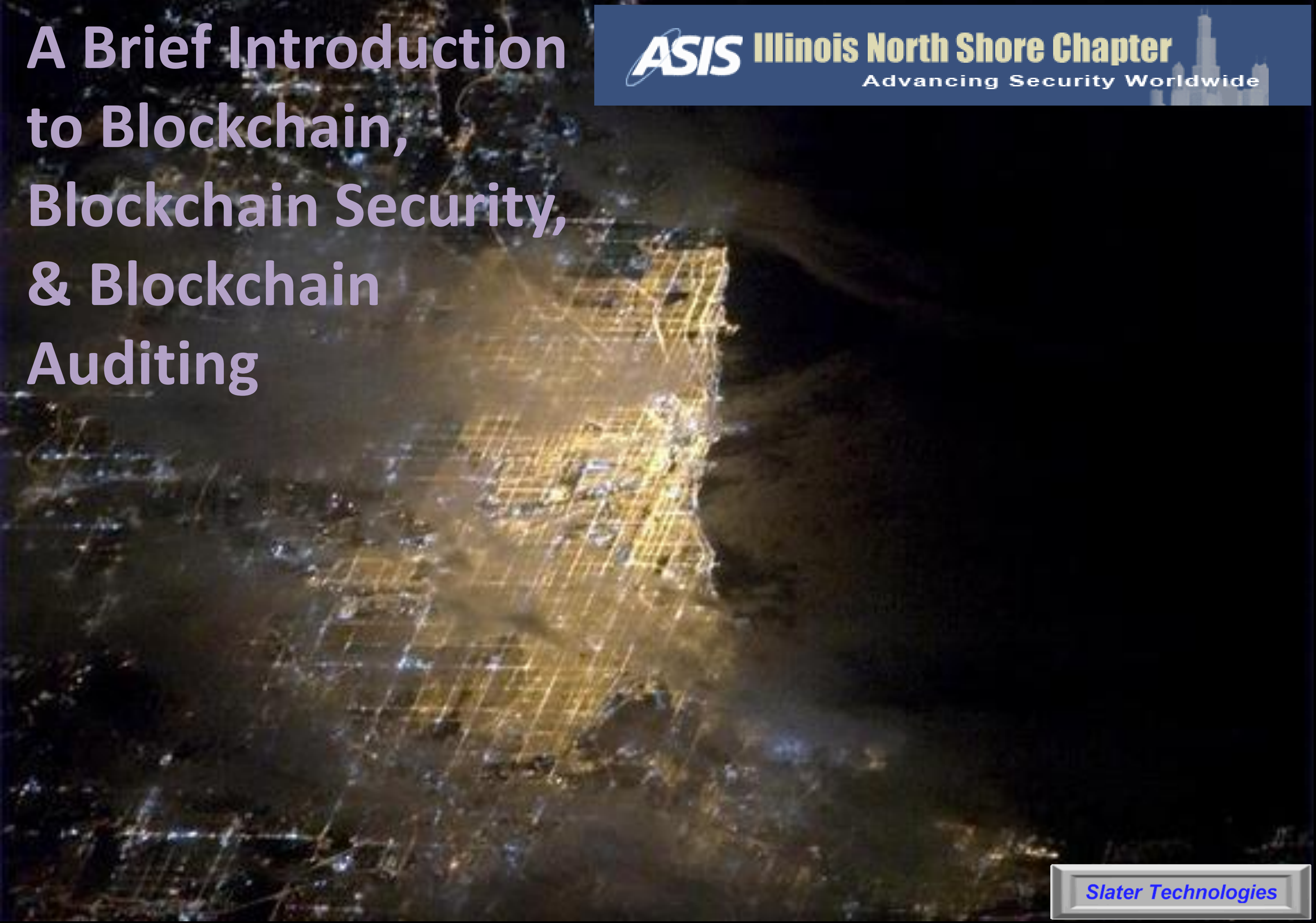
A Brief Introduction to Blockchain, Blockchain Security, & Blockchain Auditing

ASIS Illinois North Shore Chapter

Advancing Security Worldwide



Slater Technologies

ASIS Illinois North Shore Chapter

Advancing Security Worldwide

A Brief Introduction to Blockchain, Blockchain Security and Blockchain Auditing

August 15, 2019

William Favre Slater, III
M.S., MBA, PMP, CISSP, SSCP, CISA, ITIL, IPv6
Director of Blockchain Technologies & Senior IT Consultant in Cybersecurity
Chicago, Illinois
United States of America
slater@billslater.com
http://billslater.com/interview

Slater Technologies

Abstract

- Since Blockchain became well-known as the foundational set of technologies that enabled the creation and operation of Bitcoin, it has captured the attention and imagination of developers, industry leaders, and investors. This is because as a set of technologies that use consensus and peer-to-peer, decentralized systems, it creates immutable data records and enables trust and disintermediation at scale. So what is preventing Blockchain from changing the world?

- Presently, many people understand the basics of Blockchain Technology, yet they don’t understand it at a level to sufficiently address the most fundamental and important aspects of Information Assurance: Security and Auditing. This ambitious presentation will present some of the challenges that are preventing mass adoption of Blockchain, and some practical solutions to those challenges. Specifically: 1) Threats and Vulnerabilities in Blockchain-based systems; 2) How to Secure Blockchain infrastructure and applications; 3) How to perform Secure Software Development for Blockchain applications by design, coding practices, testing and verification; 4) Blockchain and Auditing 5) Concepts of Auditing the Data and Transactions in Blockchain Data Structures; and 6) Automating the Auditing of Blockchains and Blockchain Applications.

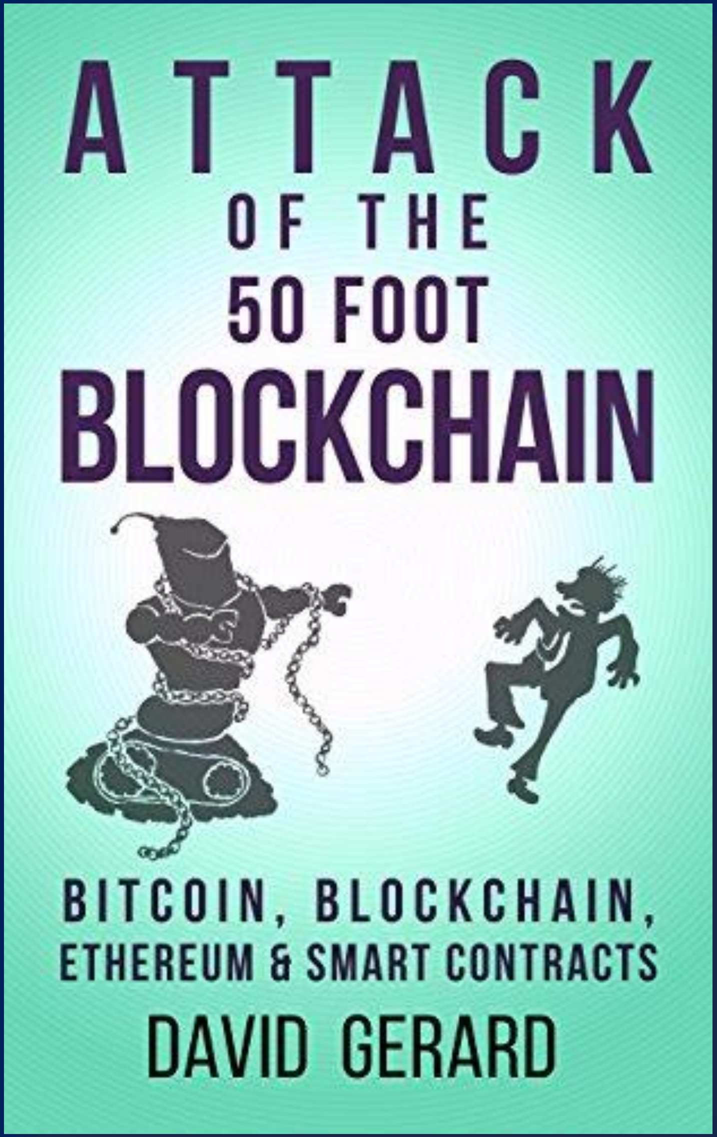
Slater Technologies

Presentation Location

http://billslater.com/writing

Slater Technologies

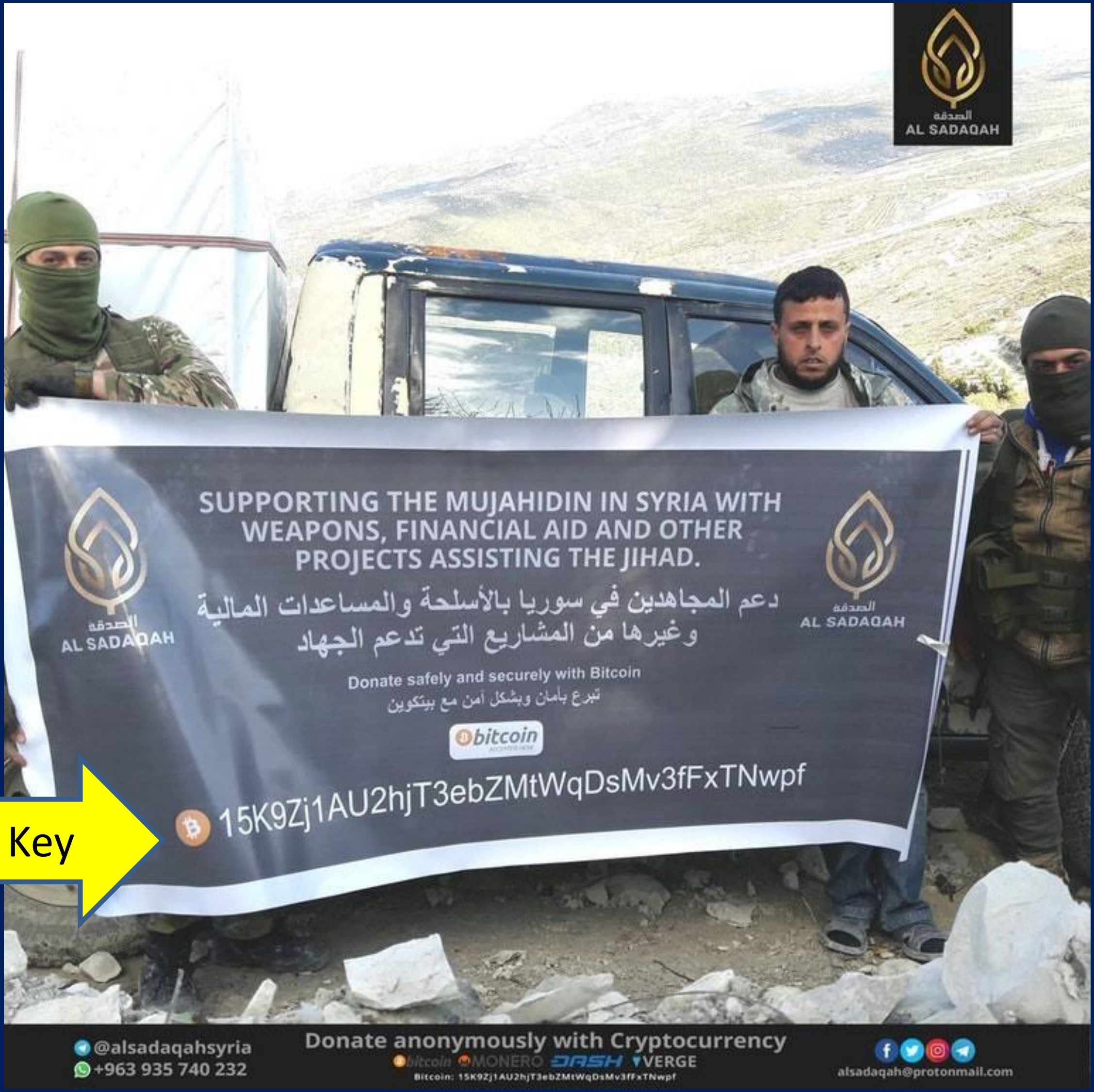
For a Cynical & Humorous View of Blockchain



This is a good and very readable book.

Slater Technologies

ISIS *Loves* Bitcoin (or They ***Did*** Love It)


الصدقة
AL SADAQAH
SUPPORTING THE MUJAHIDIN IN SYRIA WITH WEAPONS, FINANCIAL AID AND OTHER PROJECTS ASSISTING THE JIHAD.
دعم المجاهدين في سوريا بالأسلحة والمساعدات المالية
وغيرها من المشاريع التي تدعم الجهاد
Donate safely and securely with Bitcoin
تبرع بأمان وبشكل آمن مع بيتكوين
bitcoin
15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf
@alsadaqahsyria
+963 935 740 232
Donate anonymously with Cryptocurrency
bitcoin MONERO DASH VERGE
Bitcoin: 15K9Zj1AU2hjT3ebZMtWqDsMv3fFxTNwpf
alsadaqah@protonmail.com

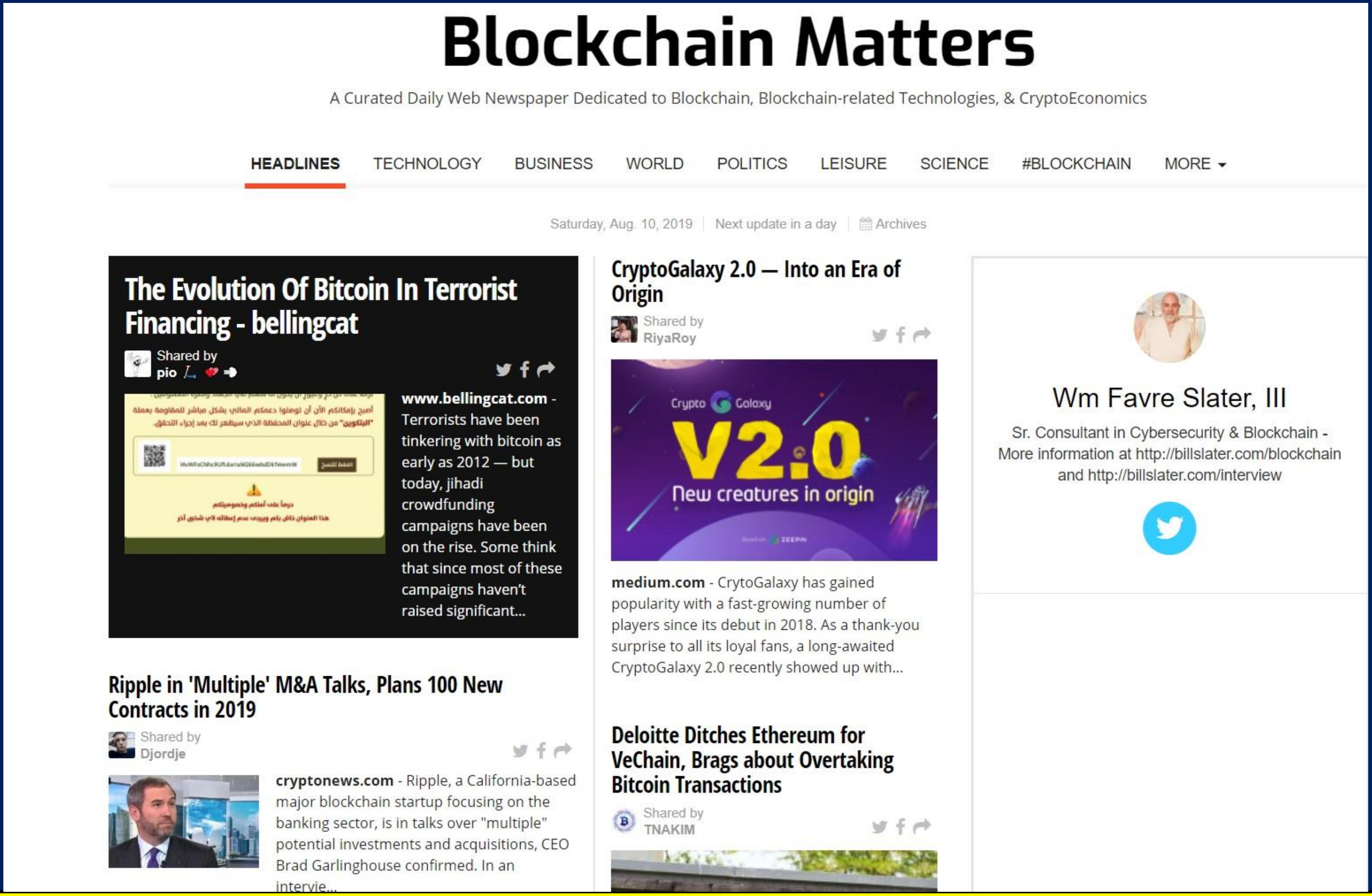
Their Public Key

Comment:
This actually didn't end well for ISIS **and their Donors**.

Enough said.

Slater Technologies

Free Blockchain Daily Newspaper:



Blockchain Matters

A Curated Daily Web Newspaper Dedicated to Blockchain, Blockchain-related Technologies, & CryptoEconomics

Saturday, Aug. 10, 2019 | Next update in a day | Archives

The Evolution Of Bitcoin In Terrorist Financing - bellingcat

Shared by pio

www.bellingcat.com - Terrorists have been tinkering with bitcoin as early as 2012 — but today, jihadi crowdfunding campaigns have been on the rise. Some think that since most of these campaigns haven't raised significant...

Ripple in 'Multiple' M&A Talks, Plans 100 New Contracts in 2019

Shared by Djordje

cryptonews.com - Ripple, a California-based major blockchain startup focusing on the banking sector, is in talks over "multiple" potential investments and acquisitions, CEO Brad Garlinghouse confirmed. In an intervie...

CryptoGalaxy 2.0 — Into an Era of Origin

Shared by RiyaRoy

medium.com - CrytoGalaxy has gained popularity with a fast-growing number of players since its debut in 2018. As a thank-you surprise to all its loyal fans, a long-awaited CryptoGalaxy 2.0 recently showed up with...

Deloitte Ditches Ethereum for VeChain, Brags about Overtaking Bitcoin Transactions

Shared by TNAKIM

Wm Favre Slater, III

Sr. Consultant in Cybersecurity & Blockchain - More information at http://billslater.com/blockchain and http://billslater.com/interview

More information: https://paper.li/billslater/1530793250#/

Agenda

- Why Blockchain Is Important?
- What Is Blockchain?
- Why Blockchain?
- Latest Blockchain News
- Blockchain Security
- Blockchain Auditing
- Conclusion
- Questions
- Final Thoughts
- References
- Supplemental Slides

Slater Technologies

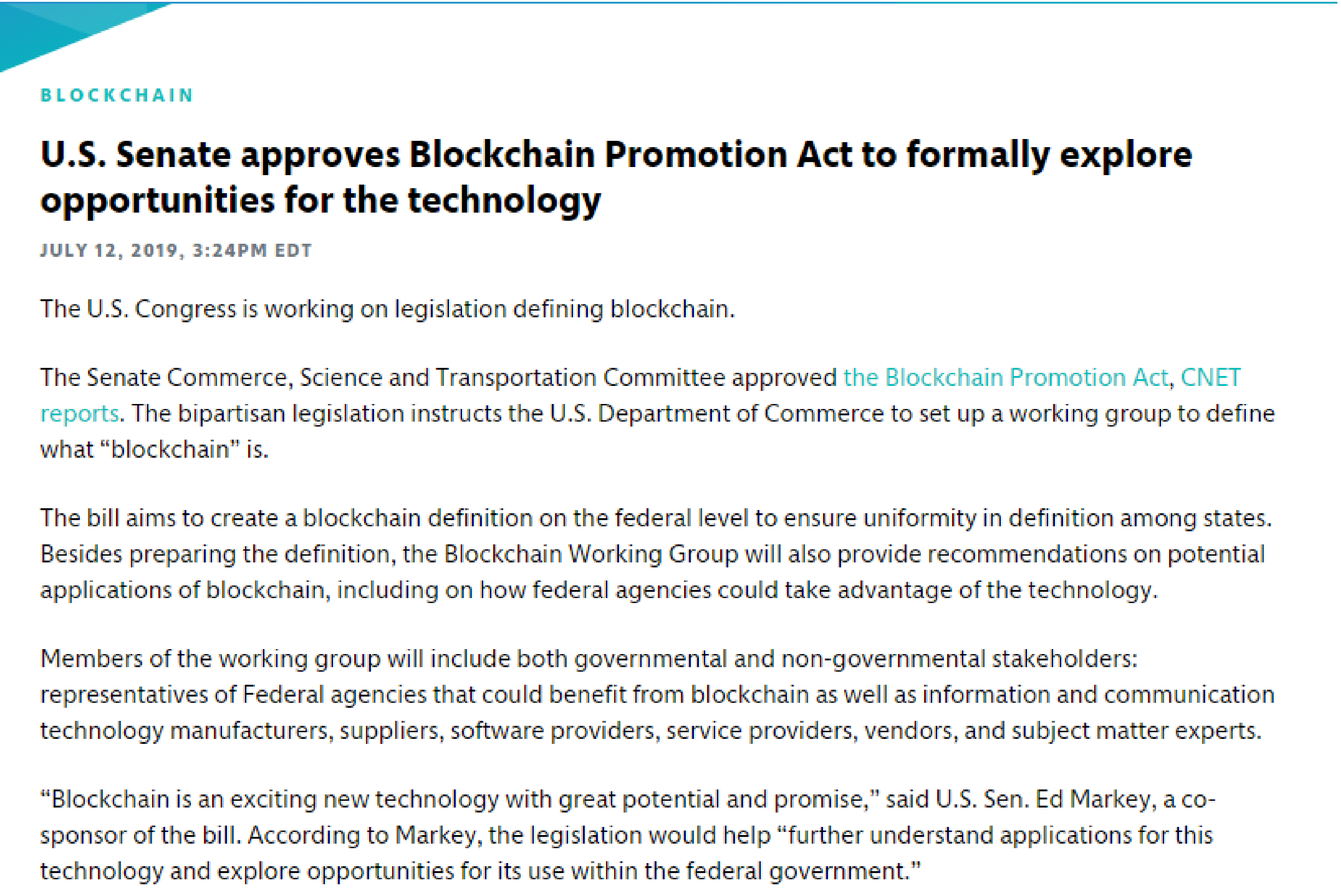
Why Is Blockchain Important?

Why is Blockchain Important?

1) Creates the capability for immutable transaction data
2) Peer-to-Peer & Decentralized
3) Secure (relatively speaking)
4) Rapidly growing in popularity
5) Large companies like WalMart, IBM, and suppliers are using it solve real-world challenges.
6) **Congress introduced a Bill in July 2019, the Blockchain Promotion Act of 2019**

Slater Technologies

Why is Blockchain Important?



BLOCKCHAIN

U.S. Senate approves Blockchain Promotion Act to formally explore opportunities for the technology

JULY 12, 2019, 3:24PM EDT

The U.S. Congress is working on legislation defining blockchain.

The Senate Commerce, Science and Transportation Committee approved the Blockchain Promotion Act, CNET reports. The bipartisan legislation instructs the U.S. Department of Commerce to set up a working group to define what "blockchain" is.

The bill aims to create a blockchain definition on the federal level to ensure uniformity in definition among states. Besides preparing the definition, the Blockchain Working Group will also provide recommendations on potential applications of blockchain, including on how federal agencies could take advantage of the technology.

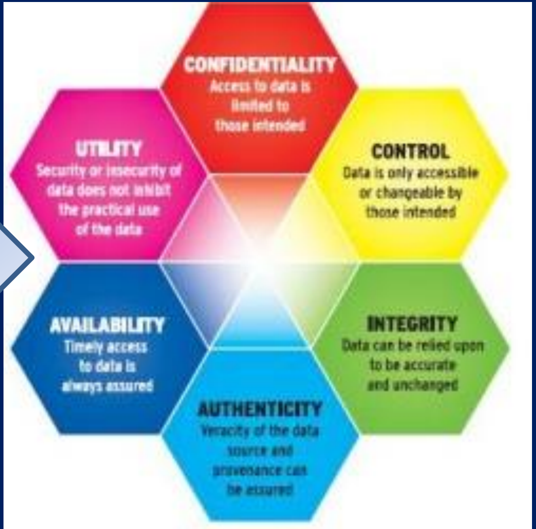
Members of the working group will include both governmental and non-governmental stakeholders: representatives of Federal agencies that could benefit from blockchain as well as information and communication technology manufacturers, suppliers, software providers, service providers, vendors, and subject matter experts.

"Blockchain is an exciting new technology with great potential and promise," said U.S. Sen. Ed Markey, a co-sponsor of the bill. According to Markey, the legislation would help "further understand applications for this technology and explore opportunities for its use within the federal government."

Slater Technologies

Why Is Blockchain Important

- Accessible
- Open source
- Easily provides three challenging elements of the **Parkerian Hexad** model for security:
  - **Authenticity**
  - **Control**
  - **Utility**
- It WORKS!
- Business enabler
- Reduces risk of computer fraud
- It is being widely adopted for trusted computing
- Blockchain developers and architects are in great demand: for every Blockchain professional there are 14 open positions



CONFIDENTIALITY
Access to data is limited to those intended

UTILITY
Security or insecurity of data does not inhibit the practical use of the data

CONTROL
Data is only accessible or changeable by those intended

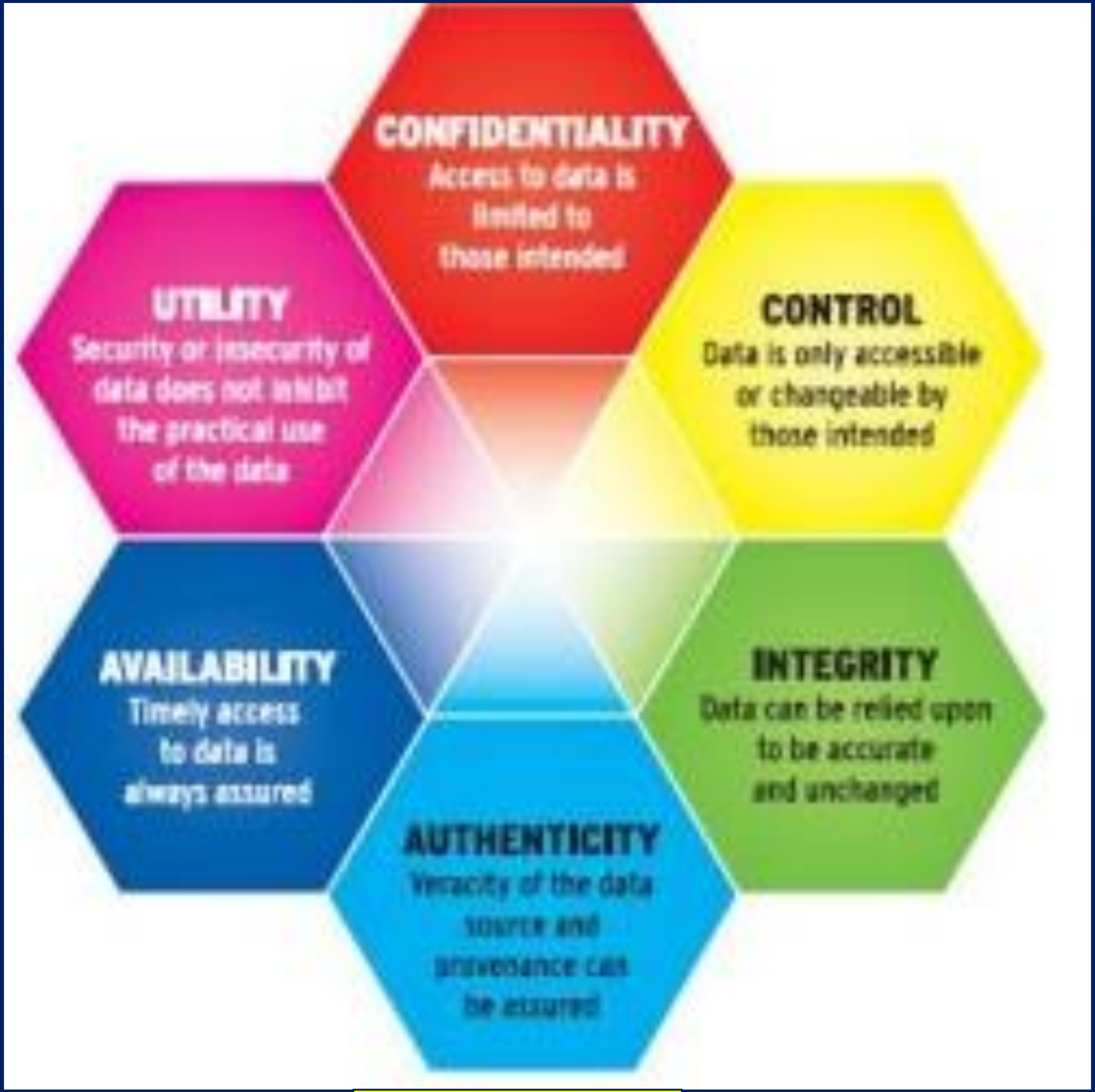
AVAILABILITY
Timely access to data is always assured

INTEGRITY
Data can be relied upon to be accurate and unchanged

AUTHENTICITY
Veracity of the data source and provenance can be assured

Donn B. Parker

Parkerian Hexad


CONFIDENTIALITY
Access to data is limited to those intended
UTILITY
Security or insecurity of data does not inhibit the practical use of the data
CONTROL
Data is only accessible or changeable by those intended
AVAILABILITY
Timely access to data is always assured
INTEGRITY
Data can be relied upon to be accurate and unchanged
AUTHENTICITY
Veracity of the data source and provenance can be assured

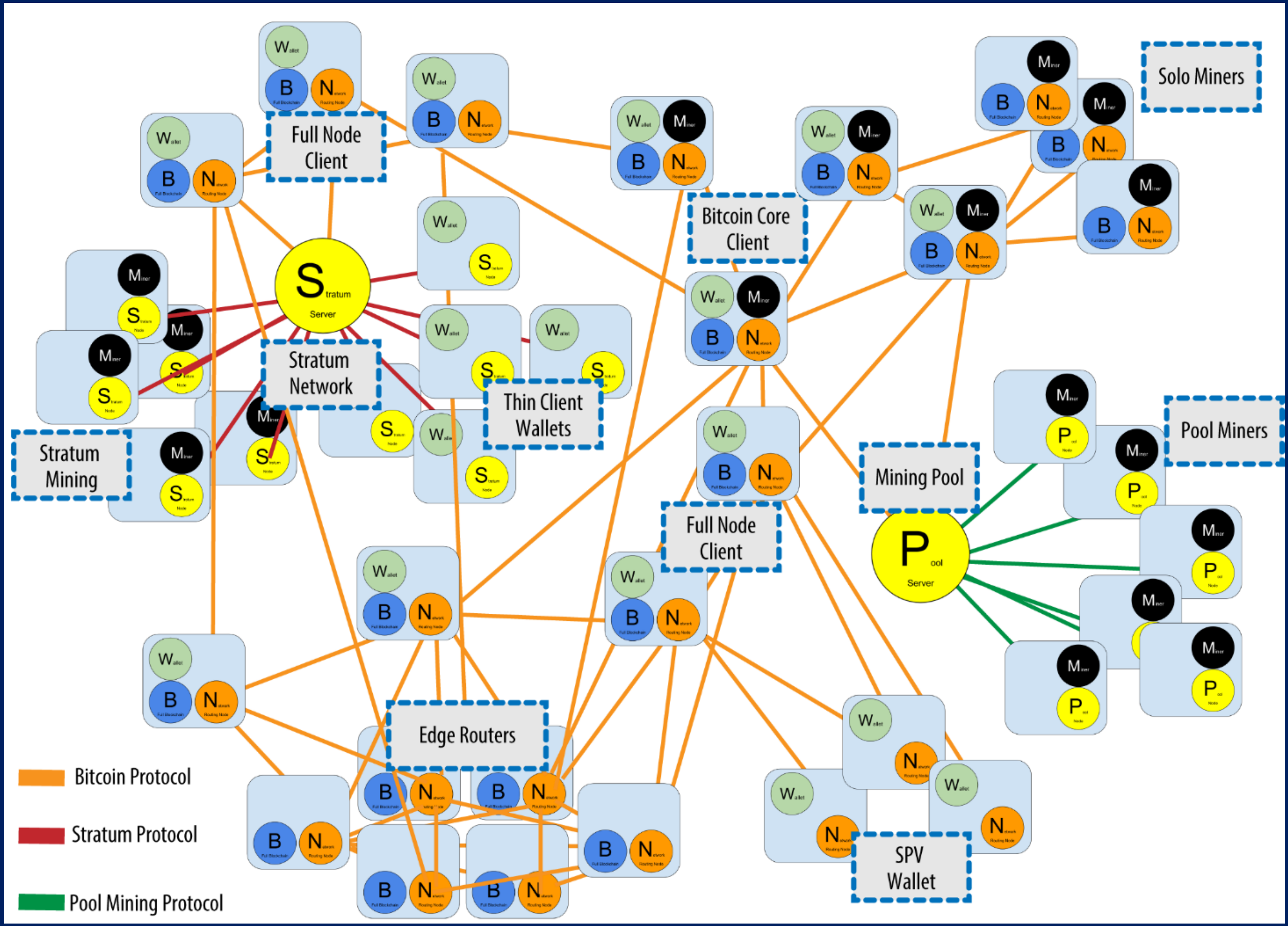
Donn B. Parker

Slater Technologies

What is Blockchain?

Slater Technologies

A Logical Diagram of a Blockchain Network



Source: This Photo by Unknown Author is licensed under CC BY-SA

Slater Technologies

What Is Blockchain?

- It's like an Operating System that rides on top on Linux, Unix, and of Windows
- Distributed Ledger
- Decentralized, Peer-to-Peer
- Popularized by Satoshi Nakamoto (Bitcoin inventor)
- Uses Public-Key Cryptography and Hashing
- Append-only Transactions (no deletes or modifications to data)
- The Open Source Code already exists in Github (Bitcoin and Ethereum)
- Immutable (cannot delete blocks or change data in blocks)
- Driven by consensus protocol(s)
  - Proof of Work
  - Proof of Stake
  - Etc.
- The world's largest Blockchain Database is the Bitcoin Blockchain Database, with 180 GB (it doesn't scale very well)
- **Blockchain IS NOT Cryptocurrency, BUT Cryptocurrency uses Blockchain**

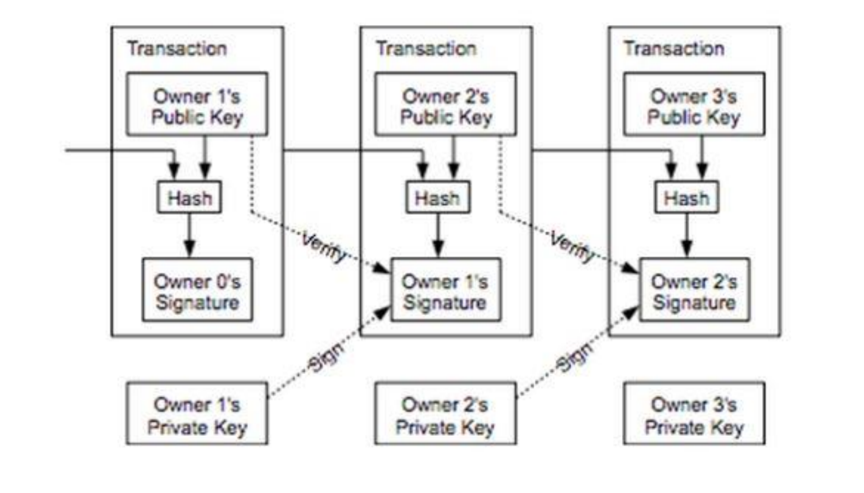


Image: Satoshi Nakamoto

Slater Technologies

What Is Blockchain?

- **From Blockchain Consensus Protocol Guide:**
  - A blockchain is a decentralized peer-to-peer system with no central authority figure.
  - While this creates a system that is devoid of corruption from a single source, it still create a major problems:

    How are any decisions made?
    How does anything get done?
    Think of a normal centralized organization.
  - All the decisions are taken by the leader or a board of decision makers. This isn't possible in a blockchain because a blockchain has no "leader". For the blockchain to make decisions, they need to come to a consensus using "consensus mechanisms".

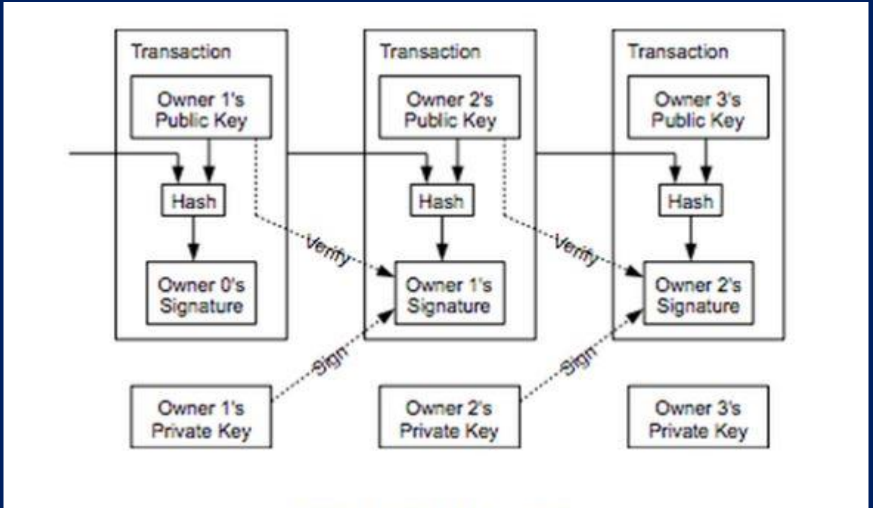


Image: Satoshi Nakamoto

Slater Technologies

The Term “Blockchain”

- Name for a data structure
- Name for an algorithm
- Name for a suite of Technologies
- An umbrella term for purely distributed peer-to-peer systems with a common application area
- A peer-to-peer-based operating system with its own unique rule set that utilizes hashing to provide unique data

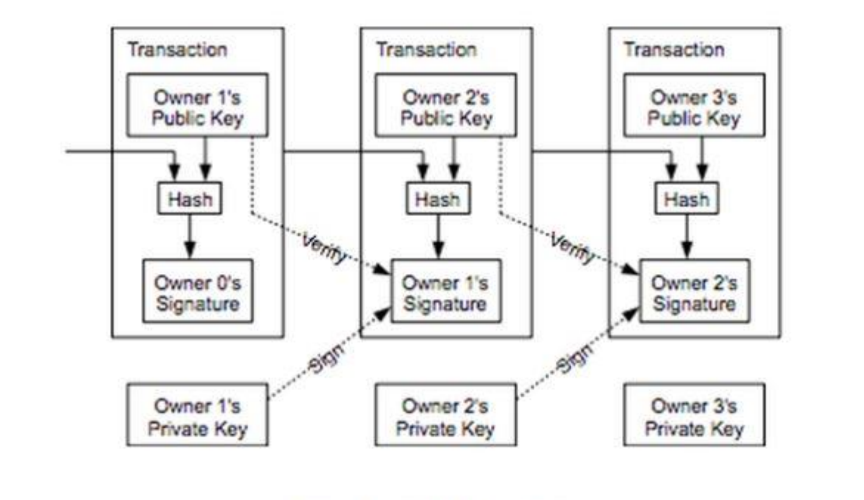


Image: Satoshi Nakamoto

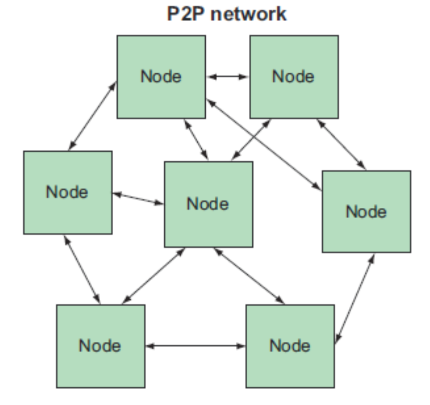


Figure 1.4 A peer-to-peer (P2P) network is made of nodes that communicate directly with each other without the coordination of a master node.

Slater Technologies

Blockchain – Simplified View

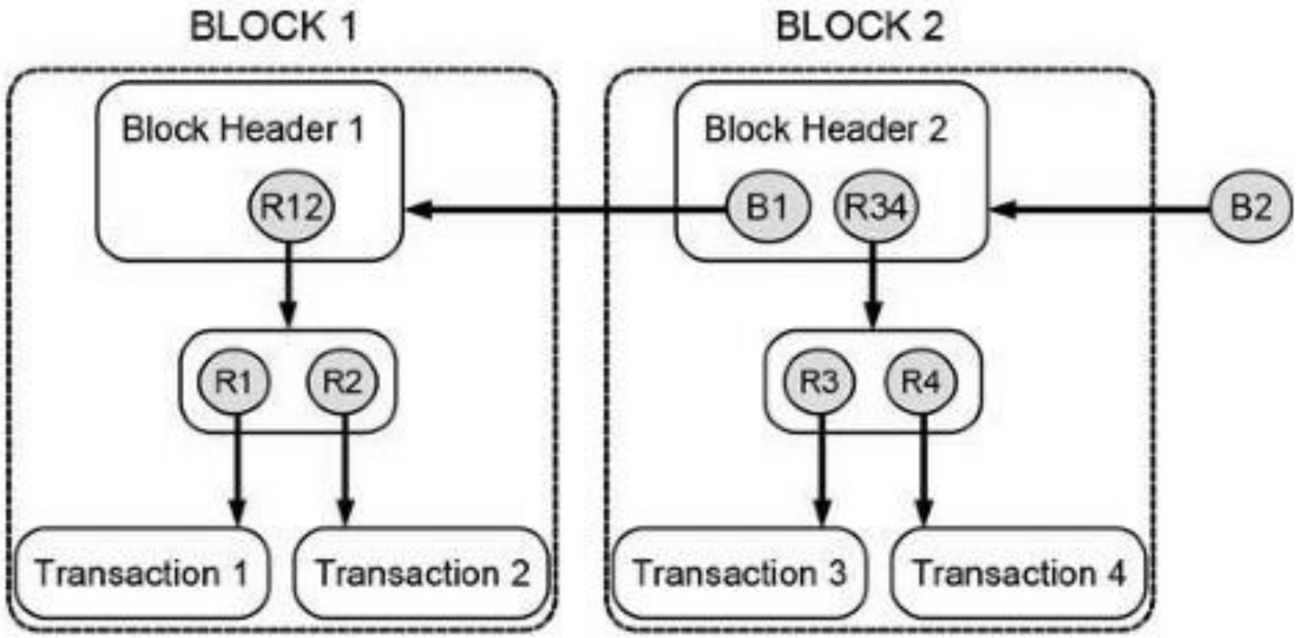


Figure 14-5. A simplified blockchain-data-structure containing four transactions

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Slater Technologies

Comparing a Centralized Application to a Decentralized Application

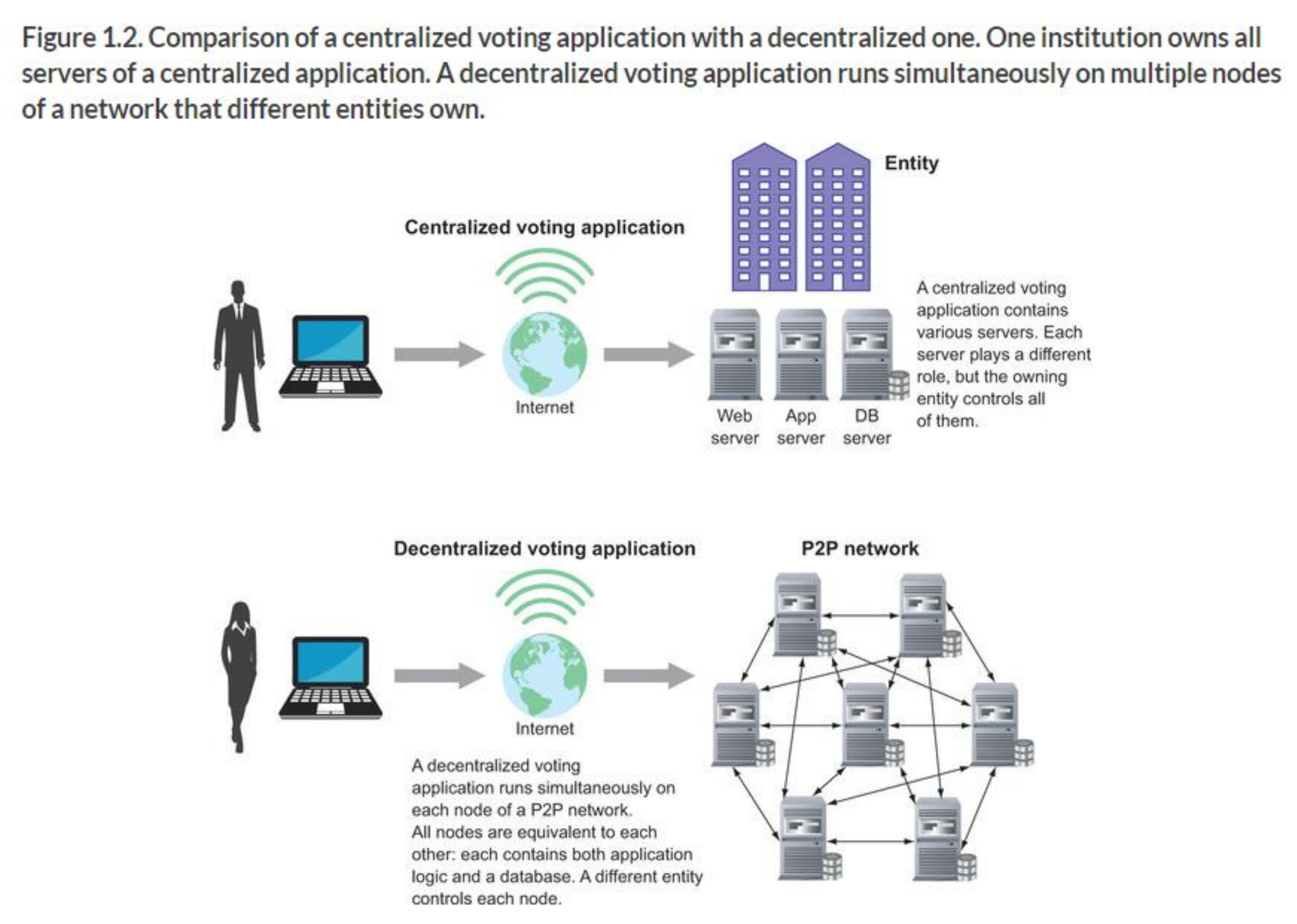


Figure 1.2. Comparison of a centralized voting application with a decentralized one. One institution owns all servers of a centralized application. A decentralized voting application runs simultaneously on multiple nodes of a network that different entities own.

