Making Dapps with JavaScript

Chris Hitchcott, Nov 2015

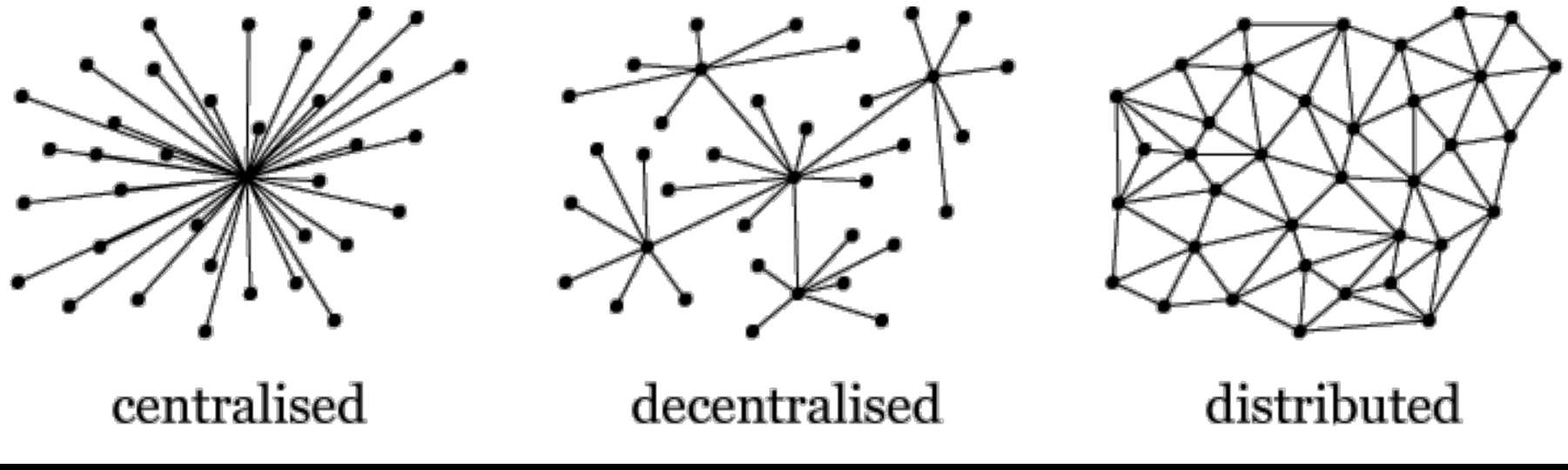
Bitcoin &
Blockchain &
Smart Contracts &
Web 3.0 &
Ethereum

Who has heard of these things?

A New Architecture for a new Web

- **Old Web 2.0** Client / Server
  HTTP, REST, FTP, ‘The Cloud’, CDN, Data Center

- **New Web 3.0** Distributed
  BitTorrent, WebRTC, Blockchain, IPFS



Web 3.0
Why Distributed is Better

- **Harder**
  Censoring is difficult if you need to censor everyone
- **Better**
  Because reasons
- **Faster**
  Lower latency and greater bandwidth
- **Stronger**
  No single points failure

BLOCKCHAIN SMART CONTRACT TECHNOLOGY

BUZZWORDS OF 2015

Blockchain

A Magical Sky Computer

INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA

The Economist

OCTOBER 31ST–NOVEMBER 6TH 2015 Economist.com

Our guide to America's best colleges

Myanmar's free-ish election

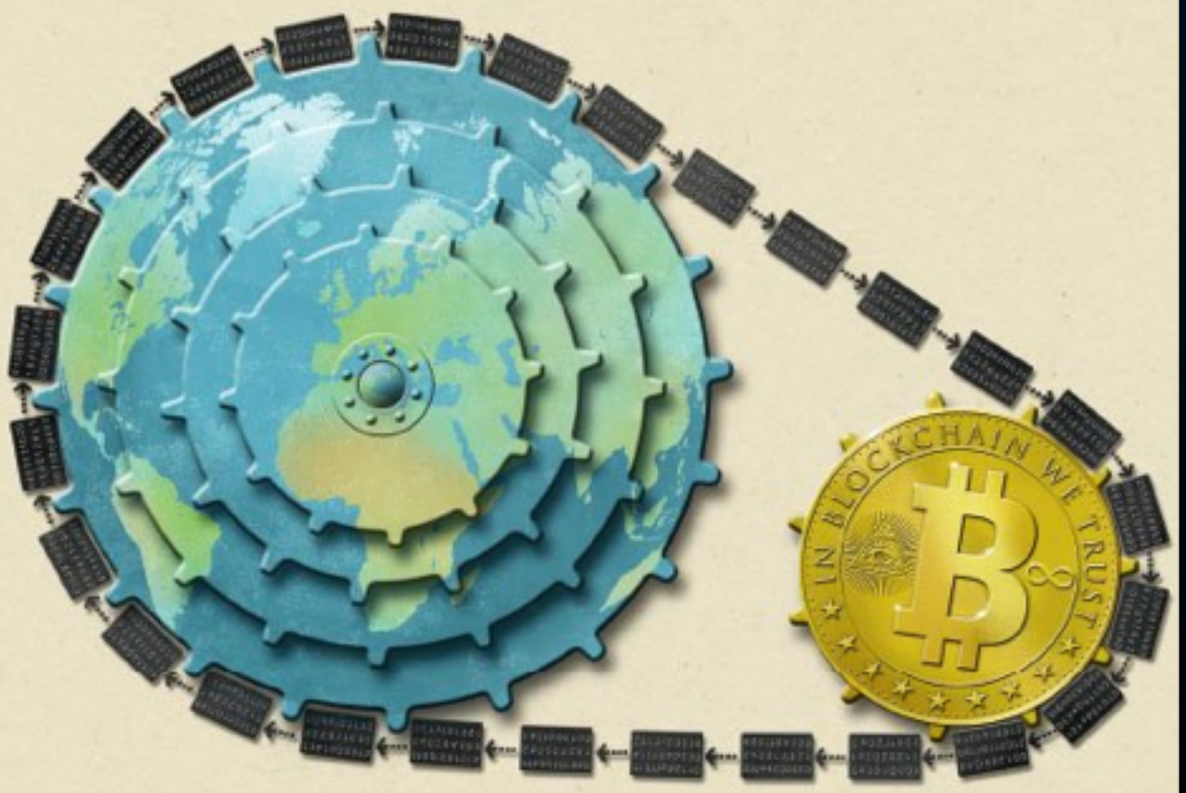
Those ever-creative accountants

America takes the fight to IS

Coywolves: the new superpredator

The trust machine

How the technology behind bitcoin could change the world



0 71486 02674 7 44

Australia	A$10 (inc. GST)	Hong Kong	HK$ 80	Korea	Won 11,000	New Zealand	NZ$12.00	Sri Lanka	Rs1,000
Bangladesh	Tk470	India	₹320	Malaysia	RM25.50	Pakistan	Rs640	Taiwan	NT$275
Cambodia	US$8.00	Indonesia	Rp77,000	Myanmar	US$8.00	Philippines	Pesos 185	Thailand	Baht 200
China	RMB 75	Japan	¥1,345 inc Tax	Nepal	NR$ 600	Singapore	S$12.50 (inc GST)	Vietnam	US$4.00

What is Blockchain?

- A peer-to-peer DBaaS that cannot be turned off or censored
- Not really a tangible ‘thing’ but a **protocol**
- The protocol allows nodes on the network to come to a **consensus** about the **state of the network**
- The protocol typically uses **cryptography** and **economic incentives** to prevent bad data it even if there are **bad actors with lots of resources**

