Cryptoeconomics

Or How I Learned to Stop Worrying and Love Internet Money

Olaf Carlson-Wee

Polychain
Bitcoin Made Easy

Coinbase is the simplest way to buy, use, and accept Bitcoin.

Email: [Your Email] Password: [Choose A Pas:] Create My Account

Balance: 186.32 BTC

<table>
<thead>
<tr>
<th>Transaction</th>
<th>Date</th>
<th>Status</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>You received bitcoins from Brian Armstrong</td>
<td>Jan 26, 2013</td>
<td>Pending</td>
<td>+0.99</td>
</tr>
<tr>
<td>You received bitcoin from Paul Graham</td>
<td>Jan 26, 2013</td>
<td>Complete</td>
<td>+0.234</td>
</tr>
<tr>
<td>You sent bitcoins to Daniel</td>
<td>Jan 25, 2013</td>
<td>Complete</td>
<td>-1.00</td>
</tr>
<tr>
<td>You sent bitcoins to Fred Ehrman</td>
<td>Jan 25, 2013</td>
<td>Complete</td>
<td>-0.3488</td>
</tr>
</tbody>
</table>
Mining
2011
Mining
2013
Mining
2015
Cryptocurrencies are human coordination mechanisms
Value = Security

- Market Capitalization of a cryptocurrency allows:
  - Transfer of $
  - Execution of contracts
  - Farther out: voting, identity, etc

- Speculators are critical to the premise of blockchains
Adversaries

- Two types of adversaries

  - Profit-motivated within the system
    - Paying miners to prevent sybil attacks
  - Profit-motivated outside the system
    - Derivative contracts mean you cannot reason about the security of a system by only examining the contract or protocol alone
Why buy coins?

• To make applications work, we must have people buying coins first
• How can we design a cryptocurrency to be friendly to speculators?
  • Launch distribution
  • Inflation curve
  • Long-term economics
• We can now use software to program assets
Distribution

• Who owns the coins?
  
  • “Of the over 85 billion tokens… the [Stellar Foundation] burned over 55 billion… the value of the burned tokens is nearly $4.7 billion.”
  
  • “The coin has reacted positively to the news, seeing a price increase of nearly 25% on the day at press time.”

• If the Foundation represents holders, why not continue to burn coins?

• Legitimacy and Fairness (Gini Coefficient)
ICOs

- No-caps auction
  - Efficient market price discovery, but timing participation is hard
- Capped-per-participant
  - Incentivizes sybil attacks as there is not price discovery in the auction
- Capped auction
  - Limits participation and encourages whales to make a “trade”
Why did ICOs raise Billions?

• block.one designed a daily auction to distribute EOS over one year
  • As EOS had price discovery, auction became simply an arbitrage for traders
  • Traders don’t care if buying from order book or someplace else
  • EOS price rising meant more capital for block.one
  • Core design problem is block.one contributing to its own auction to earn a larger % of the EOS coins.
Forks & Airdrops

- Bitcoin Cash & Bitcoin SV: “Valid chain” is simply social Schelling point
  - Forks & airdrops distribute to existing coin holder set
- Handshake: Airdrop to GitHub account SSH keys
- Dfinity: Airdrop with KYC for sybil resistance
Inflation Security

- Security = $ per hour paid to miners
- Security scales with market capitalization
  - Assumes profit from attack is inside the system
- Higher inflation = better security to market cap ratio
- Lower inflation = better asset to hold (higher market cap)
Inflation Security

- Proof of Work and Proof of Stake handle 51% attacks differently
  - In PoW, hash algorithm must be changed, *all* miners go offline
  - In PoS, *only* the attacking coins are deleted
Bitcoin Long Term Security

- $/hour to miners :: Market Cap
- As block rewards trend to zero, reliance on transactional fees
- If Market Cap grows by 50x (gold parity)...
- ...Then transactions are going to be very expensive
  - (this is still a massive unsolved problem with bitcoin)
  - Is this all priced in today?
Lock-ups?

