Blockchain

What, How, and Why

Eliezer Kanal

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

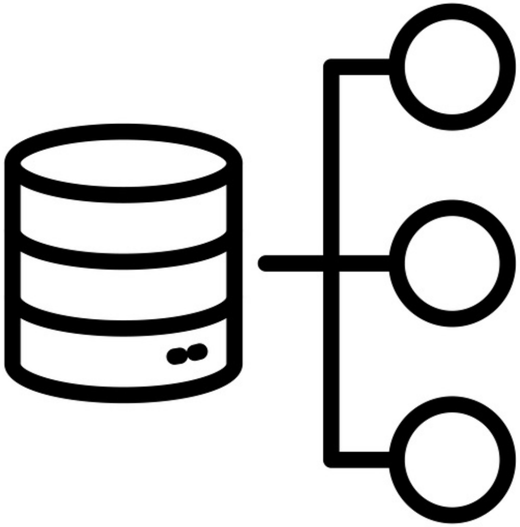
The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

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.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

DM18-0360

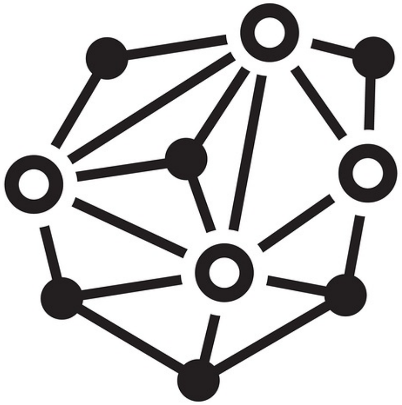
Previous models of computing



Data Storage:
Database

Program Execution:
Local

Blockchain



Data Storage:

Blockchain or Network

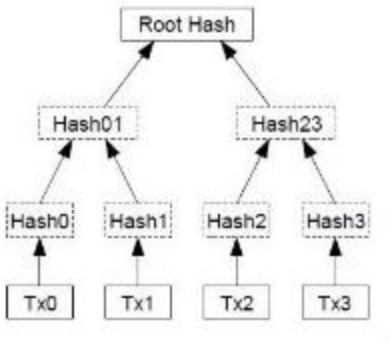
Program Execution:

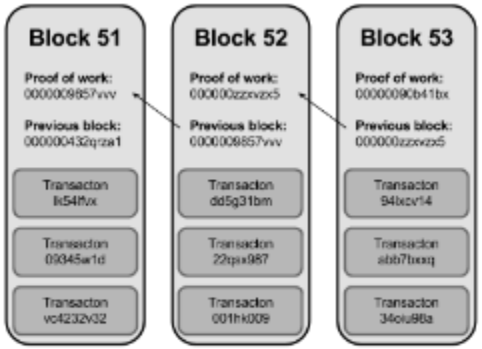
Network

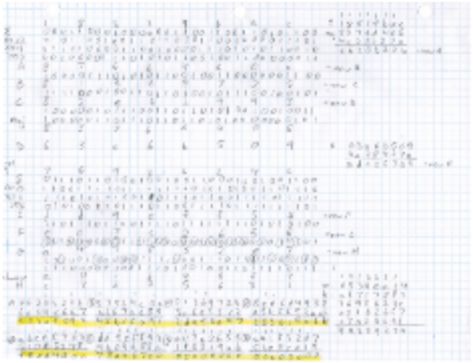
Bitcoin: Currency in a Blockchain

Three fundamental elements:

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







http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

Bitcoin: Transactions

Messages

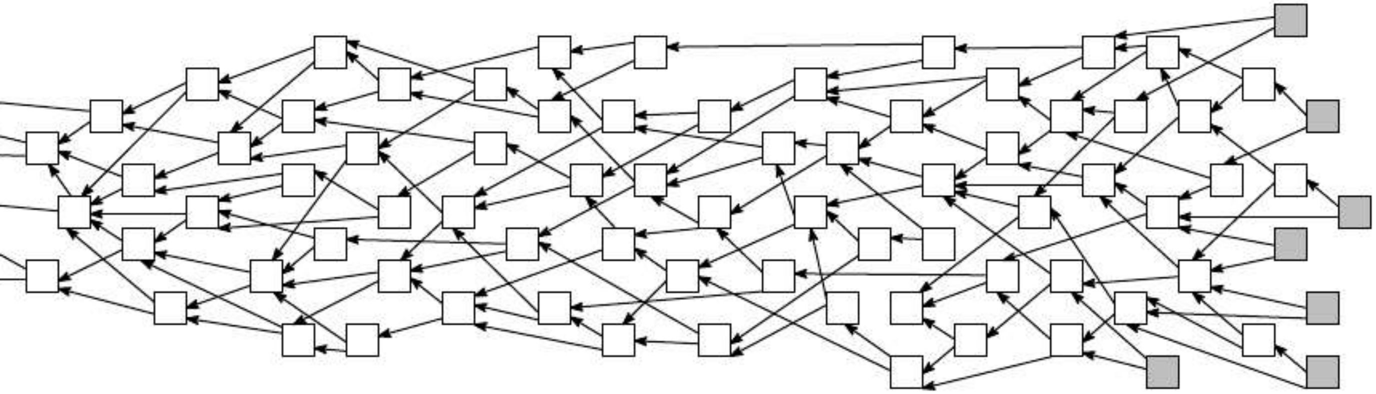
		Signature
Alice ➞ Bob	0.44 BTC	387152…
Alice ➞ Charlie	21.3 BTC	876401…
Alice ➞ Dave	0.06 BTC	746122…
Charlie ➞ Emily	1.80 BTC	076865…
⋮		