Mining

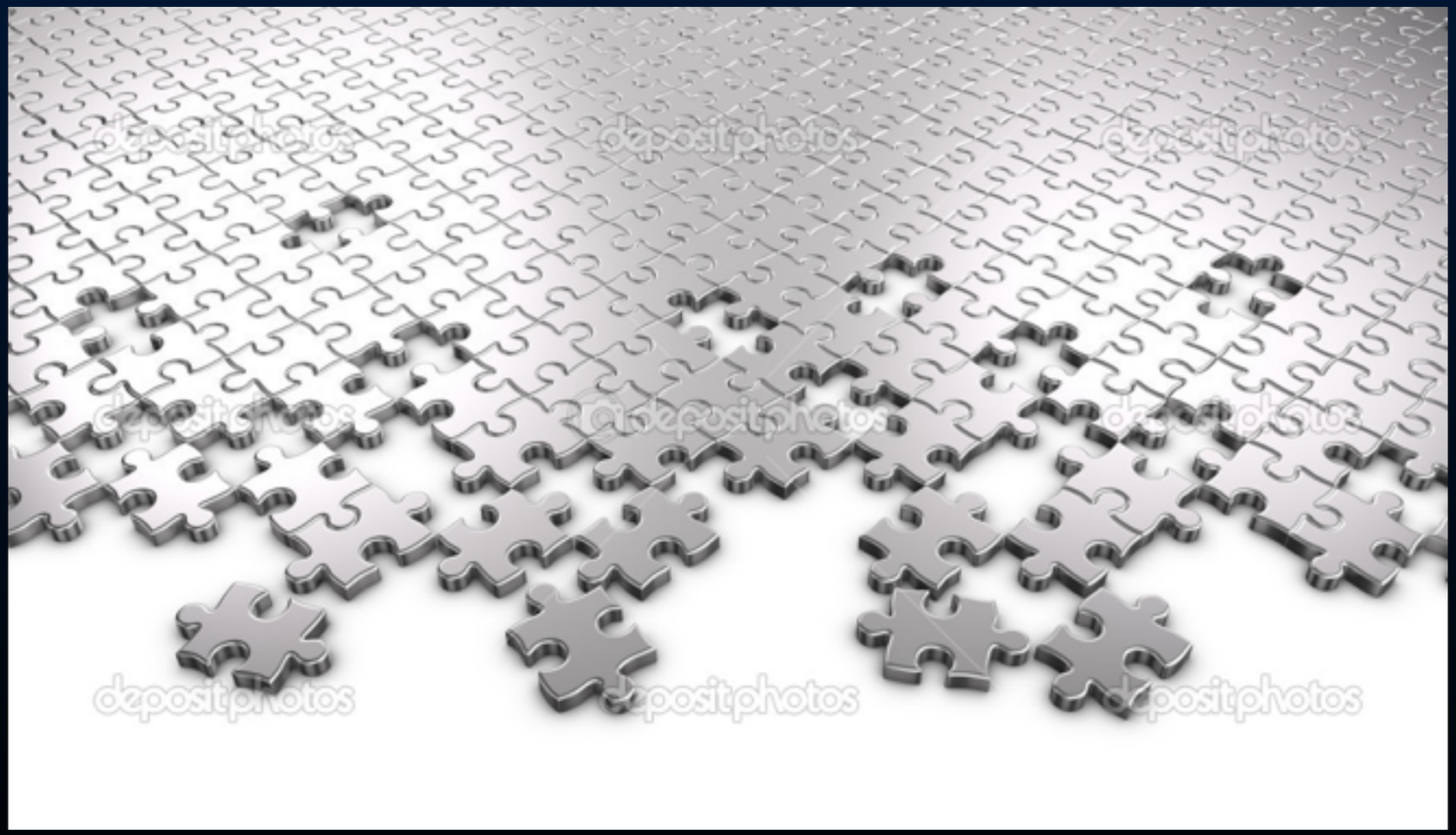
Economic Consensus

Why Blockchain?

- **Immutability** once written never forgotten

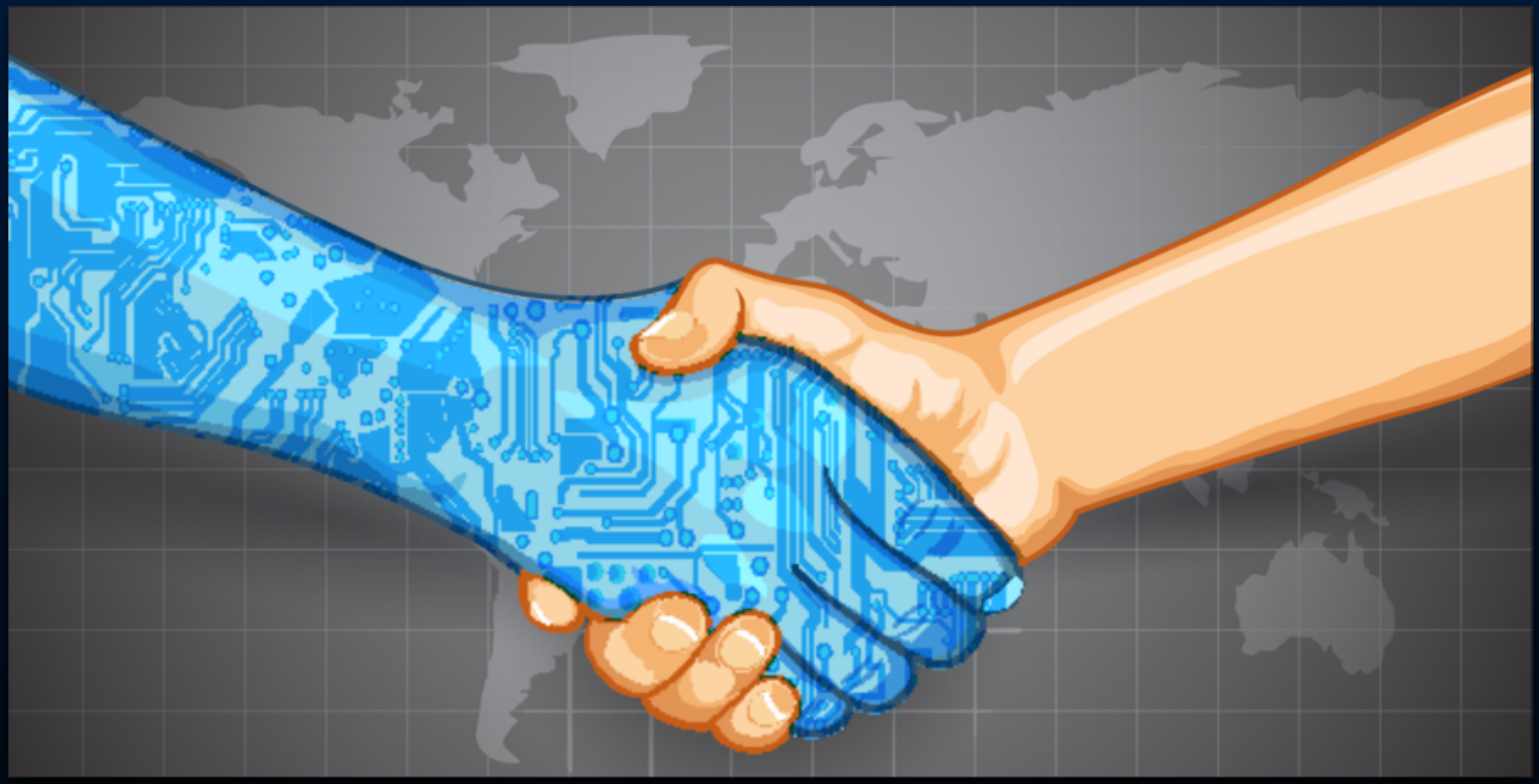
Why Blockchain?

- **Immutability** once written never forgotten



Why Blockchain?

- **Immutability** once written never forgotten
- **Availability** always on, for a small fee
- It's possible to **execute logic** on the blockchain
- **Bitcoin** is an example of this, but is **just the tip**
- **Security** that your deployed logic will behave as expected; no double spending (vs PayPal)



Smart Contract Land

A brave new world where **code is law** and information has **property rights**

With **smart contracts**, programs can do **incredible** things that they have never been able to do before *

* without there being a central point of failure

Coin

Multisig Wallet

Dead Man's Switch

Sealed Bid Auction


CHINESE
IMPERIAL
RAILWAY
FIVE PER CENT. GOLD LOAN for £1,500,000
STERLING
CANTON-KOWLOON RAILWAY.
CHINESE IMPERIAL FIVE PER CENT. GOVERNMENT GUARANTEED BOND.
AMOUNT OF LOAN £1,500,000 IN 15,000 BONDS OF £100 EACH, Nos 1 to 15000
PRINCIPAL AND INTEREST FREE FROM CHINESE TAXES AND IMPOSTS
BOND FOR £100

