BLOCKCHAIN

Worth More Than a Bitcoin

Brett Koenig

Brett@BrettKoenig.com

STIR TREK

WHY BLOCKCHAIN

- BITCOIN PRICE
- LONG BLOCKCHAIN STOCK

WHY HIM

NOT AN INVESTOR

HAVE NEVER MINED BITCOIN

NO DAPPS IN PRODUCTION

>100 HOURS OF RESEARCH

PUT A NODE ON THE ETHEREUM BLOCKCHAIN

DEPLOYED A DAPP TO A PRIVATE BLOCKCHAIN

WHO IS HE

BRETT KOENIG

Brett@BrettKoenig.com

HMB

MARRIED 3 YEARS

BLAST FACT

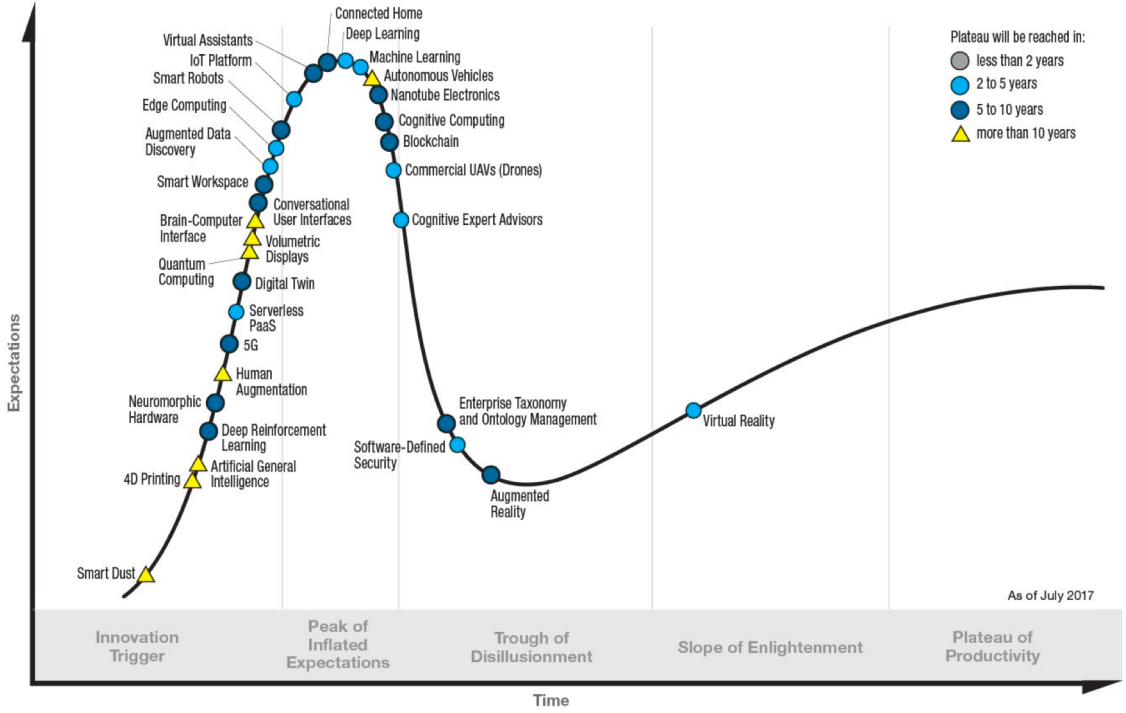
FUN FACT

Best wife ever!

DISCLAIMER

I AM NOT ENDORSING BITCOIN OR OTHER CRYPTOCURRENCIES
AS AN INVESTMENT STRATEGY

Gartner Hype Cycle for Emerging Technologies, 2017



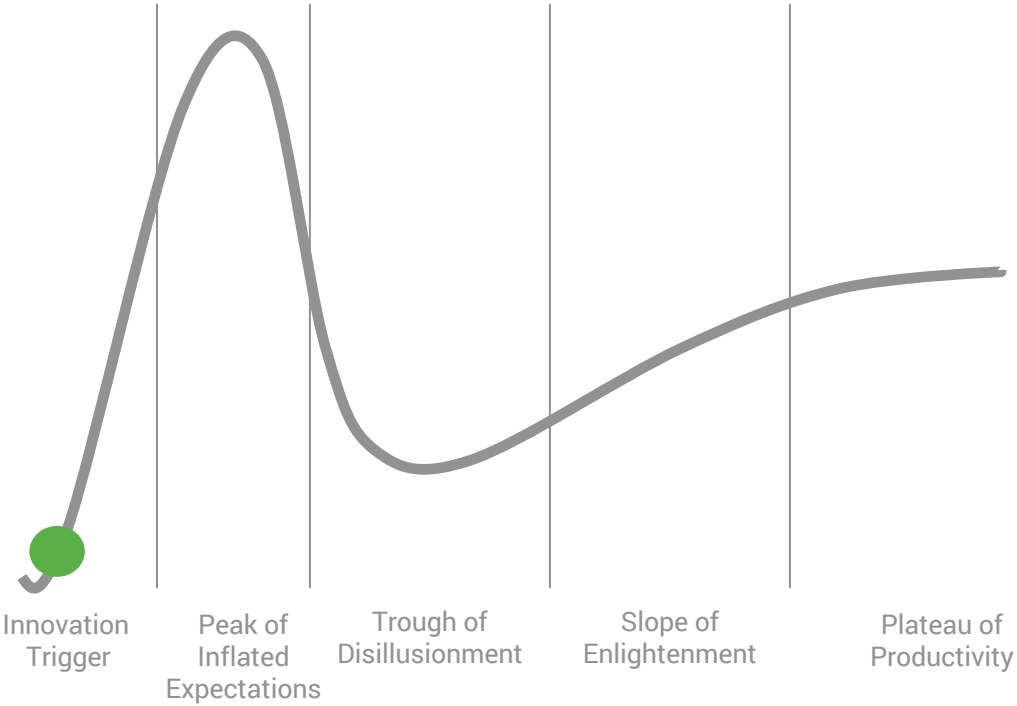
01 INNOVATION TRIGGER

02 PEAK OF INFLATED EXPECTATIONS

03 TROUGH OF DISILLUSIONMENT

04 SLOPE OF ENLIGHTENMENT

05 PLATEAU OF PRODUCTIVITY



ASSUMPTIONS

CRYPTOGRAPHIC HASH FUNCTION

A function that will take any size of input and repeatedly reproduce the same result of a fixed size.

BITCOIN != BLOCKCHAIN

Bitcoin is one implementation of blockchain, but is not the same as blockchain.