Bitcoin: Transaction Tree

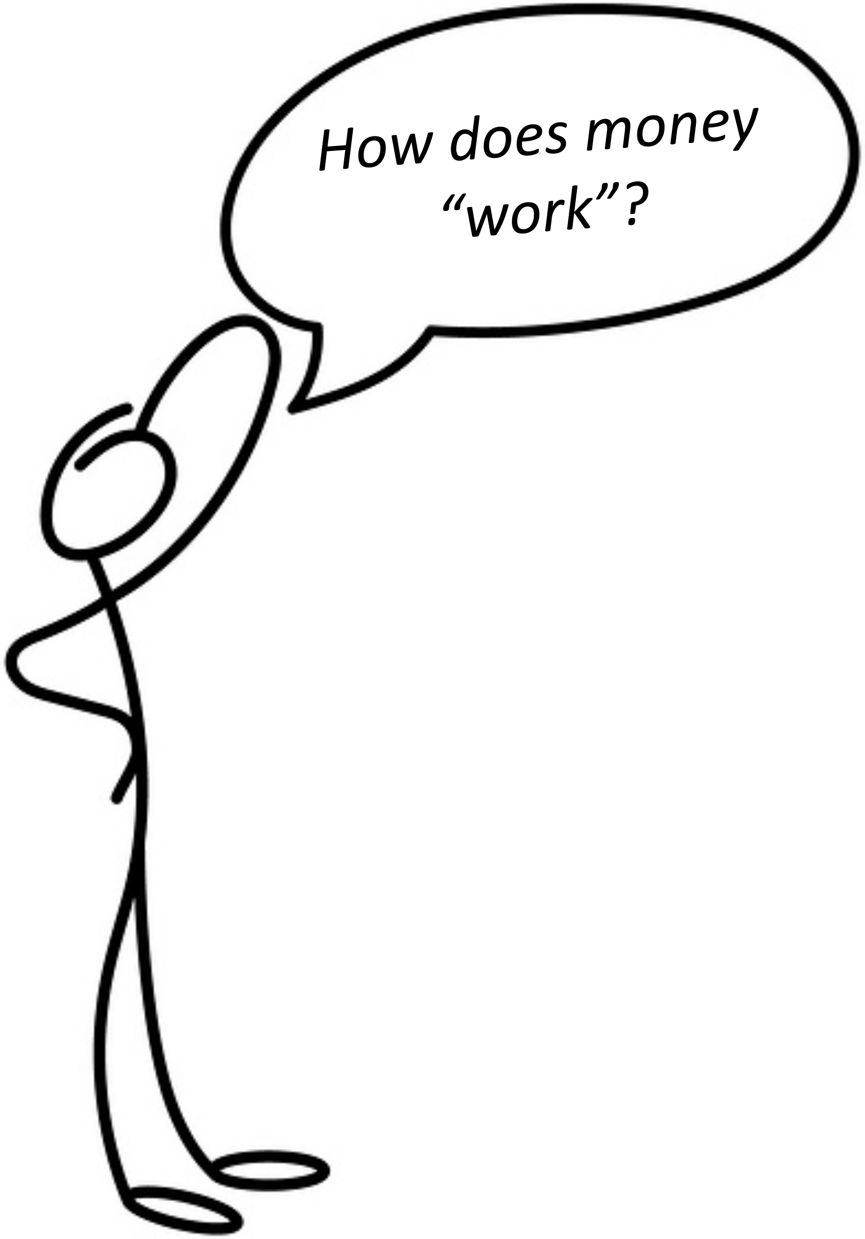
New transactions come from old ones

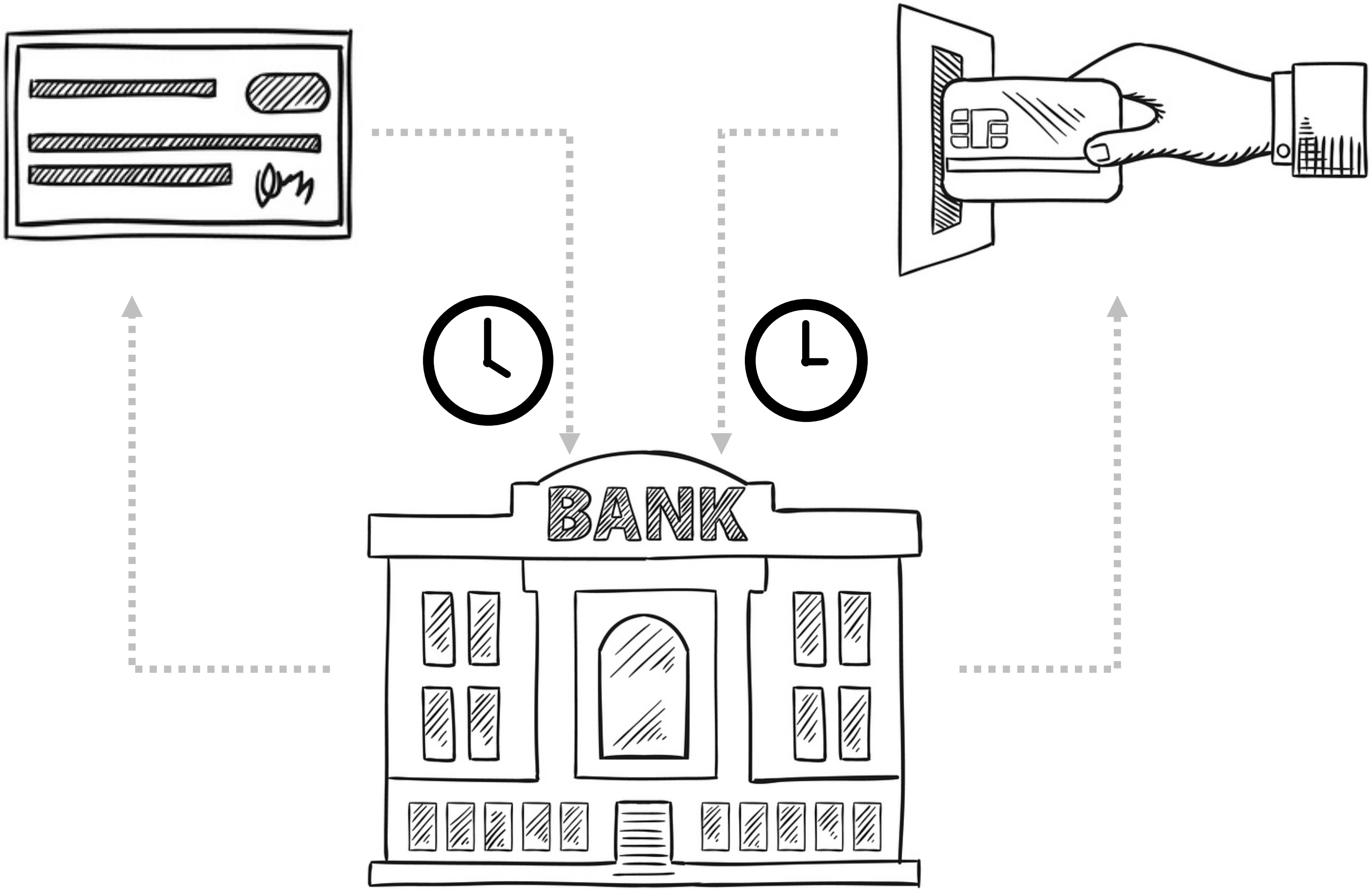
Balance = sum up incoming transactions

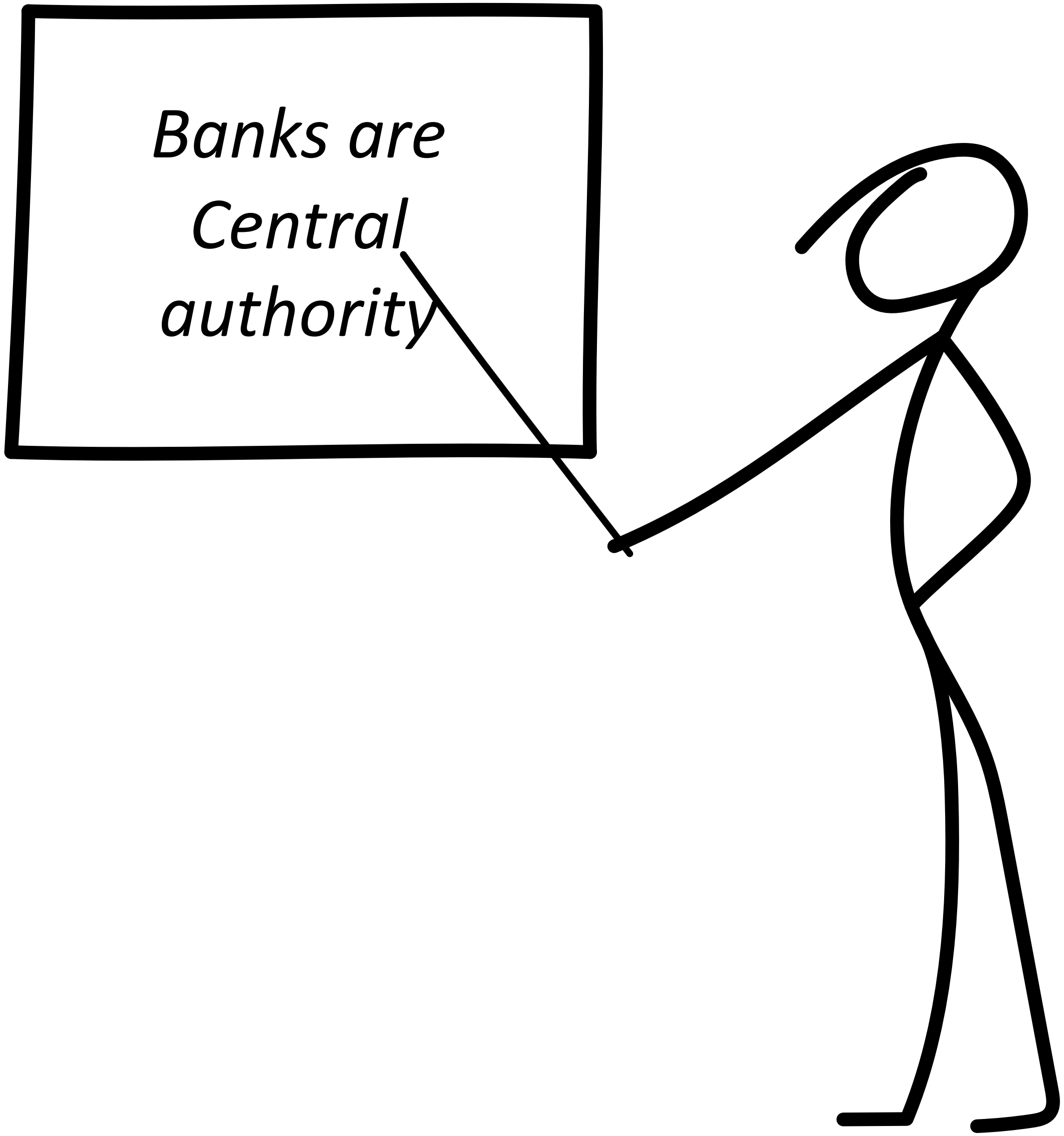
Auditable!