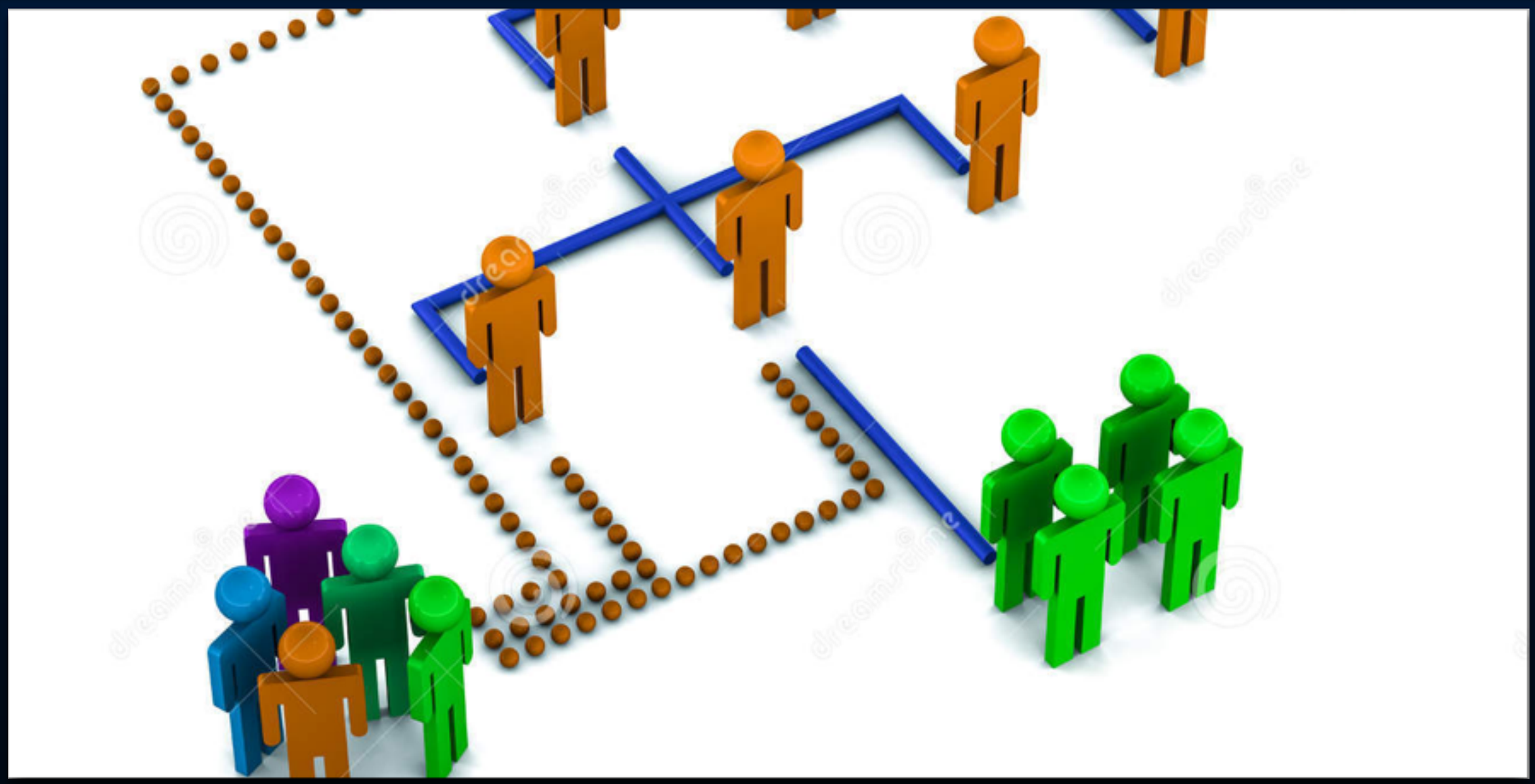
Smart Bonds

https://youtu.be/jgJxEHwj-XU?t=4m24s

Disintermediation

Cutting out the middle man

#fintech #startup



DAO

Decentralized Autonomous Organization

DAOs

- **Startup** Equity Crowd Fund + Dividend
- **Business** Salary Contracts + Board of Directors
- **Hedge Fund** Low-barrier crowd funded investments
- **Charity** remove the layers of bureaucracy
- **Government** totally transparent spending

The Kicker?

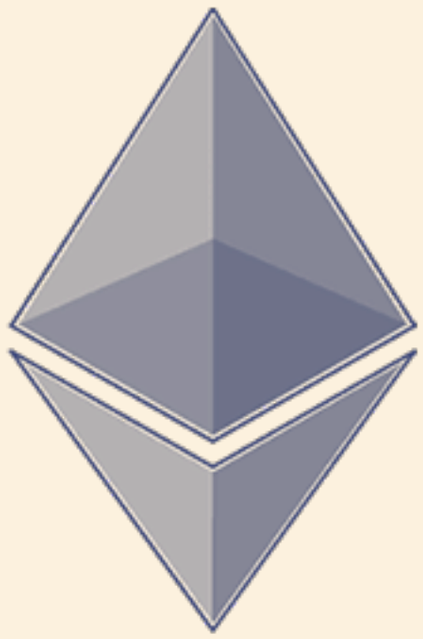
It’s all extremely low cost

Think of all the money that is spent on intermediaries today.

Use blockchain tech to automate those roles, and put that money back into the economy.

Starting to see why banks are so interested?

So **how** do you make these kinds of apps?



ethereum

With **Ethereum**, you can write and deploy **smart contracts** without having to be a **computer scientist crypto-boffin**

…just being a **web developer** will do

What is **Ethereum**?

Decentralized mining network
and **software development**
platform rolled into one

– Vitalik Buterin

Thug Life

ethereum

https://www.ethereum.org

Repositories | People 26

Filters | Find a repository...

go-ethereum

Go ★ 741 ⑂ 250

Official golang implementation of the Ethereum protocol

Updated 30 minutes ago

ethereumj

Java ★ 158 ⑂ 80

Java implementation of the Ethereum yellowpaper

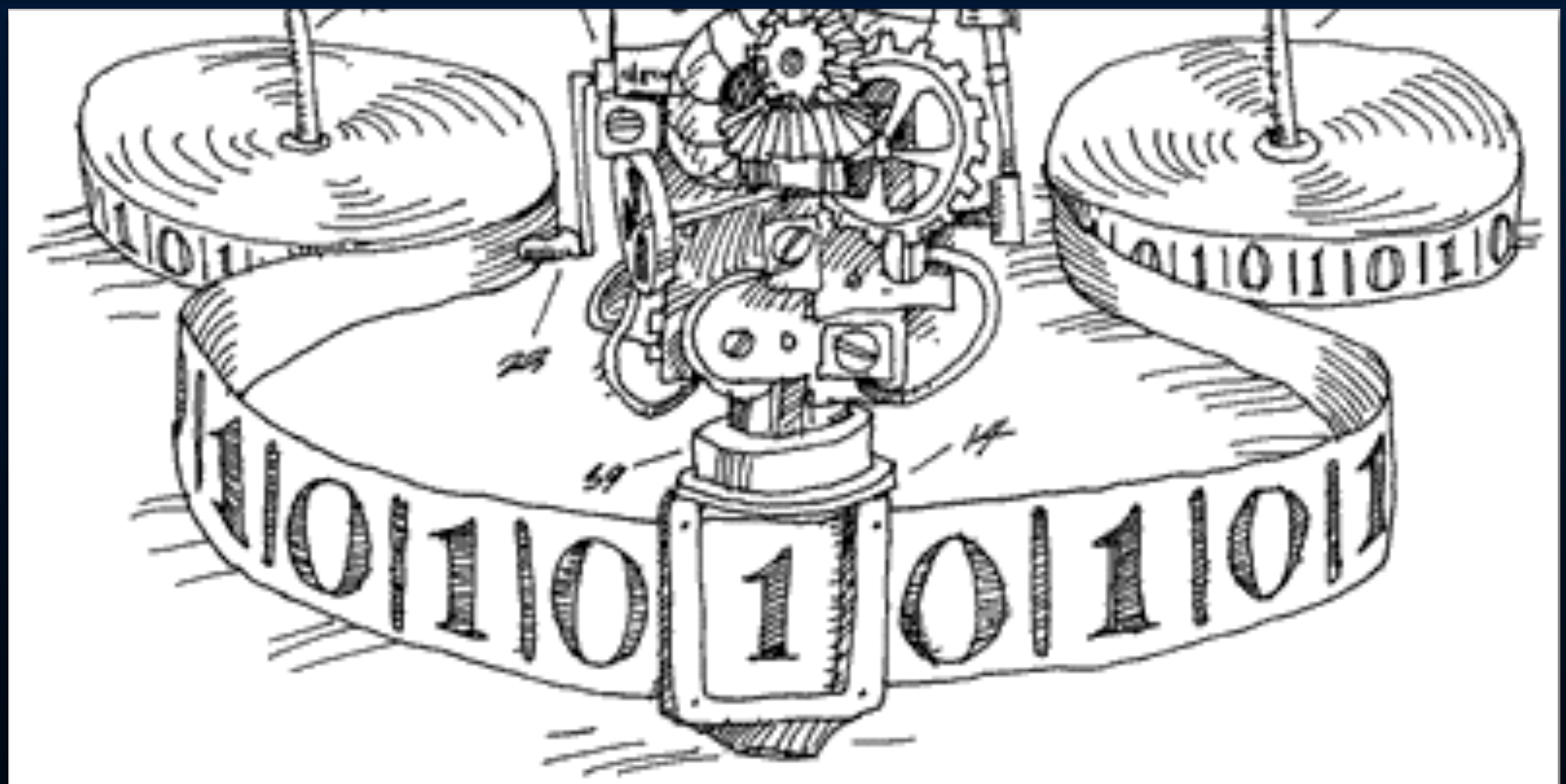
Updated 2 hours ago

libethereum

C++ ★ 15 ⑂ 18

Blockchain with bounded-VM-based state transition mechanism

Updated 2 hours ago



Blockchain Turing Machine

Run **arbitrary** code; any logic written in a language compiles to EVM **bytecode**