STORY TIME

3/3

HEALTHCARE PROFESSIONALS EXCITED ABOUT POTENTIAL

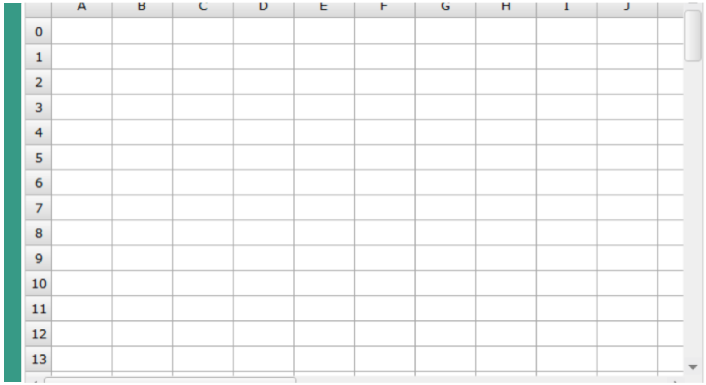
$53,213

SCHOOL OF MEDICINE TUITION AT VANDERBILT UNIVERSITY

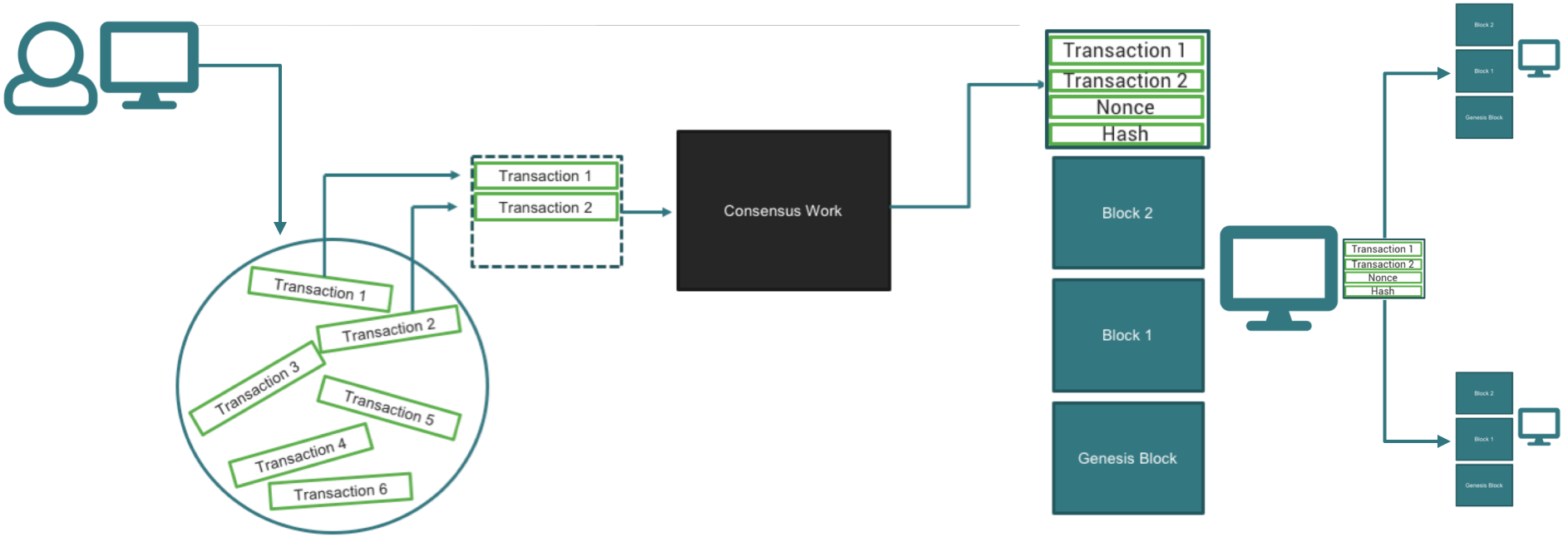
$28 BILLION

ESTIMATED SIZE OF EMR MARKET IN 2016

WHAT IS BLOCKCHAIN



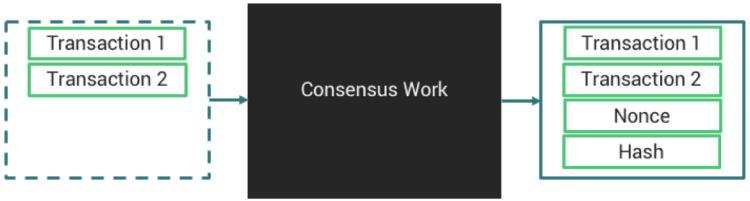
“Blockchain is a persistent, transparent, public append only ledger.”


Transaction 1
Transaction 2
Transaction 3
Transaction 4
Transaction 5
Transaction 6
Transaction 1
Transaction 2
Consensus Work
Transaction 1
Transaction 2
Nonce
Hash
Block 2
Block 1
Genesis Block
Transaction 1
Transaction 2
Nonce
Hash
Block 2
Block 1
Genesis Block
Block 2
Block 1
Genesis Block

OVERVIEW

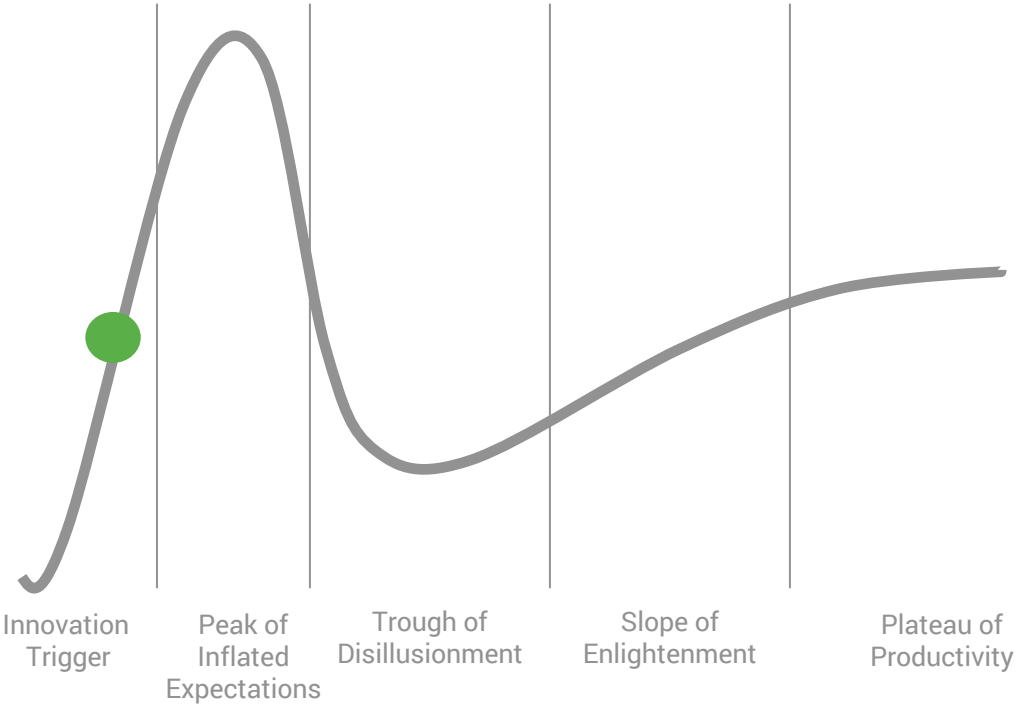
CONSENSUS WORK

```
var hashValue = null;
var nonce = 0;

while(true){
    nonce = nonce + 1;
    //or get random nonce value

    hashValue = generateHash(allTransactionsInBlock, previousBlockHash, nonce);

    if(hashValue.StartsWith("0000"))
        break;
}

validateBlock(allTransactionsInBlock, previousBlockHash, nonce);
```



The node is guessing the nonce value until a valid hash is found.

MINING


Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity

MINING

WORKING ON CONSENSUS ALGORITHM

PROOF OF WORK

HARD TO SOLVE, EASY TO VALIDATE

CONSENSUS ALGORITHMS

PROOF OF WORK

- ☑ BITCOIN & ETHEREUM ARE CURRENTLY USING
- ☒ WASTES A LOT OF ENERGY
- ☒ MOST POWERFUL NODE CAN SOLVE MORE FREQUENTLY

PROOF OF STAKE

- ☑ RANDOMLY ASSIGNED FROM POOL
- ☑ LOWER BARRIER TO ENTRY
- ☒ LOSS OF COMPUTE = LOSS OF TRUST

AND MANY MORE...

OVERVIEW

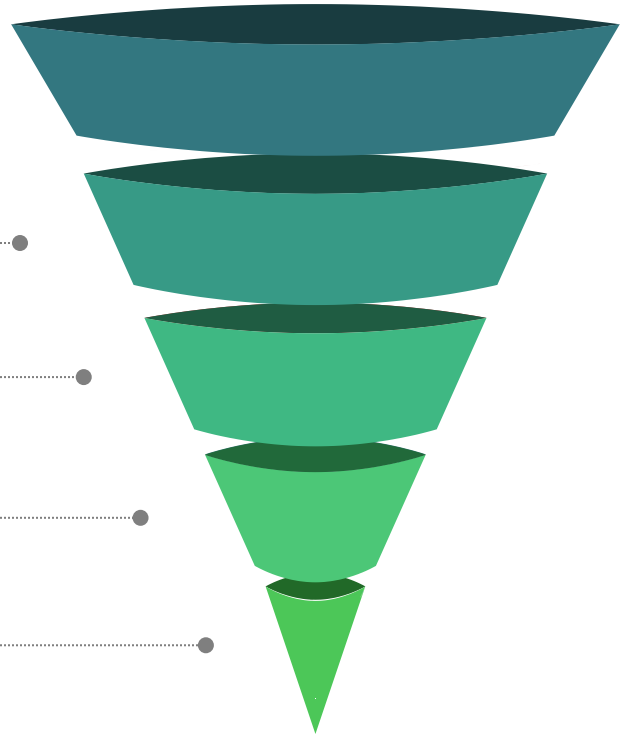
NETWORK

NODE

BLOCKCHAIN

BLOCK

TRANSACTION



TRANSACTIONS

- TRANSFER AN ASSET FROM ONE CRYPTOGRAPHIC IDENTITY TO ANOTHER
- REPRESENT A CHANGE OF STATE
- PROPAGATED THROUGH NETWORK USING P2P PROTOCOL

BLOCKS

- BLOCKS ARE A DATA STRUCTURE
- COLLECTION OF TRANSACTIONS
- TRANSACTIONS, HASH OF PREVIOUS BLOCK, NONCE

TRANSACTION 1

TRANSACTION 2

NONCE

HASH

Block

Block: # 1

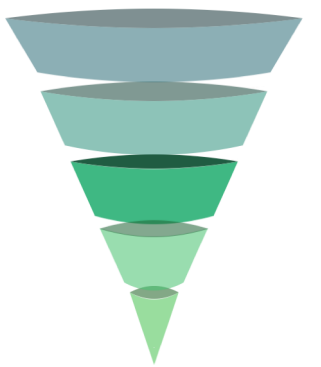
Nonce: 72608

Data:

Hash: 0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

Mine

BLOCKCHAIN

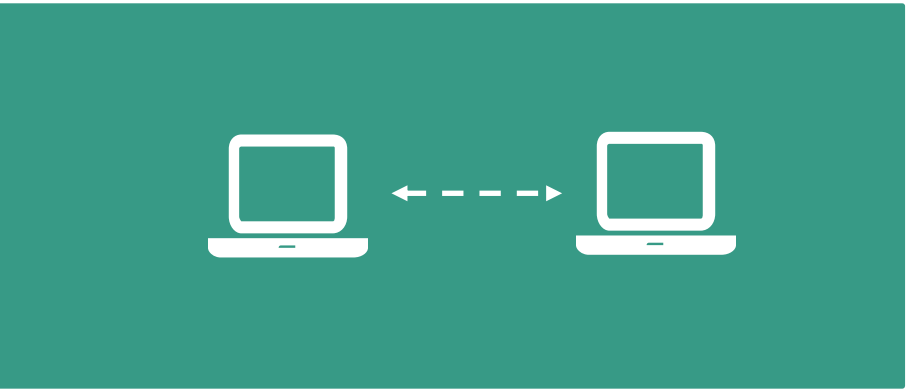


- SERIES OF BLOCKS
- STARTS WITH THE GENESIS BLOCK
- COPY ON EACH NODE IN THE NETWORK

Blockchain

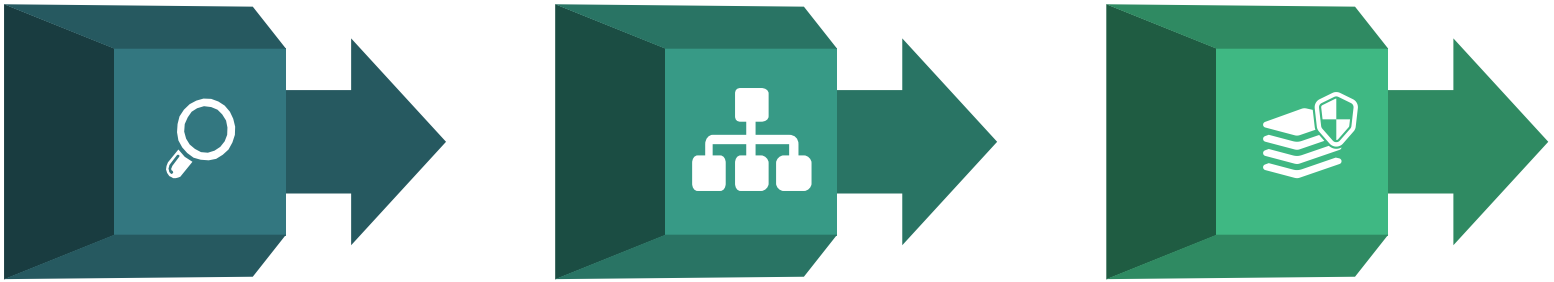
Block:	# 1	# 2	# 3
Nonce:	11316	35230	12937
Data:			
Prev:	00000000000000000000000000000000000000	000015783b764259d382017d91a36d206d0	000012fa9b916eb9078f8d
Hash:	000015783b764259d382017d91a36d206d0	000012fa9b916eb9078f8d98a7864e697ae	0000b9015ce2a08b61216b
	Mine	Mine	Mine

