



Blockchain: The Intro (and other stuff)

Eliezer Kanal

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213



Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.


[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

GOVERNMENT PURPOSE RIGHTS – Technical Data
Contract No.: FA8702-15-D-0002
Contractor Name: Carnegie Mellon University
Contractor Address: 4500 Fifth Avenue, Pittsburgh, PA 15213

The Government's rights to use, modify, reproduce, release, perform, display, or disclose these technical data are restricted by paragraph (b)(2) of the Rights in Technical Data—Noncommercial Items clause contained in the above identified contract. Any reproduction of technical data or portions thereof marked with this legend must also reproduce the markings.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

DM18-0669



The CERT Division of SEI produces technologies and practices that reduce the opportunity for, and limit the damage of, cyber attacks.

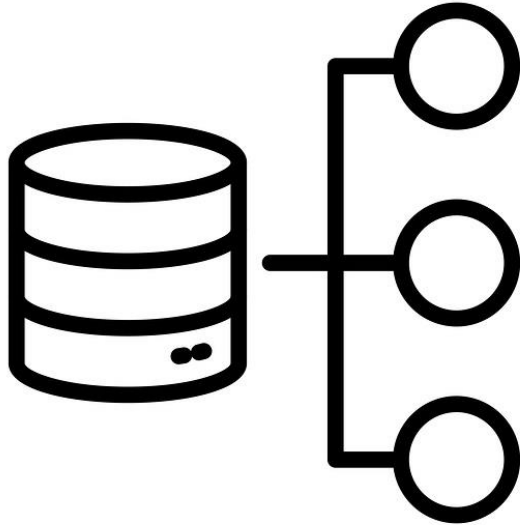
Focus areas include:

- Cyber Science Foundations
- Digital Intelligence
- Insider Threat
- Malware Analysis
- Resiliency
- Secure Coding
- Situational Awareness
- Workforce Development

Carnegie Mellon University

Software Engineering Institute

Previous models of computing

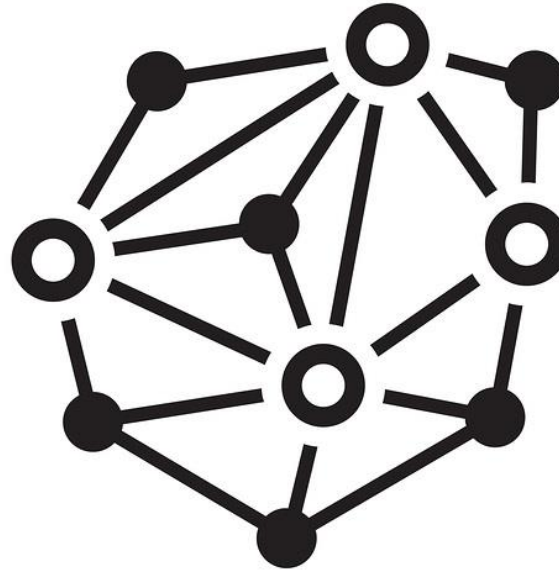


Data Storage:
Database



Program Execution:
Local

Blockchain



Data Storage:

Blockchain or Network

Program Execution:

Network

Blockchain: Executive Summary

Pros:

Authentication built-in

Easy to audit history

Easy to detect data manipulation

Very difficult to disrupt

Cons:

Proof-of-work very inefficient

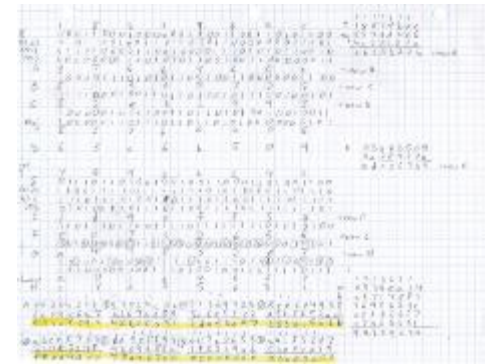
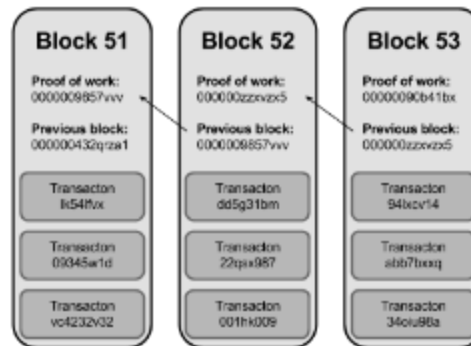
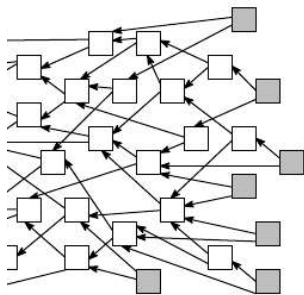
State updates are slow

Best for simple computations

Bitcoin: Currency in a Blockchain

Three fundamental elements:

1. Transaction tree (state changes)
2. Blockchain (timeline for 1)
3. “Mining” protocol



Bitcoin: Transactions



Messages

			<u>Signature</u>
Alice → Bob	0.44 BTC		387152...
Alice → Charlie	21.3 BTC		876401...
Alice → Dave	0.06 BTC		746122...
Charlie → Emily	1.80 BTC		076865...
⋮			

(Aside) PKI

Three position lock, two keys



“Private” goes from $\textcircled{A} \rightarrow \textcircled{B} \rightarrow \textcircled{C}$

“Public” goes from $\textcircled{C} \rightarrow \textcircled{B} \rightarrow \textcircled{A}$

All boxes start at \textcircled{B}

<https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5>

Bitcoin: Identity

All messages requires a Private Key to be valid

- Think “password”, but more secure

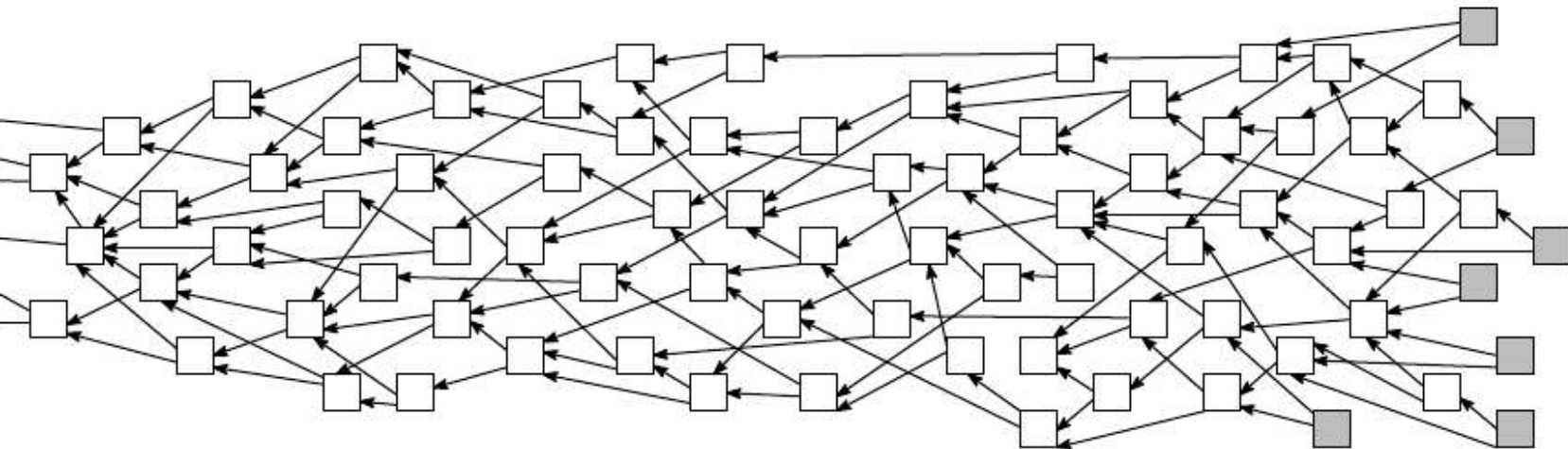
All blockchain transactions **require** authentication

