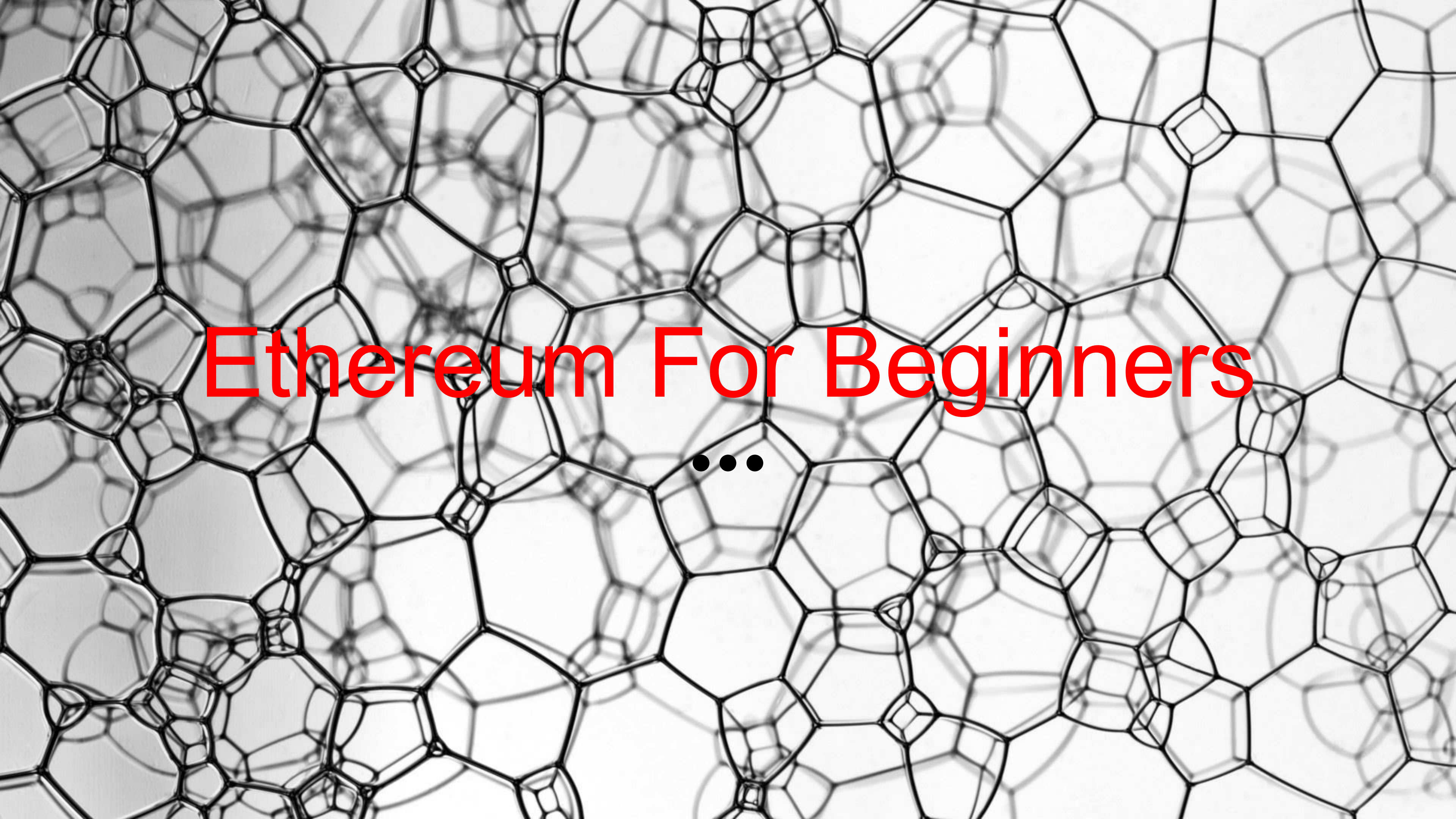
Ethereum For Beginners

•••



Introduction to Ethereum

The components of blockchain technology
The Ethereum platform and writing distributed applications
Let’s create a Crypto Currency
Implications for the web, business and society

What is Ethereum ?

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

Blockchain 2.0 - Ethereum

How is Ethereum different from Bitcoin ?

more general, not just a currency
each node has a virtual machine forming a planetary scale computer
the virtual machines run "smart contracts"
users can call functions on the contract = transactions

The core idea was simple: a blockchain with a built-in Turing-complete programming language, allowing users to build any kind of applications on top. - Vitalik Buterin
"There is nothing that bitcoin can do which Ethereum can’t. While Ethereum is less battle tested, it is moving faster, has better leadership and has more developer mindshare. " -Fred Ehrsam Coinbase co founder