INFRASTRUCTURE



- NODE – COMPUTER WITH COPY OF BLOCKCHAIN
- NODES ARE COMPETITIVELY COOPERATIVE
- NETWORK – NETWORK OF ALL OF THE NODES

JOINING THE NETWORK

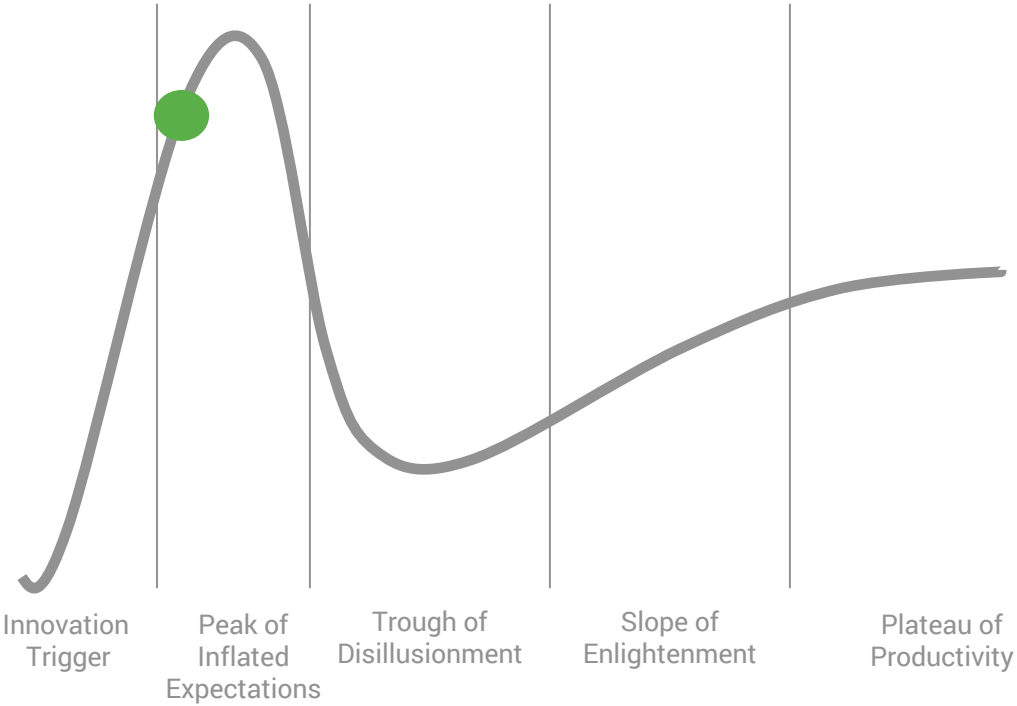


NODE LOOKS FOR NEIGHBORING NODES

NODE RECEIVES BLOCKCHAIN FROM NEIGHBORING NODES

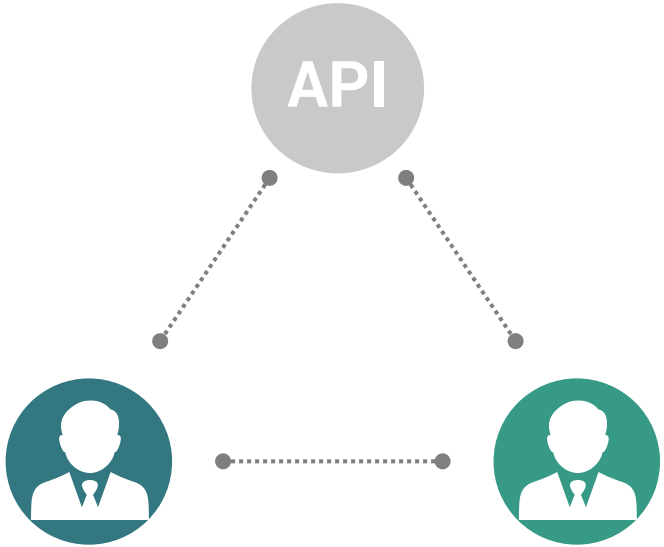
NODE STARTS VALIDATING EVERY PREVIOUS TRANSACTION

BENEFITS

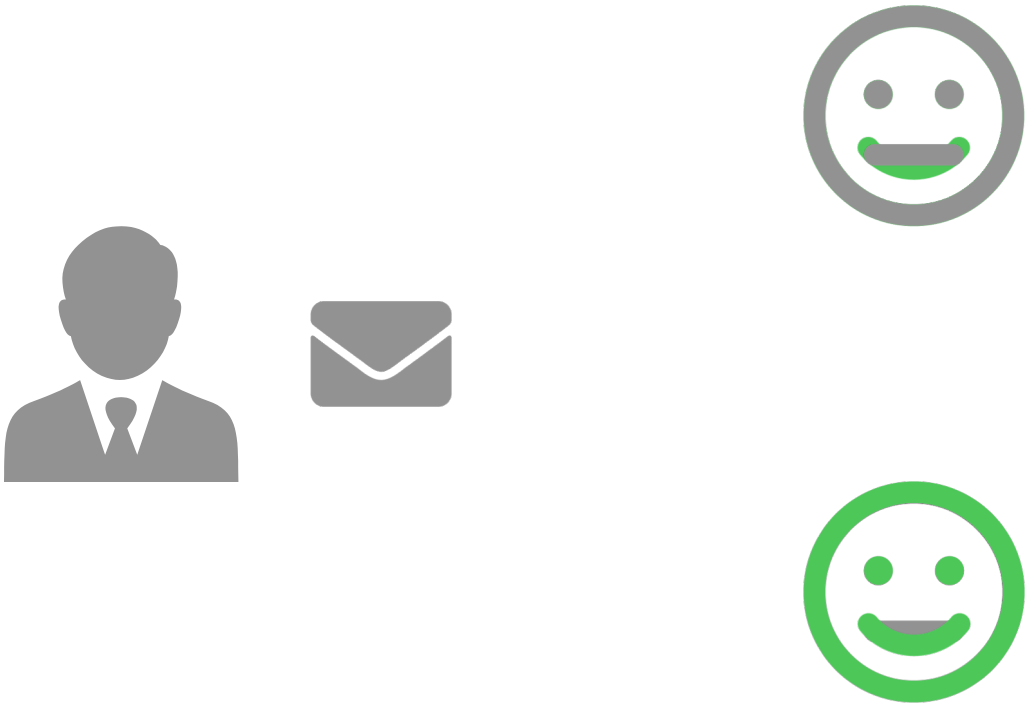

Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity

TAKE OUT THE MIDDLE MAN

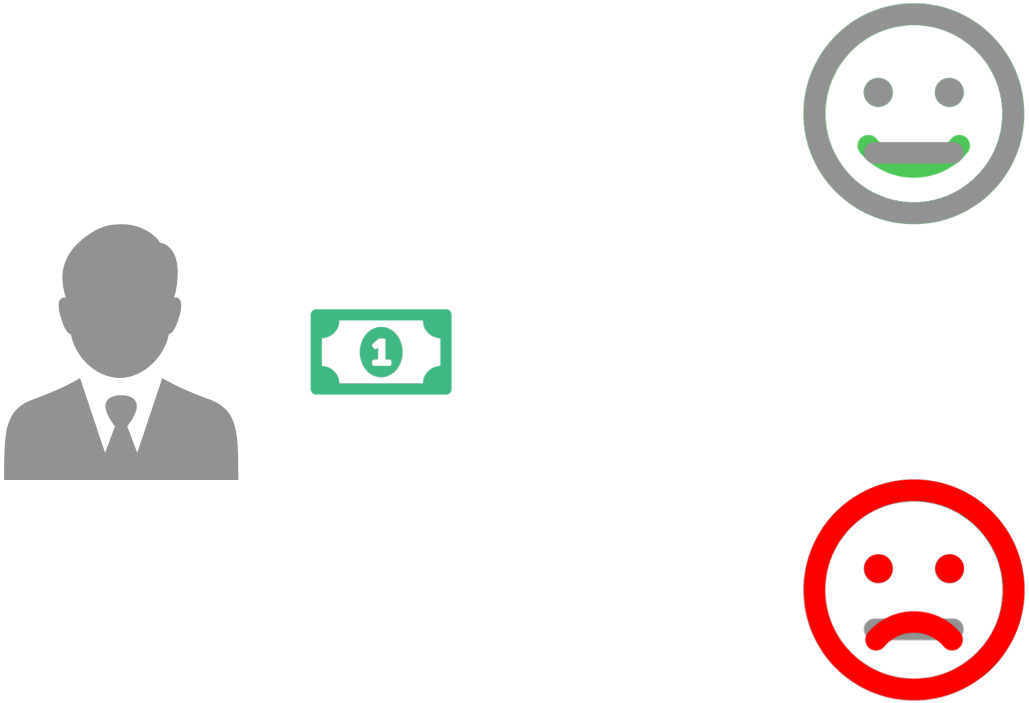
“A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.”



DOUBLE SPEND PROBLEM



DOUBLE SPEND PROBLEM



OTHER BENEFITS

DECENTRALIZED

No single point of failure

IMMUTABILITY

51% attack is a vulnerability, but would be incredibly expensive

CRYPTOGRAPHY

Asymmetric cryptography makes it hard to fake your identity

SOCIAL IMPACT

2 billion adults without access to formal financial services

51% Attack Cost

Hardware:	$7,653,659,702
Electricity:	$13,679,050
Total cost:	$7,667,338,752

Source: gobitcoin.io as of 3/25/18

INDUSTRIES

Payments – Abra

Banking - Barclays

Logistics – FedEx

Supply Chain Mgmt - Fluent

Forecasting – Augur

Networking/IoT – Samsung

Insurance – Aeternity

Ride Sharing - Arcade City

Cloud Storage - Storj.io

Charity – Bitgive

Voting - Democracy.earth

Government - Dubai (2020)

