MIT SLOAN REUNION

COME TOGETHER. RECONNECT. CONTINUE LEARNING.

2018
June 7 – 10
SOME SIMPLE ECONOMICS OF THE BLOCKCHAIN

Christian Catalini
Theodore T. Miller Career Development Professor, Associate Professor, TIES Group
Cryptocurrency & Blockchain

MIT Digital Currency Research Study (2014)
>30X Since we did the MIT Digital Currency Experiment!

The majority of MIT undergrads kept their $100 in Bitcoin in 2014. Today it is worth more than $3,000.
### Competing Standards and the .Coin Bubble

<table>
<thead>
<tr>
<th>#</th>
<th>Coin</th>
<th>Price</th>
<th>Market Cap</th>
<th>BTC</th>
<th>% Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$93,884,977,725</td>
<td>$5643.75</td>
<td>$1,465,320,000</td>
<td>16,635,212 BTC</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$29,102,811,337</td>
<td>$305.66</td>
<td>$298,133,000</td>
<td>95,212,084 ETH</td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>$6,364,233,811</td>
<td>$0.217075</td>
<td>$304,669,000</td>
<td>38,531,538,922 XRP</td>
</tr>
<tr>
<td>4</td>
<td>Bitcoin Cash</td>
<td>$5,450,024,347</td>
<td>$326.28</td>
<td>$138,878,000</td>
<td>16,706,125 BCH</td>
</tr>
<tr>
<td>5</td>
<td>Litecoin</td>
<td>$3,143,191,843</td>
<td>$58.80</td>
<td>$109,347,000</td>
<td>53,458,007 LTC</td>
</tr>
<tr>
<td>6</td>
<td>Dash</td>
<td>$2,227,446,496</td>
<td>$291.83</td>
<td>$35,753,900</td>
<td>7,632,580 DASH</td>
</tr>
<tr>
<td>7</td>
<td>NEM</td>
<td>$1,989,171,000</td>
<td>$0.221019</td>
<td>$3,281,440</td>
<td>8,999,999,999 XEM</td>
</tr>
<tr>
<td>8</td>
<td>BitConnect</td>
<td>$1,447,598,710</td>
<td>$200.49</td>
<td>$13,458,300</td>
<td>7,220,448 BCC</td>
</tr>
<tr>
<td>9</td>
<td>NEO</td>
<td>$1,432,895,000</td>
<td>$28.66</td>
<td>$30,089,600</td>
<td>50,000,000 NEO</td>
</tr>
<tr>
<td>10</td>
<td>Monero</td>
<td>$1,370,923,873</td>
<td>$89.94</td>
<td>$39,629,700</td>
<td>15,243,175 XMR</td>
</tr>
<tr>
<td>11</td>
<td>IOTA</td>
<td>$1,143,607,160</td>
<td>$0.411439</td>
<td>$14,582,700</td>
<td>2,779,530,283 MIOTA</td>
</tr>
<tr>
<td>12</td>
<td>Ethereum Classic</td>
<td>$1,087,014,605</td>
<td>$11.25</td>
<td>$24,085,000</td>
<td>96,640,701 ETC</td>
</tr>
<tr>
<td>13</td>
<td>Qtum</td>
<td>$895,920,069</td>
<td>$12.17</td>
<td>$234,267,000</td>
<td>73,600,768 QTUM</td>
</tr>
<tr>
<td>14</td>
<td>OmiseGO</td>
<td>$755,897,558</td>
<td>$7.89</td>
<td>$13,280,400</td>
<td>98,312,024 OMG</td>
</tr>
</tbody>
</table>

---

**Diagram:**
- **Bitcoin**: 55.95%
- **Ethereum**: 17.34%
- **Ripple**: 4.98%
- **Bitcoin Cash**: 3.25%
- **Litecoin**: 1.87%
- **Dash**: 1.33%
- **Other**: 13.23%

---

*标注：部分数据可能未更新至最新，仅供参考。*
Even Within the Same Cryptocurrency, Competing Standards

Fortune

Bitcoin Prepares For an Ugly Breakup

David Z. Morris
Mar 19, 2017

On Friday, a group of major cryptocurrency exchanges announced their planned response to the split of bitcoin into two separate pools of currency and processing power. That event, known as a "hard fork," is viewed as increasingly likely among bitcoin leaders, as a years-long debate about the network's technical limitations and broader vision comes to a head.