Entity
Centralized voting application
Internet
Web server
App server
DB server
Decentralized voting application
P2P network
Internet

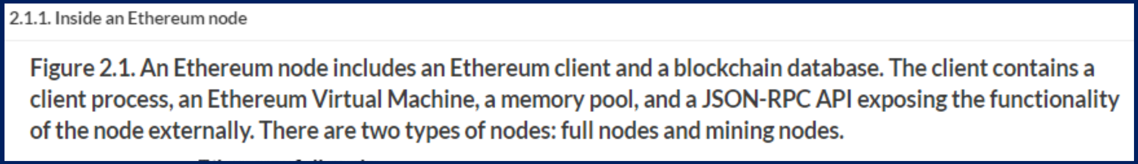
A centralized voting application contains various servers. Each server plays a different role, but the owning entity controls all of them.

A decentralized voting application runs simultaneously on each node of a P2P network. All nodes are equivalent to each other: each contains both application logic and a database. A different entity controls each node.

Source: Roberto Infante, Building Ethereum DApps, 2019

Slater Technologies

Full Ethereum Node



2.1.1. Inside an Ethereum node

Figure 2.1. An Ethereum node includes an Ethereum client and a blockchain database. The client contains a client process, an Ethereum Virtual Machine, a memory pool, and a JSON-RPC API exposing the functionality of the node externally. There are two types of nodes: full nodes and mining nodes.

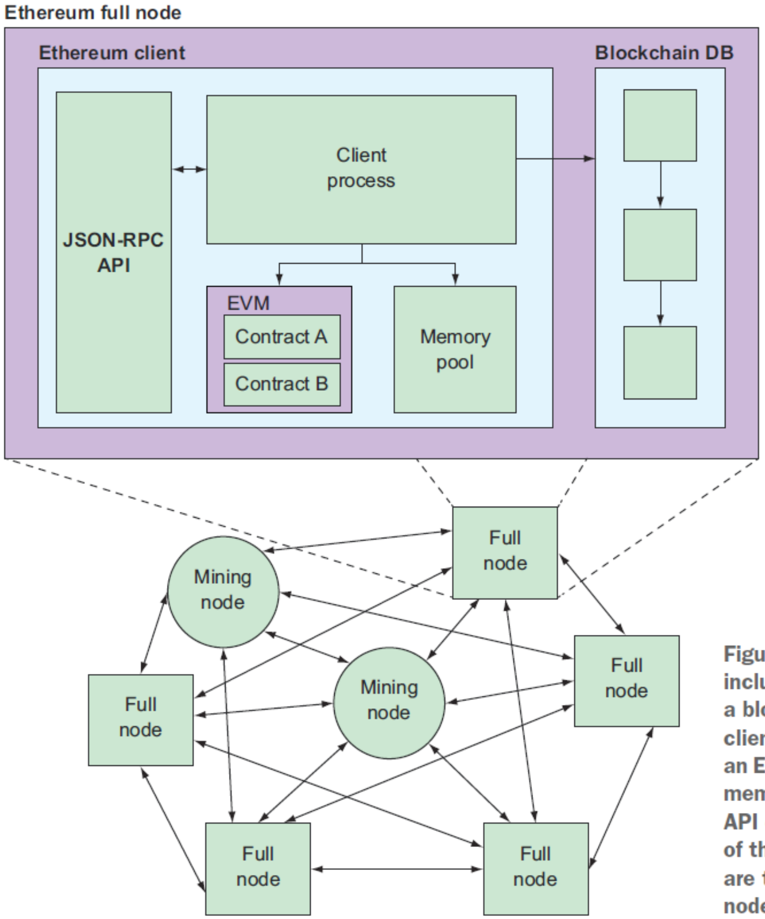
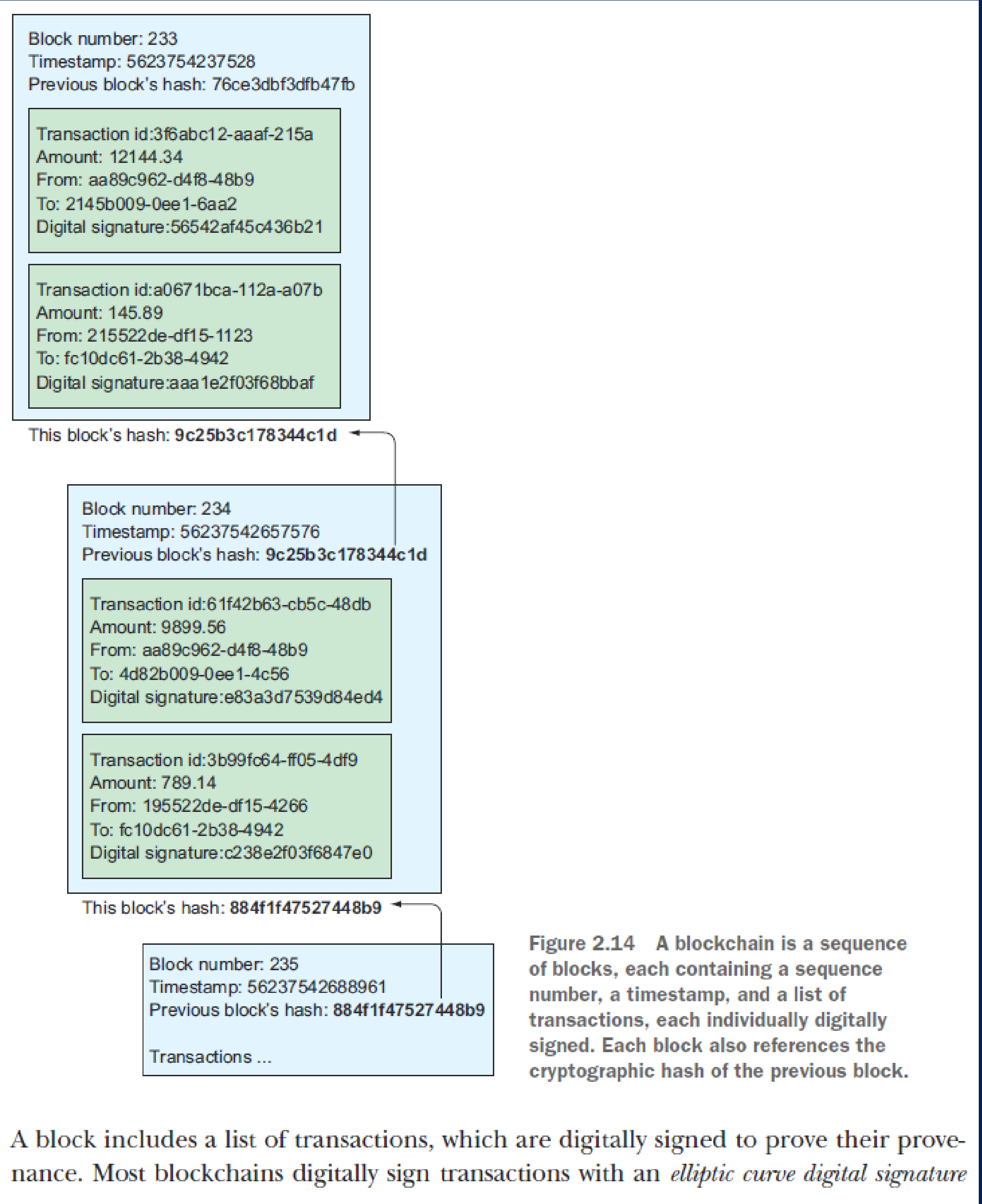


Figure 2.1 An Ethereum node includes an Ethereum client and a blockchain database. The client contains a client process, an Ethereum Virtual Machine, a memory pool, and a JSON-RPC API exposing the functionality of the node externally. There are two types of nodes: full nodes and mining nodes.

Source: Roberto Infante, Building Ethereum DApps, 2019

Slater Technologies

Example Blockchain Contents



Block number: 233
Timestamp: 5623754237528
Previous block's hash: 76ce3dbf3dfb47fb

Transaction id:3f6abc12-aaaf-215a
Amount: 12144.34
From: aa89c962-d4f8-48b9
To: 2145b009-0ee1-6aa2
Digital signature:56542af45c436b21

Transaction id:a0671bca-112a-a07b
Amount: 145.89
From: 215522de-df15-1123
To: fc10dc61-2b38-4942
Digital signature:aaa1e2f03f68bbaf

This block's hash: **9c25b3c178344c1d**

Block number: 234
Timestamp: 56237542657576
Previous block's hash: **9c25b3c178344c1d**

Transaction id:61f42b63-cb5c-48db
Amount: 9899.56
From: aa89c962-d4f8-48b9
To: 4d82b009-0ee1-4c56
Digital signature:e83a3d7539d84ed4

Transaction id:3b99fc64-ff05-4df9
Amount: 789.14
From: 195522de-df15-4266
To: fc10dc61-2b38-4942
Digital signature:c238e2f03f6847e0

This block's hash: **884f1f47527448b9**

Block number: 235
Timestamp: 56237542688961
Previous block's hash: **884f1f47527448b9**

Transactions ...

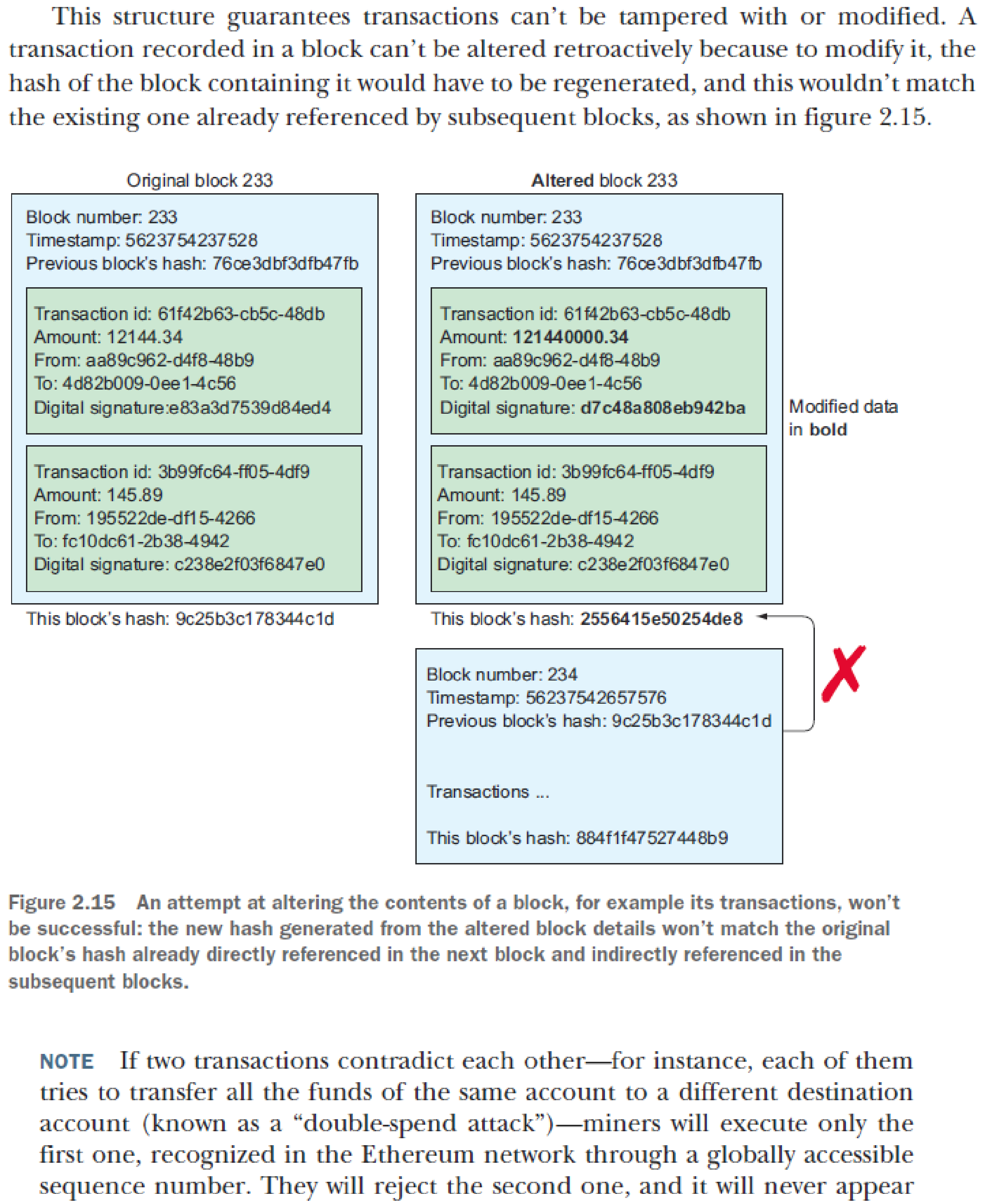
Figure 2.14 A blockchain is a sequence of blocks, each containing a sequence number, a timestamp, and a list of transactions, each individually digitally signed. Each block also references the cryptographic hash of the previous block.

A block includes a list of transactions, which are digitally signed to prove their provenance. Most blockchains digitally sign transactions with an *elliptic curve digital signature*

Source: Roberto Infante, Building Ethereum DApps, 2019

Slater Technologies

Example of Blockchain Immutability



This structure guarantees transactions can't be tampered with or modified. A transaction recorded in a block can't be altered retroactively because to modify it, the hash of the block containing it would have to be regenerated, and this wouldn't match the existing one already referenced by subsequent blocks, as shown in figure 2.15.

Original block 233

Block number: 233
Timestamp: 5623754237528
Previous block's hash: 76ce3dbf3dfb47fb

Transaction id: 61f42b63-cb5c-48db
Amount: 12144.34
From: aa89c962-d4f8-48b9
To: 4d82b009-0ee1-4c56
Digital signature:e83a3d7539d84ed4

Transaction id: 3b99fc64-ff05-4df9
Amount: 145.89
From: 195522de-df15-4266
To: fc10dc61-2b38-4942
Digital signature: c238e2f03f6847e0

This block's hash: 9c25b3c178344c1d

Altered block 233

Block number: 233
Timestamp: 5623754237528
Previous block's hash: 76ce3dbf3dfb47fb

Transaction id: 61f42b63-cb5c-48db
Amount: **121440000.34**
From: aa89c962-d4f8-48b9
To: 4d82b009-0ee1-4c56
Digital signature: **d7c48a808eb942ba**

Transaction id: 3b99fc64-ff05-4df9
Amount: 145.89
From: 195522de-df15-4266
To: fc10dc61-2b38-4942
Digital signature: c238e2f03f6847e0

This block's hash: **2556415e50254de8**

Modified data in **bold**

✗

Block number: 234
Timestamp: 56237542657576
Previous block's hash: 9c25b3c178344c1d

Transactions ...

This block's hash: 884f1f47527448b9

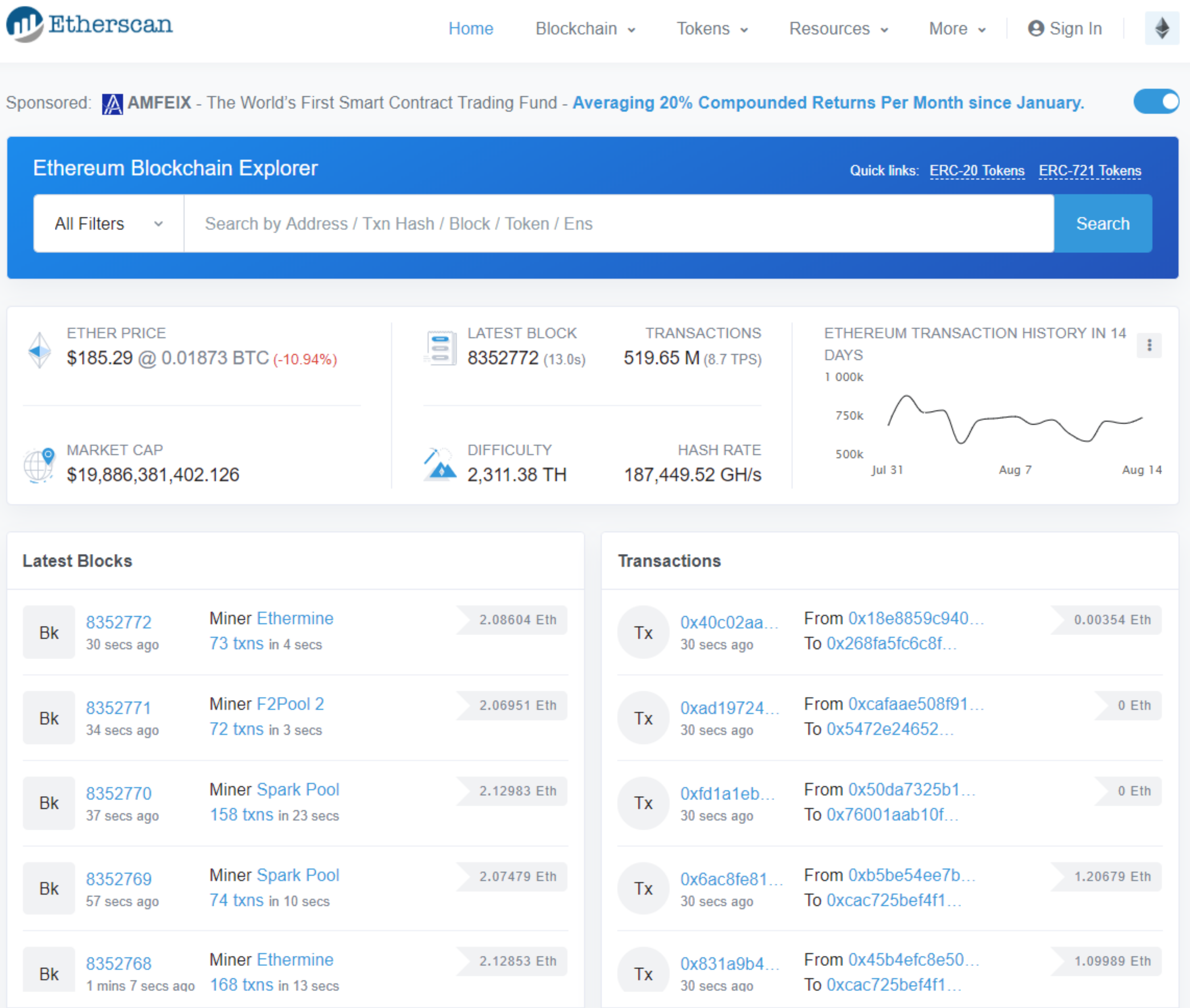
Figure 2.15 An attempt at altering the contents of a block, for example its transactions, won't be successful: the new hash generated from the altered block details won't match the original block's hash already directly referenced in the next block and indirectly referenced in the subsequent blocks.

NOTE If two transactions contradict each other—for instance, each of them tries to transfer all the funds of the same account to a different destination account (known as a "double-spend attack")—miners will execute only the first one, recognized in the Ethereum network through a globally accessible sequence number. They will reject the second one, and it will never appear

Source: Roberto Infante, Building Ethereum DApps, 2019

Slater Technologies

Actual Ethereum Main Net Blockchain



Etherscan

Home | Blockchain ⌄ | Tokens ⌄ | Resources ⌄ | More ⌄ | Sign In

Sponsored: AMFEIX - The World's First Smart Contract Trading Fund - **Averaging 20% Compounded Returns Per Month since January.**

Ethereum Blockchain Explorer

Quick links: ERC-20 Tokens ERC-721 Tokens

All Filters ⌄ | Search by Address / Txn Hash / Block / Token / Ens | Search

ETHER PRICE
$185.29 @ 0.01873 BTC (-10.94%)

LATEST BLOCK
8352772 (13.0s)

TRANSACTIONS
519.65 M (8.7 TPS)

MARKET CAP
$19,886,381,402.126

DIFFICULTY
2,311.38 TH

HASH RATE
187,449.52 GH/s

ETHEREUM TRANSACTION HISTORY IN 14 DAYS

Latest Blocks

Bk	8352772 30 secs ago	Miner Ethermine 73 txns in 4 secs	2.08604 Eth
Bk	8352771 34 secs ago	Miner F2Pool 2 72 txns in 3 secs	2.06951 Eth
Bk	8352770 37 secs ago	Miner Spark Pool 158 txns in 23 secs	2.12983 Eth
Bk	8352769 57 secs ago	Miner Spark Pool 74 txns in 10 secs	2.07479 Eth
Bk	8352768 1 mins 7 secs ago	Miner Ethermine 168 txns in 13 secs	2.12853 Eth

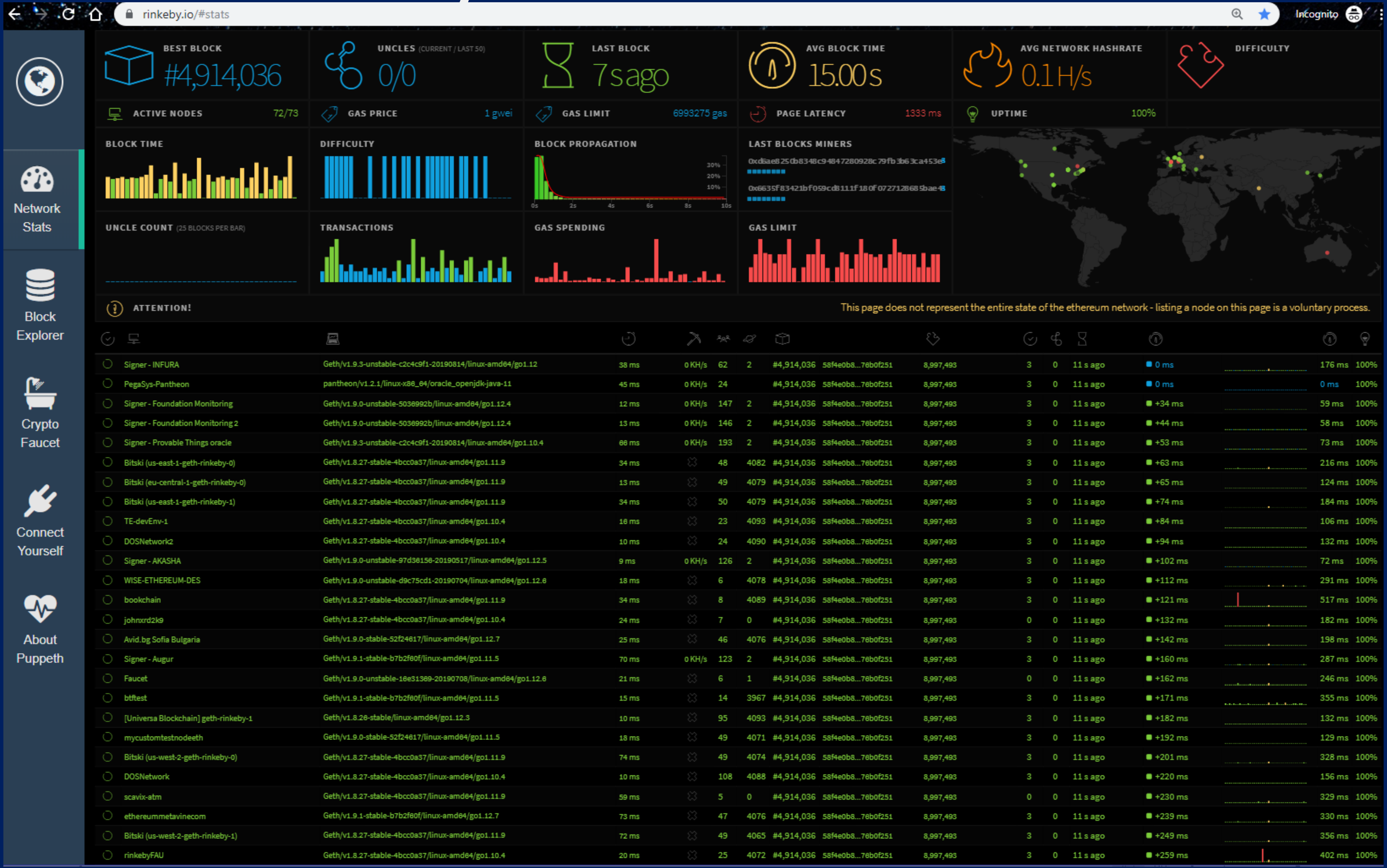
Transactions

Tx	0x40c02aa... 30 secs ago	From 0x18e8859c940... To 0x268fa5fc6c8f...	0.00354 Eth
Tx	0xad19724... 30 secs ago	From 0xcafaae508f91... To 0x5472e24652...	0 Eth
Tx	0xfd1a1eb... 30 secs ago	From 0x50da7325b1... To 0x76001aab10f...	0 Eth
Tx	0x6ac8fe81... 30 secs ago	From 0xb5be54ee7b... To 0xcac725bef4f1...	1.20679 Eth
Tx	0x831a9b4... 30 secs ago	From 0x45b4efc8e50... To 0xcac725bef4f1...	1.09989 Eth

Source: http://etherescan.io

Slater Technologies

Actual Rinkby Ethereum Test Net Blockchain



BEST BLOCK #4,914,036

UNCLES (CURRENT / LAST 50) 0/0

LAST BLOCK 7s ago

AVG BLOCK TIME 15.00s

AVG NETWORK HASHRATE 0.1 H/s

DIFFICULTY

ACTIVE NODES 72/73

GAS PRICE 1 gwei

GAS LIMIT 6993275 gas

PAGE LATENCY 1333 ms

UPTIME 100%

BLOCK TIME

DIFFICULTY

BLOCK PROPAGATION

LAST BLOCKS MINERS

0xd6ae8250b8348c94847280928c79fb3b63ca453e 8

0x6635f83421bf059cd8111f180f0727128685bae4 8

UNCLE COUNT (25 BLOCKS PER BAR)

TRANSACTIONS

GAS SPENDING

GAS LIMIT

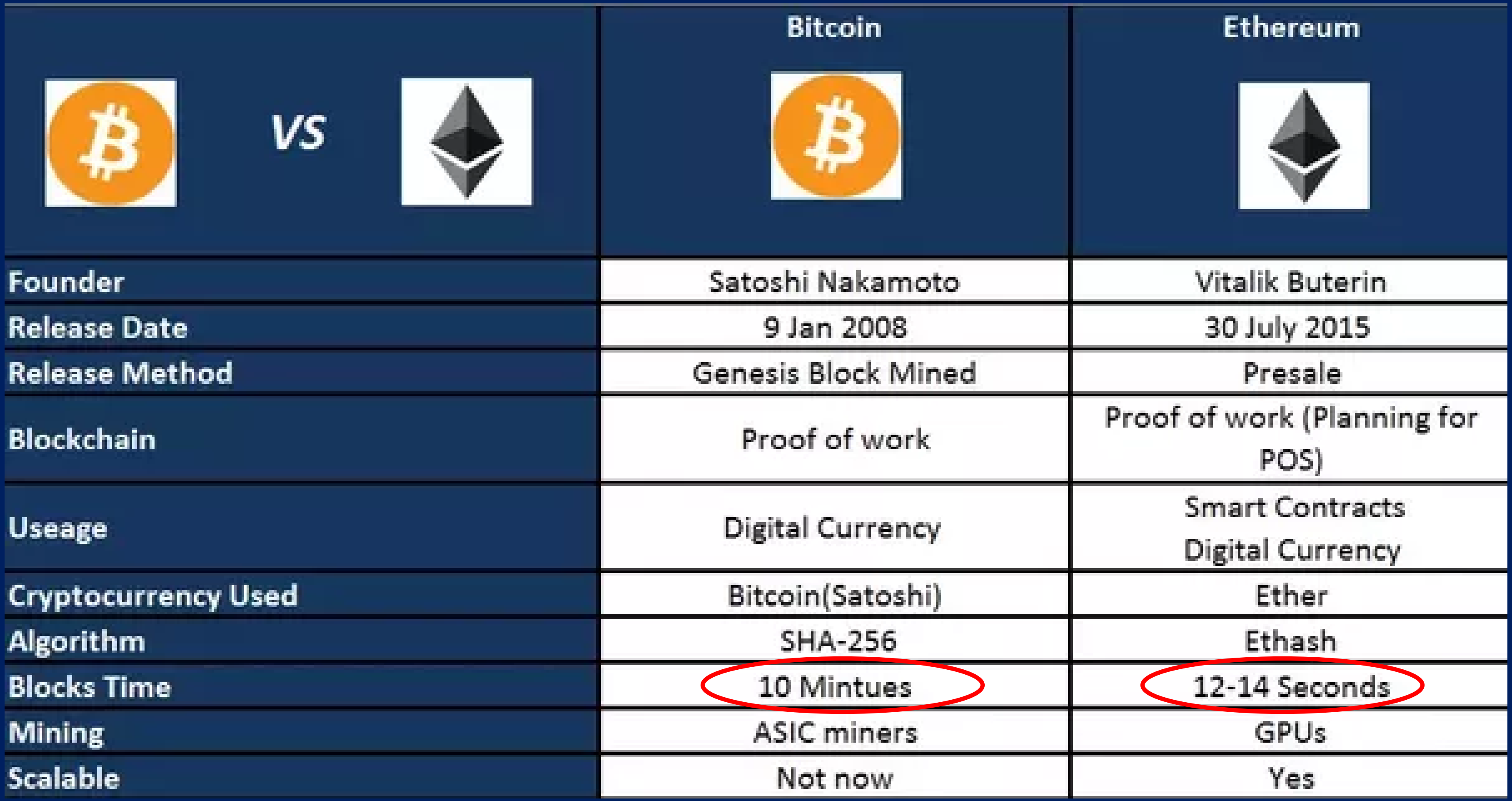
ATTENTION! This page does not represent the entire state of the ethereum network - listing a node on this page is a voluntary process.

○	Signer - INFURA	Geth/v1.9.3-unstable-c2c4c9f1-20190814/linux-amd64/go1.12	38 ms	0 KH/s	62	2	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	0 ms	176 ms	100%
○	PegaSys-Pantheon	pantheon/v1.2.1/linux-x86_64/oracle_openjdk-java-11	45 ms	0 KH/s	24		#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	0 ms	0 ms	100%
○	Signer - Foundation Monitoring	Geth/v1.9.0-unstable-5036992b/linux-amd64/go1.12.4	12 ms	0 KH/s	147	2	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+34 ms	59 ms	100%
○	Signer - Foundation Monitoring 2	Geth/v1.9.0-unstable-5036992b/linux-amd64/go1.12.4	13 ms	0 KH/s	146	2	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+44 ms	58 ms	100%
○	Signer - Provable Things oracle	Geth/v1.9.3-unstable-c2c4c9f1-20190814/linux-amd64/go1.10.4	66 ms	0 KH/s	193	2	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+53 ms	73 ms	100%
○	Bitski (us-east-1-geth-rinkeby-0)	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.11.9	34 ms	✗	48	4082	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+63 ms	216 ms	100%
○	Bitski (eu-central-1-geth-rinkeby-0)	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.11.9	13 ms	✗	49	4079	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+65 ms	124 ms	100%
○	Bitski (us-east-1-geth-rinkeby-1)	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.11.9	34 ms	✗	50	4079	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+74 ms	184 ms	100%
○	TE-devEnv-1	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.10.4	16 ms	✗	23	4093	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+84 ms	106 ms	100%
○	DOSNetwork2	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.10.4	10 ms	✗	24	4090	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+94 ms	132 ms	100%
○	Signer - AKASHA	Geth/v1.9.0-unstable-97d36156-20190517/linux-amd64/go1.12.5	9 ms	0 KH/s	126	2	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+102 ms	72 ms	100%
○	WISE-ETHEREUM-DES	Geth/v1.9.0-unstable-d9c75cd1-20190704/linux-amd64/go1.12.6	18 ms	✗	6	4078	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+112 ms	291 ms	100%
○	bookchain	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.11.9	34 ms	✗	8	4089	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+121 ms	517 ms	100%
○	johnxrd2k9	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.10.4	24 ms	✗	7	0	#4,914,036	58f4e0b8...76b0f251	8,997,493	0	0	11 s ago	+132 ms	182 ms	100%
○	Avid.bg Sofia Bulgaria	Geth/v1.9.0-stable-52f24617/linux-amd64/go1.12.7	25 ms	✗	46	4076	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+142 ms	198 ms	100%
○	Signer - Augur	Geth/v1.9.1-stable-b7b2f60f/linux-amd64/go1.11.5	70 ms	0 KH/s	123	2	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+160 ms	287 ms	100%
○	Faucet	Geth/v1.9.0-unstable-16e31369-20190708/linux-amd64/go1.12.6	21 ms	✗	6	1	#4,914,036	58f4e0b8...76b0f251	8,997,493	0	0	11 s ago	+162 ms	246 ms	100%
○	btftest	Geth/v1.9.1-stable-b7b2f60f/linux-amd64/go1.11.5	15 ms	✗	14	3967	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+171 ms	355 ms	100%
○	[Universa Blockchain] geth-rinkeby-1	Geth/v1.8.26-stable/linux-amd64/go1.12.3	10 ms	✗	95	4093	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+182 ms	132 ms	100%
○	mycustomtestnodeeth	Geth/v1.9.0-stable-52f24617/linux-amd64/go1.11.5	18 ms	✗	49	4071	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+192 ms	129 ms	100%
○	Bitski (us-west-2-geth-rinkeby-0)	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.11.9	74 ms	✗	49	4074	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+201 ms	328 ms	100%
○	DOSNetwork	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.10.4	10 ms	✗	108	4088	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+220 ms	156 ms	100%
○	scavix-atm	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.11.9	59 ms	✗	5	0	#4,914,036	58f4e0b8...76b0f251	8,997,493	0	0	11 s ago	+230 ms	329 ms	100%
○	ethereummetavinecom	Geth/v1.9.1-stable-b7b2f60f/linux-amd64/go1.12.7	73 ms	✗	47	4076	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+239 ms	330 ms	100%
○	Bitski (us-west-2-geth-rinkeby-1)	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.11.9	72 ms	✗	49	4065	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+249 ms	356 ms	100%
○	rinkebyFAU	Geth/v1.8.27-stable-4bcc0a37/linux-amd64/go1.10.4	20 ms	✗	25	4072	#4,914,036	58f4e0b8...76b0f251	8,997,493	3	0	11 s ago	+259 ms	402 ms	100%

Slater Technologies

Source: https://www.rinkeby.io/#stats

Bitcoin vs. Ethereum



VS	Bitcoin	Ethereum
Founder	Satoshi Nakamoto	Vitalik Buterin
Release Date	9 Jan 2008	30 July 2015
Release Method	Genesis Block Mined	Presale
Blockchain	Proof of work	Proof of work (Planning for POS)
Useage	Digital Currency	Smart Contracts Digital Currency
Cryptocurrency Used	Bitcoin(Satoshi)	Ether
Algorithm	SHA-256	Ethash
Blocks Time	10 Mintues	12-14 Seconds
Mining	ASIC miners	GPUs
Scalable	Not now	Yes

Important Architecture Decision

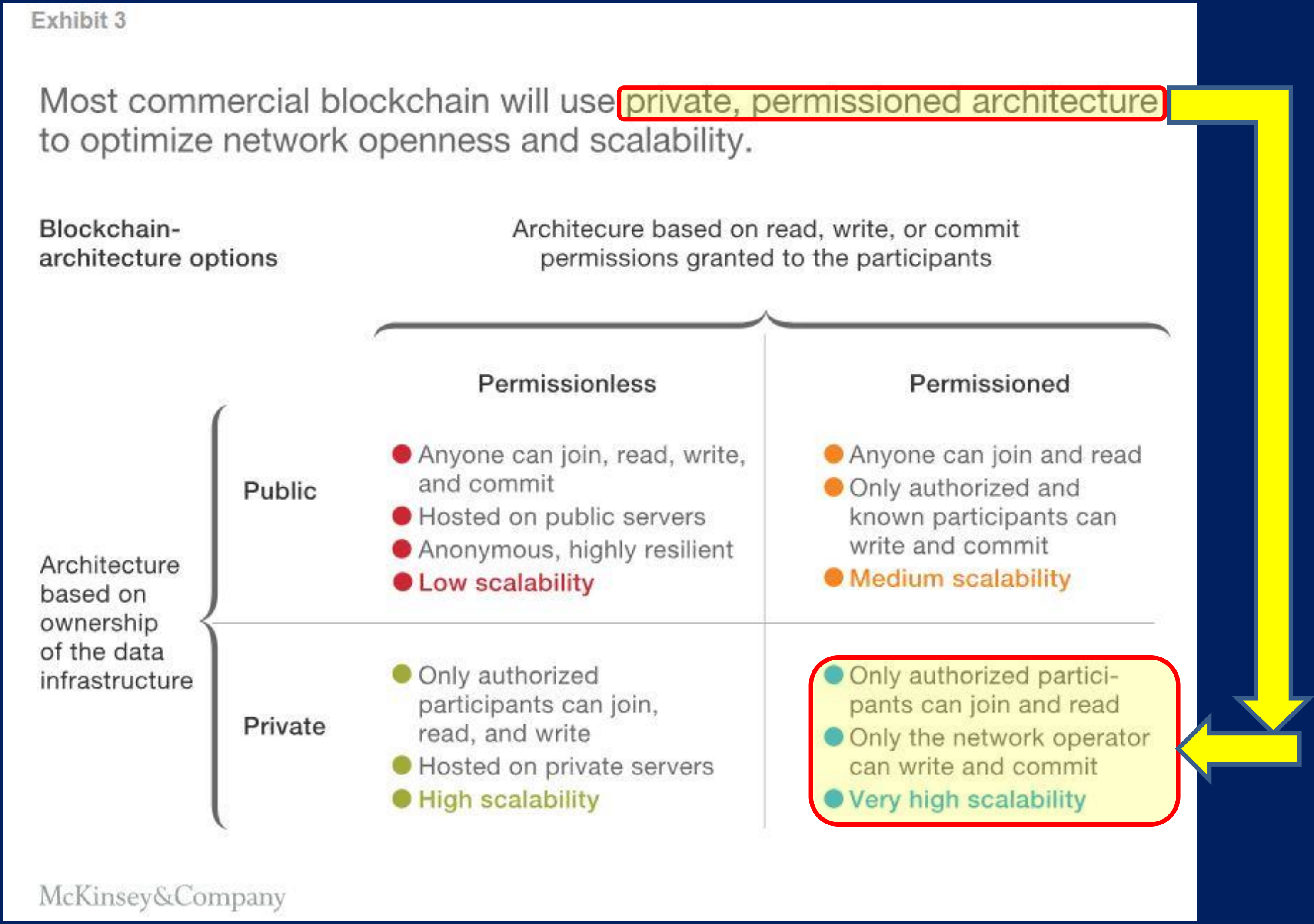


Exhibit 3

Most commercial blockchain will use private, permissioned architecture to optimize network openness and scalability.

Blockchain-architecture options

Architecure based on read, write, or commit permissions granted to the participants

Architecture based on ownership of the data infrastructure

	Permissionless	Permissioned
Public	● Anyone can join, read, write, and commit ● Hosted on public servers ● Anonymous, highly resilient ● **Low scalability**	● Anyone can join and read ● Only authorized and known participants can write and commit ● **Medium scalability**
Private	● Only authorized participants can join, read, and write ● Hosted on private servers ● **High scalability**	● Only authorized participants can join and read ● Only the network operator can write and commit ● **Very high scalability**

McKinsey&Company

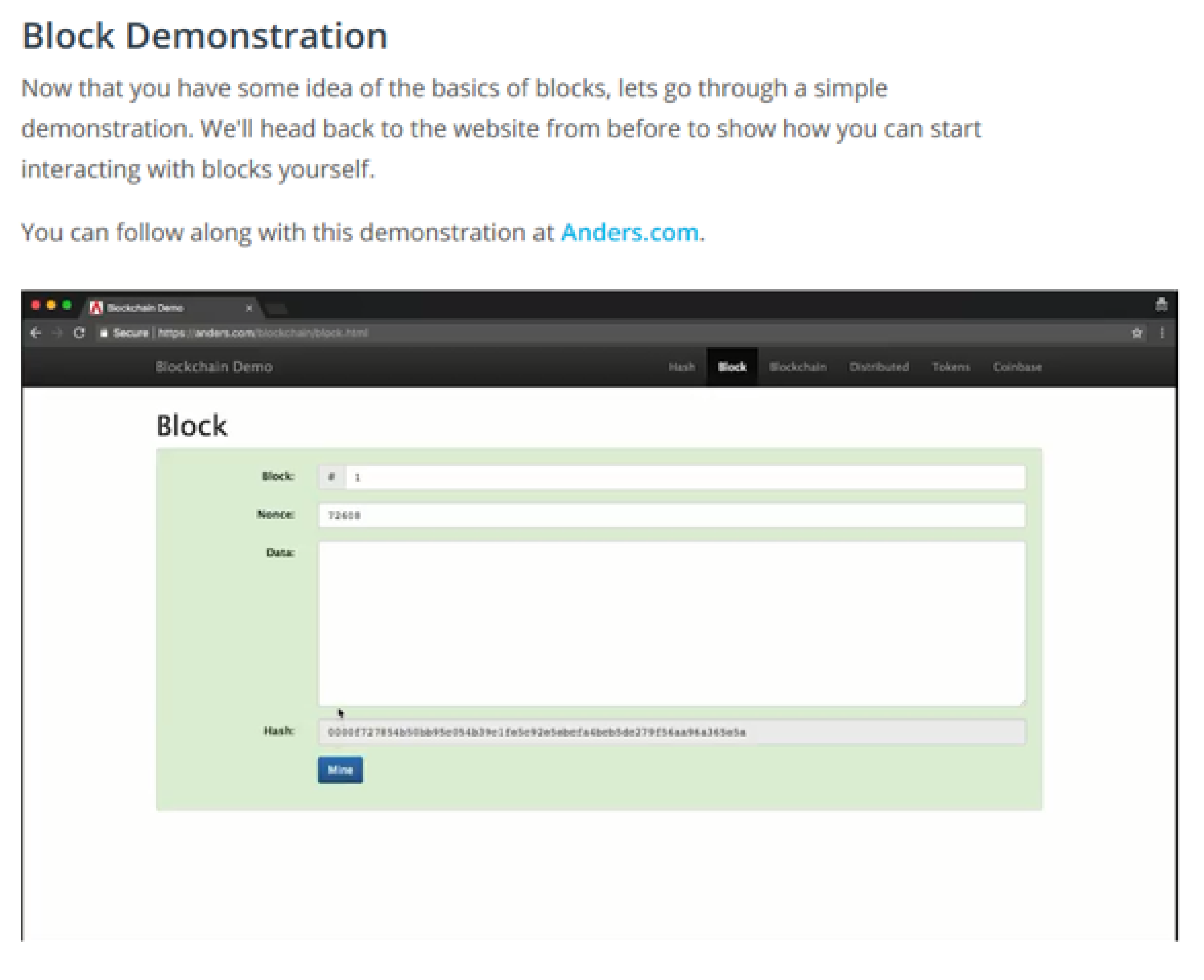
Source: McKinsey & Company 2017

Slater Technologies

DEMOS FROM ANDERS.COM

Slater Technologies

Blockchain – Simple Demonstration



Block Demonstration

Now that you have some idea of the basics of blocks, lets go through a simple demonstration. We'll head back to the website from before to show how you can start interacting with blocks yourself.

You can follow along with this demonstration at Anders.com.

Block

Block: # 1

Nonce: 72608

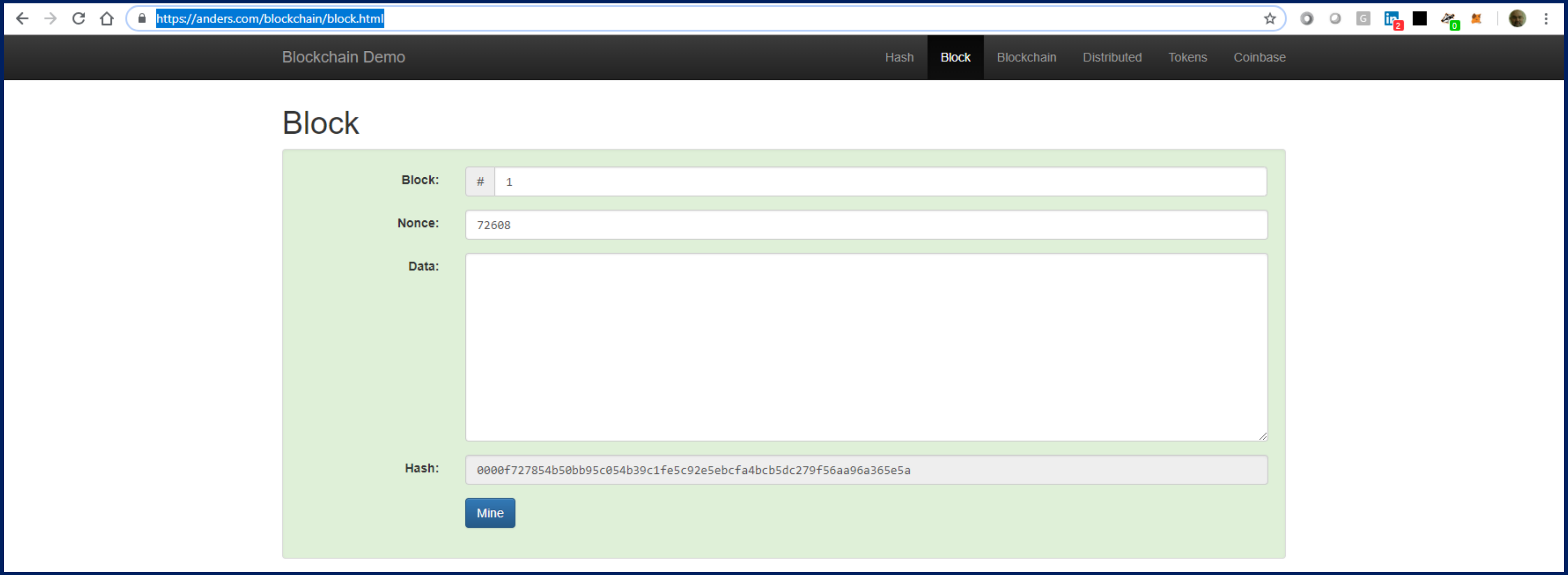
Data:

Hash: 0000f727854b50bb95e054b39e1fe5e92e5ebefa4beb5de279f56aa96a365e5a

Source: Udacity Blockchain Developer Course

Slater Technologies

Blockchain – Simple Demonstration



Block

Block: # 1

Nonce: 72608

Data:

Hash: 0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

Source: https://anders.com/blockchain/block.html

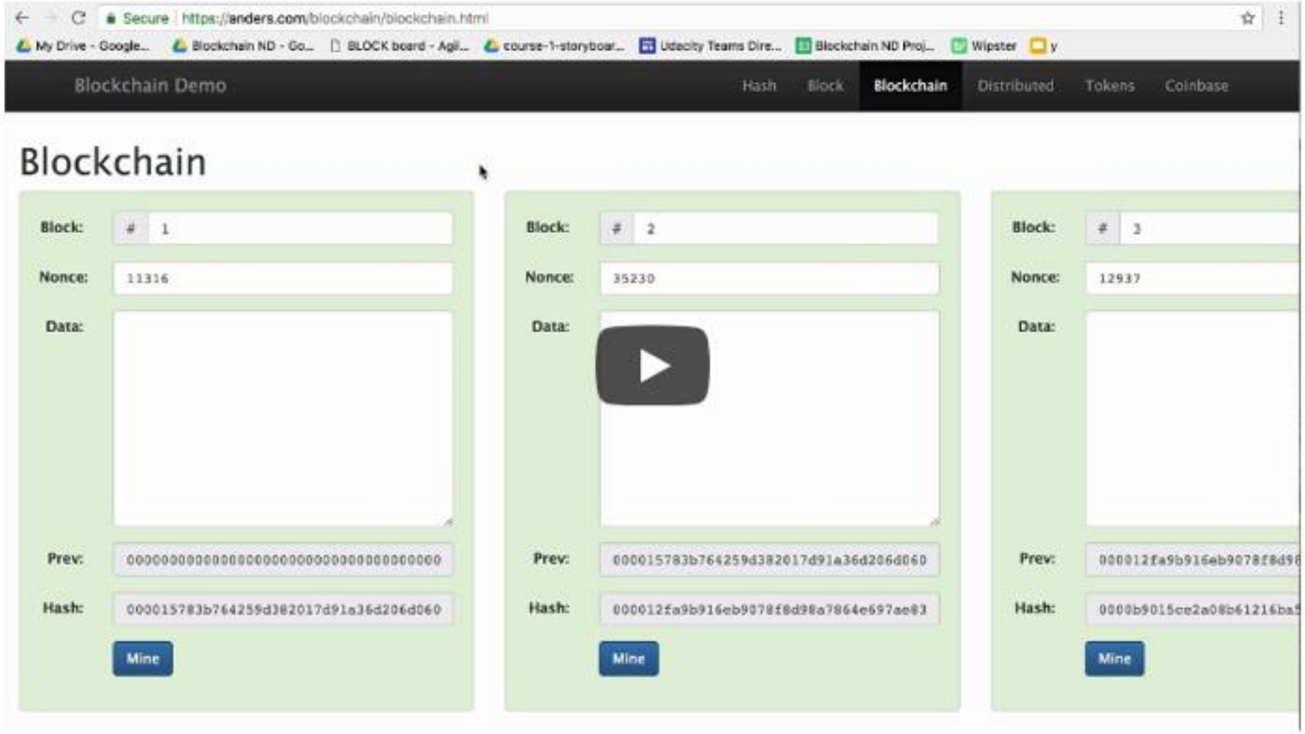
Slater Technologies

Blockchain – Simple Demonstration

Blockchain Demo

Now that you have a better understanding of the basics of blockchains, let's go through another demonstration. This expands on our demonstrations from earlier to allow you to interact with the basic ideas of the blockchain.