By Tiagodimas2 (Own work) [CC BY-SA 4.0 (https://creativecommons.org/licenses/by-sa/4.0)], via Wikimedia Commons


How does money
“work”?


BANK



Banks are Central authority

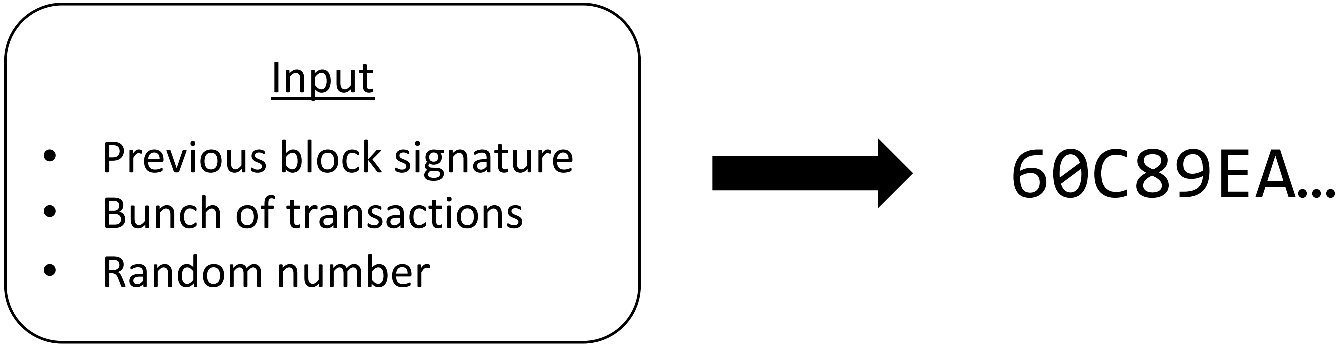
Bitcoin’s challenge:

Timing

Bitcoin’s solution:

Mining

Bitcoin: Mining



Input

- Previous block signature
- Bunch of transactions
- Random number

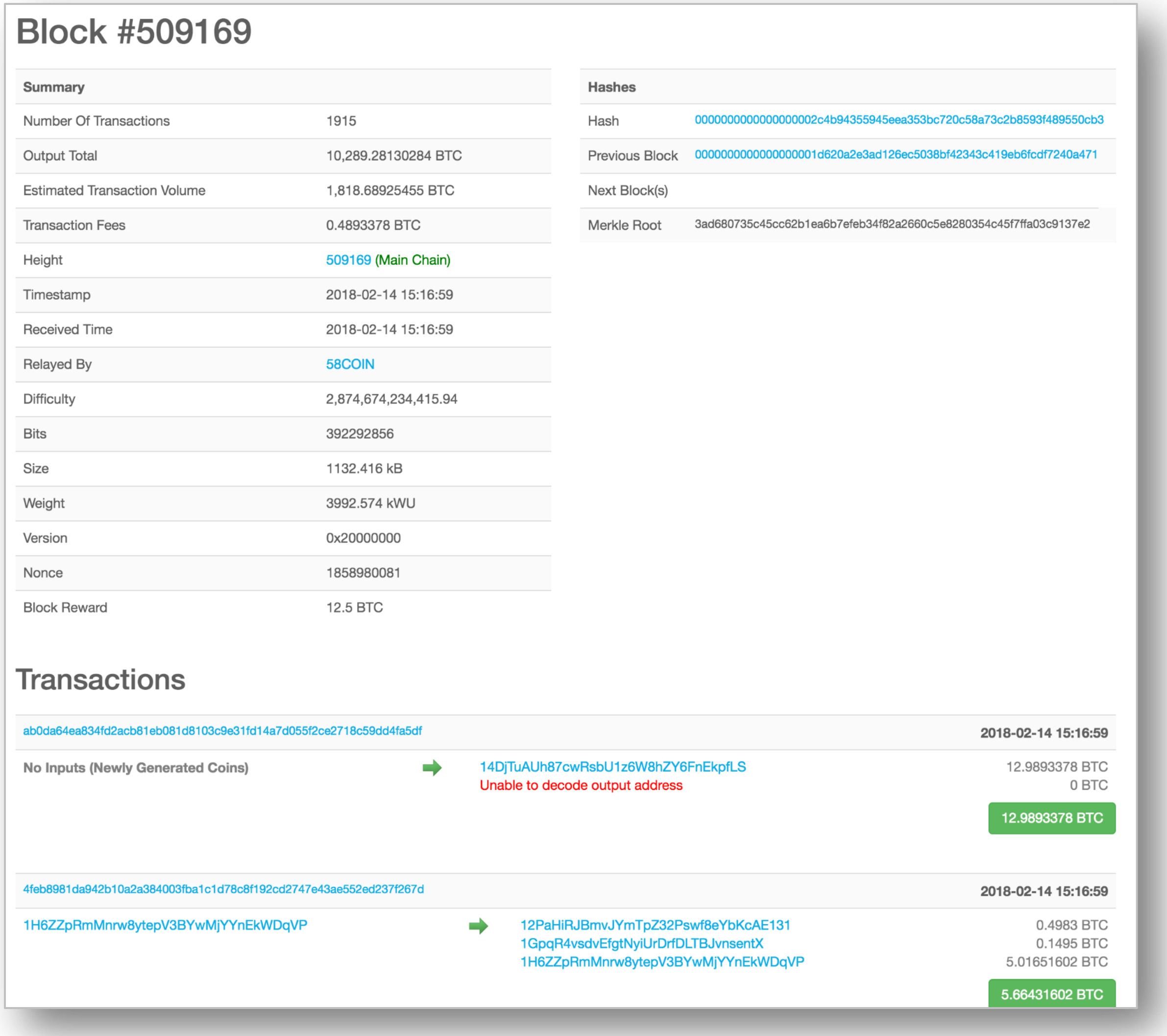
60C89EA…

Signature	Transactions	Random #	Output
482AA…	txn 1, 17, 88, 452	1	854A3…
482AA…	txn 1, 17, 88, 452	2	B4221…
482AA…	txn 1, 17, 88, 452	3	0249F…
⋮			
482AA…	txn 1, 17, 88, 452	98,401	0000A…

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	0000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Previous Block	0000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471
Next Block(s)	
Merkle Root	3ad680735c45cc62b1ea6b7efeb34f82a2660c5e8280354c45f7ffa03c9137e2

Transactions

ab0da64ea834fd2acb81eb081d8103c9e31fd14a7d055f2ce2718c59dd4fa5df — 2018-02-14 15:16:59

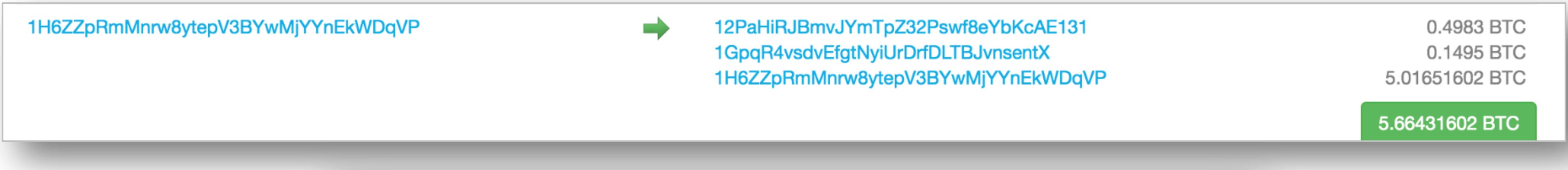
No Inputs (Newly Generated Coins) → 14DjTuAUh87cwRsbU1z6W8hZY6FnEkpfLS 12.9893378 BTC
Unable to decode output address 0 BTC