The marketplaces, including marquee portals BitStamp and Kraken, said on Friday that if a hard fork occurs, they will let users trade both conventional bitcoin, and any alternate version that emerges. The most likely bitcoin spinoff is known as Bitcoin Unlimited, which the world's largest bitcoin server group, or "mining pool," recently announced it would back.

Get Data Sheet, Fortune's technology newsletter.

Bitcoin has been pushed to the verge of this split by a years-long debate about what's known as block size. Under bitcoin's existing code, there's a tight limit on the amount of data that can be included in a batch of transactions, and as the network has grown in popularity, that limit has slowed the processing of payments. Moves that once took seconds to clear can now take hours, and all players seem to agree that some sort of change is necessary.

But there are competing visions about any fix's goals and methods. One bitcoin entrepreneur has summarized the divide as between a Bitcoin Unlimited contingent updating bitcoin to support many small transactions, and a Bitcoin Core cadre who believe in smaller changes, fewer transactions, and more stability.

Market Design

• **Transactions per second versus store of value (happening now!)**
• Decentralization versus compliance
• Degree of privacy
Battle for the Standard

New Bitcoin Blocks (as of May 24th, 2017)
The Rise of Initial Coin Offerings

Source: CB Insights, TokenData
The Blockchain

1st Block
- Transaction 1
- Transaction 2
- Transaction 3

2nd Block
- 1st Block Hash
- Transaction 4
- Transaction 5

Transaction 6?
Transaction 7?
...

Mining the next block
Where is the Breakthrough From an Economics Perspective?
Censorship Resistance?

A Letter to Jamie Dimon
And anyone else still struggling to understand cryptocurrencies

Dear Jamie,

My name is Adam Ludwin and I run a company called Chain. I have been working in and around the cryptocurrency market for several years.

Last week you said a few things about Bitcoin:

1. *DIMON: THIS IS THE LAST TIME I TALK ABOUT BITCOIN*  BN 13:30
2. *DIMON: BITCOIN IS “A GREAT PRODUCT” IF YOU ARE A CRIMINAL*  BN 13:30
3. *DIMON: GOVERNMENTS LIKE TO CONTROL THEIR ECONOMIES, CURRENCIES*  BN 13:29
4. *DIMON: GOVERNMENTS ARE GOING TO CRUSH BITCOIN ONE DAY*  BN 13:28

Bloomberg: https://twitter.com/joelht/status/918899226771427328

It’s easy to believe cryptocurrencies have no inherent value. Or that governments will crush them.

It’s also becoming fashionable to believe the opposite: that they will disrupt banks, governments, and Silicon Valley giants once and for all.
Market Power in Digital Platforms

The Antitrust Case Against Facebook, Google and Amazon

A few technology giants dominate their worlds just as Standard Oil and AT&T once did. Should they be broken up?
A Reduction in Two Key Costs

1. **Cost of Verification**

2. **Cost of Networking**

1. Cost of Verification

Transaction is born

$t_0$

Attributes
e.g., existence, timestamp, parties involved, conflict resolution rules, collateral etc.

Actions are performed

$t_1$

Reliance on transaction attributes

Problem may arise

$t_n$

Verification of attributes is required

*costly* verification through an intermediary (audit)

*costless* verification on a blockchain
Information Leakage

Transaction is born

$\tau_0$

Attributes

- e.g., existence, timestamp, parties involved, conflict resolution rules, collateral etc.

Reliance on transaction attributes

$\tau_1$

Problem may arise

Verification of attributes is required

$\tau_n$

- costly verification through an intermediary (audit)

- costless verification on a blockchain
Preventing Information Leakage

World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 10th Sep 2017)
Digital Privacy

$10 Million Settlement in Target Data Breach Gets Preliminary Approval

A federal judge on Thursday gave preliminary approval to a $10 million settlement of a lawsuit brought by customers of Target, which experienced an online attack involving confidential customer data during the holiday season in 2013.

According to documents filed with the United States District Court in Minnesota this month, shoppers affected by the breach could be awarded up to $10,000 each in damages. The settlement includes a draft of the form victims must complete to make claims, processed through a dedicated website.

Customers may still file objections to the terms of the proposed settlement, but Judge Paul A. Magnuson set a final hearing on the settlement for Nov. 20.

Molly Snyder, a Target spokeswoman, said, "We are pleased to see the process moving forward and look forward to its resolution." The pending settlement was first reported by CNBC.

