Bitcoin and ICOs

Rachel Harkins, Matt Snyder, Emil Kunkin, Ryan McSpedon
Two Monies Refresher

- $I = 1$, $n = 5$, $\omega = (100, 50, 45, 10, 5)$
- $T_B = (5, 1, 1, 0, -1)$
- $T_R = (2, 1, 1, -1, -6)$
Answer

- $\sum T^r = -3$
- $\sum T^b = 6$
  - $P^b \sum T^b + P^r \sum T^r = 0$
  - $6P^b = 3P^r$
- $P^r/P^b = 2$
  - $X_1: 100 - 5P^b - 2P^r > 0$, so $100 - 9P^b > 0$, and $P^b < 100/9$
  - $X_2: 50 - P^b - P^r > 0$, so $50 - 3P^b > 0$, and $P^b < 50/3$
  - $X_3: 45 - P^b - P^r > 0$, so $45 - 3P^b > 0$, and $P^b < 15$
- So, $P^b < 100/9 < 15 < 50/3$
Price of Bitcoin: $5991.98
What is blockchain?

1. Someone requests a transaction.
2. The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
3. Validation:
   - The network of nodes validates the transaction and the user's status using known algorithms.
4. A verified transaction can involve cryptocurrency, contracts, records, or other information.
5. Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.
6. The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
7. The transaction is complete.

- **Cryptocurrency**
  - Has intrinsic value in that it is not redeemable for another commodity such as gold.
  - Has no physical form and exists only in the network.
  - Its supply is not determined by a central bank and the network is completely decentralized.
How it works:

Someone requests a transaction.

The requested transaction is broadcast to P2P network consisting of computers, known as nodes.

Validation

The network of nodes validates the transaction and the user’s status using known algorithms.

A verified transaction can involve cryptocurrency, contracts, records, or other information.

Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

The transaction is complete.

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

Cryptocurrency

Cryptocurrency is a medium of exchange, created and stored electronically in the blockchain, using encryption techniques to control the creation of monetary units and to verify the transfer of funds. Bitcoin is the best known example.

- Has no intrinsic value in that it is not redeemable for another commodity, such as gold.
- Has no physical form and exists only in the network.
- Its supply is not determined by a central bank and the network is completely decentralized.
History of Bitcoin

Satoshi Nakamoto publishes "Bitcoin: A Peer-to-Peer Electronic Cash System"
This details how Bitcoin operates. It is considered the magna carta of Bitcoin

August 18, 2008
Satoshi Nakamoto publishes "Bitcoin: A Peer-to-Peer Electronic Cash System"

October 31, 2008
Bitcoin.com is Registered
The identity of the website owner is protected and unknown

January 3, 2009
First version of Bitcoin software is released

January 8, 2009
First Bitcoin is Mined
This is known as Block 0 or the "genesis block." It contains the text "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

January 9, 2009
Block 1 is Mined
Bitcoin mining has officially begun
### Other Cryptos

<table>
<thead>
<tr>
<th></th>
<th>Cryptocurrency</th>
<th>Market Cap</th>
<th>Price</th>
<th>24h Volume</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$99,320,566,033</td>
<td>$5970.17</td>
<td>$2,358,480,000</td>
<td>16,636,137 BTC</td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$28,886,015,917</td>
<td>$303.36</td>
<td>$397,719,000</td>
<td>95,221,822 ETH</td>
</tr>
<tr>
<td>3</td>
<td>Ripple</td>
<td>$8,132,351,010</td>
<td>$0.211057</td>
<td>$182,515,000</td>
<td>38,531,538,922 XRP</td>
</tr>
<tr>
<td>4</td>
<td>Bitcoin Cash</td>
<td>$5,458,006,863</td>
<td>$326.69</td>
<td>$160,034,000</td>
<td>16,706,838 BCH</td>
</tr>
<tr>
<td>5</td>
<td>Litecoin</td>
<td>$3,208,014,680</td>
<td>$60.00</td>
<td>$151,922,000</td>
<td>53,465,307 LTC</td>
</tr>
<tr>
<td>6</td>
<td>Dash</td>
<td>$2,206,918,542</td>
<td>$289.11</td>
<td>$47,365,200</td>
<td>7,633,517 DASH</td>
</tr>
<tr>
<td>7</td>
<td>NEM</td>
<td>$1,944,891,000</td>
<td>$0.216099</td>
<td>$4,930,170</td>
<td>8,999,999,999 XEM</td>
</tr>
<tr>
<td>8</td>
<td>BitConnect</td>
<td>$1,533,650,824</td>
<td>$212.30</td>
<td>$15,685,100</td>
<td>7,224,081 BCC</td>
</tr>
<tr>
<td>9</td>
<td>NEO</td>
<td>$1,380,765,000</td>
<td>$27.62</td>
<td>$36,785,700</td>
<td>50,000,000 NEO</td>
</tr>
<tr>
<td>10</td>
<td>Monero</td>
<td>$1,372,667,734</td>
<td>$90.04</td>
<td>$37,923,800</td>
<td>15,245,037 XMR</td>
</tr>
</tbody>
</table>
Bitcoin: investment grade asset or criminal money?

