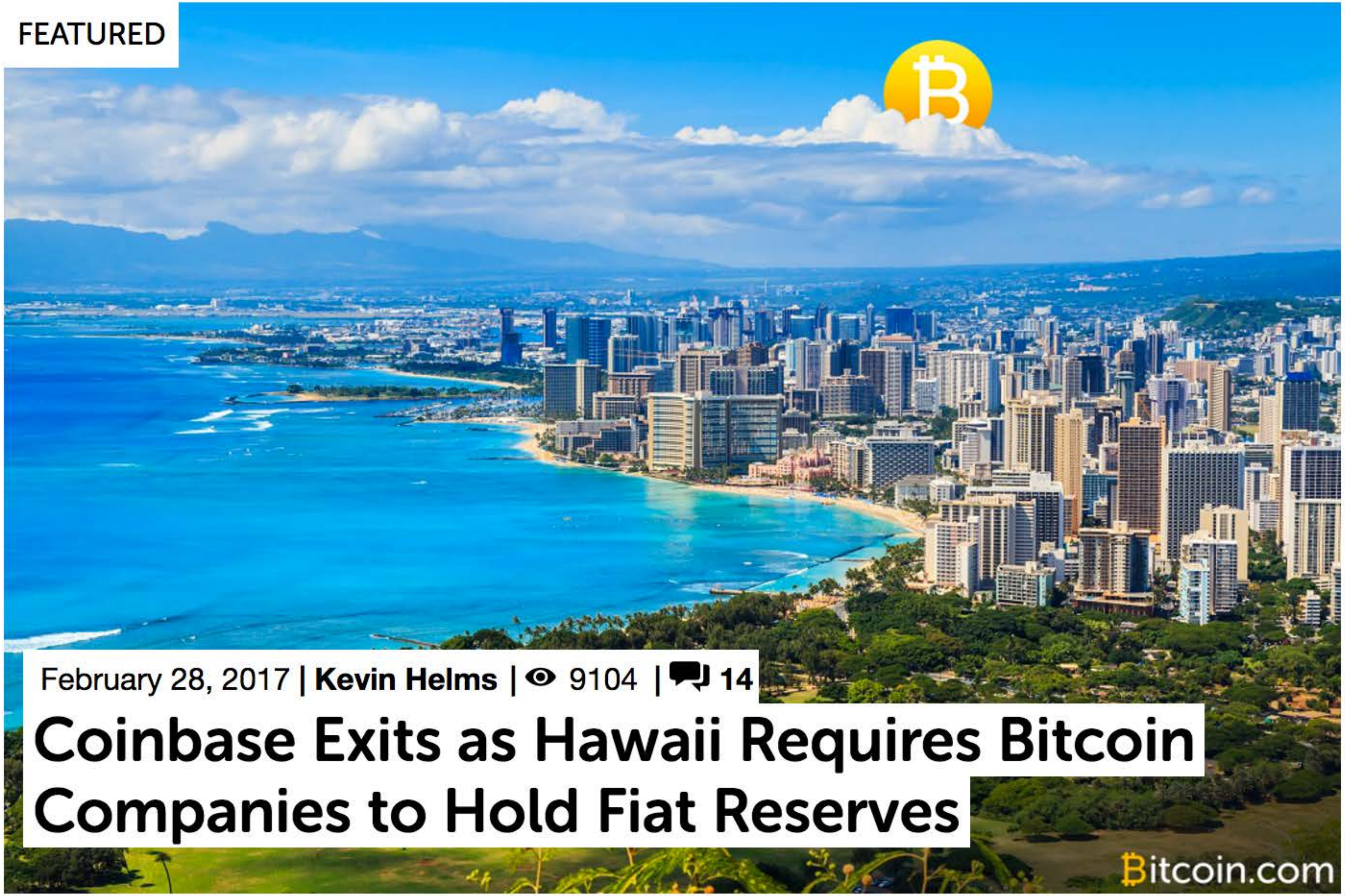


BUY AND SELL DIGITAL CURRENCY

Coinbase is the world's most popular way to buy and sell bitcoin, ethereum, and litecoin.