A

Dapp Development

Platform

Designed for **Developers**

It **makes the hard parts “easy”**

Abstracts away the **nitty gritty**
and **exposes the fun bits**

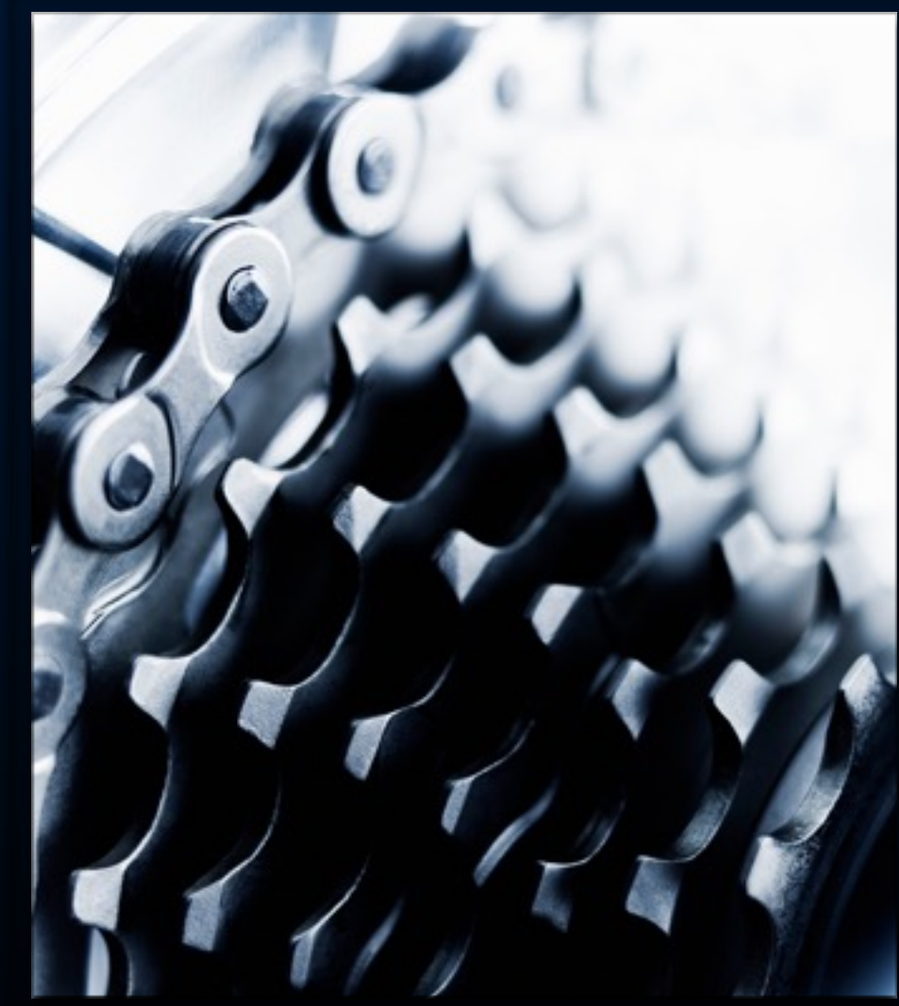
Running Smart Contracts on the Ethereum Network

- **Not free**, costs **Gas**
- **Gas** costs **Ether**
- **Ether** is currency
- **Ether** is mined and traded like **Bitcoin**
- but **Ether** has **Utility**

In Ethereum, **Smart Contracts** are **programs with super powers**

- **Own** Ether
- **Send** Ether
- **Run** other Contracts

Code with property rights



Gas Fees

Gas fees for operations in Ethereum transactions and contracts.

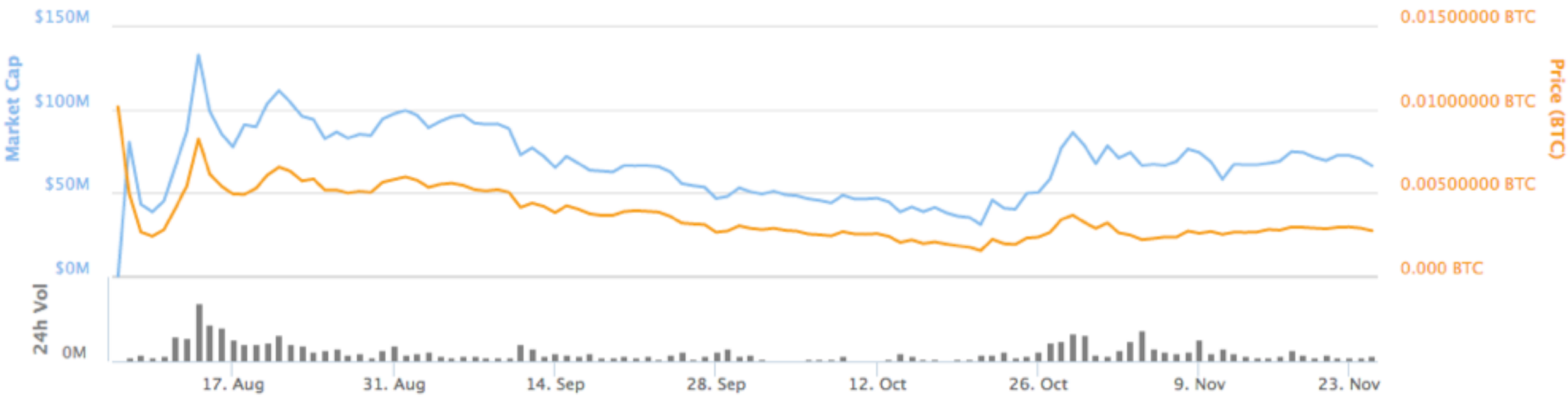
Operation name	Cost (in gas)	Description
step	1	Default amount of gas to pay for an execution cycle.
stop	0	Nothing paid for the STOP operation.
suicide	0	Nothing paid for the SUICIDE operation.
sha3	20	Paid for a SHA3 operation.
sload	20	Paid for a SLOAD operation.
sstore	100	Paid for a normal SSTORE operation (doubled or waived sometimes).
balance	20	Paid for a BALANCE operation.
create	100	Paid for a CREATE operation.
call	20	Paid for a CALL operation.
memory	1	Paid for every additional word when expanding memory.
txdata	5	Paid for every byte of data or code for a transaction.
transaction	500	Paid for every transaction.

Charts | Markets | Social

Ethereum Charts

Zoom 1d 7d 1m 3m 1y YTD ALL

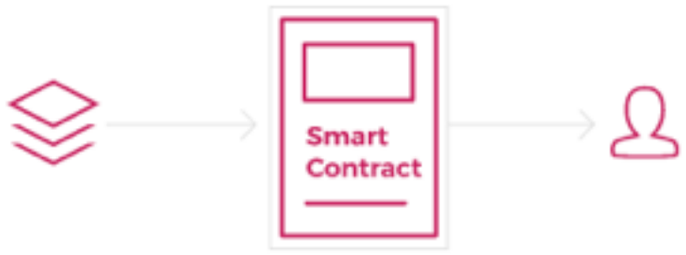
From Aug 7, 2015 To Nov 25, 2015



Ethereum Projects in the Wild

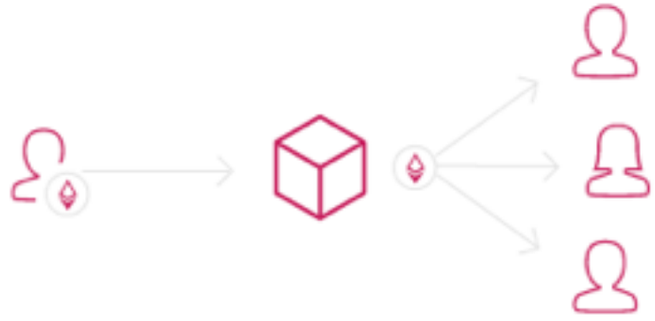
Blockchain

Creators publish ownership information and use policies on the blockchain – a permanent and transparent string of transactions viewable and stored by everybody on the network.



Smart Contracts

Anybody can use the registered content provided that they meet the terms of the policy. The right to do so is transferred automatically through a smart contract.



Instant Payment

Payments are delivered to individual stakeholders instantly and automatically using digital currency, eliminating the need for intermediaries.