12.9893378 BTC

4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552ed237f267d — 2018-02-14 15:16:59

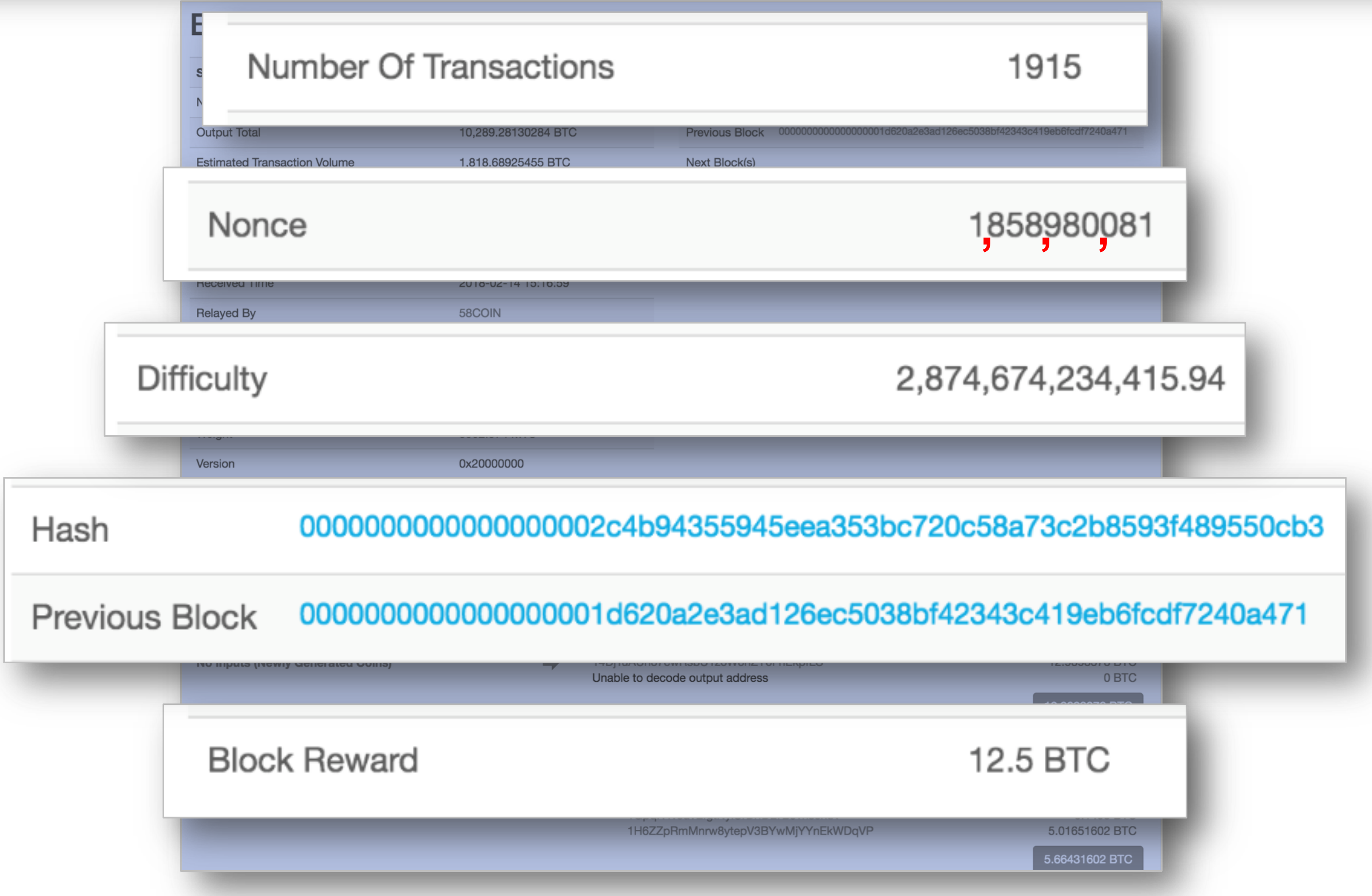
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP → 12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131 0.4983 BTC
1GpqR4vsdvEfgtNyiUrDrfDLTBJvnsentX 0.1495 BTC
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP 5.01651602 BTC

5.66431602 BTC



1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP → 12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131 0.4983 BTC
1GpqR4vsdvEfgtNyiUrDrfDLTBJvnsentX 0.1495 BTC
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP 5.01651602 BTC

5.66431602 BTC



Number Of Transactions 1915

Output Total 10,289.28130284 BTC

Previous Block 00000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471

Estimated Transaction Volume 1,818.68925455 BTC

Next Block(s)

Nonce 1,858,980,081

Received Time 2018-02-14 15:16:59

Relayed By 58COIN

Difficulty 2,874,674,234,415.94

Version 0x20000000

Hash 0000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3

Previous Block 0000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471

Unable to decode output address 0 BTC

Block Reward 12.5 BTC

1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP 5.01651602 BTC

5.66431602 BTC

Consensus alternatives

Algorithm	Properties
Proof of Work	• Probabilistic solution • Lottery by computational power
Proof of Stake	• Probabilistic solution • Lottery by total number of shares • “Nothing at stake”
BFT-based POS (“Tendermint”)	• Multi-round voting process, removes possibility of forking • May stall out if 1/3 voters offline • Favors Consistency
Proof-by-bet POS (“Casper”)	• Validators must place deposits on their “preferred” fork • Favors Availability

Blockchains – General Purpose

More than just a currency:

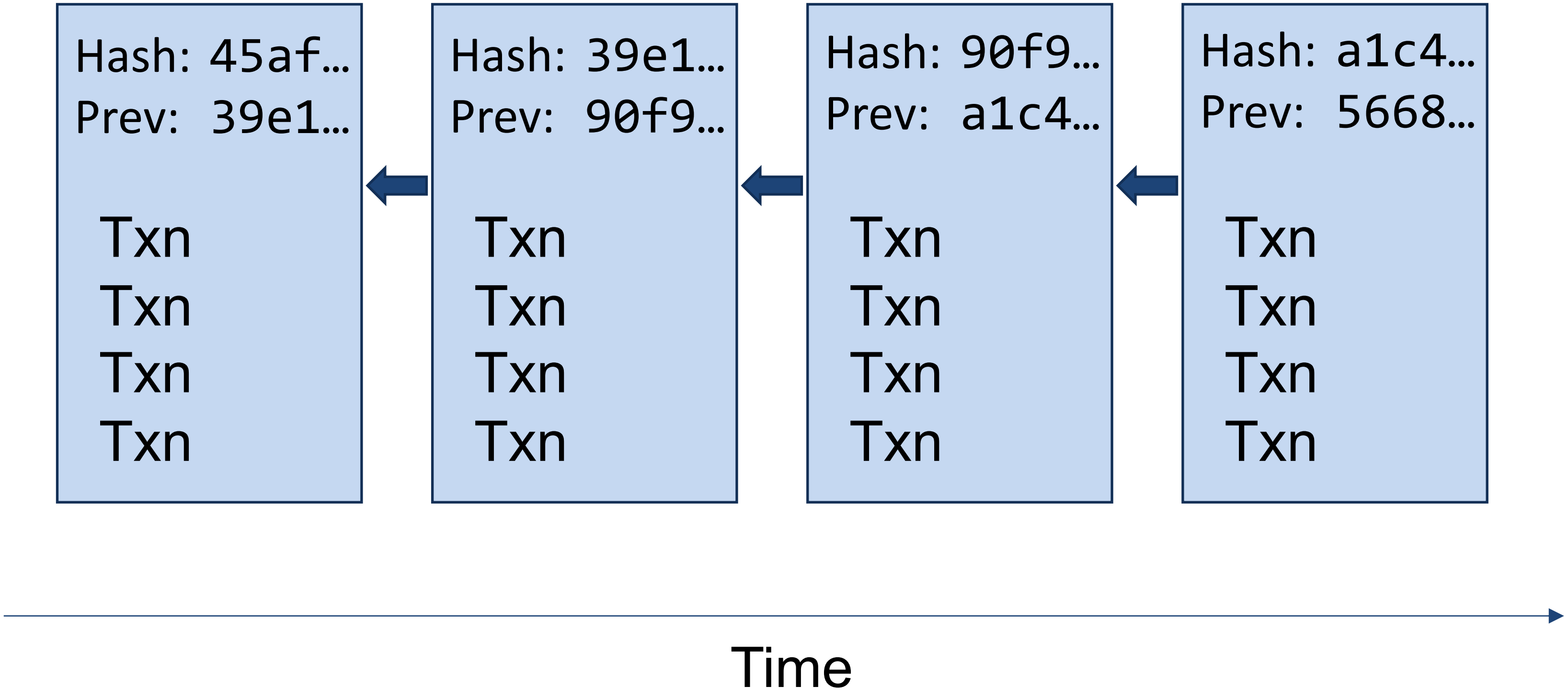
1. Transfer more than just cash
2. General purpose programming