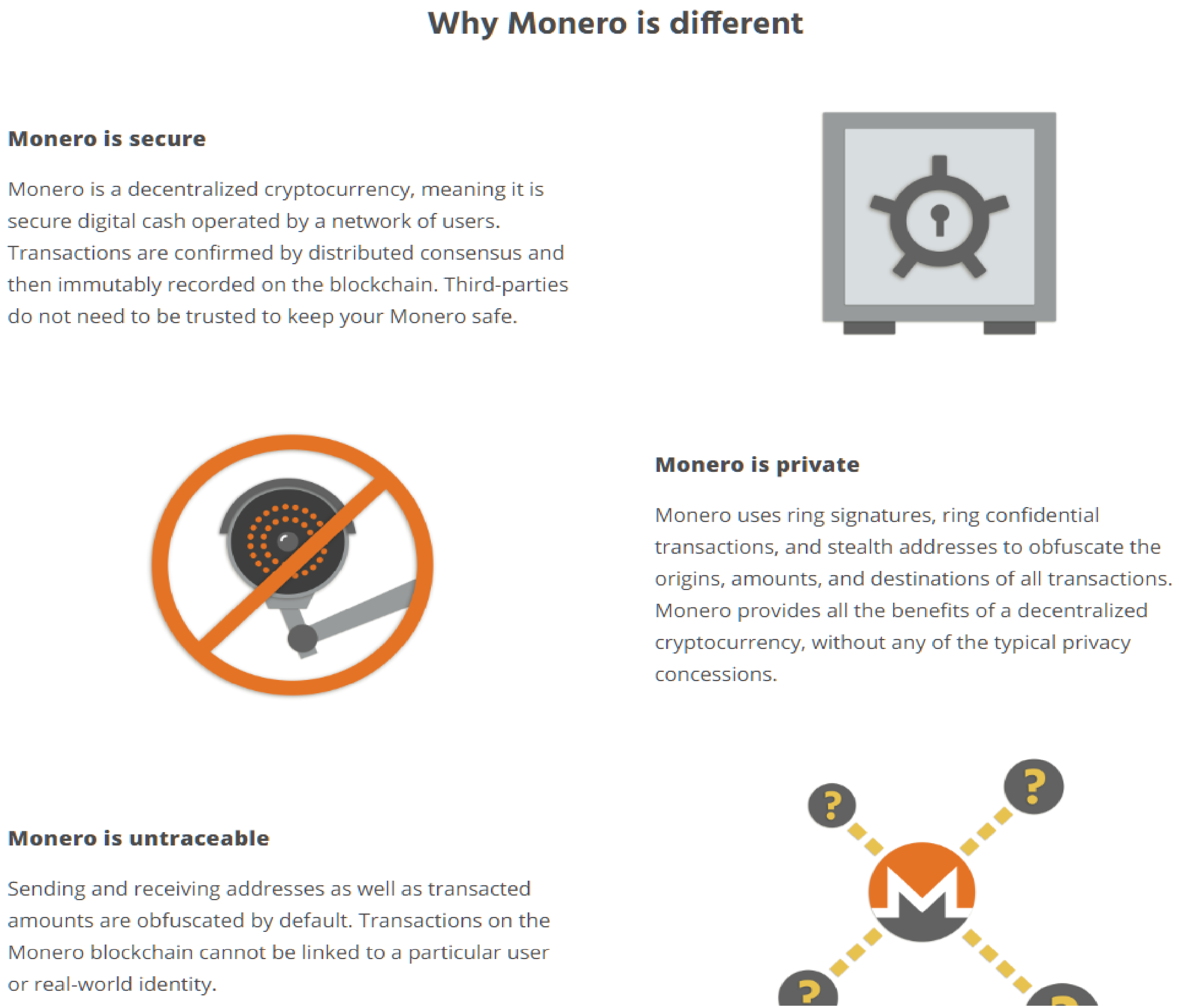
47,000 Businesses Trust Coinbase To Integrate Bitcoin Payments, Including...



