Blockchain and Cryptoeconomics

University of Bristol
Seungwon (Eugene) Jeong
Biography

- Lecturer (Assistant Professor) in Economics, University of Bristol
- Education
  - Stanford PhD in MS&E (Economics & Finance) / MS in Economics and Statistics
  - POSTECH BS in EE, CS, Math (minor in IE) / MS in Math
- Past Position
  - Facebook, New Faculty Fellow Economist
    - Hackathon Finalist
    - 2 US Patents pending
  - AOL, Research Internship (online advertising)
  - Ahnlab, Software Engineer
- Youtube lecture (in Korean) on blockchain: http://blockchainstudio.tv
유득분득 블록체인

http://steemit.com/@blockchainstudio

유득분득 facebook.com/ulockblock
Contents

• What is cryptoeconomics?
• Public Key Cryptography
• Consensus mechanism
• Cryptoeconomics in Economics
What is cryptoeconomics?
Cryptoeconomics

• Building systems that have certain desired properties
  • Use **cryptography** to prove properties about messages that happened in the past
  • Use **economic incentives** defined inside the system to encourage desired properties to hold into the future - Vitalik Buterin

• “A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols.” - Vlad Zamfir
Cryptoeconomics

- Cryptography $\Rightarrow$ CS, EE, Math

- Economics
  - Game Theory
  - Mechanism Design
  - Network
  - Governance
  - ...
Public Key Cryptography
Public Key Cryptography

• Symmetric/single key cryptography
  • Only one key for encryption and decryption
  • Cons: key exchange problem
• Public key/asymmetric key cryptography
  • Public key: can be distributed in public (Bitcoin address is “public key”)
  • Private key: should be kept secretly to its owner
• Public keys can be calculated from private keys. (Wallet address import)
• Knowing a private key from a public key is almost impossible.
• How to use? Roughly, encrypt with one, decrypt with the other.
Main uses of public key cryptography

1. Encryption: encrypt with public key, decrypt with private key
   - Ex) A wants to send an encrypted message to B.
     - 1. A encrypts the message with B’s public key.
     - 2. B decrypts with its own private key, i.e., only B can decrypt it.

2. Digital signature: encrypt with private key, decrypt with public key
   - Ex) A wants to prove that the message came from A.
     - 1. A signed the message with its own private key.
     - 2. Anyone who knows A’s public key can verify the message.
   - Bitcoin: ECDSA (Elliptic Curve Digital Signature Algorithm)
Consensus Mechanism
Consensus Mechanism

• Problems in P2P system
  • Double spending
  • Byzantine generals problem (cf. Byzantine Fault Tolerance)
• Consensus mechanism in blockchain
  • A mechanism that has nice BFT properties and reaches a consensus on the validity of sequence of transactions (i.e., no double spending)
  • PoW (Proof-of-Work), PoS (Proof-of-Stake), DPoS (Delegated PoS)
Worker

I make blocks by PoW (Proof-of-Work).

http://ulockblock.com
Bitcoin Mining Farm

Bitmain
Hashrate Distribution

- BTC.com: 26.1%
- AntPool: 14.5%
- SlushPool: 11.7%
- BTC.TOP: 10%
- VIABTC: 10%
- F2Pool: 8.8%
- BitFury: 2.6%
- BTCC Pool: 2.6%
- DPOOL: 2.2%
- BW.COM: 1.9%
- Bixin: 1.1%
- BitClub Network: 1.1%
- SBCoin: 0.9%
- KanoPool: 0.6%
- Bitcoin.com: 0.5%
- Haominer: 0.3%
- ConnectBTC: 0.2%
Bitcoin network vs Supercomputer

• “Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!” Forbes (2013.11)

• 1 Hash/s ~= 12,700 FLOPS (floating point operations per second)

• 2016.01 Bitcoin network: 1 E(Exa)Hash/s (Giga, Tera, Peta, Exa)

• 2017.11
  • Top1 supercomputer: 93,000 TFLOPS ~= 7.3 THash/s
  • Bitcoin network: 10 EHash/s
Bitcoin network vs Supercomputer

TOP 10 Sites for November 2017

For more information about the sites and systems in the list, click on the links or view the complete list.