You can follow along with this demonstration at Anders.com.



Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d060

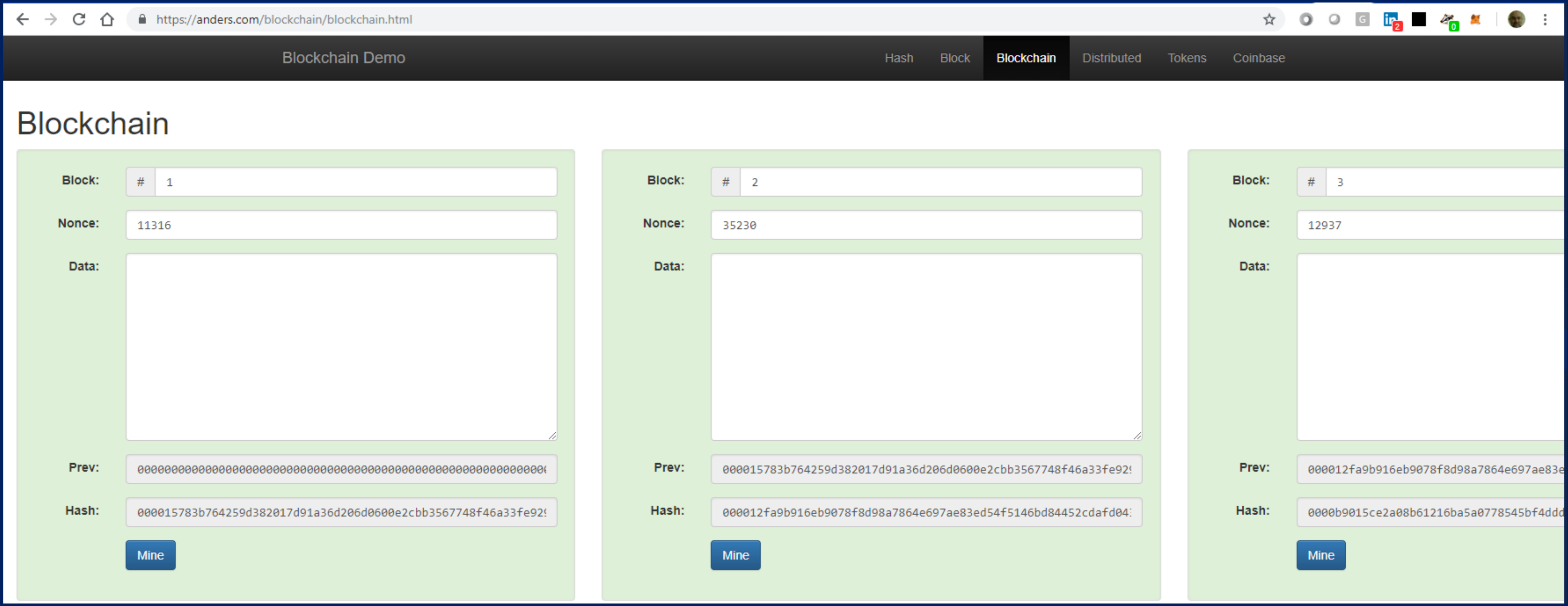
Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d060
Hash: 000012fa9b916eb9078f8d98a7864e697ae83

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98
Hash: 0000b9015ce2a08b61216ba5

Source: Udacity Blockchain Developer Course

Slater Technologies

Blockchain – Simple Demonstration



Blockchain

Block: # 1

Nonce: 11316

Data:

Prev: 000000000000000000000000000000000000000000000000000000000000

Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe92

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe92

Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd04

Mine

Block: # 3

Nonce: 12937

Data:

Prev: 000012fa9b916eb9078f8d98a7864e697ae83e

Hash: 0000b9015ce2a08b61216ba5a0778545bf4ddd

Mine

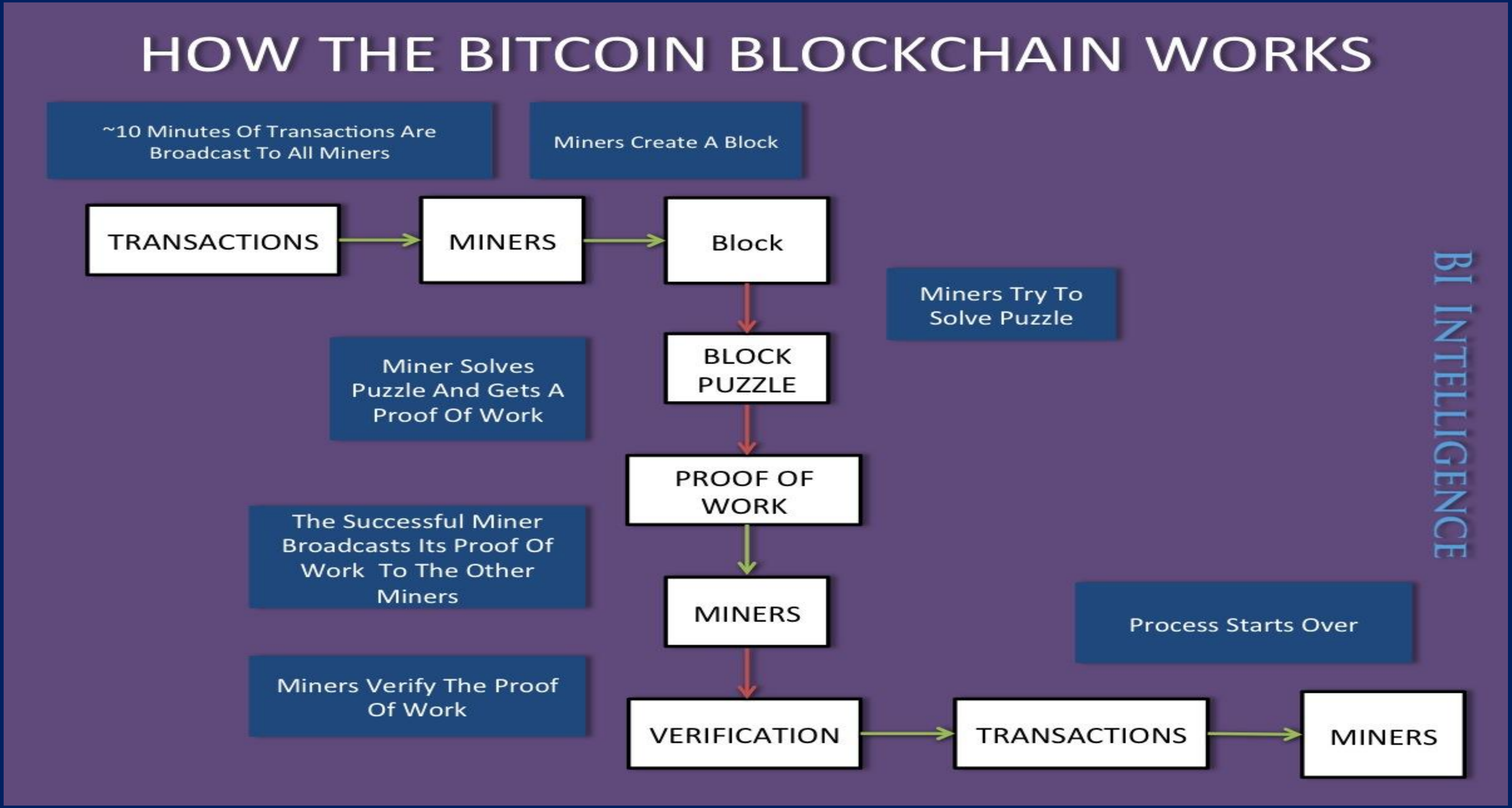
Source: https://anders.com/blockchain/block.html

Slater Technologies

HOW DOES BLOCKCHAIN WORK?

Slater Technologies

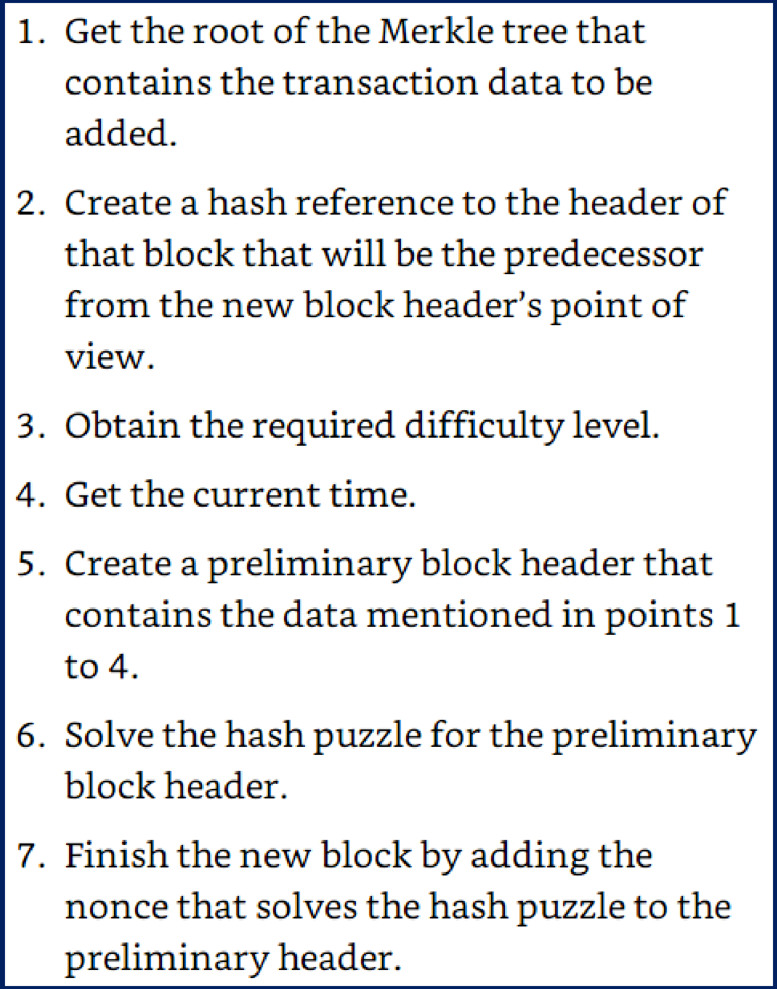
How Does a Blockchain Work?


HOW THE BITCOIN BLOCKCHAIN WORKS
~10 Minutes Of Transactions Are Broadcast To All Miners
Miners Create A Block
TRANSACTIONS
MINERS
Block
Miners Try To Solve Puzzle
Miner Solves Puzzle And Gets A Proof Of Work
BLOCK PUZZLE
PROOF OF WORK
BI INTELLIGENCE
The Successful Miner Broadcasts Its Proof Of Work To The Other Miners
MINERS
Process Starts Over
Miners Verify The Proof Of Work
VERIFICATION
TRANSACTIONS
MINERS

Source: BI Intelligence

Slater Technologies

Mining Principles: Block Creation



1. Get the root of the Merkle tree that contains the transaction data to be added.
2. Create a hash reference to the header of that block that will be the predecessor from the new block header's point of view.
3. Obtain the required difficulty level.
4. Get the current time.
5. Create a preliminary block header that contains the data mentioned in points 1 to 4.
6. Solve the hash puzzle for the preliminary block header.
7. Finish the new block by adding the nonce that solves the hash puzzle to the preliminary header.

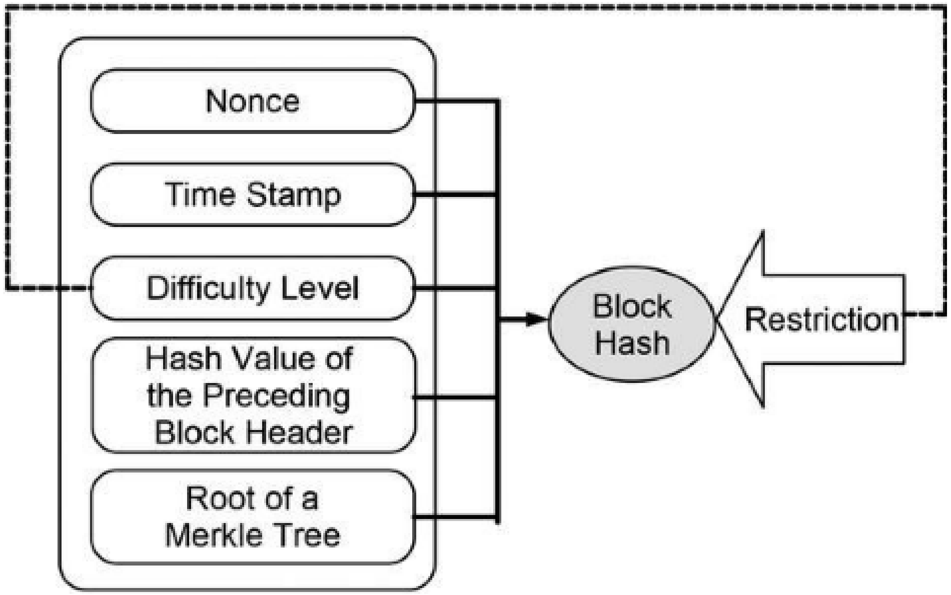


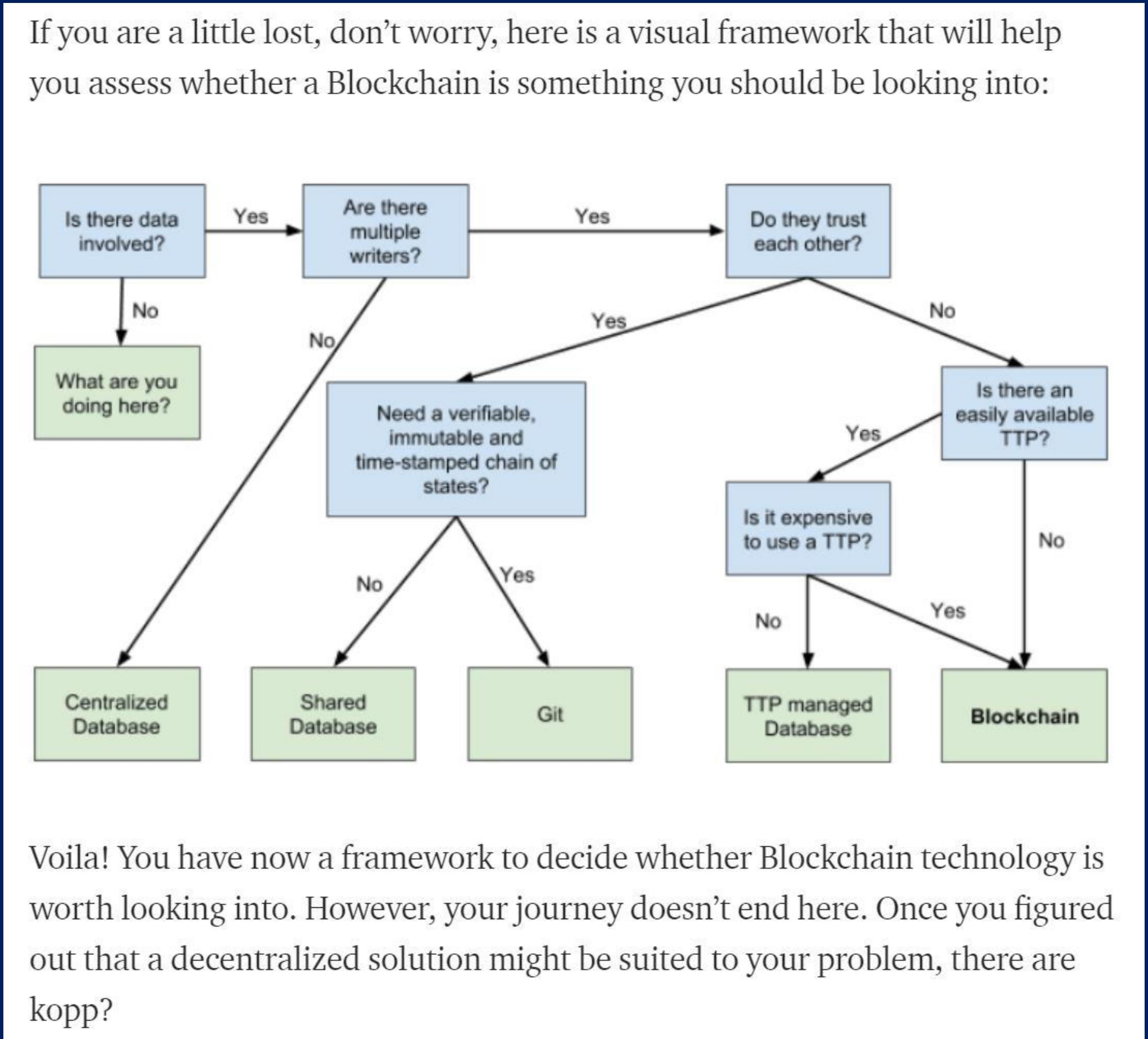
Figure 16-1. *Schematic illustration of the hash puzzle required to be solved when adding a new block to the blockchain-data- structure*

Special Note: Many other Blockchains, including Ethereum, apply these same principles.

Slater Technologies

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Why Blockchain?



If you are a little lost, don't worry, here is a visual framework that will help you assess whether a Blockchain is something you should be looking into:

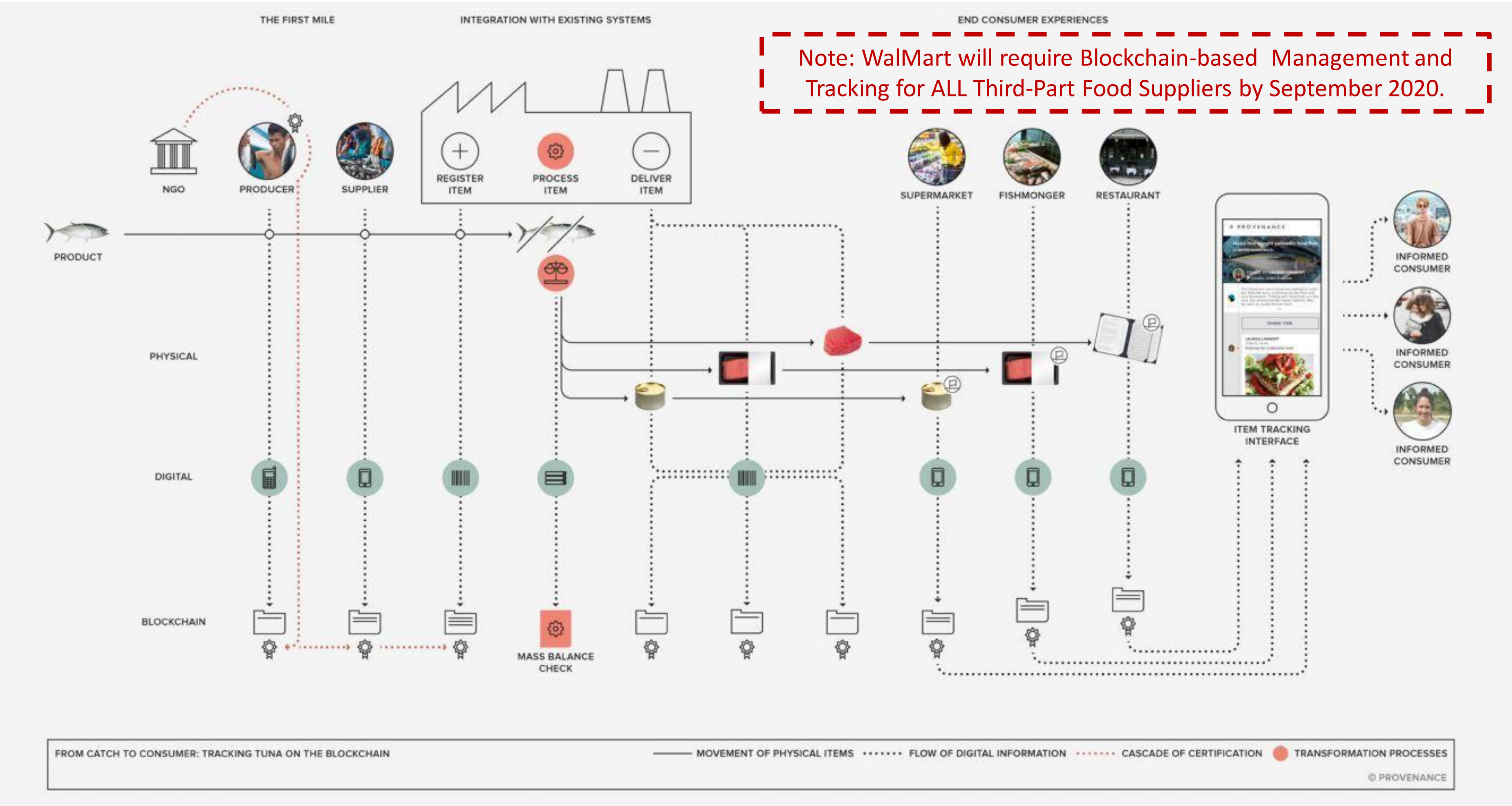
Is there data involved?
Yes
No
What are you doing here?
Are there multiple writers?
Yes
No
Centralized Database
Do they trust each other?
Yes
No
Need a verifiable, immutable and time-stamped chain of states?
No
Yes
Shared Database
Git
Is there an easily available TTP?
Yes
No
Is it expensive to use a TTP?
No
Yes
TTP managed Database
Blockchain

Voila! You have now a framework to decide whether Blockchain technology is worth looking into. However, your journey doesn't end here. Once you figured out that a decentralized solution might be suited to your problem, there are kopp?

Source: To Blockchain or not to Blockchain? https://medium.com/causys/to-blockchain-or-not-to-blockchain-aed05bf08150 Hats off to the author, Thomas Ferry of Causys

Slater Technologies

Blockchain Enhances Supply Chain Management

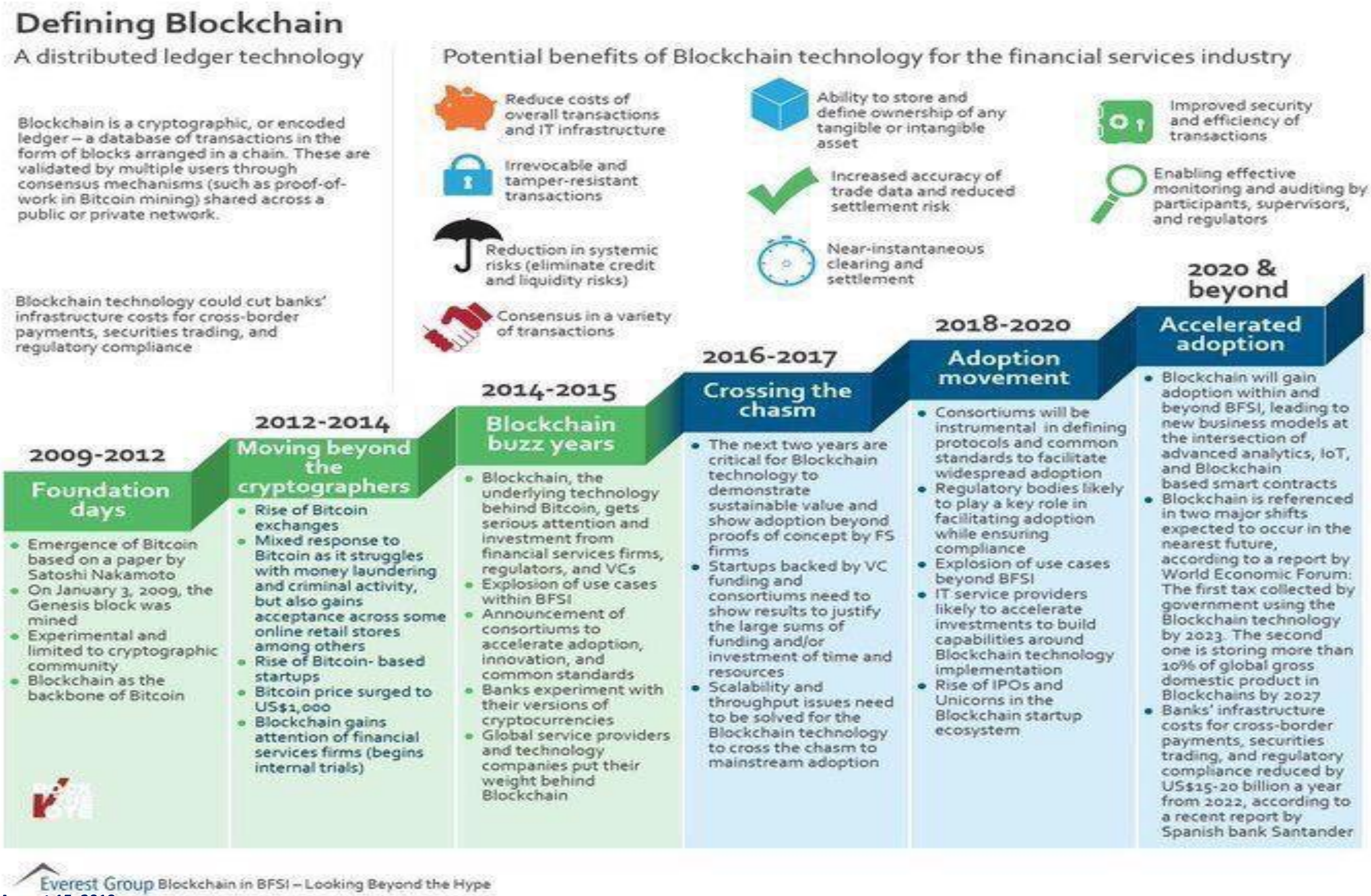


Note: WalMart will require Blockchain-based Management and Tracking for ALL Third-Part Food Suppliers by September 2020.

Figure 1: This chart shows how Provenance uses blockchain technology to not only permanently record certifications of supply chain data for tuna (up through sale), but also those of the participating NGOs tasked with ensuring the catch is slavery-free. (Source: Provenance)

Source: Provenance – Using Blockchain to Manage the Supply Chain

Blockchain Use Evolution



Defining Blockchain

A distributed ledger technology

Blockchain is a cryptographic, or encoded ledger – a database of transactions in the form of blocks arranged in a chain. These are validated by multiple users through consensus mechanisms (such as proof-of-work in Bitcoin mining) shared across a public or private network.

Blockchain technology could cut banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance

Potential benefits of Blockchain technology for the financial services industry

- Reduce costs of overall transactions and IT infrastructure
- Irrevocable and tamper-resistant transactions
- Reduction in systemic risks (eliminate credit and liquidity risks)
- Consensus in a variety of transactions
- Ability to store and define ownership of any tangible or intangible asset
- Increased accuracy of trade data and reduced settlement risk
- Near-instantaneous clearing and settlement
- Improved security and efficiency of transactions
- Enabling effective monitoring and auditing by participants, supervisors, and regulators

2009-2012
Foundation days

- Emergence of Bitcoin based on a paper by Satoshi Nakamoto
- On January 3, 2009, the Genesis block was mined
- Experimental and limited to cryptographic community
- Blockchain as the backbone of Bitcoin

2012-2014
Moving beyond the cryptographers

- Rise of Bitcoin exchanges
- Mixed response to Bitcoin as it struggles with money laundering and criminal activity, but also gains acceptance across some online retail stores among others
- Rise of Bitcoin- based startups
- Bitcoin price surged to US$1,000
- Blockchain gains attention of financial services firms (begins internal trials)

2014-2015
Blockchain buzz years

- Blockchain, the underlying technology behind Bitcoin, gets serious attention and investment from financial services firms, regulators, and VCs
- Explosion of use cases within BFSI
- Announcement of consortiums to accelerate adoption, innovation, and common standards
- Banks experiment with their versions of cryptocurrencies
- Global service providers and technology companies put their weight behind Blockchain

2016-2017
Crossing the chasm

- The next two years are critical for Blockchain technology to demonstrate sustainable value and show adoption beyond proofs of concept by FS firms
- Startups backed by VC funding and consortiums need to show results to justify the large sums of funding and/or investment of time and resources
- Scalability and throughput issues need to be solved for the Blockchain technology to cross the chasm to mainstream adoption

2018-2020
Adoption movement

- Consortiums will be instrumental in defining protocols and common standards to facilitate widespread adoption
- Regulatory bodies likely to play a key role in facilitating adoption while ensuring compliance
- Explosion of use cases beyond BFSI
- IT service providers likely to accelerate investments to build capabilities around Blockchain technology implementation
- Rise of IPOs and Unicorns in the Blockchain startup ecosystem

2020 & beyond
Accelerated adoption

- Blockchain will gain adoption within and beyond BFSI, leading to new business models at the intersection of advanced analytics, IoT, and Blockchain based smart contracts
- Blockchain is referenced in two major shifts expected to occur in the nearest future, according to a report by World Economic Forum: The first tax collected by government using the Blockchain technology by 2023. The second one is storing more than 10% of global gross domestic product in Blockchains by 2027
- Banks' infrastructure costs for cross-border payments, securities trading, and regulatory compliance reduced by US$15-20 billion a year from 2022, according to a recent report by Spanish bank Santander

Everest Group Blockchain in BFSI – Looking Beyond the Hype

Blockchain Use Cases in Business

Non-Financial Use Cases

Digital Content/Documents, Storage & Delivery

BitProof, Blockcai, Ascribe, ArtPlus, Chainy.Link, Stampery, Blocktech (Alexandria), Bisantyum, Blockparti, The Rudimental, BlockCDN

Authentication & Authorization

The Real McCoy, Degree of Trust, Everpass, BlockVerify,

Digital Identity

Sho Card, Uniquid, Onename, Trustatom

Marketplace

Providing premium rights & brand based coins: MyPowers

Smart Contracts

Otonomos, Mirror, Symbiont, New system Technologies

Real Estate

Factom

Diamonds

Everledger

Gold & Silver

BitShares, Real Asset Co., DigitalTangible (Serica), Bit Reserve

Reviews/Endorsement

TRST.im, Asimov (recruitment services), The World Table

Blockchain in IoT

Filament, Chimera-inc.io, ken Code – ePlug

App Development

Proof of ownership for modules in app development: Assembly

Network Infrastructure & APIs

Ethereum, Eris, Codius, NXT, Namecoin, Colored Coins, Hello Block, Counterparty, Mastercoin, Corona, Chromaway, BlockCypher

Other

Prediction platform: Augur

Election Voting: Follow My Vote

Patient Records management: BitHealth

Financial Use Cases

Currency Exchange & Remittance

Coinbase (Wallet), BitPesa, Billion, Ripple, Stellar, Kraken, Fundrs.org, MeXBT, CryptoSigma

P2P Transfers

BTC Jam, Codius, BitBond, BitnPlay (Donation), DeBuNe (SME's B2B transactions)

Ride Sharing

La'zooz

Data Storage

Storj.io, Peernova

Trading Platforms

equityBits, Spritzle, Secure Assets, Coins-e, DXMarkets, MUNA, Kraken, BitShares

Gaming

PlayCoin, Play(on DACx platform), Deckbound

Slater Technologies

Latest Blockchain News

Real-World Blockchain Solutions

Entity	Use	Blockchain(s)	Link
Maersk	Expedite tracking of Cargo shipment internationally	Hyperledger	https://www.ibm.com/blogs/think/2018/11/tradelens-how-ibm-and-maersk-are-sharing-blockchain-to-build-a-global-trade-platform/
U.S. State Department & Coca-Cola	Reduce risk of forced labor and child labor	Customized	https://www.digitaltrends.com/cool-tech/coca-cola-blockchain-forced-labor/
Saudi Arabia	Tracking cross-border trade	Hyperledger	https://cointelegraph.com/news/saudi-arabia-completes-ibm-tradelens-pilot-for-cross-border-blockchain-trade
Overstock	Business model change from online retail to investor in Blockchain and Cryptocurrency Start-ups	Several	https://mashable.com/article/overstock-blockchain-cryptocurrency/
Walmart	Requiring several fresh food suppliers to use Blockchain	Several	https://cointelegraph.com/news/walmart-requires-certain-produce-suppliers-to-deploy-blockchain-technology
FedEx	Supply chain and logistics management improvements.	Hyperledger	https://cointelegraph.com/news/fedex-joins-hyperledger-blockchain-hub-big-implications-for-logistics

Slater Technologies

Blockchain Security

Slater Technologies

3 Important Things Business Leaders Need to Know About Blockchain Security

- 1. Security is not just a technical problem, it is a leadership problem
- 2. Exploitation is not just a result of attacker capabilities, but also of developer errors
- 3. While attackers do compromise a blockchain itself, they more commonly exploit the configuration of the technology leveraging a blockchain

Source: Alison DeNisco Ramone, TechRepublic.com, April 18, 2019
https://www.techrepublic.com/article/how-to-secure-a-blockchain-3-things-business-leaders-need-to-know/

Slater Technologies

How to Secure Blockchain Applications and Infrastructure

- Build and lead Teams of experienced, dedicated workers
- Design securely
- Do code reviews and rigorous testing
- Implement securely
- Document ***everything***
- Test security
    - Routinely test vulnerabilities (at least quarterly)
        - https://tinyurl.com/y292y3yf
    - Penetration test semi-annually
        - https://tinyurl.com/yya4vtac
    - Test and document performance
        - https://tinyurl.com/yxpwszj7
- Do Threat Management
- Continuously review for upgrading

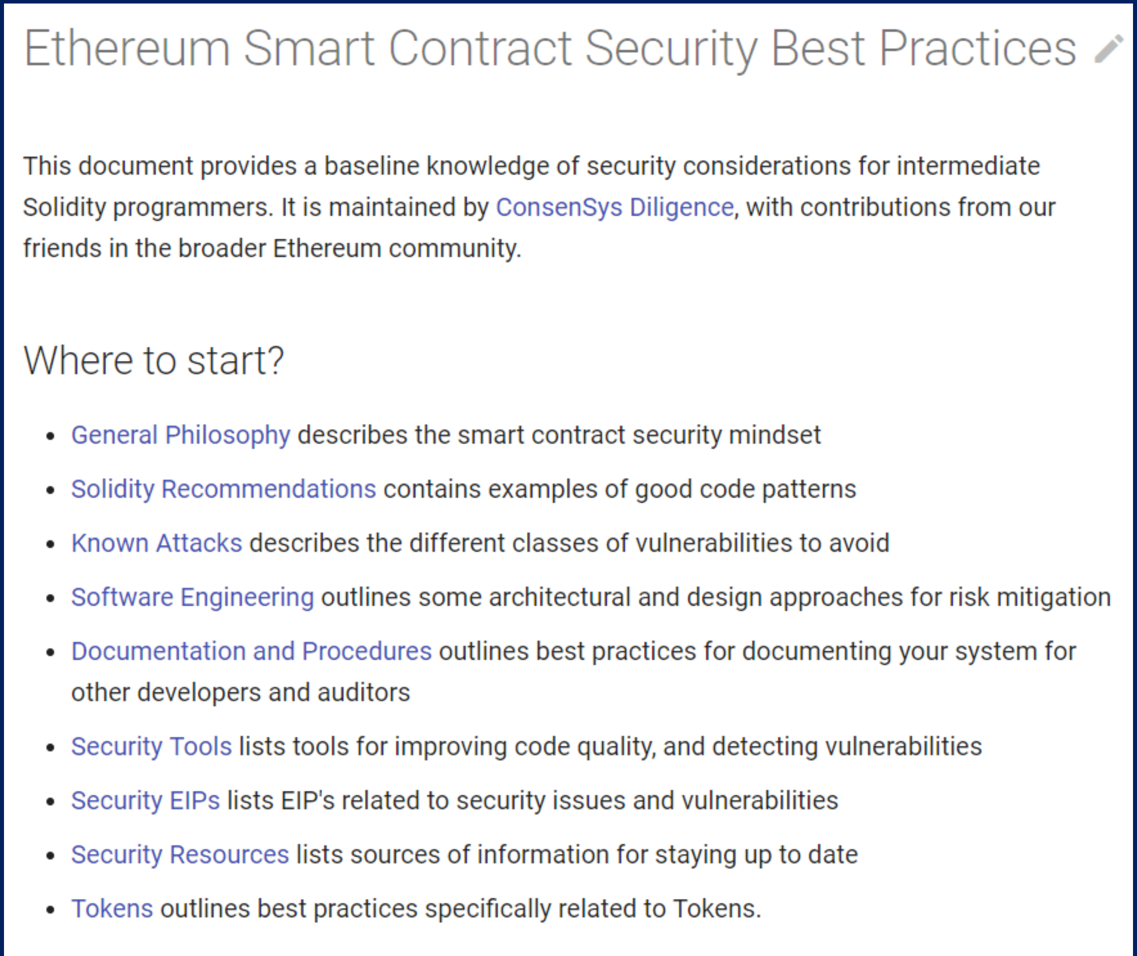
Slater Technologies

How to Perform Secure Software Development for Blockchain Applications by Design, Coding Practices, Testing and Verification

- Experienced DApp developers
- Test-driven Development
- Code Defensively
- Code reviews, by multiple experienced developers
- Understand and remediate the weakest security points, especially protection of private keys and sensitive data.
- Implement the tests on test net and understand exactly how the code will behave prior to moving to main net
- Automate Smart Contract testing when possible

Slater Technologies

Ethereum Smart Contract Security Best Practices



Ethereum Smart Contract Security Best Practices

This document provides a baseline knowledge of security considerations for intermediate Solidity programmers. It is maintained by ConsenSys Diligence, with contributions from our friends in the broader Ethereum community.

Where to start?

- General Philosophy describes the smart contract security mindset
- Solidity Recommendations contains examples of good code patterns
- Known Attacks describes the different classes of vulnerabilities to avoid
- Software Engineering outlines some architectural and design approaches for risk mitigation
- Documentation and Procedures outlines best practices for documenting your system for other developers and auditors
- Security Tools lists tools for improving code quality, and detecting vulnerabilities
- Security EIPs lists EIP's related to security issues and vulnerabilities
- Security Resources lists sources of information for staying up to date
- Tokens outlines best practices specifically related to Tokens.

Best Free Resources
On Smart Contract
Security
Best Practices

Smart Contract Security Best Practices
https://consensys.github.io/smart-contract-best-practices/

Slater Technologies

Blockchain Auditing

Blockchain and Auditing

- Blockchain Integrity and Security
- DApps
- Infrastructure
- Physical Security

Concepts of Auditing the Data and Transactions in Blockchain Data Structures

- Data should be validated and verified prior to committing as a Blockchain transaction because once written to the Blockchain it is ***immutable***.
- Sample transactions should be verified from the DApp as successfully written to the Blockchain.
- Use Blockchain Logs and Processing Events

Slater Technologies

AUTOMATING THE AUDITING OF BLOCKCHAINS AND BLOCKCHAIN APPLICATIONS

Slater Technologies

Automating the Auditing of Blockchains and Blockchain Applications

- In February 2018, ***Maian***, an open source tool to monitor Smart Contracts for being Greedy, Prodigal, or Suicidal was announced.

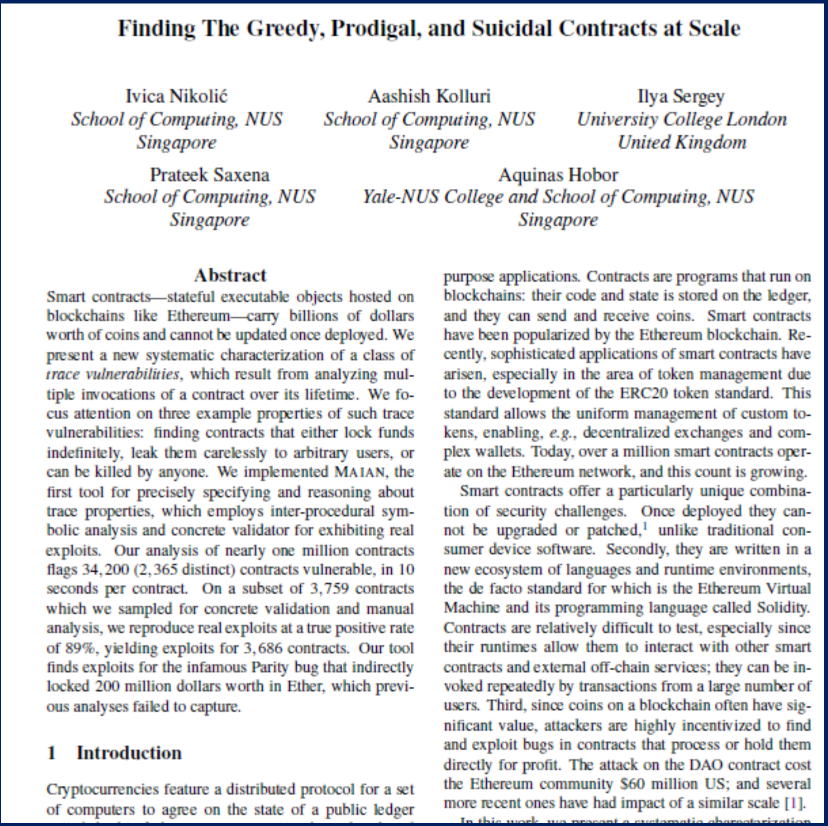
- As of April 2018, EY has Blockchain Auditing tools and technology.
  - https://www.ey.com/en_gl/news/2018/04/ey-announces-blockchain-audit-technology

- As of October 2018, How Big Four Auditors Delve Into Blockchain: PwC, Deloitte, EY and KPMG Approaches Compared
  - https://cointelegraph.com/news/how-big-four-auditors-delve-into-blockchain-pwc-deloitte-ey-and-kpmg-approaches-compared

AUTOMATING THE AUDITING OF BLOCKCHAINS WITH MAIAN

Slater Technologies

Maian: Auditing Smart Contracts at Scale



Finding The Greedy, Prodigal, and Suicidal Contracts at Scale

Ivica Nikolić
School of Computing, NUS
Singapore

Aashish Kolluri
School of Computing, NUS
Singapore

Ilya Sergey
University College London
United Kingdom

Prateek Saxena
School of Computing, NUS
Singapore

Aquinas Hobor
Yale-NUS College and School of Computing, NUS
Singapore

Abstract

Smart contracts—stateful executable objects hosted on blockchains like Ethereum—carry billions of dollars worth of coins and cannot be updated once deployed. We present a new systematic characterization of a class of *trace vulnerabilities*, which result from analyzing multiple invocations of a contract over its lifetime. We focus attention on three example properties of such trace vulnerabilities: finding contracts that either lock funds indefinitely, leak them carelessly to arbitrary users, or can be killed by anyone. We implemented MAIAN, the first tool for precisely specifying and reasoning about trace properties, which employs inter-procedural symbolic analysis and concrete validator for exhibiting real exploits. Our analysis of nearly one million contracts flags 34,200 (2,365 distinct) contracts vulnerable, in 10 seconds per contract. On a subset of 3,759 contracts which we sampled for concrete validation and manual analysis, we reproduce real exploits at a true positive rate of 89%, yielding exploits for 3,686 contracts. Our tool finds exploits for the infamous Parity bug that indirectly locked 200 million dollars worth in Ether, which previous analyses failed to capture.

1 Introduction

Cryptocurrencies feature a distributed protocol for a set of computers to agree on the state of a public ledger

purpose applications. Contracts are programs that run on blockchains: their code and state is stored on the ledger, and they can send and receive coins. Smart contracts have been popularized by the Ethereum blockchain. Recently, sophisticated applications of smart contracts have arisen, especially in the area of token management due to the development of the ERC20 token standard. This standard allows the uniform management of custom tokens, enabling, *e.g.*, decentralized exchanges and complex wallets. Today, over a million smart contracts operate on the Ethereum network, and this count is growing.