FEATURED

February 28, 2017 | **Kevin Helms** | 👁 9104 | 💬 **14**

Coinbase Exits as Hawaii Requires Bitcoin Companies to Hold Fiat Reserves



Why Monero is different

Monero is secure

Monero is a decentralized cryptocurrency, meaning it is secure digital cash operated by a network of users. Transactions are confirmed by distributed consensus and then immutably recorded on the blockchain. Third-parties do not need to be trusted to keep your Monero safe.

Monero is private

Monero uses ring signatures, ring confidential transactions, and stealth addresses to obfuscate the origins, amounts, and destinations of all transactions. Monero provides all the benefits of a decentralized cryptocurrency, without any of the typical privacy concessions.

Monero is untraceable

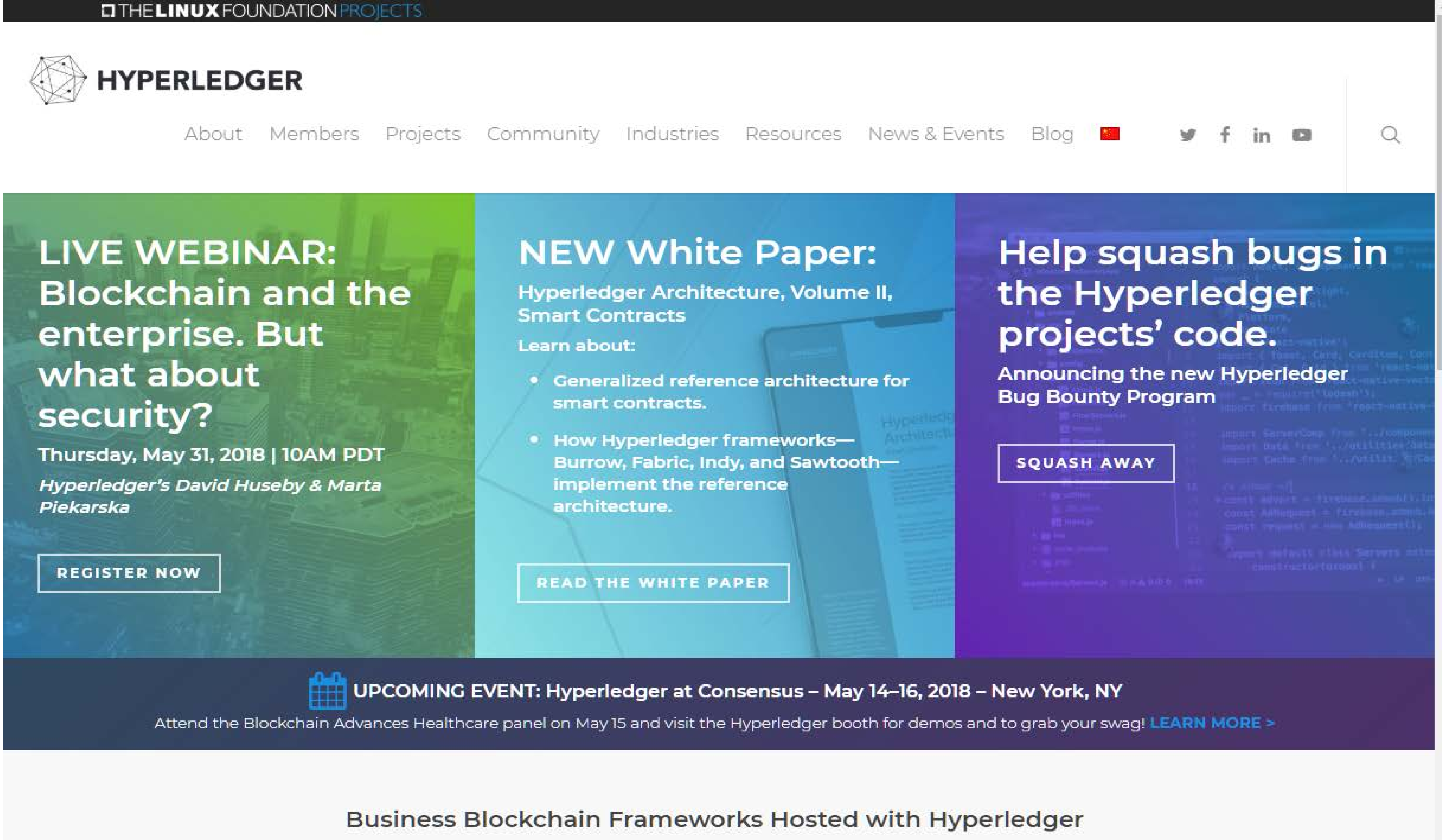
Sending and receiving addresses as well as transacted amounts are obfuscated by default. Transactions on the Monero blockchain cannot be linked to a particular user or real-world identity.

