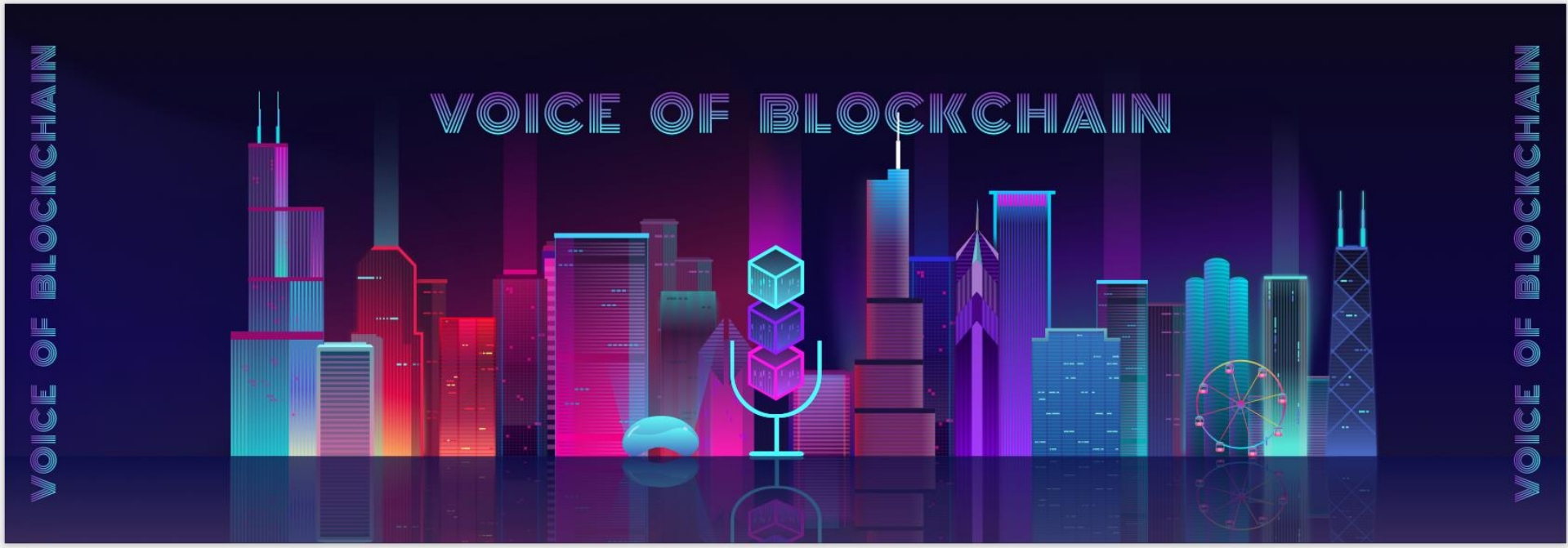


Roadmap to "Blockchain" Your IT Organization:

How to Help your IT Staff Go from Square One to Competence and Dominance in Blockchain Technologies

William Favre Slater, III
President & CEO
Slater Technologies, Inc.

August 24, 2018

Slater Technologies

Presentation Location

http://billslater.com/blockchain

Blockchain Resources

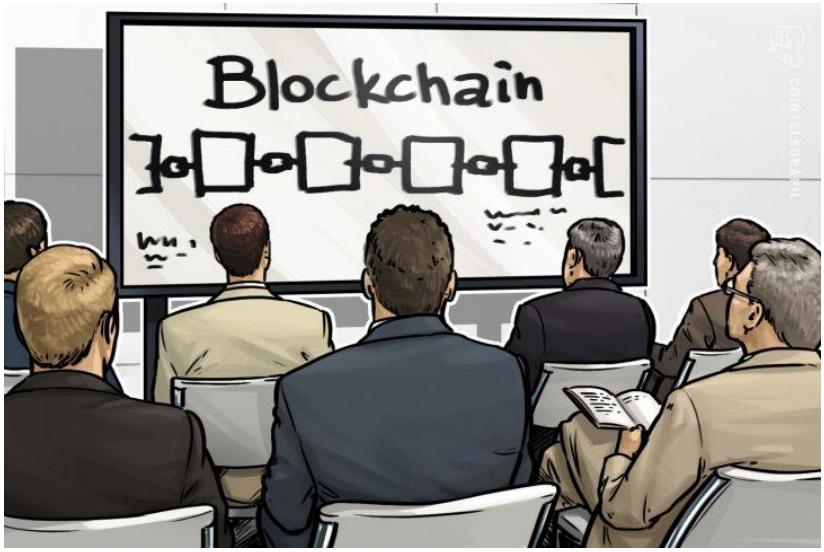
https://goo.gl/baf6Uc

Bitcoin Resources

https://goo.gl/HhtCU7

Agenda

- Introduction and Where Are We Right Now?
- The Problem
- The Solutions
- Required Skills
- DApps and DApp Environment
- Case Studies
- The Challenges
- Solving the Challenges and Winning
- The Roadmap
- Some Valuable Resources
- Conclusion
- References



Slater Technologies

INTRODUCTION AND WHERE ARE WE RIGHT NOW?

Slater Technologies

Introduction

- William Favre Slater, III
  - Career Professional in Information Technology. Specialities: Cybersecurity, Data Centers, Blockchain, Infrastructure Management, Application Development, Project Management, Program Management, Service Management and Risk Management. This is me: http://billslater.com/interview
- I am also a former U.S. Air Force Officer and a Patriotic American Citizen who loves America, believes in the U.S. Constitution and the Bill of Rights.
- I am also a writer, and Adjunct Professor at the Illinois Institute of Technology for more than 10 years.
- I am happily married to my Soul Mate, who is my Best Friend and the Love of my Life, Ms. Joanna Roguska, who is a professional web developer and a native of Warsaw, Poland. We have been happily married since December 2000, and she became a U.S. Citizen in November 2006.

Slater Technologies

A Career in Information Technology

http://billslater.com/wfs_cv.pdf

http://billslater.com/wfs_resume.pdf

http://billslater.com/career

http://billslater.com/certifications

http://billslater.com/interview

http://billslater.com/writing

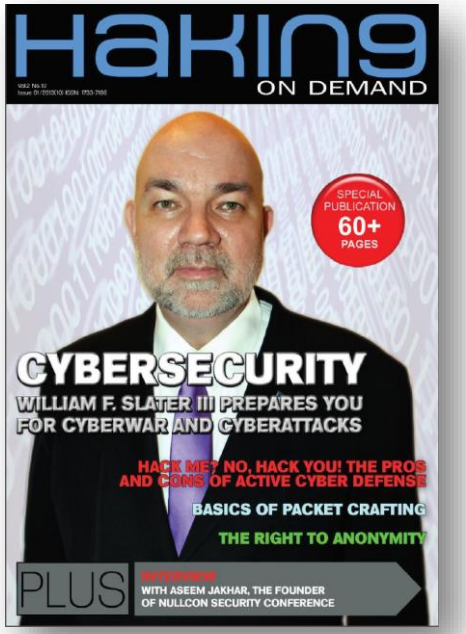
http://billslater.com/datacentermanager

http://billslater.com/iso27001

http://billslater.com/ms_cybersecurity

http://on.fb.me/fW3wH0

http://on.fb.me/vfGRVi



January 15, 2013

August 24, 2018

First Job Out of College

Strategic Air Command Headquarters
Offutt Air Force Base, NE
Circa late 1970s – UNCLASSIFIED Configuration

2LT William F. Slater, III
United States Air Force
Computer Systems Staff Officer

Slater Technologies

Microsoft Chicago Data Center

CHICAGO DATA CENTER

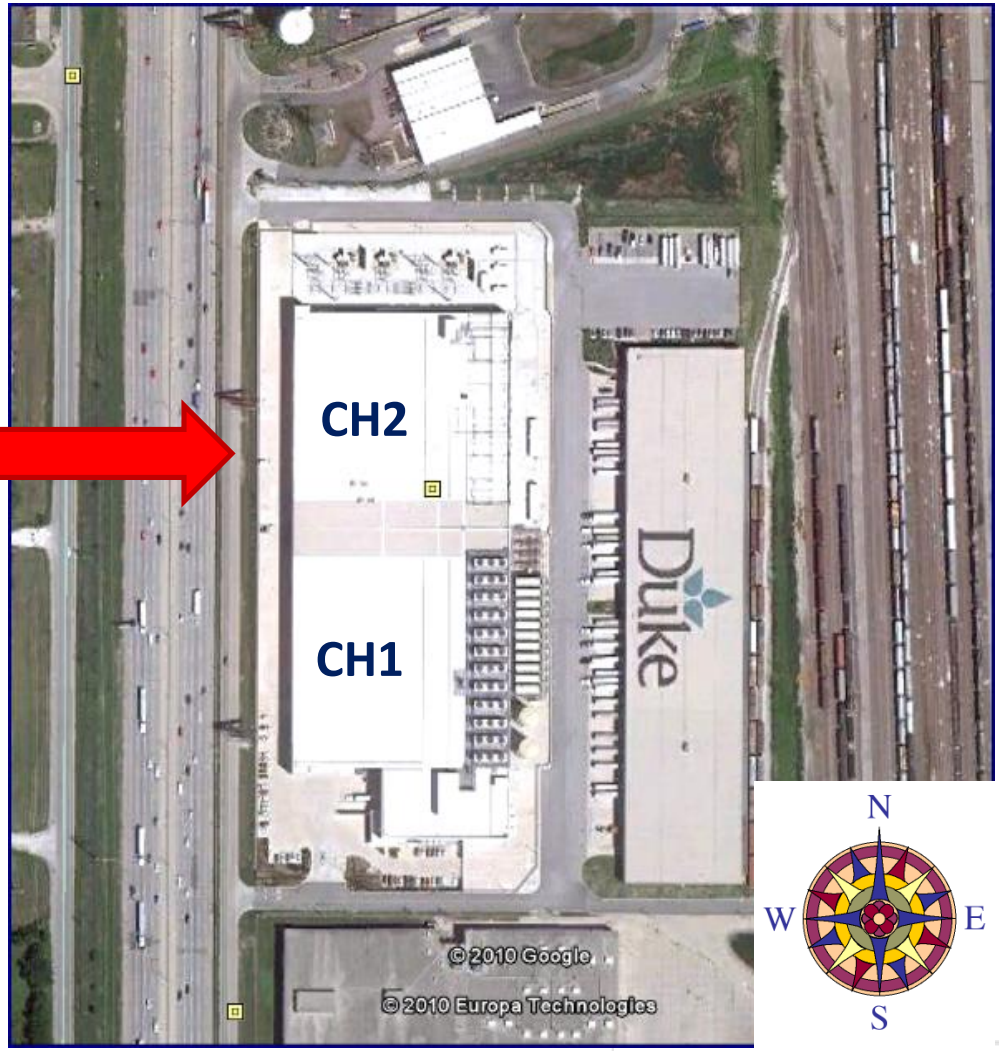
Microsoft Chicago Data Center in Northlake, IL. Actual street view photo from Google Maps

Microsoft Chicago Data Center in Northlake, IL. Actual architect's drawing from 2007 - 2008

Microsoft Chicago Data Center

CH1						
	Colo Rooms		Cabinets		Servers per Cabinet	
Second Floor	4		240		42	40,320
			Modules			
First Floor	1		56		2400	134,400

CH2						
	Colo Rooms		Cabinets		Servers per Cabinet	
Second Floor	4		240		42	40,320
			Modules			
First Floor	1		48		2400	115,200
					Total Production Servers	330,240



601 Northwest Hwy, Northlake, IL

Size:	**705,000 square feet**
Power:	**120 MW (enough to power 87,000 homes)**
Critical Load for IT Equipment:	**60 MW**
No. of Physical Servers:	**> 330,000 Servers**

CHICAGO DATA CENTER

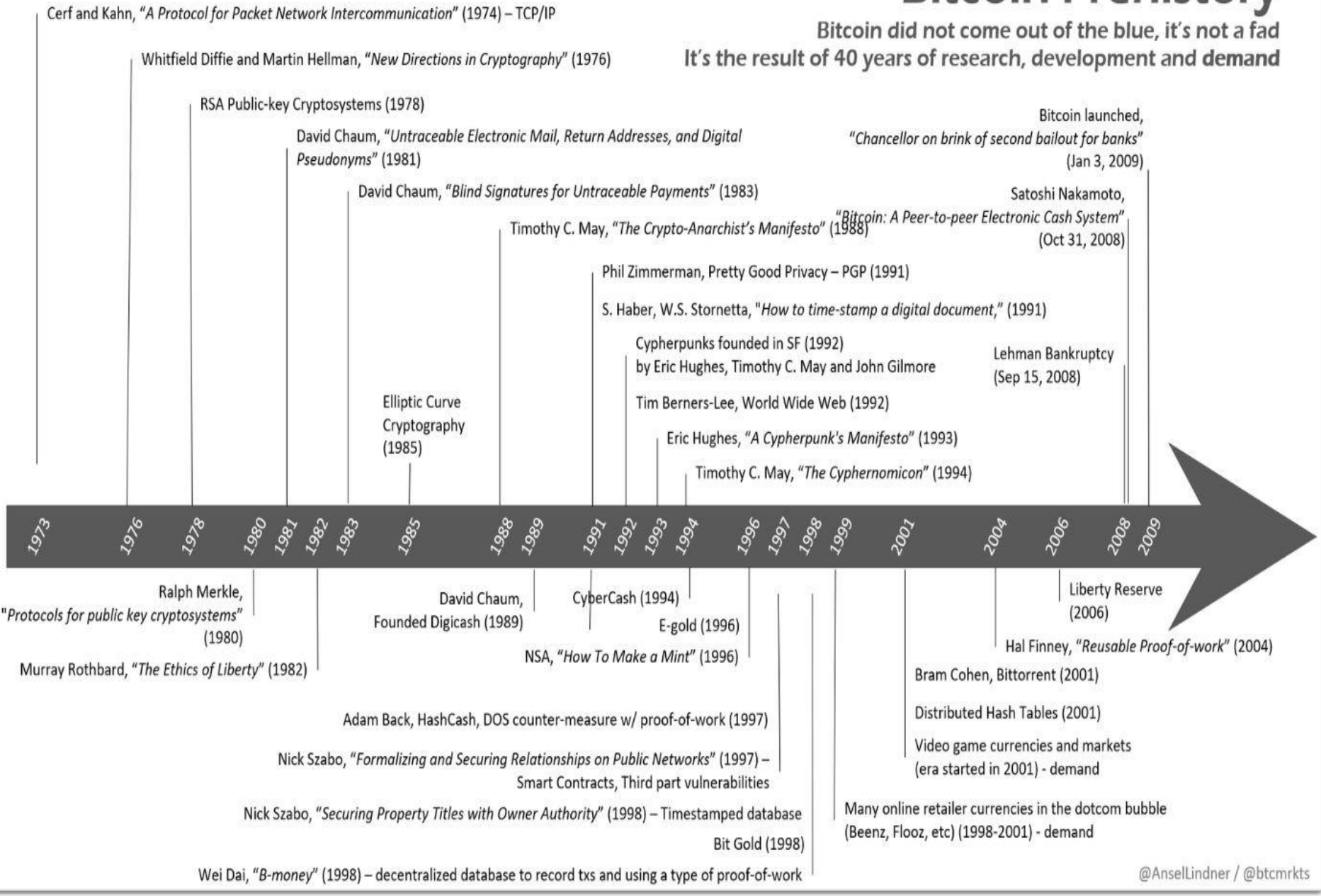
Microsoft Chicago Data Center Operations Team Summer 2008

WHERE ARE WE RIGHT NOW?