uJo Music

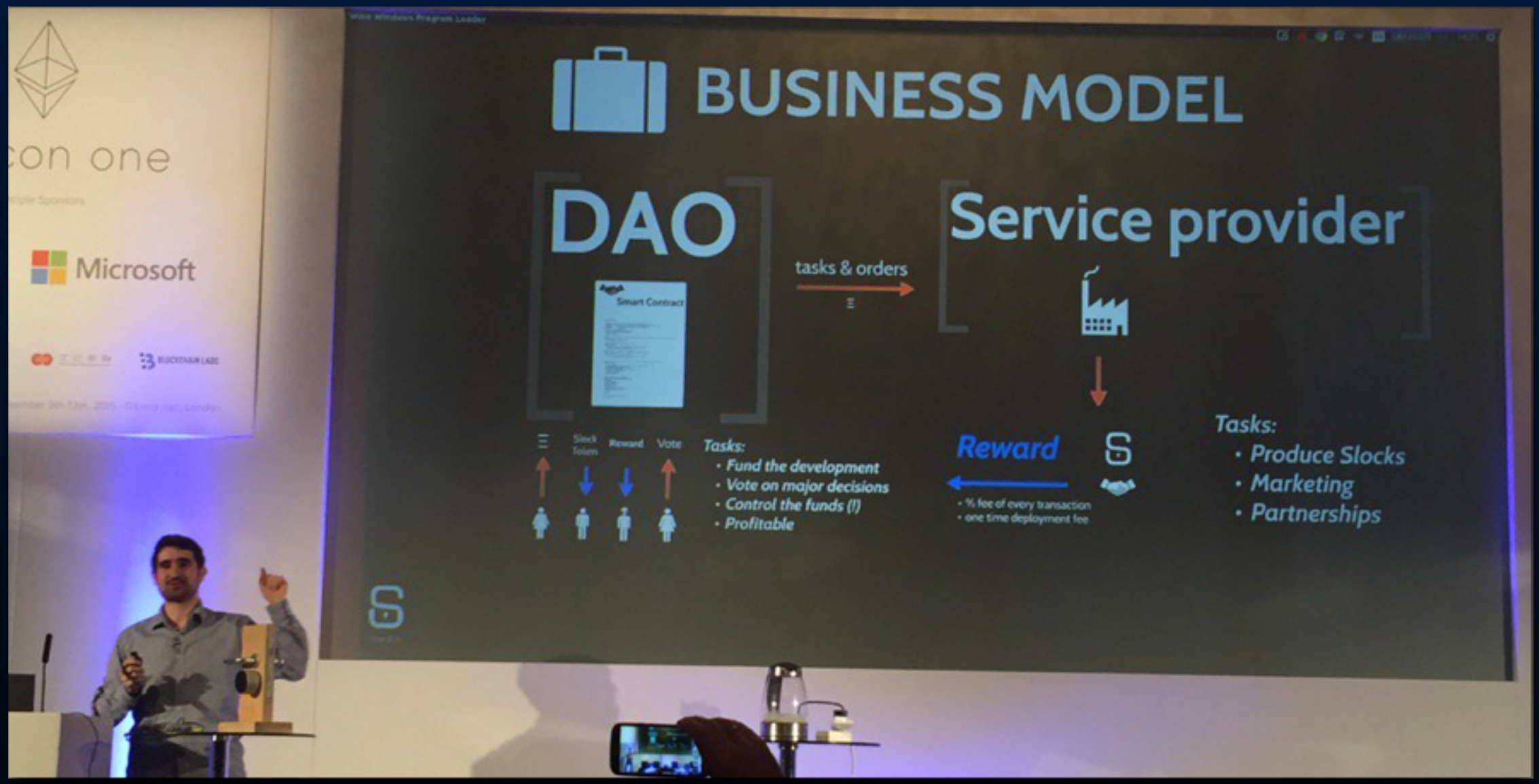
Used by Imogen Heap in August

SOLUTION

A lock that can be opened by paying money

Slock.it

If you can lock it, you can rent it



Slock.it

Decentralized Autonomous Organization

STATE OF THE ĐAPPS

http://dapps.ethercasts.com

Search

Browser-Solidity

chriseth & d11e9

Browser based solidity contract compiler & runtime

MIT

Live 2015-11-20

Taxeme

Jeffrey B. Petersen

A component of the Resilience taxation system

MIT

Work in Progress 2015-11-20

proof-of-individuality

d11e9

anti-sybil token

MIT

Work in Progress 2015-11-20

FreeMyVunk

R. Tyler Smith

Monitize your video game junk

Concept 2015-11-19

TokenEscrow

Alex Beregszaszi

Contract for running an escrow service for Ethereum token-contracts

MIT

Work in Progress 2015-11-16

Etherboard

Alex Beregszaszi

Combining a Ponzi-scheme with the MillionDollarHomepage

MIT

Working Prototype 2015-11-15

Syng

Jarrad Hope

The Mobile Client for the Ethereum Network

GPL

Working Prototype 2015-11-15

Etherdice

vnovak

Provably fair and escrowed gambling

Live 2015-11-15

String

Dominic Williams

Autonomous & open financial cloud for financial assets

Concept 2015-11-14

insurETH

Thomas Bertani

P2P flight insurance

Apache

Working Prototype 2015-11-14

Ampliative Art

Adrian Onco

A decentralized, cooperative and empowering art community

Concept 2015-11-13

Ethereum Pyramid

ethererik

Ethereum Pyramid Contract

Live 2015-11-13

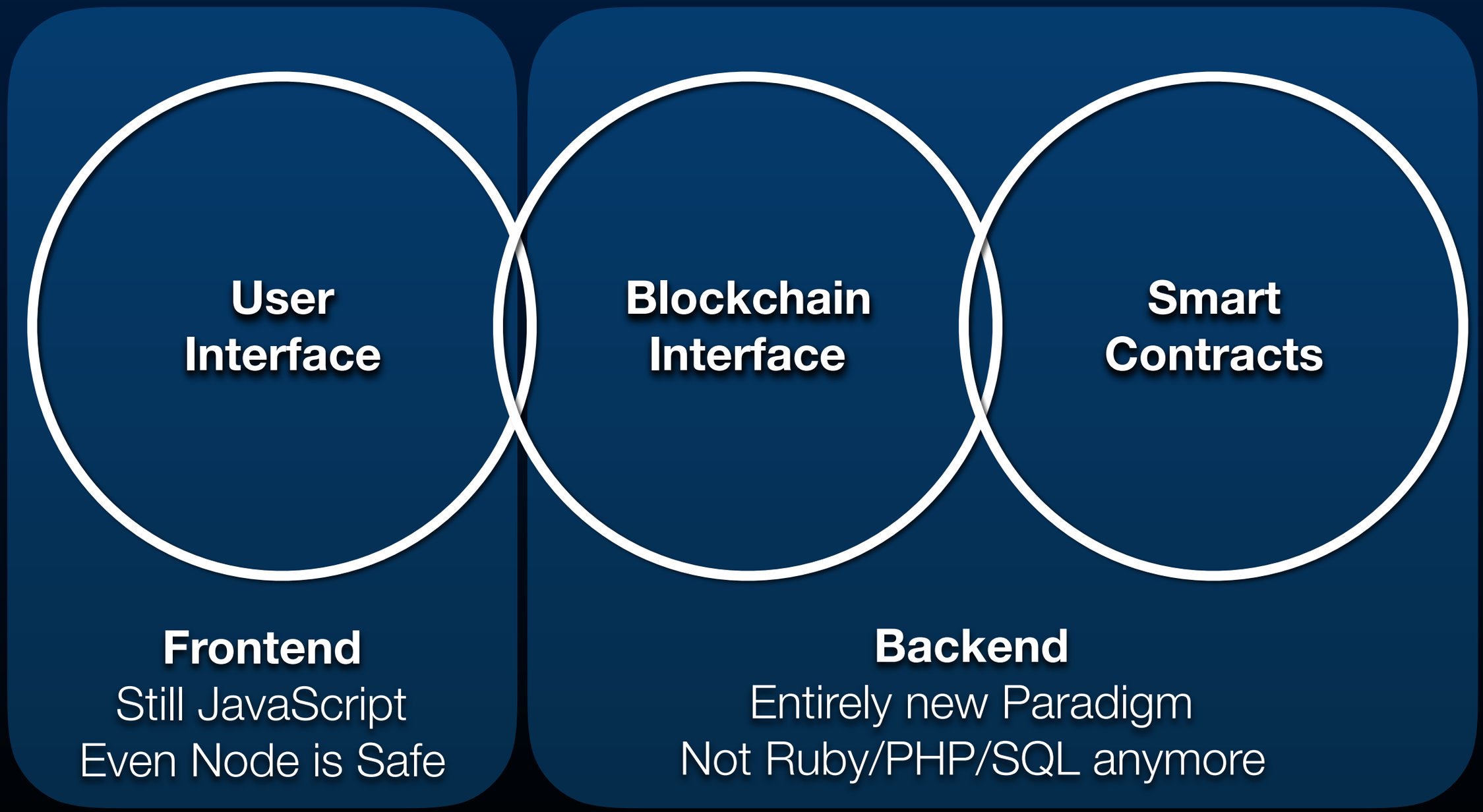
Cool story bro, but

Why are you talking about this at a JavaScript Meetup?

If you are a JavaScript Developer

It’s in your interest promote Web 3.0

Components of a Dapp
Decentralised Application



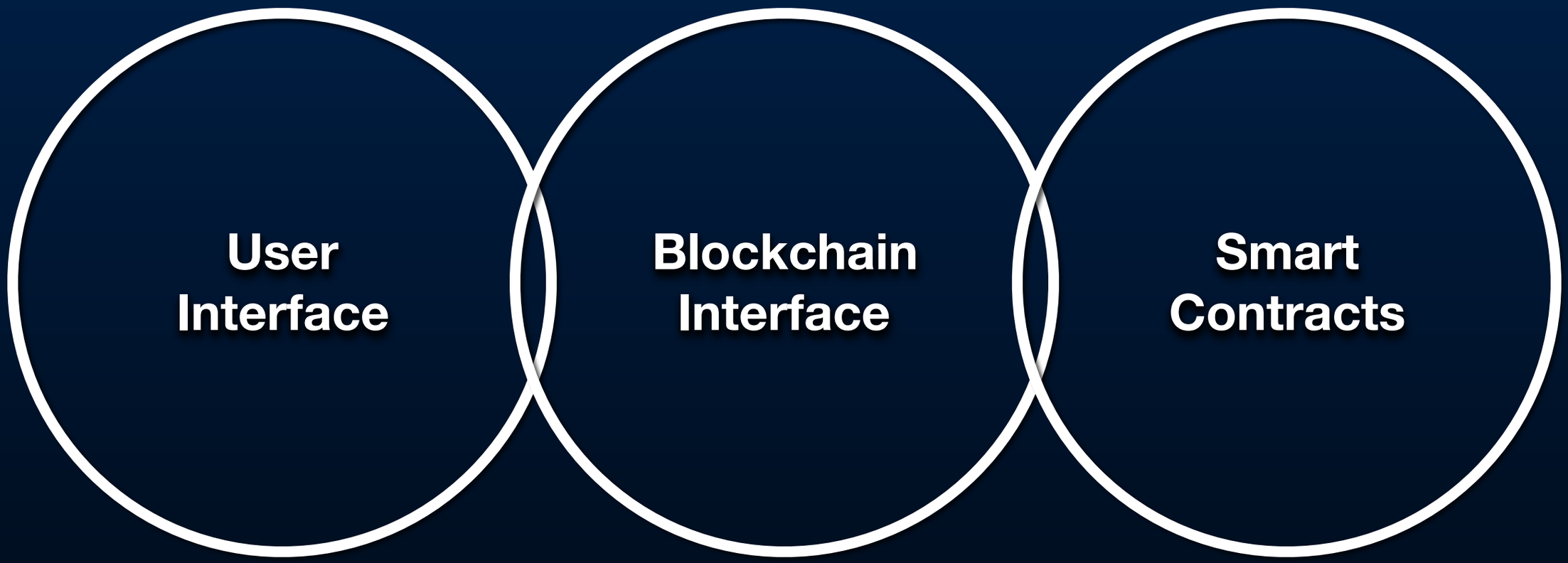
A Possible Dapp Structure for Web 3.0 Developers