ethereum

BLOCKCHAIN APP PLATFORM

Build unstoppable applications

Ethereum is a **decentralized platform that runs smart contracts**: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference.



LIVE WEBINAR: Blockchain and the enterprise. But what about security?

Thursday, May 31, 2018 | 10AM PDT

Hyperledger's David Huseby & Marta Piekarska

NEW White Paper:

Hyperledger Architecture, Volume II, Smart Contracts

Learn about:

- Generalized reference architecture for smart contracts.
- How Hyperledger frameworks—Burrow, Fabric, Indy, and Sawtooth—implement the reference architecture.

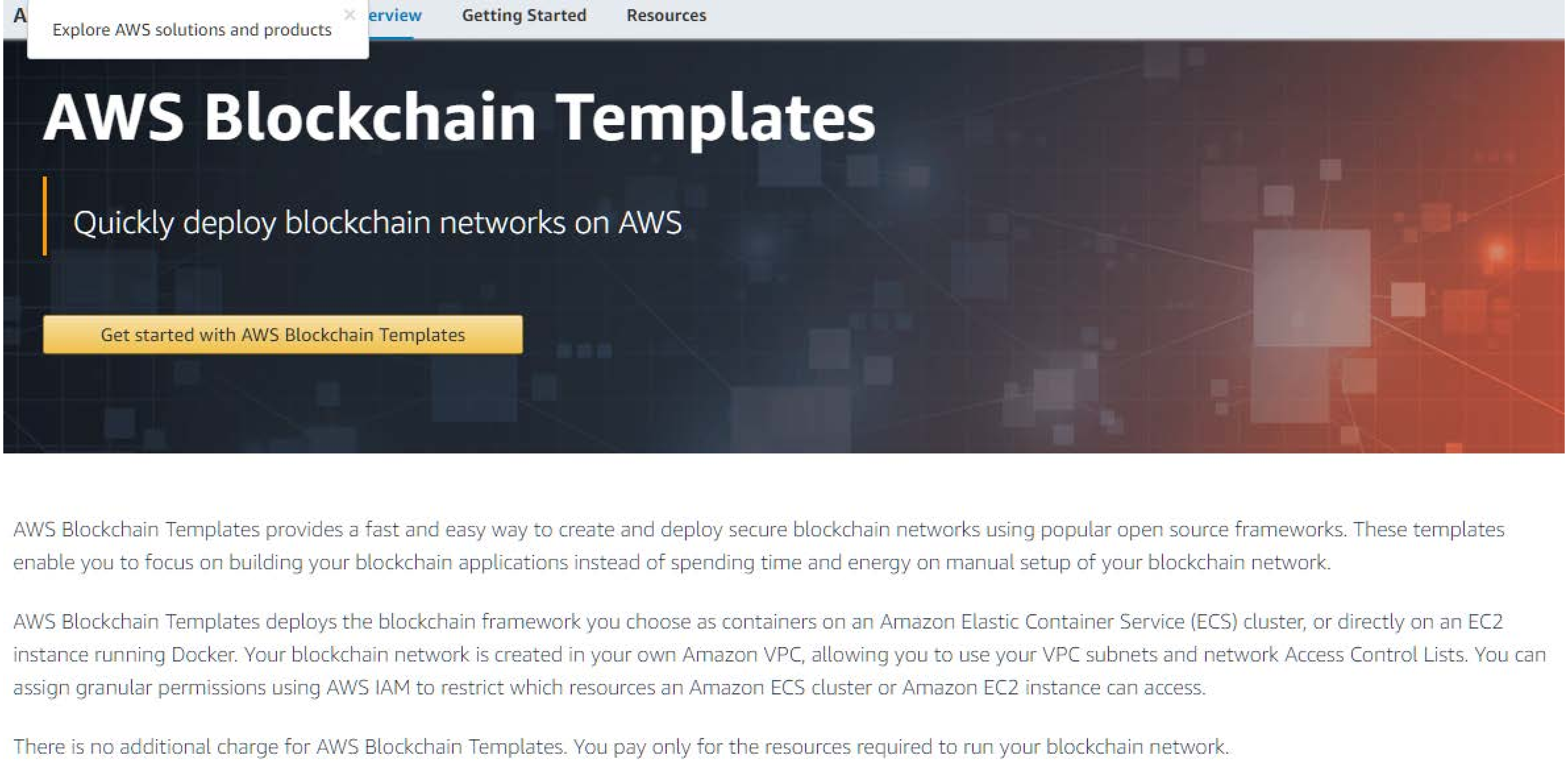
Help squash bugs in the Hyperledger projects' code.