tl:dr

There is no Central Authority
It’s all about trust

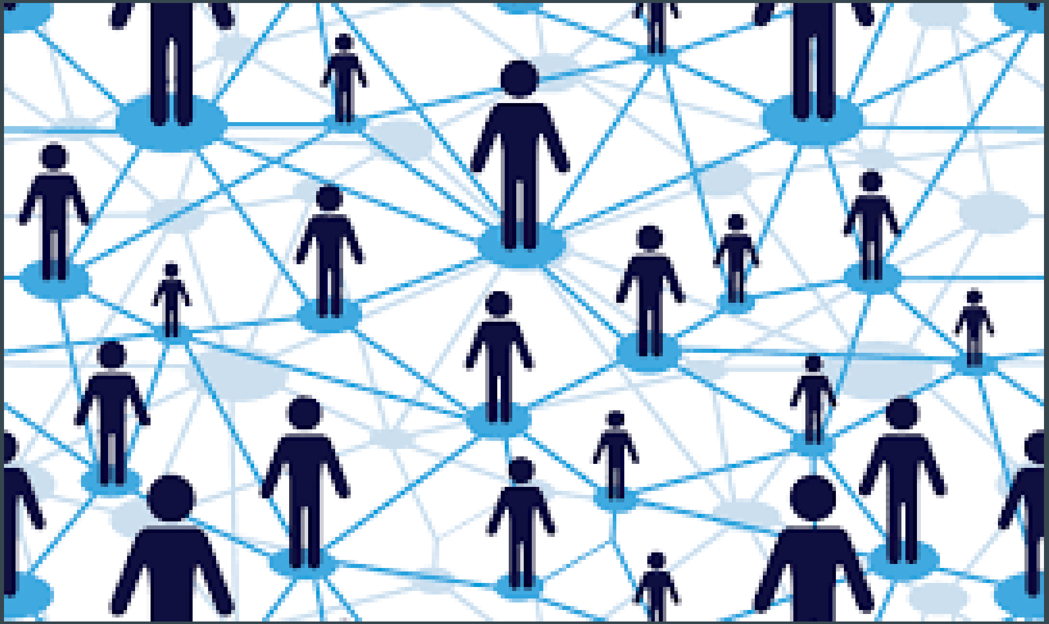
The Issue of trust

All human societies have a trust problem. Many societies have invented elaborate rituals, laws and governance systems to address this trust problem. At its most fundamental level, blockchain technology tries to do the same.
While the Internet provides us with a great way to communicate with individuals the world over, it is difficult to enter into an agreement with them; typically, we must trust either them directly (in the case of an e-commerce site, for example) or a third-party that vouches for them. Both are susceptible to the sorts of abuse that blockchain-based technology can mitigate or remove entirely. - Gavin Wood

Convergence of technologies

- Peer to peer networking
- The Blockchain Mechanism
- Cryptography

Peer to Peer Networks



A Decentralised Network

- No single point of failure
- Censorship proof
- Highly Reliable

Examples :
Napster
Bit Torrent
Spotify

The Blockchain Mechanism

A public ledger - all transactions can be seen by all users of the system

The state of the system is arrived at by a consensus protocol

Cryptography

Public / Private Key Cryptography

Transactions are tamper proof

The origin of a transaction can be verified

(The Public Key is hashed with SHA-3 to produce a 256-bit output. The upper 96 bits are discarded, and the lower 160 bits become the Account Address.)

The peer to peer network gives us a distributed, censorship resistant platform

The blockchain gives us transparency,verifiable consistency and consensus

Cryptography gives us secure, tamper proof transactions

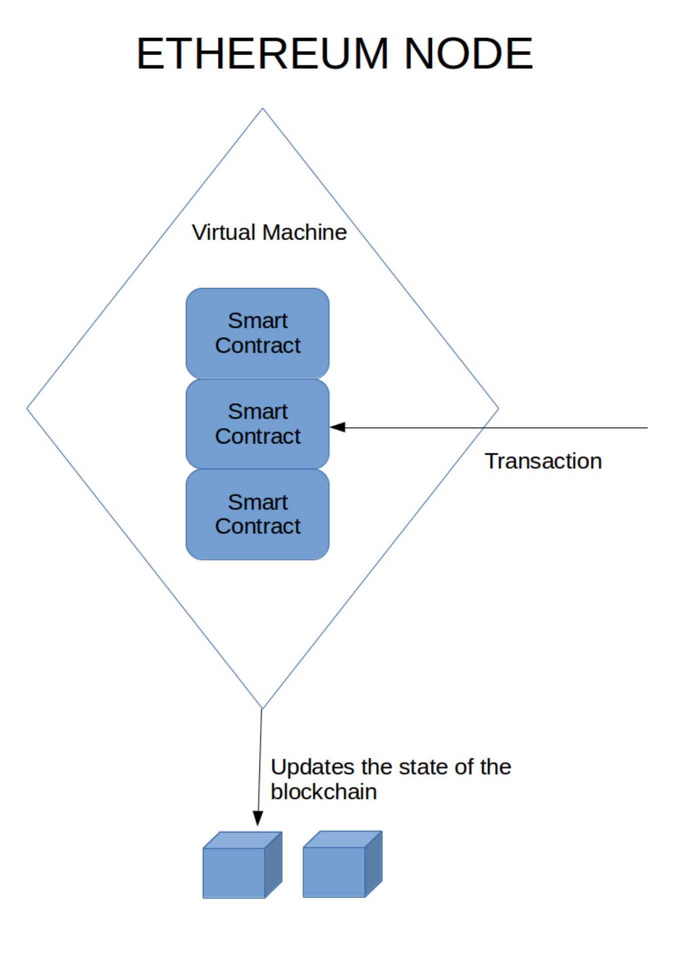
The blockchain lets people who have no particular confidence in each other collaborate without having to go through a neutral central authority.

Simply put, the blockchain is a machine for creating trust.

Smart Contracts

- Contracts lives on the Ethereum blockchain
- They have their own Ethereum address and balance
- They can send and receive transactions
- They are activated when they receive a transaction, and can be deactivated
- The Ethereum Virtual Machine runs a turing complete language
- They have a fee per CPU step, with extra for storage
- The user can run the application on their local block chain