Bitcoin: Transaction Tree

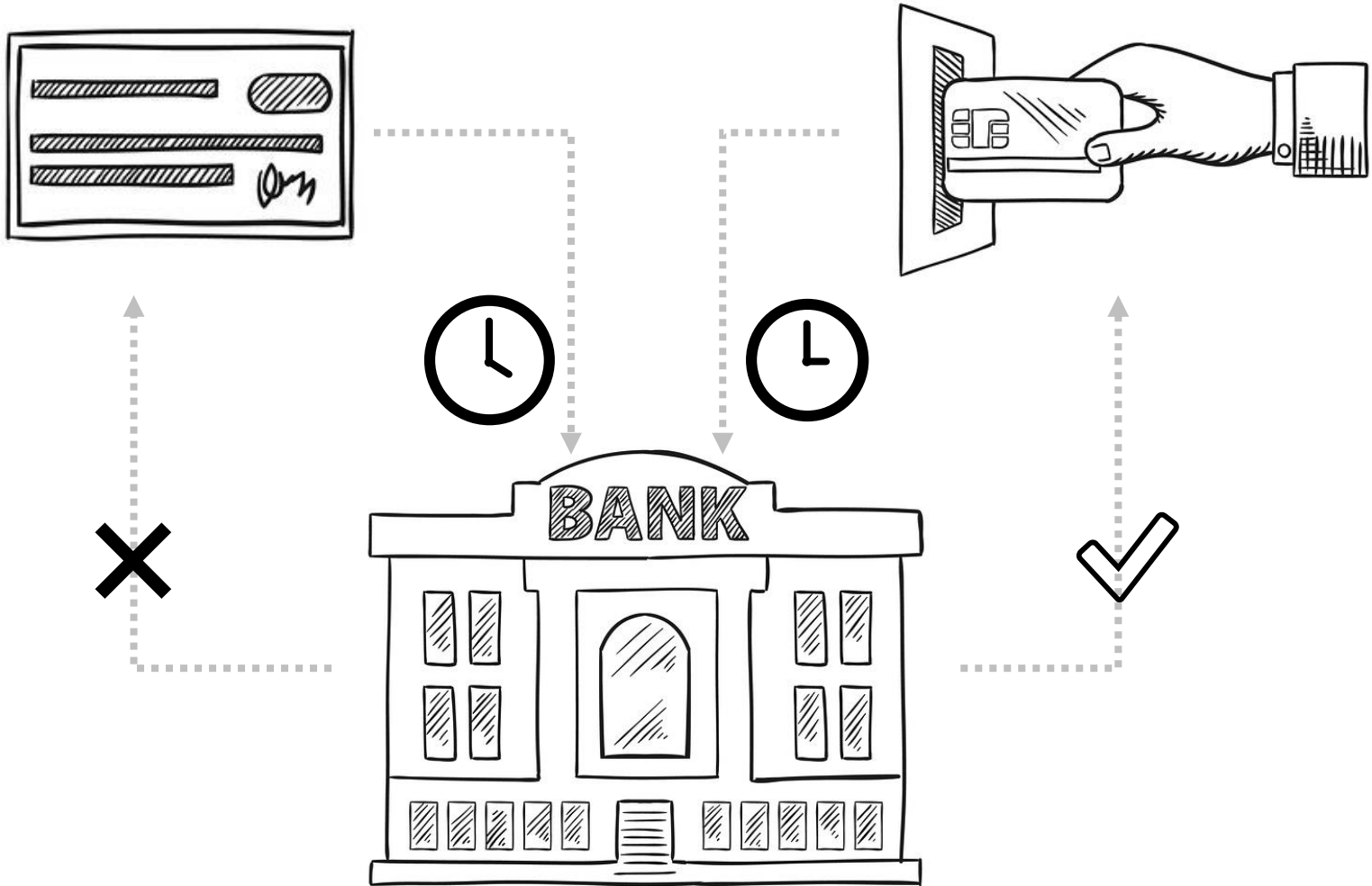
New transactions come from old ones

Balance = sum up incoming transactions

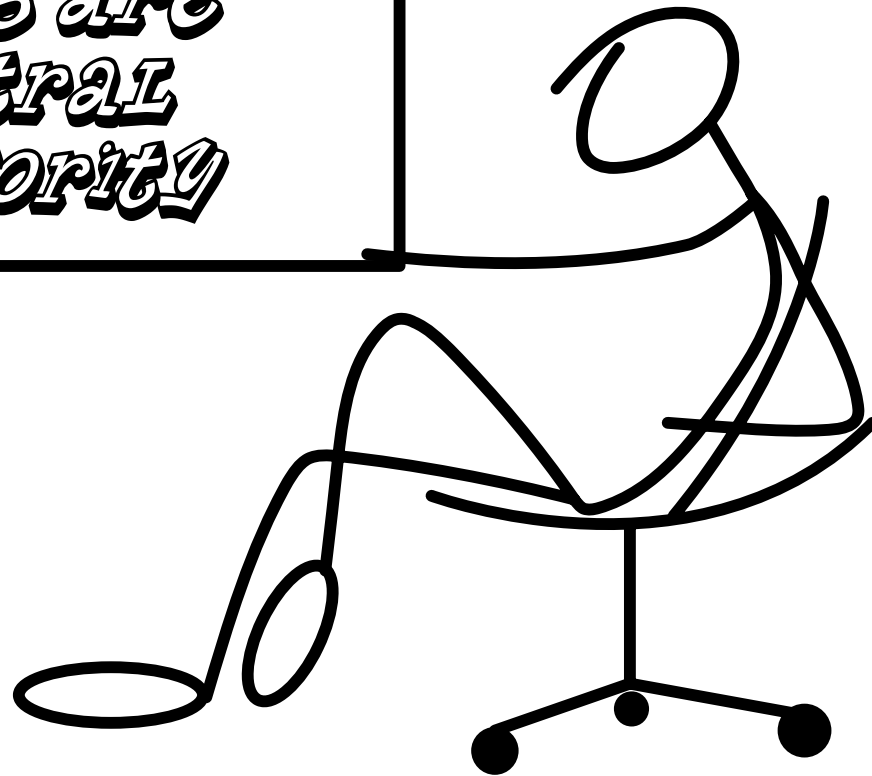
Auditable!







**BANS are
CENTRAL
AUTHORITY**



Bitcoin's challenge: **Consensus**

How to get tons of strangers to all agree on something without a central authority?

Bitcoin's solution: **Mining**

*Give everyone a really hard problem to solve
but really easy to verify and hold a race.*

Incentive: Winner gets paid!

Bitcoin: Mining

1. Select random bunch of outstanding transactions
2. Find the “magic” number for those transactions
3. First computer to find it tells everyone (1) what their transactions were and (2) their magic number
4. Everyone else verifies, if true they add those transactions to history and start again

Demo

Access demo online at <https://anders.com/blockchain/hash.html>

Play with the **Hash**, **Block**, and **Blockchain** sections (links in top-right of page)

Block #509169

Summary	
Number Of Transactions	1915
Output Total	10,289.28130284 BTC
Estimated Transaction Volume	1,818.68925455 BTC
Transaction Fees	0.4893378 BTC
Height	509169 (Main Chain)
Timestamp	2018-02-14 15:16:59
Received Time	2018-02-14 15:16:59
Relayed By	58COIN
Difficulty	2,874,674,234,415.94
Bits	392292856
Size	1132.416 kB
Weight	3992.574 kWU
Version	0x20000000
Nonce	1858980081
Block Reward	12.5 BTC

Hashes	
Hash	000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Previous Block	000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcd7240a471
Next Block(s)	
Merkle Root	3ad680735c45cc62b1ea6b7efeb34f82a2660c5e8280354c45f7ffa03c9137e2

Transactions

ab0da64ea834fd2acb81eb081d8103c9e31fd14a7d055f2ce2718c59dd4fa5df		2018-02-14 15:16:59
No Inputs (Newly Generated Coins)	 14DjTuAUh87cwRsbU1z6W8hZY6FnEkpflS Unable to decode output address	12.9893378 BTC 0 BTC
		12.9893378 BTC
4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552ed237f267d		2018-02-14 15:16:59
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	 12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131 1GpqR4vsdvEfgtNyiUrDrDLTBjvnsentX 1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	0.4983 BTC 0.1495 BTC 5.01651602 BTC
		5.66431602 BTC