Announcing the new Hyperledger Bug Bounty Program

UPCOMING EVENT: Hyperledger at Consensus – May 14–16, 2018 – New York, NY

Attend the Blockchain Advances Healthcare panel on May 15 and visit the Hyperledger booth for demos and to grab your swag!

Business Blockchain Frameworks Hosted with Hyperledger


A
Explore AWS solutions and products
×
erview
Getting Started
Resources

AWS Blockchain Templates

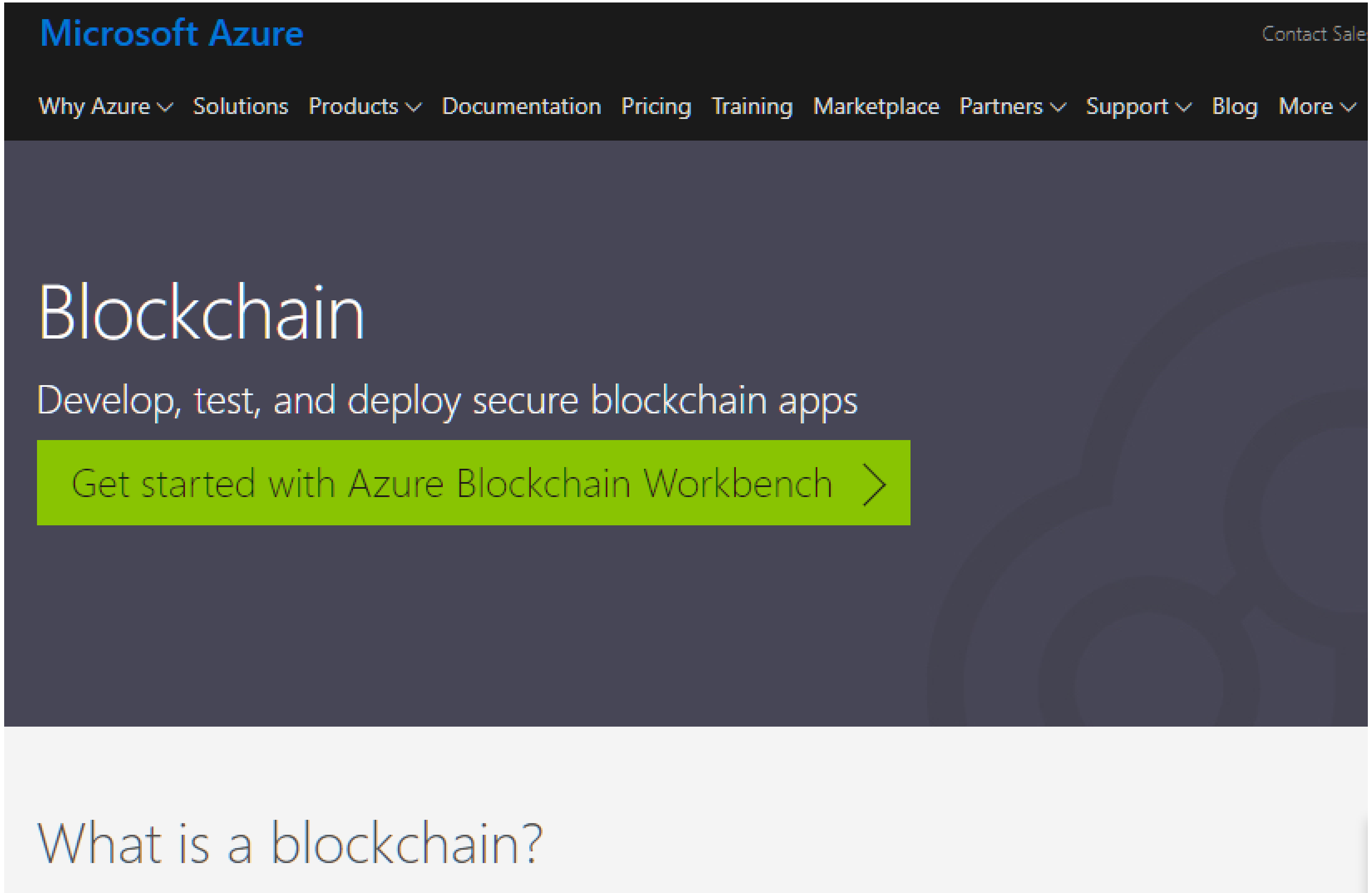
Quickly deploy blockchain networks on AWS