Smart contracts offer a particularly unique combination of security challenges. Once deployed they cannot be upgraded or patched,[1] unlike traditional consumer device software. Secondly, they are written in a new ecosystem of languages and runtime environments, the de facto standard for which is the Ethereum Virtual Machine and its programming language called Solidity. Contracts are relatively difficult to test, especially since their runtimes allow them to interact with other smart contracts and external off-chain services; they can be invoked repeatedly by transactions from a large number of users. Third, since coins on a blockchain often have significant value, attackers are highly incentivized to find and exploit bugs in contracts that process or hold them directly for profit. The attack on the DAO contract cost the Ethereum community $60 million US; and several more recent ones have had impact of a similar scale [1].

In this work, we present a systematic characterization

February 2018 Technical paper about flaws in How Ethereum and EVM handle Smart Contracts. Worth your time

Prodigal - Leak them carelessly to arbitrary users

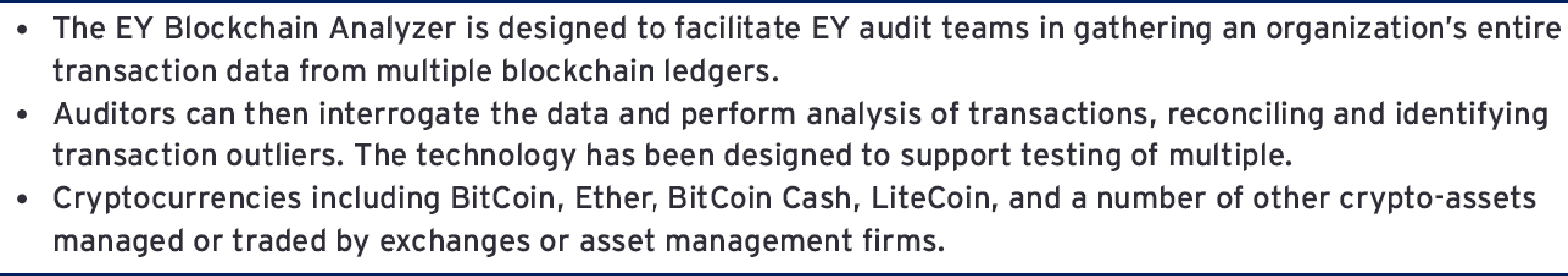
Suicidal - Can be killed by anyone

Greedy - Lock funds Indefinitely

Source:
https://www.reddit.com/r/Bitcoin/comments/7ys5nq/pdf_finding_the_greedy_prodigal_and_suicidal/

Slater Technologies

EY has a new Tool, Blockchain Analyzer with the Capability to Automate the Auditing of Blockchain Applications

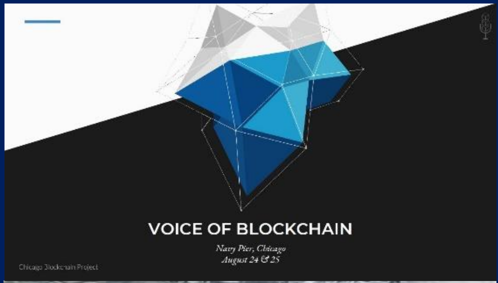


- The EY Blockchain Analyzer is designed to facilitate EY audit teams in gathering an organization's entire transaction data from multiple blockchain ledgers.
- Auditors can then interrogate the data and perform analysis of transactions, reconciling and identifying transaction outliers. The technology has been designed to support testing of multiple.
- Cryptocurrencies including BitCoin, Ether, BitCoin Cash, LiteCoin, and a number of other crypto-assets managed or traded by exchanges or asset management firms.

Slater Technologies

Conclusion

Conclusion

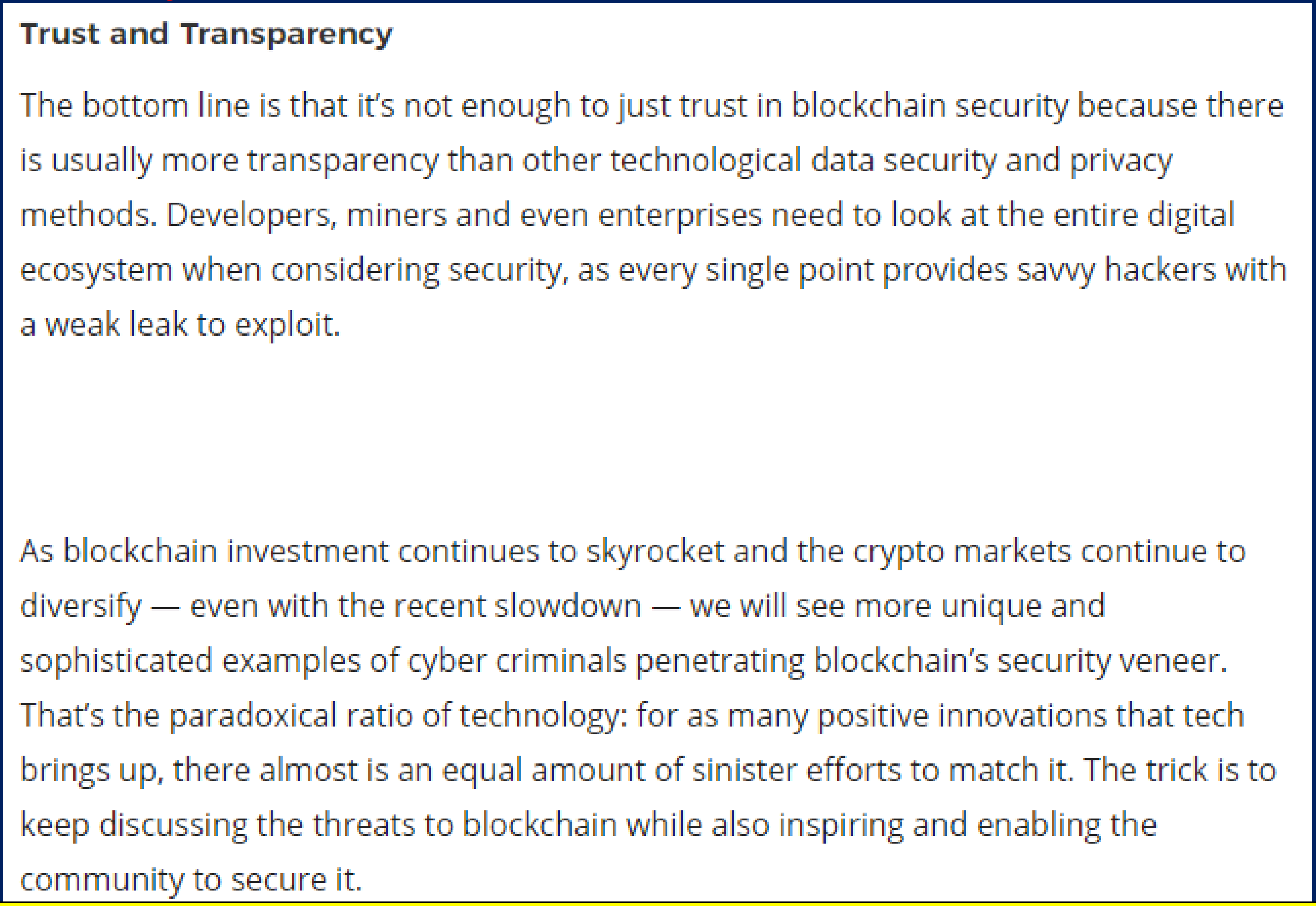


So we covered:

- Why Blockchain Is Important?
- What Is Blockchain?
- Why Blockchain?
- Latest Blockchain News
- Blockchain Security
- Blockchain Auditing

Conclusion

From James Nguyen
February 12, 2019



Trust and Transparency

The bottom line is that it's not enough to just trust in blockchain security because there is usually more transparency than other technological data security and privacy methods. Developers, miners and even enterprises need to look at the entire digital ecosystem when considering security, as every single point provides savvy hackers with a weak leak to exploit.

As blockchain investment continues to skyrocket and the crypto markets continue to diversify — even with the recent slowdown — we will see more unique and sophisticated examples of cyber criminals penetrating blockchain's security veneer. That's the paradoxical ratio of technology: for as many positive innovations that tech brings up, there almost is an equal amount of sinister efforts to match it. The trick is to keep discussing the threats to blockchain while also inspiring and enabling the community to secure it.

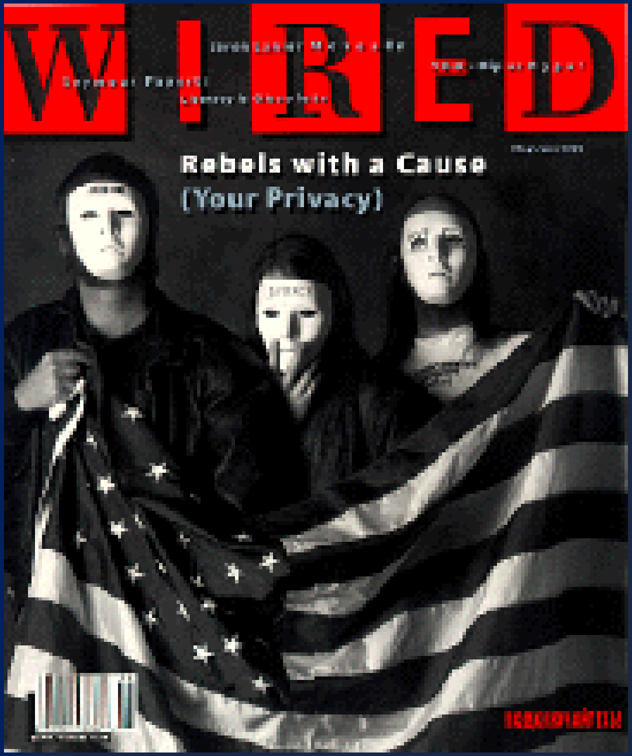
Source: **Blockchain still vulnerable to hacks despite security hype, but here are some solutions by James Nguyen.**
Retrieved from https://e27.co/blockchain-still-vulnerable-to-hacks-despite-security-hype-but-here-are-some-solutions-20190212/ -

Slater Technologies

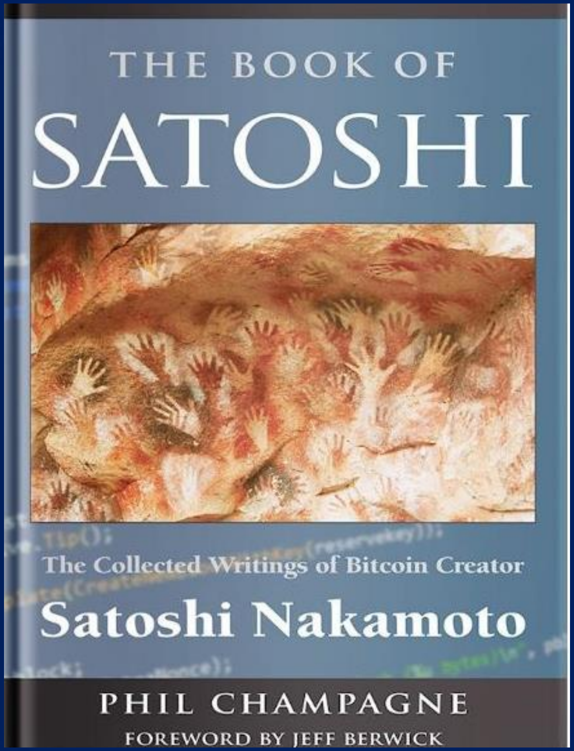
Questions?

Slater Technologies

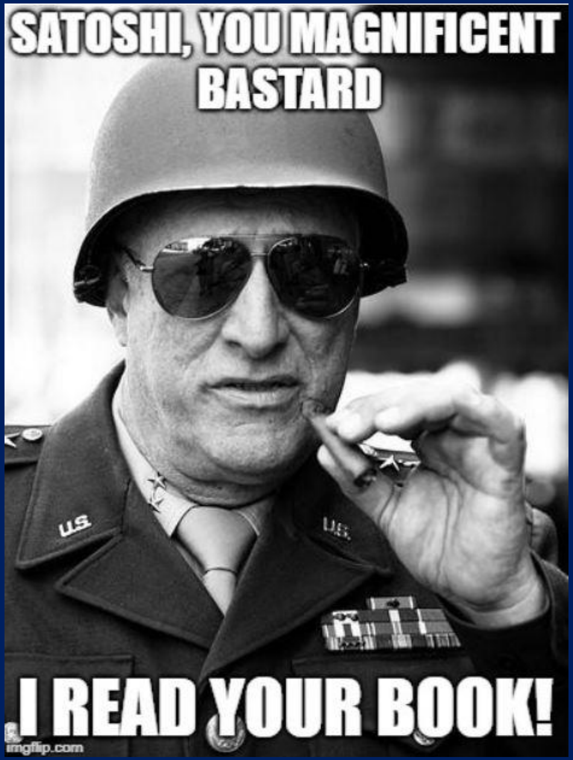
Questions?



Crypto Rebels
Revealed
Wired Magazine,
February 1993



Book of Satoshi
Collected Writings
Of Satoshi Nakamoto



General George S. Patton

Slater Technologies

References

References

- Antonopoulos, A. M. (2018). Mastering Bitcoin: Programming the Open Blockchain, second edition. Sebastopol, CA: O’Reilly Media, Inc.
- Antonopoulos, A. M. and Wood, G. (2019). Mastering Ethereum: Building Smart Contract sand DApps. Sebastopol, CA: O’Reilly Media, Inc.
- Associated Press. (2014). Mt. Gox finds 200,000 missing bitcoins. Retrieved from http://money.msn.com/business-news/article.aspx?feed=AP&date=20140321&id=17454291 on March 21, 2014.
- 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.
- BBC. (2014). Troubled MtGox Bitcoin boss emerges after shut down Retrieved from http://www.bbc.com/news/technology-26352442 on February 26, 2014.
- Bitcoin.org. (2014). Bitcoin.org FAQs.. Retrieved from https://bitcoin.org/en/faq on April 10, 2014.
- Bitcoin Scammers. (2014). Bitcoin Scammers. Retrieved from http://bitcoinscammers.com/ on April 9, 2014.
- Blockchain Training Alliance. (2019). Global Blockchain Terms, version 2.0. Retrieved from https://cdn.shopify.com/s/files/1/2137/1081/files/BTA_Global_Blockchain_Terms.pdf?2499 on August 14, 2019 .
- 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.
- Caughey, M. (2013). Bitcoin Step by Step, second edition. Amazon Digital Services.

Slater Technologies

References

- 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.
- De Havilland, P. (2018). Greedy, Prodigal, and Suicidal — Hosho to Save Smart Contracts From Three Deadly Sins. An article published at Bitsonline.com on September 3, 2018. Retrieved from https://bitsonline.com/greedy-prodigal-suicidal-hosho-smart-contracts/ on February 27, 2019.
- 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.
- Etwaru, R. (2017). Blockchain Trust Companies. Indianapolis, IN: Dog Ear Publishing.
- Ferry, T. (2019). To Blockchain or not to Blockchain. An article publsihed at Medium.com on June 8, 2018. Retrieved on January 13, 2019 from https://medium.com/causys/to-blockchain-or-not-to-blockchain-aed05bf08150 .
- Gerard, D. (2107), Attack of the 50 Foot Blockchain: Bitcoin, Blockchain, Ethereum, and Smart Contracts. Published by David Gerard. www.davidgerard.co.uk/blockchain .
- GreenBerg, A. (2019). A BlockchainBandit Is Guessing Private Keys and Scoring Millions, An article published on April 23, 2019 at Wired.com and retrieved from https://www.wired.com/story/blockchain-bandit-ethereum-weak-private-keys/ on April 23, 2019.

References

- Hornyak, T. (2014). 'Malleability' attacks not to blame for Mt. Gox's missing bitcoins, study says. Retrieved from http://www.pcworld.com/article/2114200/malleability-attacks-not-to-blame-for-mt-goxs-missing-bitcoins-study-says.html on March 27, 2014.
- Incencio, R. (2014). Ransomware and Bitcoin Theft Combine in BitCrypt. Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-and-bitcoin-theft-combine-in-bitcrypt/ on March 27, 2014.
- 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.
- Ma, M. (2017). Blockchain Design Sprint: An Agile Innovation Workbook to Implement an Agile Design Sprint for your Blockchain Business. Published by Future Lab www.futurelabconsulting.com .
- Markowitz, E. (2014). Cryptocurrencies Are the New Spam Frontier. Retrieved from http://www.vocativ.com/tech/bitcoin/cryptocurrencies-new-spam-frontier/ on March 28, 2014.
- Nakamoto. S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf on November 1, 2013.
- Nguyen, J. (2019). Blockchain still vulnerable to hacks despite security hype, but here are some solutions. Retrieved from https://e27.co/blockchain-still-vulnerable-to-hacks-despite-security-hype-but-here-are-some-solutions-20190212/ on February 13, 2019.
- O'Ham, T. (2018). Singapore Research Team Codifies 3 new Ethereum VM Vulnerabilities. An article published at Bitsonline.com on February 21, 2018. Retrieved from https://bitsonline.com/singapore-research-ethereum/ on February 27, 2019.
- Orcutt, M. (2019). Once Hailed as Unhackable, Blockchains Are now Getting Hacked. An article in MIT Review. Published February 19, 2019. Retrieved from https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ on February 24, 2019.

Slater Technologies

References

- Popper, N. (2013). Into the Bitcoin Mines, Retrieved from http://dealbook.nytimes.com/2013/12/21/into-the-bitcoin-mines/?hp&_r=0 on December 21, 2013.
- Prusty, N. (2017). Building Blockchain Projects: Building Decentralized Blockchain Applications with Ethereum and Solidity. Birmingham, UK: Pact Publishing.
- Ramone, A. D. (2019). How to Secure a Blockchain: 3 Things Business Leaders Know. An article publisged at Techrepublic.com on April 18, 2019. Retrieved from https://www.techrepublic.com/article/how-to-secure-a-blockchain-3-things-business-leaders-need-to-know/ on April 23, 2019.
- 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.
- Sharkey, T. (2014. Inside Bitcoins NYC Day 1: Bitcoin 2.0 Takes Center Stage. Retrieved from http://www.coindesk.com/inside-bitcoins-nyc-day-1-bitcoin-2-0-takes-center-stage/ on April 8, 2014.
- Smith, B. (2019). The Evolution of Cryptocurrency in Terrorism. Retrieved from Blockchain Training Alliance. (2019). Global Blockchain Terms, version 2.0. Retrieved on August 14, 2019 from https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/ on Augus 10, 2019.
- Zenko, M. (2017). Bitcoins for Bombs – a Blog published at the Council on Foreign Relations on August 17, 2017. Retrieved from https://www.cfr.org/blog/bitcoin-bombs on February 13, 2019.

References – The Best Blockchain Books

- **Mastering Ethereum**
  - by Andreas M. Antonopoulos and Dr. Gavin Wood
- **Blockchain Applications: A Hands-On Approach**
  - by Arshdeep Bahga and Vijay Madisetti
  - **Building Ethereum DApps**
  - By Roberto Infante
- **Truffle Quick Start Guide**
  - by Nikhil Bhaskar
- **Mastering Blockchain - Second Edition**
  - by Imran Bashir
- **Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners**
  - By Chris Dannen
- **Ethereum, Tokens & Smart Contracts: Notes on getting started**
  - by Eugenio Noyola
- **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You**
  - by Vikram Dhillon, David Metcalf, Max Hooper
- **Foundations of Blockchain**
  - By Koshik Raj
- **The Book of Satoshi: The Collected Writings od Bitcoin Creator Satoshi Nakamoto**
  - By Phil Champagne

References – 13 Free Blockchain Resources

1. William Slater’s Blockchain Resource Page http://billslater.com/blockchain
2. Factom University http://www.factom.com/university
3. Ethereum 101 http://www.ethereum101.org
4. Build on Ripple http://ripple.com/build
5. Programmable money by Ripple https://goo.gl/g8vFPL
6. DigiKnow https://youtu.be/scr68zFddso
7. Blockchain University http://blockchainu.co
8. Bitcoin Core https://bitcoin.org
9. Blockchain Alliance http://www.blockchainalliance.org
10. Multichain Blog http://www.mutichain,com/blog
11. HiveMind http://bitcoinhivemind.com
12. Chicago Blockchain Project http://chicagoblockchainproject.com/
13. Chicago Bitcoin and Open Blockchain Meetup Group https://www.meetup.com/Bitcoin-Open-Blockchain-Community-Chicago/

Slater Technologies

References - 10 Rules to Never Break the Blockchain

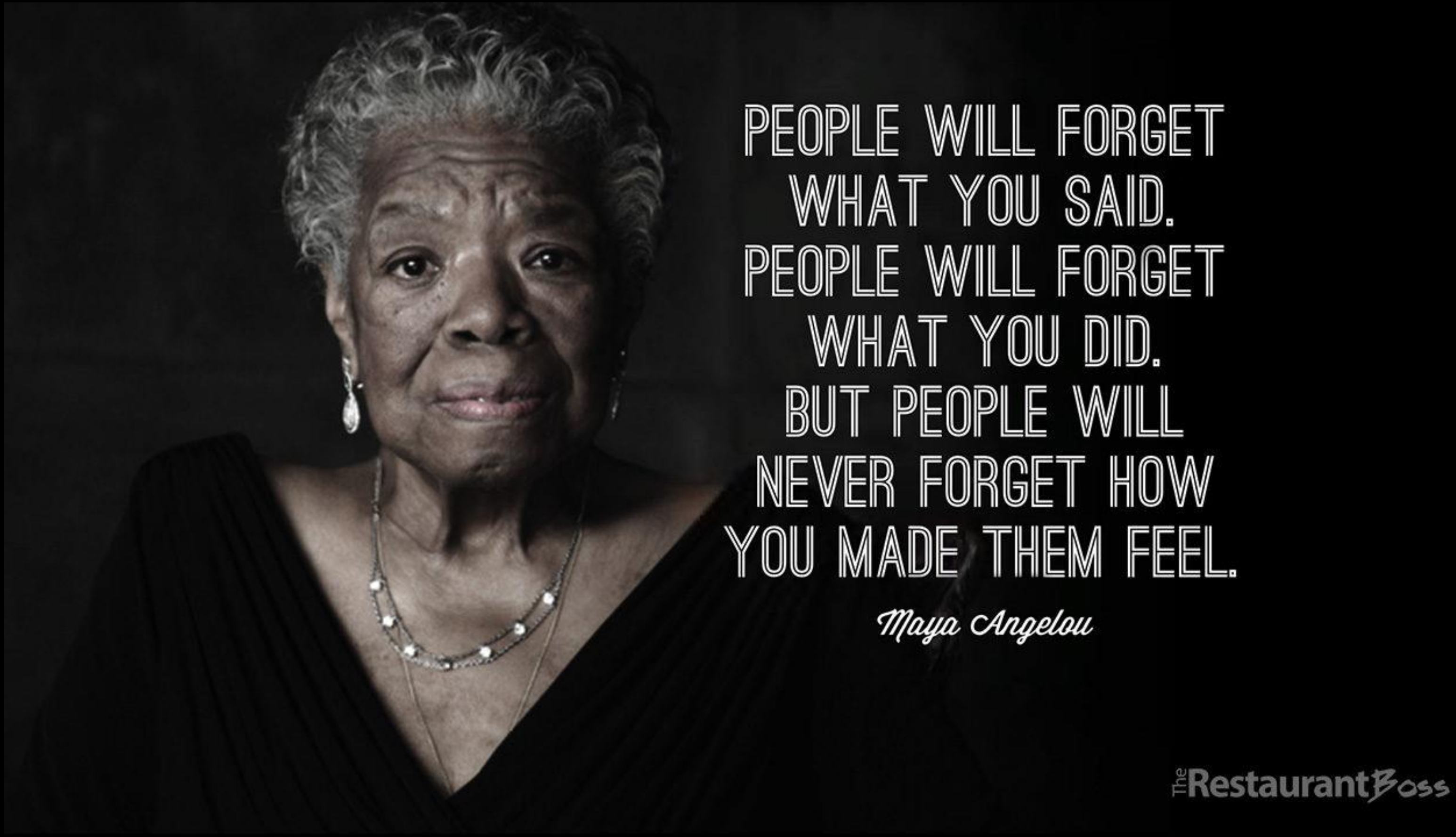
1. Don’t use Cryptocurrency or Blockchain to Skirt the Law
2. Keep your contracts as simple as possible
3. Publish with great caution
4. Back Up, Back Up, Back Up Your Private Keys
5. Triple-check the Address Before Sending Currency
6. Take Care When Using Exchanges
7. Beware Wi-Fi
8. Identify Your Blockchain Dev
9. Don’t Get Suckered
10. Don’t Trade Tokens Unless You Know What You’re Doing

Slater Technologies

References – 10 Free Blockchain Projects

- The R3 Consortium http://www.r3cev.com
- T ZERO: Overstocking the Stock Market http://www.overstock.com
- Blockstream’s Distributed Systems http://www.blockstream.com
- OpenBazaar’s Blockchain http://www.openbazaar.com
- Code Valley: Find Your Coder http://www.codevalley.com
- Bitfury’s Digital Assets http://www.bitfury.com
- Any Coin Can Shapeshift http://www.shapeshift.io
- Machine-Payable Apps on 21 http://www.21.co
- Anonymous Transactions on Dash http://www.dash.org
- ConsenSys: Decentralized Applications: http://www.consensys.net

Final Thoughts



PEOPLE WILL FORGET
WHAT YOU SAID.
PEOPLE WILL FORGET
WHAT YOU DID.
BUT PEOPLE WILL
NEVER FORGET HOW
YOU MADE THEM FEEL.

Maya Angelou

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

Slater Technologies

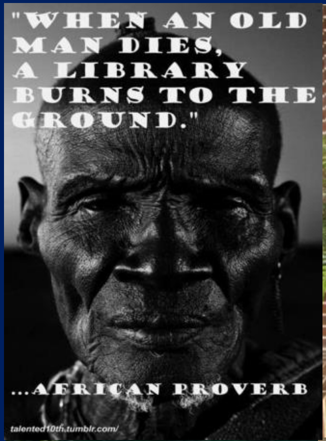
DEDICATION & THANKS

Slater Technologies

Dedication

This work is dedicated with love, admiration, gratitude, and great respect to *James P. Jarnagin* (January 25, 1935 – December 2, 2018), the Man who was my Mentor and Father-figure since March 1985. He is one of the biggest reasons for my career success and personal success. What I owe him can never be repaid.

We'll meet again, Jim. You can count on it…



June 2013

June 1994

October 2015

Slater Technologies

Special Thanks To:

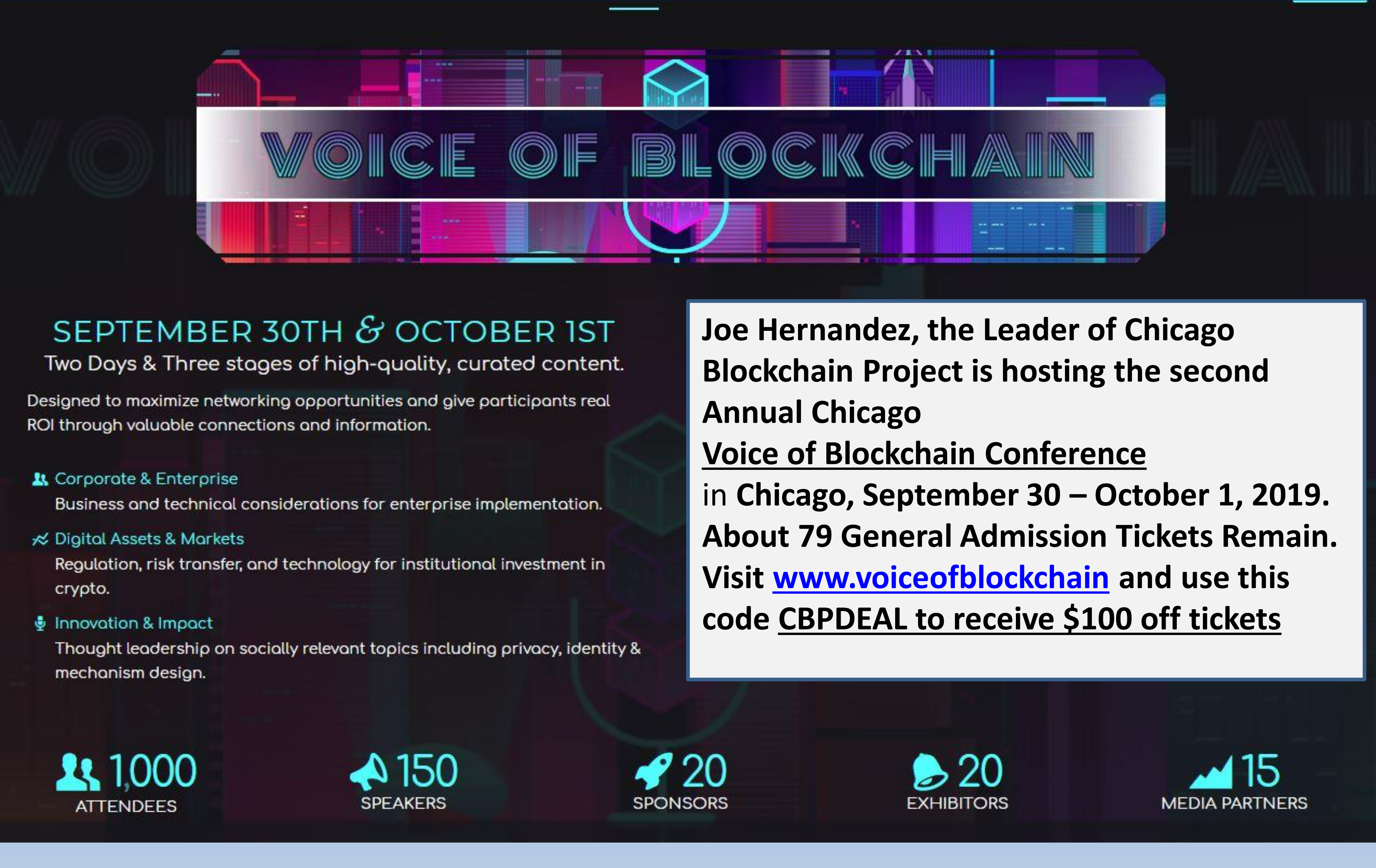
CBP CHICAGO BLOCKCHAIN PROJECT

Joe Hernandez
Co-Founder of the
Chicago Blockchain Project

COMMUNITY CHICAGO VIRES IN NUMERIS B.O.B. BITCOIN AND OPEN BLOCKCHAIN

Hannah Rosenburg
Director at the Chicago Blockchain Institute an
Co-Founder of the
Chicago Bitcoin and Open
Blockchain Meetup (3800 Members!)

Special Promotion



VOICE OF BLOCKCHAIN

SEPTEMBER 30TH & OCTOBER 1ST

Two Days & Three stages of high-quality, curated content.

Designed to maximize networking opportunities and give participants real ROI through valuable connections and information.

- Corporate & Enterprise
  Business and technical considerations for enterprise implementation.
- Digital Assets & Markets
  Regulation, risk transfer, and technology for institutional investment in crypto.
- Innovation & Impact
  Thought leadership on socially relevant topics including privacy, identity & mechanism design.

1,000	150	20	20	15
ATTENDEES	SPEAKERS	SPONSORS	EXHIBITORS	MEDIA PARTNERS

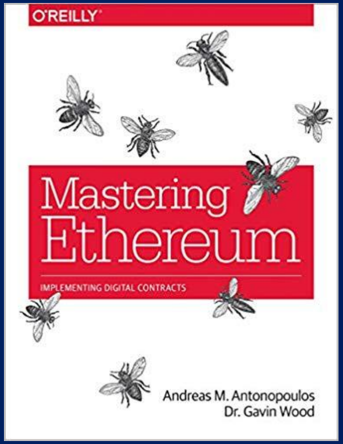
Joe Hernandez, the Leader of Chicago Blockchain Project is hosting the second Annual Chicago
Voice of Blockchain Conference
in **Chicago, September 30 – October 1, 2019. About 79 General Admission Tickets Remain. Visit www.voiceofblockchain and use this code CBPDEAL to receive $100 off tickets**

Special Promotion

Only 79 GA Tickets Left w/ Discount - Two Days, Three Stages, 200 Speakers!
The Chicago Blockchain Project discount code for $100 off is running out!
Use code: CBPDEAL to receive $100 off tickets
Buy yours today: https://voiceofblockchain.com
Check out all the newest additions including FINRA, CFTC, TD Ameritrade, Fidelity, and Deloitte at the website!

PRE - Voice of Blockchain Event on August 27th at Workbox downtown! FREE!
Meet the creator of the **Petro**, a cryptocurrency made by the Venezuelan government.
Gabriel Jimenez escaped from Venezuela while the electricity was out across the country. The story is nothing like what was originally reported in the news.
Meet Gabriel and see a panel with Colleen Sullivan, Partner & CEO at CMT Digital and Geoff Kasselbaum, former Executive Director of Newmark Knight Frank at our collaborative event with Tony P's Networking events and Workbox Coworking.
Sign up for FREE here: https://www.eventbrite.com/e/voice-of-blockchain-networking-event-in-collaboration-with-tony-p-tickets-64478905141

Special Thanks To:


O'REILLY

Mastering Ethereum

IMPLEMENTING DIGITAL CONTRACTS

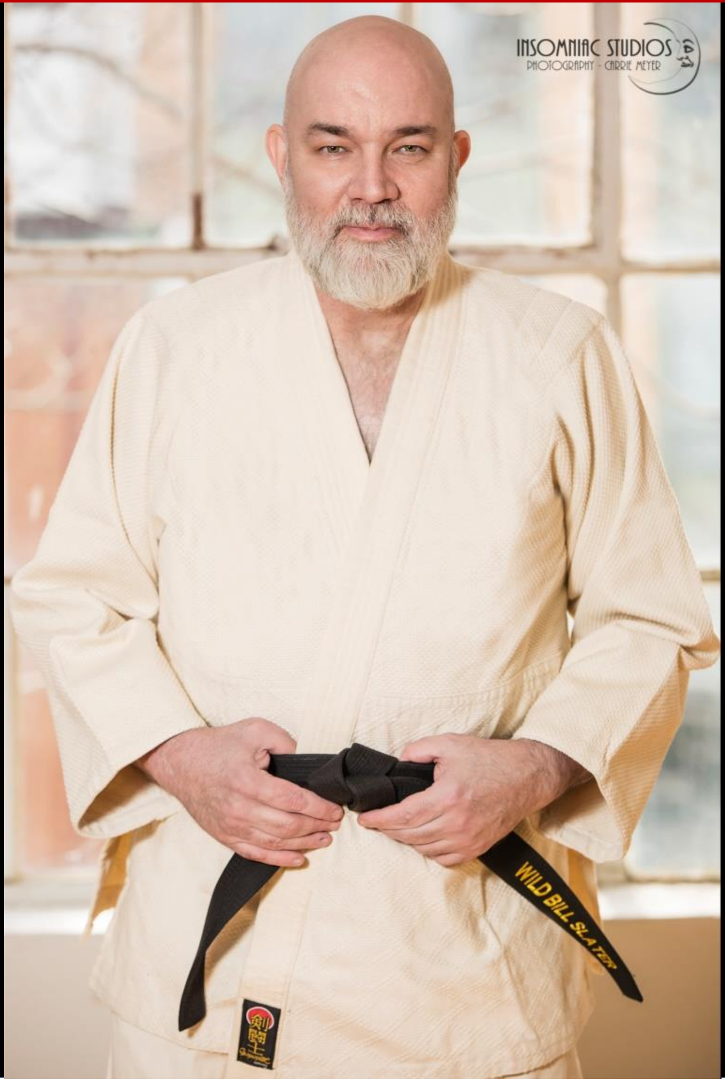
Andreas M. Antonopoulos
Dr. Gavin Wood

Andreas Antonopoulos
and Dr. Gavin Wood
Co-authors of
Mastering Ethereum

Special Thanks To:

Vitalik Buterin
Inventor of Ethereum
@VitalikButerin on #Twitter

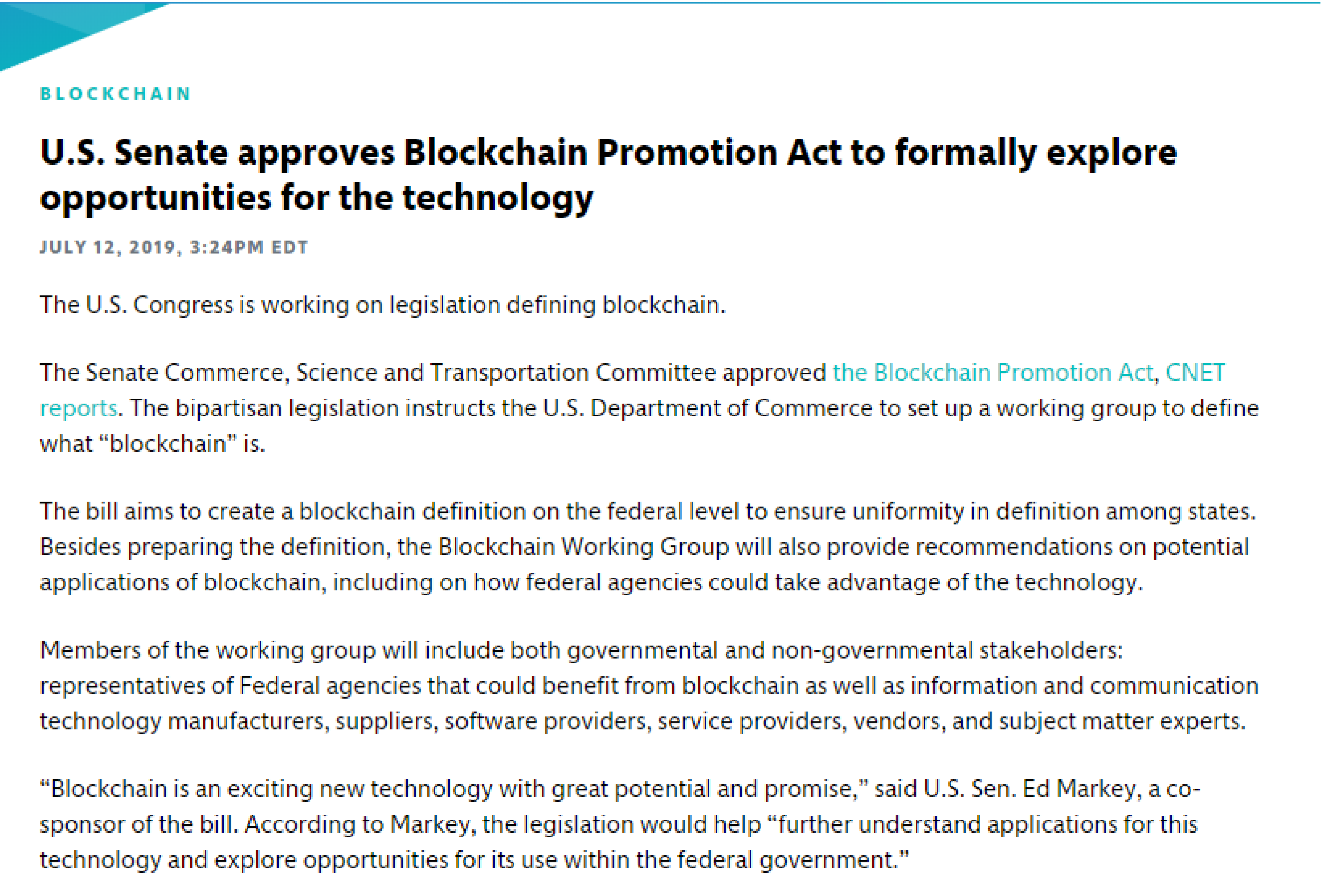
Thank You!
ASIS Northshore Chapter!



Supplemental Slides

Why Is Blockchain Important?

Why is Blockchain Important?



BLOCKCHAIN

U.S. Senate approves Blockchain Promotion Act to formally explore opportunities for the technology

JULY 12, 2019, 3:24PM EDT

The U.S. Congress is working on legislation defining blockchain.

The Senate Commerce, Science and Transportation Committee approved the Blockchain Promotion Act, CNET reports. The bipartisan legislation instructs the U.S. Department of Commerce to set up a working group to define what "blockchain" is.

The bill aims to create a blockchain definition on the federal level to ensure uniformity in definition among states. Besides preparing the definition, the Blockchain Working Group will also provide recommendations on potential applications of blockchain, including on how federal agencies could take advantage of the technology.

Members of the working group will include both governmental and non-governmental stakeholders: representatives of Federal agencies that could benefit from blockchain as well as information and communication technology manufacturers, suppliers, software providers, service providers, vendors, and subject matter experts.

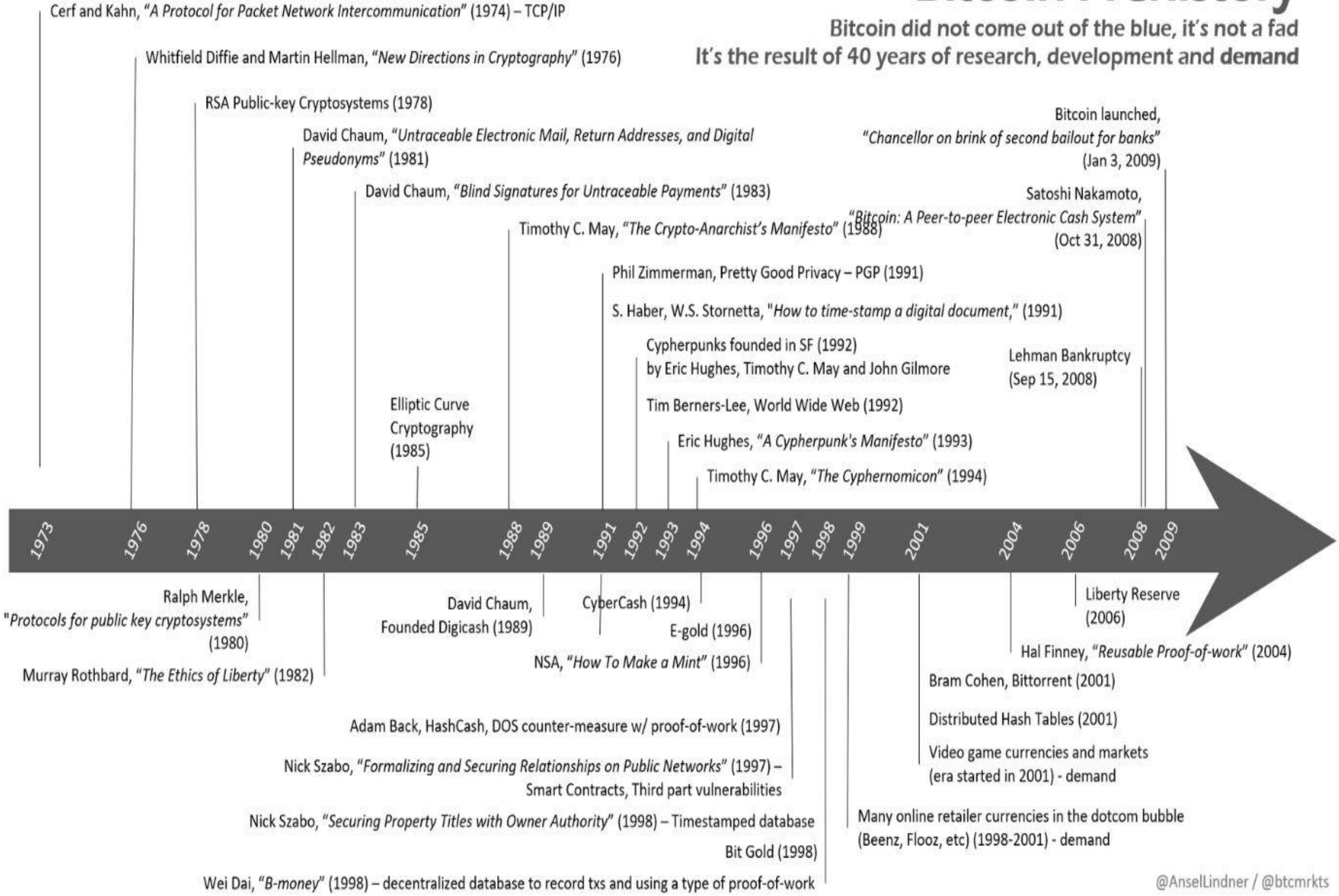
"Blockchain is an exciting new technology with great potential and promise," said U.S. Sen. Ed Markey, a co-sponsor of the bill. According to Markey, the legislation would help "further understand applications for this technology and explore opportunities for its use within the federal government."

Slater Technologies

What is Blockchain?