Ethereum Node



Ethereum Programming Languages

Smart contracts can be written in

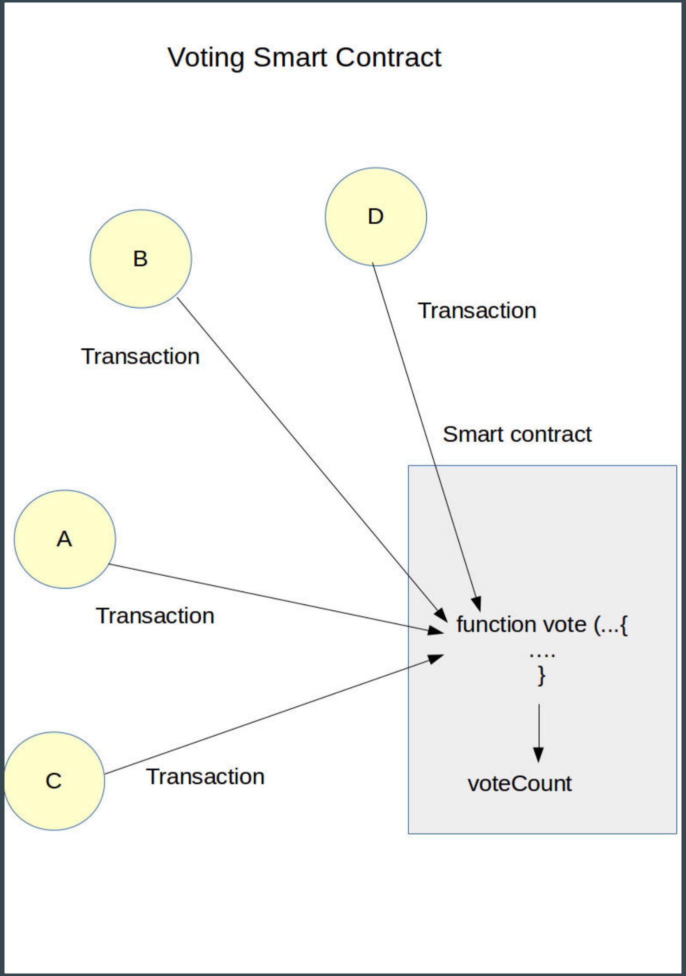
Solidity (a **JavaScript-like** language)
Serpent (a **Python-like** language),
Mutan (C-like)
LLL (**Lisp**-like).

They are compiled into bytecode before being deployed to the **blockchain**.

An Example Smart Contract - A voting application

The state of the contract (voteCount) is maintained on the blockchain along with the smart contract

After a certain time the smart contract will end the election and publish the results



```
contract Ballot {

    struct Voter {
        uint weight;
        bool voted;
        uint8 vote;
        address delegate;
    }
    struct Proposal {
        uint voteCount;
    }

    address chairperson;
    mapping(address => Voter) voters;
    Proposal[] proposals;

    // Create a new ballot
    function Ballot(uint8 _numProposals) {
        chairperson = msg.sender;
        voters[chairperson].weight = 1;
        proposals.length = _numProposals;
    }

}
```

```
    // Give a single vote
    function vote(uint8 proposal) {
        Voter sender = voters[msg.sender];
        if (sender.voted || proposal >= proposals.length)
return;
        sender.voted = true;
        sender.vote = proposal;
        proposals[proposal].voteCount += sender.weight;
    }

    function winningProposal() constant returns (uint8
winningProposal) {
        uint256 winningVoteCount = 0;
        for (uint8 proposal = 0; proposal <
proposals.length; proposal++)
            if (proposals[proposal].voteCount >
winningVoteCount) {
                winningVoteCount =
proposals[proposal].voteCount;
                winningProposal = proposal;
            }
    }
```