Slater Technologies

Bitcoin Prehistory

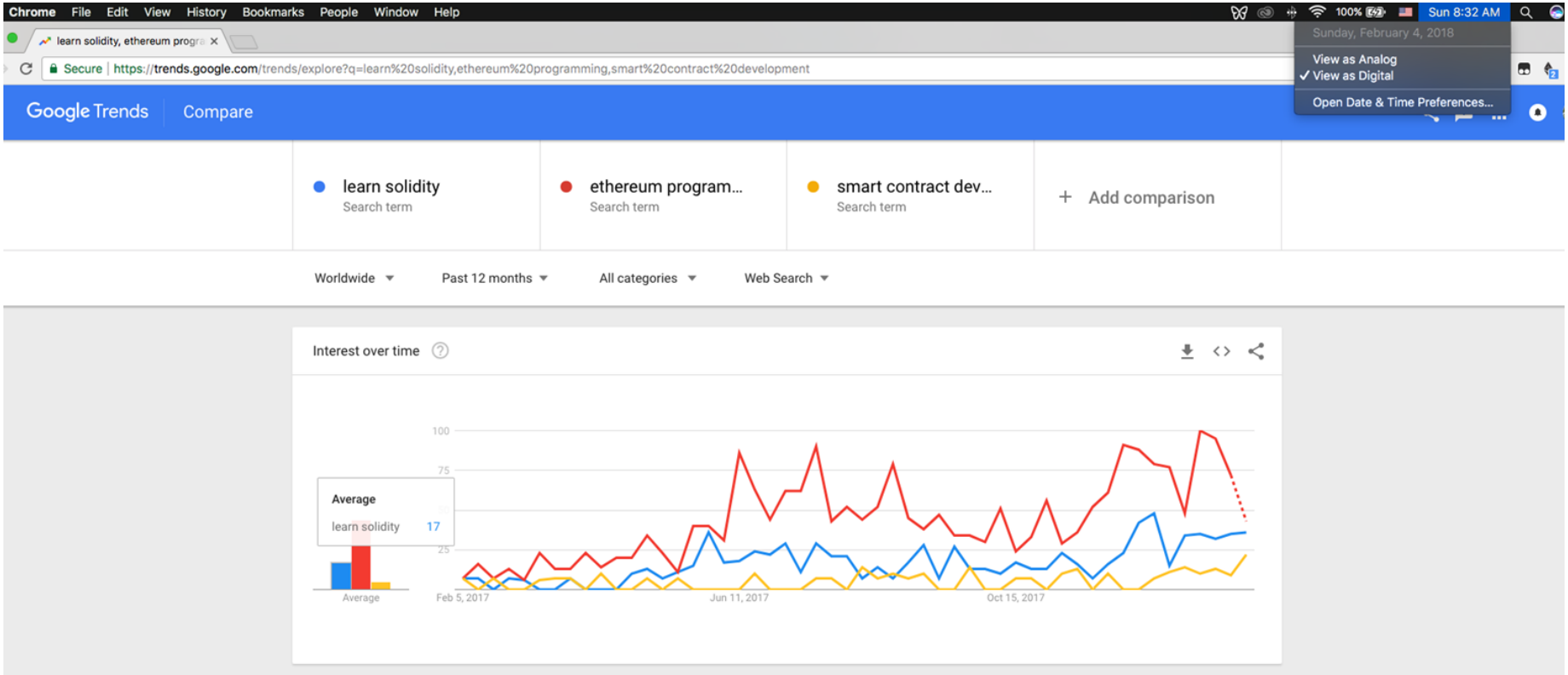
Bitcoin did not come out of the blue, it's not a fad
It's the result of 40 years of research, development and demand



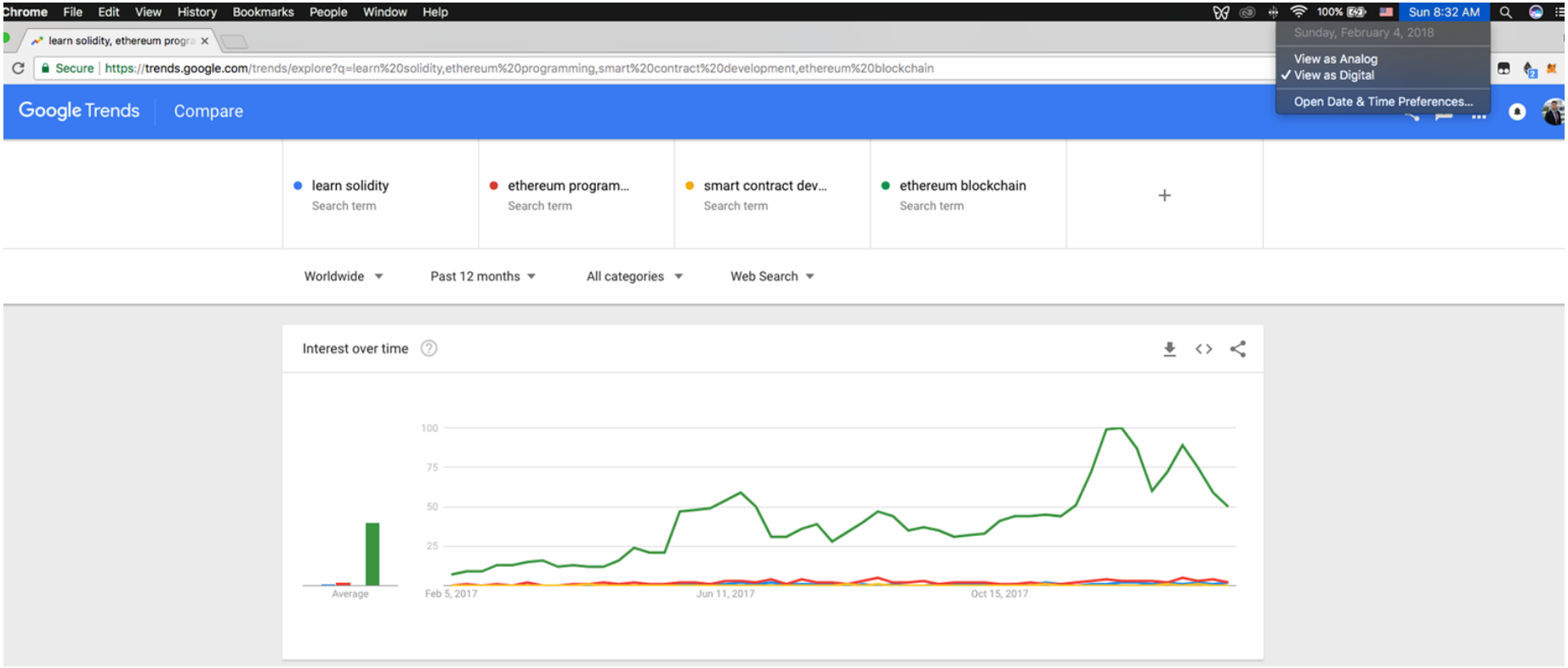
PURPOSE

A lot of talk,
not a lot of walk.

Slater Technologies



Slater Technologies



Slater Technologies

Shortage.
Huge shortage.

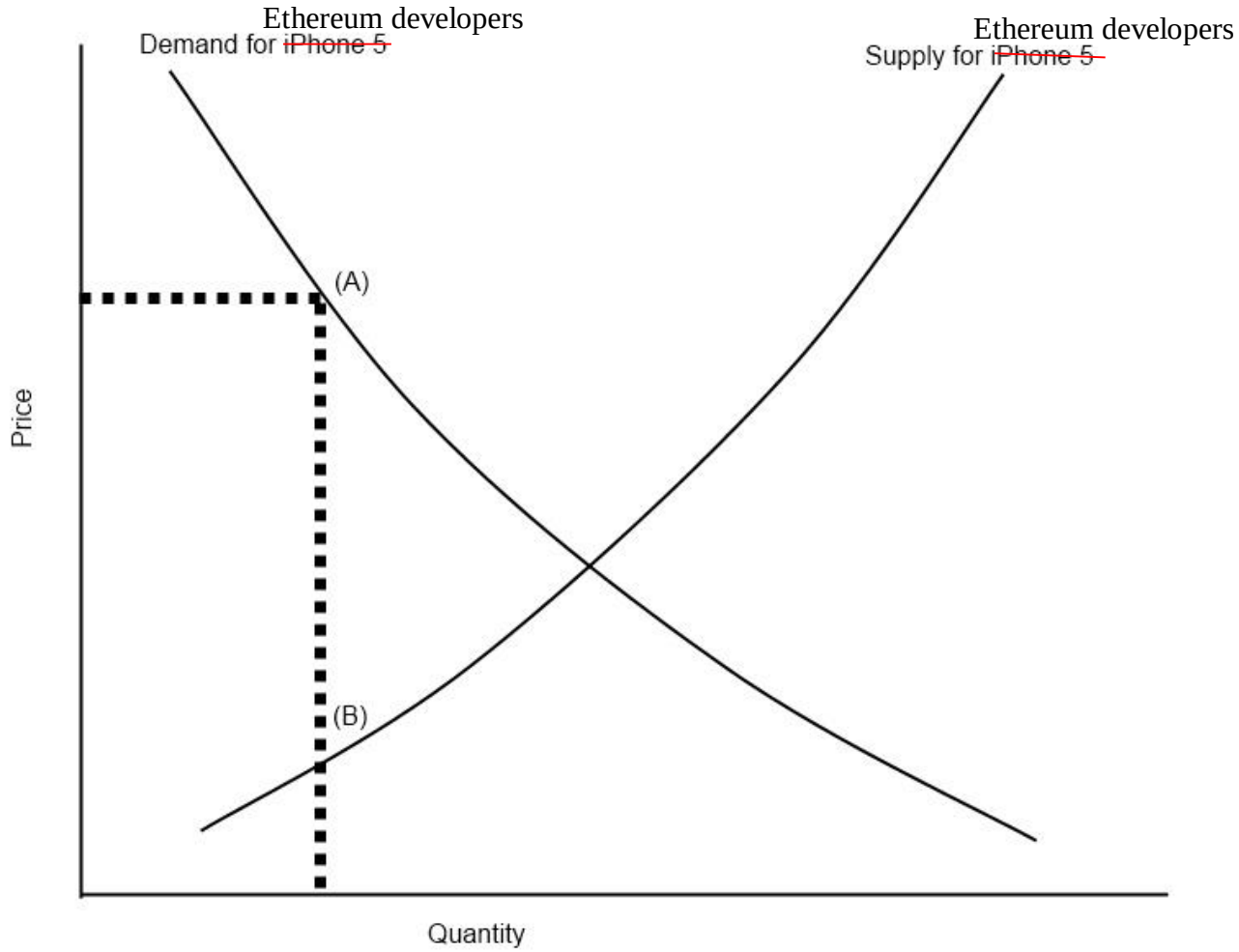
Slater Technologies

Slater Technologies

PURPOSE

Simple economics.

Slater Technologies



Slater Technologies

PURPOSE

Still very early.

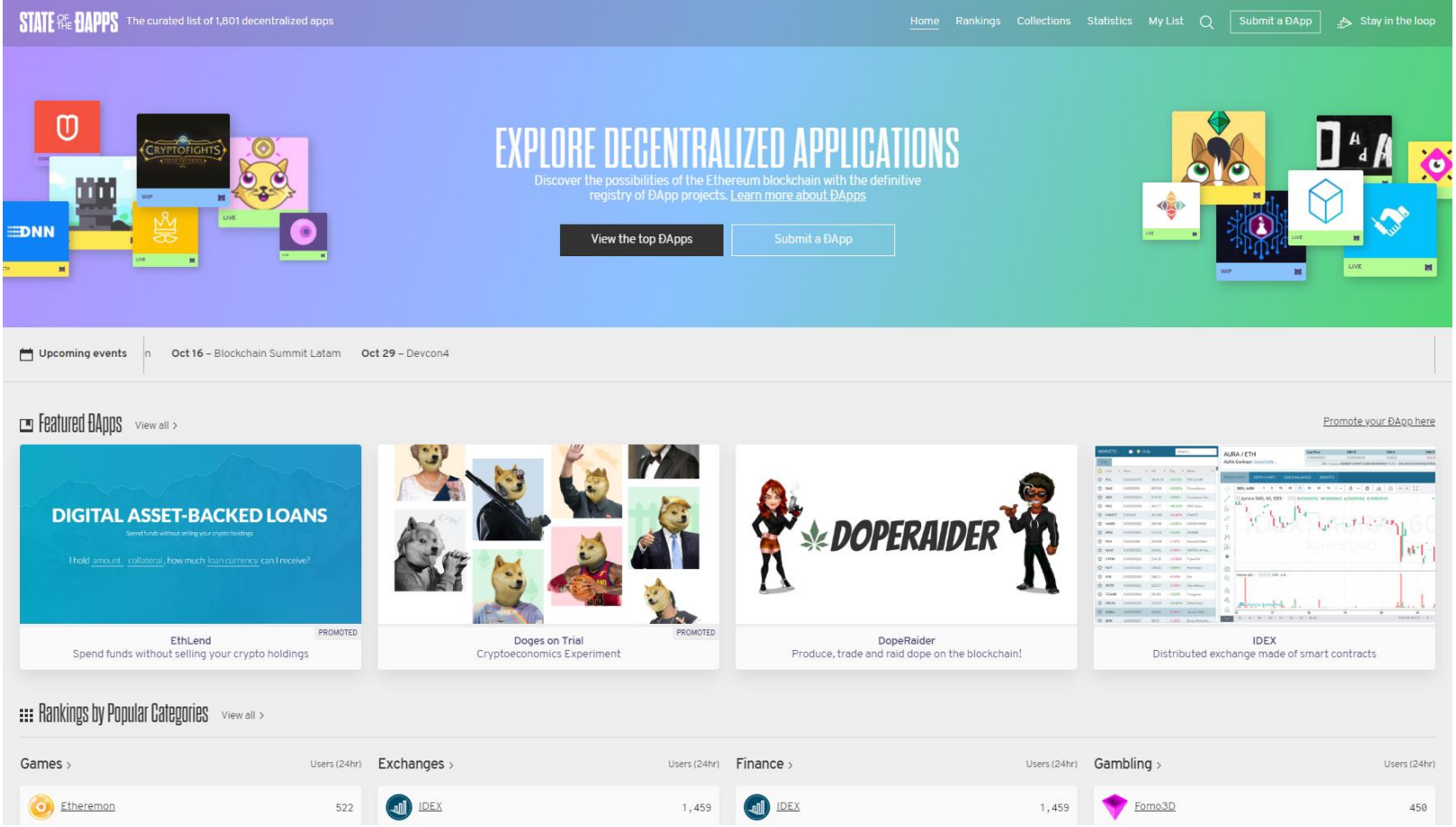
Slater Technologies

Ethereum / Initial release date

July 30, 2015

Ethereum was proposed in late 2013 by Vitalik Buterin, a cryptocurrency researcher and programmer. Development was funded by an online crowdsale that took place between July and August 2014. The system went live on **30 July 2015**, with 11.9 million coins "premined" for the crowdsale.

Slater Technologies



1801 Ethereum DApps currently

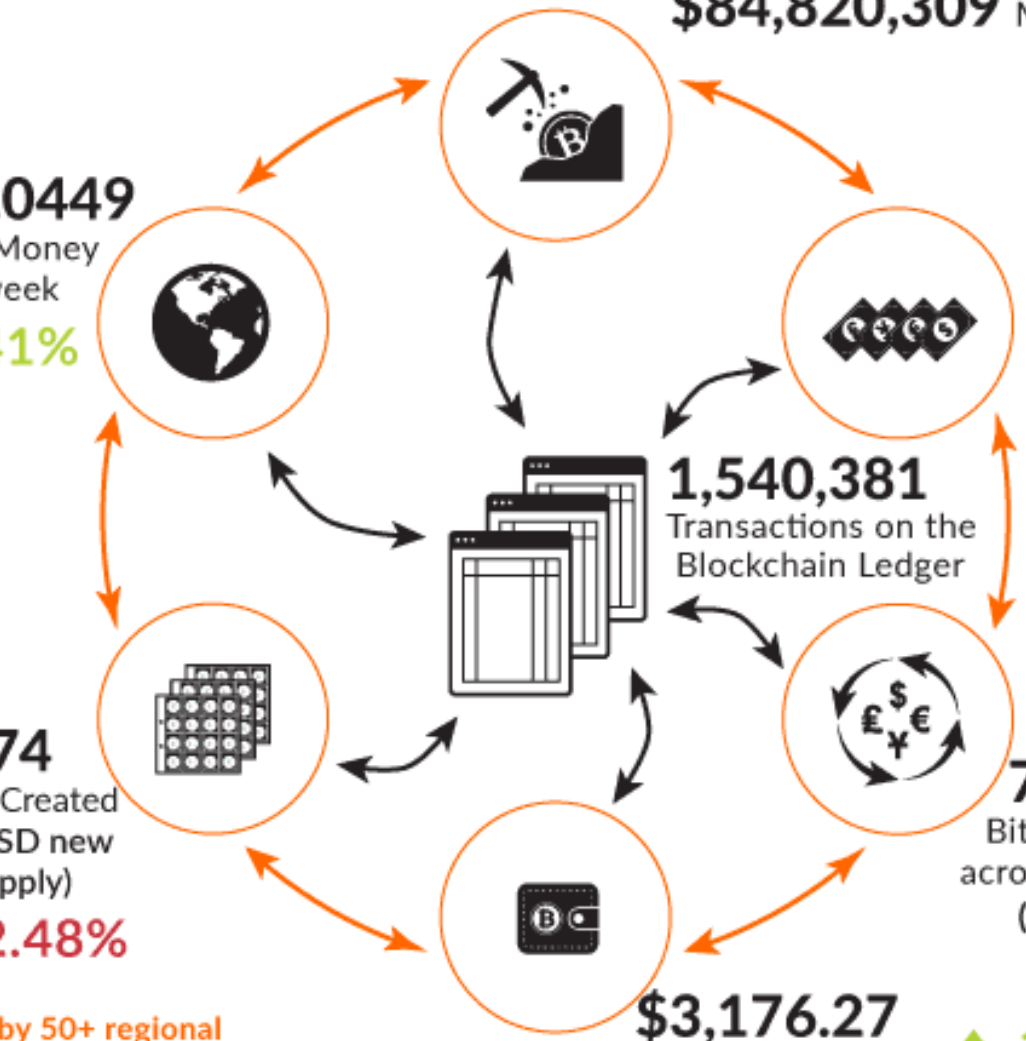
Source: https://www.stateofthedapps.com/

Slater Technologies

Slater Technologies

Weekly Bitcoin & Blockchain Statistics

The week of: August 13th - 20th, 2018



$84,820,309 Miners Revenue in USD
▼ 4.62%

Ratio: 0.0449
Velocity of Money for the week
▲ 7.41%

BLX
Average price this week:
$6,318.10USD
▼ 2.39%

1,540,381
Transactions on the Blockchain Ledger

13,274
New Bitcoin Created ($83.86M USD new money supply)
▼ 2.48%

774,389k ▲ 7.49%
Bitcoin Transacted across the Blockchain ($4.89B USD)

$3,176.27 ▲ 1.69%
Average Blockchain Transaction in USD

Bitcoin is traded by 50+ regional markets (fiat pairs) across 200+ trading platforms.