Public Sector – Govcoin

Healthcare

Energy Management

Online Media

Food Supply

Retail – OpenBazaar

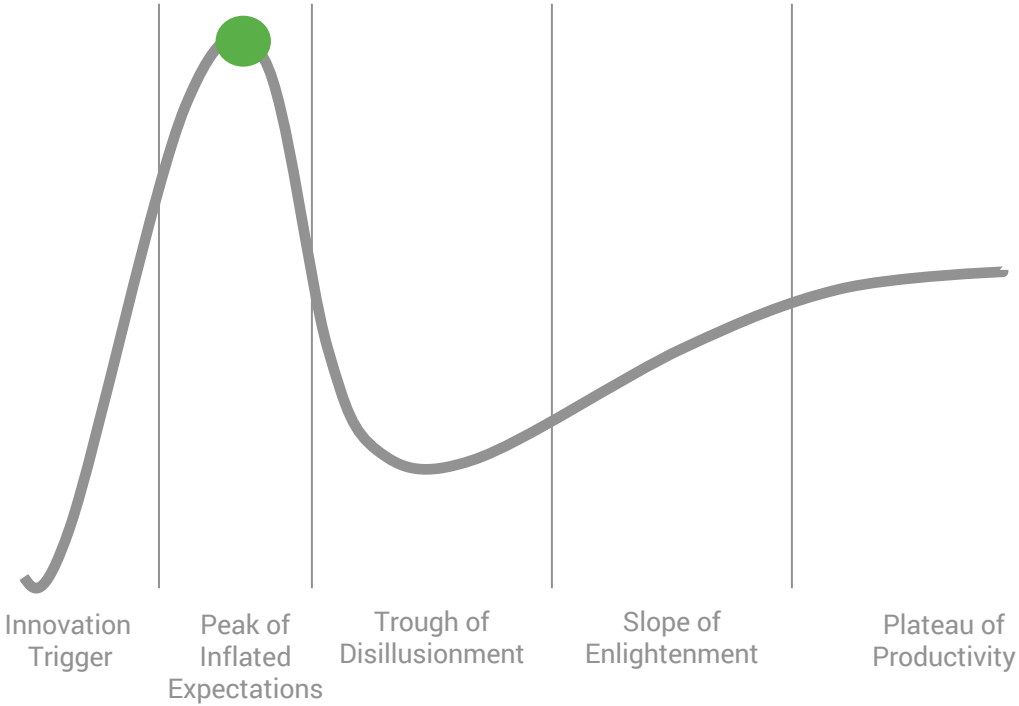
Clothing

Real Estate – Ubitquity

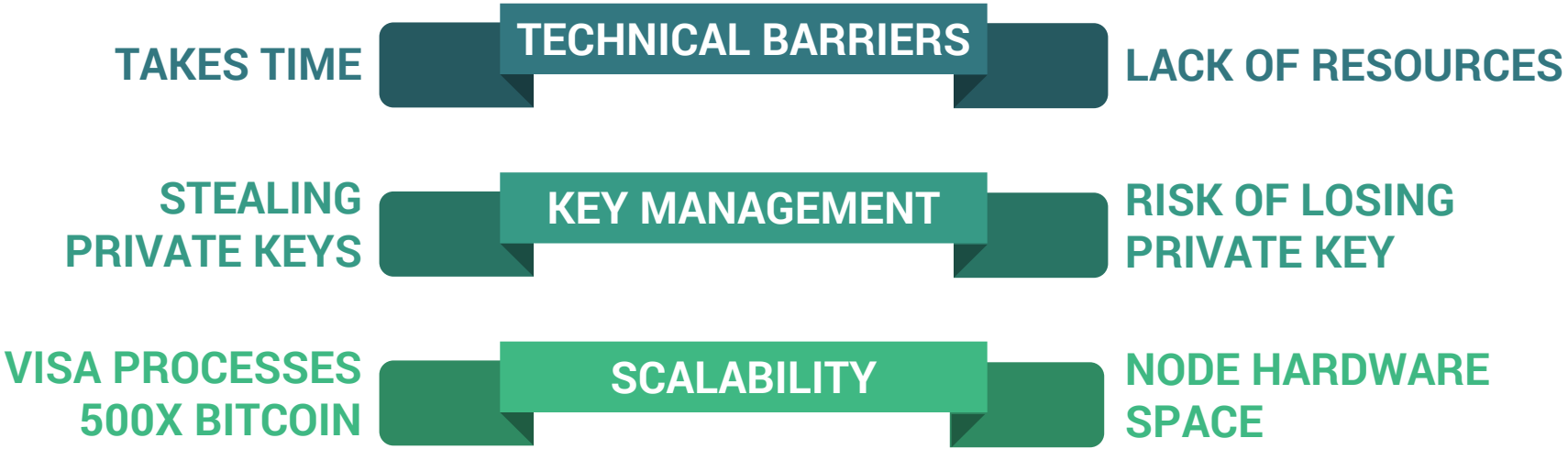
Crowdfunding

Stocks - Shapeshift

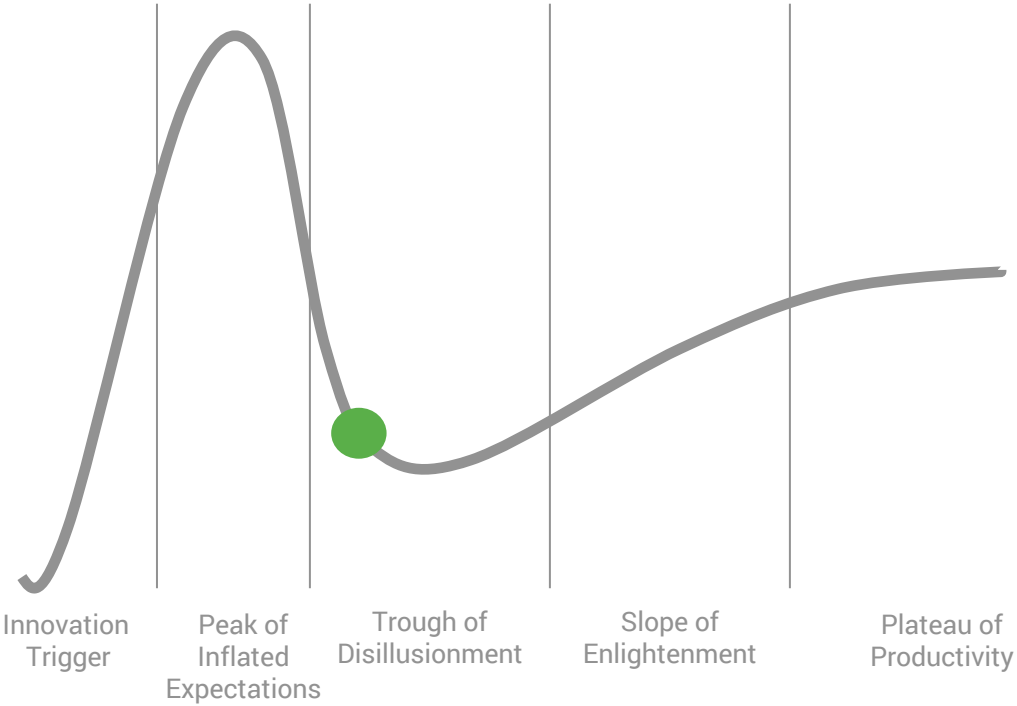
WHY NOT


Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity

NEGATIVES


TAKES TIME
TECHNICAL BARRIERS
LACK OF RESOURCES
STEALING PRIVATE KEYS
KEY MANAGEMENT
RISK OF LOSING PRIVATE KEY
VISA PROCESSES 500X BITCOIN
SCALABILITY
NODE HARDWARE SPACE