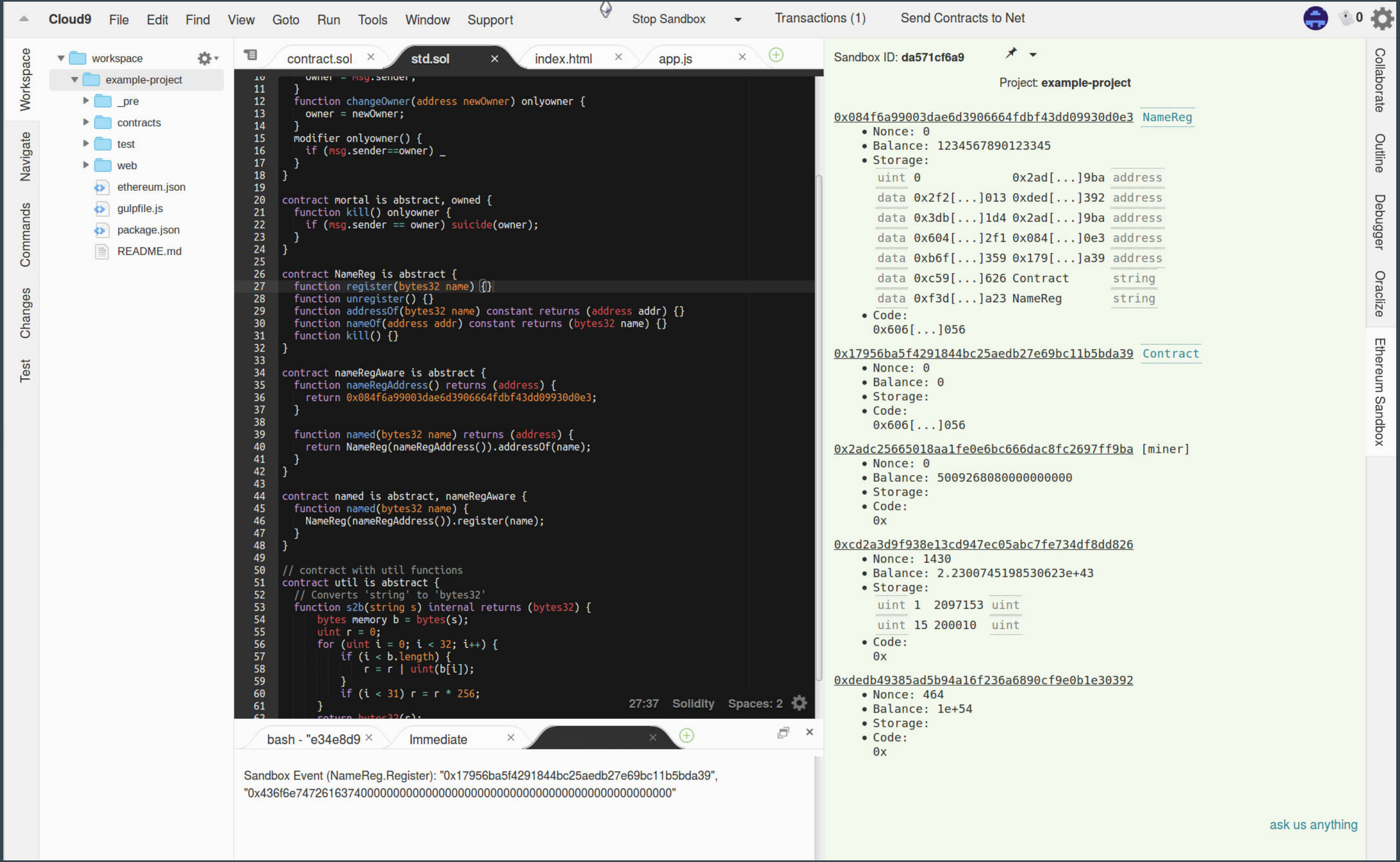
ethereum

Ether buys GAS to fuel the EVM

Every opcode instruction executed by the EVM uses up Gas.

Creating a Crypto Currency Demo

Ethereum IDEs



```
    owner = msg.sender;
  }
  function changeOwner(address newOwner) onlyowner {
    owner = newOwner;
  }
  modifier onlyowner() {
    if (msg.sender==owner) _
  }
}

contract mortal is abstract, owned {
  function kill() onlyowner {
    if (msg.sender == owner) suicide(owner);
  }
}

contract NameReg is abstract {
  function register(bytes32 name) {}
  function unregister() {}
  function addressOf(bytes32 name) constant returns (address addr) {}
  function nameOf(address addr) constant returns (bytes32 name) {}
  function kill() {}
}

contract nameRegAware is abstract {
  function nameRegAddress() returns (address) {
    return 0x084f6a99003dae6d3906664fdbf43dd09930d0e3;
  }

  function named(bytes32 name) returns (address) {
    return NameReg(nameRegAddress()).addressOf(name);
  }
}

contract named is abstract, nameRegAware {
  function named(bytes32 name) {
    NameReg(nameRegAddress()).register(name);
  }
}

// contract with util functions
contract util is abstract {
  // Converts 'string' to 'bytes32'
  function s2b(string s) internal returns (bytes32) {
      bytes memory b = bytes(s);
      uint r = 0;
      for (uint i = 0; i < 32; i++) {
          if (i < b.length) {
              r = r | uint(b[i]);
          }
          if (i < 31) r = r * 256;
      }
      return bytes32(r);
```

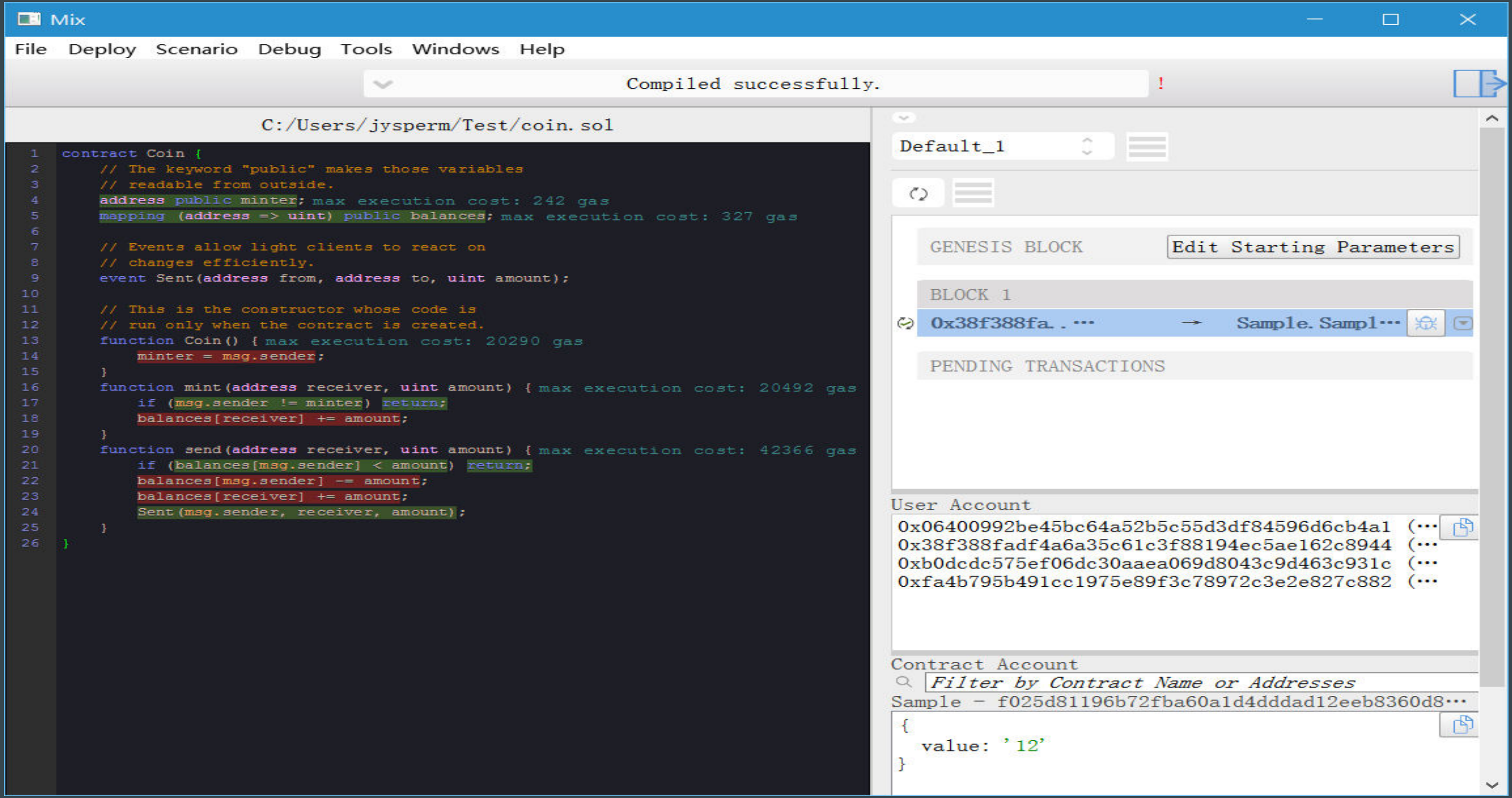
```
Sandbox ID: da571cf6a9

Project: example-project

0x084f6a99003dae6d3906664fdbf43dd09930d0e3 NameReg
  • Nonce: 0
  • Balance: 1234567890123345
  • Storage:
    uint 0                0x2ad[...]9ba address
    data 0x2f2[...]013 0xded[...]392 address
    data 0x3db[...]1d4 0x2ad[...]9ba address
    data 0x604[...]2f1 0x084[...]0e3 address
    data 0xb6f[...]359 0x179[...]a39 address
    data 0xc59[...]626 Contract      string
    data 0xf3d[...]a23 NameReg       string
  • Code:
    0x606[...]056

0x17956ba5f4291844bc25aedb27e69bc11b5bda39 Contract
  • Nonce: 0
  • Balance: 0
  • Storage:
  • Code:
    0x606[...]056

0x2adc25665018aa1fe0e6bc666dac8fc2697ff9ba [miner]
  • Nonce: 0
  • Balance: 5009268080000000000
  • Storage:
  • Code:
    0x

0xcd2a3d9f938e13cd947ec05abc7fe734df8dd826
  • Nonce: 1430
  • Balance: 2.2300745198530623e+43
  • Storage:
    uint 1  2097153 uint
    uint 15 200010  uint
  • Code:
    0x

0xdedb49385ad5b94a16f236a6890cf9e0b1e30392
  • Nonce: 464
  • Balance: 1e+54
  • Storage:
  • Code:
    0x
```

```
Sandbox Event (NameReg.Register): "0x17956ba5f4291844bc25aedb27e69bc11b5bda39",
"0x436f6e7472616374000000000000000000000000000000000000000000000000"
```