Get started with AWS Blockchain Templates

AWS Blockchain Templates provides a fast and easy way to create and deploy secure blockchain networks using popular open source frameworks. These templates enable you to focus on building your blockchain applications instead of spending time and energy on manual setup of your blockchain network.

AWS Blockchain Templates deploys the blockchain framework you choose as containers on an Amazon Elastic Container Service (ECS) cluster, or directly on an EC2 instance running Docker. Your blockchain network is created in your own Amazon VPC, allowing you to use your VPC subnets and network Access Control Lists. You can assign granular permissions using AWS IAM to restrict which resources an Amazon ECS cluster or Amazon EC2 instance can access.

There is no additional charge for AWS Blockchain Templates. You pay only for the resources required to run your blockchain network.



Blockchain

Develop, test, and deploy secure blockchain apps

What is a blockchain?

Cryptocurrencies and Blockchains

- Cryptocurrencies and technology are here to stay…
  - http://www.bitcoin.org/ - Started Satoshi Nakamoto, 10/08
  - www.ZeroCoin.org - Extend Bitcoin to make it private
  - www.Litecoin.org - Open Source P2P Internet Currency
  - www.Ethereum.org - Smart Contracts (Microsoft)
  - www.Hyperledger.org - Blockchains for Business (IBM)
  - www.getmonero.org – Monero Cryptocurrency (XMR)
  - https://aws.amazon.com/blockchain/templates/ AWS
  - https://azure.microsoft.com/en-us/solutions/blockchain/ MS Azure
- Security is an issue just like anything else
  - Consumers: Social Engineering, Malware, Phishing etc.
  - Exchanges: Hacks, Botnets, Malware, Phishing, APT etc.

Acknowledgements

Some of the slides, content, or pictures are borrowed from the following resources, and some pictures are obtained through Google search without being referenced below:

- Most of the OSINT content in this presentation is from - Online Class on Open Source Intelligence (OSINT) 2016 class at Cyber Watch West (CWW) by Anastacia Webster, Adjunct Instructor at California State University, San Bernardino, CA
- Michael Bazzell- Open Source Intelligence Techniques; Hiding from The Internet; Privacy and Security; Personal Digital Security
- Johnny Long- No Tech Hacking : Google Hacking
- L24-BitCoin and Security, many of the slides borrowed from this presentation with modifications.
- Presentation by Amir Houmansadr from Umass CS entitled “Secure Digital Currency: Bitcoin”, CS660, Spring 2015

UNIVERSITY of HAWAI'I®
MAUI COLLEGE

Dr. Debasis Bhattacharya, JD, DBA

debasisb@hawaii.edu

@uhmcabit

http://maui.hawaii.edu/cybersecurity