- Offline, contractual lockups of coins means some % of coins which cannot be sold, will be sold in the future

- Means skewed pricing based on imperfect information and opaque offline contracts

- Large supplies which will be “unlocked” is a bad environment to be a buyer

- As we saw with Stellar, any Foundation is usually adversarial with holders
A Buyer’s Market

• At the end of the day, you can’t make people buy coins

• You can, however, program a system which encourages people to buy coins
  • This is a critical part of building a secure system!
Once we have a base layer with value we can build so much more!
Decentralized Finance

• Now that we know how to bootstrap programmable assets, what can we build on top of these blockchains?

• Financial services (DeFi):
  • Lending
  • Synthetic assets (stablecoins)
  • Trading
  • Information Markets? Insurance Pools?
Oracles

• Most financial services rely on Oracles

• Feeding data into the blockchain is equally difficult as determining if a block is valid! However, the stakes are usually lower.

• Most constructions today are a consortium model of trusted parties

• This continues to be an area of significant research
  • Could a PoS model be used to feed data into contracts?
Lending

• Lending rates in PoS protocols will never be lower than the staking inflation rate!
  • Contracts and underlying protocols have interactions
• Lending can be pooled and market based (Compound Finance)
  • Or fixed rate (MakerDAO)
• Lenders seeking yield
• Borrowers going short or getting leverage
Synthetic Assets

• MakerDAO allows participants to collateralize ETH to get a loan in DAI
  • Use your ETH to get a loan directly from a contract!

• DAI tracks USD
  • In theory a DAI-like instrument can track anything!

• Once we bootstrap base coin value, and have a price oracle, we can have infinite synthetics
Trading

• 0x model
  • Orderbook off chain?
  • ZKPs may massively improve performance

• MerkleX
  • “Batching” of trades means trusting exchange for a ~1 minute

• Uniswap
  • Automatic Market Maker model
Proof of Weak Hands

• In PoWH contract, people buy and sell tokens direct from the contract
  • Buys, sells, transactions are penalized by 10% fee which goes to holders
  • Exotic financial products we’ve never seen before now built by individual hackers
Software has Bugs

- $50,000,000 stolen in theDAO hack
  - Chain hard fork results in Ethereum Classic
- $30,000,000 stolen in Parity Multisig hack
- $150,000,000 frozen in the Parity Multisig contract
  - “I accidentally killed it” -Devops199
- $2,300,000 lost in PoWH contract
  - “i made it, but you’re all idiots” -functionZer0
Blockchains are Complicated

• “Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges”
  • By controlling what transactions are included in blocks, time-sensitive contracts can be manipulated

• Multi-Collateral Dai launched today!
  • Synthetics backing synthetics

• A “Tether” to the real world legal system is an alternative to crypto-collateralized synthetics with its own complexities
Free Riders?

- Are tokens and contracts value additive to the underlying cryptocurrency!?
- Today, most are parasitic
- However, they drive speculation, so it has worked out OK for Ethereum
- Could contracts ever cause significant problems for the base chain?
  - For example, trading on hash rates
Crypto Corporations

• MKR as buyer of last resort in Dai stablecoin system

• BNB operating a buy-and-burn with a % of company revenues

• CoinFlex:
  • The coin is issued to traders who provide liquidity on the exchange
  • % of revenues used in buy-and-burn
  • As coin value rises, liquidity rises, buy-and-burn rises, increasing buyer interest
Company Coins

• These “protocols” are simply company constructions

• However, the company is the #1 holder! Most skin-in-the-game.

• Is that enough incentive alignment to know the rules won’t be broken?
  • Is this all priced in?

• Will we have Gameplay Mining, Content Mining, Driver Mining??
Company Coins

• Coins like BNB, MKR, and FLEX rely on the value of base blockchains

• However these coins are not purely speculative - the value is “Real”

• So we need to bootstrap money in order to have corporations
  • Just like IRL!
Longer Term

- The project is to replace all money with internet money
- Then, replace all financial services with smart contracts
- Could smart contracts guide even more complicated systems?
  - Taxation, Voting, Global Resource Allocation
Thanks!*

*We are hiring