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



Cerf and Kahn, *"A Protocol for Packet Network Intercommunication"* (1974) – TCP/IP

Whitfield Diffie and Martin Hellman, *"New Directions in Cryptography"* (1976)

RSA Public-key Cryptosystems (1978)

David Chaum, *"Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms"* (1981)

David Chaum, *"Blind Signatures for Untraceable Payments"* (1983)

Elliptic Curve Cryptography (1985)

Timothy C. May, *"The Crypto-Anarchist's Manifesto"* (1988)

Phil Zimmerman, Pretty Good Privacy – PGP (1991)

S. Haber, W.S. Stornetta, "*How to time-stamp a digital document,*" (1991)

Cypherpunks founded in SF (1992)
by Eric Hughes, Timothy C. May and John Gilmore

Tim Berners-Lee, World Wide Web (1992)

Eric Hughes, *"A Cypherpunk's Manifesto"* (1993)

Timothy C. May, *"The Cyphernomicon"* (1994)

Lehman Bankruptcy
(Sep 15, 2008)

Satoshi Nakamoto,
"Bitcoin: A Peer-to-peer Electronic Cash System"
(Oct 31, 2008)

Bitcoin launched,
"Chancellor on brink of second bailout for banks"
(Jan 3, 2009)

Ralph Merkle,
"*Protocols for public key cryptosystems"*
(1980)

Murray Rothbard, *"The Ethics of Liberty"* (1982)

David Chaum,
Founded Digicash (1989)

CyberCash (1994)

E-gold (1996)

NSA, *"How To Make a Mint"* (1996)

Adam Back, HashCash, DOS counter-measure w/ proof-of-work (1997)

Nick Szabo, *"Formalizing and Securing Relationships on Public Networks"* (1997) –
Smart Contracts, Third part vulnerabilities

Nick Szabo, *"Securing Property Titles with Owner Authority"* (1998) – Timestamped database

Bit Gold (1998)

Wei Dai, *"B-money"* (1998) – decentralized database to record txs and using a type of proof-of-work

Many online retailer currencies in the dotcom bubble
(Beenz, Flooz, etc) (1998-2001) - demand

Bram Cohen, Bittorrent (2001)

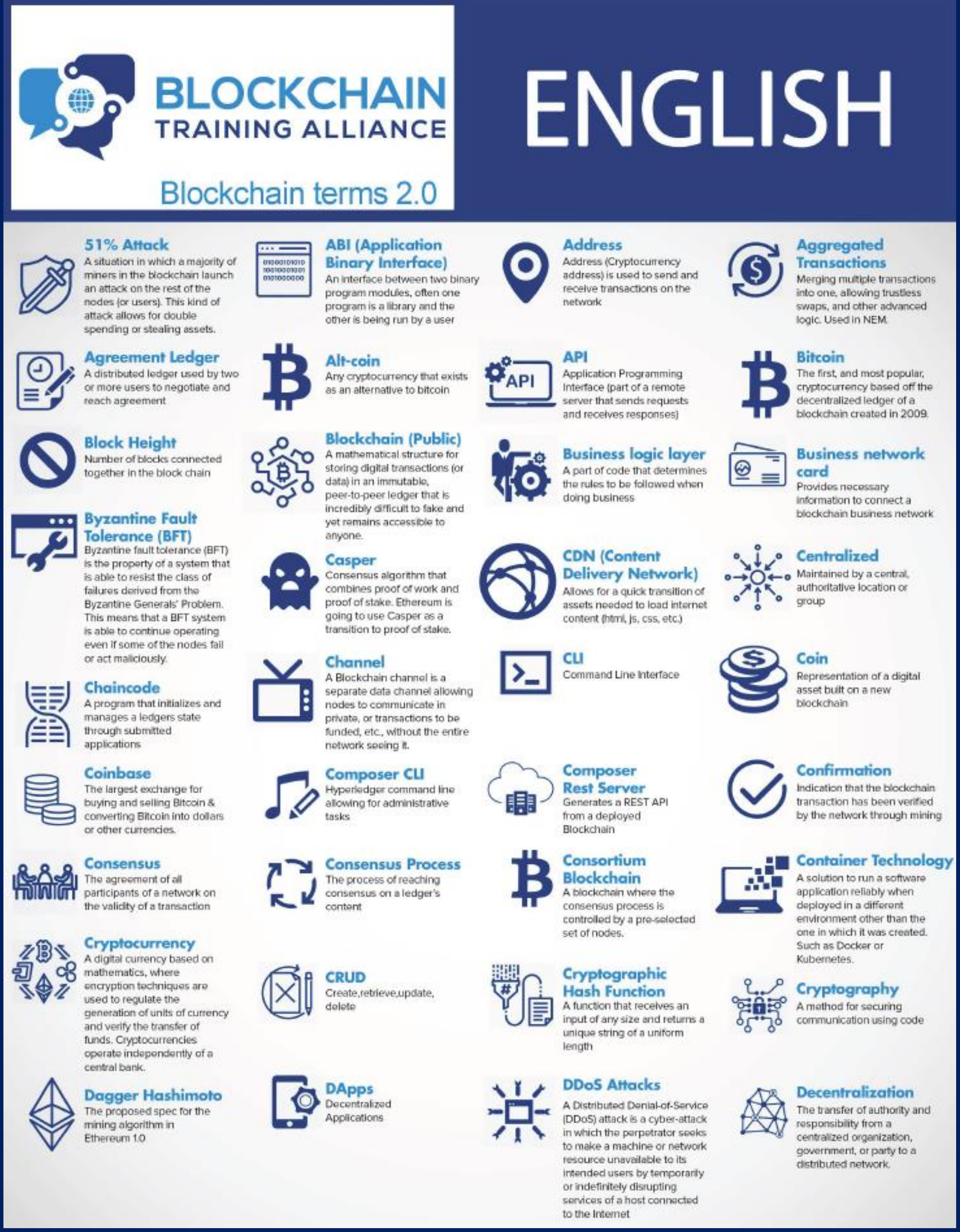
Distributed Hash Tables (2001)

Video game currencies and markets
(era started in 2001) - demand

Hal Finney, *"Reusable Proof-of-work"* (2004)

Liberty Reserve
(2006)

@AnselLindner / @btcmrkts



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

ENGLISH

51% Attack
A situation in which a majority of miners in the blockchain launch an attack on the rest of the nodes (or users). This kind of attack allows for double spending or stealing assets.

ABI (Application Binary Interface)
An interface between two binary program modules, often one program is a library and the other is being run by a user

Address
Address (Cryptocurrency address) is used to send and receive transactions on the network

Aggregated Transactions
Merging multiple transactions into one, allowing trustless swaps, and other advanced logic. Used in NEM.

Agreement Ledger
A distributed ledger used by two or more users to negotiate and reach agreement

Alt-coin
Any cryptocurrency that exists as an alternative to bitcoin

API
Application Programming Interface (part of a remote server that sends requests and receives responses)

Bitcoin
The first, and most popular, cryptocurrency based off the decentralized ledger of a blockchain created in 2009.

Block Height
Number of blocks connected together in the block chain

Blockchain (Public)
A mathematical structure for storing digital transactions (or data) in an immutable, peer-to-peer ledger that is incredibly difficult to fake and yet remains accessible to anyone.

Business logic layer
A part of code that determines the rules to be followed when doing business

Business network card
Provides necessary information to connect a blockchain business network

Byzantine Fault Tolerance (BFT)
Byzantine fault tolerance (BFT) is the property of a system that is able to resist the class of failures derived from the Byzantine Generals' Problem. This means that a BFT system is able to continue operating even if some of the nodes fail or act maliciously.

Casper
Consensus algorithm that combines proof of work and proof of stake. Ethereum is going to use Casper as a transition to proof of stake.

CDN (Content Delivery Network)
Allows for a quick transition of assets needed to load internet content (html, js, css, etc.)

Centralized
Maintained by a central, authoritative location or group

Chaincode
A program that initializes and manages a ledgers state through submitted applications

Channel
A Blockchain channel is a separate data channel allowing nodes to communicate in private, or transactions to be funded, etc., without the entire network seeing it.

CLI
Command Line Interface

Coin
Representation of a digital asset built on a new blockchain

Coinbase
The largest exchange for buying and selling Bitcoin & converting Bitcoin into dollars or other currencies.

Composer CLI
Hyperledger command line allowing for administrative tasks

Composer Rest Server
Generates a REST API from a deployed Blockchain

Confirmation
Indication that the blockchain transaction has been verified by the network through mining

Consensus
The agreement of all participants of a network on the validity of a transaction

Consensus Process
The process of reaching consensus on a ledger's content

Consortium Blockchain
A blockchain where the consensus process is controlled by a pre-selected set of nodes.

Container Technology
A solution to run a software application reliably when deployed in a different environment other than the one in which it was created. Such as Docker or Kubernetes.

Cryptocurrency
A digital currency based on mathematics, where encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. Cryptocurrencies operate independently of a central bank.

CRUD
Create,retrieve,update, delete

Cryptographic Hash Function
A function that receives an input of any size and returns a unique string of a uniform length

Cryptography
A method for securing communication using code

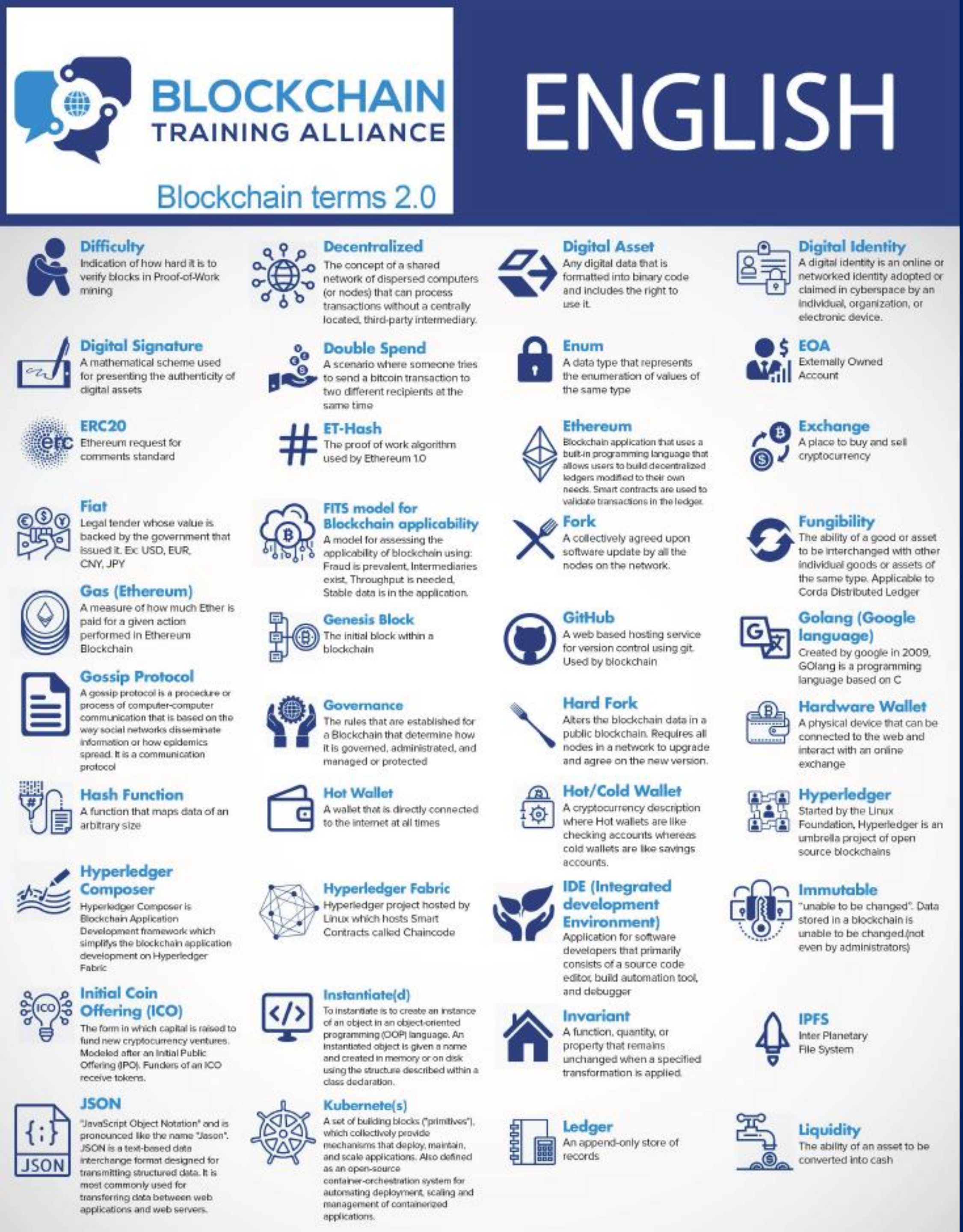
Dagger Hashimoto
The proposed spec for the mining algorithm in Ethereum 1.0

DApps
Decentralized Applications

DDoS Attacks
A Distributed Denial-of-Service (DDoS) attack is a cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet

Decentralization
The transfer of authority and responsibility from a centralized organization, government, or party to a distributed network.

Slater Technologies



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

ENGLISH

Difficulty
Indication of how hard it is to verify blocks in Proof-of-Work mining

Decentralized
The concept of a shared network of dispersed computers (or nodes) that can process transactions without a centrally located, third-party intermediary.

Digital Asset
Any digital data that is formatted into binary code and includes the right to use it.

Digital Identity
A digital identity is an online or networked identity adopted or claimed in cyberspace by an individual, organization, or electronic device.

Digital Signature
A mathematical scheme used for presenting the authenticity of digital assets

Double Spend
A scenario where someone tries to send a bitcoin transaction to two different recipients at the same time

Enum
A data type that represents the enumeration of values of the same type

EOA
Externally Owned Account

ERC20
Ethereum request for comments standard

ET-Hash
The proof of work algorithm used by Ethereum 1.0

Ethereum
Blockchain application that uses a built-in programming language that allows users to build decentralized ledgers modified to their own needs. Smart contracts are used to validate transactions in the ledger.

Exchange
A place to buy and sell cryptocurrency

Fiat
Legal tender whose value is backed by the government that issued it. Ex: USD, EUR, CNY, JPY

FITS model for Blockchain applicability
A model for assessing the applicability of blockchain using: Fraud is prevalent, Intermediaries exist, Throughput is needed, Stable data is in the application.

Fork
A collectively agreed upon software update by all the nodes on the network.

Fungibility
The ability of a good or asset to be interchanged with other individual goods or assets of the same type. Applicable to Corda Distributed Ledger

Gas (Ethereum)
A measure of how much Ether is paid for a given action performed in Ethereum Blockchain

Genesis Block
The initial block within a blockchain

GitHub
A web based hosting service for version control using git. Used by blockchain

Golang (Google language)
Created by google in 2009, GOlang is a programming language based on C

Gossip Protocol
A gossip protocol is a procedure or process of computer-computer communication that is based on the way social networks disseminate information or how epidemics spread. It is a communication protocol

Governance
The rules that are established for a Blockchain that determine how it is governed, administrated, and managed or protected

Hard Fork
Alters the blockchain data in a public blockchain. Requires all nodes in a network to upgrade and agree on the new version.

Hardware Wallet
A physical device that can be connected to the web and interact with an online exchange

Hash Function
A function that maps data of an arbitrary size

Hot Wallet
A wallet that is directly connected to the internet at all times

Hot/Cold Wallet
A cryptocurrency description where Hot wallets are like checking accounts whereas cold wallets are like savings accounts.

Hyperledger
Started by the Linux Foundation, Hyperledger is an umbrella project of open source blockchains

Hyperledger Composer
Hyperledger Composer is Blockchain Application Development framework which simplifys the blockchain application development on Hyperledger Fabric

Hyperledger Fabric
Hyperledger project hosted by Linux which hosts Smart Contracts called Chaincode

IDE (Integrated development Environment)
Application for software developers that primarily consists of a source code editor, build automation tool, and debugger

Immutable
"unable to be changed". Data stored in a blockchain is unable to be changed.(not even by administrators)

Initial Coin Offering (ICO)
The form in which capital is raised to fund new cryptocurrency ventures. Modeled after an Initial Public Offering (IPO). Funders of an ICO receive tokens.

Instantiate(d)
To instantiate is to create an instance of an object in an object-oriented programming (OOP) language. An instantiated object is given a name and created in memory or on disk using the structure described within a class declaration.

Invariant
A function, quantity, or property that remains unchanged when a specified transformation is applied.

IPFS
Inter Planetary File System

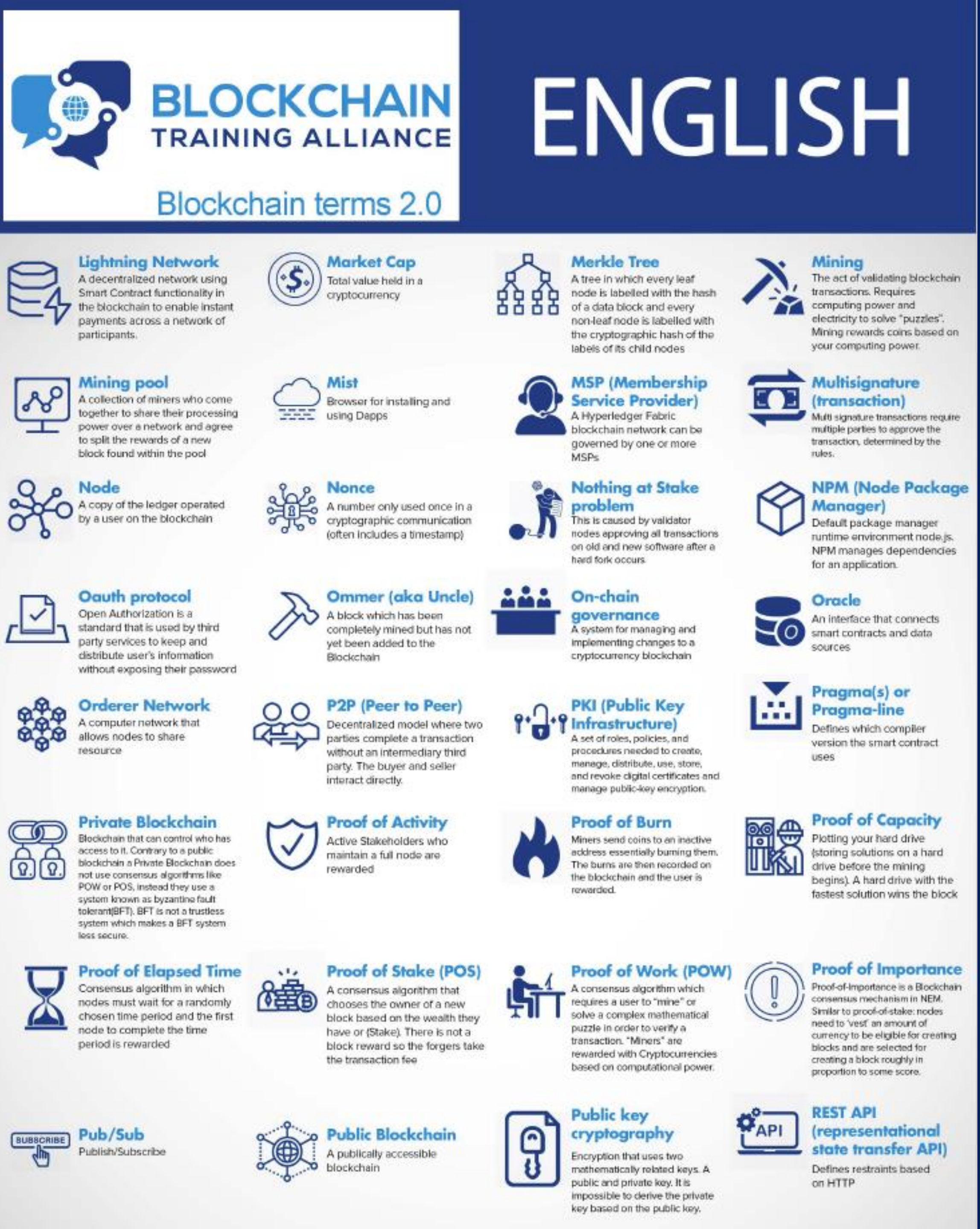
JSON
"JavaScript Object Notation" and is pronounced like the name "Jason". JSON is a text-based data interchange format designed for transmitting structured data. It is most commonly used for transferring data between web applications and web servers.

Kubernete(s)
A set of building blocks ("primitives"), which collectively provide mechanisms that deploy, maintain, and scale applications. Also defined as an open-source container-orchestration system for automating deployment, scaling and management of containerized applications.

Ledger
An append-only store of records

Liquidity
The ability of an asset to be converted into cash

Slater Technologies



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

ENGLISH

Lightning Network
A decentralized network using Smart Contract functionality in the blockchain to enable instant payments across a network of participants.

Market Cap
Total value held in a cryptocurrency

Merkle Tree
A tree in which every leaf node is labelled with the hash of a data block and every non-leaf node is labelled with the cryptographic hash of the labels of its child nodes

Mining
The act of validating blockchain transactions. Requires computing power and electricity to solve "puzzles". Mining rewards coins based on your computing power.

Mining pool
A collection of miners who come together to share their processing power over a network and agree to split the rewards of a new block found within the pool

Mist
Browser for installing and using Dapps

MSP (Membership Service Provider)
A Hyperledger Fabric blockchain network can be governed by one or more MSPs

Multisignature (transaction)
Multi signature transactions require multiple parties to approve the transaction, determined by the rules.

Node
A copy of the ledger operated by a user on the blockchain

Nonce
A number only used once in a cryptographic communication (often includes a timestamp)

Nothing at Stake problem
This is caused by validator nodes approving all transactions on old and new software after a hard fork occurs

NPM (Node Package Manager)
Default package manager runtime environment node.js. NPM manages dependencies for an application.

Oauth protocol
Open Authorization is a standard that is used by third party services to keep and distribute user's information without exposing their password

Ommer (aka Uncle)
A block which has been completely mined but has not yet been added to the Blockchain

On-chain governance
A system for managing and implementing changes to a cryptocurrency blockchain

Oracle
An interface that connects smart contracts and data sources

Orderer Network
A computer network that allows nodes to share resource

P2P (Peer to Peer)
Decentralized model where two parties complete a transaction without an intermediary third party. The buyer and seller interact directly.

PKI (Public Key Infrastructure)
A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

Pragma(s) or Pragma-line
Defines which compiler version the smart contract uses

Private Blockchain
Blockchain that can control who has access to it. Contrary to a public blockchain a Private Blockchain does not use consensus algorithms like POW or POS, instead they use a system known as byzantine fault tolerant(BFT). BFT is not a trustless system which makes a BFT system less secure.

Proof of Activity
Active Stakeholders who maintain a full node are rewarded

Proof of Burn
Miners send coins to an inactive address essentially burning them. The burns are then recorded on the blockchain and the user is rewarded.

Proof of Capacity
Plotting your hard drive (storing solutions on a hard drive before the mining begins). A hard drive with the fastest solution wins the block

Proof of Elapsed Time
Consensus algorithm in which nodes must wait for a randomly chosen time period and the first node to complete the time period is rewarded

Proof of Stake (POS)
A consensus algorithm that chooses the owner of a new block based on the wealth they have or (Stake). There is not a block reward so the forgers take the transaction fee

Proof of Work (POW)
A consensus algorithm which requires a user to "mine" or solve a complex mathematical puzzle in order to verify a transaction. "Miners" are rewarded with Cryptocurrencies based on computational power.

Proof of Importance
Proof-of-Importance is a Blockchain consensus mechanism in NEM. Similar to proof-of-stake: nodes need to 'vest' an amount of currency to be eligible for creating blocks and are selected for creating a block roughly in proportion to some score.

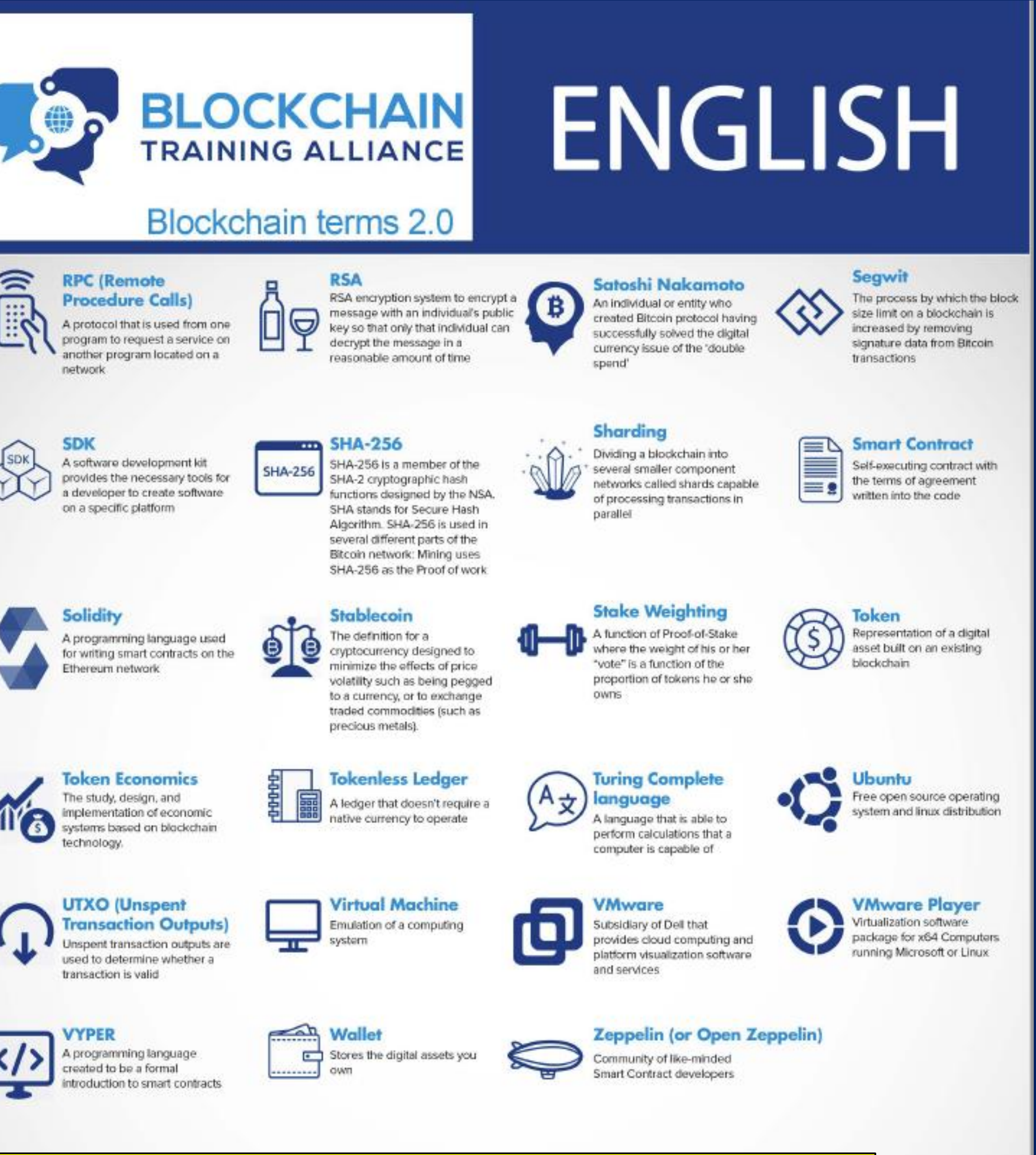
Pub/Sub
Publish/Subscribe

Public Blockchain
A publically accessible blockchain

Public key cryptography
Encryption that uses two mathematically related keys. A public and private key. It is impossible to derive the private key based on the public key.

REST API (representational state transfer API)
Defines restraints based on HTTP

Slater Technologies



BLOCKCHAIN TRAINING ALLIANCE

Blockchain terms 2.0

ENGLISH

RPC (Remote Procedure Calls)
A protocol that is used from one program to request a service on another program located on a network

RSA
RSA encryption system to encrypt a message with an individual's public key so that only that individual can decrypt the message in a reasonable amount of time

Satoshi Nakamoto
An individual or entity who created Bitcoin protocol having successfully solved the digital currency issue of the 'double spend'

Segwit
The process by which the block size limit on a blockchain is increased by removing signature data from Bitcoin transactions

SDK
A software development kit provides the necessary tools for a developer to create software on a specific platform

SHA-256
SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA. SHA stands for Secure Hash Algorithm. SHA-256 is used in several different parts of the Bitcoin network: Mining uses SHA-256 as the Proof of work

Sharding
Dividing a blockchain into several smaller component networks called shards capable of processing transactions in parallel

Smart Contract
Self-executing contract with the terms of agreement written into the code

Solidity
A programming language used for writing smart contracts on the Ethereum network

Stablecoin
The definition for a cryptocurrency designed to minimize the effects of price volatility such as being pegged to a currency, or to exchange traded commodities (such as precious metals).

Stake Weighting
A function of Proof-of-Stake where the weight of his or her "vote" is a function of the proportion of tokens he or she owns

Token
Representation of a digital asset built on an existing blockchain

Token Economics
The study, design, and implementation of economic systems based on blockchain technology.

Tokenless Ledger
A ledger that doesn't require a native currency to operate

Turing Complete language
A language that is able to perform calculations that a computer is capable of

Ubuntu
Free open source operating system and linux distribution

UTXO (Unspent Transaction Outputs)
Unspent transaction outputs are used to determine whether a transaction is valid

Virtual Machine
Emulation of a computing system

VMware
Subsidiary of Dell that provides cloud computing and platform visualization software and services

VMware Player
Virtualization software package for x64 Computers running Microsoft or Linux

VYPER
A programming language created to be a formal introduction to smart contracts

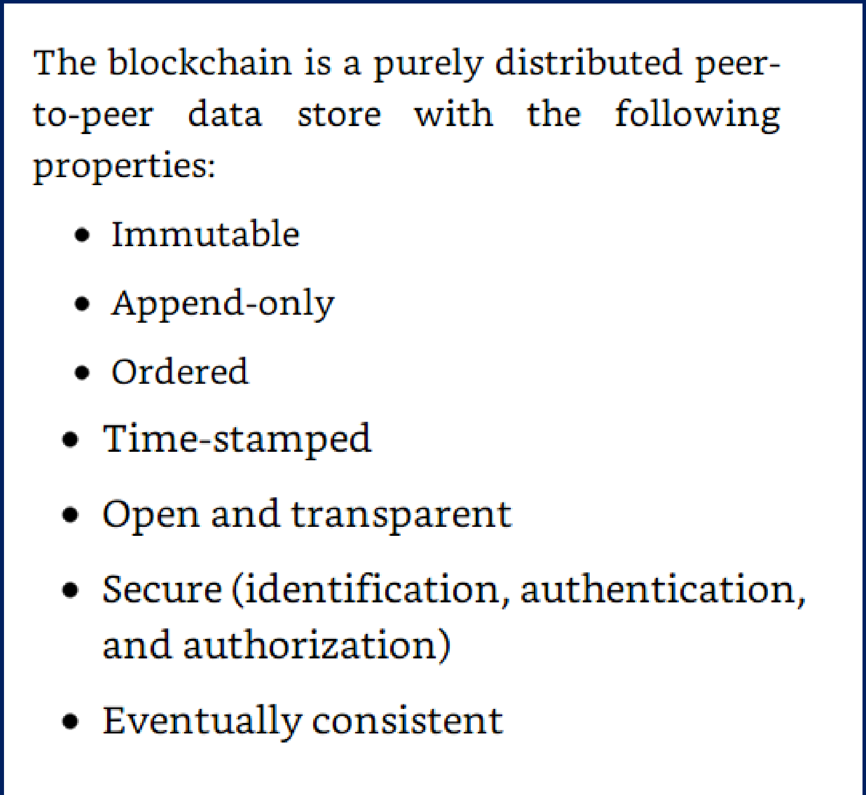
Wallet
Stores the digital assets you own

Zeppelin (or Open Zeppelin)
Community of like-minded Smart Contract developers

Source: Blobal Blockchain Terms by the Blockchain Training Alliance.
https://cdn.shopify.com/s/files/1/2137/1081/files/BTA_Global_Blockchain_Terms.pdf?2499

Slater Technologies

The Term "Blockchain"



The blockchain is a purely distributed peer-to-peer data store with the following properties:

- Immutable
- Append-only
- Ordered
- Time-stamped
- Open and transparent
- Secure (identification, authentication, and authorization)
- Eventually consistent

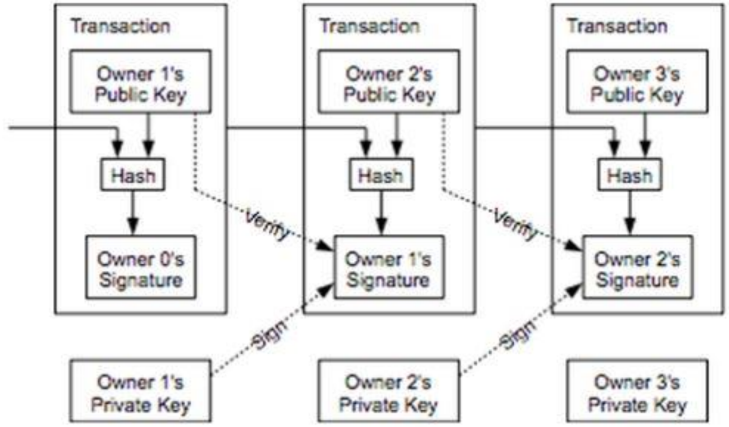
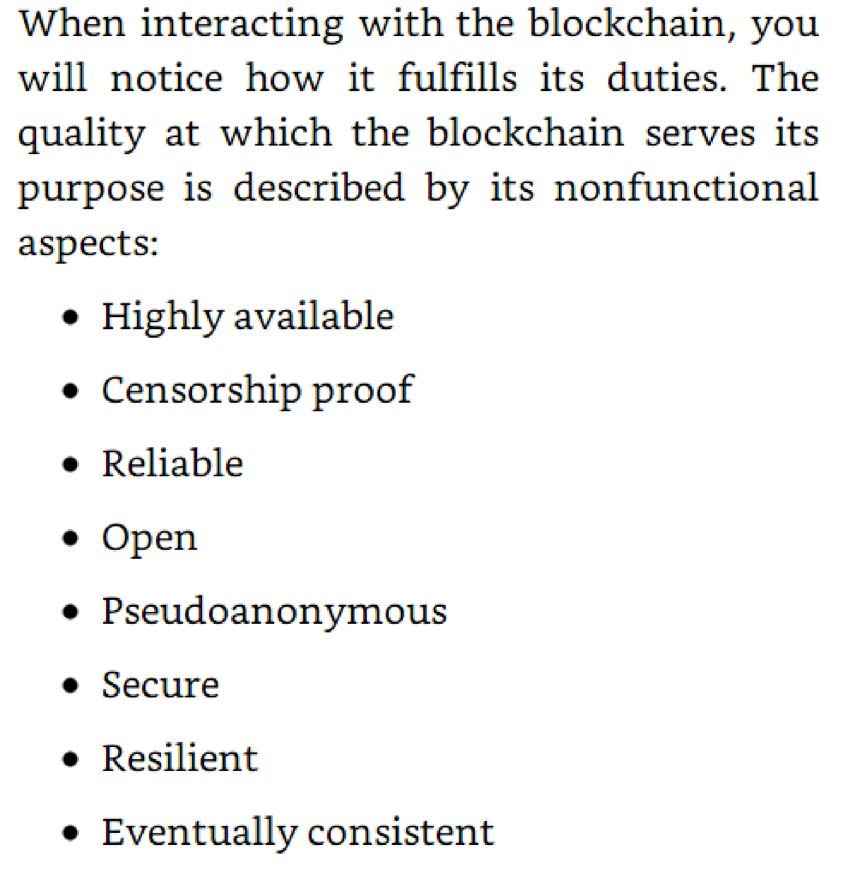


Image: Satoshi Nakamoto

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Properties of Blockchain’s Nonfunctional Aspects



When interacting with the blockchain, you will notice how it fulfills its duties. The quality at which the blockchain serves its purpose is described by its nonfunctional aspects:

- Highly available
- Censorship proof
- Reliable
- Open
- Pseudoanonymous
- Secure
- Resilient
- Eventually consistent

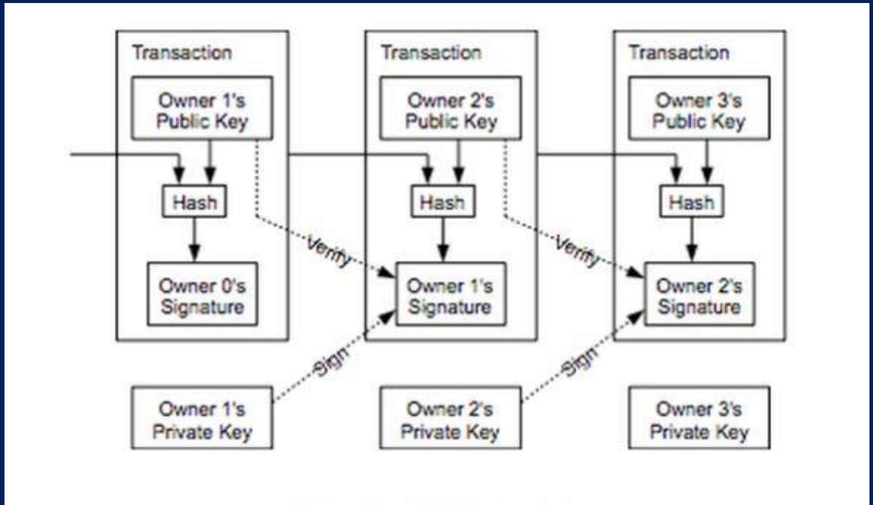


Image: Satoshi Nakamoto

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

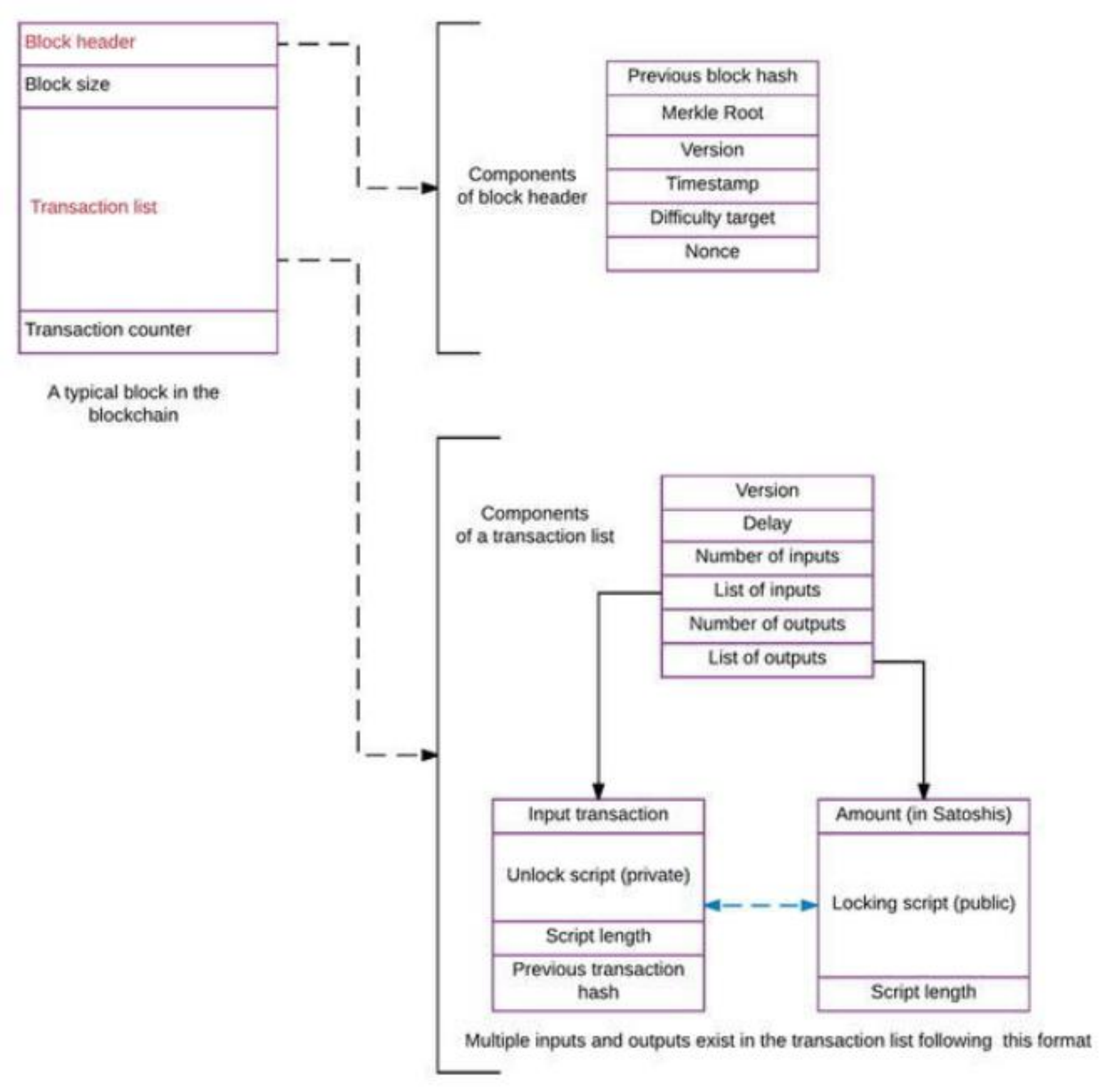
Slater Technologies

HOW DOES BLOCKCHAIN WORK?

Slater Technologies

Typical Blockchain Composition

- Block Header
- Block Transactions



Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

Slater Technologies

Creating a Block: The Blockchain Mining Processs

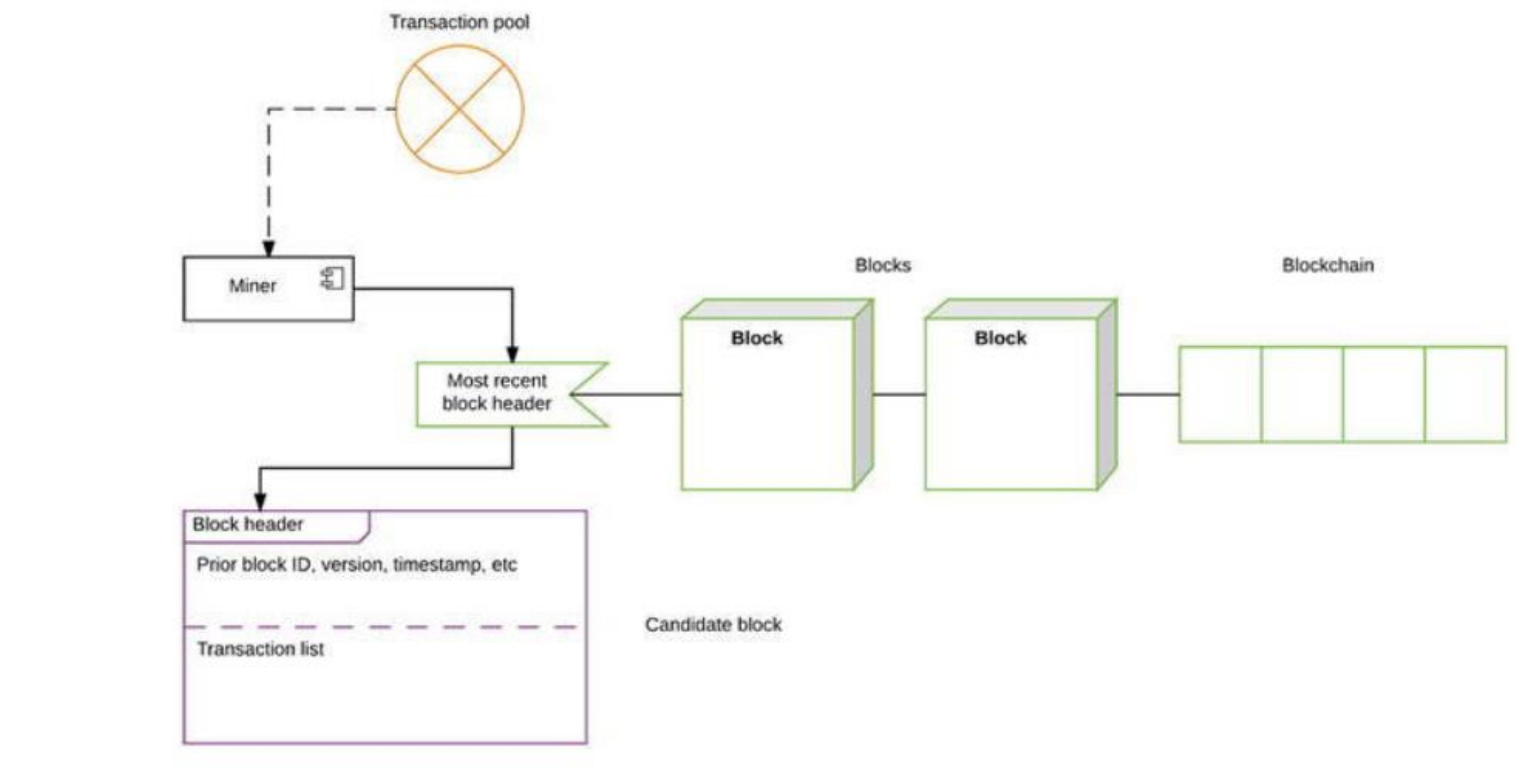


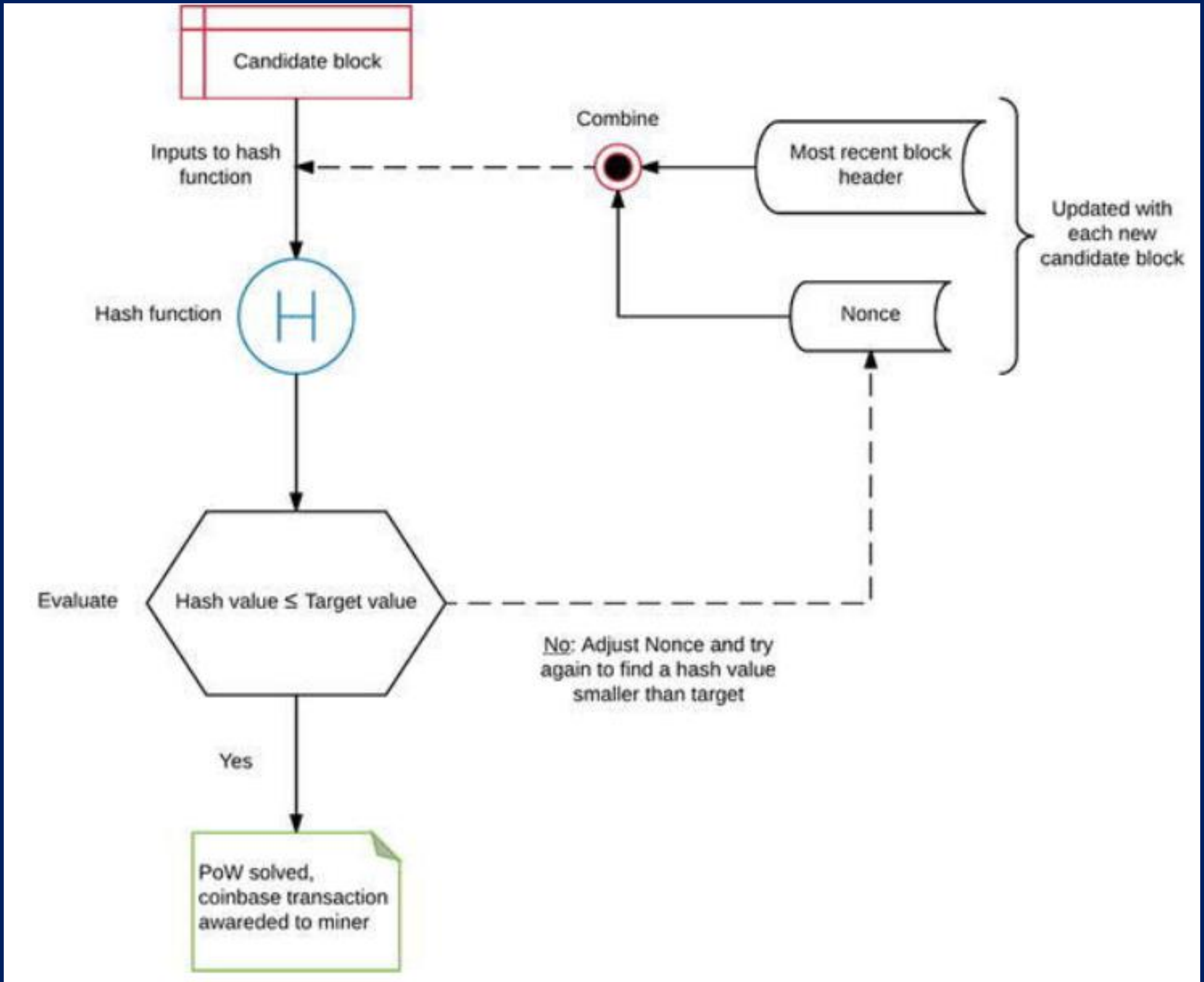
Figure 2-1.