BRAVE NEWCOIN.
Digital Currency Insights

The Problem

- A significant shortage of Blockchain Developer Talent
  - As of February 2018, it was reported that for every experienced Blockchain Engineer, there are 14 jobs available.
- The technical concepts and value are sound and the tools exist, but experienced people and project managers are very difficult to find.

Slater Technologies

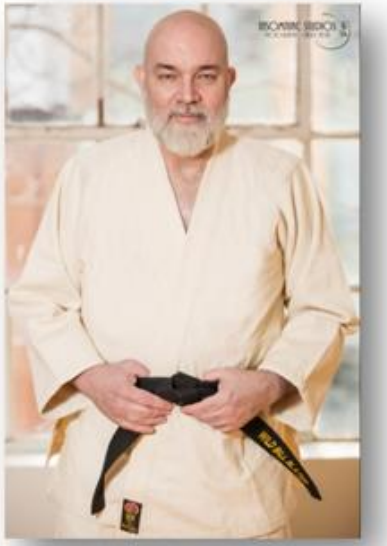
The Solutions

- Train your staff with in-house training and/or mentors that experienced “experts”
- Send your staff to one or more Blockchain Developer Bootcamps (think DApperNetwork by Eric Chung)
- Provide self-training courses and hope for the best

Slater Technologies

Dappernetwork Ethereum DApp Bootcamp Attendees from Our Blockchain Team – at mHub, Chicago, Illinois, August 11, 2018

Kristen Counter



William Slater

Sara Shatdarsanam

Slater Technologies

The Required Skills for a Blockchain Development Staff

Blockchain Developer Skill Set
Top 30 Co-occurring IT Skills

For the 6 months to 12 July 2018, Blockchain Developer job roles required the following IT skills in order of popularity. The figures indicate the absolute number co-occurrences and as a proportion of all permanent job ads featuring Blockchain Developer in the job title.

1	397 (100.00%)	Blockchain	15	111 (27.96%)	Smart Contracts
2	200 (50.38%)	Finance	16	107 (26.95%)	Solidity
3	184 (46.35%)	JavaScript	17	106 (26.70%)	Linux
4	168 (42.32%)	Node.js	18	104 (26.20%)	AngularJS
5	151 (38.04%)	Ethereum	19	101 (25.44%)	Docker
6	146 (36.78%)	Bitcoin	20	98 (24.69%)	Redis
7	142 (35.77%)	SQL	21	93 (23.43%)	MySQL
8	139 (35.01%)	Cryptocurrency	21	93 (23.43%)	Banking
9	134 (33.75%)	Java	22	92 (23.17%)	Amazon AWS
10	125 (31.49%)	NoSQL	23	88 (22.17%)	HTML
11	123 (30.98%)	Git (software)	24	85 (21.41%)	Telecoms
12	122 (30.73%)	React	24	85 (21.41%)	PostgreSQL
13	118 (29.72%)	Test Automation	25	84 (21.16%)	Agile Software Development
13	118 (29.72%)	GitHub	25	84 (21.16%)	ES6
14	115 (28.97%)	Front End Development	26	77 (19.40%)	CSS

Slater Technologies

Additional Required Skills for a Blockchain Development Staff

- Web3.js
- DApp development
- UI and UX Design and Testing Skills
- Deep understanding of compiled code, Gas, and the Ethereum Virtual Machine (EVM)
- Secure coding
- Defensive coding
- Egoless Programming
- Stringent Code Reviews
- Networking
- Understanding of Protocols
- Planning
- Requirements
- Technical Specifications and Writing
- Design
- Architecture – Infrastructure, Data, and Security
- Testing – Testing – Testing
- Simulation
- Troubleshooting

And don't forget PROJECT MANAGEMENT!

Slater Technologies

Web3.js

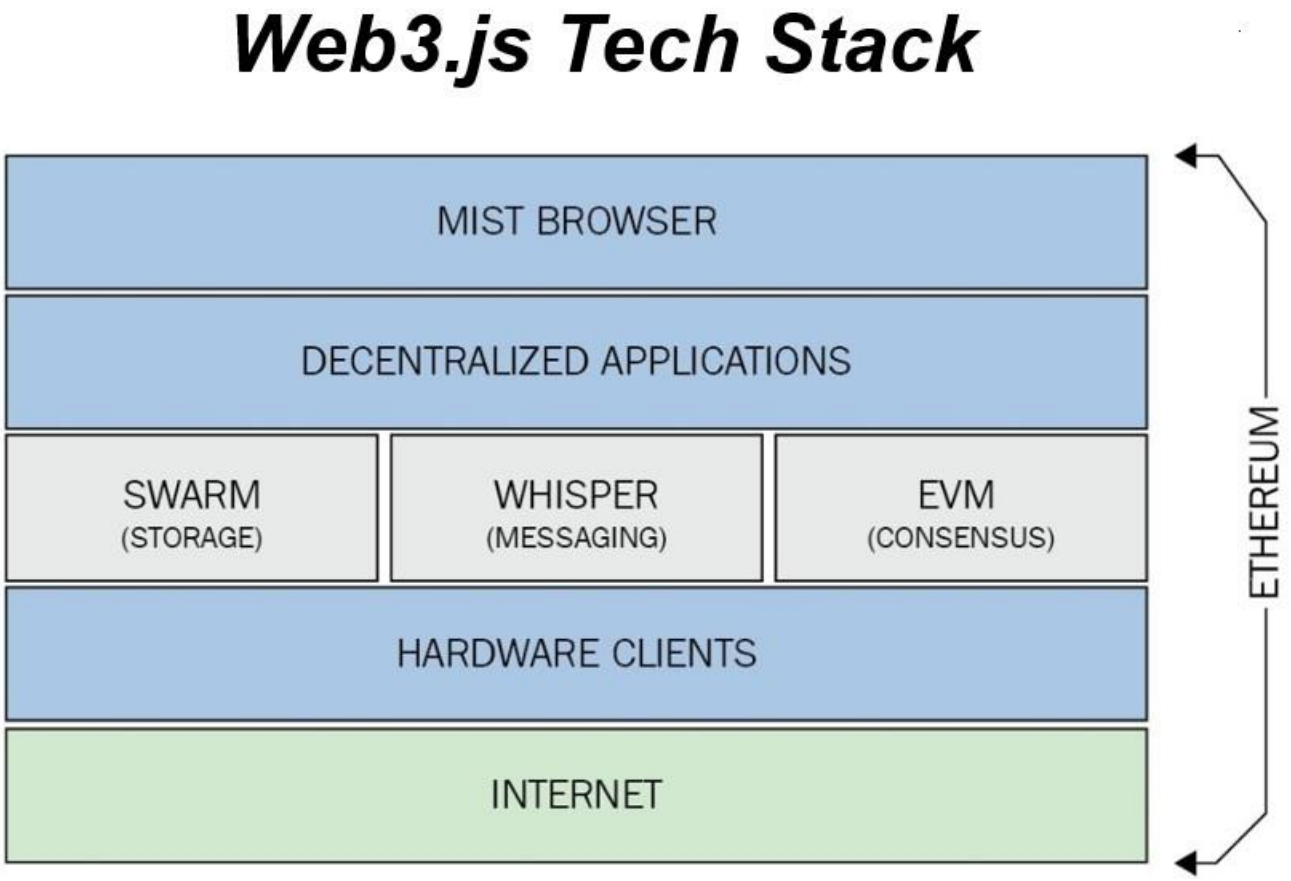


Figure 2.4: Web 3.0 tech stack for Ethereum, Source: Ethereum stack exchange

Slater Technologies

The Required Skills - Quick Preview

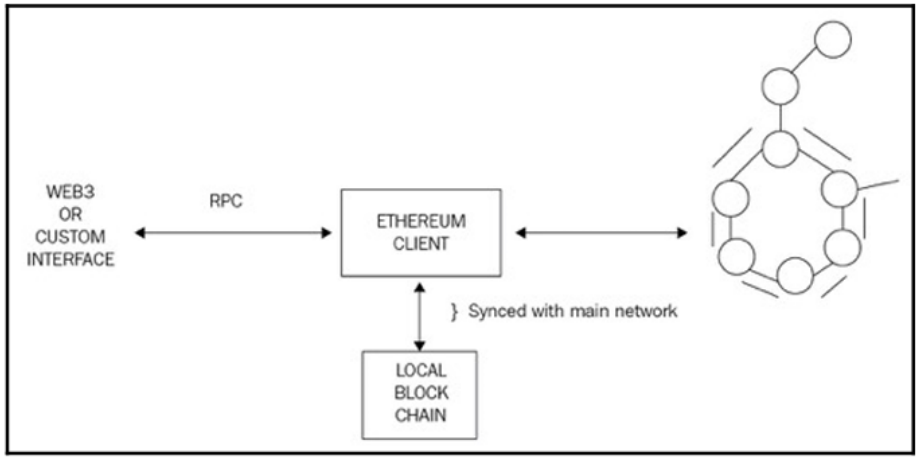
- Web3.js
- EVM
- Ethereum Blockchain
- Ethereum Ecosystem
- Gas

Slater Technologies

Ethereum Architecture

The Ethereum blockchain stack consists of various components. At the core, there is the Ethereum blockchain running on the peer-to-peer Ethereum network. Secondly, there's an Ethereum client (usually Geth) that runs on the nodes and connects to the peer-to-peer Ethereum network from where blockchain is downloaded and stored locally. It provides various functions, such as mining and account management. The local copy of the blockchain is synchronized regularly with the network. Another component is the `web3.js` library that allows interaction with the `geth` client via the **Remote Procedure Call** (**RPC**) interface.

This architecture can be visualized in the following diagram:

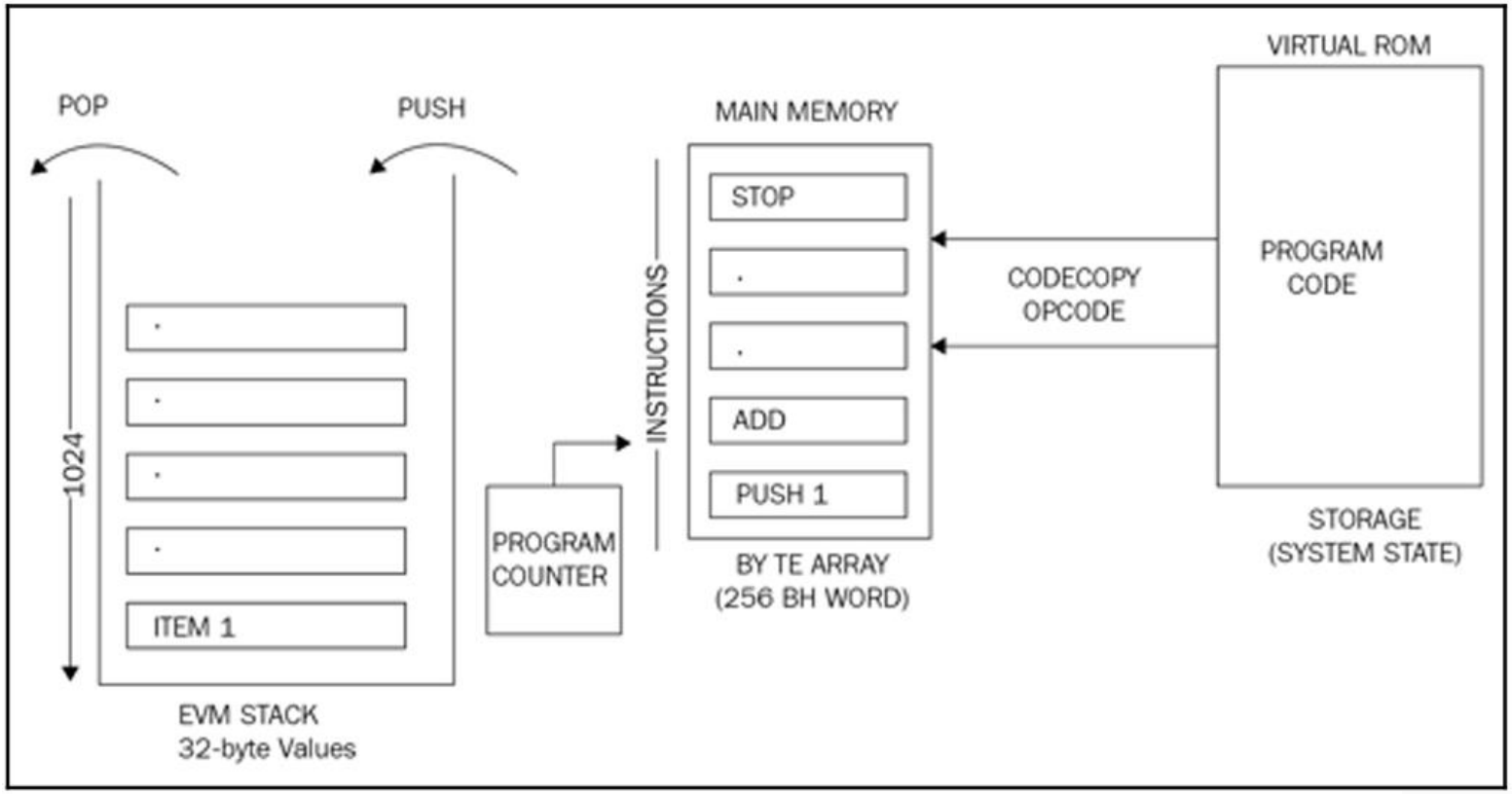


The Ethereum stack showing various components

Slater Technologies

Source: Mastering Blockchain by Imran Bashir (Published by Packt.)

EVM Operation and Architecture



EVM operation

Slater Technologies

Source: Mastering Blockchain by Imran Bashir (Published by Packt.)

Byte Code Executed by the EVM

Runtime bytecode

Raw hex codes:

```
606060405260e060020a6000350463989e17318114601c575b6000565b346000576029600435
5603b565b604080519182525190819003602001905f35b600281015b91905056
```

Opcodes:

```
PUSH1 0x60 PUSH1 0x40 MSTORE PUSH1 0x2 PUSH1 0x0 SSTORE CALLVALUE PUSH1 0x0
JUMPI JUMPDEST PUSH1 0x45 DUP1 PUSH1 0x1A PUSH1 0x0 CODECOPY PUSH1 0x0
RETURN PUSH1 0x60 PUSH1 0x40 MSTORE PUSH1 0xE0 PUSH1 0x2 EXP PUSH1 0x0
CALLDATALOAD DIV PUSH4 0x989E1731 DUP2 EQ PUSH1 0x1C JUMPI JUMPDEST PUSH1
0x0 JUMP JUMPDEST CALLVALUE PUSH1 0x0 JUMPI PUSH1 0x29 PUSH1 0x4
CALLDATALOAD PUSH1 0x3B JUMP JUMPDEST PUSH1 0x40 DUP1 MLOAD SWAP2 DUP3
MSTORE MLOAD SWAP1 DUP2 SWAP1 SUB PUSH1 0x20 ADD SWAP1 RETURN JUMPDEST
PUSH1 0x2 DUP2 ADD JUMPDEST SWAP2 SWAP1 POP JUMP
```

Slater Technologies

Source: Mastering Blockchain by Imran Bashir (Published by Packt.)