- **Smart Contracts**
  Open source code on Github or write your own

- **Blockchain Interface**
  Locally running Ethereum Node (geth) & Web3.js

- **User Interface**
  Web-based UI running a browser
  Any JS framework is good

Ethereum Makes Dapp Development Easy

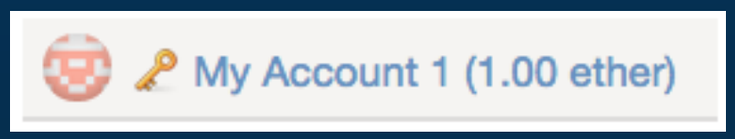


elements
Meteor Package

Web3
JS API

Geth
Ethereum Node

Solidity
Programming Language



Mist
Dapp Browser

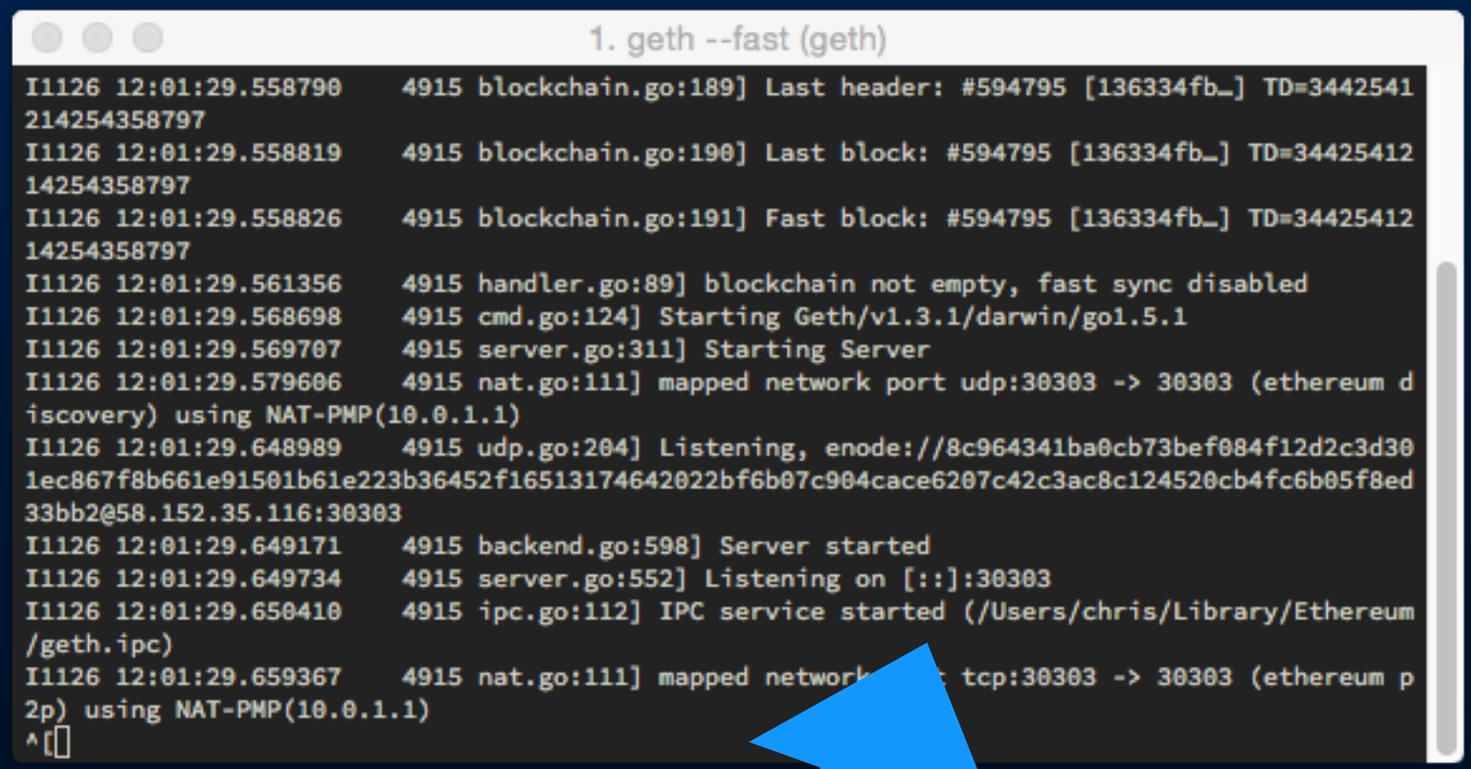
Ethereum ❤️ JavaScript

Web3.js

A JS dev's **first class ticket** to Ethereum

- **Browser**
  <script src="web3.js">
- **NPM**
  Web3 = require('web3')
- **Meteor**
  meteor add ethereum:web3

How does it work?



- **Connect to an Ethereum node**
  web3.setProvider(new web3.providers.HttpProvider('http://localhost:8545')
- **JSON RPC Interface**
  —> {"id":67,"jsonrpc":"2.0",**"method":"web3_clientVersion"**,"params":[]}
  <— {"id":67,"jsonrpc":"2.0",**"result":"Mist/v0.9.3/darwin/go1.4.1"**}
- **Short Polling over HTTP** to synchronise state

What does **Web3.js** give you

- **Eth** accounts, transactions, miner info, block#
- **Compiler** convert source code string to EVM bytecode
- **Dynamic Contract API** myContract.payout()
- **filter.watch** listens to events on the blockchain
- **Whisper** secure messaging protocol
- **Helpers** sha3, fromWei, toHex, isAddress

Using Web3.js

- Start with Contract Code (Solidity string)
- Compile the Contract Code (bytecode + ABI)
- Parse the ABI to get a Contract API
- Use that Contract Object in JavaScript

Solidity Contract Code

```
contract test {
  function multiply(uint a) returns(uint d) {
    return a * 7;
  }
}
```

```
var source = "" +
    "contract test {\n" +
    "   function multiply(uint a) returns(uint d) {\n" +
    "       return a * 7;\n" +
    "   }\n" +
    "}\n";
```

Compiled Contract

```
var compiled = web3.eth.compile.solidity(source);

console.log(compiled);

{
  "test": {
    "code": "0x605280600c6000396000f3006000357c010000000000000000
    "info": {
      "source": "contract test {\n\tfunction multiply(uint a) retu
      "language": "Solidity",
      "languageVersion": "0",
      "compilerVersion": "0.8.2",
      "abiDefinition": [
        {
```