ethereum

corda

HYPERLEDGER

Quorum™



Hash: 45af…
Prev: 39e1…

Txn
Txn
Txn
Txn

Hash: 39e1…
Prev: 90f9…

Txn
Txn
Txn
Txn

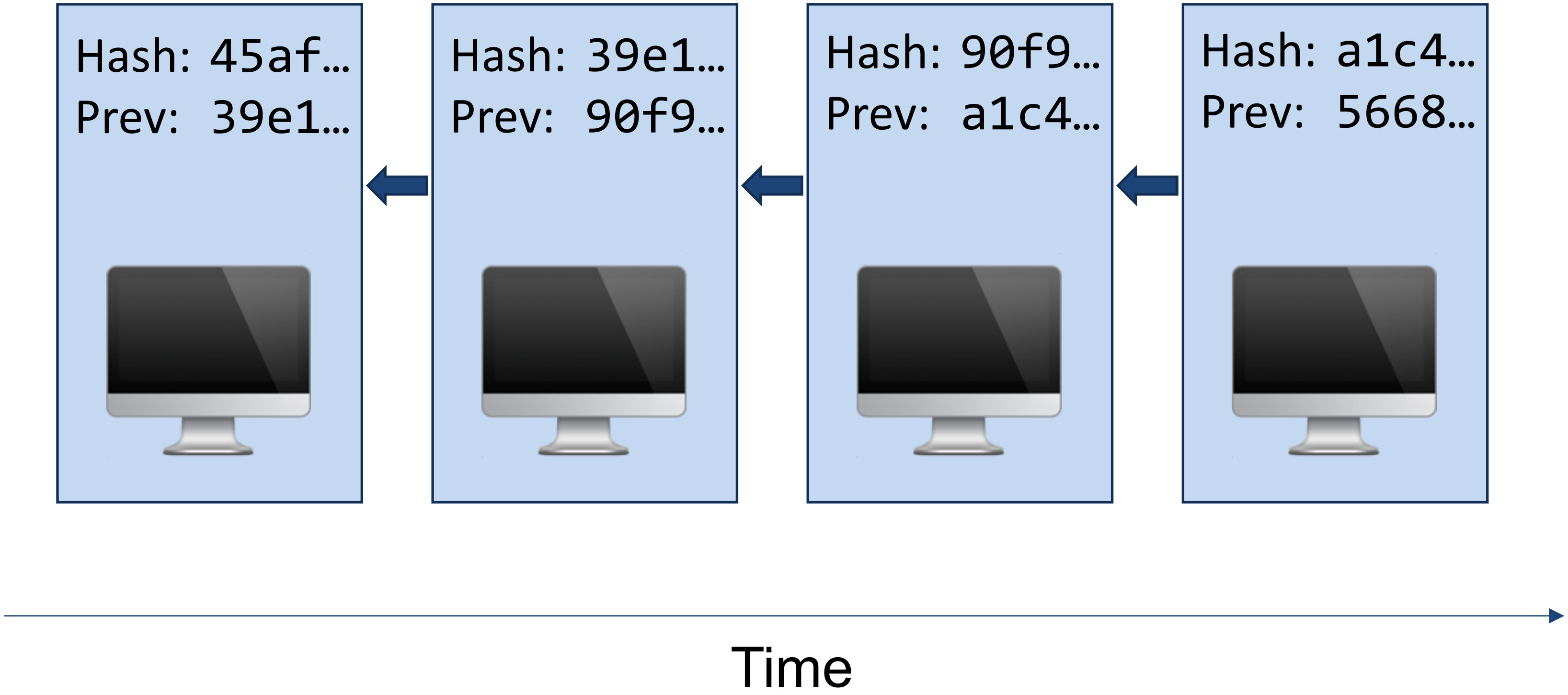
Hash: 90f9…
Prev: a1c4…

Txn
Txn
Txn
Txn

Hash: a1c4…
Prev: 5668…

Txn
Txn
Txn
Txn

Time



Hash: 45af…
Prev: 39e1…

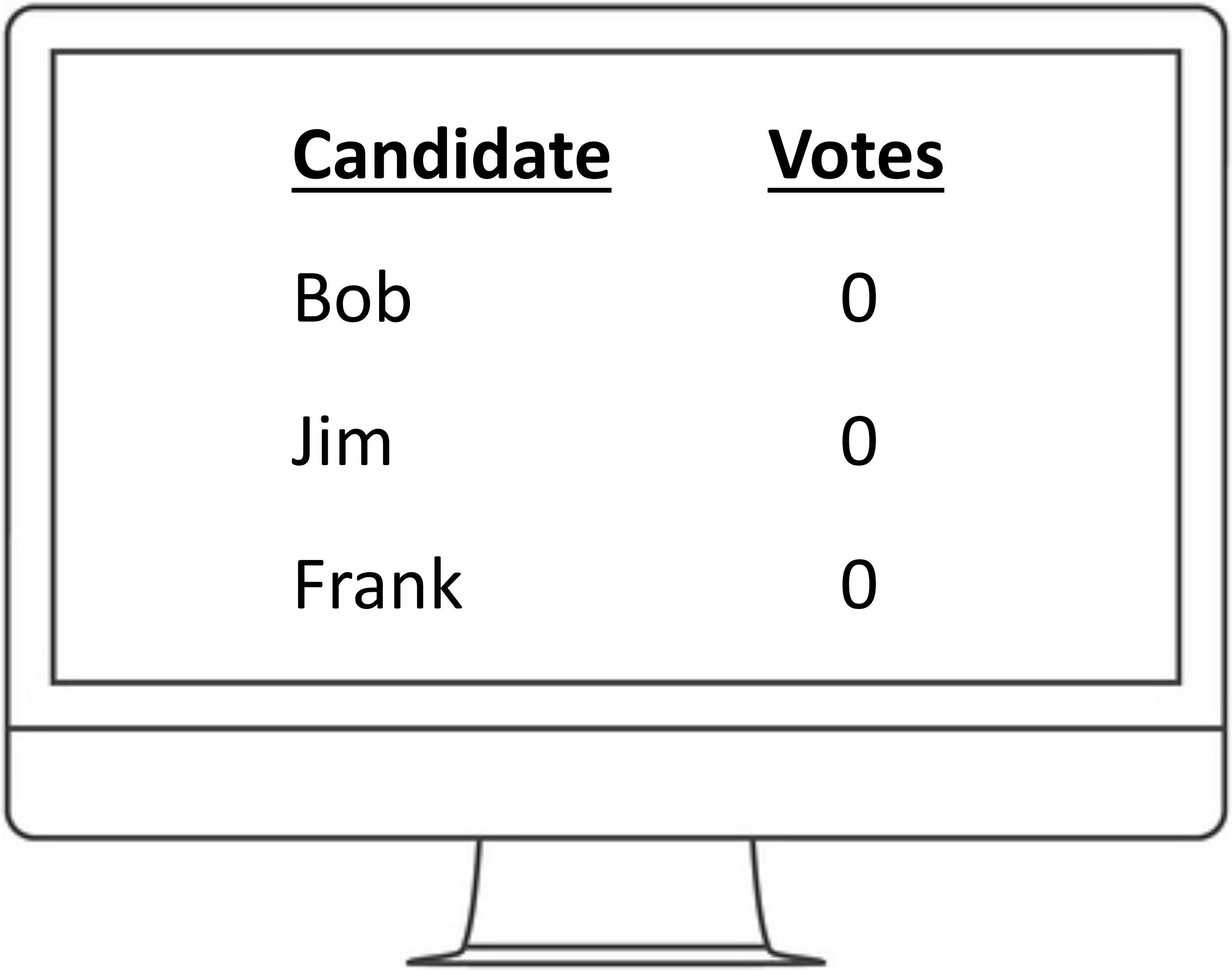
Hash: 39e1…
Prev: 90f9…

Hash: 90f9…
Prev: a1c4…

Hash: a1c4…
Prev: 5668…

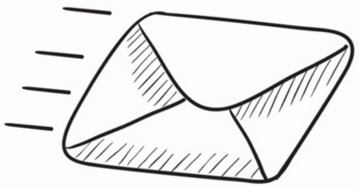