Gas and Units of Ether and Wei

While wei is the most used unit, there are also others denominations, here's a brief overview & conversion table of them in Ether :

wei	0.000000000000000001
kwei - ada	0.000000000000001
mwei - babbage	0.000000000001
gwei -shannon	0.000000001
szabo	0.000001
finney	0.001
ether	**1**
kether-grand-einstein	1000
mether	1,000,000
gether	1,000,000,000
tether	1,000,000,000,000

And in wei:

wei	**1**
kwei - ada	1,000
mwei - babbage	1,000,000
gwei -shannon	1,000,000,000
szabo	1,000,000,000,000
finney	1,000,000,000,000,000
ether	1,000,000,000,000,000,000
kether-grand-einstein	1,000,000,000,000,000,000,000
mether	1,000,000,000,000,000,000,000,000
gether	1,000,000,000,000,000,000,000,000,000
tether	1,000,000,000,000,000,000,000,000,000,000

Note: Your Solidity Code compiles to Byte Code. Each Byte Code Instruction has a predetermined Amount of Gas Value required for execution. Run out of Gas and your program stops. Or worse, Write a bad program that:

1) loops endlessly
2) Needlessly allocates huge array structures
3) Thoughtlessly allocates storage
4) Or, instantiates Smart Contracts too often and things will get EXPENSIVE REALLY FAST

Source: Ethereum, Tokens & Smart Contracts: Notes on getting started by Eugenio Noyola

Slater Technologies

Gas

Gas is required to be paid for every operation performed on the Ethereum blockchain. This is a mechanism that ensures that infinite loops cannot cause the whole blockchain to stall due to the Turing-complete nature of the EVM. A transaction fee is charged as some amount of Ether and is taken from the account balance of the transaction originator.

A fee is paid for transactions to be included by miners for mining. If this fee is too low, the transaction may never be picked up; the more the fee, the higher are the chances that the transactions will be picked up by the miners for inclusion in the block. Conversely, if the transaction that has an appropriate fee paid is included in the block by miners but has too many complex operations to perform, it can result in an out-of-gas exception if the gas cost is not enough. In this case, the transaction will fail but will still be made part of the block, and the transaction originator will not get any refund.

Transaction cost can be estimated using the following formula:

$$Total\ cost = gasUsed * gasPrice$$

Here, *gasUsed* is the total gas that is supposed to be used by the transaction during the execution and *gasPrice* is specified by the transaction originator as an incentive to the miners to include the transaction in the next block. This is specified in Ether. Each EVM opcode has a fee assigned to it. It is an estimate because the gas used can be more or less than the value specified by the transaction originator originally. For example, if computation takes too long or the behavior of the smart contract changes in response to some other factors, then the transaction execution may perform more or fewer operations than intended initially and can result in consuming more or fewer gas. If the execution runs out of gas, everything is immediately rolled back; otherwise, if the execution is successful and there is some remaining gas, then it is returned to the transaction originator.

A website that keeps track of latest gas price and provides other valuable statistics and calculators is available at `https://ethgasstation.info/index.php`.

Gas

Note: Your Solidity Code compiles to Byte Code. Each Byte Code Instruction has a predetermined Amount of Gas Value required for execution. Run out of Gas and your program stops. Or worse, Write a bad program that:

1) loops endlessly
2) Needlessly allocates huge array structures
3) Thoughtlessly allocates storage
4) Or, instantiates Smart Contracts too often and things will get EXPENSIVE REALLY FAST

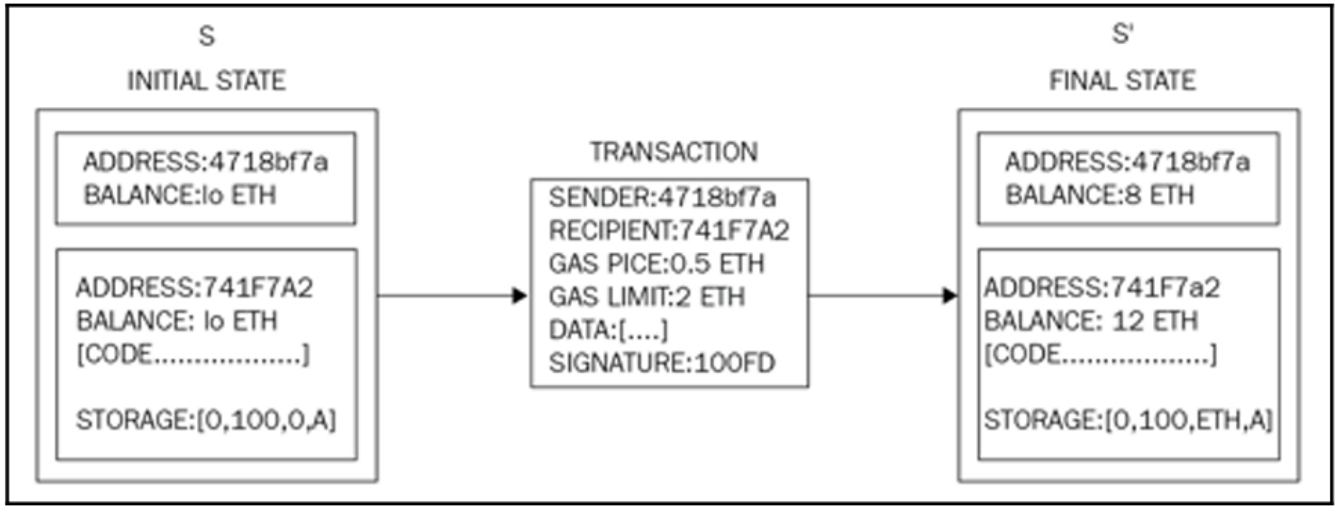
Slater Technologies

Source: Mastering Blockchain by Imran Bashir (Published by Packt.)

Ethereum Blockchain

Ethereum, just like any other blockchain, can be visualized as a transaction-based state machine. This definition is mentioned in the Ethereum yellow paper written by Dr. Gavin Wood.

The core idea is that in Ethereum blockchain, a genesis state is transformed into a final state by executing transactions incrementally. The final transformation is then accepted as the absolute undisputed version of the state. In the following diagram, the Ethereum state transition function is shown, where a transaction execution has resulted in a state transition:



Slater Technologies

Source: Mastering Blockchain by Imran Bashir (Published by Packt.)

Ethereum Blocks and the Ethereum Blockchain

Blocks and blockchain

As discussed earlier in this chapter, blocks are the main building blocks of a blockchain. Ethereum blocks consist of various elements, which are described as follows:

- The block header
- The transactions list
- The list of headers of ommers or uncles

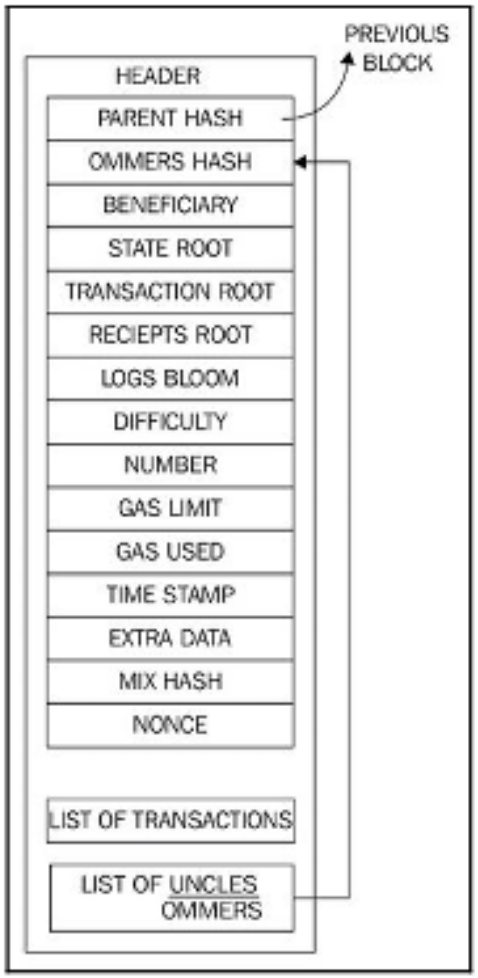
The transaction list is simply a list of all transactions included in the block. Also, the list of headers of uncles is also included in the block.

The most important and complex part of a block in Ethereum is the block header. Block header consists of various elements which are introduced here.

Source: Mastering Blockchain by Imran Bashir (Published by Packt.)

Ethereum Blocks and the Ethereum Blockchain

The following figure shows the detailed structure of the block and block header:



A detailed diagram of block structure with block header

Source: Mastering Blockchain by Imran Bashir (Published by Packt.)

Slater Technologies

Ethereum Blocks and the Ethereum Blockchain

The genesis block

The genesis block varies slightly from normal blocks due to the data it contains and the way it has been created. It contains 15 items that are described here.

From `https://etherscan.io/`, the actual version is shown as follows:

Element	Description
Timestamp	(Jul-30-2015 03:26:13 PM +UTC)
Transactions	8893 transactions and 0 contract internal transactions in this block
Hash	0xd4e56740f876aef8c010b86a40d5f56745a118d0906a34e69aec8c0db1cb8fa3
Parent hash	0x0000000000000000000000000000000000000000000000000000000000000000
SHA3 uncles	0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347
Mined by	0x0000000000000000000000000000000000000000 IN 15 secs
Difficulty	17,179,869,184
Total difficulty	17,179,869,184
Size	540 bytes
Gas used	0
Nonce	0x0000000000000042
Block reward	5 Ether
Uncles reward	0
Extra data	
Gas limit	5,000

Source: Mastering Blockchain by Imran Bashir (Published by Packt.)

Slater Technologies

Bitcoin Blockchain History & Trivia

On January 3rd, 2009 Satoshi Nakamoto unleashed the genesis block into the wild. The genesis block contains the first 50 BTC block reward and cannot be spent by anyone. The bitcoin software was released on Sourceforge the web-based service for open source developers. The original Satoshi client was compiled using Microsoft's visual studio and is written in the programming language C++. Satoshi began building the code in 2007 and was the only developer that made software changes to the bitcoin protocol up until mid-2010.

The first block also includes text from the UK Times newspaper saying "03/Jan/2009 Chancellor on brink of second bailout for banks," a reference to bitcoin's birth-date and possibly mocking fractional reserve banking. With Satoshi's creation, the total number of bitcoins in circulation will never exceed 21 million BTC.

Slater Technologies

Source: https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today/

Bitcoin Blockchain History & Trivia

```
00000000   01 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000010   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000020   00 00 00 00 3B A3 ED FD   7A 7B 12 B2 7A C7 2C 3E   ....;£íýz{.²zÇ,>
00000030   67 76 8F 61 7F C8 1B C3   88 8A 51 32 3A 9F B8 AA   gv.a.È.Ã^ŠQ2:Ÿ¸ª
00000040   4B 1E 5E 4A 29 AB 5F 49   FF FF 00 1D 1D AC 2B 7C   K.^J)«_Iÿÿ...¬+|
00000050   01 01 00 00 00 01 00 00   00 00 00 00 00 00 00 00   ................
00000060   00 00 00 00 00 00 00 00   00 00 00 00 00 00 00 00   ................
00000070   00 00 00 00 00 00 FF FF   FF FF 4D 04 FF FF 00 1D   ......ÿÿÿÿM.ÿÿ..
00000080   01 04 45 54 68 65 20 54   69 6D 65 73 20 30 33 2F   ..EThe Times 03/
00000090   4A 61 6E 2F 32 30 30 39   20 43 68 61 6E 63 65 6C   Jan/2009 Chancel
000000A0   6C 6F 72 20 6F 6E 20 62   72 69 6E 6B 20 6F 66 20   lor on brink of
000000B0   73 65 63 6F 6E 64 20 62   61 69 6C 6F 75 74 20 66   second bailout f
000000C0   6F 72 20 62 61 6E 6B 73   FF FF FF FF 01 00 F2 05   or banksÿÿÿÿ..ò.
000000D0   2A 01 00 00 00 43 41 04   67 8A FD B0 FE 55 48 27   *....CA.gŠý°þUH'
000000E0   19 67 F1 A6 71 30 B7 10   5C D6 A8 28 E0 39 09 A6   .gñ¦q0·.\Ö¨(à9.¦
000000F0   79 62 E0 EA 1F 61 DE B6   49 F6 BC 3F 4C EF 38 C4   ybàê.aÞ¶Iö¼?Lï8Ä
00000100   F3 55 04 E5 1E C1 12 DE   5C 38 4D F7 BA 0B 8D 57   óU.å.Á.Þ\8M÷º..W
00000110   8A 4C 70 2B 6B F1 1D 5F   AC 00 00 00 00            ŠLp+kñ._¬....
```

Raw hex version of the genesis block with bank bailout message. 1/3/09

The genesis block has received 1,073 transactions since its inception, with random people adding over 16 BTC to this unspendable address. No one knows why the genesis block was created to be unspendable, as there is no explanation in the Satoshi source code version 0.1. Additionally, the genesis block was hard-coded, and nearly all altcoins derived from bitcoin have this initial unspendable block reward.

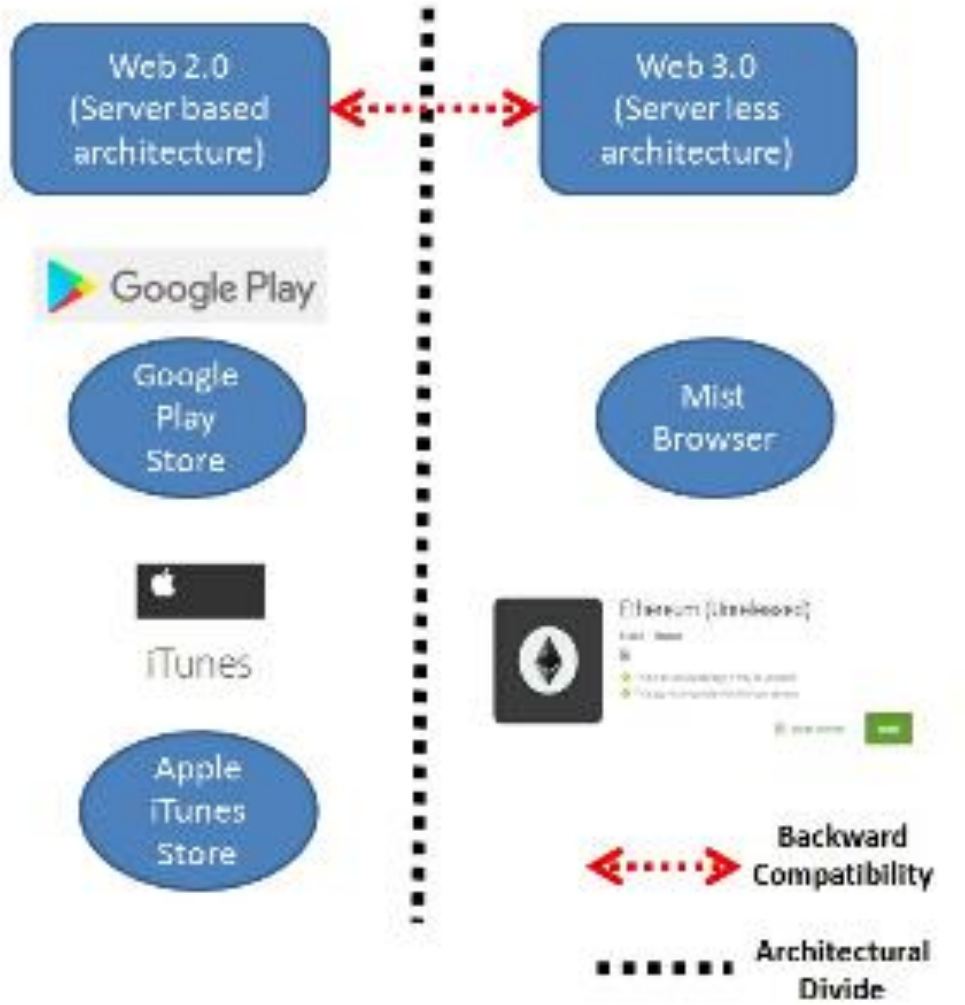
Source: https://news.bitcoin.com/bitcoins-quirky-genesis-block-turns-eight-years-old-today
https://www.investopedia.com/news/what-genesis-block-bitcoin-terms/