TRUFFLE

Truffle is a development environment, testing framework and asset pipeline for Ethereum,
Automated contract testing with Mocha and Chai.

MIX IDE



Compiled successfully.

C:/Users/jysperm/Test/coin.sol

```
contract Coin {
    // The keyword "public" makes those variables
    // readable from outside.
    address public minter; max execution cost: 242 gas
    mapping (address => uint) public balances; max execution cost: 327 gas

    // Events allow light clients to react on
    // changes efficiently.
    event Sent(address from, address to, uint amount);

    // This is the constructor whose code is
    // run only when the contract is created.
    function Coin() { max execution cost: 20290 gas
        minter = msg.sender;
    }
    function mint(address receiver, uint amount) { max execution cost: 20492 gas
        if (msg.sender != minter) return;
        balances[receiver] += amount;
    }
    function send(address receiver, uint amount) { max execution cost: 42366 gas
        if (balances[msg.sender] < amount) return;
        balances[msg.sender] -= amount;
        balances[receiver] += amount;
        Sent(msg.sender, receiver, amount);
    }
}
```

User Account

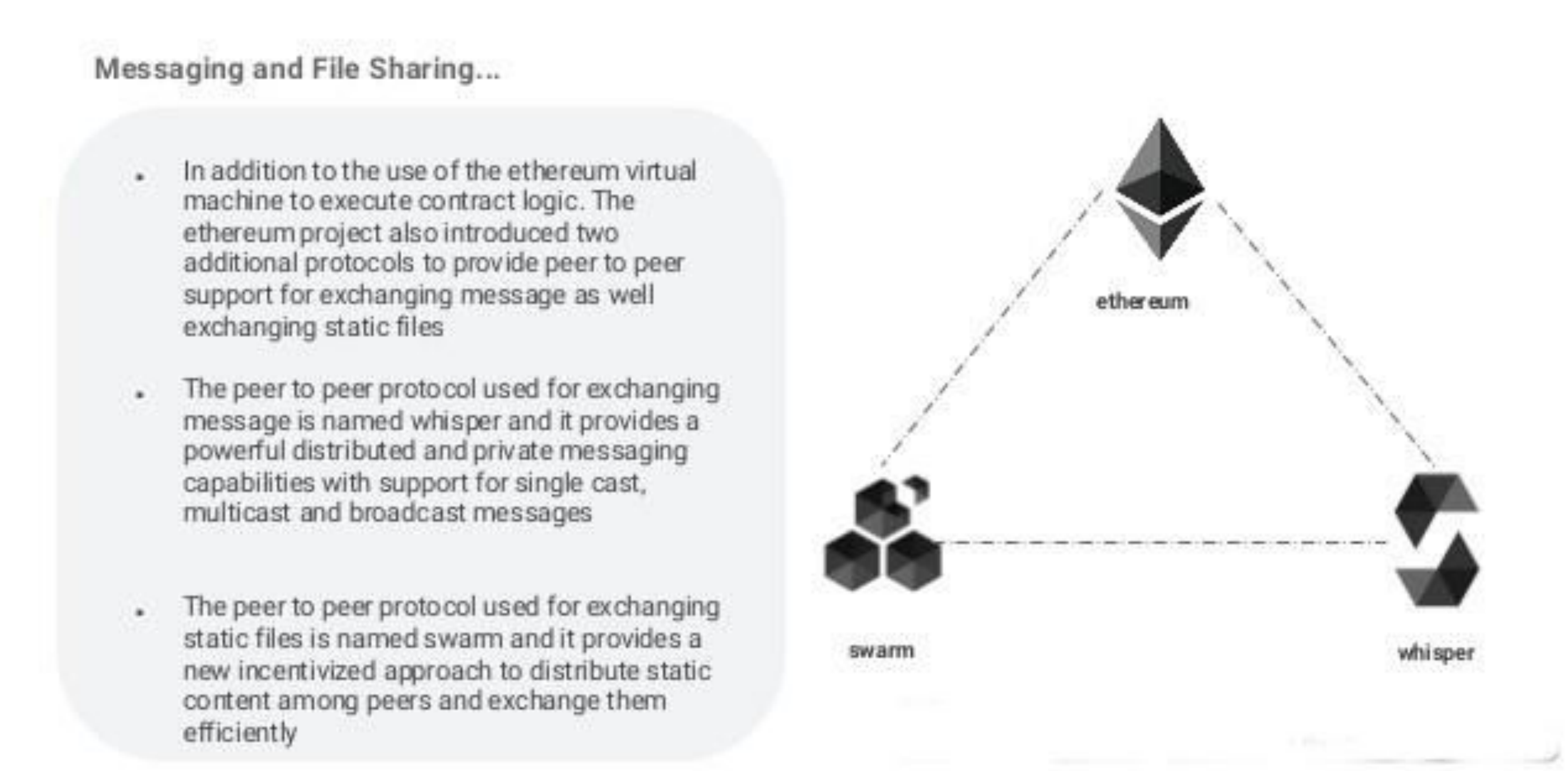
```
0x06400992be45bc64a52b5c55d3df84596d6cb4a1 (···
0x38f388fadf4a6a35c61c3f88194ec5ae162c8944 (···
0xb0dcdc575ef06dc30aaea069d8043c9d463c931c (···
0xfa4b795b491cc1975e89f3c78972c3e2e827c882 (···
```