Time

State: 1

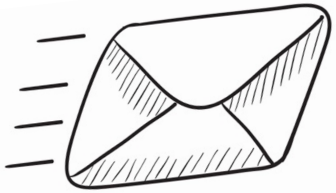


Candidate	Votes
Bob	0
Jim	0
Frank	0

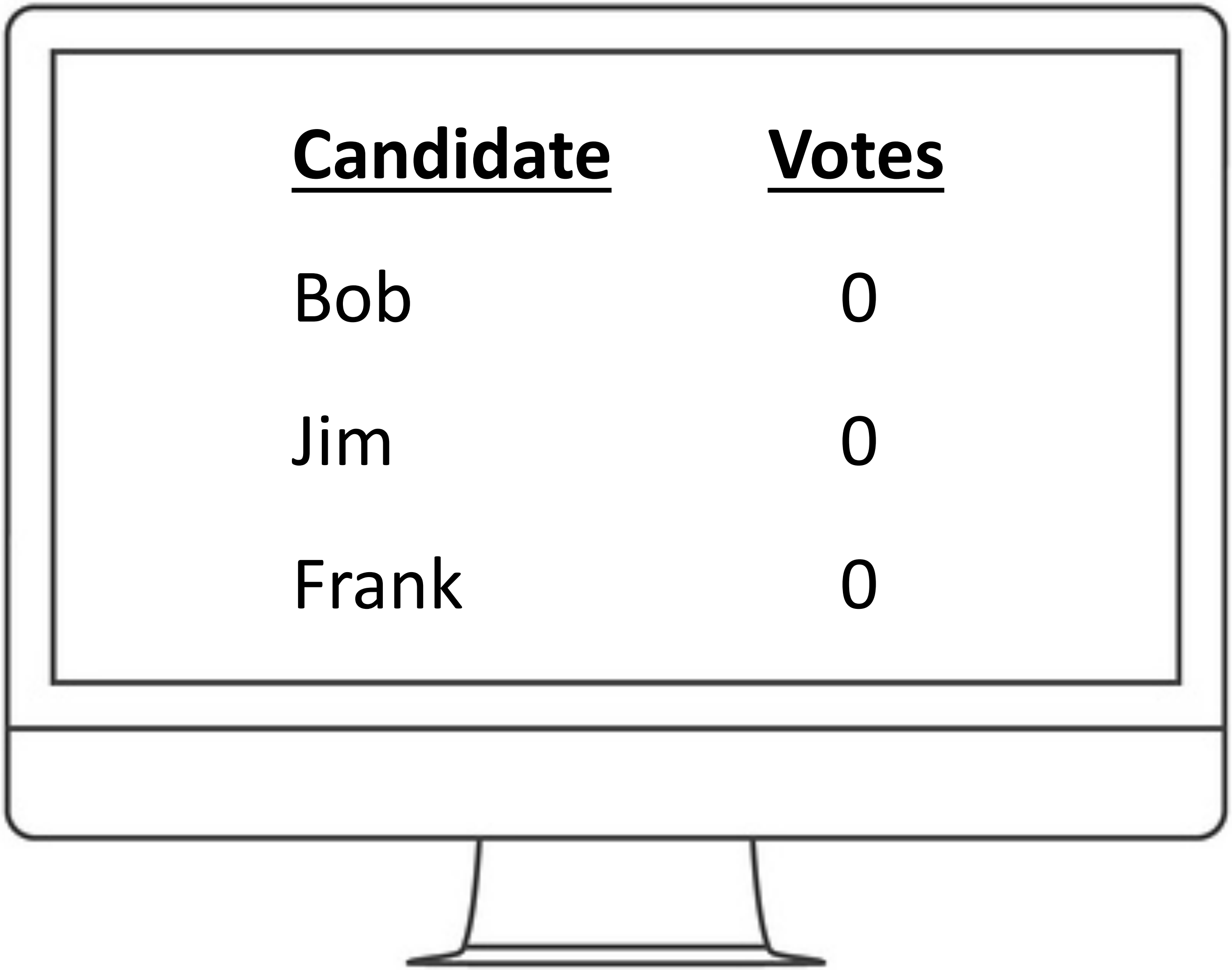
State: 1



Bob: 1 vote

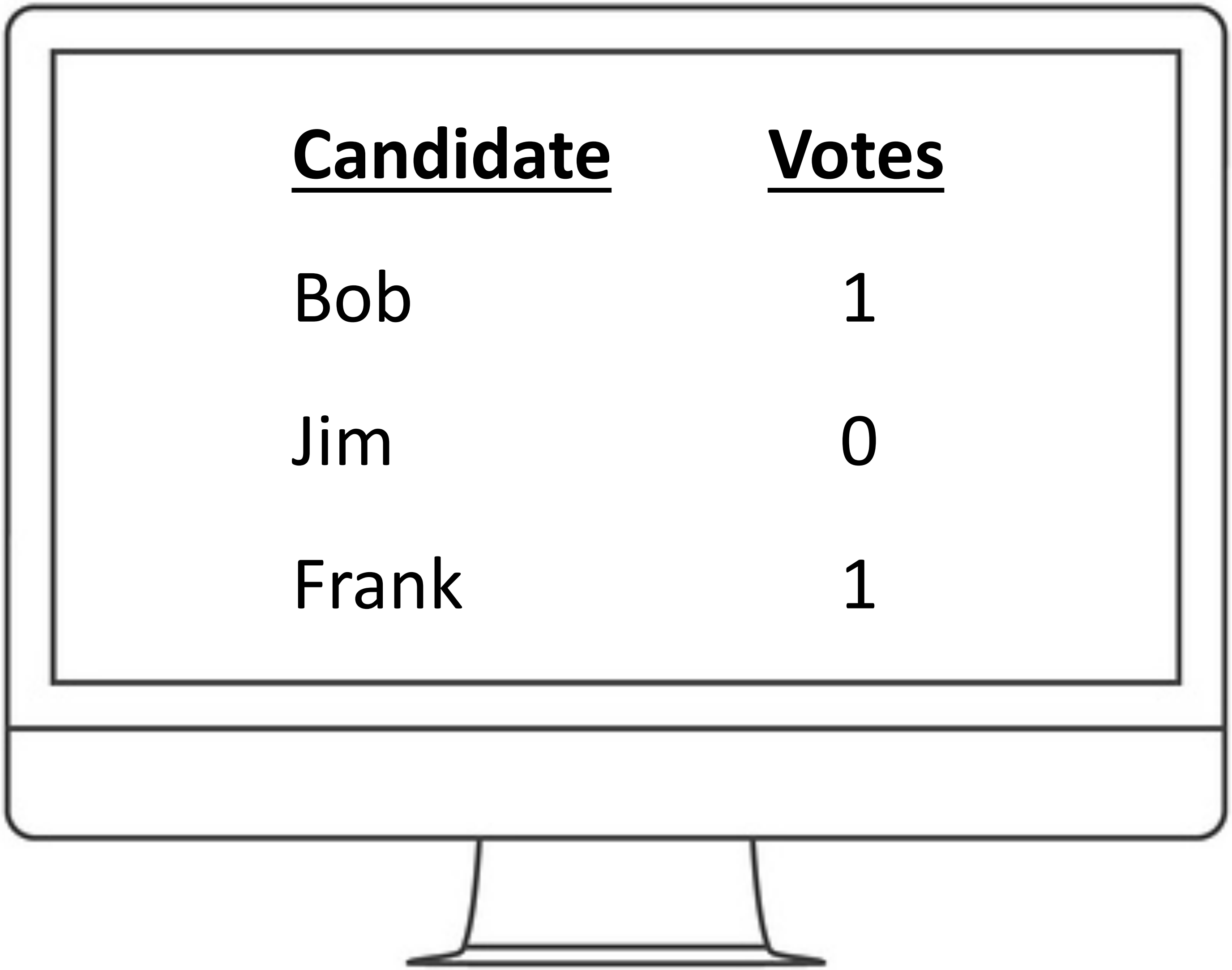


Frank: 1 vote



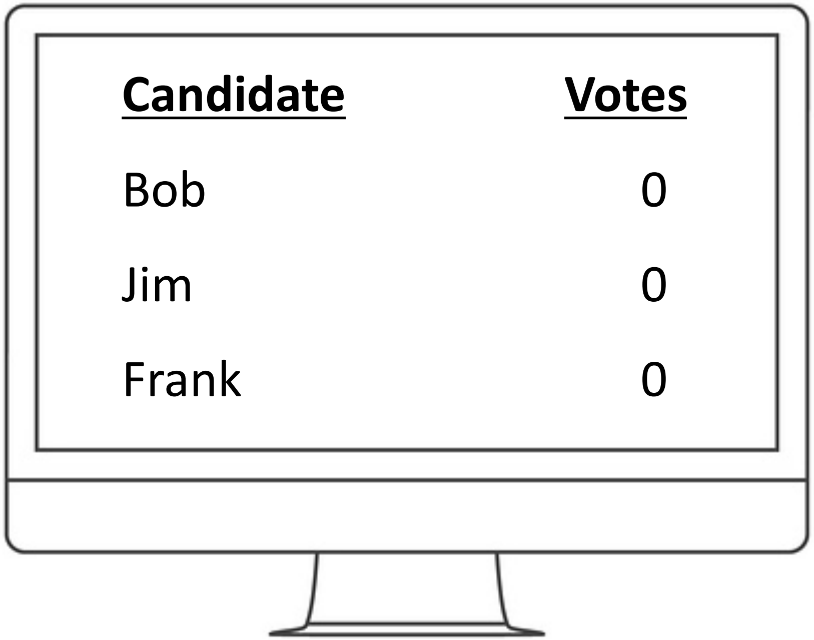
Candidate	Votes
Bob	0
Jim	0
Frank	0

State: 2



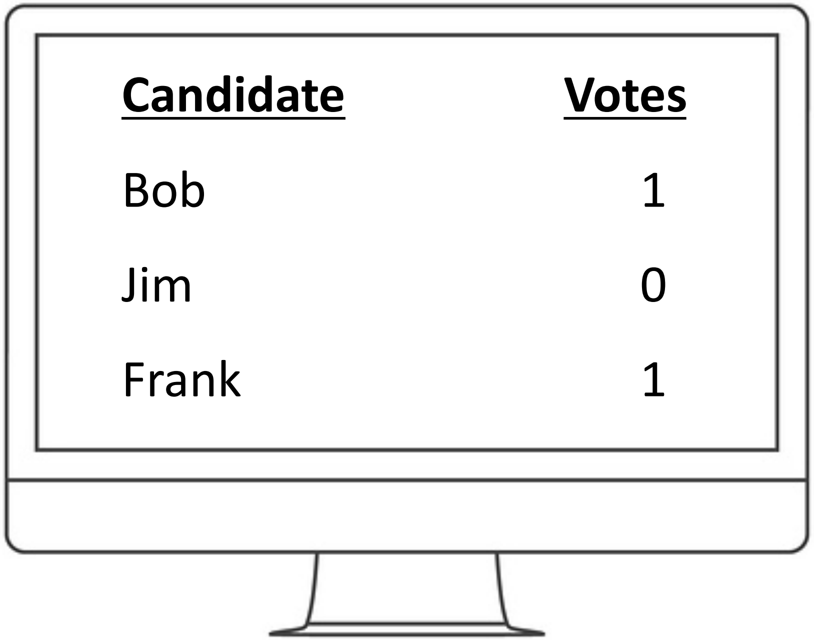
Candidate	Votes
Bob	1
Jim	0
Frank	1

State: 1