ABI

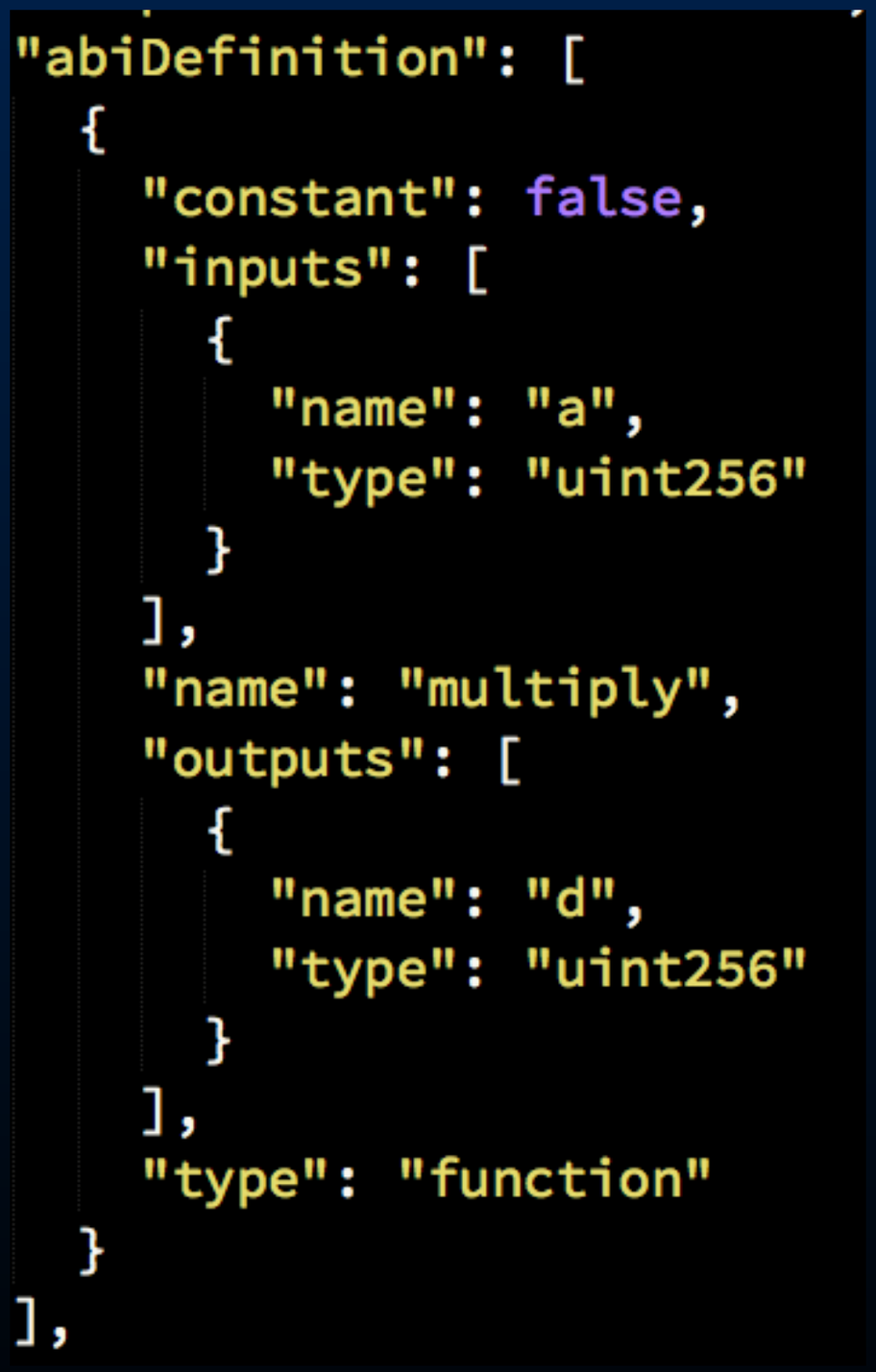
Application *Binary* Interface

(for Bytecode)

API

Application *Program* Interface

(for Source Code)


"abiDefinition": [
{
"constant": false,
"inputs": [
{
"name": "a",
"type": "uint256"
}
],
"name": "multiply",
"outputs": [
{
"name": "d",
"type": "uint256"
}
],
"type": "function"
}
],

```
var abiArray = compiled.test.info.abiDefinition;
var contractCode = compiled.test.code;

var MyContract = web3.eth.contract(abiArray);

// deploy new contract
var contractInstance = MyContract.new({
  data: contractCode,
  from: eth.accounts[0],
  gas: 1000000
});

// instantiate by address
var contractInstance = MyContract.at(['0x12345...']);
```

What about hosting?

IPFS

Ethereum ❤️ Meteor

ETHEREUM

Meteor packages

ethereum:web3

Ethereum JavaScript API, middleware to talk to a ethreum node over RPC

812 ★ 7

ethereum:elements

Basic elements for Dapps

597 ★ 8

ethereum:accounts

Provides and updates the ethereum accounts in the Accounts collection

107 ★ 6

ethereum:dapp-styles

CSS/LESS framework for dapps

36 ★ 1

ethereum:tools

Helper functions for dapps

513 ★ 4

ethereum:blocks

Provides informations about the current and last 50 blocks

71 ★ 4

RECAP:

- **Blockchain** a distributed p2p virtual machine
- **Smart Contract** a bit of code running on the machine
- **Dapp** contracts combined with UI to make an app
- **Ethereum** a ‘Dapp Development Platform’
- **Web3.js** a JavaScript Library for in-browser Dapps

Let’s demo

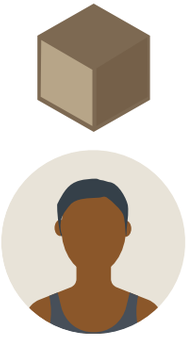
A Distributed Market Dapp

Definitely not Silk Road 3.0

- **Registry Contract**
  A list of things that people want to sell
- **Escrow Contract**
  A mechanism that forces people to trust each other. Available on github

