Decentralized Autonomous Organization

- Purpose: Venture Capital Fund for blockchain based investments that would be directed by investors (owners of the DAO token)
- Smart contract on Ethereum blockchain designed by Slock.it
- Vision: no management structure, no Board of Directors, no employees
- Code was open-source
- The DAO was stateless – (not tied to any country) – so not obvious how it would (or could) be regulated
Decentralized Autonomous Organization

- Launched –April 4-April 30, 2016 on Ethereum block 1428757 with a crowdsale to fund the organization.
- Ether value about $150 million by May 21 (about 14% of all ether at the time).
- DAO tokens were traded on various exchanges by May 28
- Early example of tokenizing ether
## Background

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price</th>
<th>Available Supply</th>
<th>Volume (24h)</th>
<th>% Change (24h)</th>
<th>Price Graph (7d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$ 11,459,744,792</td>
<td>$ 731.67</td>
<td>15,662,450 BTC</td>
<td>$ 154,246,000</td>
<td>7.09 %</td>
<td><img src="https://example.com/graph-bitcoin" alt="Graph for Bitcoin" /></td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$ 1,527,999,289</td>
<td>$ 18.85</td>
<td>81,060,110 ETH</td>
<td>$ 22,585,100</td>
<td>1.42 %</td>
<td><img src="https://example.com/graph-ethereum" alt="Graph for Ethereum" /></td>
</tr>
<tr>
<td>3</td>
<td>Litecoin</td>
<td>$ 250,487,328</td>
<td>$ 5.42</td>
<td>46,242,676 LTC</td>
<td>$ 4,773,220</td>
<td>4.25 %</td>
<td><img src="https://example.com/graph-litecoin" alt="Graph for Litecoin" /></td>
</tr>
<tr>
<td>4</td>
<td>Ripple</td>
<td>$ 236,709,866</td>
<td>$ 0.006789</td>
<td>34,868,679,462 XRP *</td>
<td>$ 3,391,510</td>
<td>-4.55 %</td>
<td><img src="https://example.com/graph-ripple" alt="Graph for Ripple" /></td>
</tr>
<tr>
<td>5</td>
<td>The DAO</td>
<td>$ 205,587,485</td>
<td>$ 0.175300</td>
<td>1,172,775,159 DAO *</td>
<td>$ 1,901,380</td>
<td>3.35 %</td>
<td><img src="https://example.com/graph-the-dao" alt="Graph for The DAO" /></td>
</tr>
</tbody>
</table>

June 16, 2016
Background

Reentrancy Bug

- June 9, 2016, two developers reported that most Ethereum based contracts that managed funds were vulnerable to a bug that could empty funds.
- June 12, 2016 Stephan Tual, founder of Slock.it reported that The DAO code was not vulnerable to this exploit.
Background

Reentrancy Bug

• Crucial part of code had two lines in the wrong order (allowing withdrawal of ether repeatedly before checking if the attacker was entitled to withdraw)

• Suppose you have $100 in a bank account. Think of bringing the bank teller a stack of $100 withdrawal slips and the teller gives you $100 for each one until the bank runs out of money. At that point, they register the $100 debit and have no idea you took everything.
Background

Decentralized Autonomous Organization

- June 17, 2016 The DAO attacked and user gained access to about $50 million of ETH (30% of ether in the contract)
- Simultaneously, another group, Robin Hood Group (RHG), used the same exploit (but promised to return all ether to the original owners) (they got the remaining 70%)

https://github.com/ethereumbook/ethereumbook/blob/develop/appdx-forks-history.asciidoc
Background

Decentralized Autonomous Organization

- Funds put in a 28-day holding period (as per the contract) before they could be withdrawn
- Community debated what to do with a July 20 deadline (end of 28-day period): should they rewrite history by hard forking?

https://github.com/ethereumbook/ethereumbook/blob/develop/appdx-forks-history.asciidoc
<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>Market Cap</th>
<th>Price (USD)</th>
<th>Available Supply</th>
<th>Volume (24h)</th>
<th>% Change (24h)</th>
<th>Price Graph (7d)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Bitcoin</td>
<td>$11,601,336,569</td>
<td>$740.40</td>
<td>15,667,150 BTC</td>
<td>$292,422,000</td>
<td>0.72%</td>
<td><img src="" alt="Graph" /></td>
</tr>
<tr>
<td>2</td>
<td>Ethereum</td>
<td>$1,344,508,652</td>
<td>$16.58</td>
<td>81,100,025 ETH</td>
<td>$78,067,600</td>
<td>-15.46%</td>
<td><img src="" alt="Graph" /></td>
</tr>
<tr>
<td>3</td>
<td>Litecoin</td>
<td>$250,234,196</td>
<td>$5.41</td>
<td>46,260,851 LTC</td>
<td>$12,661,100</td>
<td>0.17%</td>
<td><img src="" alt="Graph" /></td>
</tr>
<tr>
<td>4</td>
<td>Ripple</td>
<td>$234,018,766</td>
<td>$0.006666</td>
<td>35,108,326,973 XRP*</td>
<td>$2,869,430</td>
<td>-0.63%</td>
<td><img src="" alt="Graph" /></td>
</tr>
<tr>
<td>5</td>
<td>The DAO</td>
<td>$91,336,316</td>
<td>$0.077881</td>
<td>1,172,775,159 DAO*</td>
<td>$6,282,860</td>
<td>-56.52%</td>
<td><img src="" alt="Graph" /></td>
</tr>
</tbody>
</table>
Mechanism

Hard fork

• July 20, 2016 hard fork at block 1,920,000 and rewrote history returning the DAO directed ether to the investors

• The old protocol became Ethereum Classic (ETC) preserved history (and immutability property). RHG now needs to return 70% of the ETC to the original investors
Mechanism

Hard forks vs. soft forks

• Soft forks are relatively minor software changes
• Soft forks are software upgrades that are backward compatible with previous versions
• Nodes do not need to upgrade to new version to form consensus
Mechanism

Hard forks vs. soft forks

- Hard forks are major software changes
- Hard forks are not backward compatible with previous versions
- Nodes need to follow new rules for consensus
- Hard forks can be planned (Constantinople) or contentious (ETC)

https://www.mycryptopedia.com/hard-fork-soft-fork-explained/
Is it a Security?

Decentralized Autonomous Organization

• July 26, 2016 The SEC rules that DAO tokens were “securities” subject to federal securities laws.

• ...issuers of distributed ledger or blockchain technology-based securities must register offers and sales of such securities unless a valid exemption applies. Those participating in unregistered offerings also may be liable for violations of the securities laws. Additionally, securities exchanges providing for trading in these securities must register unless they are exempt. The purpose of the registration provisions of the federal securities laws is to ensure that investors are sold investments that include all the proper disclosures and are subject to regulatory scrutiny for investors' protection.

Lessons

Smart Contracts

• Not all smart contracts are smart
• Once contract is deployed, it cannot be “fixed”
Reading

Here is a list of reading (including DAICO and Curation)

• [http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/](http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/)
  – [https://ethresear.ch/t/explanation-of-daicos/465](https://ethresear.ch/t/explanation-of-daicos/465)
• [https://medium.com/@simondlr/tokens-2-0-curved-token-bonding-in-curation-markets-1764a2e0bee5](https://medium.com/@simondlr/tokens-2-0-curved-token-bonding-in-curation-markets-1764a2e0bee5)
• [https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7](https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7)