A simplified overview of the mining process

Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

Slater Technologies

Mining Principles: Proof of Work

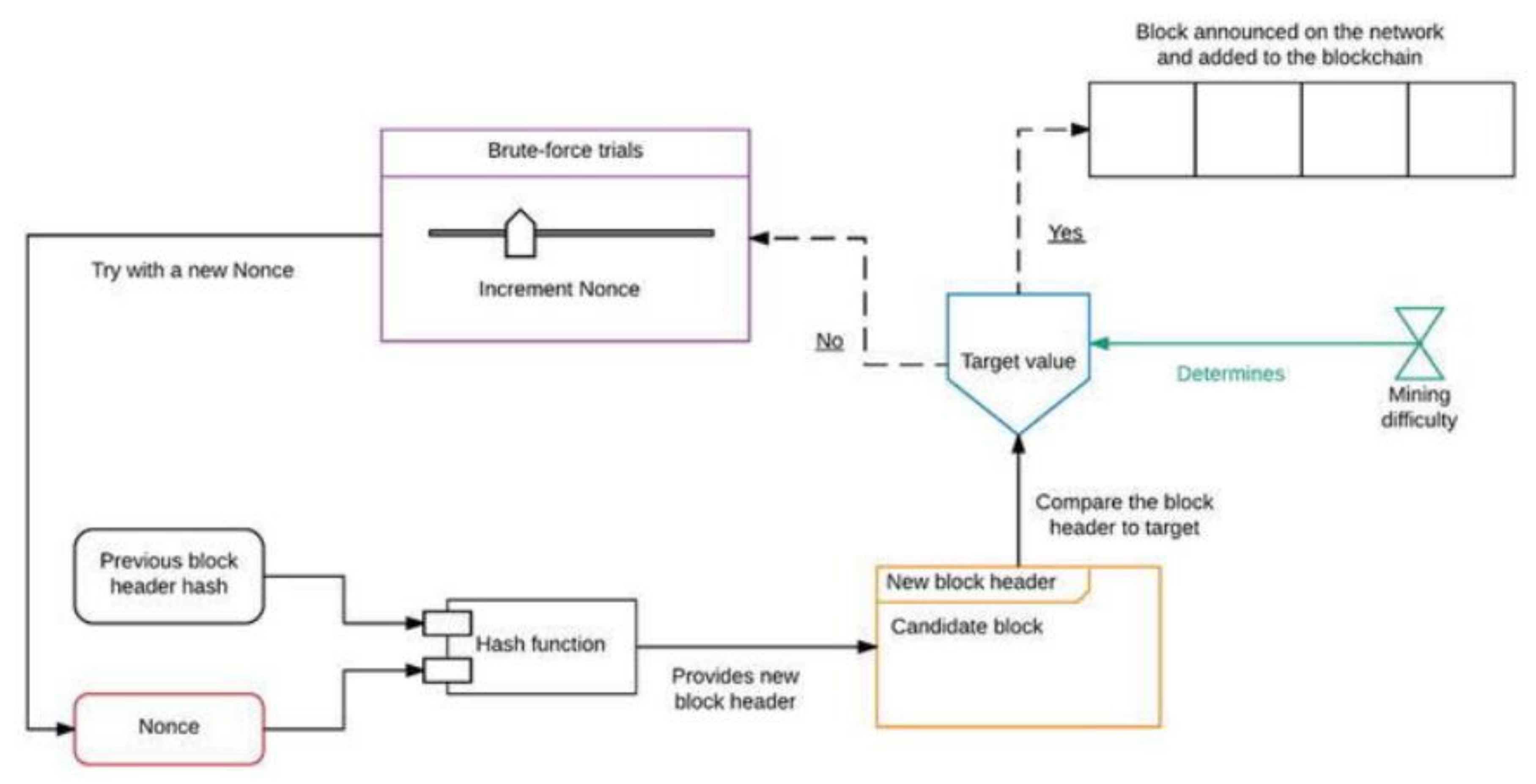

Candidate block
Combine
Inputs to hash function
Most recent block header
Updated with each new candidate block
Hash function
H
Nonce
Evaluate
Hash value ≤ Target value
No: Adjust Nonce and try again to find a hash value smaller than target
Yes
PoW solved, coinbase transaction awareded to miner

Special Note: Many other Blockchains, including Ethereum, apply these same principles.

Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

Slater Technologies

Mining Principles: Solving the Proof of Work

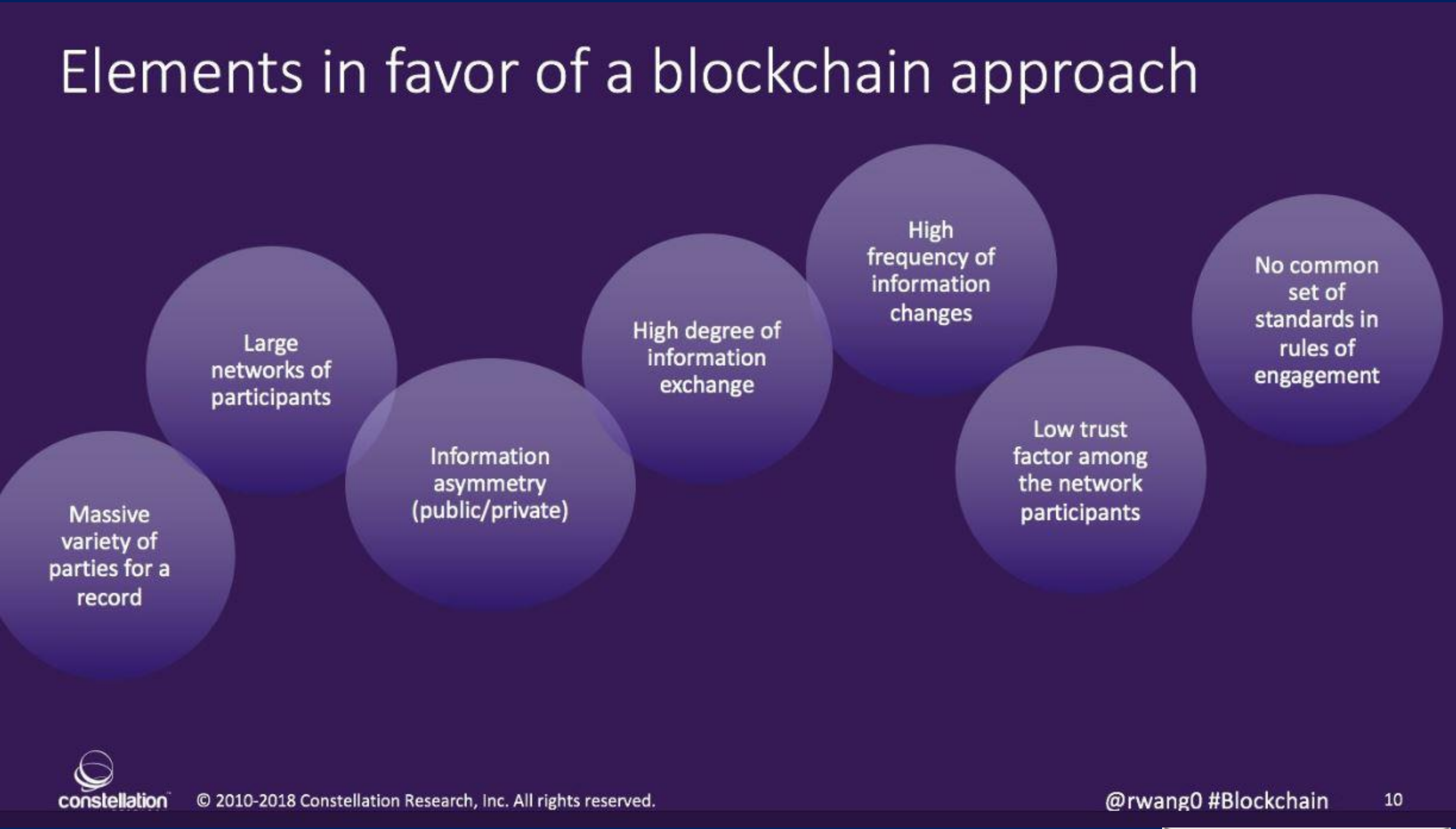


Special Note: Many other Blockchains, including Ethereum, apply these same principles.

Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

Slater Technologies

Why Blockchain?



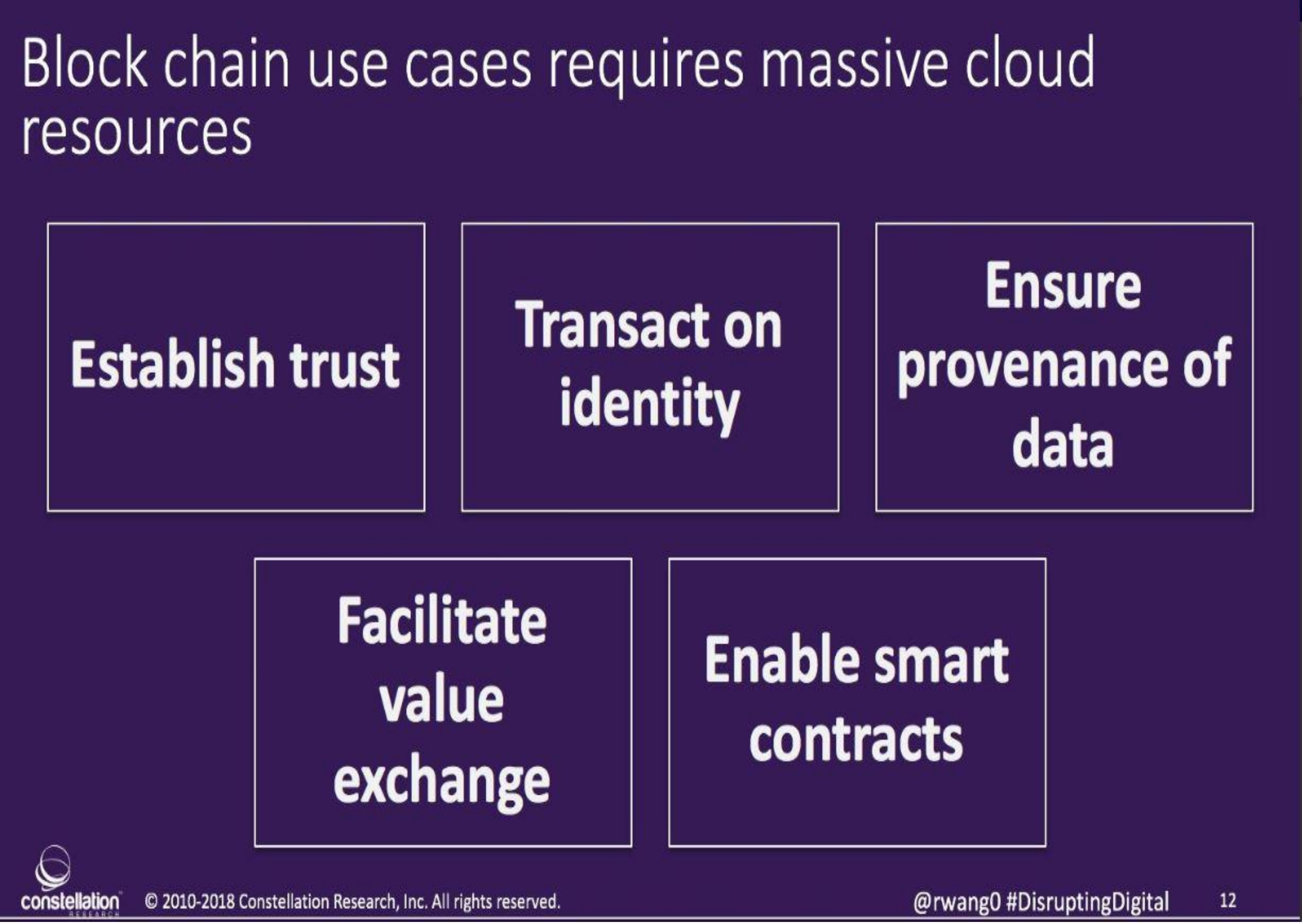
Elements in favor of a blockchain approach

- Massive variety of parties for a record
- Large networks of participants
- Information asymmetry (public/private)
- High degree of information exchange
- High frequency of information changes
- Low trust factor among the network participants
- No common set of standards in rules of engagement

constellation

@rwang0 #Blockchain

Slater Technologies



Block chain use cases requires massive cloud resources

Establish trust

Transact on identity

Ensure provenance of data

Facilitate value exchange

Enable smart contracts

constellation RESEARCH

@rwang0 #DisruptingDigital 12

Latest Blockchain News

Blockchain Security

Blockchain Security –
Threats and Vulnerabilities & Remediation – Part 1

Threat or Vulnerability	Description	Remediation	Comment(s)
Threat	51% Attack	Securely design, implement, monitor, maintain, test & upgrade.	Happened to Bitcoin in June 2014. http://tinyurl.com/y5malrxc
Threat	Sybil Attack	Securely design, implement, monitor, maintain, test & upgrade.	Need better education and experience.
Vulnerability	Bad Private Key Management	Understand & Securely manage private keys.	Need better education and tools.
Vulnerability	Centralization	Understand the CAP Theorem and Decentralization. Design and implement accordingly.	Need better education.
Vulnerability	Scalability	Securely design, implement, monitor, maintain, test & upgrade.	Need better education and experience.
Vulnerability	Network Security	Securely design, implement, monitor, maintain, test & upgrade.	Need better education.
Vulnerability	Smart Contracts – Coding errors	Securely design, implement, monitor, maintain, test & upgrade.	Need better education and experience.
Vulnerability	Smart Contracts – Configuration Errors	Securely design, implement, monitor, maintain, test & upgrade.	Need better education and experience.
Vulnerability	Blockchain & Smart Contracts - Inexperience	Use Secure Development practices, and experienced developers and testers.	Need better education and experience.

Slater Technologies

Blockchain Security –
Threats and Vulnerabilities & Remediation – Part 2

Threat or Vulnerability	Description	Remediation	Comment(s)
Vulnerability	Reentrancy	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Unexpected Ether	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	DELEGATECALL	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Default Visibilities	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Entropy Illusion	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	External Contract Referencing	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Short Address / Parameter Attack	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Unchecked CALL Return Value	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Race Conditions / Front Running	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.

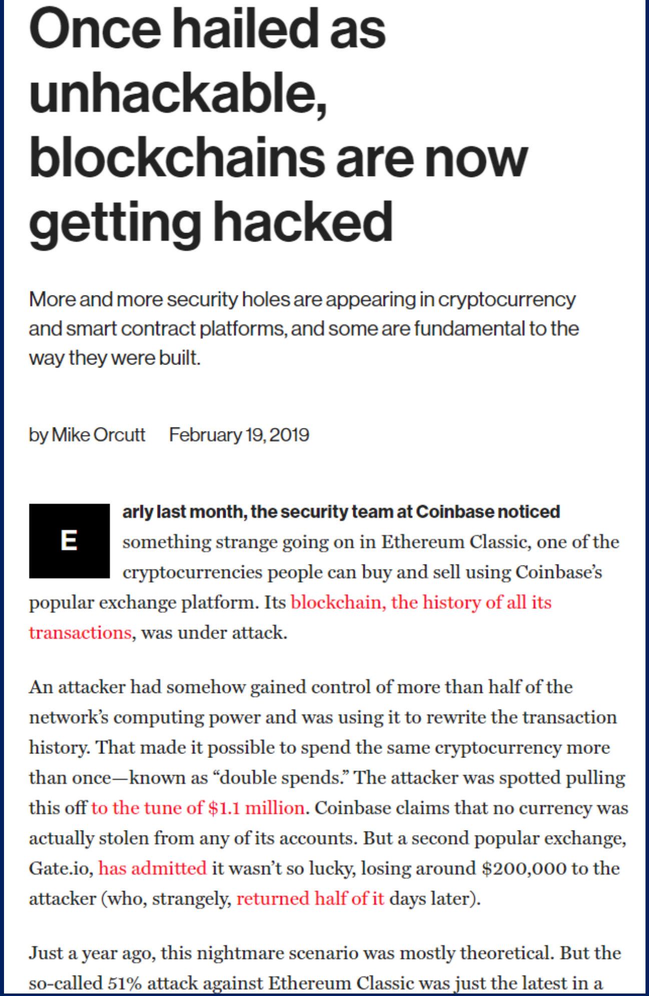
Slater Technologies

Blockchain Security –
Threats and Vulnerabilities & Remediation – Part 3

Threat or Vulnerability	Description	Remediation	Comment(s)
Vulnerability	Denial of Service	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Block Timestamp Manipulation	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Constructions with Care	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Uninitialized Storage Pointers	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Floating Point and Precision	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Transaction Origin Authentication	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Vulnerability	Contract Libraries	Securely design, implement, monitor, maintain, test & upgrade. Code reviews & Audits.	See ***Mastering Ethereum***, Chapter 9.
Threat	**Shor's Algorithm (Using Quantum Computing)**	**Stronger, better encryption, perhaps Quantum Cryptography.**	**Closer than you think**

Slater Technologies

MIT Article – Blockchains Are Now Getting Hacked



Once hailed as unhackable, blockchains are now getting hacked

More and more security holes are appearing in cryptocurrency and smart contract platforms, and some are fundamental to the way they were built.

by Mike Orcutt   February 19, 2019

Early last month, the security team at Coinbase noticed something strange going on in Ethereum Classic, one of the cryptocurrencies people can buy and sell using Coinbase's popular exchange platform. Its blockchain, the history of all its transactions, was under attack.

An attacker had somehow gained control of more than half of the network's computing power and was using it to rewrite the transaction history. That made it possible to spend the same cryptocurrency more than once—known as "double spends." The attacker was spotted pulling this off to the tune of $1.1 million. Coinbase claims that no currency was actually stolen from any of its accounts. But a second popular exchange, Gate.io, has admitted it wasn't so lucky, losing around $200,000 to the attacker (who, strangely, returned half of it days later).

Just a year ago, this nightmare scenario was mostly theoretical. But the so-called 51% attack against Ethereum Classic was just the latest in a

51% Attack on Ethereum Classic – January 2019

Source: MIT Review, Mike Orcutt, February 19, 2019
https://www.technologyreview.com/s/612974/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/

Slater Technologies

CASE STUDIES

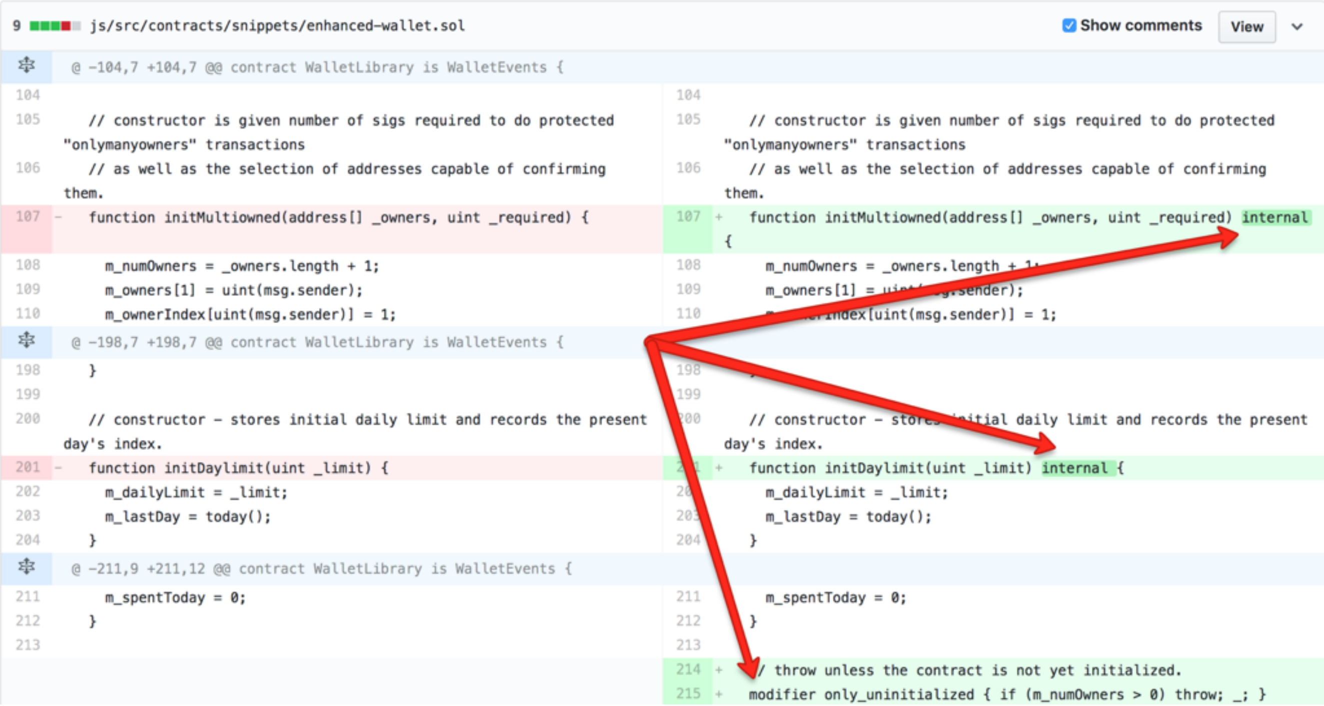
Slater Technologies

Case Study 1

- Timeframe: November 2017
- Location: User ***devops199*** somewhere on the Ethereum Blockchain
- 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

@ -104,7 +104,7 @@ contract WalletLibrary is WalletEvents {

    // constructor is given number of sigs required to do protected "onlymanyowners" transactions
    // as well as the selection of addresses capable of confirming them.
-   function initMultiowned(address[] _owners, uint _required) {
      m_numOwners = _owners.length + 1;
      m_owners[1] = uint(msg.sender);
      m_ownerIndex[uint(msg.sender)] = 1;

    // constructor is given number of sigs required to do protected "onlymanyowners" transactions
    // as well as the selection of addresses capable of confirming them.
+   function initMultiowned(address[] _owners, uint _required) internal {
      m_numOwners = _owners.length + 1;
      m_owners[1] = uint(msg.sender);
      m_ownerIndex[uint(msg.sender)] = 1;

@ -198,7 +198,7 @@ contract WalletLibrary is WalletEvents {
    }

    // constructor - stores initial daily limit and records the present day's index.
-   function initDaylimit(uint _limit) {
      m_dailyLimit = _limit;
      m_lastDay = today();
    }

    }

    // constructor - stores initial daily limit and records the present day's index.
+   function initDaylimit(uint _limit) internal {
      m_dailyLimit = _limit;
      m_lastDay = today();
    }

@ -211,9 +211,12 @@ contract WalletLibrary is WalletEvents {
      m_spentToday = 0;
    }


      m_spentToday = 0;
    }

+   // throw unless the contract is not yet initialized.
+   modifier only_uninitialized { if (m_numOwners > 0) throw; _; }
```

Slater Technologies

Blockchain Auditing

Concepts of Auditing the Data and Transactions in Blockchain Data Structures

- Blockchain Log Entries on geth
- Examine using Javascript in geth console using *web3.eth.filter()*
- Options include:
  - **fromBlock:** Number of the earliest block for fetching the logs or use ‘latest’ or ‘pending’
  - **toBlock:** Number of the latest block for fetching the logs or use ‘latest’ or ‘pending’
  - **address:** An address or list of addresses to only get logs from particular accounts
  - **topics:** List of log topics
- When *web3.eth.filter()* is set to ‘pending’ it returns a transaction hash of the most recent pending transaction.

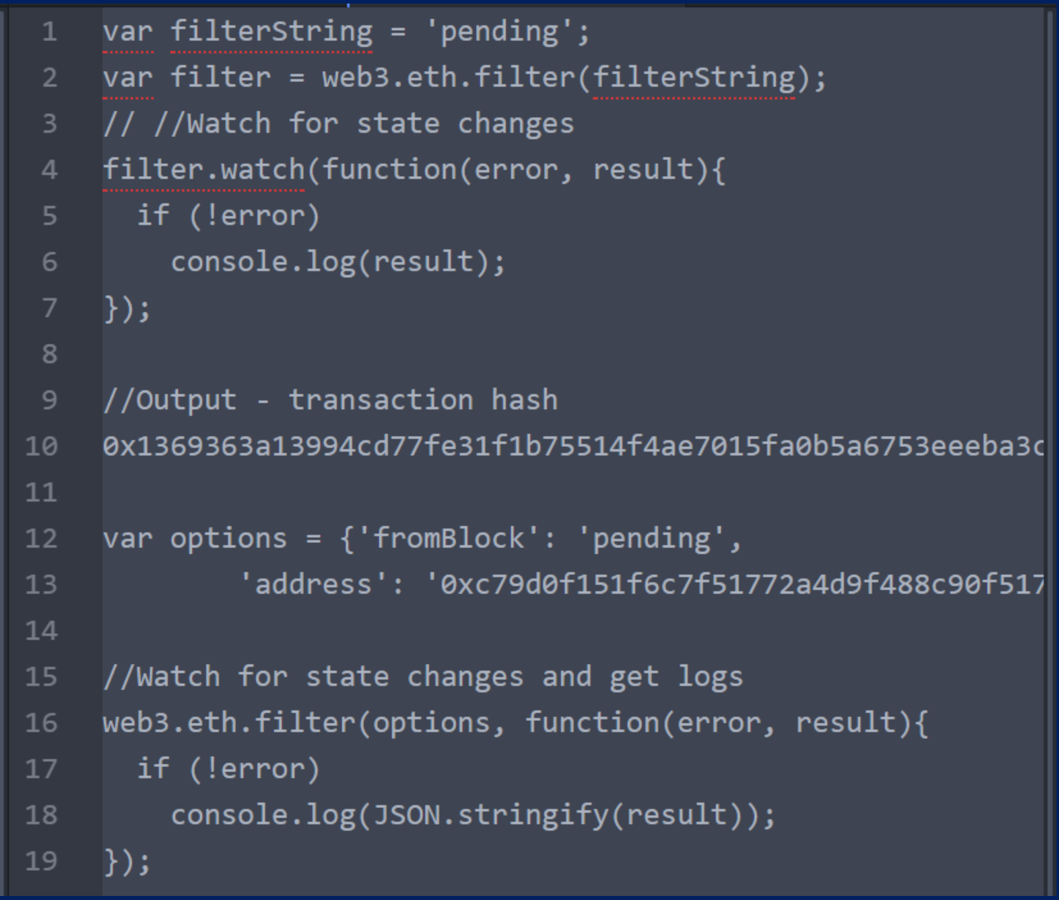
Slater Technologies

Concepts of Auditing the Data and Transactions in Blockchain Data Structures

- Blockchain Log Entries on geth
- Examine using Javascript in geth console using *web3.eth.filter()*
- Log object fields you can examine include
  - **logIndex:** Log index position of the block.
  - **transactionIndex:** Transaction index position the log was created from.
  - **transactionHash:** Hash of the transaction this log was created from.
  - **blockHash:** Hash of the block this log was in.
  - **blockNumber:** Block number where this log was in.
  - **address:** Address from which this log originated.
  - **data:** Includes non-indexed arguments of the log.
  - **topics:** Includes indexed log arguments.

Concepts of Auditing the Data and Transactions in Blockchain Data Structures

Example Log review code using Javascript

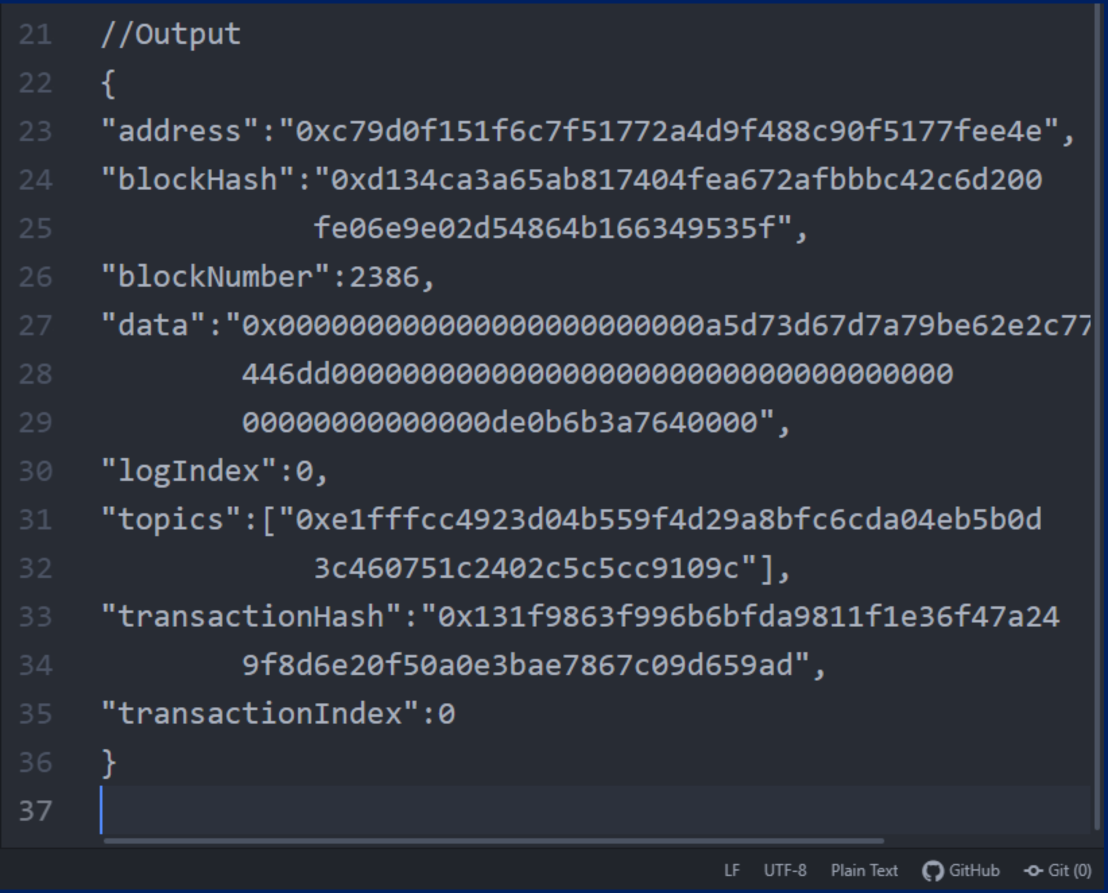


```javascript
var filterString = 'pending';
var filter = web3.eth.filter(filterString);
// //Watch for state changes
filter.watch(function(error, result){
  if (!error)
    console.log(result);
});

//Output - transaction hash
0x1369363a13994cd77fe31f1b75514f4ae7015fa0b5a6753eeeba3c

var options = {'fromBlock': 'pending',
        'address': '0xc79d0f151f6c7f51772a4d9f488c90f517

//Watch for state changes and get logs
web3.eth.filter(options, function(error, result){
  if (!error)
    console.log(JSON.stringify(result));
});
```

Slater Technologies

Concepts of Auditing the Data and Transactions in Blockchain Data Structures

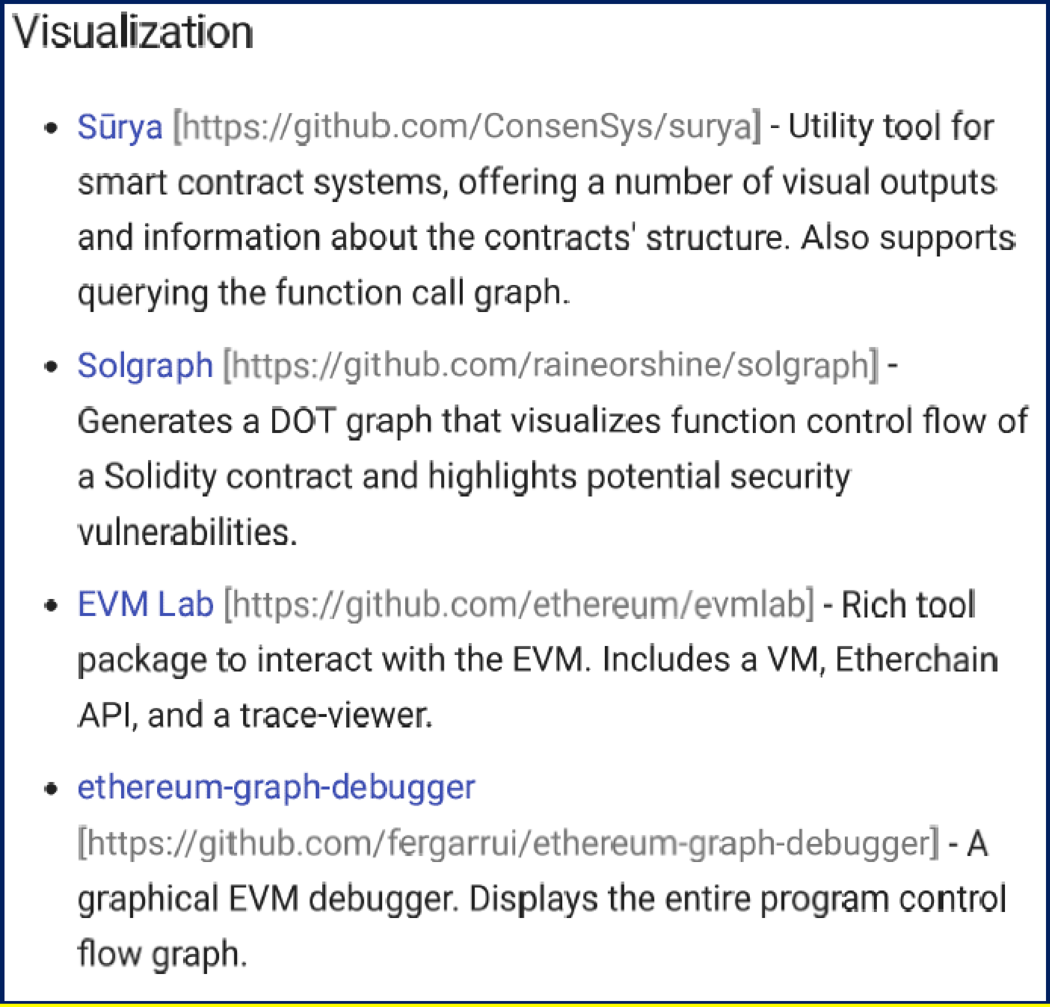
Example Log review code using Javascript