Slater Technologies

DAPPS AND
DAPP DEVELOPMENT

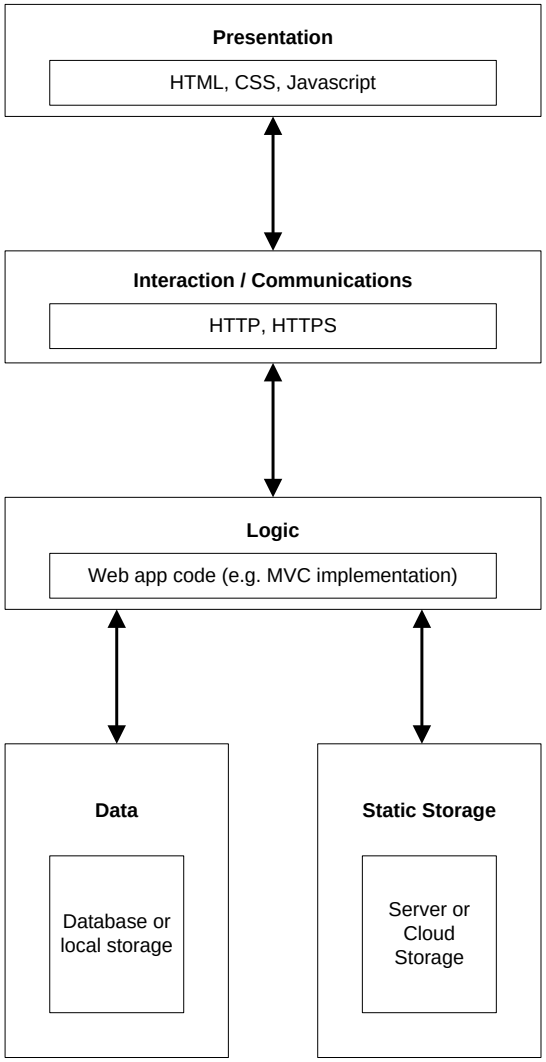
Slater Technologies

Web Apps and DApps

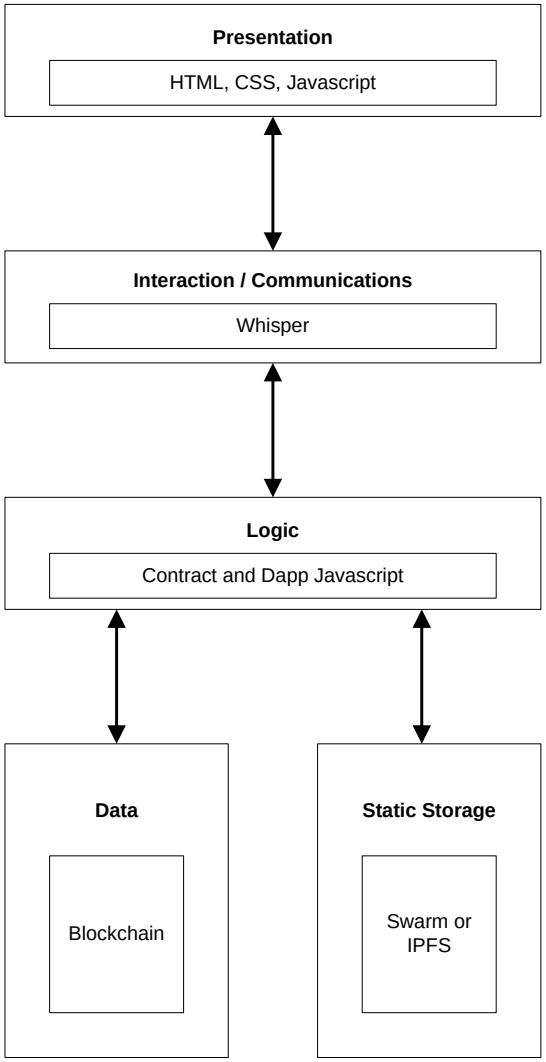


Slater Technologies

Web Application



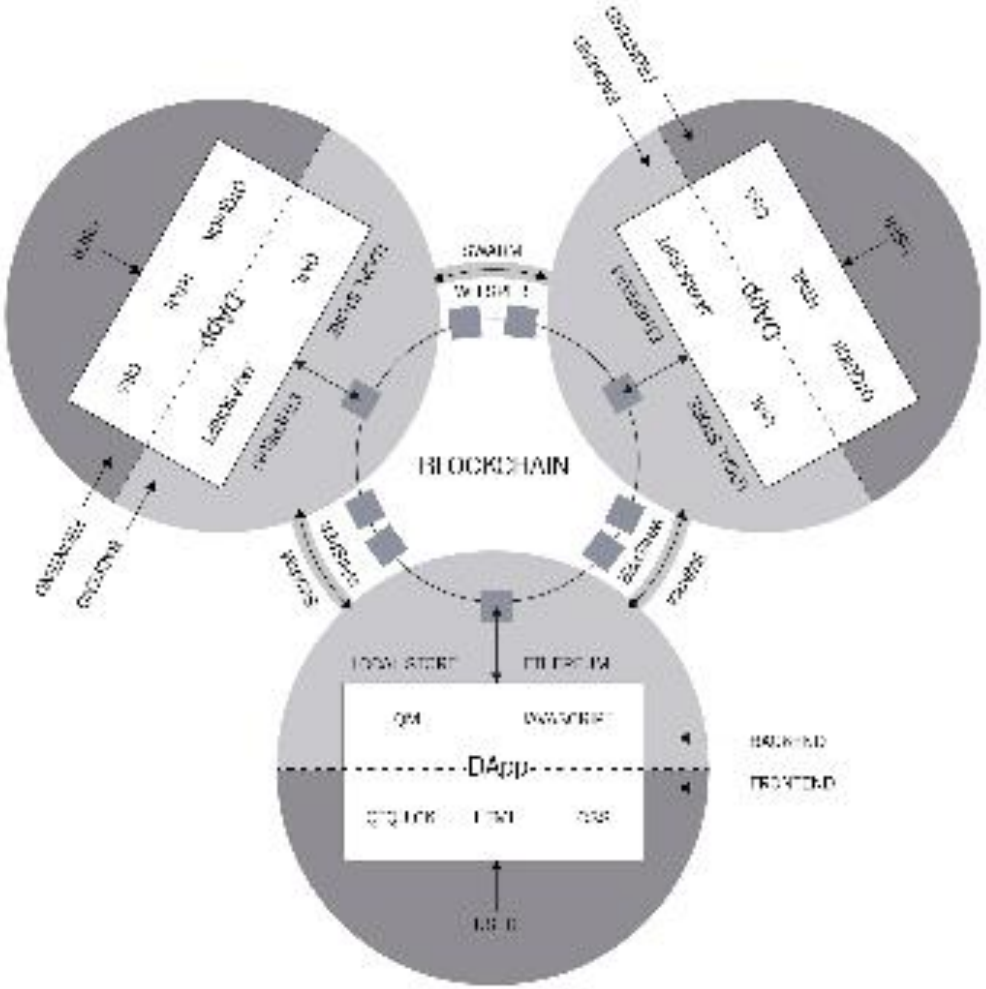
Decentralized Application (Dapp)



Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

Slater Technologies

DApps



Decentralized architecture, Source:

Ethereum stack exchange

Slater Technologies

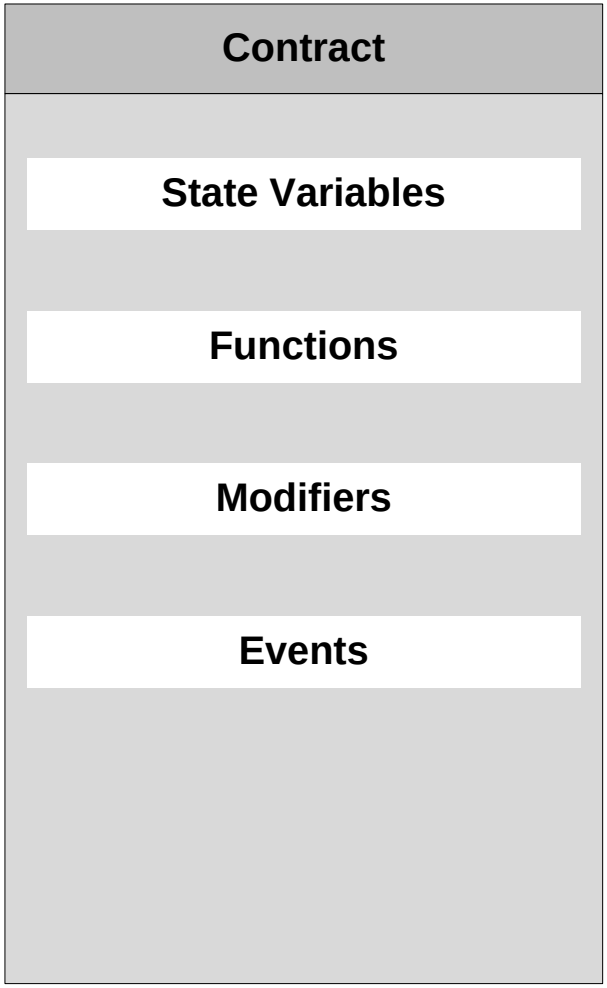
```
contract Sample
{
  //state variables
  uint256 data;
  address owner;

  //event definition
  event logData(uint256 dataToLog);

  //function modifier
  modifier onlyOwner() {
    if (msg.sender != owner) throw;
    _;
  }

  //constructor
  function Sample(uint256 initData, address initOwner){
    data = initData;
    owner = initOwner;
  }
  //functions
  function getData() returns (uint256 returnedData){
    return data;
  }

  function setData(uint256 newData) onlyOwner{
    logData(newData);
    data = newData;
  }
}
```



```
contract Sample
{
  //state variables
  uint256 data;
  address owner;

  //event definition
  event logData(uint256 dataToLog);

  //function modifier
  modifier onlyOwner() {
    if (msg.sender != owner) throw;
    _;
  }

  //constructor
  function Sample(uint256 initData, address initOwner){
    data = initData;
    owner = initOwner;
  }
  //functions
  function getData() returns (uint256 returnedData){
    return data;
  }

  function setData(uint256 newData) onlyOwner{
    logData(newData);
    data = newData;
  }
}
```

Contract Crowdfunding

State Variables

- struct Backer {address addr; uint amount;}
- address public owner;
- uint public backers;
- uint public deadline;
- string public campaignStatus;
- bool ended;
- uint public goal;
- uint public amountRaised;
- mapping (uint => Backer) backers;

Functions

- Crowdfunding(uint_deadline, uint_goal)
- checkGoalReached ()
- fund()
- destroy()

Modifiers

- onlyOwner()

Events

- Deposit (address_from,uint_amount)
- Refund (address_to,uint_amount)

Slater Technologies

Steps to DApp Development

Analysis

Identify the entities involved, their roles and types of interactions between them (e.g. contract owner, users, devices)

Design

Model the entity attributes as state variables and interactions between them as functions. Also capture the dependencies and constraints

Implementation

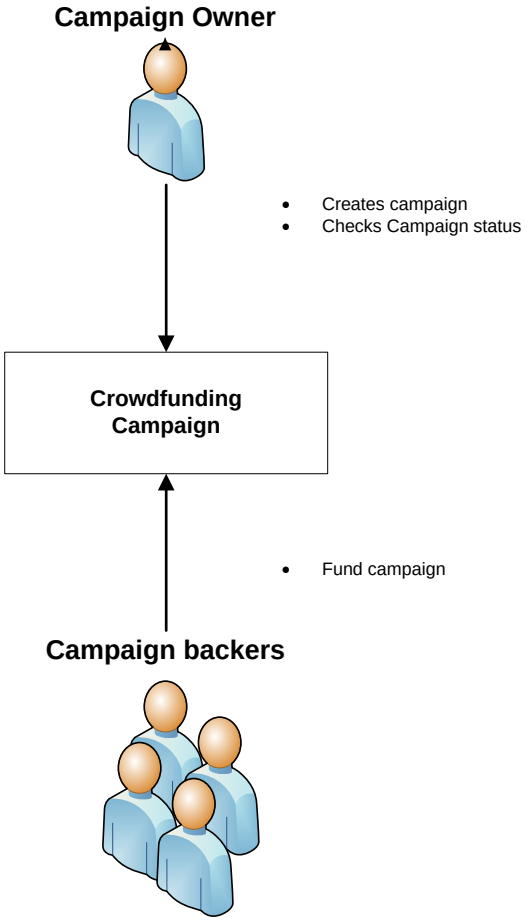
Implement the contracts (including state variables, functions, modifier and events) in a higher-level languages such as Solidity For Dapp, also implement the front-end (HTML and CSS) and backend (Javascript).

Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

Slater Technologies

Analysis Stage

(Example Business Case: Crowdfunding Application)



Slater Technologies

Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

Design Stage

(Example Business Case: Crowdfunding Application)

State Variables

- address public owner;
- uint public backers;
- uint public deadline;
- string public campaignStatus;
- bool ended;
- uint public goal;
- uint public amountRaised;
- struct Backer {address addr; uint amount;}
- mapping (uint => Backer) backers;

Functions

- Crowdfunding(uint_deadline, uint_goal)
- checkGoalReached ()
- fund()

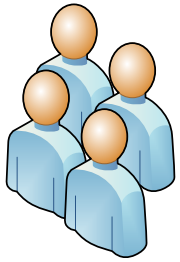
Campaign Owner

- Creates campaign
- Checks Campaign status

Crowdfunding Campaign

- Fund campaign

Campaign backers

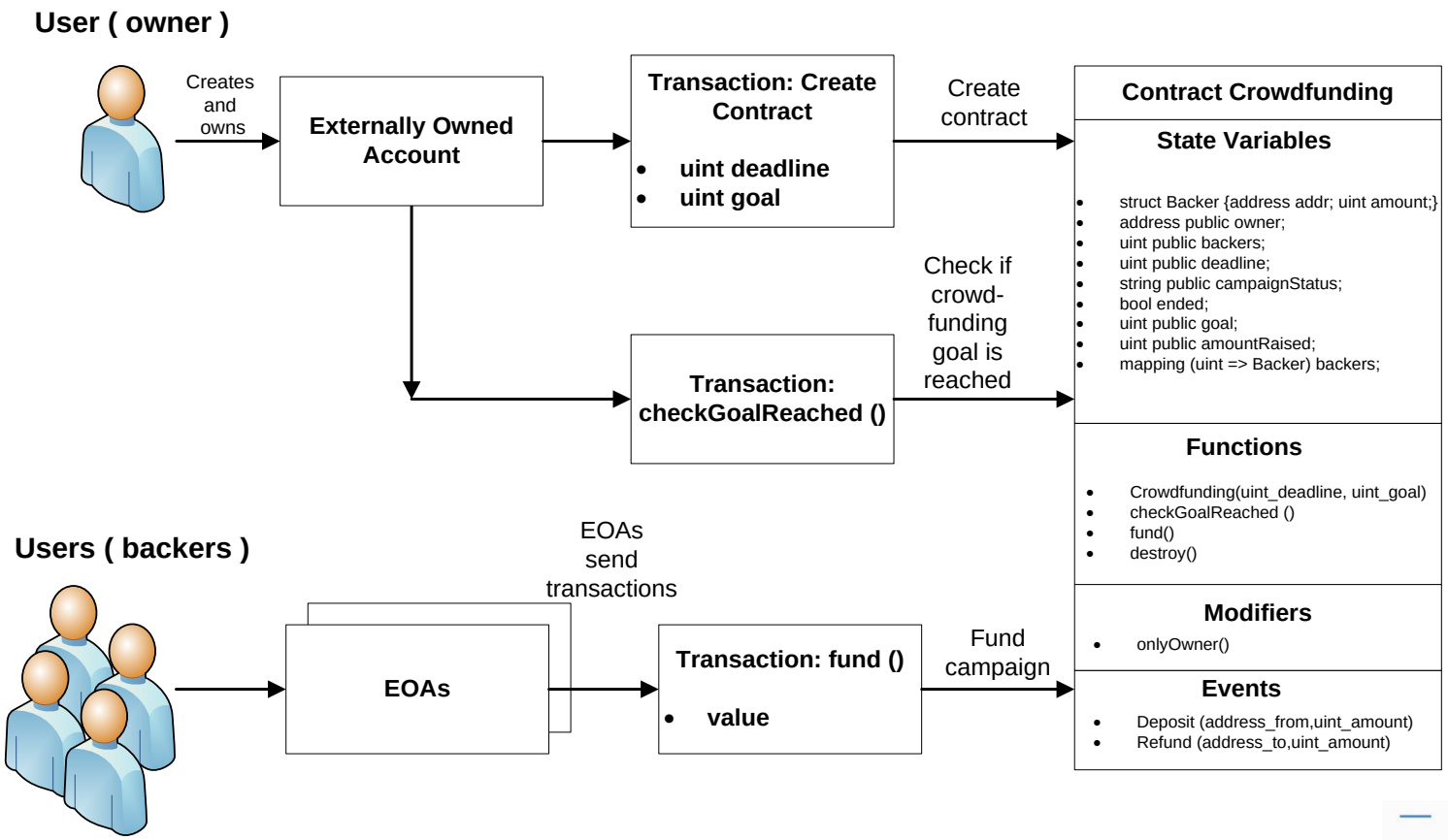


Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

Slater Technologies

Implementation Stage

(Example Business Case: Crowdfunding Application)



Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

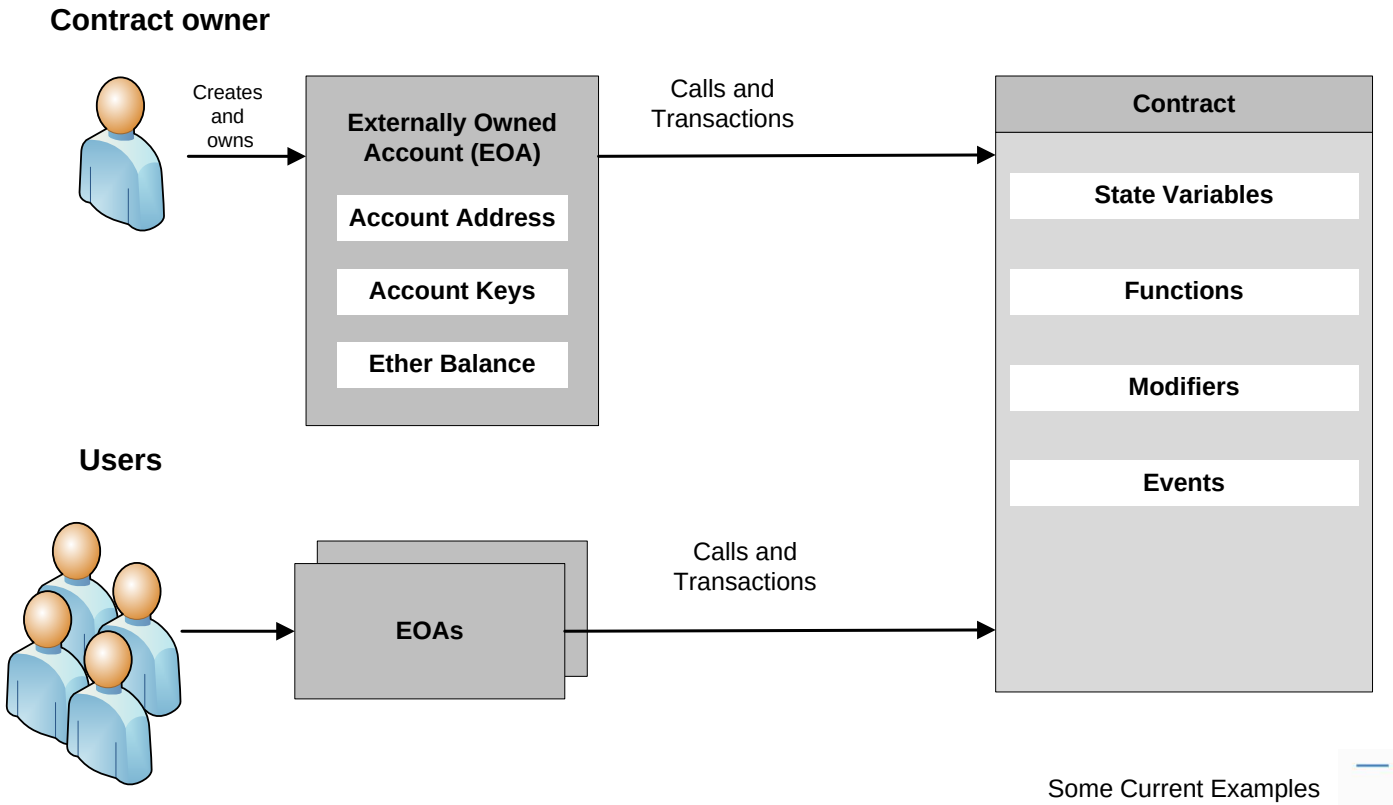
Slater Technologies

BLOCKCHAIN APPLICATION TEMPLATES

Slater Technologies

Blockchain Application Templates

Many-to-One



Some Current Examples

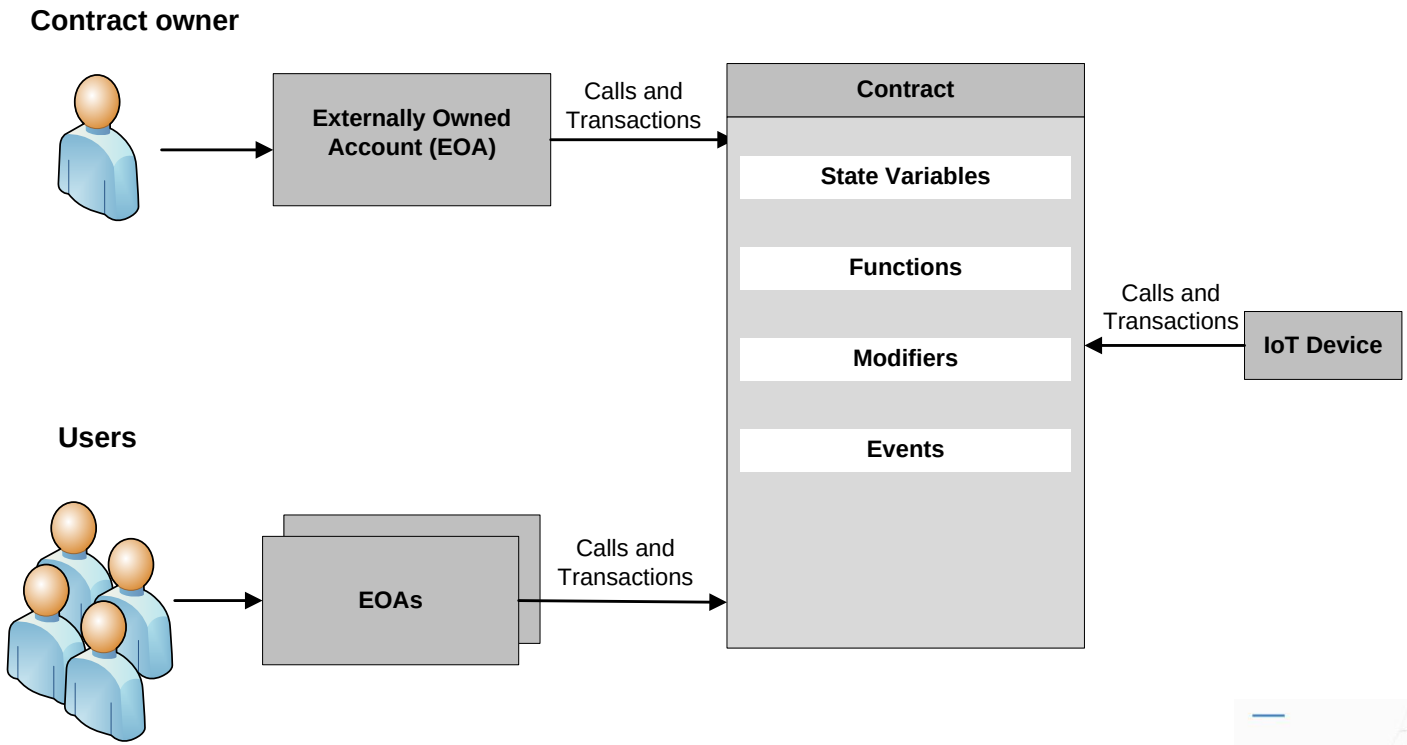
- Crowdfunding
- Event Registration
- Voting
- Name Registration

Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

Slater Technologies

Blockchain Application Templates

Many-to-One for IoT Applications



Some Current Examples

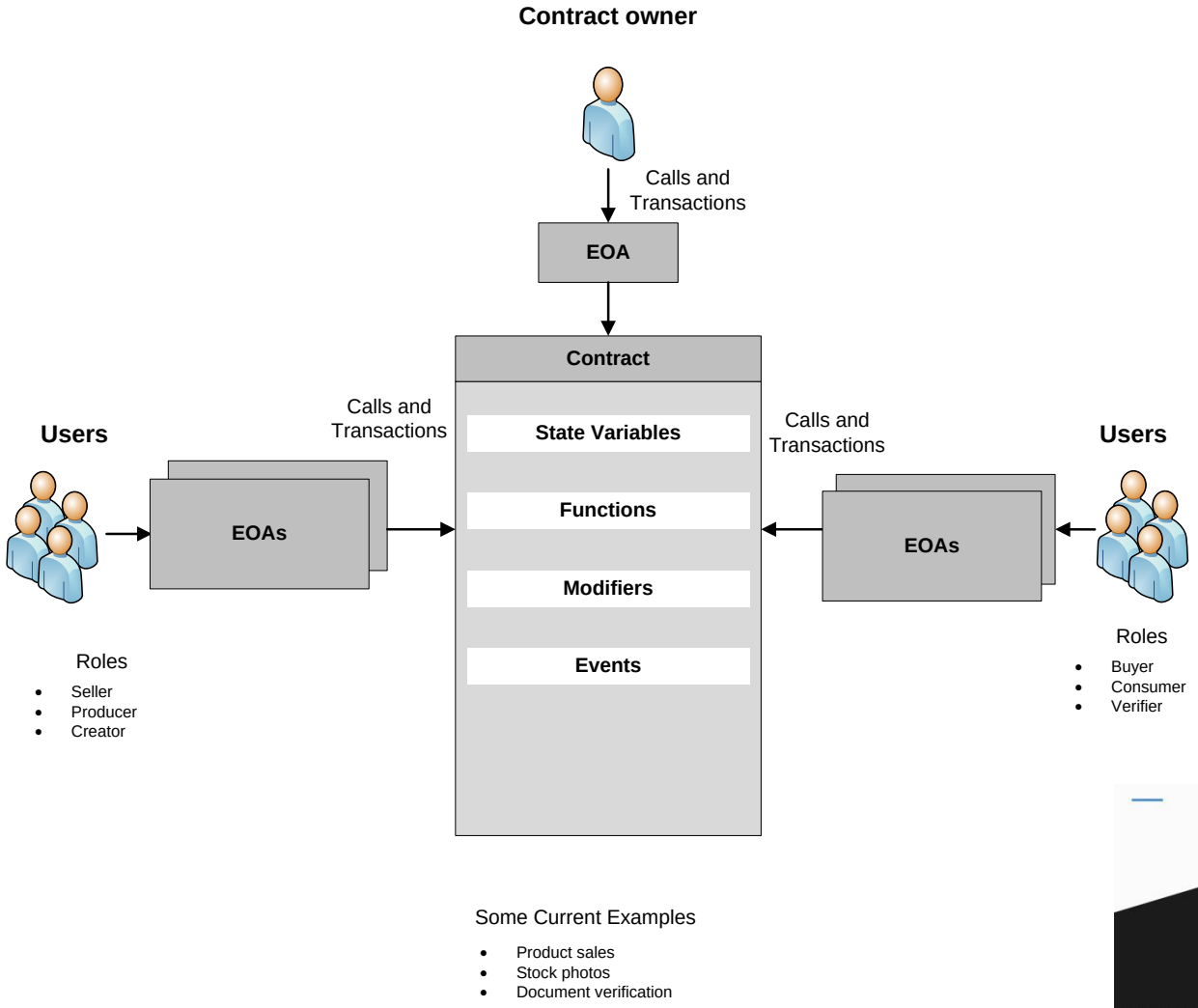
- Solar charging stations
- Smart switch

Slater Technologies

Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

Blockchain Application Templates

Many-to-One for Financial Applications



Some Current Examples

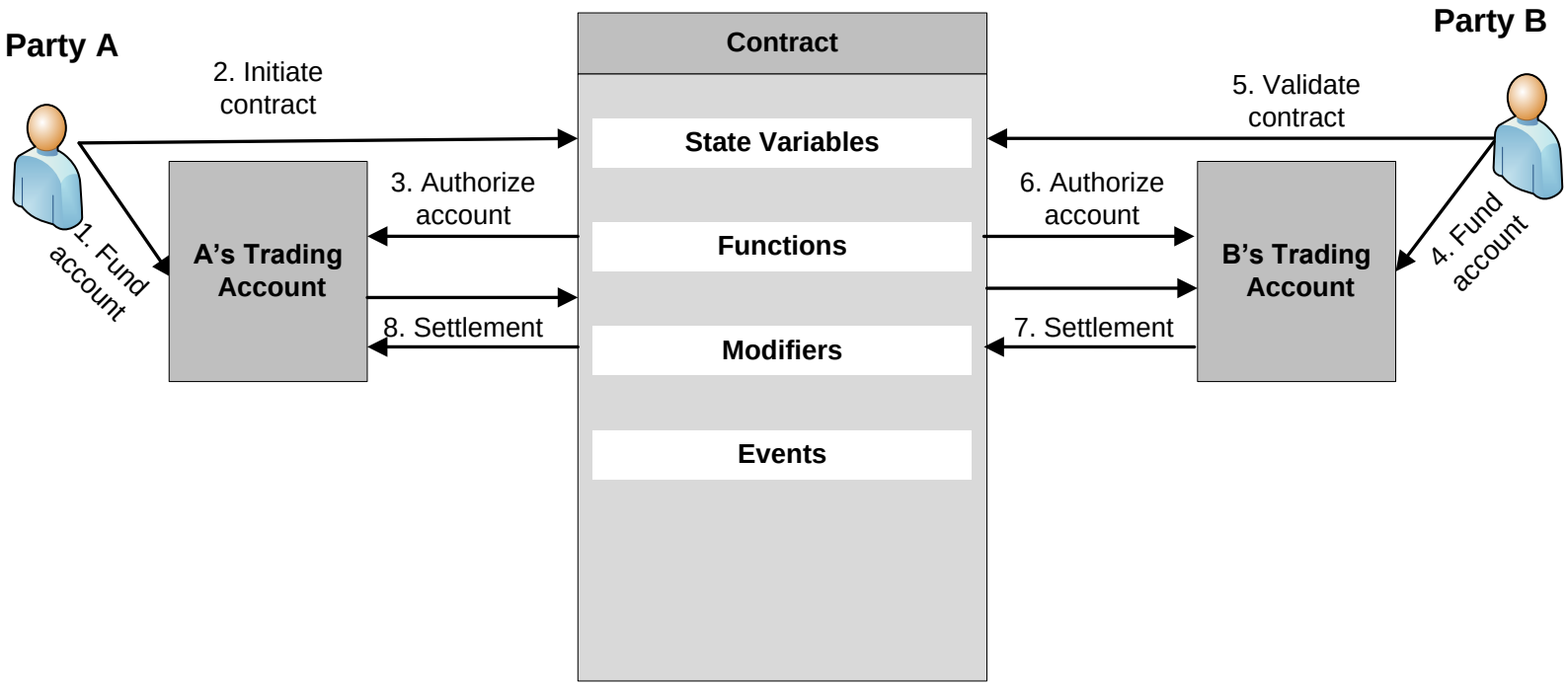
- Product sales
- Stock photos
- Document verification

Slater Technologies

Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

Blockchain Application Templates

Many-to-Many or Peer-to-Peer



Some Current Examples

- Call option
- Interest rate swap

Slater Technologies

Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

DEVELOPMENT TOOLS

Slater Technologies

Development Tools

- Blockchain
  - Geth
  - Parity
  - Ganache
- Frameworks
  - Truffle
  - RiskBlock
- Editors
  - Atom
  - Sublime
  - Notepad
  - Eclipse
  - Your favorite text editor
- Languages
  - Solidity
  - Javascript
  - LLL
  - Viper
  - Mulu
- Testing
  - https://test.eth.guide
- Publicly listed Contracts
  - http://etherchain.org/contracts

Slater Technologies

Preparation

- Installation

You'll need Git, Node Package Manager, MetaMask and Truffle set up.