<table>
<thead>
<tr>
<th>Rank</th>
<th>System</th>
<th>Cores</th>
<th>Rmax (TFlop/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sunway TaihuLight - Sunway MPP, Sunway SW26010 260C 1.45GHz, Sunway, NRCPC National Supercomputing Center in Wuxi, China</td>
<td>10,649,600</td>
<td>93,014.6</td>
</tr>
<tr>
<td>2</td>
<td>Tianhe-2 (MilkyWay-2) - TH-ⅡB-FEP Cluster, Intel Xeon E5-2692 12C 2.20GHz, TH Express-2, Intel Xeon Phi 31S1P, NJIIT National Supercomputer Center in Guangzhou, China</td>
<td>3,120,000</td>
<td>33,842.7</td>
</tr>
<tr>
<td>3</td>
<td>Piz Daint - Cray XC50, Xeon E5-2690v3 12C 2.6GHz, Aries interconnect, NVIDIA Tesla P100, Cray Inc. Swiss National Supercomputing Centre (CSCS) Switzerland</td>
<td>361,760</td>
<td>19,590.0</td>
</tr>
<tr>
<td>4</td>
<td>Gyoukou - ZettaScaler-2.2 HPC system, Xeon D-1571 16C 1.3GHz, Infiniband EDR, PEZ1-SC2 700MHz, ExaScaler Japan Agency for Marine-Earth Science and Technology Japan</td>
<td>19,840,000</td>
<td>19,135.8</td>
</tr>
<tr>
<td>5</td>
<td>Titan - Cray XK7, Opteron 6274 16C 2.20GHz, Cray Gemini interconnect, NVIDIA K20x, Cray Inc. DOE/SC/Oak Ridge National Laboratory United States</td>
<td>560,640</td>
<td>17,590.0</td>
</tr>
</tbody>
</table>
Bitcoin Network Energy Consumption

Bitcoin Energy Consumption Relative to Several Countries

- United States
- Russian Federation
- Canada
- Germany
- France
- United Kingdom
- Italy
- Australia
- Netherlands
- Czech Republic
I make blocks by PoS (Proof-of-Stake).

http://ulockblock.com
PoS (Proof-of-Stake)

- Who produces the next block is determined by the stakes in the coin.
  - Weighting: coin-age, ...
- Nxt, Peercoin, Ethereum (Casper Protocol)

- Pros: Fast, Efficient, safe from 51% attack
- Cons: Nothing at Stake, Hard to implement without other problems, centralization by stakes
Witness

I make blocks by DPoS (Delegated Proof-of-Stake).

http://ulockblock.com
DPoS (Delegated Proof-of-Stake)

- Witnesses (or Block Producers), who are elected by stake-weighted voting, produce blocks.
- Bitshares, Steemit, EOS

Pros: Pros of PoS + democratic(?), easier to implement than PoS
Cons: same problems as in the reality: collusions of witnesses, no interests in voting, no way to mine except for witnesses, …
Incentive Compatibility of Bitcoin Consensus Mechanism

- A mechanism is incentive compatible if a player cannot be better off by misreporting.
- 51% attack
- Bitcoin consensus mechanism is **not** incentive compatible, but seems working well, why?
- The more computing power, the more coins they already have or will have from mining properly.
- Thus, if they do 51% attack, they will have a huge loss.
- The same idea applies to other consensus mechanisms, i.e., PoS, DPoS.
51% Attack is really almost impossible?

- 2018.5.29 Bitcoin Gold $18 mn.
- 2018.4-6 3 times! Verge (XVG) $1 mn
- 2018.6.4 ZenCash $0.55 mn

- Note: Attackers can easily test their computing powers (i.e., simulate attacks) in advance.
- Solution to 51% attack?
  - more confirmations
Cryptoeconomics in Economics
Cryptoeconomics in Economics (Econ-CS)

Cryptoeconomics in Economics

Thank you so much!

http://blockchainstudio.tv