```
//Output
{
"address":"0xc79d0f151f6c7f51772a4d9f488c90f5177fee4e",
"blockHash":"0xd134ca3a65ab817404fea672afbbbc42c6d200
            fe06e9e02d54864b166349535f",
"blockNumber":2386,
"data":"0x000000000000000000000000a5d73d67d7a79be62e2c77
        446dd00000000000000000000000000000000000
        00000000000000de0b6b3a7640000",
"logIndex":0,
"topics":["0xe1fffcc4923d04b559f4d29a8bfc6cda04eb5b0d
            3c460751c2402c5c5cc9109c"],
"transactionHash":"0x131f9863f996b6bfda9811f1e36f47a24
        9f8d6e20f50a0e3bae7867c09d659ad",
"transactionIndex":0
}
```

Slater Technologies

Security Tools for Auditing & Visualizing Transactions in Blockchain Data Structures



Visualization

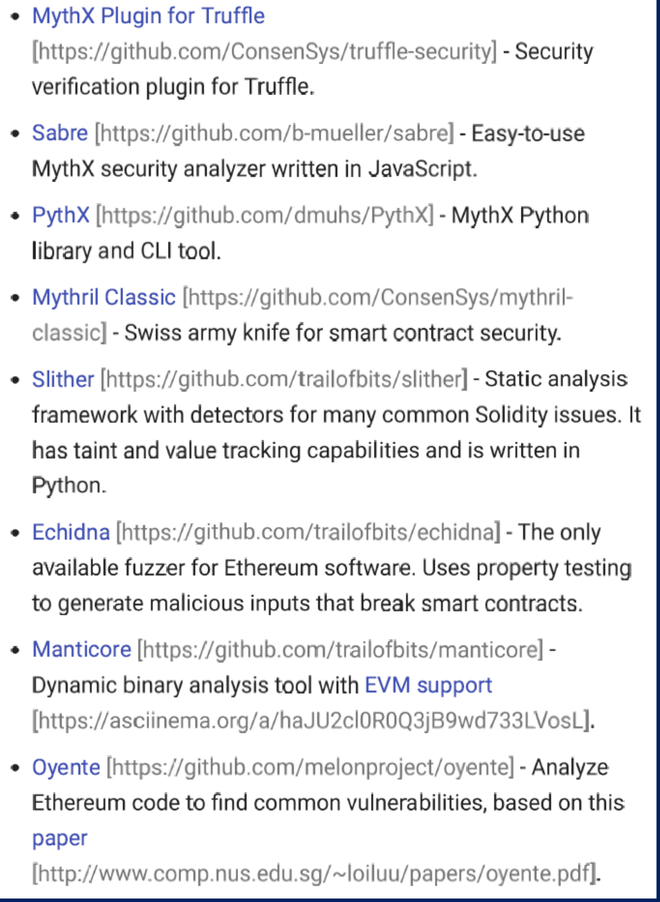
- Sūrya [https://github.com/ConsenSys/surya] - Utility tool for smart contract systems, offering a number of visual outputs and information about the contracts' structure. Also supports querying the function call graph.
- Solgraph [https://github.com/raineorshine/solgraph] - Generates a DOT graph that visualizes function control flow of a Solidity contract and highlights potential security vulnerabilities.
- EVM Lab [https://github.com/ethereum/evmlab] - Rich tool package to interact with the EVM. Includes a VM, Etherchain API, and a trace-viewer.
- ethereum-graph-debugger [https://github.com/fergarrui/ethereum-graph-debugger] - A graphical EVM debugger. Displays the entire program control flow graph.

Source: Smart Contract Security: https://consensys.github.io/smart-contract-best-practices/

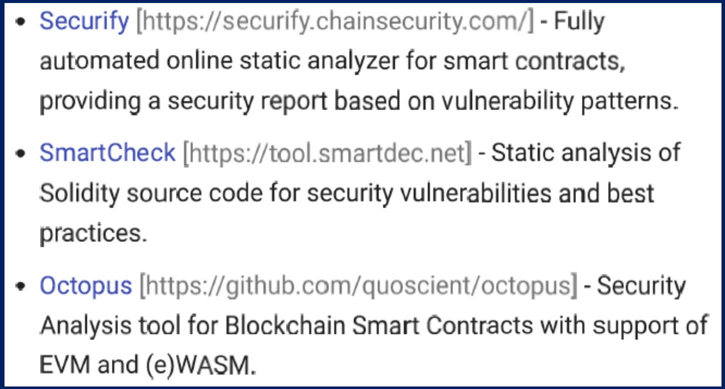
Slater Technologies

Security Tools for Auditing & Visualizing Transactions in Blockchain Data Structures

Static & Dynamic Analysis



- MythX Plugin for Truffle [https://github.com/ConsenSys/truffle-security] - Security verification plugin for Truffle.
- Sabre [https://github.com/b-mueller/sabre] - Easy-to-use MythX security analyzer written in JavaScript.
- PythX [https://github.com/dmuhs/PythX] - MythX Python library and CLI tool.
- Mythril Classic [https://github.com/ConsenSys/mythril-classic] - Swiss army knife for smart contract security.
- Slither [https://github.com/trailofbits/slither] - Static analysis framework with detectors for many common Solidity issues. It has taint and value tracking capabilities and is written in Python.
- Echidna [https://github.com/trailofbits/echidna] - The only available fuzzer for Ethereum software. Uses property testing to generate malicious inputs that break smart contracts.
- Manticore [https://github.com/trailofbits/manticore] - Dynamic binary analysis tool with EVM support [https://asciinema.org/a/haJU2cl0R0Q3jB9wd733LVosL].
- Oyente [https://github.com/melonproject/oyente] - Analyze Ethereum code to find common vulnerabilities, based on this paper [http://www.comp.nus.edu.sg/~loiluu/papers/oyente.pdf].

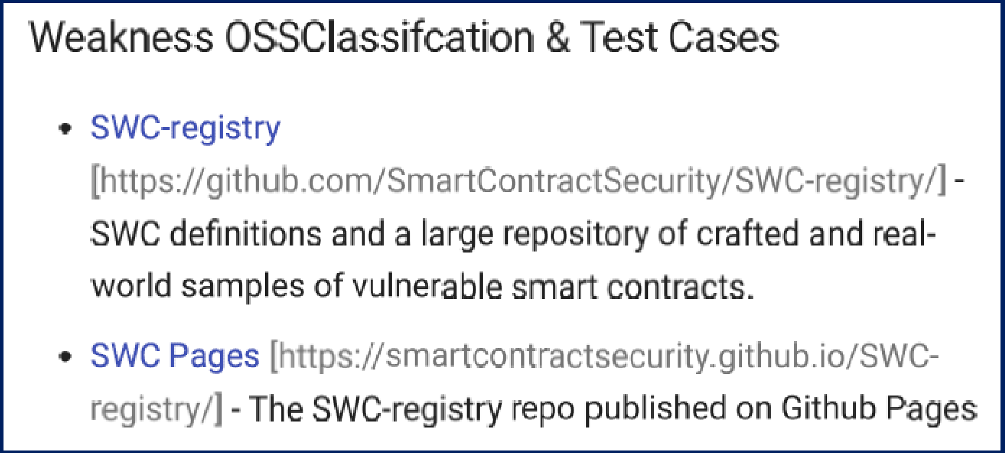


- Securify [https://securify.chainsecurity.com/] - Fully automated online static analyzer for smart contracts, providing a security report based on vulnerability patterns.
- SmartCheck [https://tool.smartdec.net] - Static analysis of Solidity source code for security vulnerabilities and best practices.
- Octopus [https://github.com/quoscient/octopus] - Security Analysis tool for Blockchain Smart Contracts with support of EVM and (e)WASM.

Source: Smart Contract Security: https://consensys.github.io/smart-contract-best-practices/

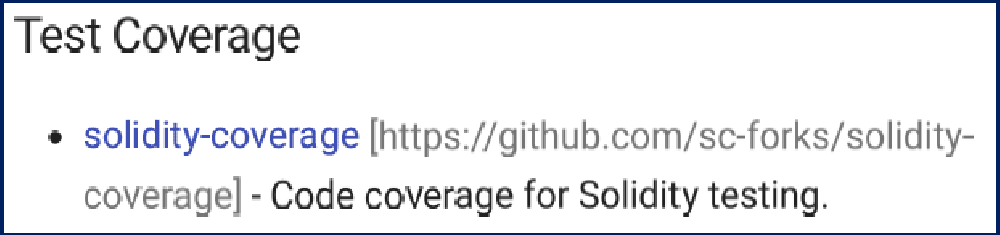
Slater Technologies

Security Tools for Auditing & Visualizing Transactions in Blockchain Data Structures



Weakness OSSClassifcation & Test Cases

- SWC-registry [https://github.com/SmartContractSecurity/SWC-registry/] - SWC definitions and a large repository of crafted and real-world samples of vulnerable smart contracts.
- SWC Pages [https://smartcontractsecurity.github.io/SWC-registry/] - The SWC-registry repo published on Github Pages



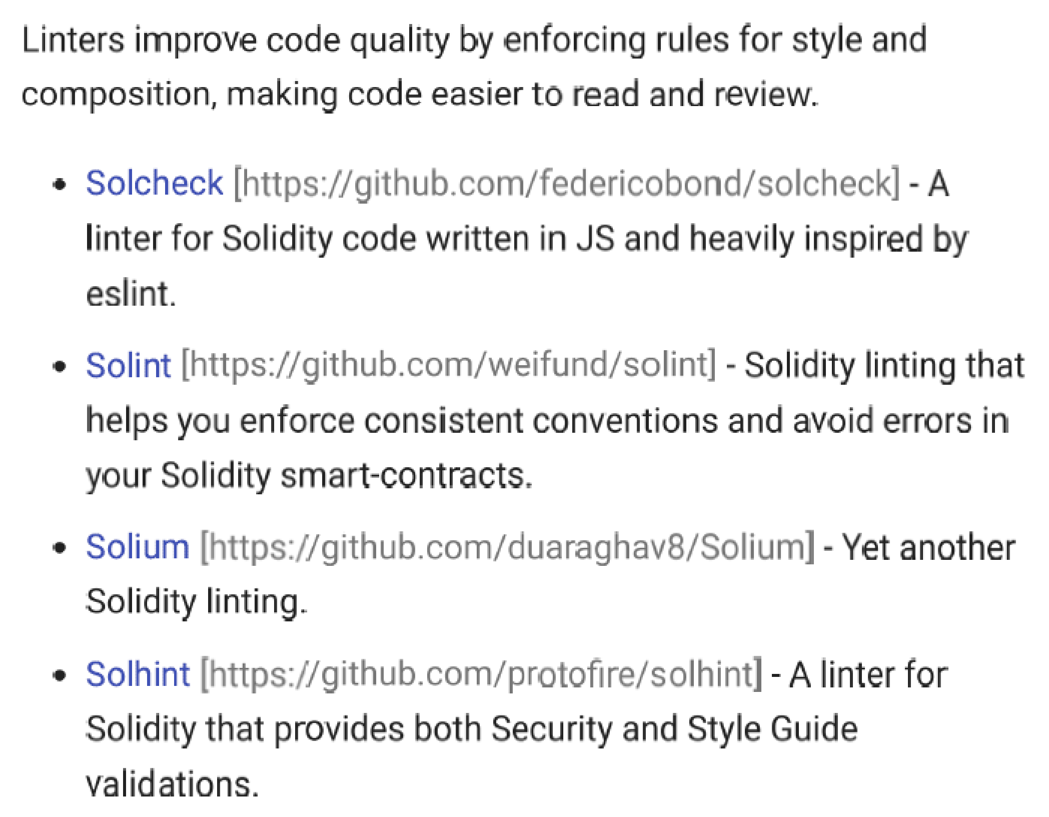
Test Coverage

- solidity-coverage [https://github.com/sc-forks/solidity-coverage] - Code coverage for Solidity testing.

Source: Smart Contract Security: https://consensys.github.io/smart-contract-best-practices/

Security Tools for Auditing & Visualizing Transactions in Blockchain Data Structures

Linters



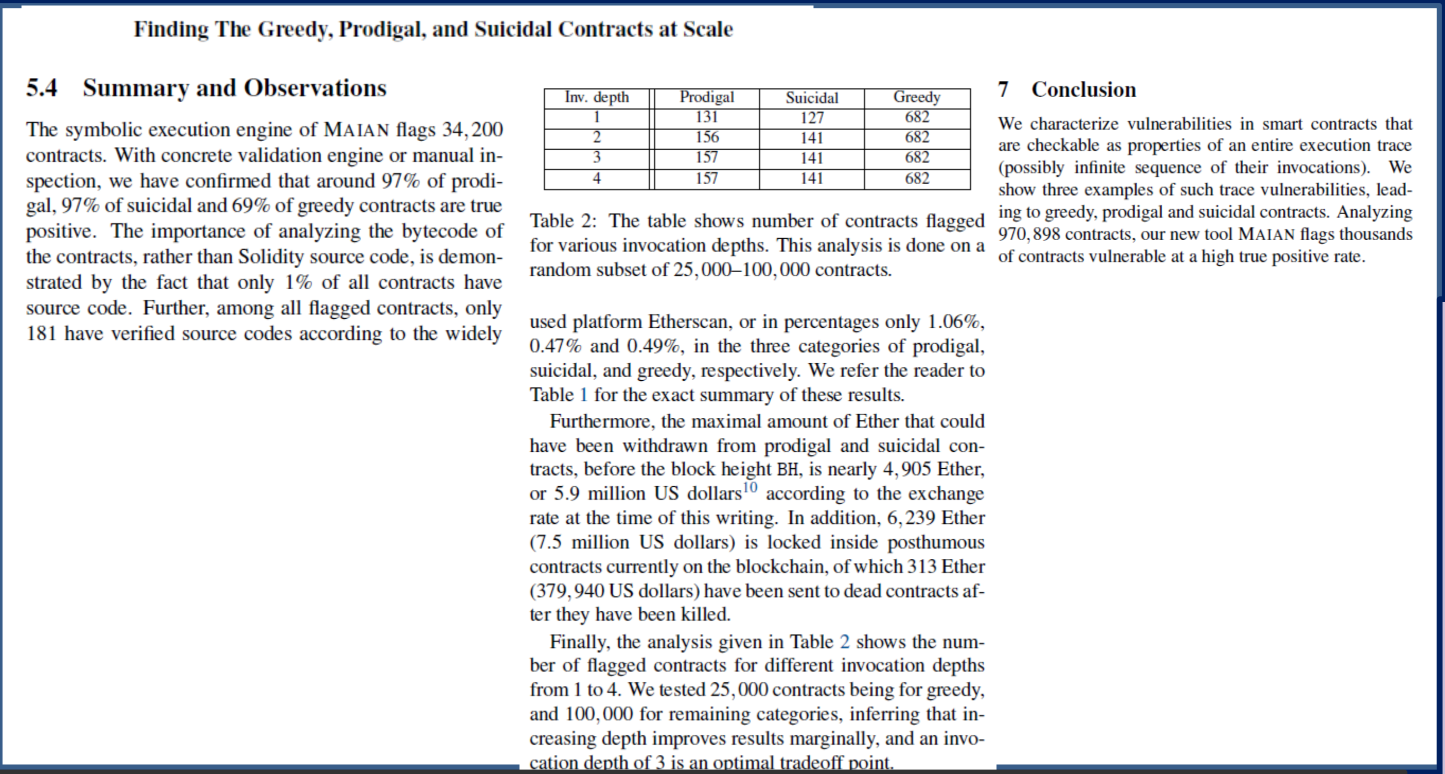
Linters improve code quality by enforcing rules for style and composition, making code easier to read and review.

- Solcheck [https://github.com/federicobond/solcheck] - A linter for Solidity code written in JS and heavily inspired by eslint.
- Solint [https://github.com/weifund/solint] - Solidity linting that helps you enforce consistent conventions and avoid errors in your Solidity smart-contracts.
- Solium [https://github.com/duaraghav8/Solium] - Yet another Solidity linting.
- Solhint [https://github.com/protofire/solhint] - A linter for Solidity that provides both Security and Style Guide validations.

Source: Smart Contract Security: https://consensys.github.io/smart-contract-best-practices/

Slater Technologies

Maian: Auditing Smart Contracts at Scale



Finding The Greedy, Prodigal, and Suicidal Contracts at Scale

5.4 Summary and Observations

The symbolic execution engine of MAIAN flags 34,200 contracts. With concrete validation engine or manual inspection, we have confirmed that around 97% of prodigal, 97% of suicidal and 69% of greedy contracts are true positive. The importance of analyzing the bytecode of the contracts, rather than Solidity source code, is demonstrated by the fact that only 1% of all contracts have source code. Further, among all flagged contracts, only 181 have verified source codes according to the widely used platform Etherscan, or in percentages only 1.06%, 0.47% and 0.49%, in the three categories of prodigal, suicidal, and greedy, respectively. We refer the reader to Table 1 for the exact summary of these results.

Inv. depth	Prodigal	Suicidal	Greedy
1	131	127	682
2	156	141	682
3	157	141	682
4	157	141	682

Table 2: The table shows number of contracts flagged for various invocation depths. This analysis is done on a random subset of 25,000–100,000 contracts.

Furthermore, the maximal amount of Ether that could have been withdrawn from prodigal and suicidal contracts, before the block height BH, is nearly 4,905 Ether, or 5.9 million US dollars[10] according to the exchange rate at the time of this writing. In addition, 6,239 Ether (7.5 million US dollars) is locked inside posthumous contracts currently on the blockchain, of which 313 Ether (379,940 US dollars) have been sent to dead contracts after they have been killed.

Finally, the analysis given in Table 2 shows the number of flagged contracts for different invocation depths from 1 to 4. We tested 25,000 contracts being for greedy, and 100,000 for remaining categories, inferring that increasing depth improves results marginally, and an invocation depth of 3 is an optimal tradeoff point.

7 Conclusion

We characterize vulnerabilities in smart contracts that are checkable as properties of an entire execution trace (possibly infinite sequence of their invocations). We show three examples of such trace vulnerabilities, leading to greedy, prodigal and suicidal contracts. Analyzing 970,898 contracts, our new tool MAIAN flags thousands of contracts vulnerable at a high true positive rate.

Prodigal - Leak them carelessly to arbitrary users

Suicidal - Can be killed by anyone

Greedy - Lock funds Indefinitely

Bottom Line: three to four percent of the smart contracts on Ethereum's blockchain still contain trace vulnerabilities, according to the researchers' new analysis methodology.

Sources: https://www.reddit.com/r/Bitcoin/comments/7ys5nq/pdf_finding_the_greedy_prodigal_and_suicidal/ and https://bitsonline.com/singapore-research-ethereum/

Slater Technologies

Maian: Auditing Smart Contracts at Scale

Opacity Is Hampering Ethereum Security

Another interesting point raised in the paper is the unavailability of smart contract source code for Ethereum smart contracts, estimating the number at only one percent of the 970 thousand contracts they analyzed.

Fixing serious security vulnerabilities at scale requires **peer review**, and the **culture of propriety on the Ethereum network** forced the research team to directly analyze EVM bytecode instead of the sources to complete their research. Were the source code for these contracts more available and reviewed, Trace Vulnerabilities on Ethereum may not have proliferated in the first place.

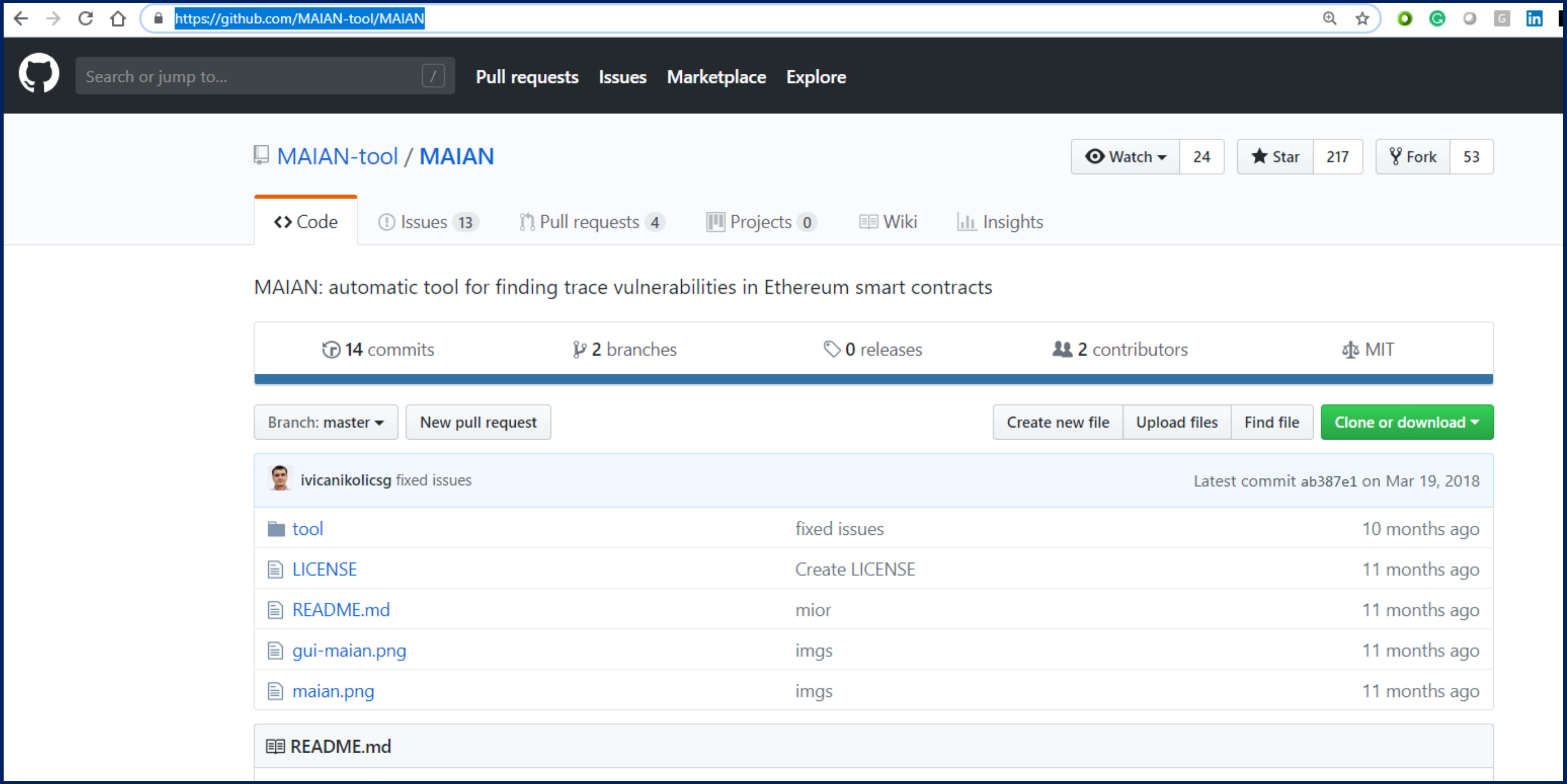
Bottom Line: three to four percent of the smart contracts on Ethereum's blockchain still contain trace vulnerabilities, according to the researchers' new analysis methodology.

Sources: https://www.reddit.com/r/Bitcoin/comments/7ys5nq/pdf_finding_the_greedy_prodigal_and_suicidal/ and https://bitsonline.com/singapore-research-ethereum/

Slater Technologies

Maian: Auditing Smart Contracts at Scale

This tool is Open Source and it’s FREE on Github!



https://github.com/MAIAN-tool/MAIAN

MAIAN-tool / MAIAN

MAIAN: automatic tool for finding trace vulnerabilities in Ethereum smart contracts

14 commits · 2 branches · 0 releases · 2 contributors · MIT

ivicanikolicsg fixed issues — Latest commit ab387e1 on Mar 19, 2018

tool	fixed issues	10 months ago
LICENSE	Create LICENSE	11 months ago
README.md	mior	11 months ago
gui-maian.png	imgs	11 months ago
maian.png	imgs	11 months ago

README.md

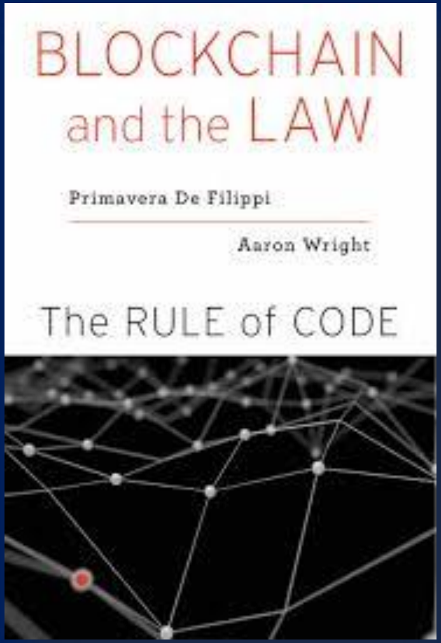
Source https://github.com/MAIAN-tool/MAIAN

Slater Technologies

Blockchain and the Law

Blockchain & The Law

- Blockchain establishes ownership, confirmed transactions, control, and transfer of ownership.
- Blockchain will force lawyers to understand technology better
- Blockchain could also make room for “smart contracts,” where assets would be transferred automatically once certain conditions are met.
- Blockchain could resolve disputes very directly and efficiently, saving lawyers and their clients a great deal of work. This also could mean the end of escrow accounts where the law firm holds onto money and distributes funds once conditions have been met.
- Contracts and transactions could be a logical first-step in the blockchain adoption journey.
- Blockchain could very well improve the effectiveness of the criminal justice system;