Click these links and follow directions:
- Git: https://git-scm.com/downloads
- MetaMask: https://chrome.google.com/webstore/detail/metamask/nkbihfbeogaeaoehlefnkodbefgpgknn?hl=en
- Node (choose LTS option): https://nodejs.org/en/
- Truffle: http://truffleframework.com/docs/getting_started/installation
- If you have Windows: http://truffleframework.com/tutorials/how-to-install-truffle-and-testrpc-on-windows-for-blockchain-development

Slater Technologies

Preparation

- Reading Material

Reading Material
Bitcoin Whitepaper: https://bitcoin.org/bitcoin.pdf
Ethereum Whitepaper: https://github.com/ethereum/wiki/wiki/White-Paper
Prehistory of Ethereum protocol by Vitalik: https://vitalik.ca/general/2017/09/14/prehistory.html
Just Enough Bitcoin for Ethereum: https://media.consensys.net/time-sure-does-fly-ed4518792679
Ethereum - Bitcoin Plus Everything: https://medium.com/@ConsenSys/ethereum-bitcoin-plus-everything-a506dc780106
Byzantine Fault Tolerance primer: https://www.nasdaq.com/article/byzantine-fault-tolerance-the-key-for-blockchains-cm810058
Mechanism Design & Cryptoeconomics primer: https://medium.com/blockchannel/a-crash-course-in-mechanism-design-for-cryptoeconomic-applications-a9f06ab6a976

Slater Technologies

Solidity Preparation

- Create an Ethereum UserID and Wallet
- Install Blockchain software (geth, partity, or ganache)
  - Geth https://geth.ethereum.org/downloads/
  - Parity http://parity.io
  - Ganache https://github.com/trufflesuite/ganache
- Install Node.js and NPM (NPM is installed with node.js) https://nodejs.org/en
- Install Web3.js (gets automatically installed with parity) otherwise: https://github.com/ethereum/web3.js/
- Install Mist blockchain explorer https://github.com/ethereum/mist
- Install Metamask https://metamask.io/
- Remix Solidity IDE Editor & Compiler
  - http://remix.ethereum.org/#optimize=true&version=soljson-v0.4.24
- Kovan (Rinkeby) Blockchain
  - https://www.rinkeby.io/#stats
- Install the Solidity Complier https://github.com/ethereum/solidity
  - http://solidity.readthedocs.io/en/latest/installing-solidity.html
- Install an editor (preferably Atom, but Eclipse or sublime or another is OK)

Slater Technologies

CASE STUDIES

Slater Technologies

Case Study 1

- Timeframe: Summer of 2018
- Location: Chicago
- Topic: Teaching Interns who are Technical People with Graduate degrees free Blockchain classes
- 33 started, 8 remain
- First Project: We are converting and existing Time Tracking GUI Applictaion to an Ethereum DApp
- Second Project: Designing and Implementing a DApp Solution from Scratch
- We are working together from June 1 – December 31

Slater Technologies

Case Study 2

- Timeframe: November 2017
- Location: Chicago
- Topic: Placement in Production of flawed Smart Contract
- Results: Loss of over $150 million

Slater Technologies

$150,000,000 bug

9 ■■■■ js/src/contracts/snippets/enhanced-wallet.sol — Show comments — View

```
@ -104,7 +104,7 @@ contract WalletLibrary is WalletEvents {
104
105   // constructor is given number of sigs required to do protected "onlymanyowners" transactions
106   // as well as the selection of addresses capable of confirming them.
107 -   function initMultiowned(address[] _owners, uint _required) {
107 +   function initMultiowned(address[] _owners, uint _required) internal {
108     m_numOwners = _owners.length + 1;
109     m_owners[1] = uint(msg.sender);
110     m_ownerIndex[uint(msg.sender)] = 1;
@ -198,7 +198,7 @@ contract WalletLibrary is WalletEvents {
198   }
199
200   // constructor - stores initial daily limit and records the present day's index.
201 -   function initDaylimit(uint _limit) {
201 +   function initDaylimit(uint _limit) internal {
202     m_dailyLimit = _limit;
203     m_lastDay = today();
204   }
@ -211,9 +211,12 @@ contract WalletLibrary is WalletEvents {
211     m_spentToday = 0;
212   }
213
214 + // throw unless the contract is not yet initialized.
215 + modifier only_uninitialized { if (m_numOwners > 0) throw; _; }
```

Slater Technologies

The Challenges

- Huge Learning Curve
- DApps with Web3 and the EVM are not your Father's Web Developer Workbench
- You can really screw this up – easily
- Learning Egoless Programming
- Turnover – Once people get training and experience the may leave

Slater Technologies

Solving the Challenges and Winning

- Find and utilize quality resources to accelerate your learning curve and immersion into the Blockchain World
- Establish a Blockchain Expert or Champion imbued with the responsibility to be the Blockchain Evangelist
- Build strong Learning Teams – Use Peter Senge's Learning Team Disciplines
  - Shared Vision
  - Personal Mastery
  - Mental Modeling
  - Team Learning
  - Systems Thinking
- Stay abreast of Blockchain Technologies and Blockchain Politics and Blockchain Evolution
- Join and participate in Local Blockchain Meetups
- Go International - Get involved with the Internet Society and the Blockchain Special Interest Group - Both are free and the Blockchain SIG has great projects and leadership
  - www.internetsociety.com
  - https://www.isoc-bsig.org/
  - https://www.linkedin.com/company/isoc-blockchain-sig/

Slater Technologies

Roadmap to "Blockchain" Your IT Organization: How to Help Your IT Staff Go from Square One to Competence & Dominance in Blockchain Technologies

Orientation

Start → Learn the Terminology and Concepts. → Perform a Baseline Skills Inventory and Assessment → Blockchain Introduction and Orientation → Review Real-World Use Cases and Applications → Read Papers & Join Blockchain Meetup Groups, and other Blockchain-related Organizations like www.isoc-bsig.org

Preparation

Analyze your initial Blockchain Needs and Requirements → Baseline your Capabilities → Perform Gap Analysis of Needs versus Capabilities → Remediate Skills Gap with Consultants, Training, and/or Mentoring → Perform Detailed Requirements Analysis → Create a Blockchain Solution Design Based on the Detailed Analysis

Crawl

Select the Type of Blockchain → Prepare and Validate the Blockchain DApp Development Environment → Implement a Prototype a Proof of Concept DApp solution → Validate the DApp Prototype → Add Additional Features to the DApp Prototype → Test, Validate, and Publish Results

Walk

Perform Detailed Requirements Analysis → Identify the Appropriate Blockchain Solutions Template → Create a Blockchain Solution Design Based on the Detailed Analysis and the Appropriate DApp Template → Create an Implementation Diagram for the Blockchain Dapp Solution based on the Design → Implement the Blockchain DApp Solution based on the Implementation Diagram → Test and Optimize the DApp for Optimal Performance, and Validate against Requirements

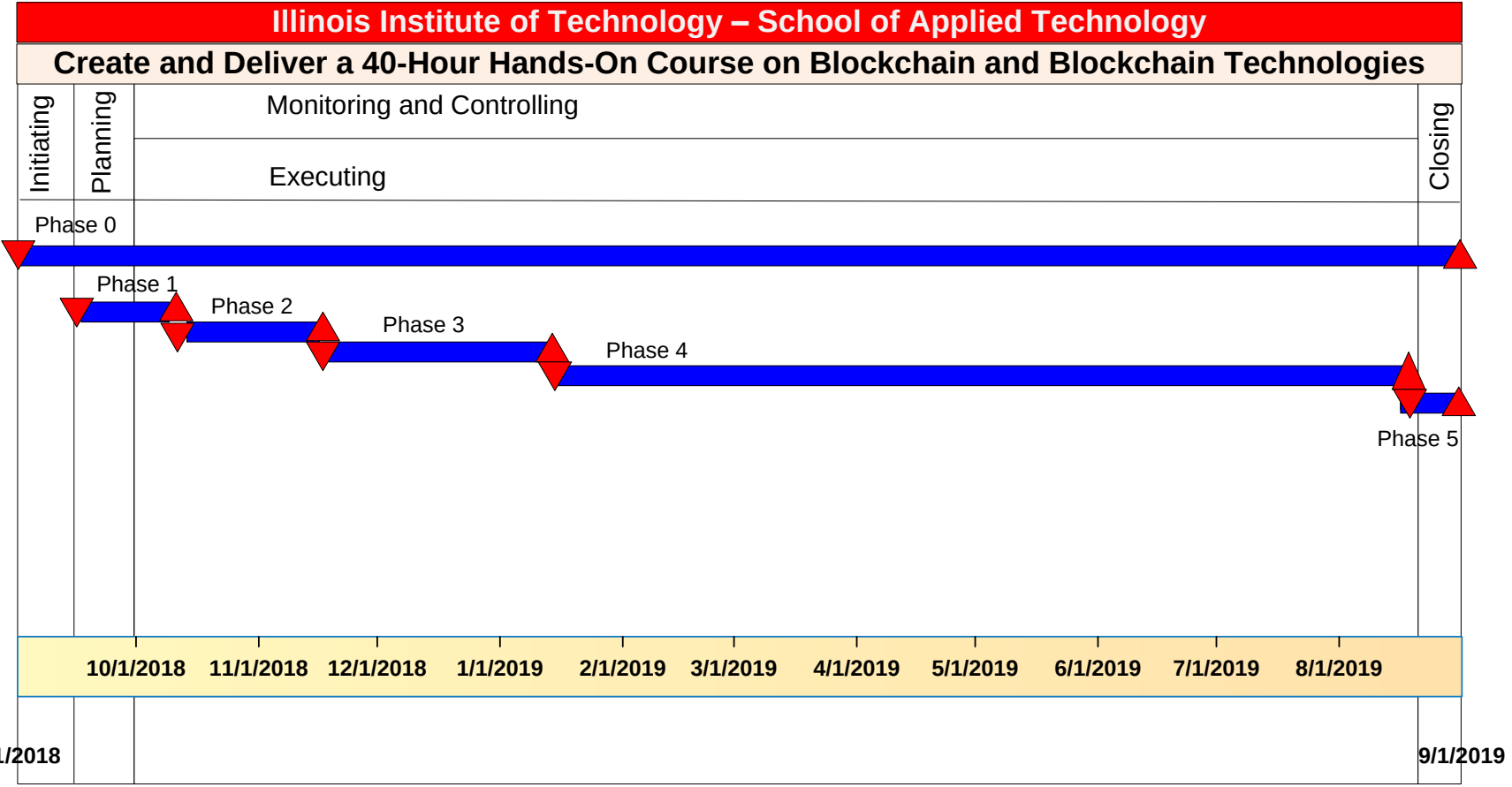
Run

Review Lessons Learned from Previous Tracks or DApps → Focus on Implementing Techniques to Optimize the Analysis, Design, Testing and Implementation → Incorporate the use of Agile/Scrum and DevOps in the Blockchain Solution Development Lifecycle → Perform Analysis, Design Testing and Implementation based on Previous Experience and Lessons Learned → Test and Optimize the DApp for Optimal Performance, and Validate against Requirements & **Publish Results** → Continue Continuosly

Illinois Institute of Technology – School of Applied Technology

Create and Deliver a 40-Hour Hands-On Course on Blockchain and Blockchain Technologies

The High-Level Project Plan

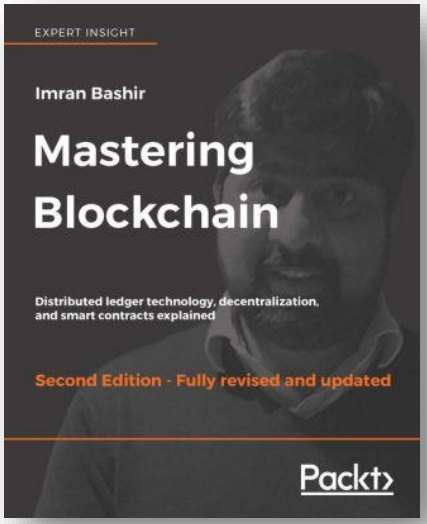


Legend	
Phase 0	Project Initiation, Planning, and Management
Phase 1	Analysis – Determine all topical areas to be covered
Phase 2	Design – Modules, Lectures, Exercises
Phase 3	Implementation – Create the Modules, Lectures, Exercises for the One Third Content Delivery on January 31, 2019
Phase 4	Implementation – Create the Modules, Lectures, Exercises for the Remaining Two Thirds Content Delivery on September 1, 2019
Phase 5	Pilot Delivery

SOME VALUABLE RESOURCES

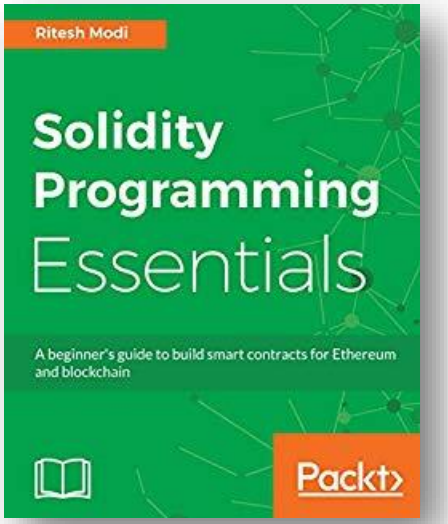
Slater Technologies

Sample Code Resources



Mastering Blockchain, Second Edition
by Imran Bashir

Ethereum Smart Contract Development
by Mayukh Mukhopadhyay

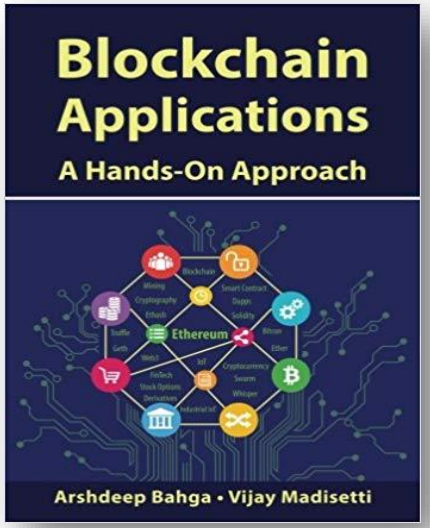


Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain
by Ritesh Modi

Slater Technologies

Sample Code Resources

Building Blockchain Projects: Building Decentralized Blockchain Applications with Ethereum and Solidity
By Narayan Prusty



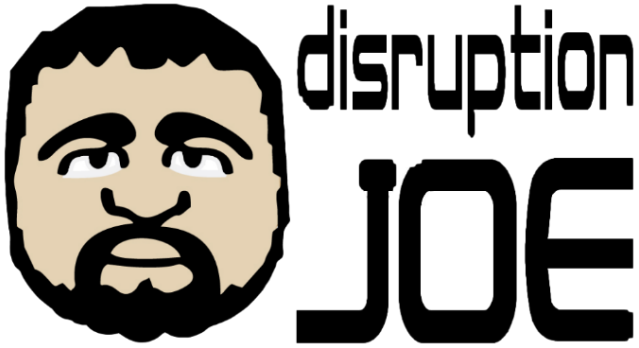
Blockchain Applications: A Hands-On Approach
by Arshdeep Bahga and Vijay Madisetti

Ethereum, Tokens & Smart Contracts: Notes on getting started
by Eugenio Noyola

Conclusion

- We covered:
  - Introduction and Where Are We Right Now?
  - The Problem
  - The DApp Environment
  - The Solutions
  - Case Studies
  - The Challenges
  - Solving the Challenges and Winning
  - The Roadmap
  - Some Valuable Resources

Special Thanks To
Chicago's Best Blockchain Buddies:



Joe Hernandez
Co-Founder of the
Chicago Blockchain Project

Hannah Rosenburg
Co-Founder of the
Chicago Bitcoin and Open
Blockchain Meetup

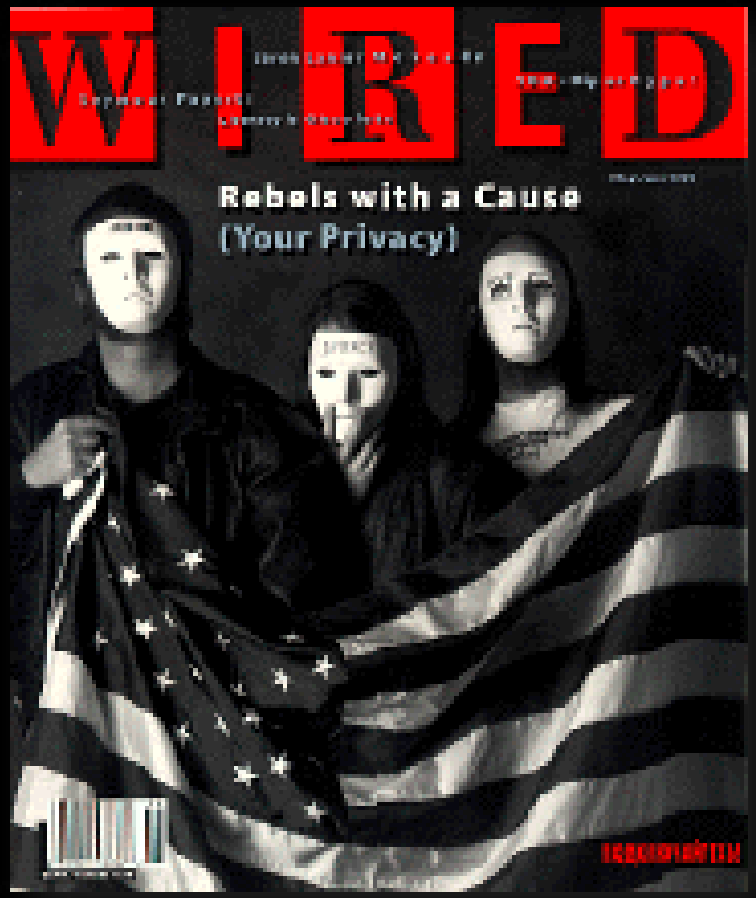
Slater Technologies

Special Thanks To:

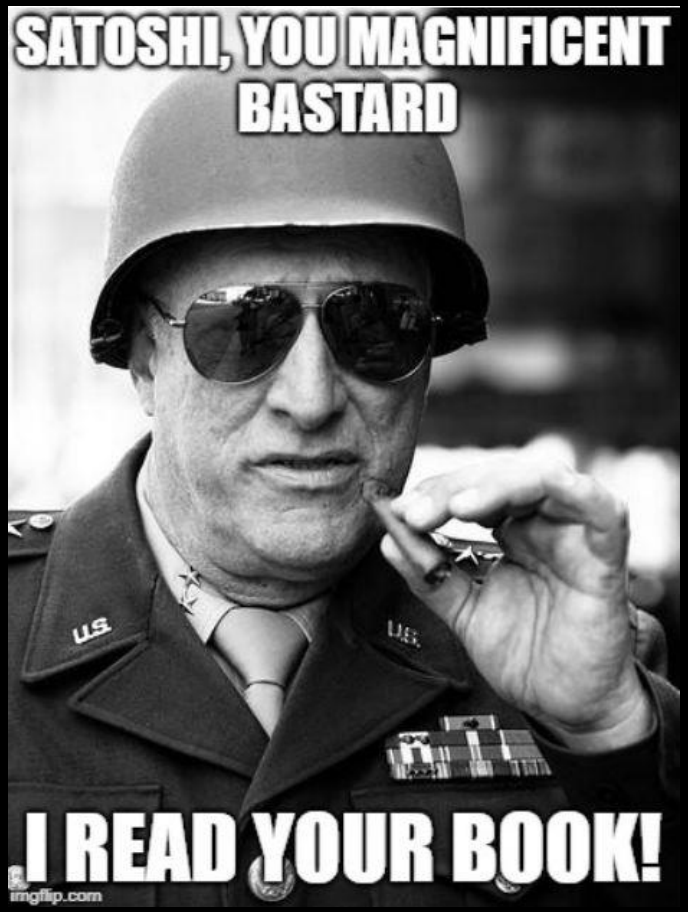
Vitalik Buterin
Inventor of Ethereum

Slater Technologies

Questions?