Contract Account

Sample − f025d81196b72fba60a1d4dddad12eeb8360d8···

```
{
  value: '12'
}
```

Not just Smart Contracts



Messaging and File Sharing...

- In addition to the use of the ethereum virtual machine to execute contract logic. The ethereum project also introduced two additional protocols to provide peer to peer support for exchanging message as well exchanging static files
- The peer to peer protocol used for exchanging message is named whisper and it provides a powerful distributed and private messaging capabilities with support for single cast, multicast and broadcast messages
- The peer to peer protocol used for exchanging static files is named swarm and it provides a new incentivized approach to distribute static content among peers and exchange them efficiently

Why Use Ethereum ?

Uptime
Security
Almost Free
Transparency
Micro payments
DAOs ,Consensus applications , governance
Identity / Reputation Services

Limitations

The Ethereum Virtual Machine is slow, don’t use it for large computations
Storage on the block chain is expensive, use IPFS / Swarm
Scalability is an issue, there is a trade off with decentralisation
Private block chains are likely to proliferate

Implications

- third-party intermediaries are not needed in order to conduct transactions between two (or several) parties.
- end-to-end resolution to be self-managed between computers that represent the interests of the users.
- disintermediation

Who should be worried about Ethereum

Middle Men

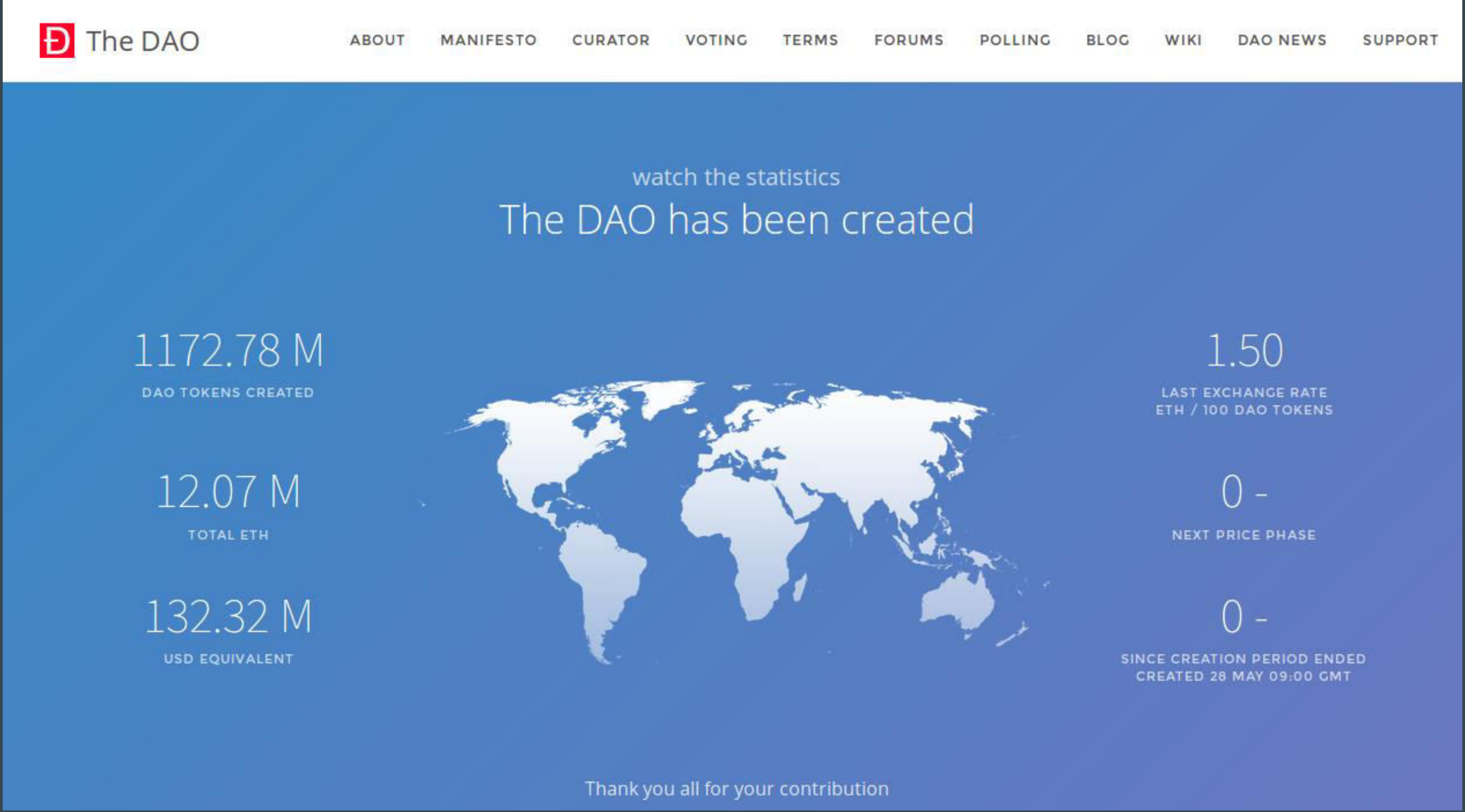
- Kickstarter take a 5% fee
- OpaVote charges $500 for an election
- Uber / Amazon / * Agencies
- Meetup
- Anyone involved in corruption
- Centralised Businesses and Organisations