Candidate	Votes
Bob	0
Jim	0
Frank	0

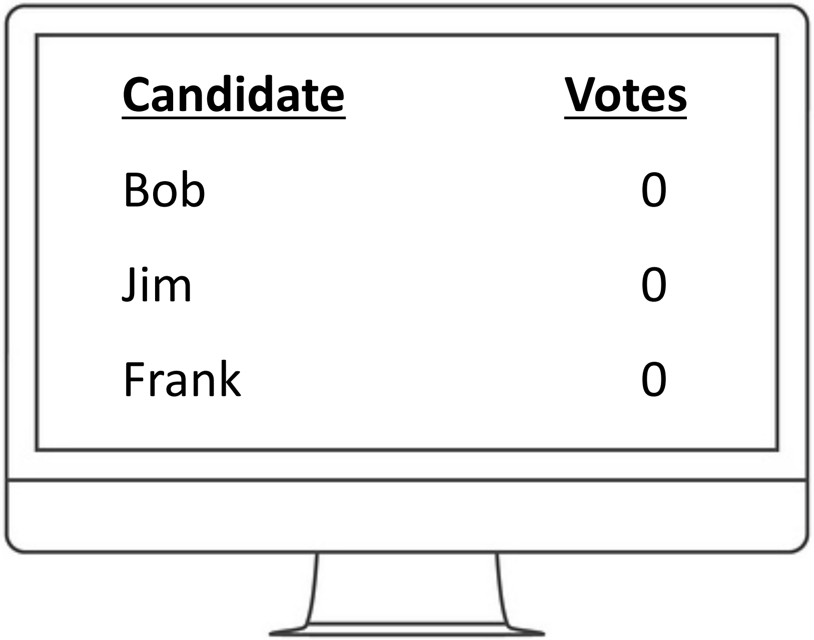
State: 2



Candidate	Votes
Bob	1
Jim	0
Frank	1

Equivalent to:

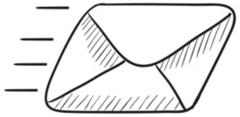
State: 1



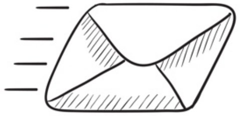
Candidate	**Votes**
Bob	0
Jim	0
Frank	0

State: 2

State 1 plus…



Bob: 1 vote



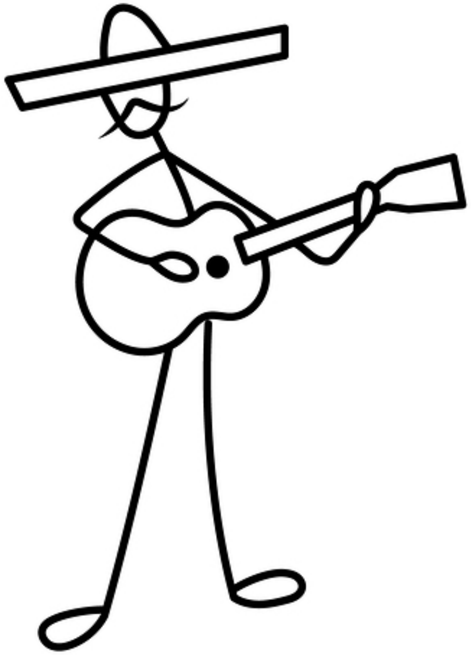
Frank: 1 vote

General purpose blockchains

Messages are… anything!