1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP



12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131
1GpqR4vsdvEfgtNyiUrDrfDLTBjvnsentX
1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP

0.4983 BTC
0.1495 BTC
5.01651602 BTC

5.66431602 BTC

Output Total 10,289.28130284 BTC Previous Block 000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471

Estimated Transaction Value

Transaction Fees

Number Of Transactions

1915

354c45f7ffa03c9137e2

Height

Timestamp

2018-02-14 15:16:59

Received Time

Relayed By

Nonce

1858980081

Difficulty

Bits

392292856

Size

Difficulty

2,874,674,234,415.94

Weight

Version

Nonce

1858980081

Hash

000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3

Previous Block

000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471

No Inputs (Newly Generated Coins)



14DTyAlh8ZowPehL1z6W9hZV6EnEkrfL

12.9893378 BTC
0 BTC

Block Reward

12.5 BTC

12.9893378 BTC

4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552ed237f267d

2018-02-14 15:16:59

1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP



12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131
1GpqR4vsdvEfgtNyiUrDrfDLTBjvnsentX
1H6ZZpRmMnrw8ytepV3BYwMjYnEkWDqVP

0.4983 BTC
0.1495 BTC
5.01651602 BTC

5.66431602 BTC

Consensus alternatives

Algorithm	Properties
Proof of Work	<ul style="list-style-type: none">• Probabilistic solution• Lottery by computational power
Proof of Stake	<ul style="list-style-type: none">• Probabilistic solution• Lottery by total number of shares• “Nothing at stake”
BFT-based POS (“ Tendermint ”)	<ul style="list-style-type: none">• Multi-round voting process, removes possibility of forking• May stall out if 1/3 voters offline• Favors Consistency
Proof-by-bet POS (“ Casper ”)	<ul style="list-style-type: none">• Validators must place deposits on their “preferred” fork• Favors Availability



Blockchains – General Purpose

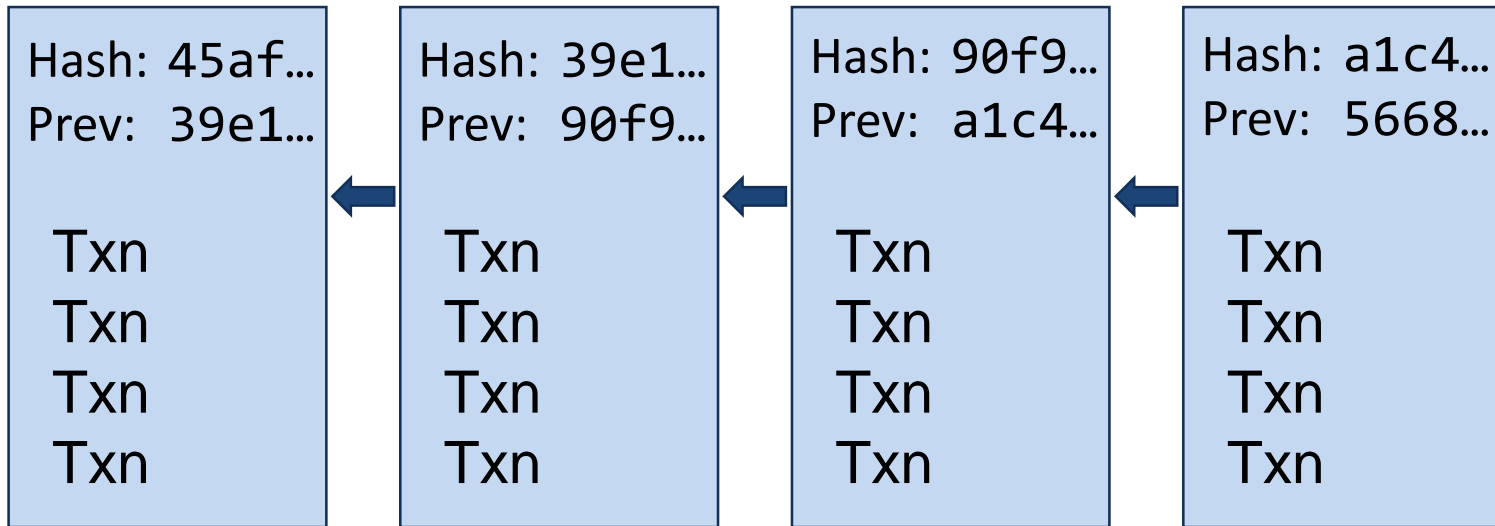
Wish list:

1. More than just monetary transactions

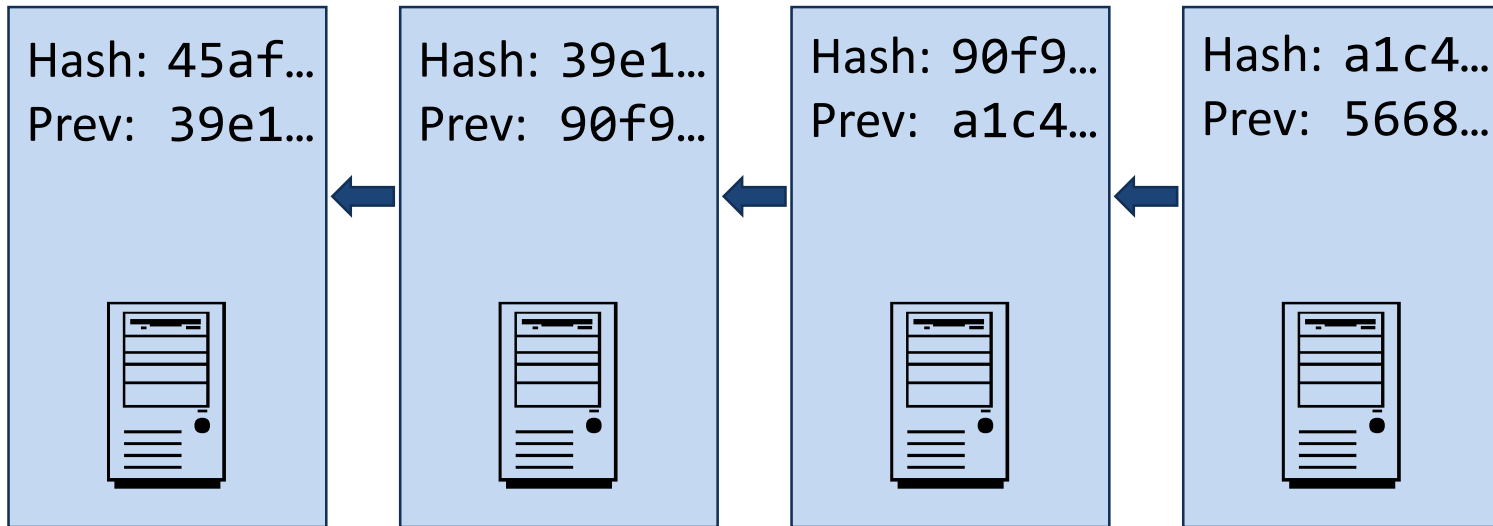


c.rda

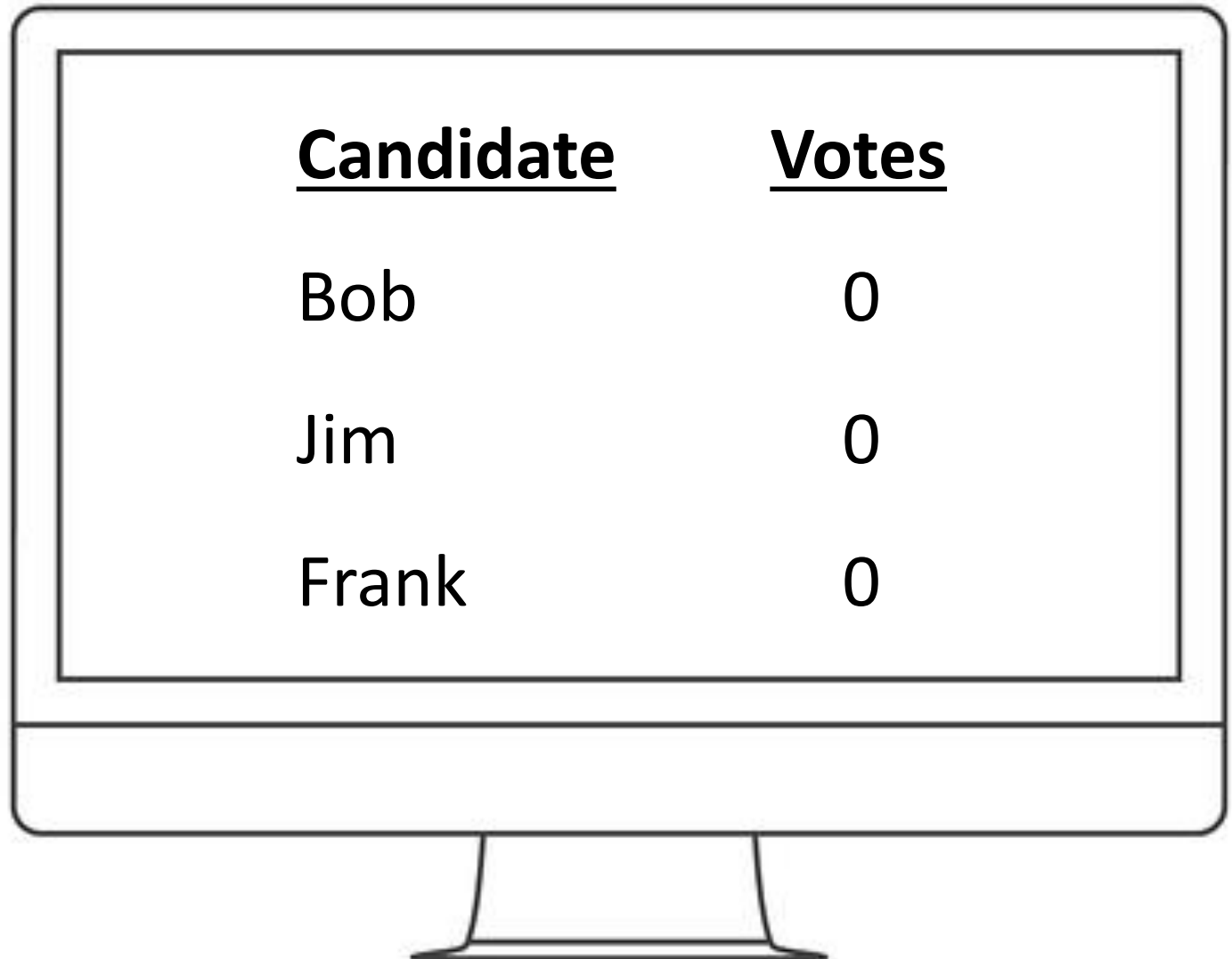




Time

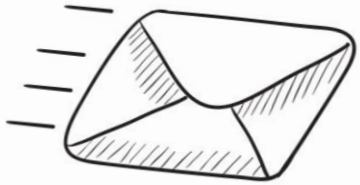


Time

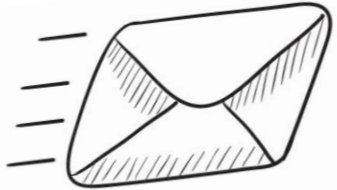


A computer monitor is shown with a table of election results on its screen. The table has two columns: 'Candidate' and 'Votes'. The candidates listed are Bob, Jim, and Frank, each with 0 votes.