Decentralised Autonomous Organisations

A Business organisation run according to rules specified in a smart contract

The DAO contains some kind of internal property that is valuable in some way, and it has the ability to use that property as a mechanism for rewarding certain activities.

- Outsiders can see the governance algorithm
- It may use voting or prediction markets to choose policy



watch the statistics

The DAO has been created

1172.78 M
DAO TOKENS CREATED

12.07 M
TOTAL ETH

132.32 M
USD EQUIVALENT

1.50
LAST EXCHANGE RATE
ETH / 100 DAO TOKENS

0 -
NEXT PRICE PHASE

0 -
SINCE CREATION PERIOD ENDED
CREATED 28 MAY 09:00 GMT

Thank you all for your contribution

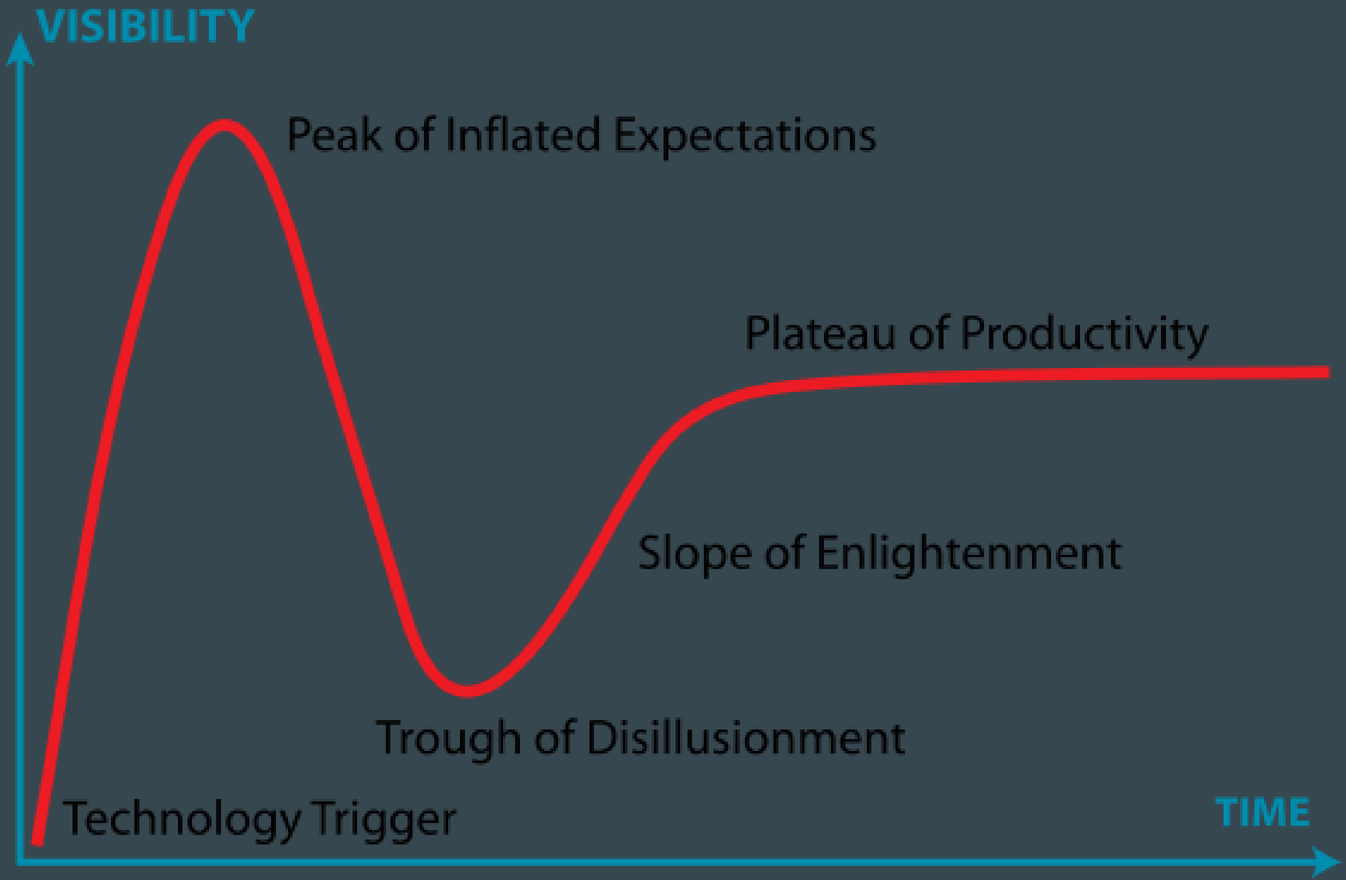
A Call for a Temporary Moratorium on The DAO

