CRYPTOCURRENCIES (SESSION II)

Topics in Computer Science and Law
RECAP OF SESSION I:

- Bitcoin - complicated currency
  - Advantages
    - Budding/poorer economies
    - Anonymity…
  - Disadvantages
    - Slow transactions
  - Confusion
    - Anti-institution
    - Commodity or currency?
WHAT WE HOPE TO COVER THIS TIME...

1. Who are the stakeholders, what are their goals, and how do these goals influence one another?

2. How do Bitcoin and other alternative cryptocurrencies, such as Ethereum, Ripple, ZCoin, meet these goals?
In an ideal world, we have a cryptocurrency that:

- is secure, prevents double-spending, is safe
- is independent… but can be trusted like a reputable bank
- is anonymous… but not so anonymous that law enforcement cannot investigate crimes using the cryptocurrency
- has zero transaction fees, infinite money
- supports complex contracts
- supports fast transactions, but is also light-weight, and maybe decentralized
DISCUSSION (PT. I)

• What are the goals of the different stakeholders involved, and how do these goals complement/conflict with one another?
• 3 largest in trading market cap [Bitcoin, Ripple Ethereum]
• Strong anonymity [ZCoin]
• Rigorous white papers

[coinmarketcap.com]
SUMMARY - BITCOIN

• Created in 2009 by “Satoshi Nakomoto”
• Numerous forks - Bitcoin Cash, Bitcoin Gold, Bitcoin Diamond, SegWit2x
CONTEXT - ETHEREUM

• Created in 2015 by Vitalik Buterin
• Blockchain with a built-in Turing-complete programming language
• DAO attack in 2016, loss of $150m – Ethereum branched off the old version of Ethereum Classic
• Casper update: moving to proof of stake in the future
• Created in 2012 by the Ripple Company (Ryan Fugger - 2004)
• Solution to consensus issues: Ripple consensus algorithm + centralization
• Partnerships with banks, others, including:
  • Accenture, American Express, BMO Financial group, RBS, Bank of England, SAP, UBS…
• Created in 2016 by Matthew Green of Johns Hopkins University
• Extension to bitcoin to provide cryptographic anonymity
• Built around the Zerocoin protocol:
  • creation of $C$ from $S$ and $r$
  • usage of accumulators (one-way membership functions)
  • zerocoin escrow pool
# SUMMARY - COINS

<table>
<thead>
<tr>
<th>Coin</th>
<th>Launched</th>
<th>Market Cap</th>
<th>Max Supply</th>
<th>Anonymity</th>
<th>Tx Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitcoin</td>
<td>2009</td>
<td>$124b</td>
<td>~21m</td>
<td>Low</td>
<td>10 min</td>
</tr>
<tr>
<td>Ethereum</td>
<td>2015</td>
<td>$39.7b</td>
<td>infinite</td>
<td>Low</td>
<td>3-5 sec</td>
</tr>
<tr>
<td>Ripple</td>
<td>2012</td>
<td>$20.7b</td>
<td>100b</td>
<td>Low</td>
<td>14 sec</td>
</tr>
<tr>
<td>ZCoin</td>
<td>2016</td>
<td>$135m</td>
<td>~21m</td>
<td>Med-high</td>
<td>&gt;10 min</td>
</tr>
</tbody>
</table>
DISCUSSION (PART II)

• How do Bitcoin and other alternative cryptocurrencies, such as Ethereum, Ripple, and ZCoin, meet the goals discussed in the first part?
  • Do they meet these goals in a technically and legally sound way?
  • Are they practically implemented and/or scalable? Can they be widely adopted?
• If they do not meet the goals, then how should the cryptocurrency community proceed?