WHEN


Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity

BAD USE CASES

YOUR COMPANY'S INTRANET

TODO LIST APP

SNAPCHAT

GOOD USE CASES

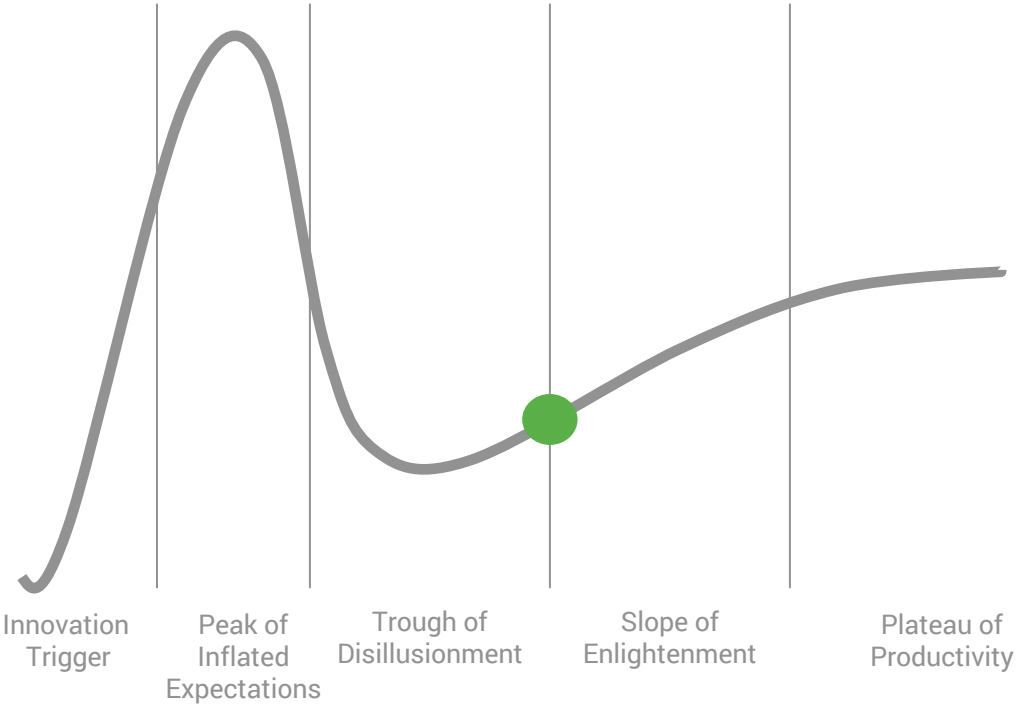
TRACKING ENTITIES OVER TIME

- ☑ AUDITABLE
- ☑ FULL PICTURE THROUGH TIME
- ☑ REMOVES OVERHEAD

SHARING DATA ACROSS ORGS

- ☑ INHERENTLY TRUST THE DATA
- ☑ FULL PICTURE THROUGH TIME
- ☑ ELIMINATE COST

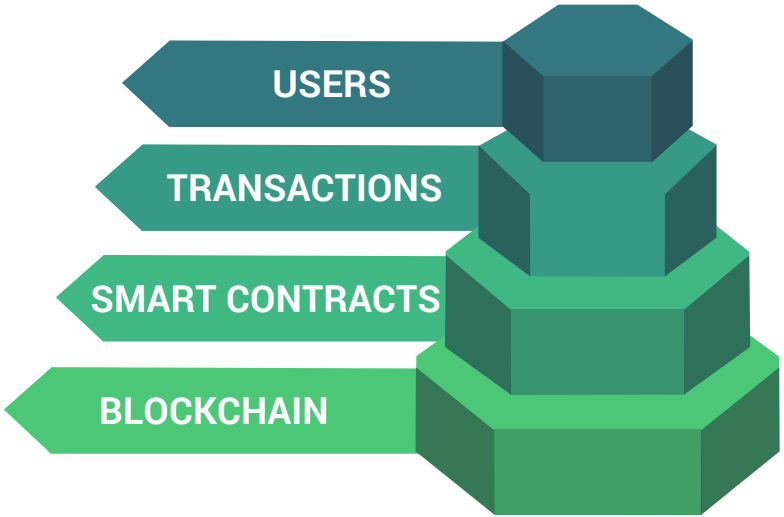
HOW


Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity

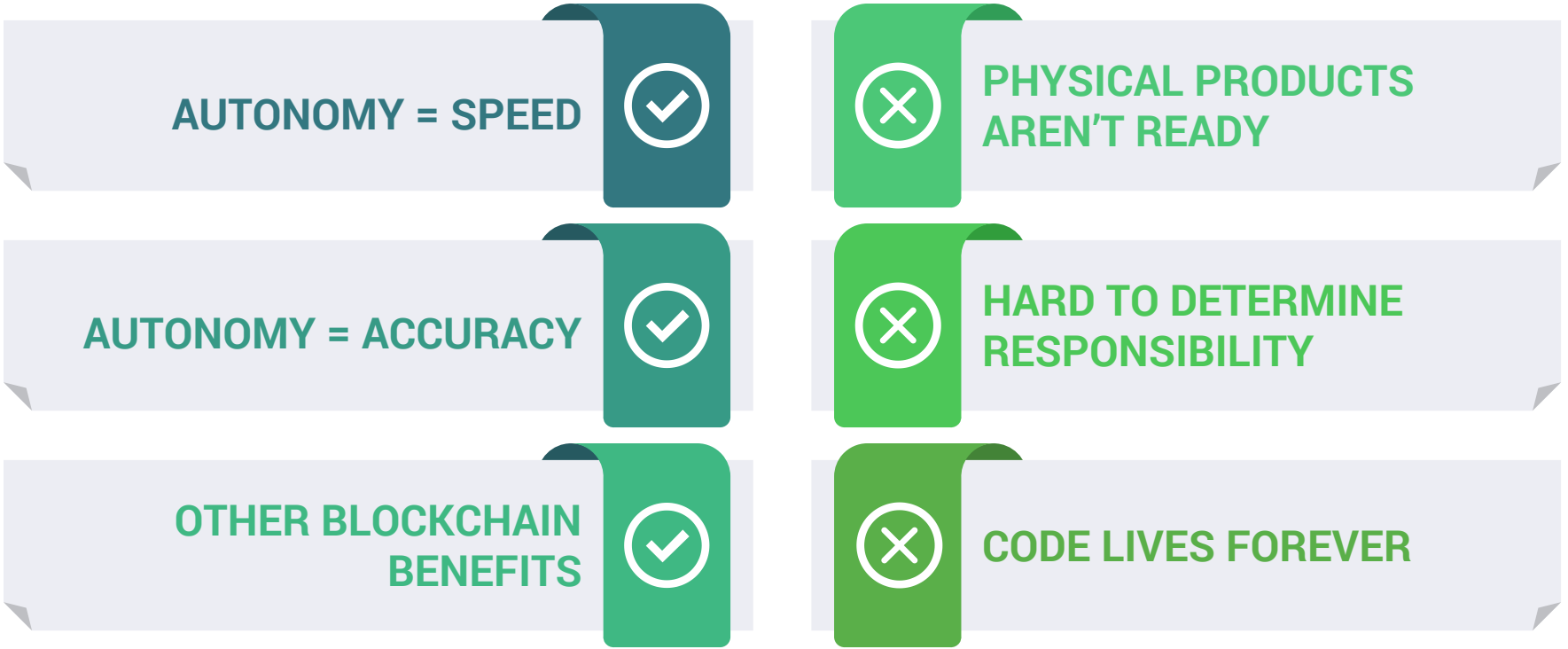
SMART CONTRACTS

The Building Blocks

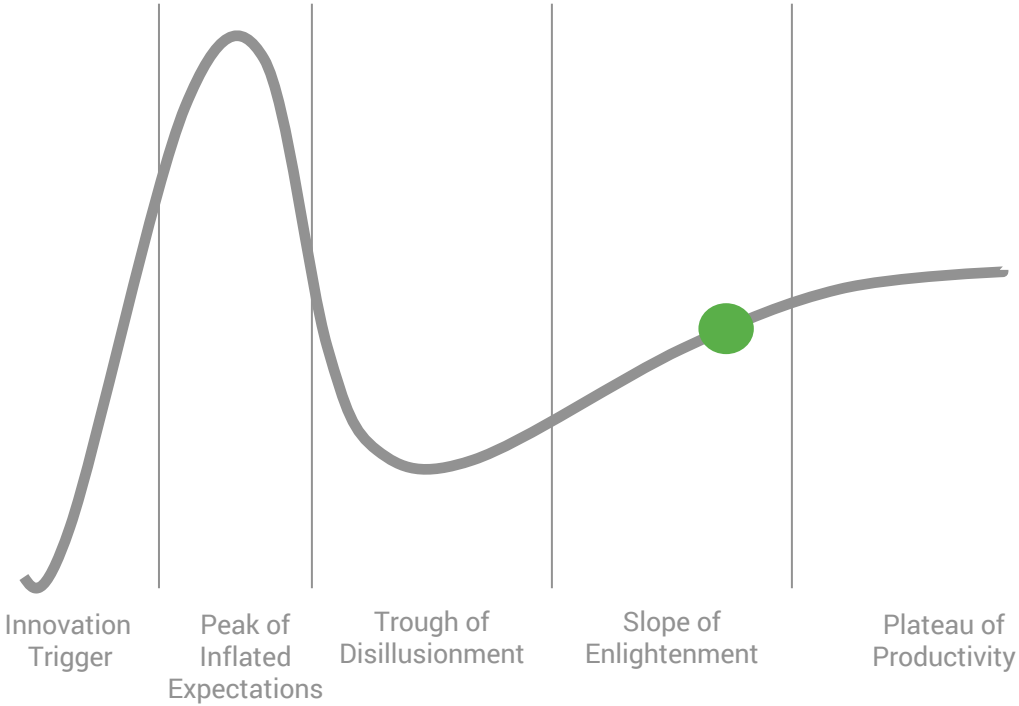
- EXCHANGE THINGS OF VALUE IN A SECURE, TRANSPARENT WAY
- ACT LIKE A SERVER, LOOK LIKE A CLASS

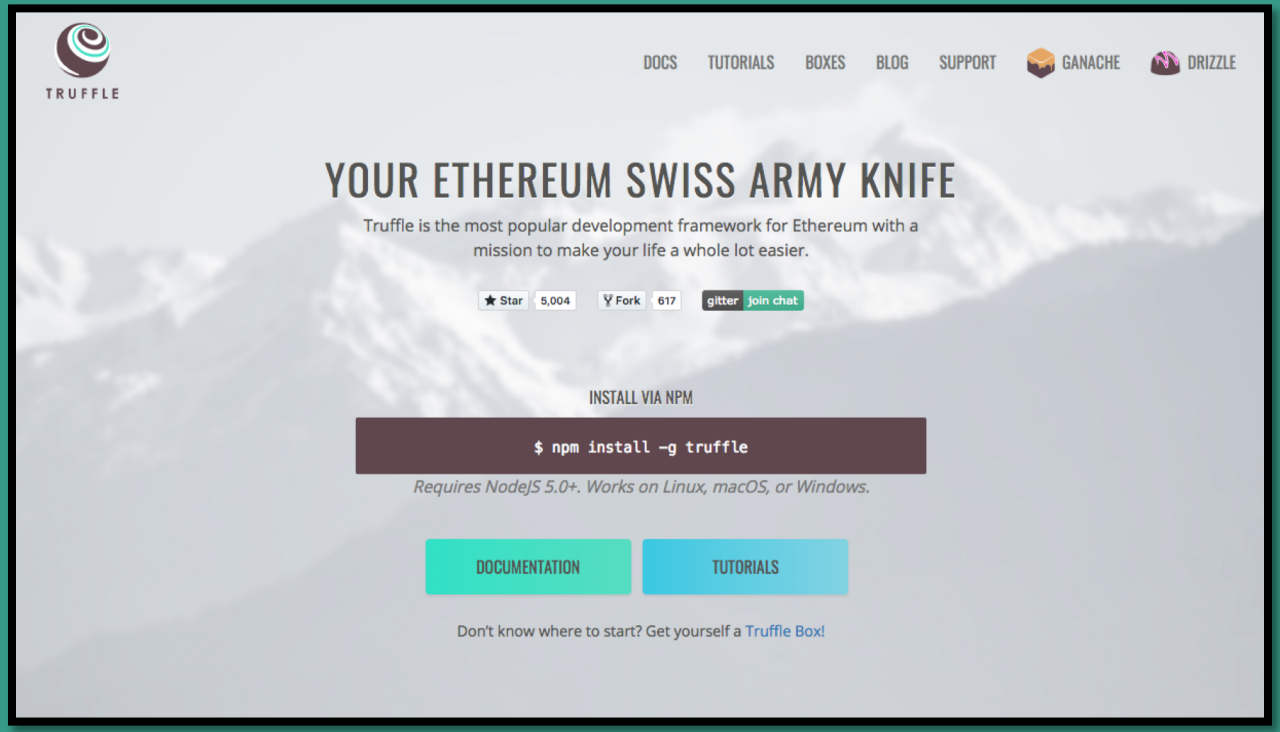


SMART CONTRACT PROS & CONS



DEMO


Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity


TRUFFLE
DOCS
TUTORIALS
BOXES
BLOG
SUPPORT
GANACHE
DRIZZLE
YOUR ETHEREUM SWISS ARMY KNIFE
Truffle is the most popular development framework for Ethereum with a mission to make your life a whole lot easier.
Star 5,004
Fork 617
gitter join chat
INSTALL VIA NPM
$ npm install -g truffle
Requires NodeJS 5.0+. Works on Linux, macOS, or Windows.
DOCUMENTATION
TUTORIALS
Don't know where to start? Get yourself a Truffle Box!

TRUFFLE BOXES

Truffle Boxes are helpful boilerplates that allow you to focus on what makes your dapp unique. In addition to Truffle, Truffle Boxes can contain other helpful modules, Solidity contracts & libraries, front-end views and more; all the way up to complete example dapps.

Official Boxes

Our official boxes come from the developers at Truffle. This first set of boxes is aimed at integration with the React library, with others on the way. Reach out with other official Truffle Boxes you'd like to see, or scroll down to get more information on making your own boxes.

drizzle

★ Star 44

This box comes with everything you need to start using smart contracts from a react app with Drizzle. It includes `drizzle`, `drizzle-react` and `drizzle-react-components` to give you a complete overview of Drizzle's capabilities.

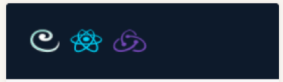
drizzle webpack webapp official

react

★ Star 231

This box comes with everything you need to start using smart contracts from a react app. This is as barebones as it gets, so nothing stands in your way.

react webpack webapp official

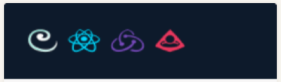


react-auth

★ Star 127

This box adds react-router, redux and redux-auth-wrapper for authentication powered by a smart contract. Great for building your own auth system.