Google DeepMind’s Untrendy Play to Make the Blockchain Actually Useful
Data Integrity with Costless Verification

Step 1 of 5
Computing local hash [DONE]

Step 2 of 5
Fetching remote hash [DONE]

Step 3 of 5
Comparing local and remote hashes [DONE]

Step 4 of 5
Checking Merkle root [DONE]

Step 5 of 5
Checking receipt [DONE]

 Verified

Public Key
1HYPitzwR83M3Sw6GAs5XeQzEBoJAEes

Blockchain Address
4bf64ff1517554dac3496e9da0a28-ca9ae492682b0898e384ea17e7f90ee1295
Verifying Credentials, IP, Equity, Contracts...
Lower Cost of Verification

- Cross-Border, Bank Payments
- Financial Assets
- Consumer Payments
- Private Equity

Intensive Margin ➔ Cheaper Settlement and Reconciliation
Lower Cost of Verification

Intensive Margin ➔ Monetary Policy, Taxation, QE, KYC…
The “Double Spending” Problem

Ability to Define Scarce, Digital Property Rights
Lower Cost of Verification

Store of Value

Computation

Data Storage

Extensive Margin → New Digital Property Rights
People have spent over $1M buying virtual cats on the Ethereum blockchain

-Launched a few days ago, CryptoKitties is essentially like an digital version of Pokemon cards but based on the Ethereum blockchain. And like most viral sensations that catch on in the tech world, it's blowing up fast.

-Built by Vancouver and San Francisco-based design studio AxiomZen, the game is the latest fad in the world of cryptocurrency and probably soon tech in general.

-People are spending a crazy amount of real money on the game. So far about $1.3M has been transacted, with multiple kittens selling for ~50 ETH (around $23,000) and the "genesis" kitten being sold for a record ~246 ETH (around $113,000). This third party site tracks the largest purchases made to date on the game. And like any good viral sensation prices are rising and fluctuating fast. Right now it will cost you around .03 ETH, or $12 to buy the least expensive kitten in the game.

-So now we have people using Ether, an asset with arguably little tangible utility – to purchase an asset with unarguably zero tangible utility. Welcome to the internet in 2017.

-CryptoKitties

🚨🚨🚨 Due to network congestion, we are increasing the birthing fee from 0.001 ETH to 0.002 ETH. This will ensure your kittens are born on time! The extra is needed to incentivize miners to add birthing txs to the chain. Long-term solution will be explored very soon! 🚨🚨🚨

5:13 PM - Dec 3, 2017

37 Retweets 99 Likes 347 Favorites
Provenance
Costless Verification?

- Verification goes from being **costly, scarce** and **prone to abuse**, to being **cheap** and **reliable**

- The **initial mapping** between offline events and their digital representations is still costly to bootstrap and **maintain!**
  - IoT as a complement (e.g. provenance)
  - A change in the **nature** of intermediation
2. Cost of Networking

• **Internet-Level Consensus:** blockchain technology allows
  
  - A network of economic agents
  
  - To agree at regular intervals
  
  - On the true state of shared data

• A fundamental change in our ability to bootstrap and operate a marketplace!
2. Cost of Networking

- Consequences of market power (intermediary) in digital platforms
  - Prices
  - Data ownership (we are all renters on the internet!)
  - Single point of failure
  - Lock-in, barriers to entry
  - Less innovation
New Approaches To…

- Startup fundraising
- Digital platforms
- Software protocols
- Public goods provision
- Data ownership & licensing
- Reputation systems and auctions
Agenda

• Introduction
  - Some Simple Economics of the Blockchain
    ‣ Cost of Verification
    ‣ Cost of Networking
  - The Role of Tokens in Crowdfunding, Crowdsourcing and Network Effects
Incentives for Early Adopters (miners, investors, users)
Lowering the Cost of Experimentation!

Only 75 lines of code!