<u>Candidate</u>	<u>Votes</u>
Bob	0
Jim	0
Frank	0

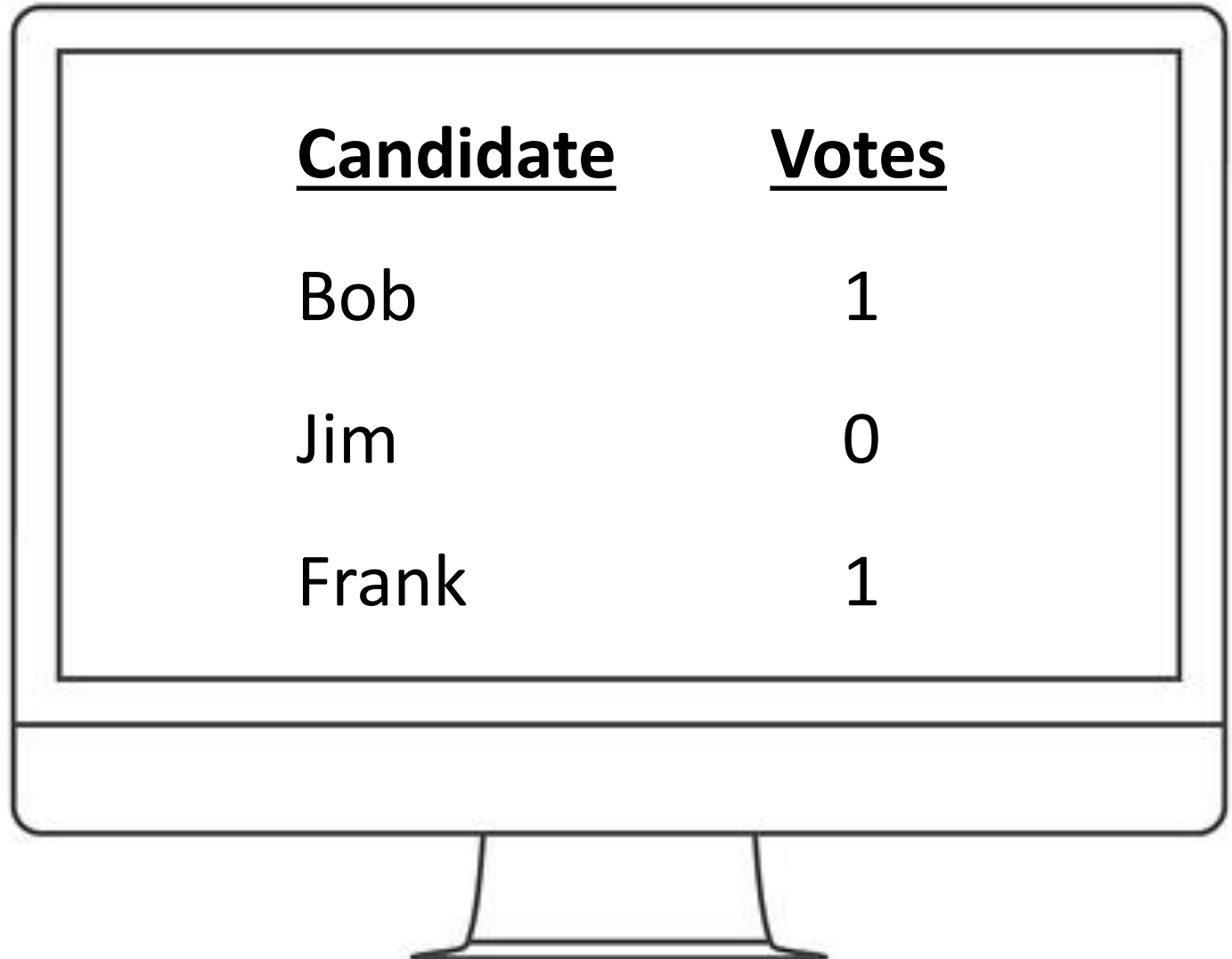


Bob: 1 vote



Frank: 1 vote

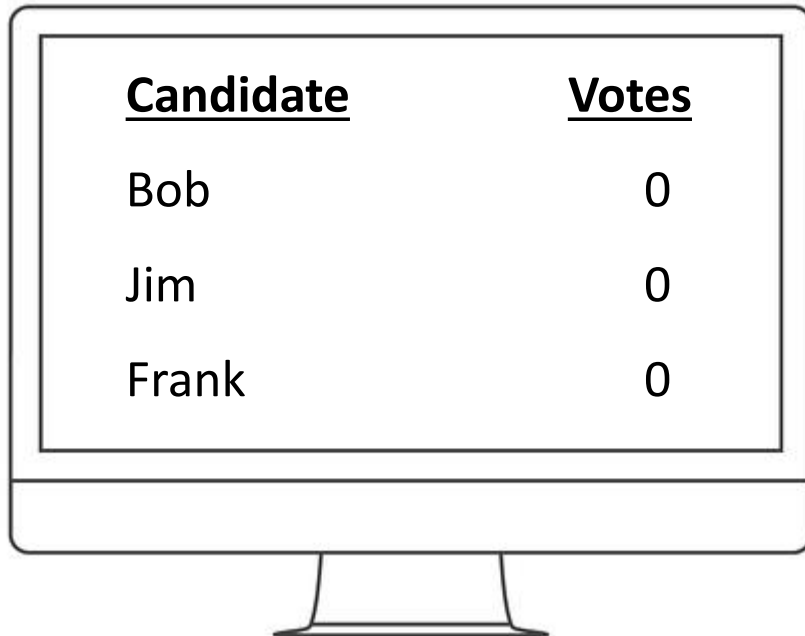
<u>Candidate</u>	<u>Votes</u>
Bob	0
Jim	0
Frank	0



A computer monitor is shown with a table of election results on its screen. The table has two columns: 'Candidate' and 'Votes'. The candidates listed are Bob, Jim, and Frank, with their respective vote counts being 1, 0, and 1.

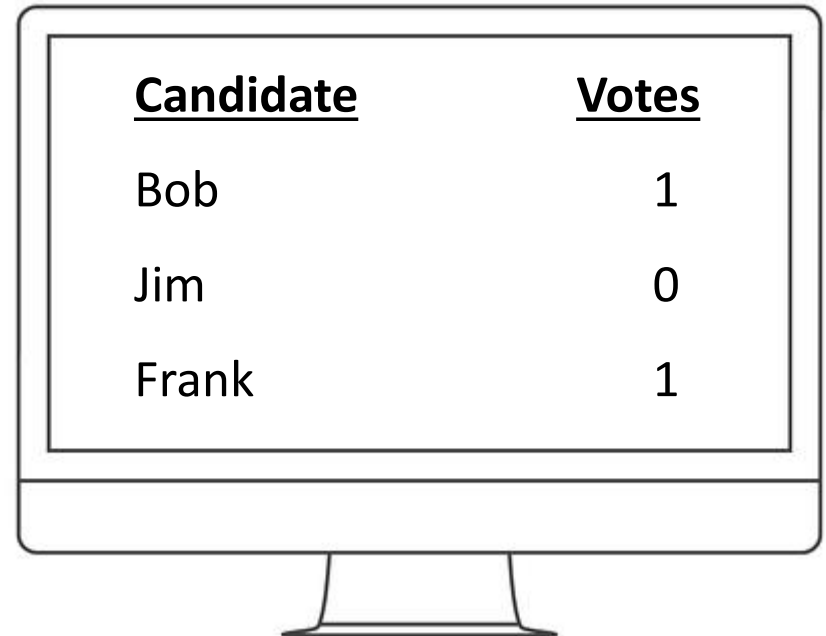
<u>Candidate</u>	<u>Votes</u>
Bob	1
Jim	0
Frank	1

State: 1



<u>Candidate</u>	<u>Votes</u>
Bob	0
Jim	0
Frank	0

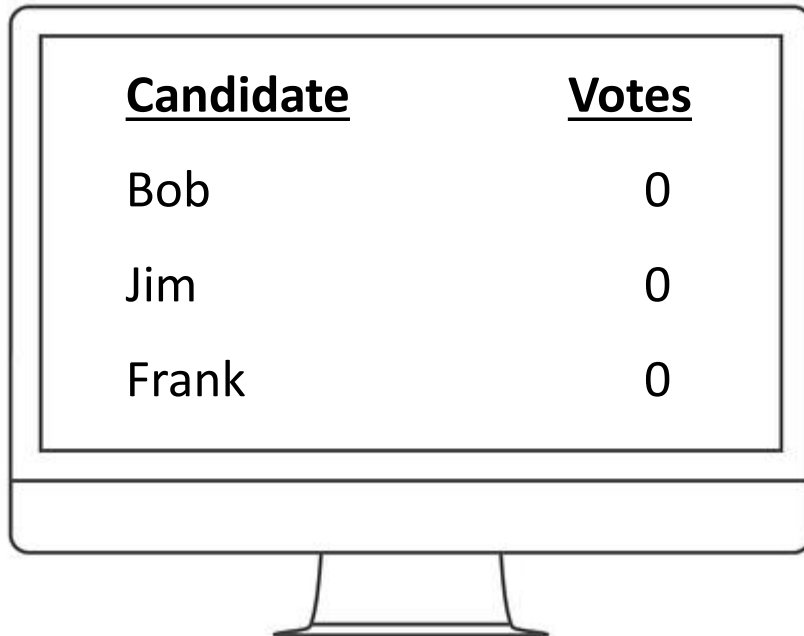
State: 2



<u>Candidate</u>	<u>Votes</u>
Bob	1
Jim	0
Frank	1

Equivalent to:

State: 1



<u>Candidate</u>	<u>Votes</u>
Bob	0
Jim	0
Frank	0

State: 2

State 1 plus...

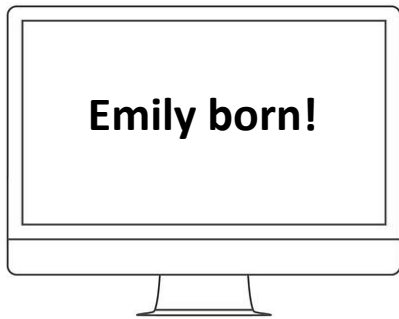


Bob: 1 vote

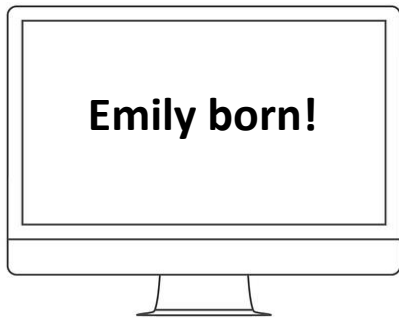


Frank: 1 vote

State: 1



State: 1



State: 2



Emily gets
vaccines

State: 8



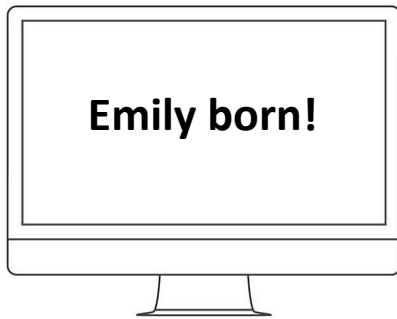
Emily has
a well visit

State: 55



Emily goes to
audiologist

State: 1



State: 2



Emily gets vaccines

State: 8



Emily has a well visit

State: 55



Emily goes to audiologist

State: 181



Insurance

State: 5,352



Prescription

State: You get the idea



Hospital stay

General purpose blockchains

Messages are... anything!