auth react redux webpack webapp official



react-uport

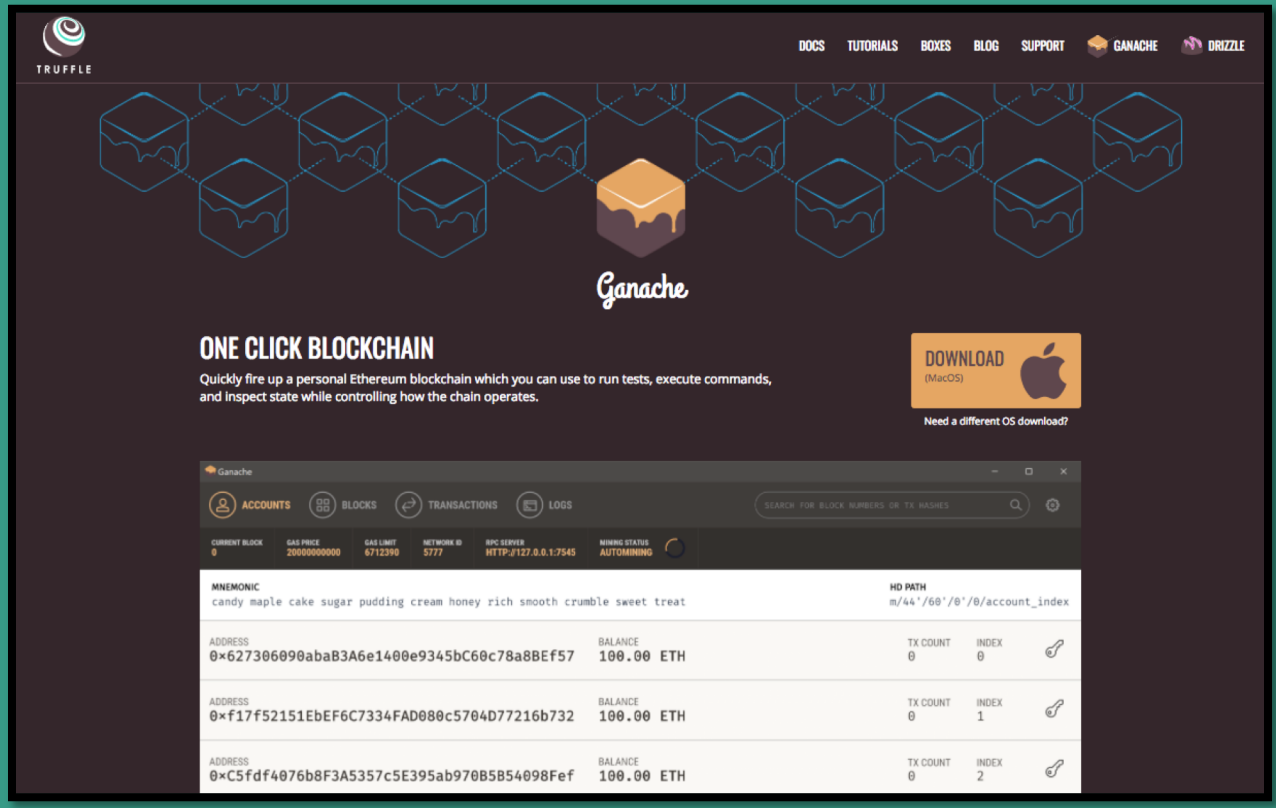
★ Star 68

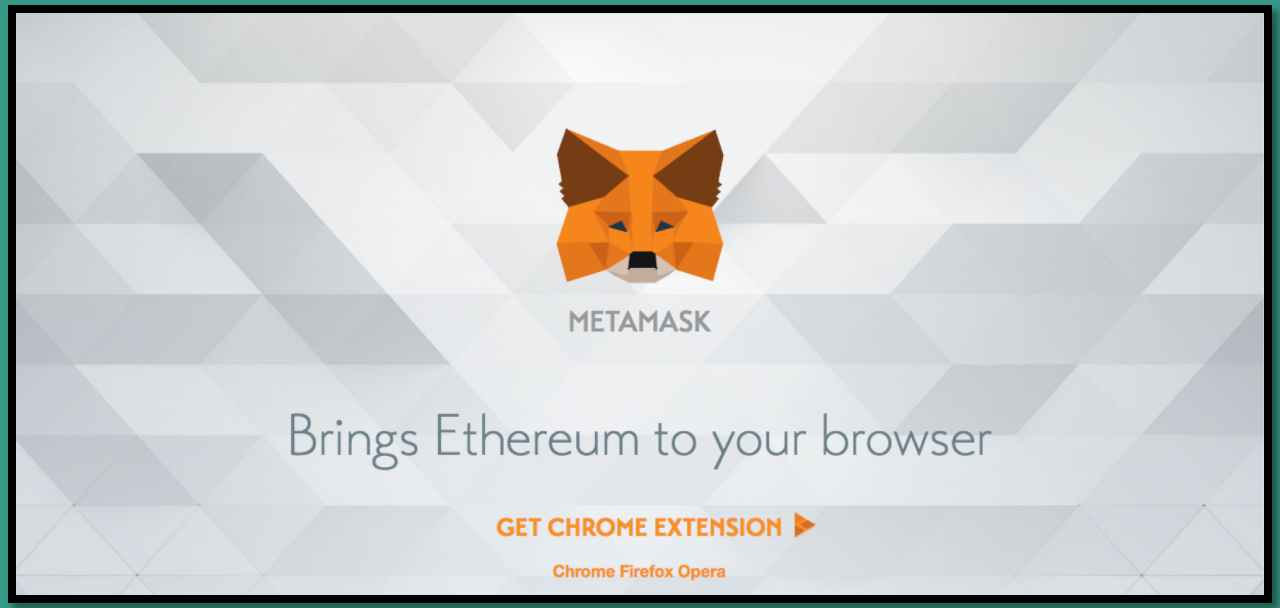
pet-shop

★ Star 65

tutorialtoken

★ Star 24


TRUFFLE
DOCS
TUTORIALS
BOXES
BLOG
SUPPORT
GANACHE
DRIZZLE
Ganache
ONE CLICK BLOCKCHAIN
Quickly fire up a personal Ethereum blockchain which you can use to run tests, execute commands, and inspect state while controlling how the chain operates.
DOWNLOAD
(MacOS)
Need a different OS download?
Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 0
GAS PRICE 20000000000
GAS LIMIT 6712390
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
MNEMONIC
candy maple cake sugar pudding cream honey rich smooth crumble sweet treat
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS 0x627306090abaB3A6e1400e9345bC60c78a8BEf57
BALANCE 100.00 ETH
TX COUNT 0
INDEX 0
ADDRESS 0xf17f52151EbEF6C7334FAD080c5704D77216b732
BALANCE 100.00 ETH
TX COUNT 0
INDEX 1
ADDRESS 0xC5fdf4076b8F3A5357c5E395ab970B5B54098Fef
BALANCE 100.00 ETH
TX COUNT 0
INDEX 2


METAMASK
Brings Ethereum to your browser
GET CHROME EXTENSION
Chrome Firefox Opera

EXPLORER

OPEN EDITORS
- app.js app/javascripts

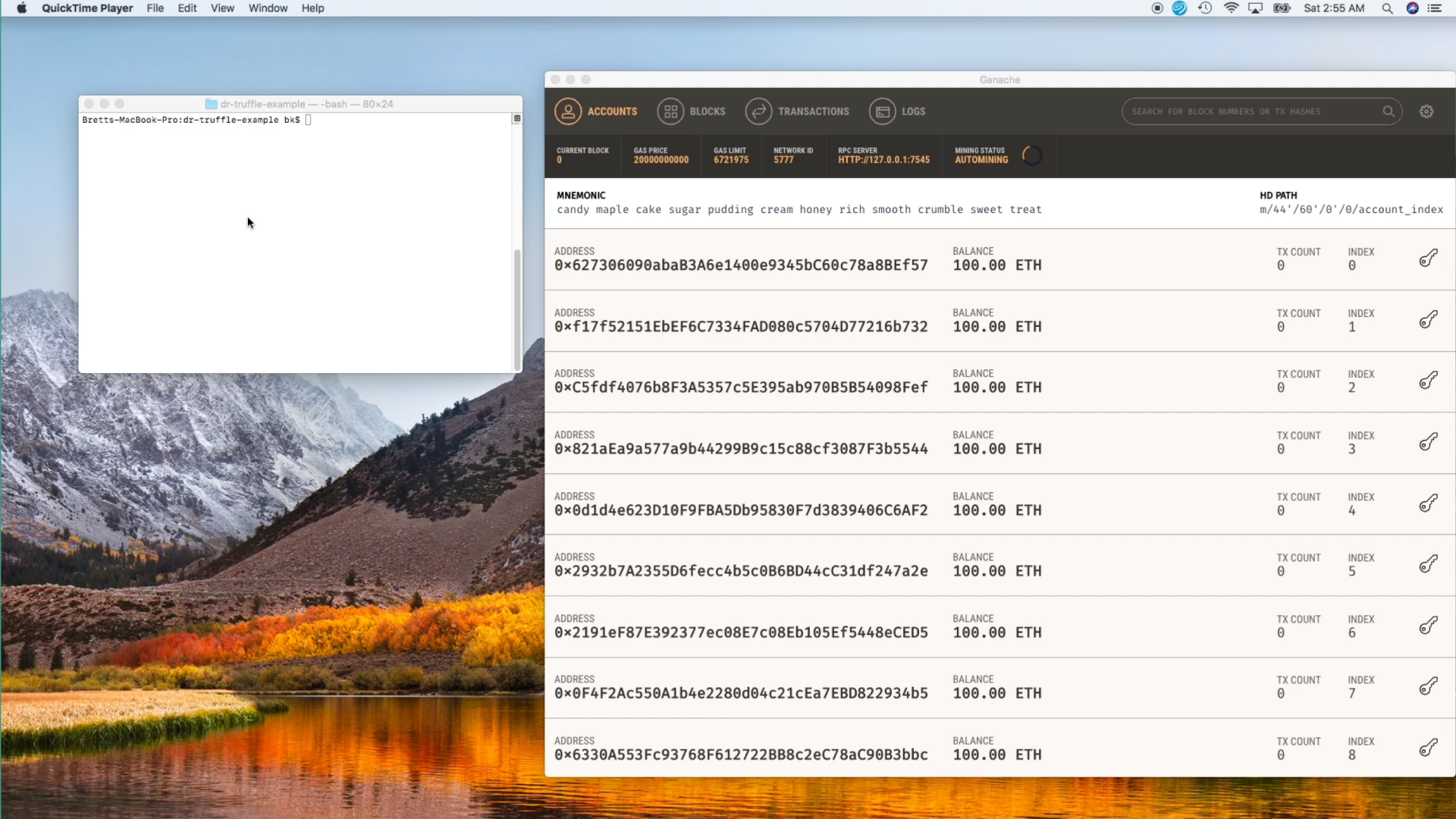
DR-TRUFFLE-EXAMPLE
- app
  - assets
  - javascripts
    - app.js
  - stylesheets
    - app.css
  - favicon.ico
  - index.html
- build
- contracts
  - zeppelin
  - MedicalRecord.sol
  - Migrations.sol
- migrations
- node_modules
- test
- .babelrc
- .eslintignore
- .eslintrc
- .gitignore
- box-img-lg.png
- box-img-sm.png
- npm-debug.log
- package.json
- truffle.js
- webpack.config.js