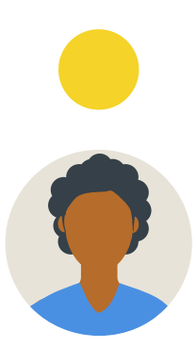
ETHEREUM

Bob

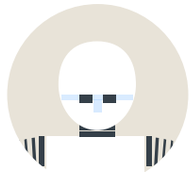


Alice

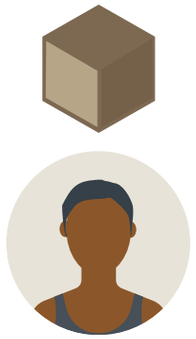
ETHEREUM



Bob

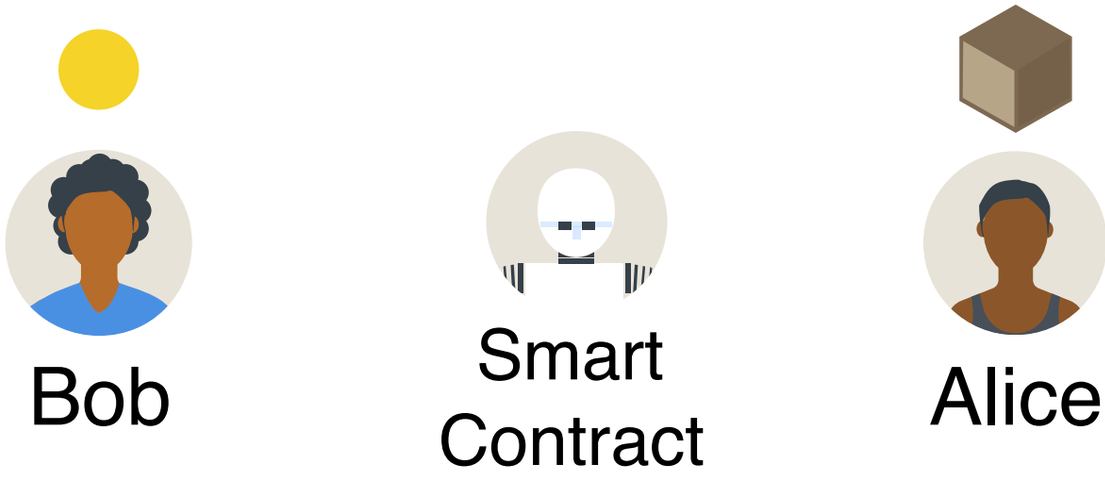


Smart Contract



Alice

ETHEREUM

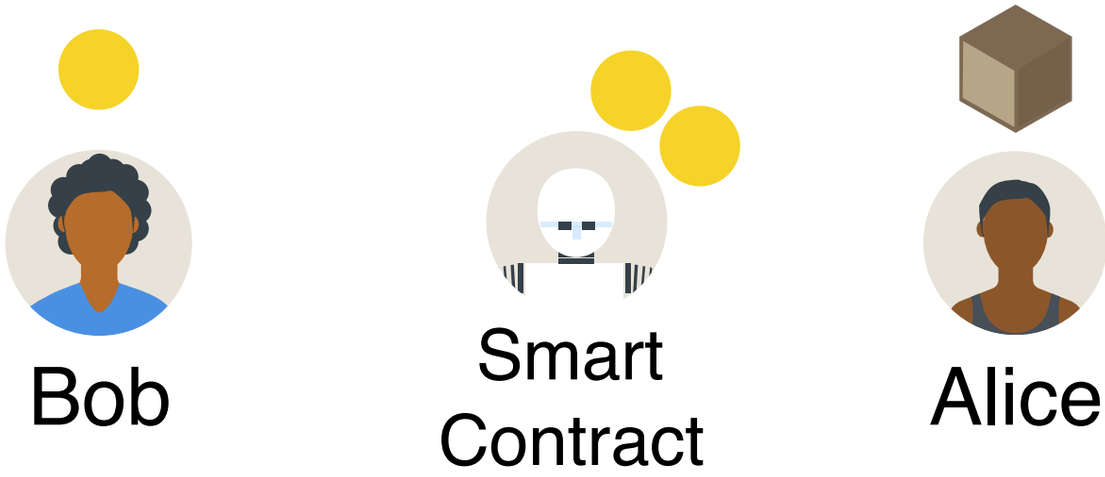


Bob

Smart Contract

Alice

ETHEREUM

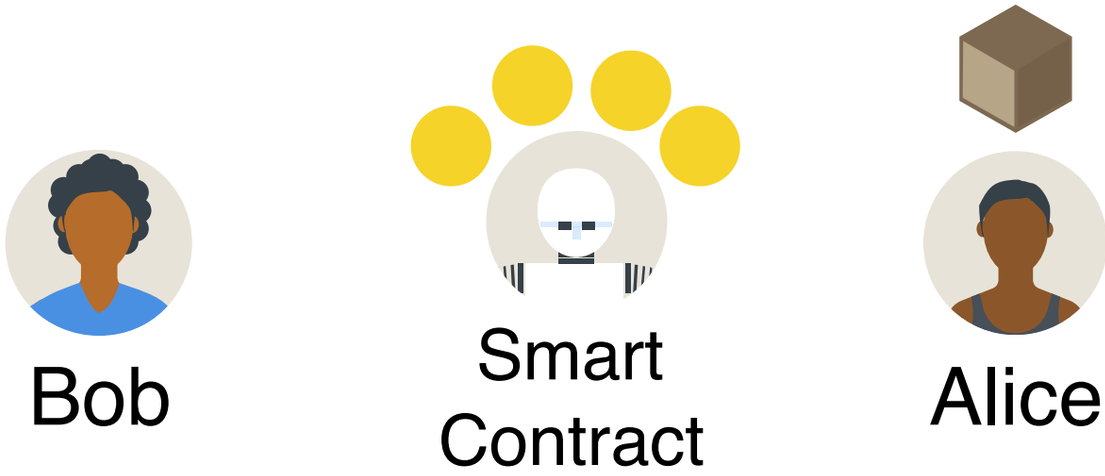


Bob

Smart Contract

Alice

ETHEREUM

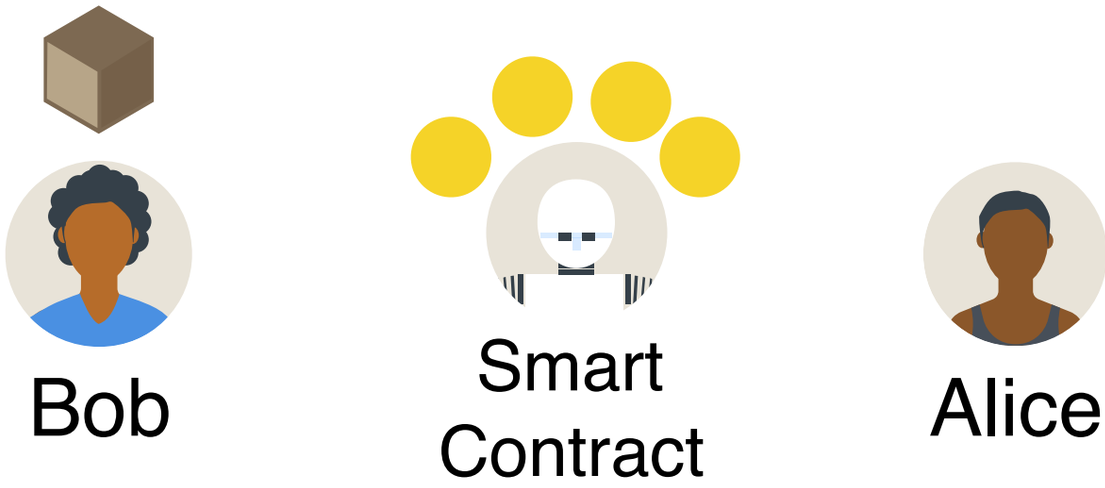


Bob

Smart Contract

Alice

ETHEREUM

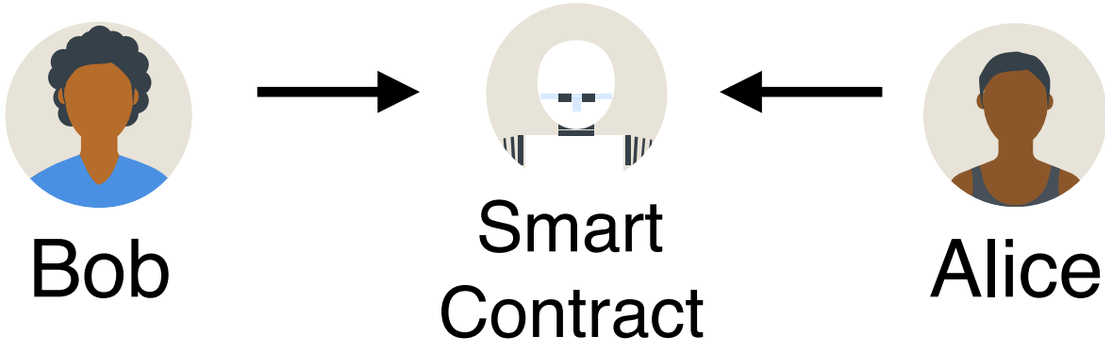


Bob

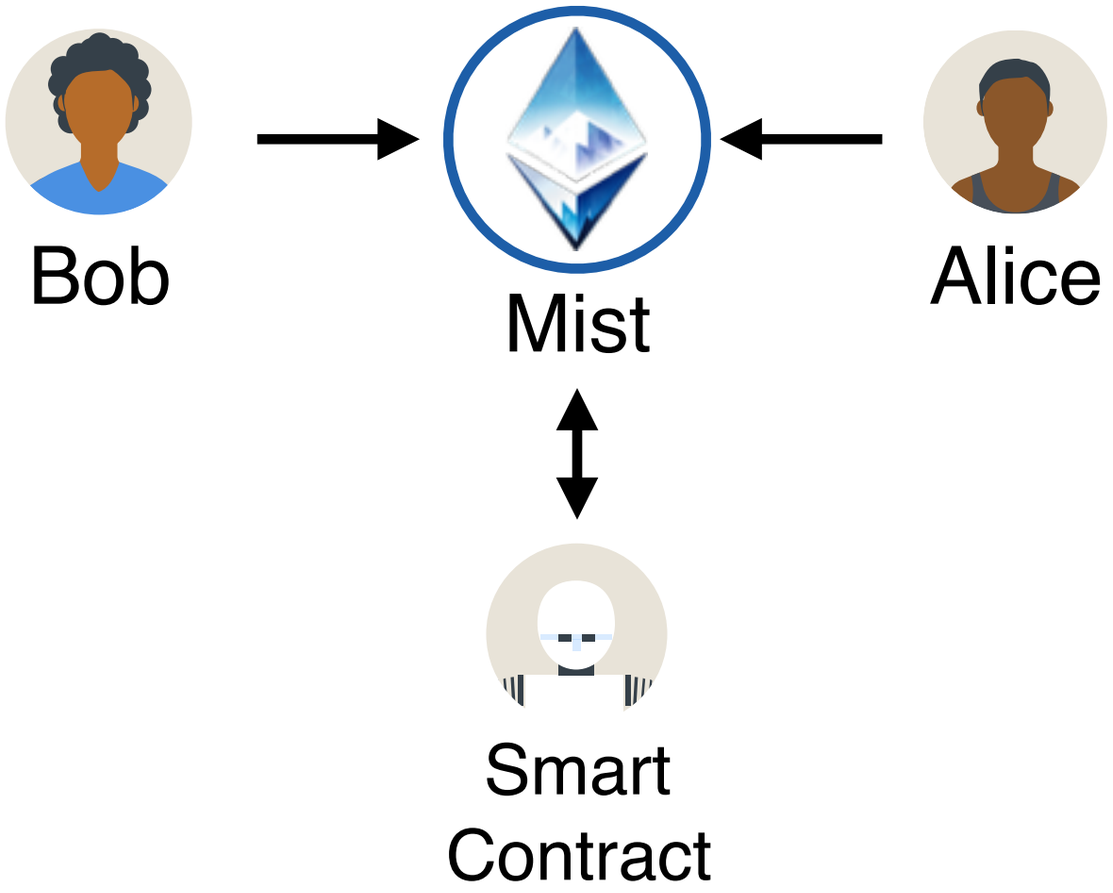
Smart Contract

Alice

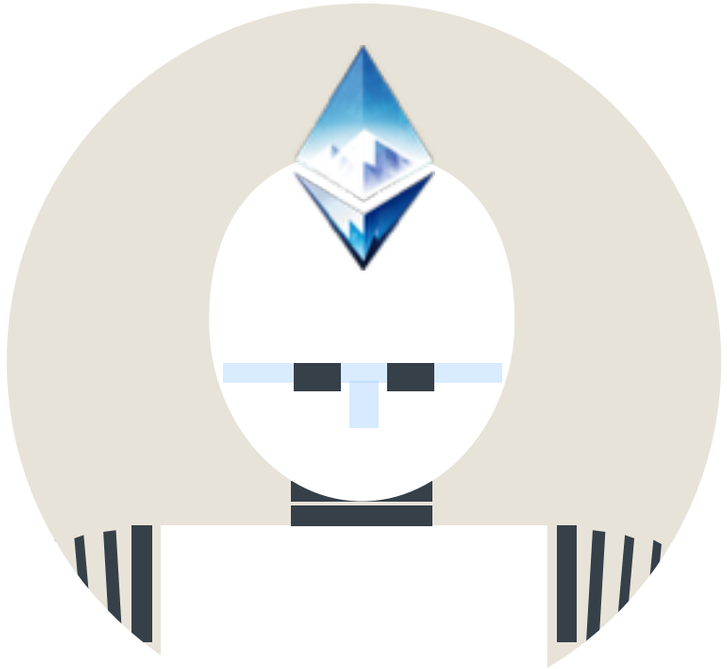
ETHEREUM



ETHEREUM



ETHEREUM



Show me!

Q&A