Each block is the system state at that time

$$\textit{Current State} = \textit{Original state} + \textit{All Changes}$$

Blockchains – General Purpose

Wish list:

1. More than just monetary transactions
2. More efficient consensus

Casper the Friendly Finality Gadget

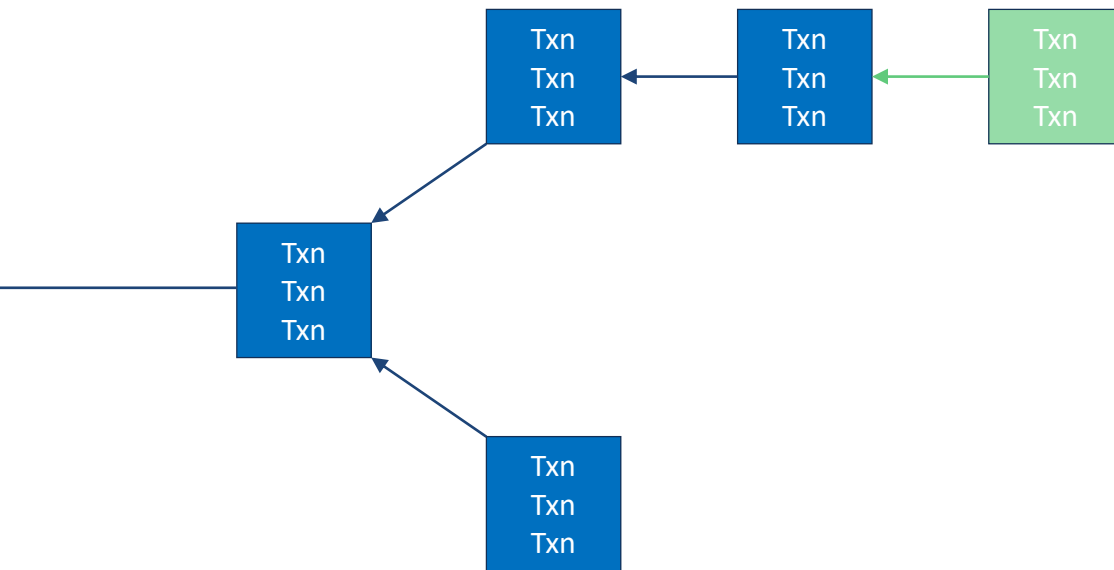
Vitalik Buterin and **Virgil Griffith**
Ethereum Foundation

Abstract

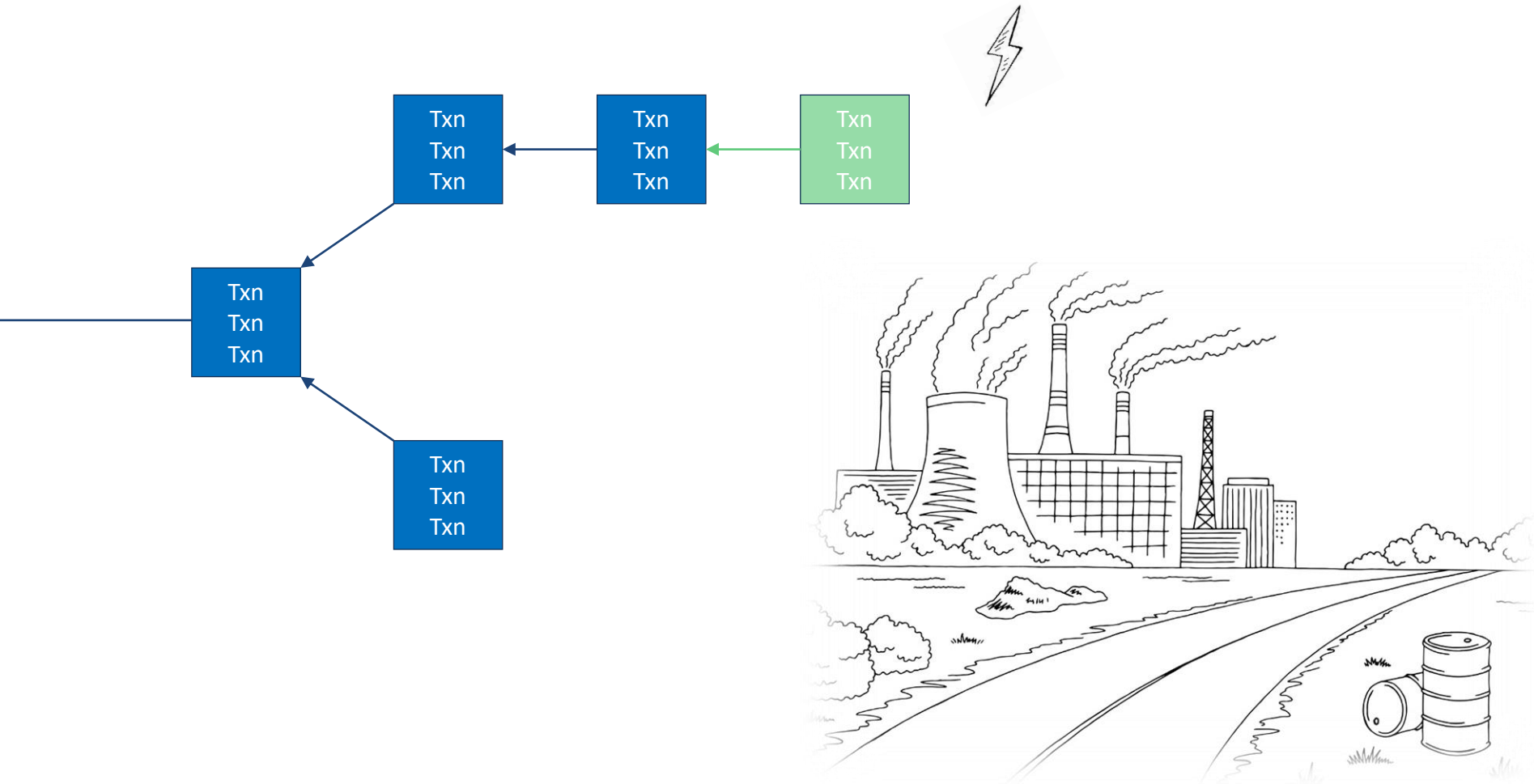
We introduce Casper, a proof of stake-based finality system which overlays an existing proof of work blockchain. Casper is a partial consensus mechanism combining proof of stake algorithm research and Byzantine fault tolerant consensus theory. We introduce our system, prove some desirable features, and show defenses against long range revisions and catastrophic crashes. The Casper overlay provides almost any proof of work chain with additional protections against

Nov 2017

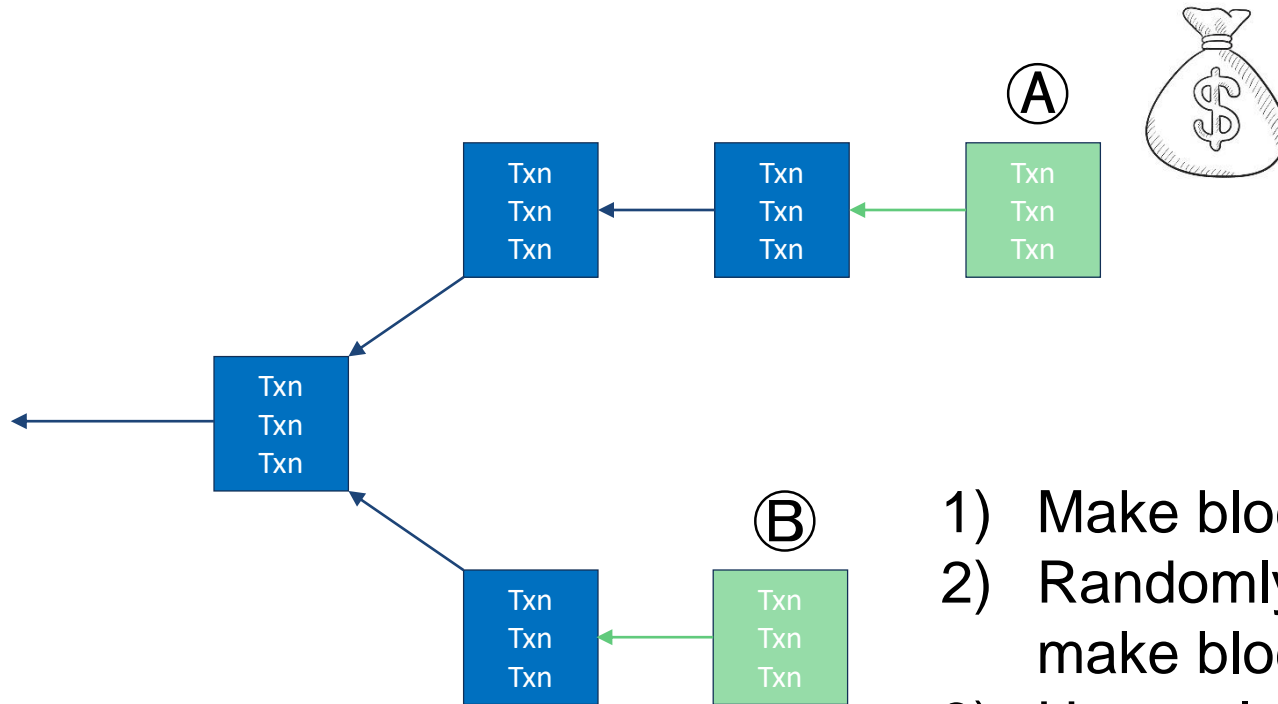
Consensus – Proof of Work (review)



Consensus – Proof of Work (review)



Consensus – Proof of Stake



- 1) Make blocks easier to create
- 2) Randomly assign who gets to make blocks
- 3) Users place bets on which block they think is top

Consensus – Proof of Stake

Many other aspects to PoS

- Highly developed behavioral economics theory
- “Safety” – system will converge (if 33% of users behave)
- “Liveliness” – blocks will finalize (if 66% of users behave)
- More sophisticated block creator selection
- Dealing with more sophisticated attacks
- Many other Proof-of-something efforts (ownership, authority, existence, ...)