Crypto Rebels Revealed
Wired Magazine, February 1993



General George S. Patton

Slater Technologies

PARTING THOUGHTS

Slater Technologies

"Our deepest fear is not that we think we are inadequate. Our deepest fear is that we are powerful beyond measure. It is our light, not our darkness, that most frightens us. We ask ourselves, who am I to be brilliant, gorgeous, talented and fabulous? Actually who are you not to be? You are a child of God. Your playing small doesn't serve the world. There is nothing enlightened about shrinking so that other people won't feel insecure around you."

Nelson Mandela
South African Leader
Author – *Long Walk to Freedom*
Nobel Peace Prize Laureate
nmandela@anc.org.za

1998 - Nelson Mandela shows Bill Clinton his jail cell where he was imprisoned for 18 years because of his stance on Aparteid issues

ATTENTION

There are three types of people in the World:

People who
Make Things
Happen

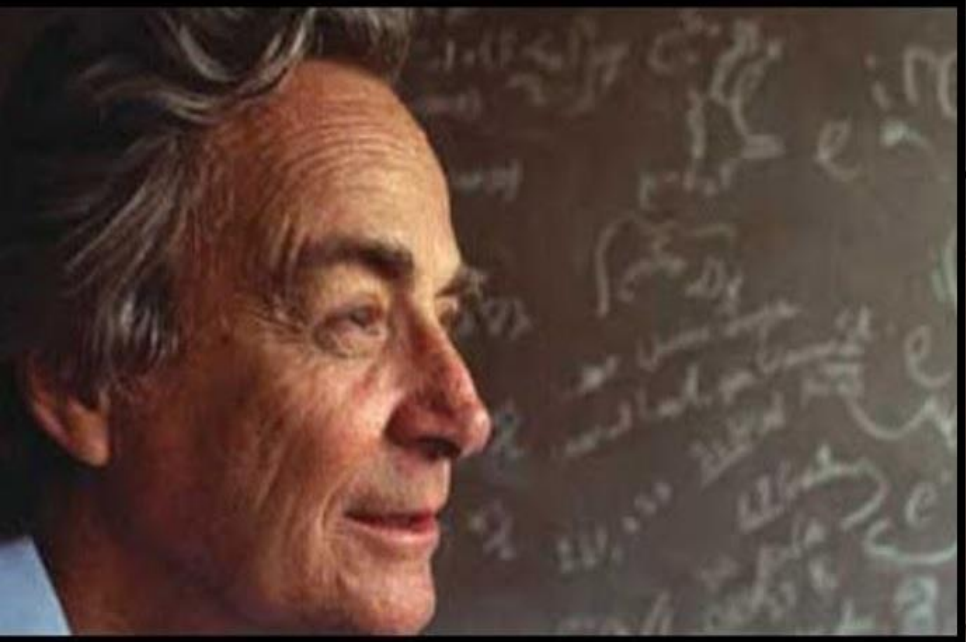
People who
Watch Things
Happen

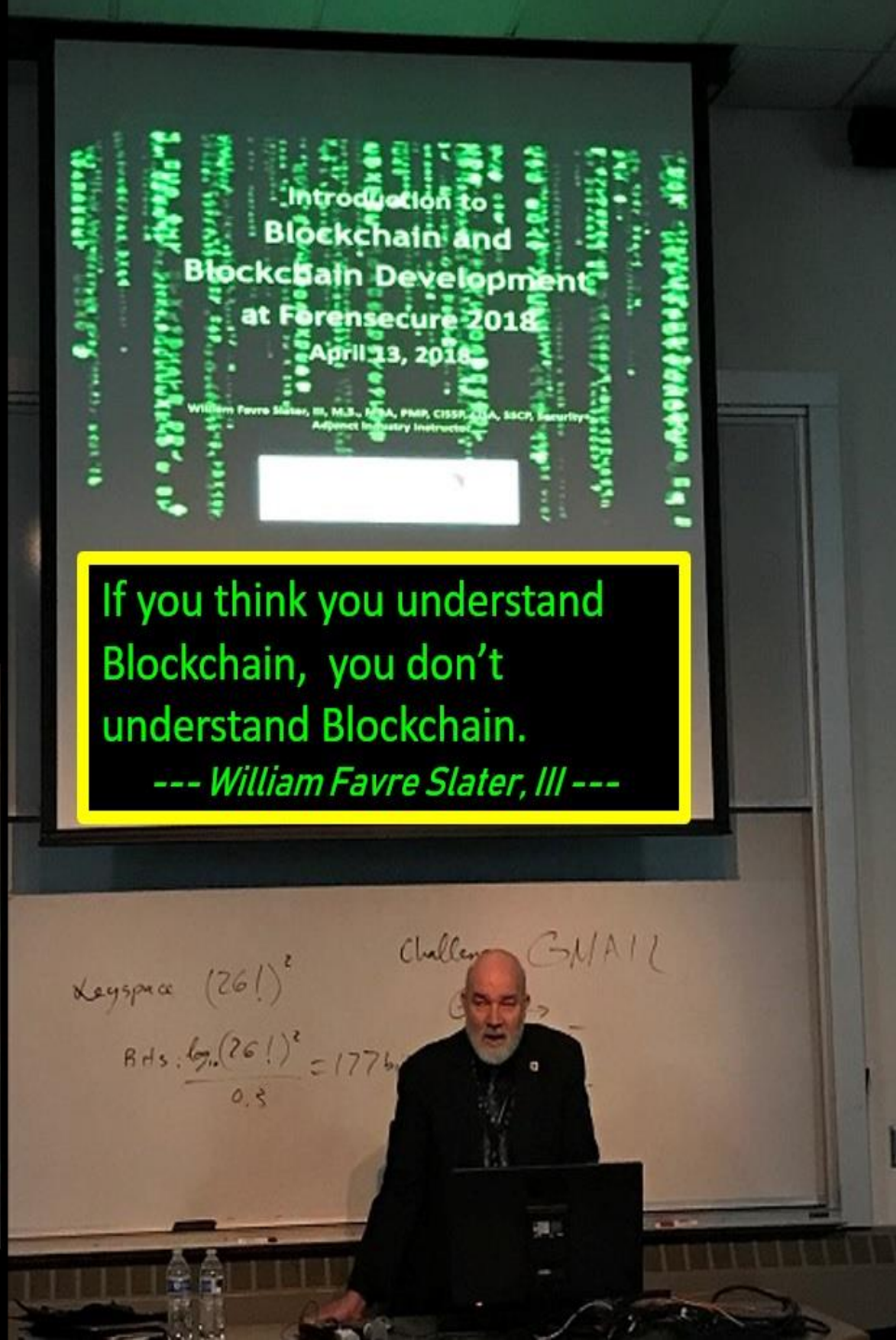
People who say,
"What Happened?"

Andreas Vollenweider
Milwaukee, Wisconsin
October 1998
Photo by John Owrey

If you think you understand quantum mechanics, you don't understand quantum mechanics.

— Richard P. Feynman —





If you think education is expensive, consider the cost of ignorance.

REFERENCES

Slater Technologies

References:
Best Blockchain Texts

- **Blockchain Basics: A Non-technical Introduction in 25 Steps**
  - **by Daniel Drescher**
- **Building Blockchain Projects: Building Decentralized Blockchain Applications with Ethereum and Solidity**
  - **By Narayan Prusty**
- **Ethereum, Tokens & Smart Contracts: Notes on getting started**
  - **by Eugenio Noyola**
- **Blockchain Applications: A Hands-On Approach**
  - **by Arshdeep Bahga and Vijay Madisetti**
- **Ethereum Smart Contract Development**
  - **by Mayukh Mukhopadhyay**
- **Solidity Programming Essentials: A beginner's guide to build smart contracts for Ethereum and blockchain**
  - **by Ritesh Modi**
- **Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners**
  - **By Chris Dannen**
- **Mastering Blockchain - Second Edition**
  - **by Imran Bashir**

Slater Technologies

References:
Best Blockchain Texts

- **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You**
  - **by Vikram Dhillon, David Metcalf, Max Hooper**
- **Distributed Ledger Technology: The Science of the Blockchain**
  - **by Roger Wattenhofer**
- **The Book of Satoshi: The Collected Writings od Bitcoin Creator Satoshi Nakamoto**
  - **By Phil Champagne**

Slater Technologies

References

- Antonopoulos, A. M. (2018). Mastering Bitcoin: Programming the Open Blockchain, second edition. Sebastopol, CA: O'Reilly Media, Inc.
- Back, A. (2017). Exploring Ethereum with Raspberry Pi - Part 1: Getting Started. Retrieved from https://www.rs-online.com/designspark/exploring-ethereum-with-raspberry-pi-part-1-getting-started on March 1, 2018.
- Back, A. (2017). Exploring Ethereum with Raspberry Pi Part 2: Creating a Private Blockchain. Retrieved from https://www.rs-online.com/designspark/exploring-ethereum-with-raspberry-pi-part-2-creating-a-private-blockchain on March 1, 2018.
- Bahga, A. and Madisetti, V. (2017). Blockchain Applications: A Hands-On Approach. Published by Arshdeep Bahga and Vijay Madisetti. www.blockchain-book.com .
- Bambara, J. J. and Allen P. R. (2018). Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions. New York, NY: McGraw-Hill Education.
- Bashir, I. (2018). Mastering Blockchain, second edition. Birmingham, UK: Packt Publishing Ltd.
- Bitcoin. (2014). Bitcoin. Retrieved from https://bitcoin.com/ on April 10, 2014.
- Buterin, V. (2015). The Problem of Censorship. Retrieved from http://blog.ethereum.org/2015/06/06/the-problem-of-censorship/ on April 15, 2018.
- Buterin, V. (2015). Visions - Part 1: The Value of Blockchain Technology
- Buterin, V. (2015). Visions - Part 2: The Problem of Trust
- Buterin, V. (2015). Light Clients – Proof of Stake.
- Buterin, V. (2015). SuperRationality DAOs.

Slater Technologies

References

- Casey, M. J. and Vigna, P. (2018). The Truth Machine: The Blockchain Reference and the Future of Everything. New York, NY: St. Martin's Press.
- Champagne, P. (2014). The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto. Published by E53 Publishing, LLC.
- Dannen, C. (2017). Introducing Ethereum and Solidity: Foundations of Crytocurrency and Blockchain Programming for Beginners. New York, NY: Apress
- De Filippi, P. and Wright, A. (2018). Blockchain and the Law: the Rule of Code. Cambridge, MA: President and Fellows of Harvard College.
- Dhillon, V., Metcalf, D., and Hooper, M. (2017). Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Nake It Work for You. New York, NY: Apress.
- Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.
- Eddison, L. (2017). Ethereum: A Deep Dive into Ethereum. Published by Leonard Eddison.
- Ethereum Community. (2017). Ethereum Homestead Documentation 0.1, March 1, 2017. Retrieved from https://media.readthedocs.org/pdf/ethereum-homestead/latest/ethereum-homestead.pdf on March 20, 2018.
- Ethereum Ecosystem Contributors. (2018). Various articles and resources. Retrieved from http://ecosystem.eth.guide on April 15, 2018.
- Etwaru, R. (2017). Blockchain Trust Companies. Indianapolis, IN: Dog Ear Publishing.

Slater Technologies

References

- Gerard, D. (2107), Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum, and Smart Contracts. Published by David Gerard. www.davidgerard.co.uk/blockchain .
- Holton, J. and Fratangelo, T. (2016). Raspberry Pi Architecture. Retrieved from https://www.macs.hw.ac.uk/~hwloidl/Courses/F28HS/slides_RPi_arch.pdf on April 15, 2018.
- Laurence, T. (2017). Blockchain for Dummies. Hoboken, NJ: John Wiley & Sons, Inc.
- Lee, T. B. (2013). 12 questions about Bitcoin you were too embarrassed to ask. Retrieved from http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/19/12-questions-you-were-too-embarrassed-to-ask-about-bitcoin/ on November 19, 2013.
- Nakamoto. S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf on November 1, 2013.
- Noyola, E. (2018). Ethereum: Ethereum, Tokens and Smart Contracts. Published by Eugenio Noyola.
- Peterson, O. (2018). An Introduction of Programmable Smart Contracts in Ethereum (Pt 1). Retrieved from https://www.linkedin.com/pulse/introduction-programmable-smart-contracts-ethereum-p1-%CE%BE%CE%BE%CE%BE-oliver/ on February 1, 2018.
- Prusty, N. (2017). Building Blockchain Projects: Building Decentralized Blockchain Applications with Ethereum and Solidity. Birmingham, UK: Pact Publishing.
- SCGNEWS. (2014). The IRS Just Declared War on Bitcoin - Retroactively. Retrieved from http://scgnews.com/the-irs-just-declared-war-on-bitcoin-retroactively on March 27, 2014.

Slater Technologies

References

- Slater, W. F. (2018). An Introduction to Blockchain and Blockchain Development. A presentation delivered on April 13, 2018 at Forensecure 2018, at the Illinois Institute of Technology. Retrieved August 21, 2018 from http://billslater.com/forensecure/blockchain_2018_slater.pdf.
- Slater, W. F. (2018). Introduction to Setting Up Ethereum on a Small Raspberry Pi Network. A presentation delivered on April 21, 2018 at Chicago Blockckahin Meetup at Haymarket Pub in Chicago, IL. Retrieved August 21, 2018 from http://www.billslater.com/blockchain/Ethereum_on_Raspberry_Pi_by_Wm_F_Slater_III_v_01.0.pdf.
- Slater, W F. (2014). Bitcoin: A Current Look at the World's Most Popular, Enigmatic and Controversial Digital Cryptocurrency. A presentation delivered on April 10, 2014 at Forensecure 2014, at the Illinois Institute of Technology. Retrieved August 21, 2018 from http://www.billslater.com/bitcoin/Bitcoin_and_Cryptocurrency_by_W_F_Slater_for_Forensecure_2014_v02.11_.pdf.
- White, A. (2018). Blockchain: Discover the Technology Behind Smart Contracts, Wallets, Mining, and Cryptocurrency. Published by Andrew K. White.

Slater Technologies

Dedication

- Dedicated with never-ending love, respect, and gratitude to my dear Father-in-law and Mother-in-Law, Wiesiek Roguski (http://billslater.com/wiesiek) and Wiesia Roguska (http://billslater.com/wiesia).

Slater Technologies

Presenter Bio:
William Favre Slater, III

- **Lives in Chicago; Cybersecurity professional by day, Professor at night**
- **Married to my Best Friend and Soul Mate, Ms. Joanna Roguska**
- **Current Position – Project Manager / Sr. IT Consultant at Slater Technologies, Inc.** Working on projects related to
  - Security reviews and auditing
  - Blockchain consulting
  - ISO 27001 Project Implementations
  - Subject Matter Expert for preparing Risk Management and Security Exams at Western Governor's State University in UT
  - Providing subject matter expert services to Data Center product vendors and other local businesses.
  - Designing and creating a database application that streamlines program management, security management, risk management and reporting activities, for management of teams of IT workers and developers in teleworking environments. It will first be a Windows application and then be ported to the web.
  - Developing and presenting technical training materials for undergraduate and graduate students at the Illinois Institute of Technology in the areas of Blockchain and Blockchain development, Data Center Operations, Data Center Architecture, Cybersecurity Management, and Information Technology hardware and software.
  - Created an eBook with articles about Security, Risk Management, Cyberwarfare, Project Management and Data Center Operations
  - Professor at Illinois Tech for 10 years

Slater Technologies

William Favre Slater, II

- 312-758-0307
- slater@billslater.com
- williamslater@gmail.com
- http://billslater.com/interview
- 1515 W. Haddon Ave., Unit 309
  Chicago, IL 60642
  United States of America

William Favre Slater, III