http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/

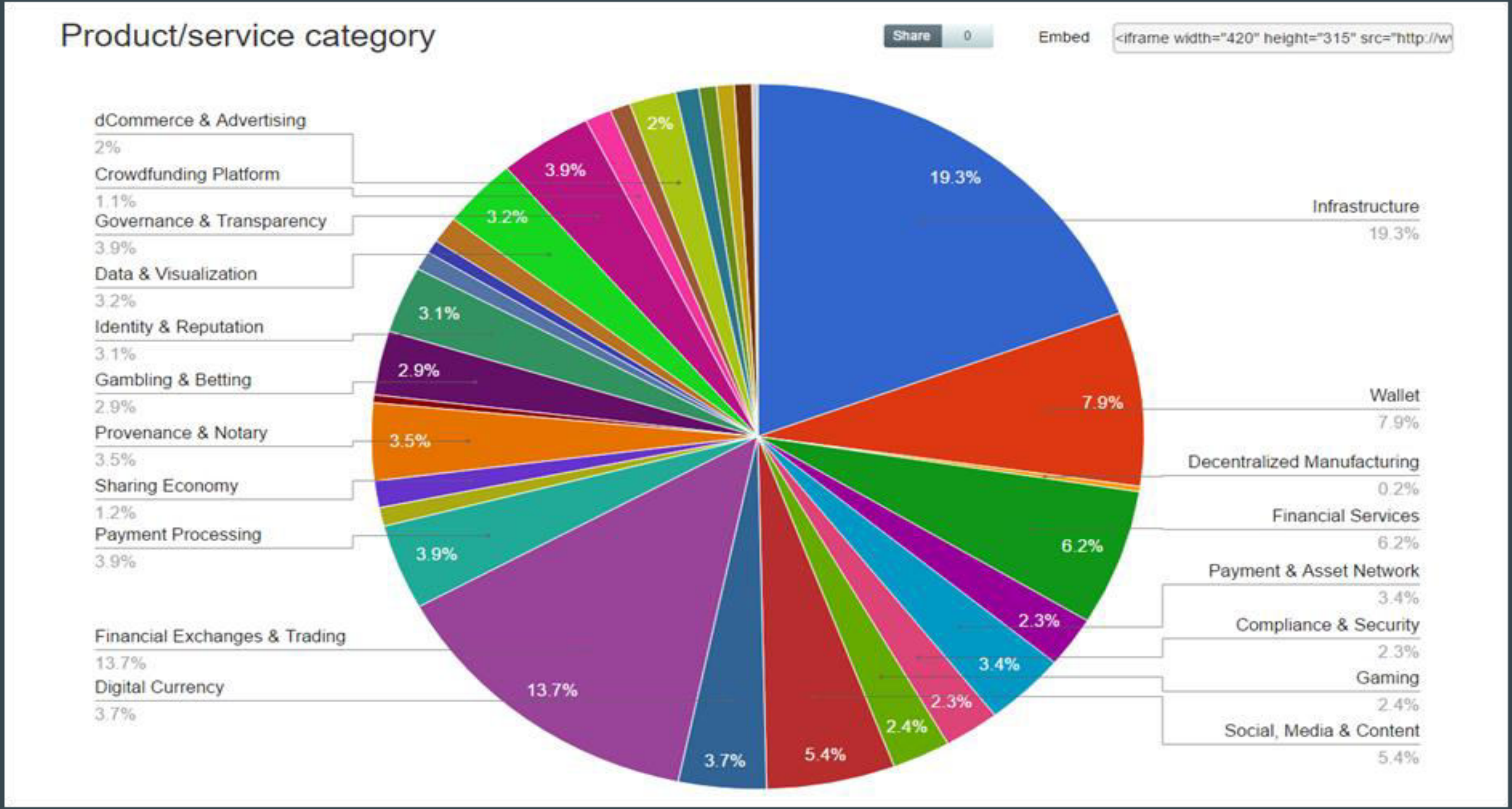
Governance

- Liquid Democracy
- Holacracy
- Futarchy

Is this all a lot of hype ?



Who is using Ethereum Now ?



augur

Decentralised Prediction Market

Provenance

Provenance powers supply chain transparency and secure traceability for materials, ingredients and products.

COLONY

Colony harnesses the wisdom of the crowd using AI to make sure that the right things get done by the right people, at the right time.

MAKER

Autonomous bank & market maker

ujo MUSIC

Rebuilding the music industry on the block chain

Storj - Encrypted distributed storage
Rent out space on your hard drive

TRANSACTIVEGRID

Blockchain based microgrid
Brooklyn consumers can transform their homes into connected power stations.

Safemarket - Ethereum version of Open Bazaar

OTONOMOS

TAKE YOUR COMPANY FROM ANALOG TO DIGITAL

ETHEREUM AND IOT

Slock.it

Rent, sell or share anything - without middlemen
With Slock.it, Airbnb apartments become fully automated, wifi routers can be rented on demand and unused office spaces get a new lease on life. It's the future infrastructure of the Sharing Economy.

HYPE ‘R’ LEDGER

Next Steps

Proof of Stake
Sharding
Ring Signature Mixer
Micro payments
DAOs ,Consensus applications , governance
Identity / Reputation Services

Proof of Stake

50000-foot view summary: the blockchain is a prediction market on itself. - Vitalik Buterin

Links

Ethereum Oxford
LJC Hack The Tower - June 11