Blockchains – General Purpose for Businesses

Wish list:

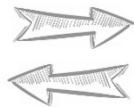
1. More than just monetary transactions
2. More efficient consensus
3. Better identification & authentication
4. Privacy
5. Permission restrictions

Hyperledger Fabric example

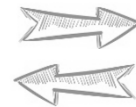
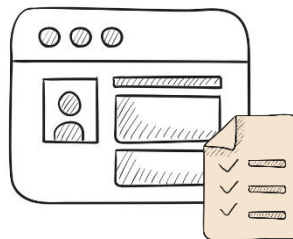
**MSP for each element
of the system**



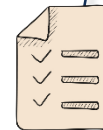
User



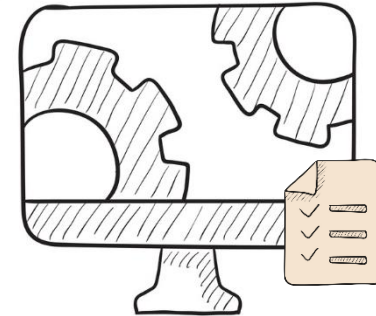
Application



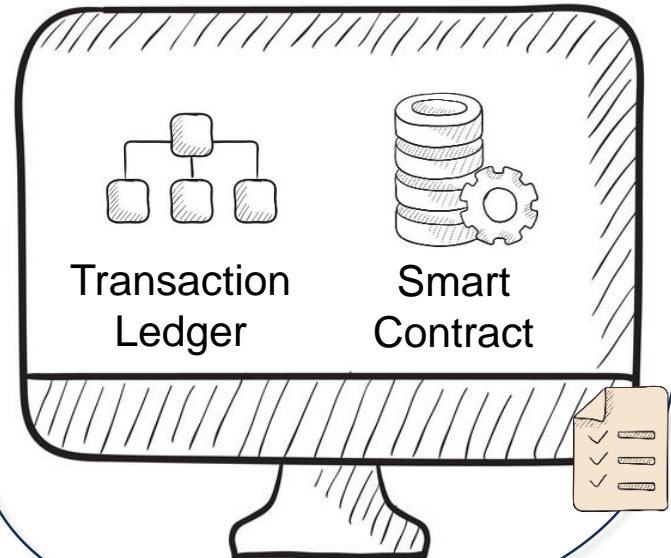
Channel



Orderer



Peer



General purpose blockchains

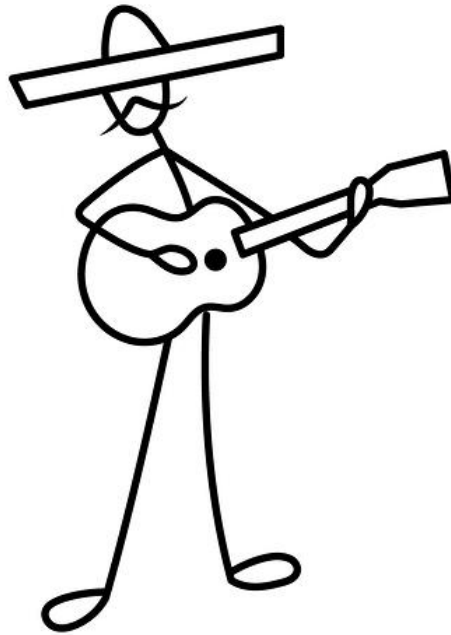
Other things being addressed:

Replace proof-of-work mining (expensive!)

Allow private blockchains

Allow private transactions

Reduce barrier to entry for usage



Blockchain: Executive Summary

Pros:

Authentication built-in

Easy to audit history

Easy to detect data manipulation

Very difficult to disrupt

Cons:

Proof-of-work very inefficient

State updates are slow

Best for simple computations

How can people be harmed through blockchain?

How can people be harmed through blockchain?

Messaging

Abuse

Publish private information

Publish false information

Business

Abuse public contracts (money, business loss)

Theft

Intellectual Property

Business Partnerships gone sour

In Practice

TheDAO

Bitfiniex

Ripple

KLINT FINLEY BUSINESS 06.18.16 04:30 AM

A \$50 MILLION HACK JUST SHOWED THAT THE DAO WAS ALL TOO HUMAN



In Practice

TheDAO

Bitfiniex

Ripple

Hacked Bitcoin exchange Bitfinex will reduce balances by 36% to distribute losses amongst all users



Fitz Tepper @fitztepper / Aug 8, 2016

Comment



In Practice

TheDAO

Bitfiniex

Ripple

BUSINESS
INSIDER



Regulators just demonstrated they are serious about making digital currency companies follow the rules



Shane Ferro



May 5, 2015, 6:49 PM 2,810



FACEBOOK



LINKEDIN



TWITTER

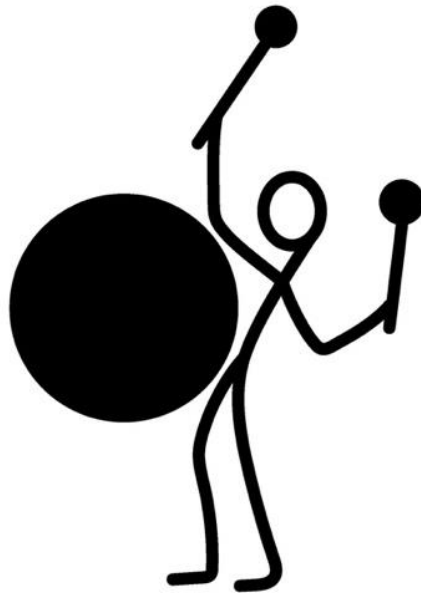


FinCEN, the Financial Crimes Enforcement Network, has levied its first fine on a virtual currency exchange.

Ripple Labs, which distributes and exchanges its own cryptocurrency, XRP, is being fined \$700,000 by FinCEN, a division of the Treasury Department, for "acting as a money services business (MSB), and selling its virtual currency... without registering with FinCEN," as well as for "failing to implement and maintain an adequate anti-money laundering (AML) program designed to protect its products from use by money launderers or terrorist financiers," according to FinCEN.



Ripple Labs YouTube / Ripple





ONC Blockchain Activities

Debbie Bucci, Office of the National Coordinator for Health IT (ONC)





Home / Older Posts / Security / Blockchain to cut fraud in healthcare supply chains

Blockchain to cut fraud in healthcare supply chains

Better track and trace means field agencies can have more confidence that medications are real thing.

James Hayes | 9th May 18

Products & Services Security Tech Trends



Blockchain* will play a key role in the support of supply chain transformation in the healthcare sector by helping to reduce fraud and better manage quality in the manufacturing and distribution of pharmaceutical products.

Data analytics company [GlobalData](#) has said that several technology and pharmaceutical companies are working on innovative solutions that combine digital marking of pharmaceutical products with the secure distributed ledger technology of blockchain. Their aim is to provide a means to securely and reliably track

Staff Experience, Standards Impact Healthcare Blockchain Adoption

Healthcare blockchain may be slow to catch on due to the technology being so different from other legacy health IT infrastructure solutions.