- Bitcoin has two main uses:
  - Speculative Asset
    - The price of bitcoin has fluctuated massively over the last year
    - An investor who bought in October 2016 would have earned a return of roughly 900%
  - Currency
    - Bitcoin can be used as a legitimate currency
      - Some brick-and-mortar retailers accept bitcoin
    - Bitcoin and similar currencies are also the preferred method of payment for illicit online transactions
    - Mainstream financial institutions are somewhat resistant to cryptocurrencies
Governments have considered using cryptocurrencies and moving the technology from the dark web to central banks.

Cryptocurrencies could be used for:
- New form of central bank money
- Securities clearing
- Wholesale Payments by central banks
Cryptocurrencies and Central Banks

- Positives of Using Cryptocurrencies in a Central Bank:
  - Efficient
  - Cost-Effective
  - Online + Electronic
  - Anonymous

- Negatives of Using Cryptocurrencies in a Central Bank:
  - Still evolving
  - Implementation risks
  - Anonymous
ICOs

- An ICO is a popular way for blockchain start-ups to raise capital by issuing crypto-based tokens/coins.

How it works:

1. Company releases its whitepaper which typically outlines the details of their product in greater technical depth, how much money is necessary to complete the venture, how many tokens the founders will keep, the type of money accepted, and the duration of the ICO.

2. On the start date, investors and early adopters of the firm’s project can purchase tokens using Ethereum or other cryptocurrencies such as Bitcoin.

3. Once the maximum number of tokens have been purchased or time runs out the ICO closes.

- For start-ups, an ICO provides capital to fund the development of their project/business, while investors receive tokens that 1) could potentially appreciate in value if the project is successful and 2) often provide access to the company’s product.
Market for ICOs

- The market for ICOs has grown exponentially since its inception, with ICO investment totaling $26 million in 2014, $103 million in 2016, and $1.27 billion in the first half of 2017.
- The earliest ICOs began in 2013 on a Bitcointalk.org forum. Developers of cryptocurrencies had lots of interest but no money to fund their projects. NXT and Mastercoin funded their development by selling a portion of their coins. They raised $6,000 and $500,000, respectively.
- This growth has been fueled by both an increase in number and size of ICOs. Most recently, Tezos, a “self-amending cryptoledger” and competitor to Ethereum, raised $232 million in its ICO, making it the largest in history. Tezos drew criticism for its uncapped ICO, meaning it could raise unlimited amounts of money. Prior to Tezos, the largest ICOs, both of which were introduced earlier in 2017, were Bancor at $153 million in three hours of funding and EOS at $185 million from 5 days.
ICOs and the Free Banking Era

- Section 10 of the US Constitution prevents states from printing or coining official currency.
- Banks, instead, would issue bills of credit in exchange for deposits of gold or silver.
- This was inherently risky, specie deposits did not necessarily match redemption notes.
- These notes were thus considered risky and were discounted based on riskiness.
- Similar to the free banking era, ICOs involve an independent organization issuing assets that hold inherent risks as the coins become worthless if the company fails.
George Soros and the Bank of England

- The European Exchange Rate Mechanism fixed the Pound to the other European currencies, but the end of the cold war changed the monetary landscape.
- Britain had high inflation rates, and the German central bank raised interest rates.
- Fund Manager George Soros recognized that England could not stay in the ERM long term.
- He shorted the pound against the German Mark, and earned roughly $1 Billion when Britain was forced to withdraw.
Cryptocurrencies as a Bubble

- Cryptocurrencies are seen as more of an asset than a currency.
- As such, it is speculated that investing in them could create a bubble.
- Cryptocurrencies have seen large price fluctuations.
- In the overlapping generations model, the money bubble will eventually deflate from its monetary steady state.
- Cryptocurrencies are at a disadvantage to other fiat currencies, as taxes are not payable in bitcoin.
- Bitcoin’s value only makes sense when seen as an asset, not a currency.
Regulation

● The SEC released a report on July 25th detailing its investigation of the DAO, a decentralized investment fund. They determined that the DAO tokens were securities, and though they are not pressing charges against anyone affiliated with the company, this report released a warning that the SEC expects ICOs to comply with federal securities laws.

● The report insinuated that the SEC will investigate past and future ICOs to determine which tokens offered should be considered securities. If deemed a security, the token must be registered with the SEC and may only be traded on a national securities exchange. Any sale of securities, which now includes certain ICOs, must register with the SEC.