app.js

```
import { default as Web3 } from 'web3';
import { default as contract } from 'truffle-contract'

// Import our contract artifacts and turn them into usable abstractions.
import medicalrecord_artifacts from '../../build/contracts/MedicalRecord.json'

var MedicalRecord = contract(medicalrecord_artifacts);

var accounts;
var patient;
var doctorsNames;
var contractInstance;

window.App = {
  start: function () {
    var self = this;

    // Bootstrap the MetaCoin abstraction for Use.
    MedicalRecord.setProvider(web3.currentProvider);

    // Get the initial account balance so it can be displayed.
    web3.eth.getAccounts(function (err, accs) {
      if (err != null) {
        alert("There was an error fetching your accounts.");
        return;
      }

      if (accs.length == 0) {
        alert("Couldn't get any accounts! Make sure your Ethereum client is configured correctly.");
        return;
      }
      patient = accs[0];
      MedicalRecord.deployed().then(function(instance) {
        contractInstance = instance;
      })
      self.getDoctors();
      self.getNotes();
    });
```

```
pragma solidity ^0.4.17;

import './zeppelin/lifecycle/Killable.sol';

contract MedicalRecord is Killable {
    struct Doctor {
        bytes16 name;
        uint id;
    }

    address public patient;
    uint private doctorId;
    bytes16[] public doctorsNames;
    bytes16[] notes;
    mapping (address => Doctor) private doctors;

    modifier onlypatient {
        require(msg.sender == patient);
        _;
    }

    modifier isCurrentDoctor {
        require(!(doctors[msg.sender].id <= doctorId));
        _;
    }

    function MedicalRecord() public {
        patient = msg.sender;
        doctorId = 0;
    }
```

```
32      function giveDoctorAccess(address drAddress, bytes16 name)
33      public
34      onlypatient
35      returns (bytes16)
36      {
37          doctors[drAddress] = Doctor (name, doctorId);
38          doctorId++;
39          doctorsNames.push(name);
40          return (name);
41      }
```


QuickTime Player File Edit View Window Help
Sat 2:55 AM
dr-truffle-example — -bash — 80×24
Bretts-MacBook-Pro:dr-truffle-example bk$
Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 0
GAS PRICE 20000000000
GAS LIMIT 6721975
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
MNEMONIC
candy maple cake sugar pudding cream honey rich smooth crumble sweet treat
HD PATH
m/44'/60'/0'/0/account_index
ADDRESS 0×627306090abaB3A6e1400e9345bC60c78a8BEf57 BALANCE 100.00 ETH TX COUNT 0 INDEX 0
ADDRESS 0×f17f52151EbEF6C7334FAD080c5704D77216b732 BALANCE 100.00 ETH TX COUNT 0 INDEX 1
ADDRESS 0×C5fdf4076b8F3A5357c5E395ab970B5B54098Fef BALANCE 100.00 ETH TX COUNT 0 INDEX 2
ADDRESS 0×821aEa9a577a9b44299B9c15c88cf3087F3b5544 BALANCE 100.00 ETH TX COUNT 0 INDEX 3
ADDRESS 0×0d1d4e623D10F9FBA5Db95830F7d3839406C6AF2 BALANCE 100.00 ETH TX COUNT 0 INDEX 4
ADDRESS 0×2932b7A2355D6fecc4b5c0B6BD44cC31df247a2e BALANCE 100.00 ETH TX COUNT 0 INDEX 5
ADDRESS 0×2191eF87E392377ec08E7c08Eb105Ef5448eCED5 BALANCE 100.00 ETH TX COUNT 0 INDEX 6
ADDRESS 0×0F4F2Ac550A1b4e2280d04c21cEa7EBD822934b5 BALANCE 100.00 ETH TX COUNT 0 INDEX 7
ADDRESS 0×6330A553Fc93768F612722BB8c2eC78aC90B3bbc BALANCE 100.00 ETH TX COUNT 0 INDEX 8

WHAT'S NEXT

LEARN

SOFTWARE ENGINEERING DAILY PODCAST

EXPLAIN BLOCKCHAIN PODCAST

KHAN ACADEMY & UDEMY

MASTERING BITCOIN

GOOGLE "LEARN BLOCKCHAIN BY BUILDING ONE"

CODE

FORK BITCOIN

ETHERUM.ORG/TOKEN

TRUFFLE

WEB3

METAMASK

RESEARCH

CONSENSUS ALGORITHMS

INCREASING THROUGHPUT

GAME THEORY

STATE SYNCHRONIZATION

ECONOMICS

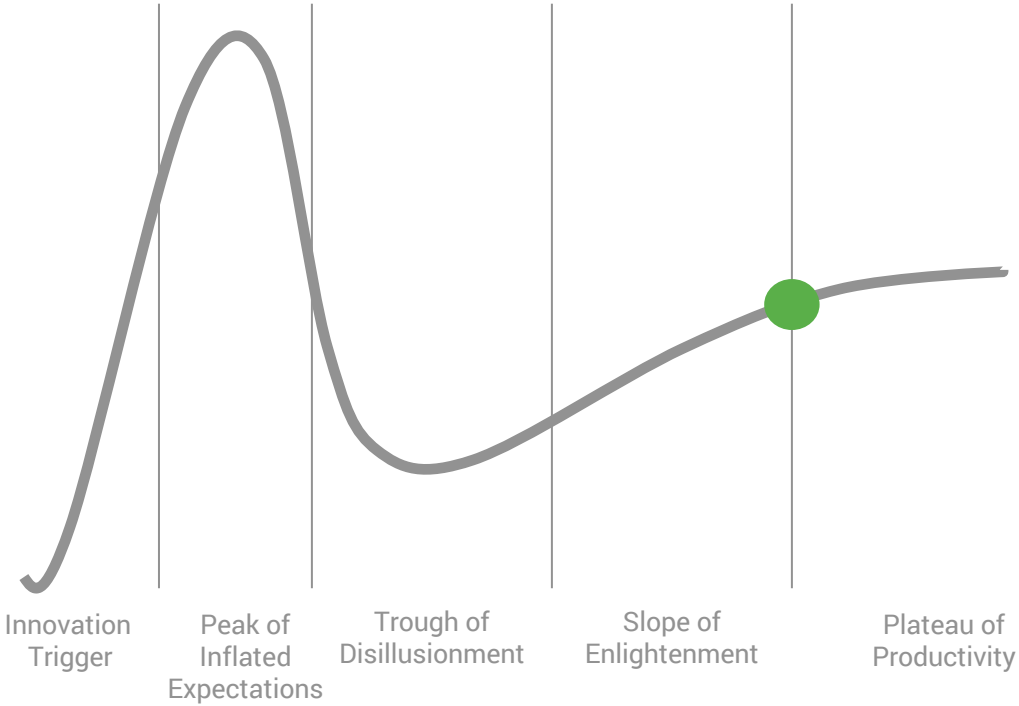
INVESTIGATE

HYPERLEDGER SUITE

CORDA

EMAIL BRETT@BRETTKOENIG.COM

END


Innovation Trigger
Peak of Inflated Expectations
Trough of Disillusionment
Slope of Enlightenment
Plateau of Productivity

SOURCES & RESOURCES

Software engineering daily podcast
Unchained podcast
Explain blockchain podcast
Khan academy
Udemy
Mastering Bitcoin: Programming the Open Blockchain
Parker Mccurley - Decent Crypto
Chris Slee - AWH
https://anders.com/blockchain/block.html
https://anders.com/blockchain/blockchain.html
News.blockchaininformer.com
youtube.com/georgelevy
Blockexplorer.com
blockchain.info
https://blogs.wsj.com/cio/2018/02/07/l-l-bean-to-link-boots-coats-to-a-blockchain/
https://medium.freecodecamp.org/how-does-blockchain-really-work-i-built-an-app-to-show-you-6b70cd4caf7d
http://blockchaindemo.io/
https://www.youtube.com/watch?v=hYip_Vuv8J0
https://www.khanacademy.org/economics-finance-domain/core-finance/money-and-banking/bitcoin/v/bitcoin-transaction-block-chains
https://devchat.tv/js-jabber/jsj-287-blockchain-js-ari-lerner
Blockchain for Dummies IBM
http://ccwikia.com/the-ultimate-3500-word-plain-english-guide-to-blockchain/
https://codeburst.io/build-your-first-ethereum-smart-contract-with-solidity-tutorial-94171d6b1c4b
https://www.ethereum.org/greeter
https://hackernoon.com/ethereum-development-walkthrough-part-2-truffle-ganache-geth-and-mist-8d6320e12269
http://truffleframework.com/tutorials/
http://www.worldbank.org/en/news/video/2016/03/10/2-billion-number-of-adults-worldwide-without-access-to-formal-financial-services
https://blockgeeks.com/guides/cryptocurrencies-cryptography/
FontAwesome Icons - https://fontawesome.com/license

QUESTIONS

BRETT@BRETTKOENIG.COM

softwareengineeringdaily.com

explainblockchain.io

hyperledger.org

ethereum.org/token

ethereum.org/greeter

anders.com/blockchain

truffleframework.com