Source: Thinkstock



By Elizabeth O'Dowd

May 10, 2018 - Healthcare blockchain is creating a lot of industry buzz and several solutions have been released this year. Blockchain development and implementation are quickly gaining momentum, but the technology may not be a standard part of health IT infrastructure as soon as predicted.

Many Players...

Players

- Hospital administrators
- Medical providers
- Insurance companies
- Pharmaceuticals
- Device manufacturers

- ...oh yeah, and the patient

Many Players...

Players

- Hospital ad
- Me
- Insu
- Phar
- Devic
- ...oh y



Blockchain Security and Privacy

Why Does It Matter to the Homeland Security Enterprise?



**Homeland
Security**

Science and Technology

Championing Globally Interoperable Specifications Decentralized Identifiers

- Globally Unique Identifier without the need for a central registration authority
 - Immutable
 - Identifier is permanent
 - Resolvable
 - Identifier can be looked up to identify metadata about entity it identifies
 - Cryptographically Verifiable
 - Identifier's ownership can be established and verified using public/private cryptographic keys



Decentralized Identifiers (DIDs) v0.7

Data Model and Syntaxes for Decentralized Identifiers (DIDs)



Draft Community Group Report 09 December 2017

Latest editor's draft:

<https://w3c-ccg.github.io/did-spec/>

Editors:

[Drummond Reed, Evernym](#)
[Manu Sporny, Digital Bazaar](#)

Authors:

[Drummond Reed, Evernym](#)
[Manu Sporny, Digital Bazaar](#)
[Dave Longley, Digital Bazaar](#)
[Christopher Allen, Blockstream](#)
[Ryan Grant](#)
[Markus Sabadello, Danube Tech](#)

Participate:

[GitHub w3c-ccg/did-spec](#)
[File a bug](#)
[Commit history](#)

Copyright © 2017 the Contributors to the Decentralized Identifiers (DIDs) v0.7 Specification, published by the [Credentia Community Group](#) under the [W3C Community Contributor License Agreement \(CLA\)](#). A [human-readable summary](#) is available.

Abstract

Decentralized Identifiers (DIDs) are a new type of identifier intended for verifiable digital identity that is "self-sovereign", i.e., fully under the control of an entity and not dependent on a centralized registry, identity provider, or certificate authority. DIDs resolve to DID Documents — simple documents that contain all the metadata needed to interact with the DID. Specifically, a DID Document typically contains at least three things. The first is a set of mechanisms that may be used to authenticate as a particular DID (e.g. public keys, pseudonymous biometric templates, etc.). The second is a set of authorization information that outlines which entities may modify the DID Document. The third is a set of service endpoints, which may be used to initiate trusted interactions with the entity. This document specifies a common data model, format, and operations that all DIDs support.

3

Championing Globally Interoperable Specifications

Verifiable Claims Data Model

- Digital version of physical credentials/attestations
 - Driver's Licenses
 - Passports
 - Training Certificates
 - Educational Certificates
 - ...
- Interoperability across issuers, holders and verifiers
 - Standardization of data formats
 - Standardization of digital signature schemes



Verifiable Claims Data Model and Representations



W3C First Public Working Draft 03 August 2017

This version:

<https://www.w3.org/TR/2017/WD-verifiable-claims-data-model-20170803/>

Latest published version:

<https://www.w3.org/TR/verifiable-claims-data-model/>

Latest editor's draft:

<https://w3c.github.io/vc-data-model/>

Editors:

[Daniel C. Burnett, Standards Play](#)

[Manu Sporny, Digital Bazaar](#)

[Dave Longley, Digital Bazaar](#)

[Gregg Kellogg, Spec-Ops](#)

Authors:

[Manu Sporny, Digital Bazaar](#)

[Dave Longley, Digital Bazaar](#)

Participate:

[GitHub w3c/vc-data-model](#)

[File a bug](#)

[Commit history](#)

Copyright © 2017 W3C® (MIT, ERCIM, Keio, Beihang). W3C liability, trademark and permissive document license rules apply.

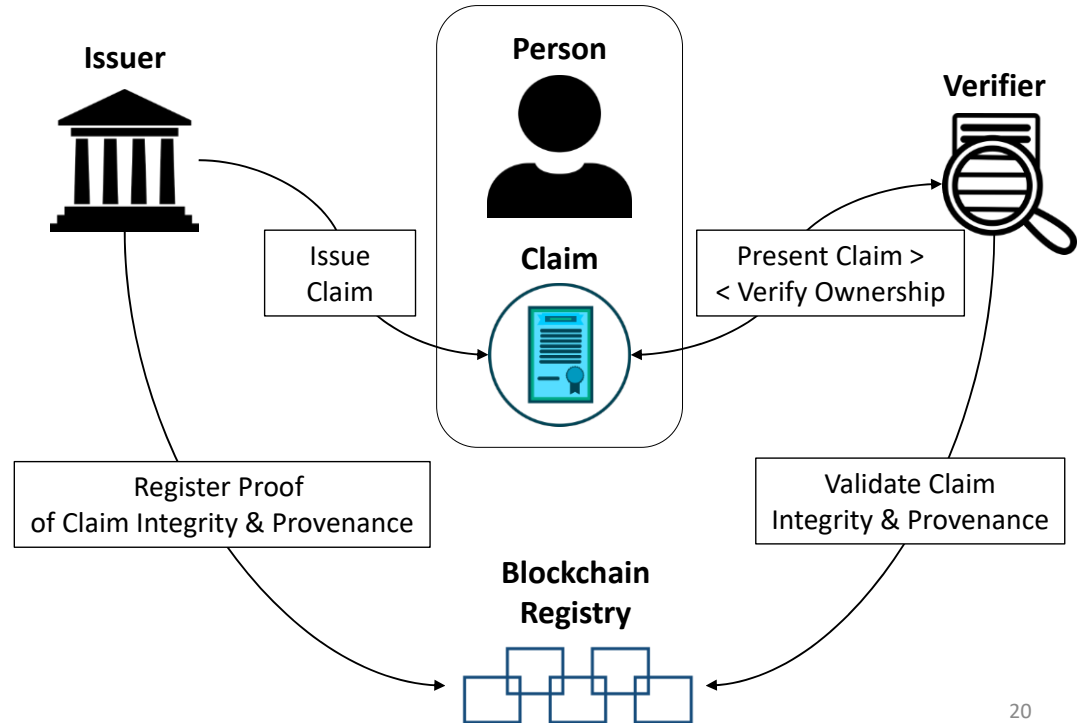
Abstract

Driver's licenses are used to claim that we are capable of operating a motor vehicle, university degrees can be used to claim our education status, and government-issued passports enable holders to travel between countries. This specification provides a standard way to express these sorts of claims on the Web in a way that is cryptographically secure, privacy respecting, and automatically verifiable.

14

Digital Counter-Fraud Tactics and Technologies to Mitigate Forgery & Counterfeiting of Official Licenses & Certificates

- Person-ownership of verifiable claims and certificates
- Selective disclosure of claim information with the Person's consent
- Pluralism of operators and technologies
- Support for online and off-line presentation of claim
- Non-CRL based revocation methods (Issuer initiated, Person initiated and/or Multi-sig based) that removes issuer dependency
- Very high resistance to data deletion, modification, masking or tampering



20

LEVERAGING BLOCKCHAIN SOLUTIONS

DISA
JFHQ DODIN

Defense Information Systems Agency
Joint Force Headquarters – DOD Information Networks

Much the same as DHS

Potential Use Cases



- Identity.
- Property management.
- Military Interdepartmental Purchase Requests (MIPRs).
- Secure messaging.
- Advanced persistent threat detection.
- PKI time stamping and code signing support.
- Access control.
- Cross domain solutions.
- Data storage.
- Contracting support.
- Human resource records management.
- Supply chain risk management.
- Auditing system change logs for security.



Thanks!

Eliezer Kanal

Technical Manager & Principle Researcher

Telephone: +1 412.268.5204

Email: ekanal@sei.cmu.edu