CROWDSALE
RAISING FUNDS FROM FRIENDS WITHOUT A THIRD PARTY
Tokens and Capital

The DAO (organization)

- **Type**: Decentralized autonomous organization
- **Industry**: Cryptocurrency software venture capital fund
- **Founded**: 2016
- **Area served**: World (stateless)[1]
- **Key people**: Stephan Tual, Simon Jentzsch, Christoph Jentzsch
- **Total assets**: ETH 11.5 million[2]
- **Owners**: +18,000 stakeholders[3]
- **Number of employees**: 0 (automated)[4]
- **Website**: daohub.org

DealBook

A Venture Fund With Plenty of Virtual Capital, but No Capitalist

By NATHANIEL POPPER  MAY 21, 2016

TECH

Chiefless Company Rakes In More Than $100 Million

Group called DAO is running itself via computer code

By Paul Vigna
May 16, 2016

Can a company run itself without executives or managers or a board of directors? One of the more radical experiments in technology aims to find out.
Tulip mania: the classic story of a Dutch financial bubble is mostly wrong

February 12, 2018 1:14am EST

Right now, it’s Bitcoin. But in the past we’ve had dotcom stocks, the 1929 crash, 19th-century railways and the South Sea Bubble of 1720. All these were compared by contemporaries to “tulip mania”, the Dutch financial craze for tulip bulbs in the 1630s. Bitcoin, according some sceptics, is “tulip mania 2.0”.

Author

Anne Goldgar
Professor of Early Modern History, King’s College London
ICOs over Time

Density

2011m1 2012m1 2013m1 2014m1 2015m1 2016m1 2017m1 2018m1
Total Capital Raised by Size

- 0-5K
- 5K-50K
- 50K-300K
- 300K-1M
- 1M-5M
- 5M-10M
- 10M-25M
- 25M-50M
- >50M

Total Capital Raised (Millions)
Age Distribution
Crypoeconomics
Total Capital
ICOs versus Series A Capital in Tech

- Log(ICO Funding PC) against Log(Series A Funding PC)
- Countries represented:
  - Argentina
  - Australia
  - Austria
  - Belgium
  - Canada
  - China
  - Estonia
  - France
  - Germany
  - Hong Kong
  - India
  - Ireland
  - Israel
  - Italy
  - Japan
  - Lithuania
  - Luxembourg
  - Malta
  - Mexico
  - Netherlands
  - Nigeria
  - Norway
  - Poland
  - Romania
  - Russia
  - Singapore
  - Slovakia
  - South Africa
  - South Korea
  - Spain
  - Switzerland
  - Taiwan
  - Thailand
  - UAE
  - United Kingdom
  - United States
  - Vietnam
ICOs versus Seed Capital in Tech (US)
Underwater

Current price < min(ICO price)
Technical White Papers Attract Most of the Capital. Plagiarism is Not Rewarded by the Market

$$\forall x \in L, z \in \{0, 1\}^*, \text{View}_V \left[ P(x) \leftrightarrow \hat{V}(x, z) \right] = S(x, z)$$
More Developed and Active Codebases Attract More Funding
ICOs With Stronger Technical Teams and Codebases Have Better Early Performance
Towards a “Crypto” Valley?

Singapore and Switzerland Have Not Attracted More Fraud and Scams
Multiple “Crypto” Valleys?

Favorable Legislations are Performing Well
Bootstrapping an Ecosystem

1. **Bootstrapping phase** (highly volatile): native token is used to **crowdfund** the development of the platform, and to **crowdsourc**e key contributions. Can rely on high-powered incentives similar to the venture capital model to attract:

   - **Early adopters** deriving utility from helping develop the technology
   - **Top global talent** (not only signalling and pro-social incentives as in open source)
   - **Investors** expecting the token to appreciate in value
   - **Users!** Building critical mass for network effects

2. **Operating phase** (less volatile): **incentive system** and **innovation policy** to coordinate and reward contributions & key resources (talent, capital, ideas, etc.)
Crowdsourcing Key Resources

Amazon EC2

OneDrive

Cloud Storage

EARN FILECOIN FOR HOSTING FILES

EXCHANGE FILECOIN FOR USD, BTC, ETH AND MORE

RELIABLY STORE FILES AT HYPERCOMPETITIVE PRICES
Attracting Top Talent

Figure 1: An overfitting curve where the blue test error continues to decrease with more submissions from data scientists, but the error on new data increases. [2]
Incentivizing Early Adopters

Delays discourage early adopters, undermining broader diffusion by later adopters

Delayed access to bitcoin discourages natural early adopters (NEAs) from persisting in more close-knit social environments in dorms but not among those living off campus (left). Natural late adopters (NLAs) are less likely to persist (center) or to be highly active (right) if they live in dorms that had an above-median share of delayed NEAs.

Governance?

- Trust in a platform operator is replaced by trust in the underlying incentives, code, consensus rules and governance

- Open source as a model

- Risk of crowding out pro-social incentives with monetary ones
ANY QUESTIONS?

#SLOANIEREUNION
THANK YOU!

#SLOANIEREUNION