- If corporations and websites agree to give law firms access to records automatically collected through blockchain, those records could cause new, reliable evidence to surface more quickly.
- Expect that those with evidence on their side will embrace this concept, and others will prefer to drag their adversary through a drawn-out process.
- As more companies adopt Blockchain technologies and require their third-party suppliers to adopt Blockchain technologies, expect this requirement to be written into legally binding business contracts.



BLOCKCHAIN and the LAW

Primavera De Filippi

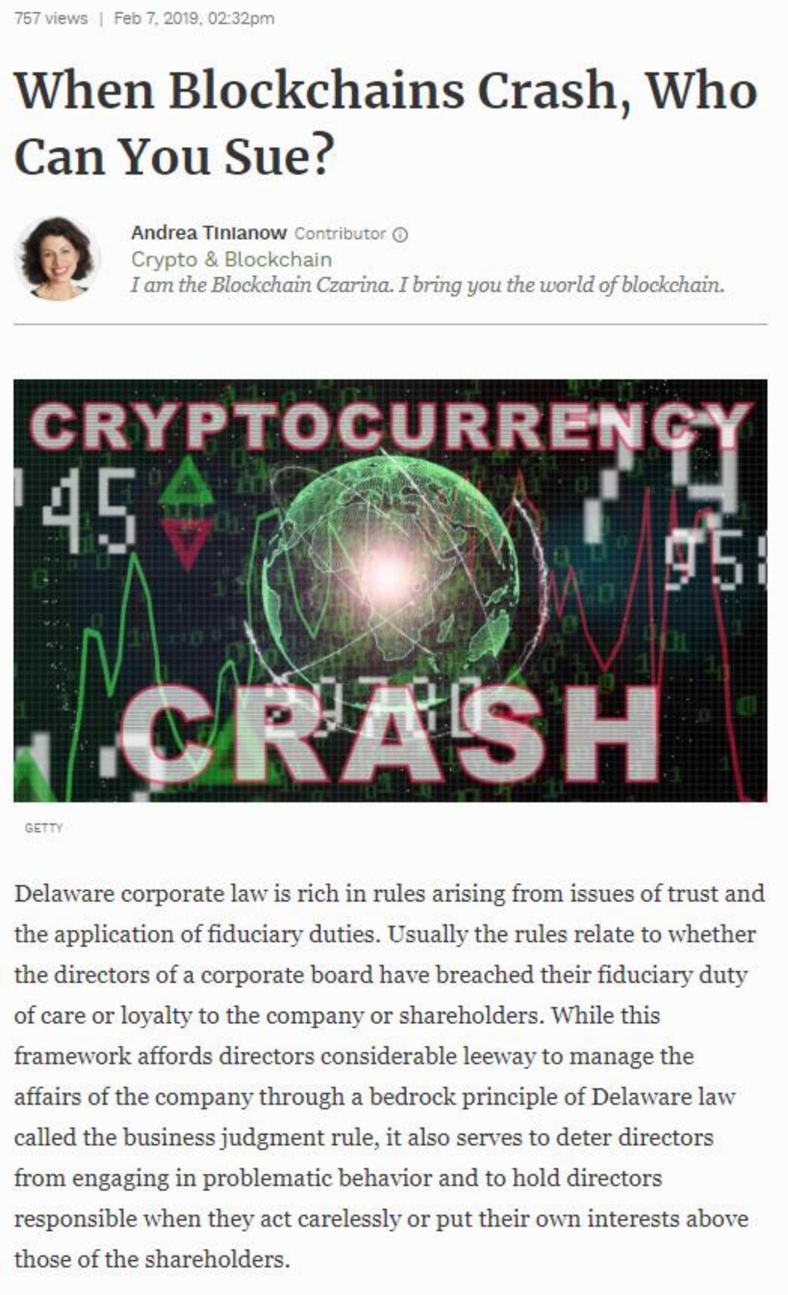
Aaron Wright

The RULE of CODE

For more information
Get
Blockchain & the Law
By Primavera De Filippi
And Aaron Wright, 2018

Source: https://www.forbes.com/sites/ianaltman/2018/06/29/blockchain-changes-business-law/#698d3605cb9f

When Blockchains Crash, Who Can We Sue?



757 views | Feb 7, 2019, 02:32pm

When Blockchains Crash, Who Can You Sue?

Andrea Tinianow Contributor ⓘ
Crypto & Blockchain
I am the Blockchain Czarina. I bring you the world of blockchain.

GETTY

Delaware corporate law is rich in rules arising from issues of trust and the application of fiduciary duties. Usually the rules relate to whether the directors of a corporate board have breached their fiduciary duty of care or loyalty to the company or shareholders. While this framework affords directors considerable leeway to manage the affairs of the company through a bedrock principle of Delaware law called the business judgment rule, it also serves to deter directors from engaging in problematic behavior and to hold directors responsible when they act carelessly or put their own interests above those of the shareholders.

Published February 7, 2019 at Forbes.com

Source: https://www.forbes.com/sites/andreatinianow/2019/02/07/when-blockchains-crash-whom-can-you-sue/#760e20707775

Slater Technologies

Blockchain & The Law

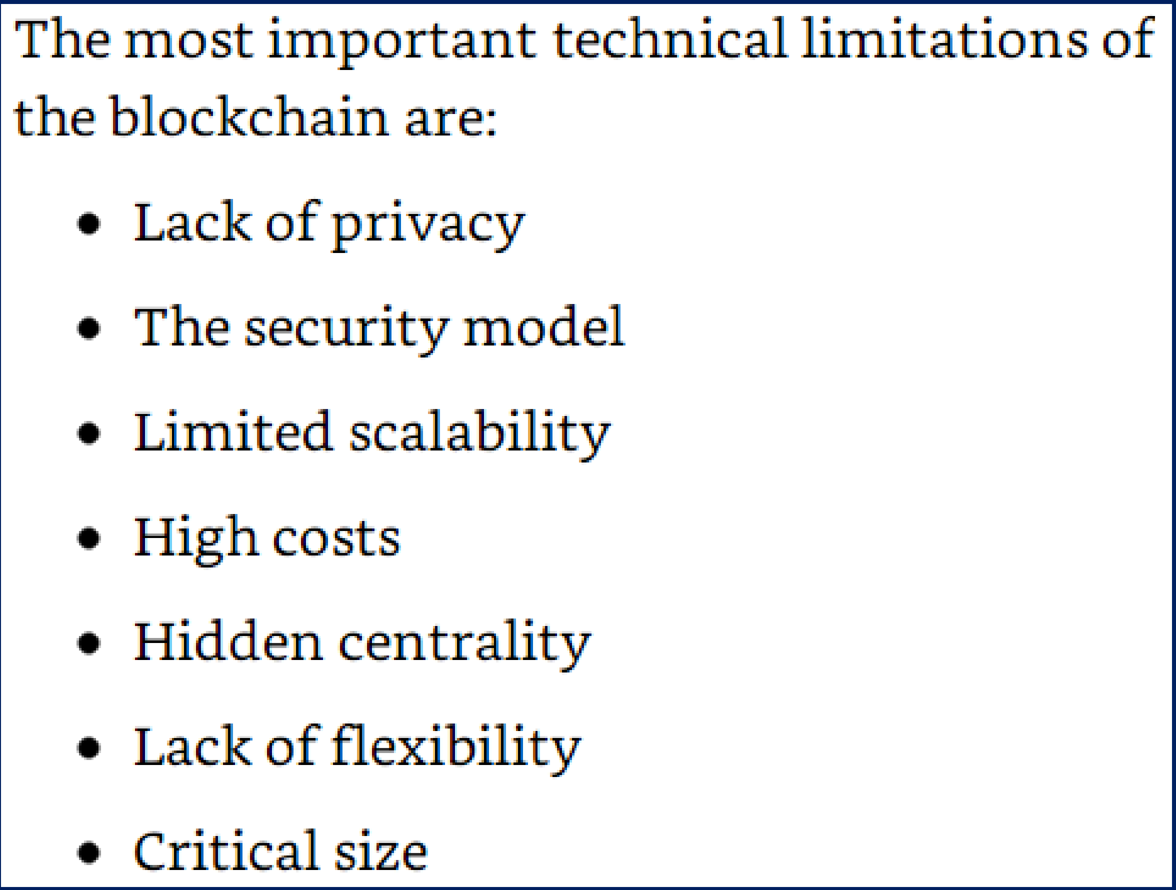
Nelson Rosario
Chicago
https://www.linkedin.com/in/nelsonrosario/

Ms. Puneet Bhasin
Mumbai, India
https://www.linkedin.com/in/advpuneetbhasincyberlawyer/

Slater Technologies

Blockchain Limits and Challenges

Technical Limitations



The most important technical limitations of the blockchain are:

- Lack of privacy
- The security model
- Limited scalability
- High costs
- Hidden centrality
- Lack of flexibility
- Critical size

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Slater Technologies

Technical Limitations

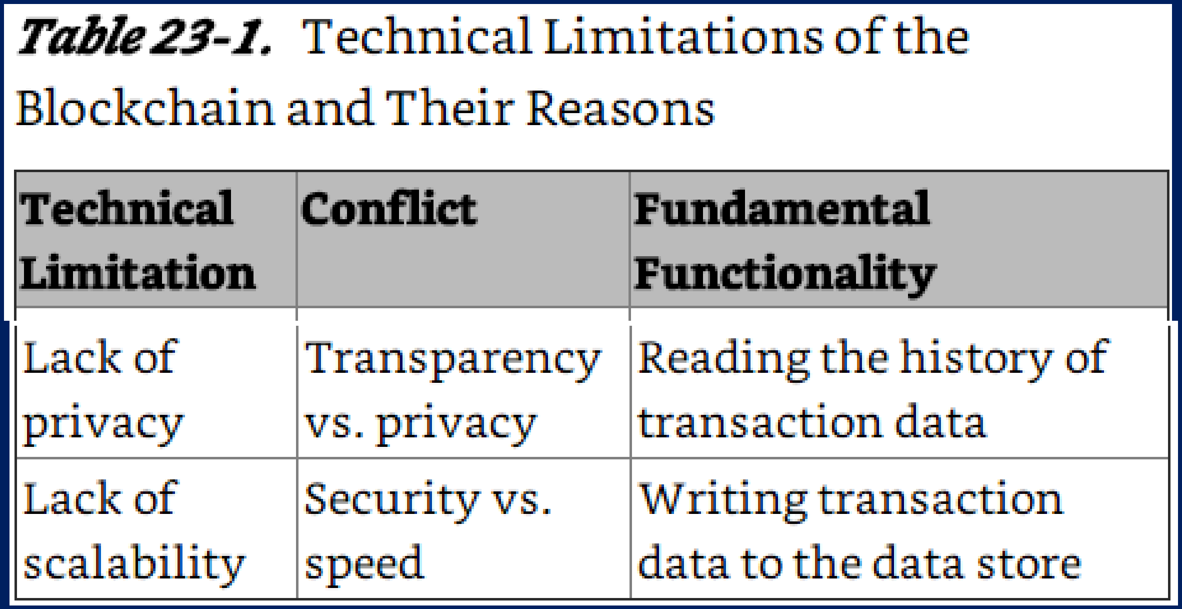
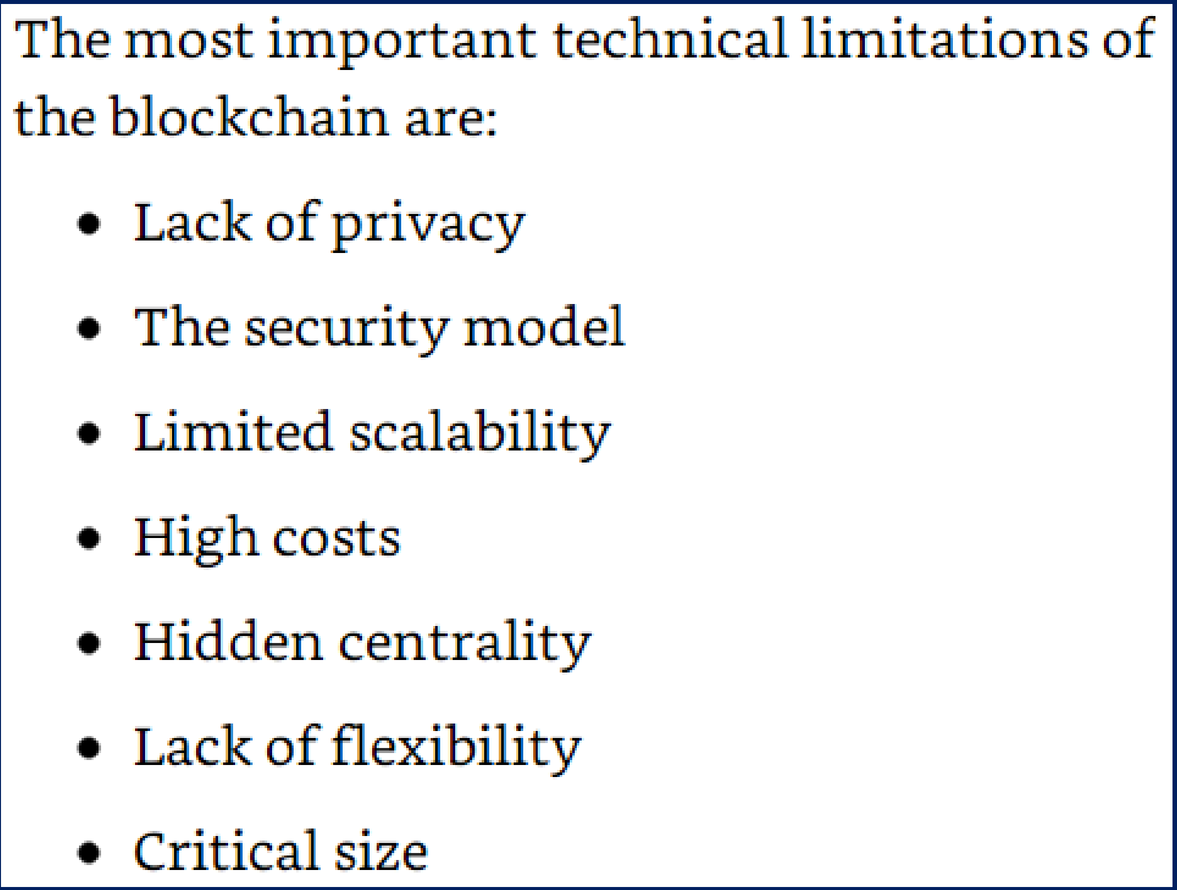


Table 23-1. Technical Limitations of the Blockchain and Their Reasons

Technical Limitation	Conflict	Fundamental Functionality
Lack of privacy	Transparency vs. privacy	Reading the history of transaction data
Lack of scalability	Security vs. speed	Writing transaction data to the data store

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Technical Limitations



The most important technical limitations of the blockchain are:

- Lack of privacy
- The security model
- Limited scalability
- High costs
- Hidden centrality
- Lack of flexibility
- Critical size

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Slater Technologies

Limits and Challenges

- Scalability
- Performance (Bitcoin – 600 seconds / block; Ethereum, 14 to 17 seconds / block)
- Security, especially with user wallets
- Weaknesses in the technologies, i.e. deployment of bad contracts, can cause very expensive blunders and loss of confidence and reputation
- Finding the right people to develop DApps and manage the technologies
- Resistance to change
- Anti-trust issues (Norton Rose Fulbright):
  - Does blockchain allow for improper information sharing and facilitate collusion among competitors?
  - Do blockchain standards and rules create or enhance market power by favoring one or several industry participant(s) over others?
  - Does a permissioned blockchain amount to a concerted refusal to deal?

Source: Drescher, D. (2017). Blockchain Basics. Frankfort am Main, Germany: Apress.

Ethereum Blockchain DApps and Dapp Design & Development

Overview of Ethereum

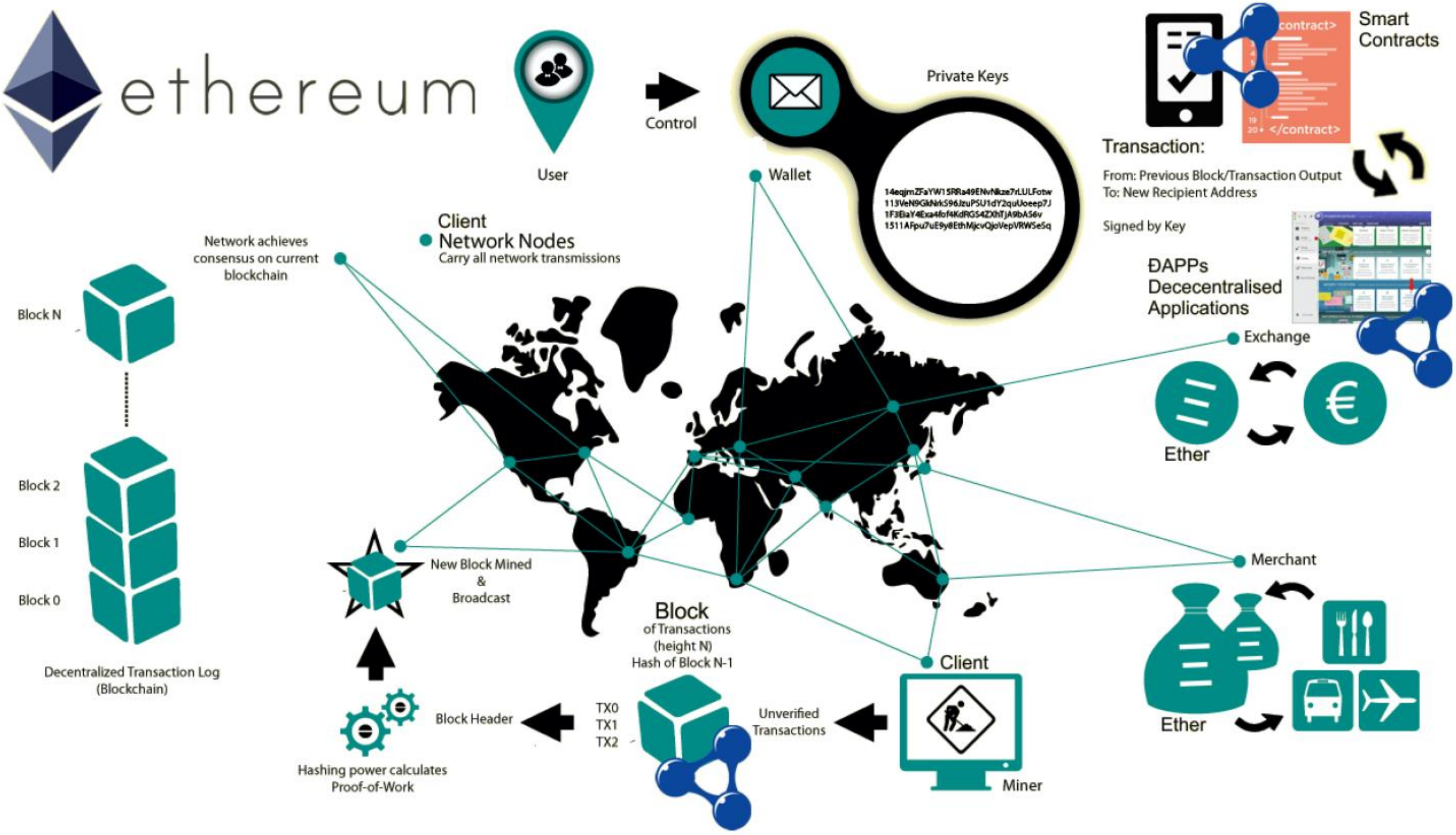


Fig. 6. Ethereum framework elements, modified from [39, p.16]

Slater Technologies

Source: https://www.researchgate.net/publication/315619465_A_more_pragmatic_Web_30_Linked_Blockchain_Data

Ethereum DApp Architecture

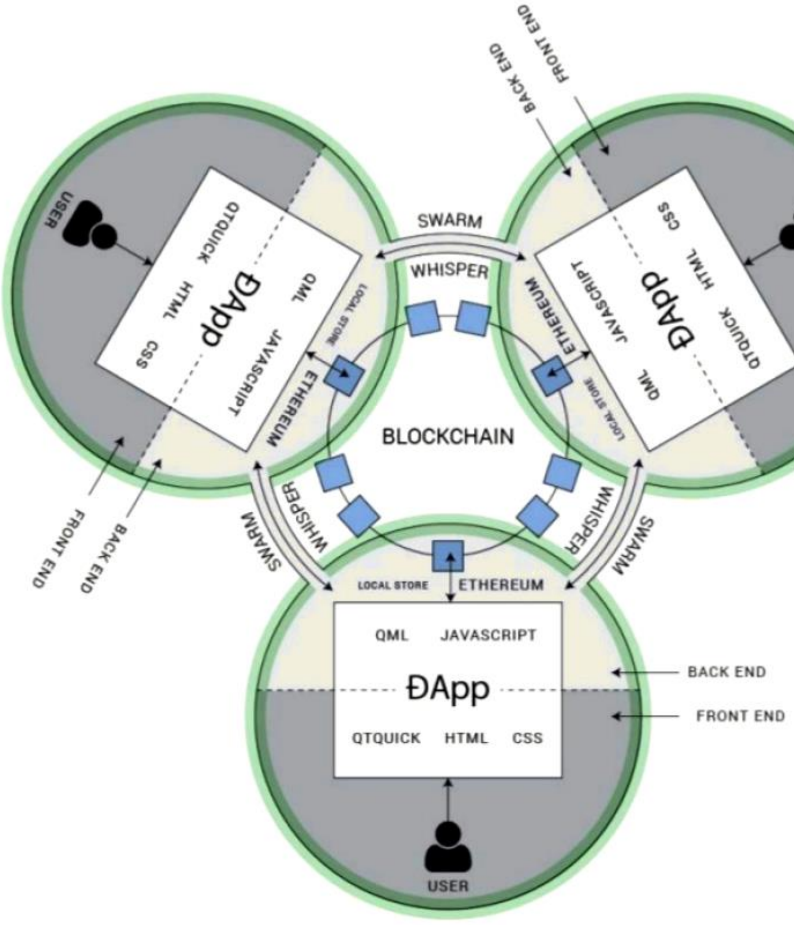
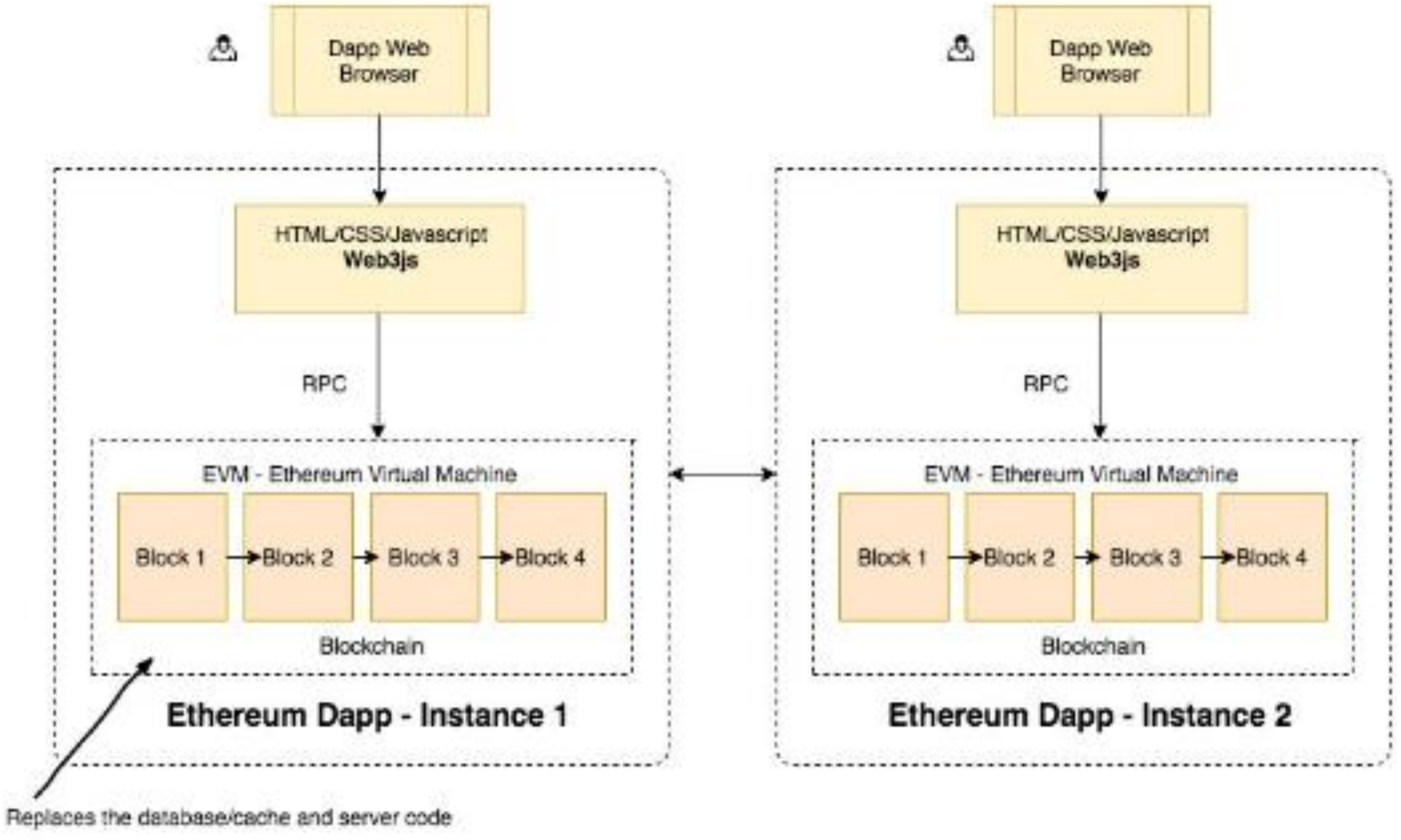


Fig. 11. Ethereum Architecture [52]

Slater Technologies

Source: https://www.researchgate.net/publication/315619465_A_more_pragmatic_Web_30_Linked_Blockchain_Data



High-Level DApp Architecture

Figure 4.1: High-level DApp architecture, Source: Mahesh Murthy, medium.com

Source: Ethereum Smart Contract Development by Mayukh Mukhopadhyay

Slater Technologies

Web3.js Tech Stack

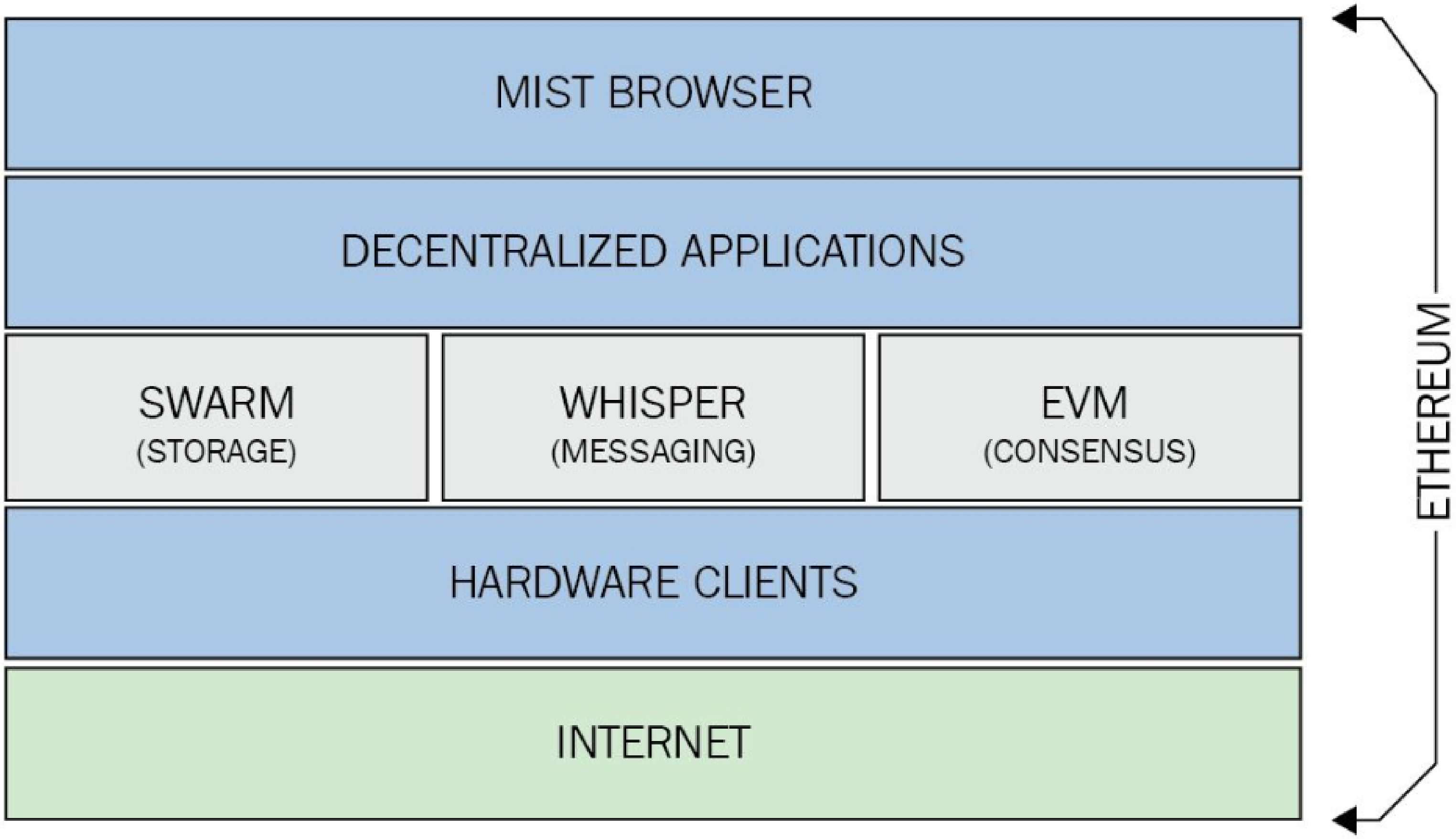
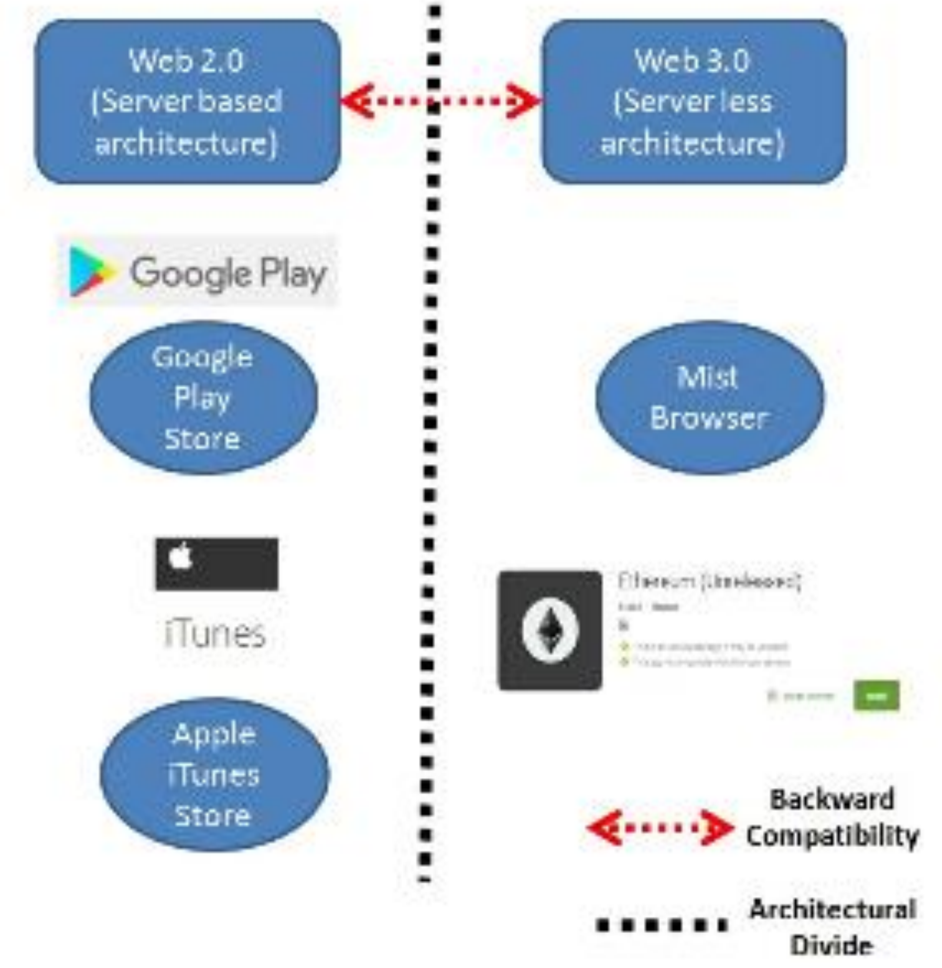


Figure 2.4: Web 3.0 tech stack for Ethereum, Source: Ethereum stack exchange

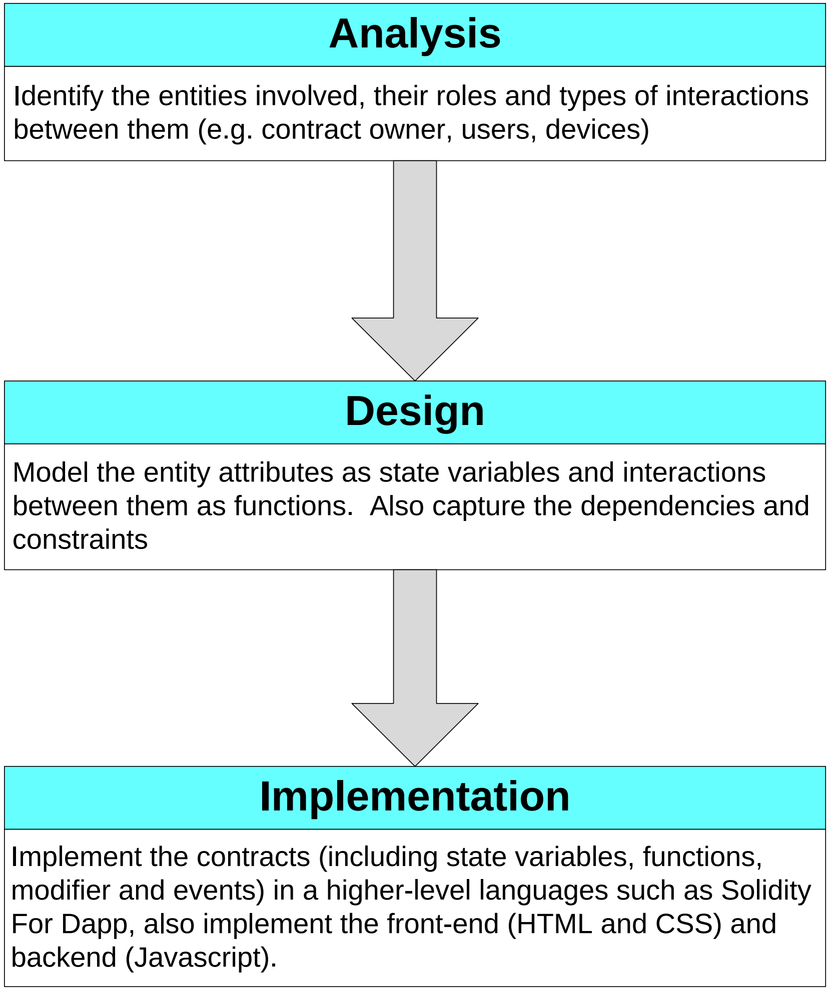
Web Apps and DApps - Compared



Slater Technologies

DApp Development Steps

1. Analysis
2. Design
3. Implementation



Analysis

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

Design

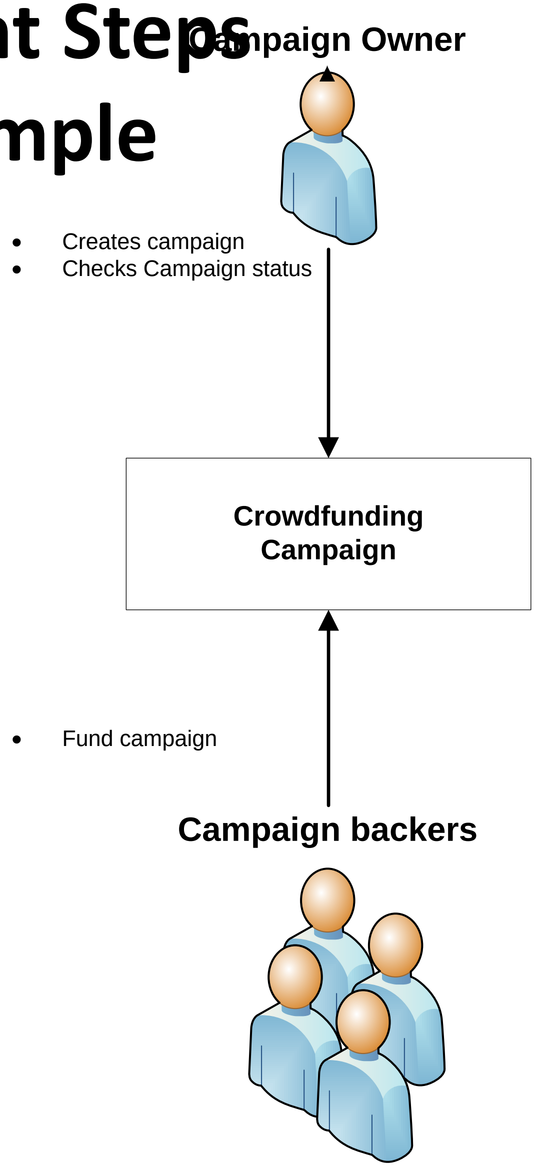
Model the entity attributes as state variables and interactions between them as functions. Also capture the dependencies and constraints

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).

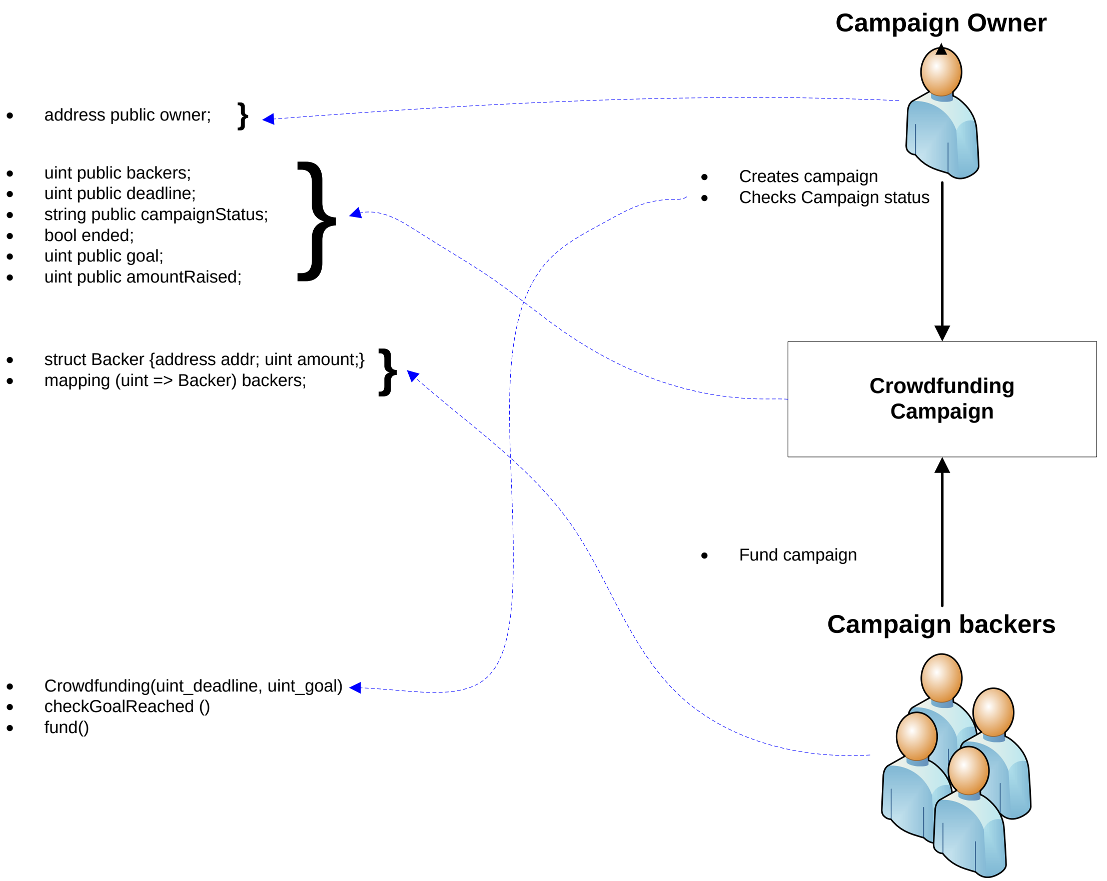
Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

DApp Development Steps – Analysis - Example



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

DApp Development Steps – Design - Example



- 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;

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

Campaign Owner

- Creates campaign
- Checks Campaign status

Crowdfunding Campaign

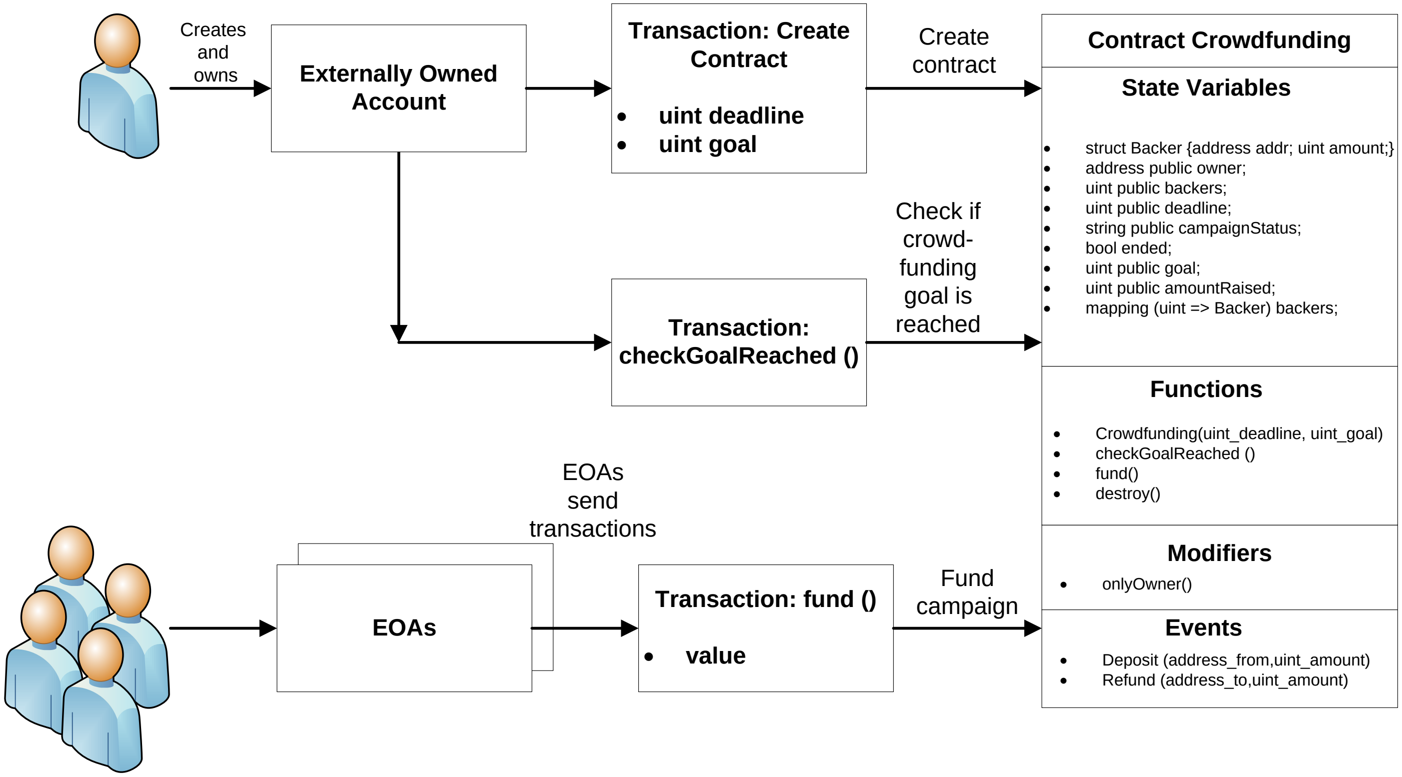
- Fund campaign

Campaign backers

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

DApp Development Steps – Implementation - Example

(Example Business Case: Crowdfunding Application)



Creates and owns

Externally Owned Account

Transaction: Create Contract

- **uint deadline**
- **uint goal**

Create contract

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;

Transaction: checkGoalReached ()

Check if crowd-funding goal is reached

Functions

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

EOAs send transactions

EOAs

Transaction: fund ()

- **value**

Fund campaign

Modifiers

- onlyOwner()

Events

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

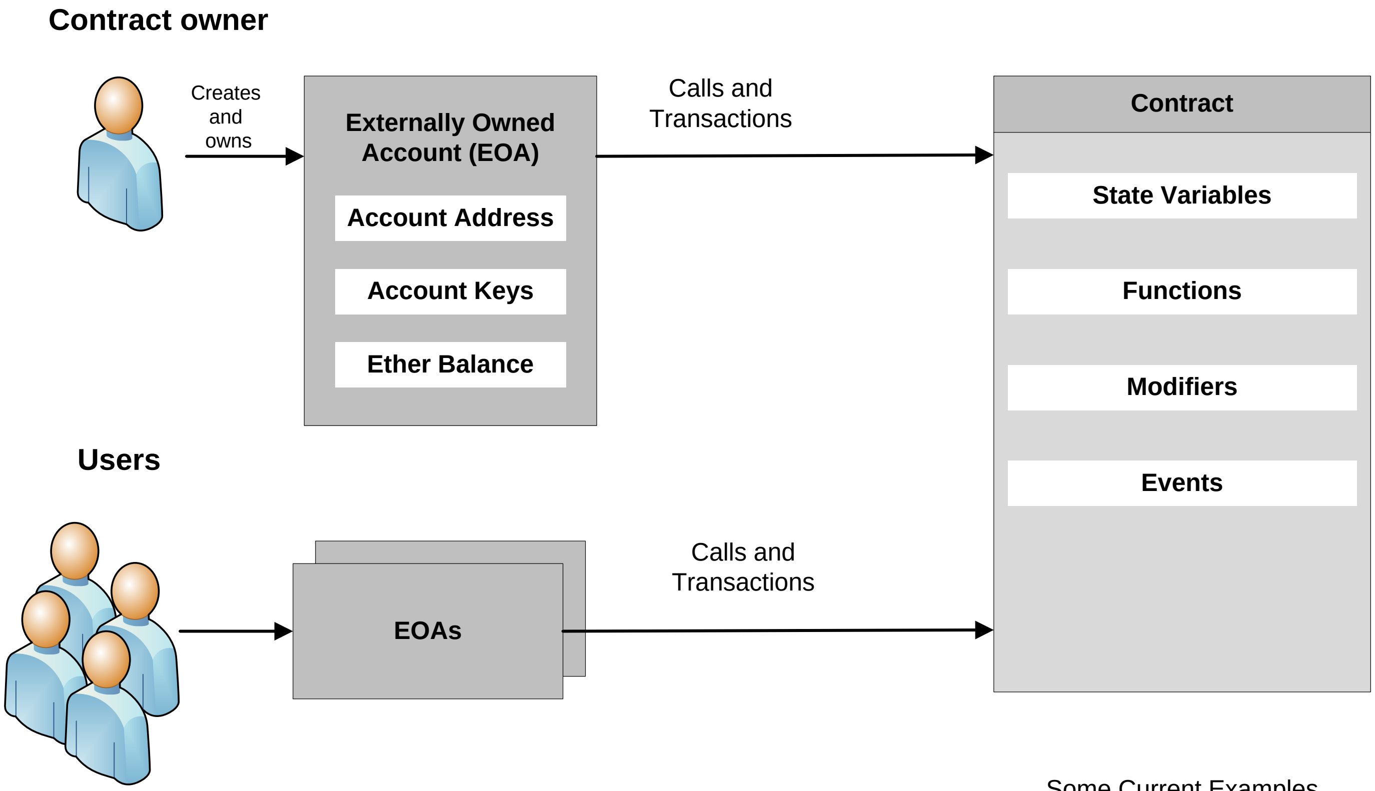
Source: Blockchain Applications: A Hands-on Approach by Arsheep Bahga and Vijay Madisetti

BLOCKCHAIN APPLICATION TEMPLATES

Slater Technologies

Blockchain Application Templates

Many-to-One



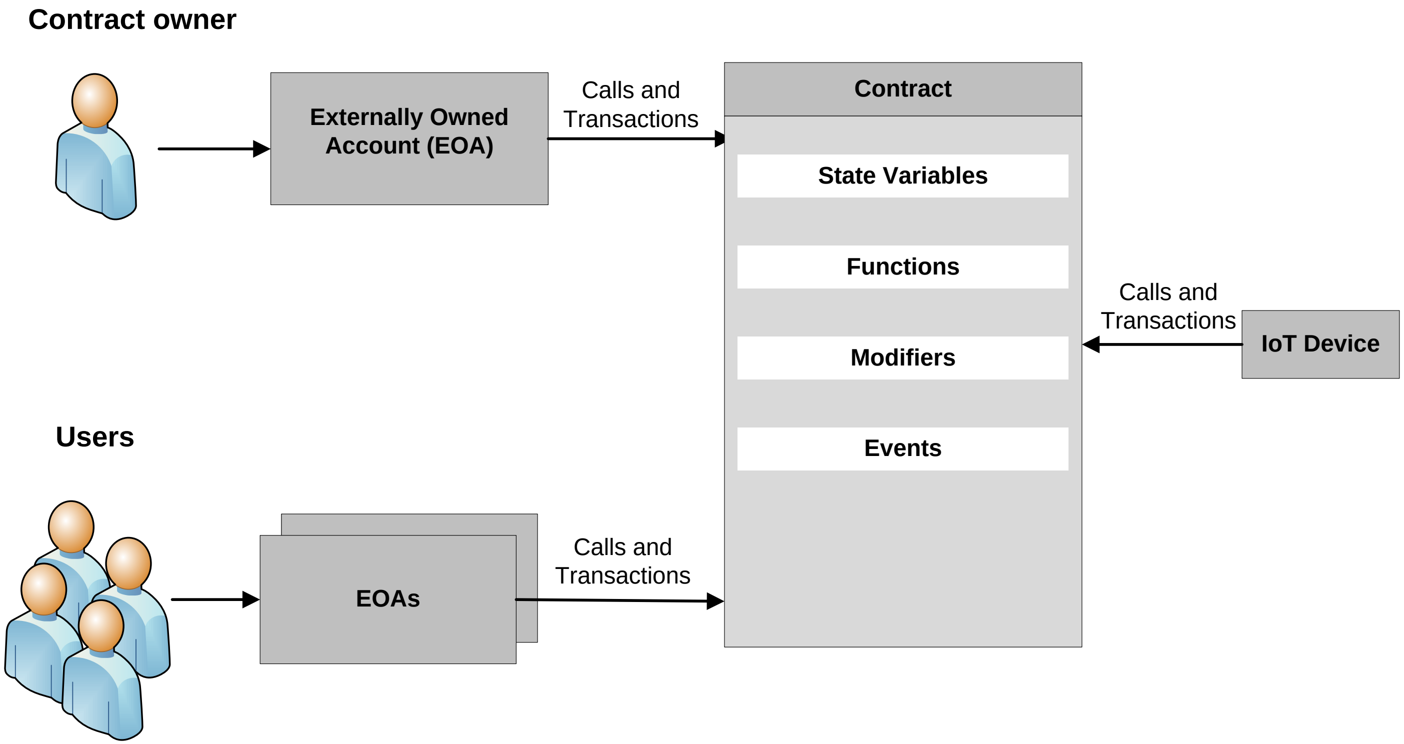
Some Current Examples

- Crowdfunding
- Event Registration
- Voting
- Name Registration

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

Blockchain Application Templates

Many-to-One for IoT Applications



Some Current Examples

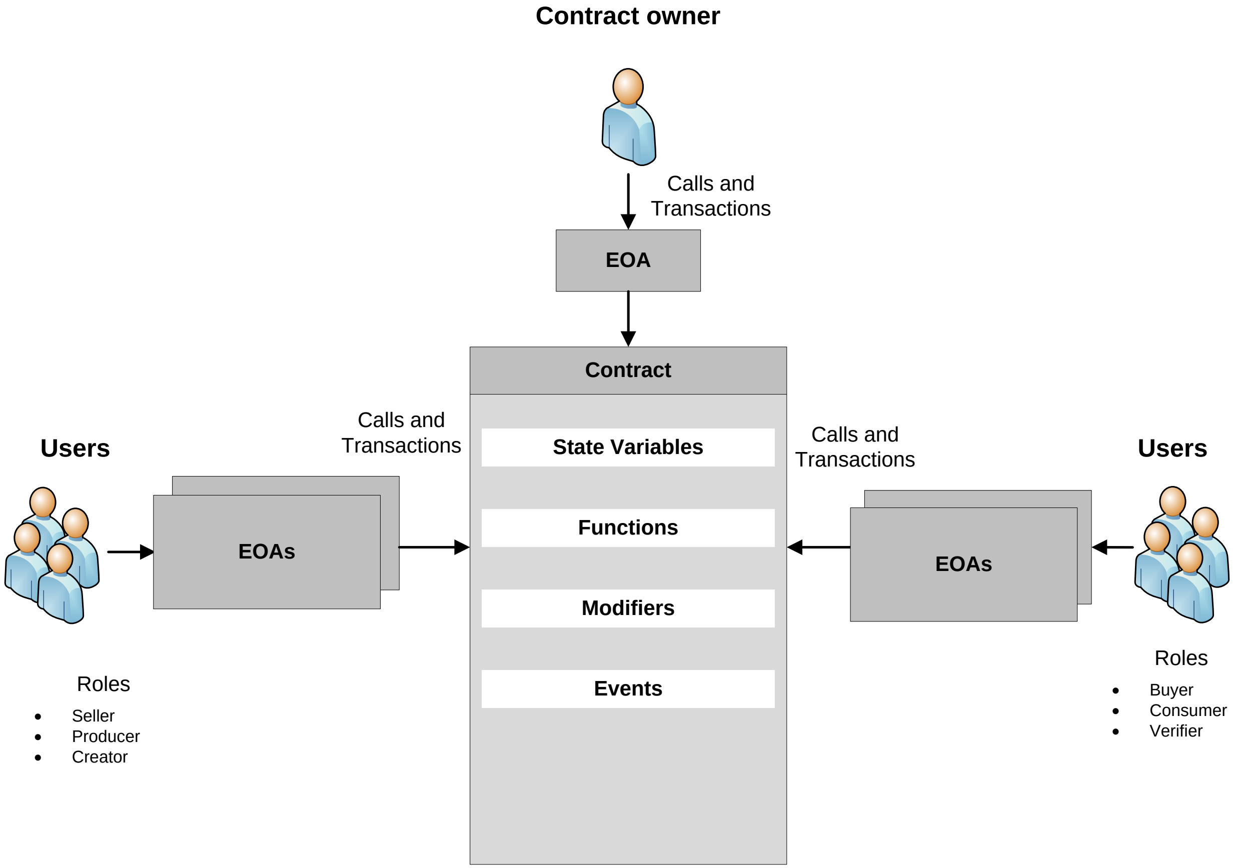
- Solar charging stations
- Smart switch

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

Slater Technologies

Blockchain Application Templates

Many-to-One for Financial Applications



Roles

- Seller
- Producer
- Creator

Roles

- Buyer
- Consumer
- Verifier

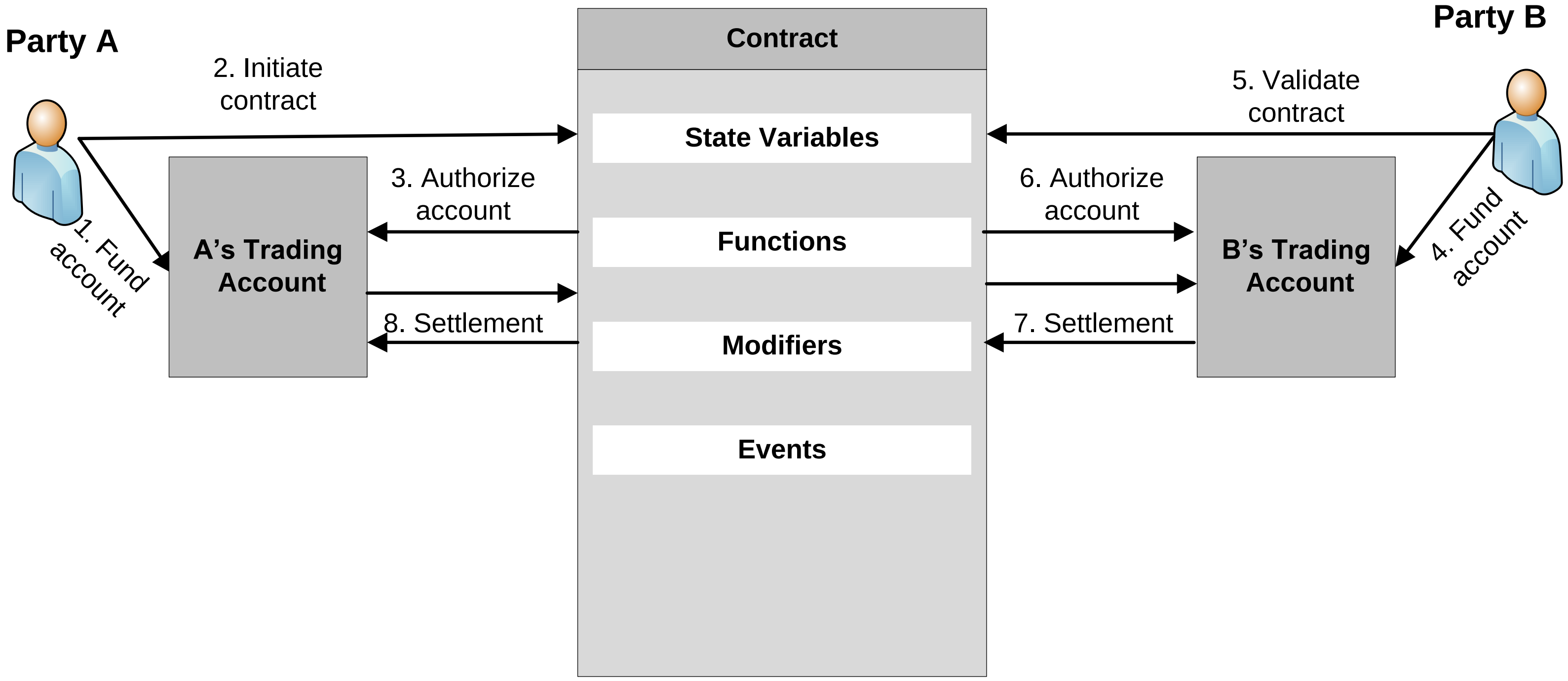
Some Current Examples

- Product sales
- Stock photos
- Document verification

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

Blockchain Application Templates

Many-to-Many or Peer-to-Peer

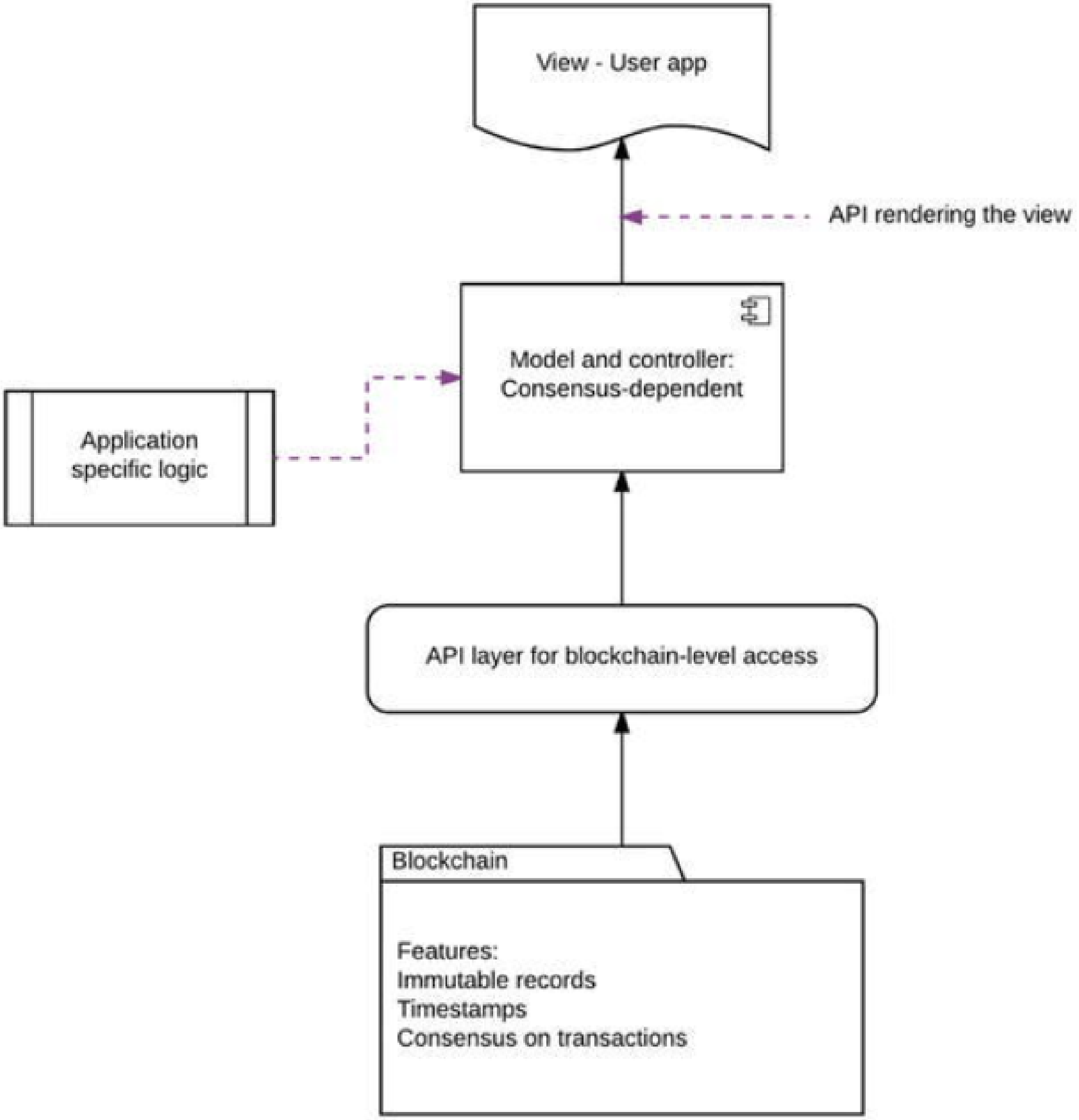


Some Current Examples

- Call option
- Interest rate swap

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

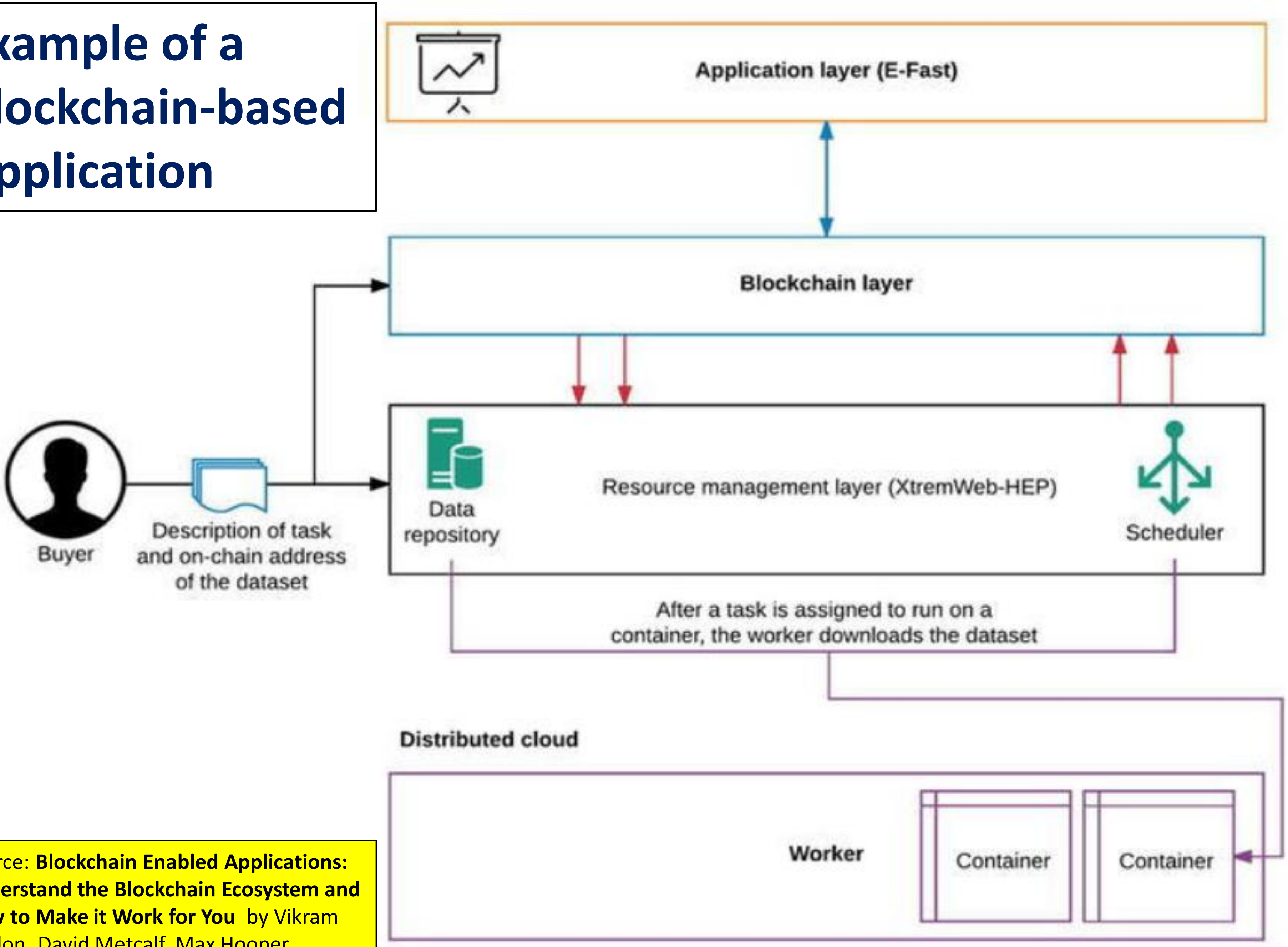
Simple Blockchain Application Model



Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

Slater Technologies

Example of a Blockchain-based Application

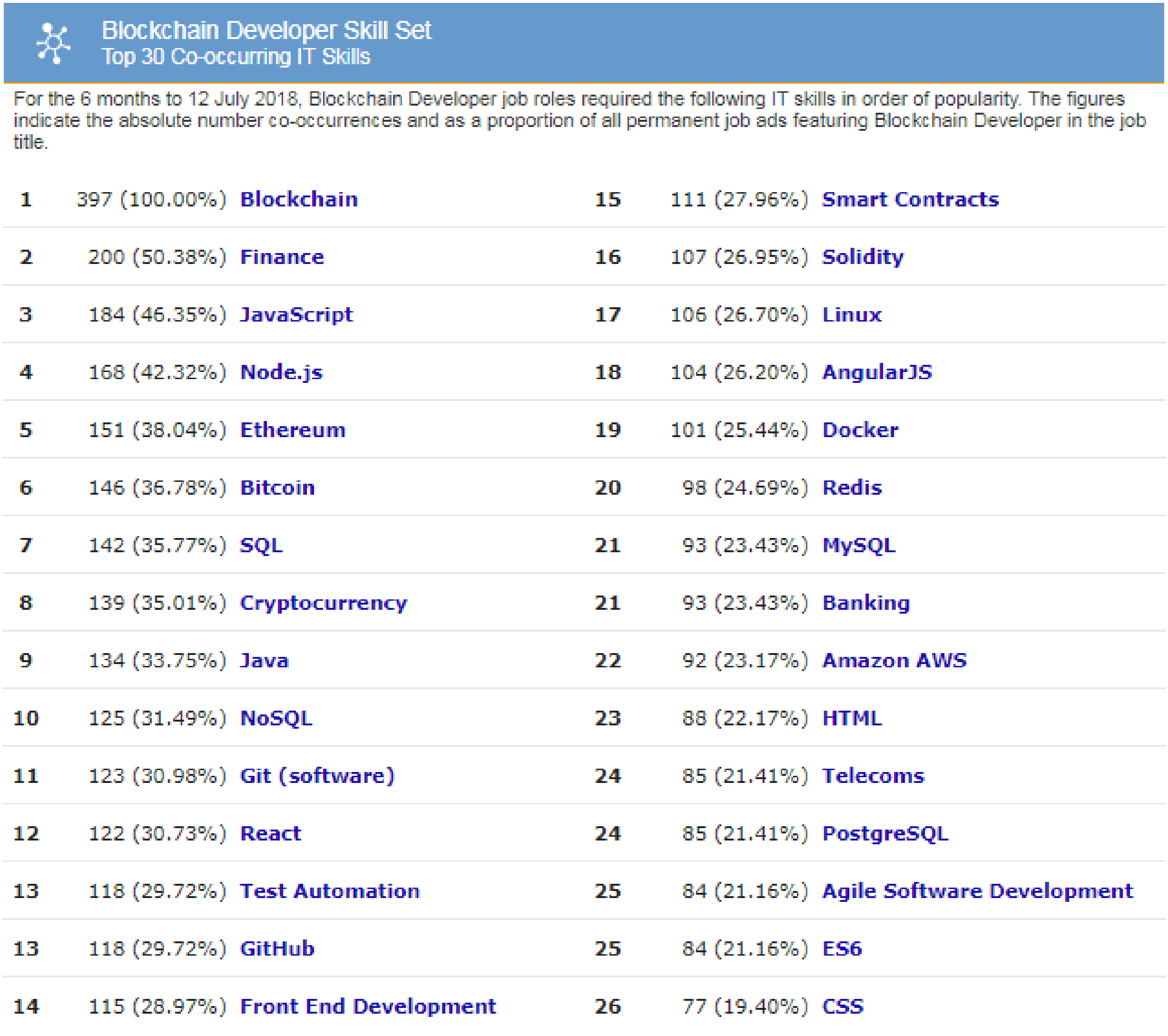

Application layer (E-Fast)
Blockchain layer
Buyer
Description of task and on-chain address of the dataset
Data repository
Resource management layer (XtremWeb-HEP)
Scheduler
After a task is assigned to run on a container, the worker downloads the dataset
Distributed cloud
Worker
Container
Container

Source: **Blockchain Enabled Applications: Understand the Blockchain Ecosystem and How to Make it Work for You** by Vikram Dhillon, David Metcalf, Max Hooper

HOW TO HELP YOUR ORGANIZATION RAPIDLY RAMP UP SKILLS AND READINESS FOR BLOCKCHAIN APPLICATION DEVELOPMENT

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

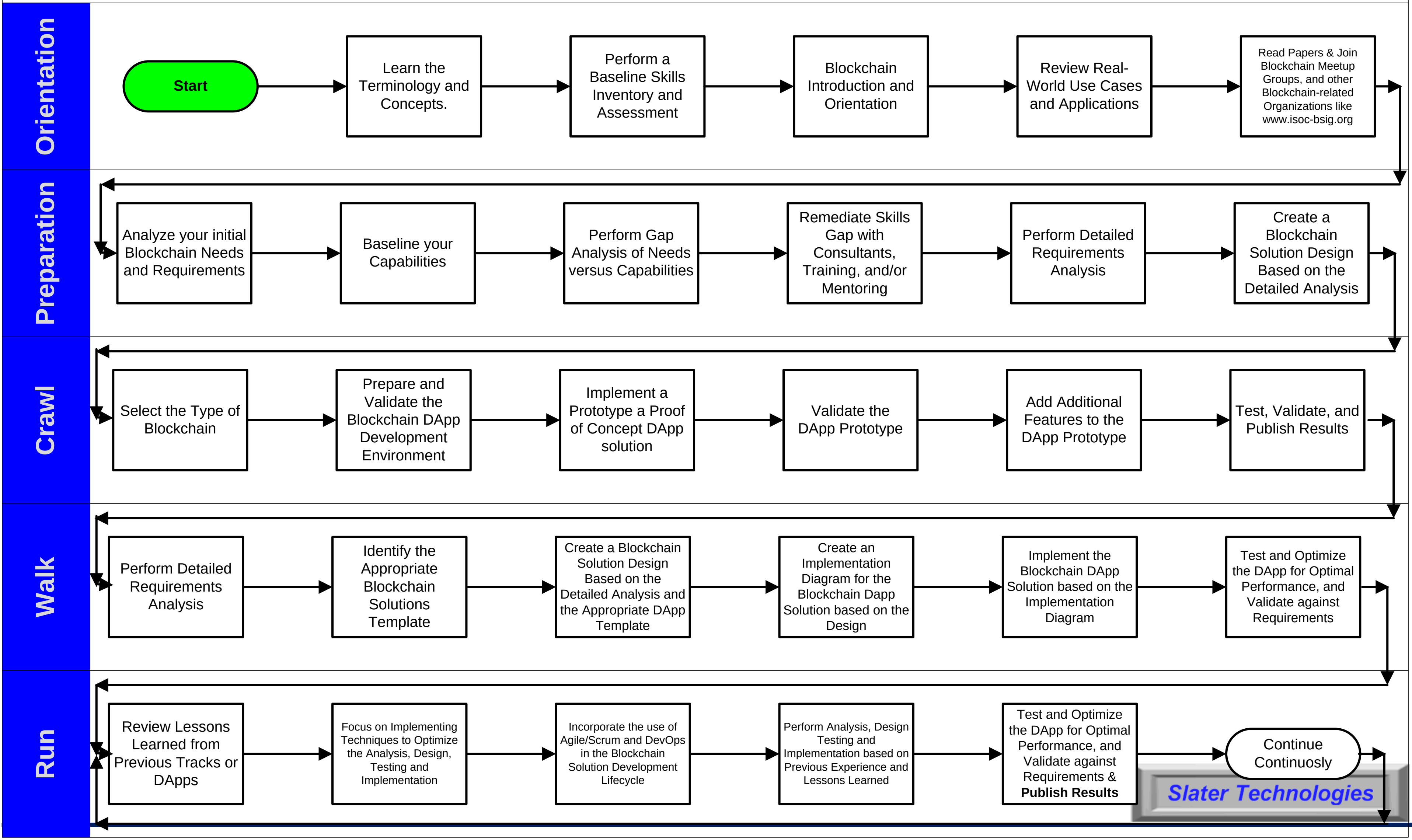
Slater Technologies

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 &
PROGRAM MANAGEMENT!

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

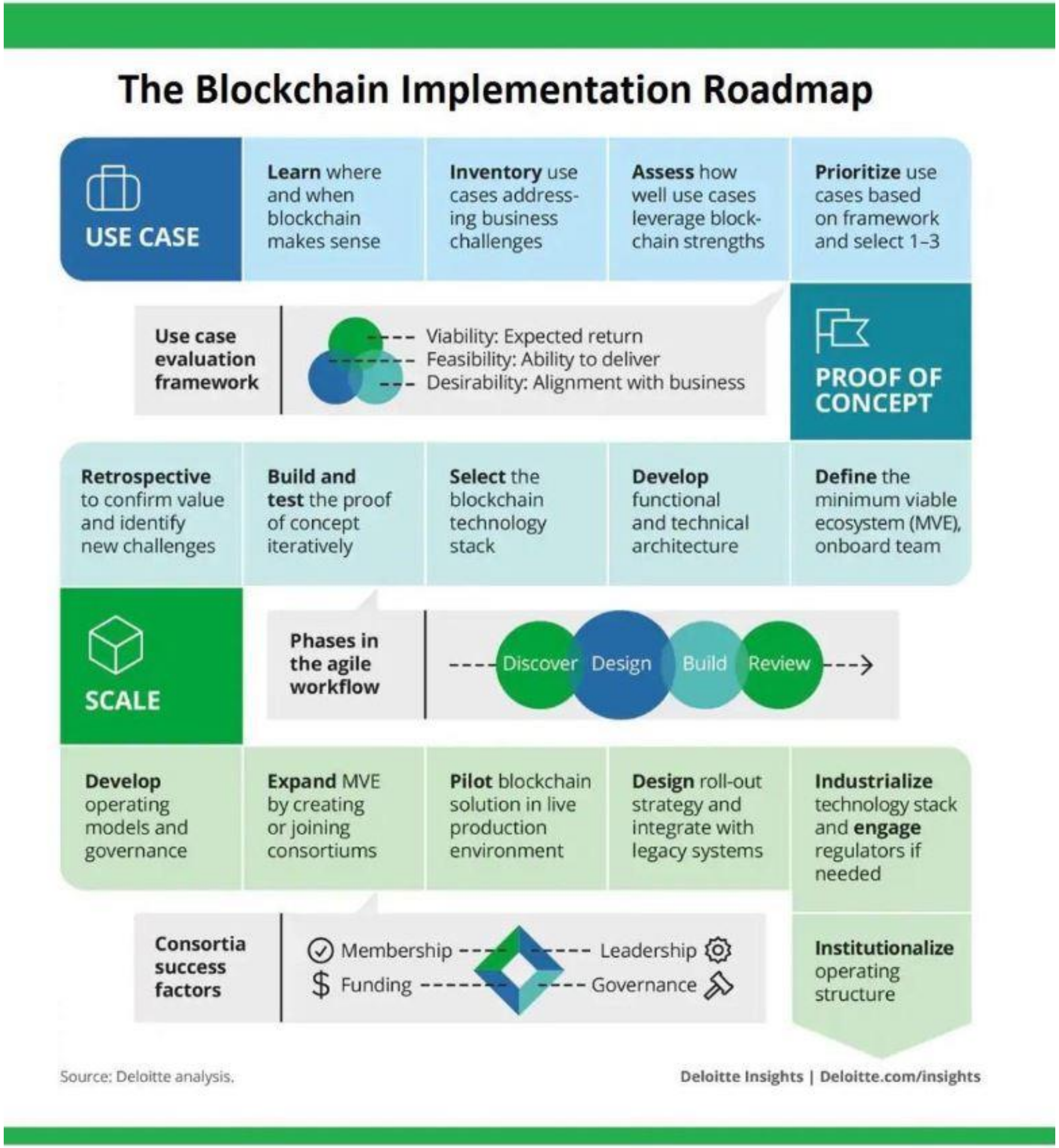
Incorporate the use of Agile/Scrum and DevOps in the Blockchain Solution Development Lifecycle

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

Slater Technologies



The Blockchain Implementation Roadmap

USE CASE

- **Learn** where and when blockchain makes sense
- **Inventory** use cases addressing business challenges
- **Assess** how well use cases leverage blockchain strengths
- **Prioritize** use cases based on framework and select 1–3

Use case evaluation framework

- Viability: Expected return
- Feasibility: Ability to deliver
- Desirability: Alignment with business

PROOF OF CONCEPT

- **Define** the minimum viable ecosystem (MVE), onboard team
- **Develop** functional and technical architecture
- **Select** the blockchain technology stack
- **Build and test** the proof of concept iteratively
- **Retrospective** to confirm value and identify new challenges

Phases in the agile workflow

Discover → Design → Build → Review →

SCALE

- **Develop** operating models and governance
- **Expand** MVE by creating or joining consortiums
- **Pilot** blockchain solution in live production environment
- **Design** roll-out strategy and integrate with legacy systems
- **Industrialize** technology stack and **engage** regulators if needed
- **Institutionalize** operating structure

Consortia success factors

- Membership
- Leadership
- Funding
- Governance

Source: Deloitte analysis.

Deloitte Insights | Deloitte.com/insights

Source: **Deloitte**

Slater Technologies