Each block is the system state at that time

Current State = Original state + All Changes



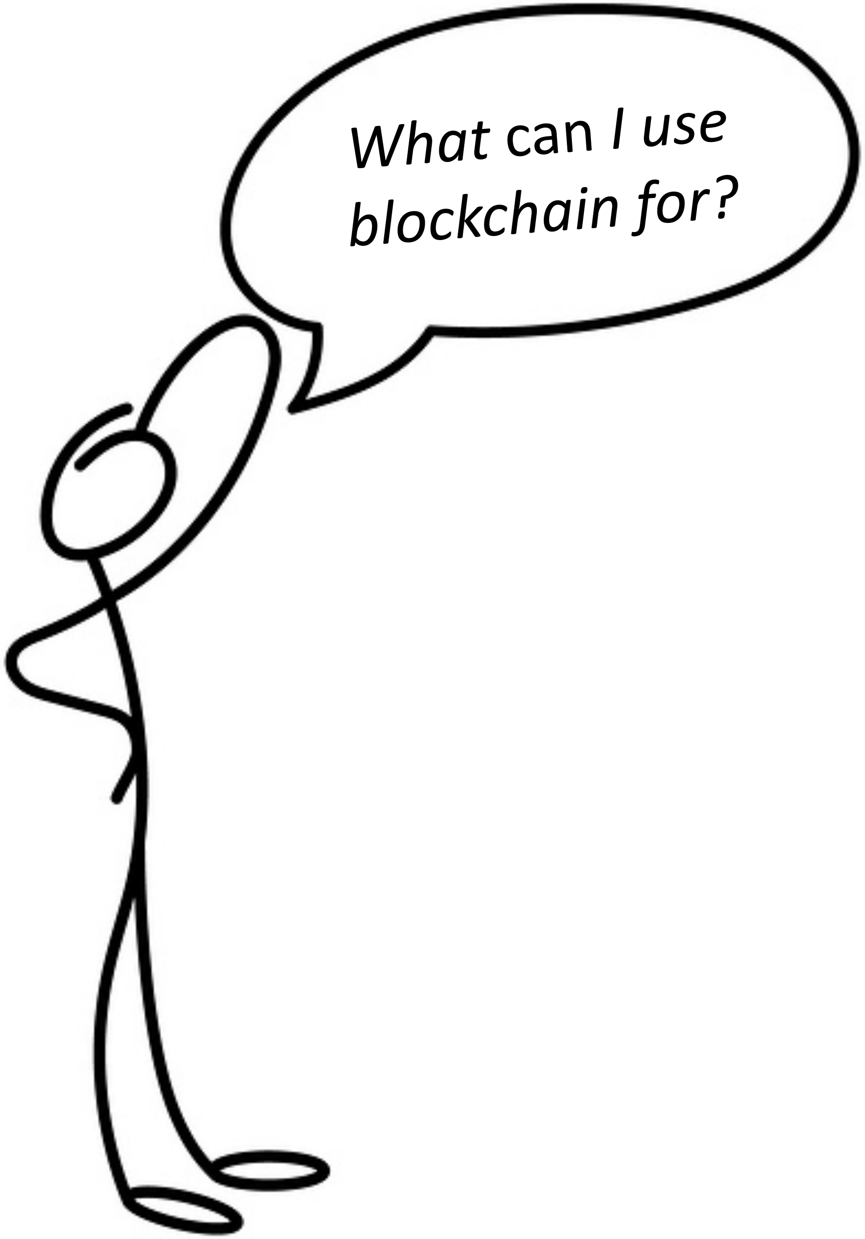
Recap

You now know:

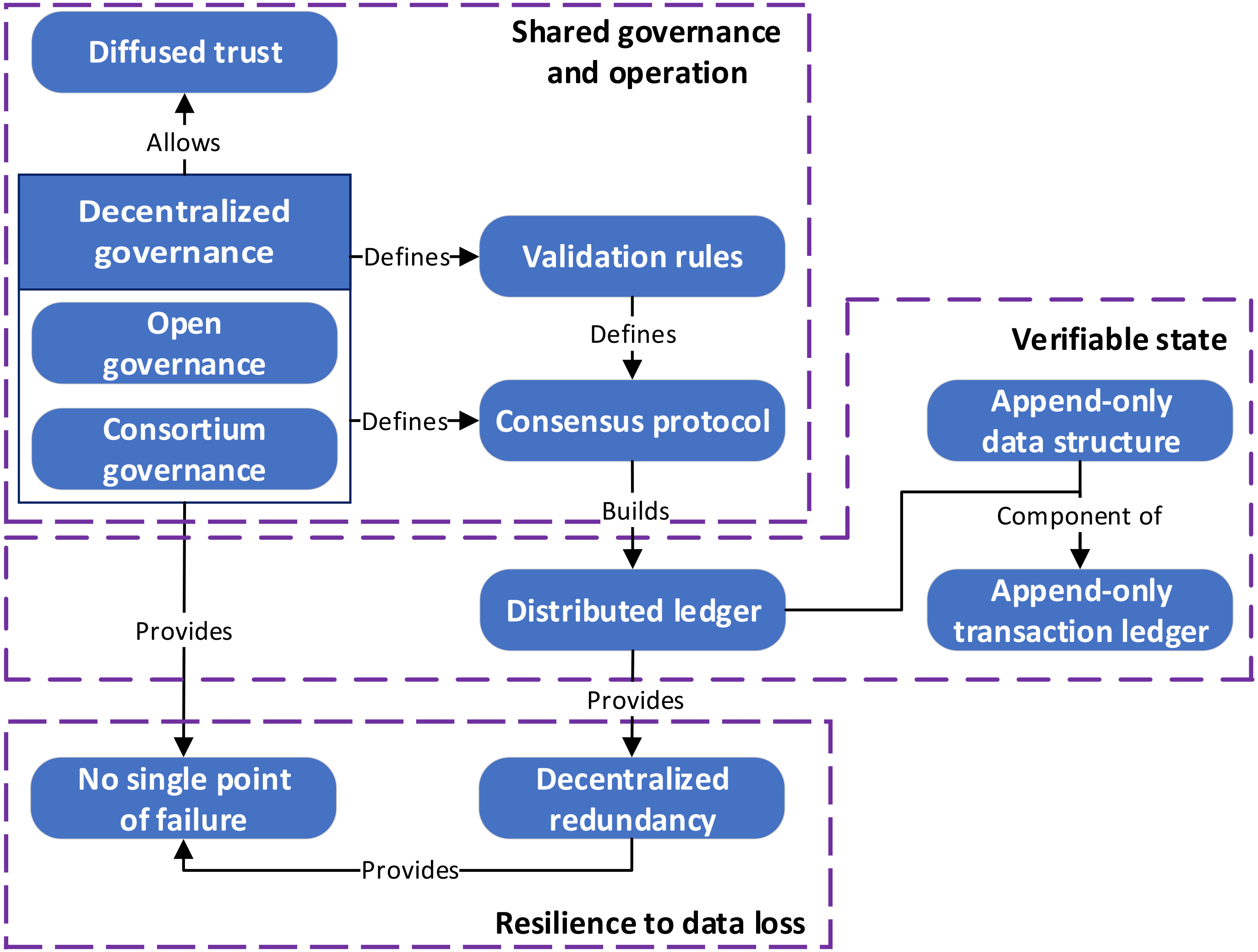
- What blockchains are (linked, signed transactions)
- How & why we “mine”
- Blockchain for cryptocurrency
- Blockchain for applications

Things you probably still wonder:

- What can I use it for?
- How do I use blockchain?
- Who’s used it? Did it prove useful for them?
- What’s for lunch?

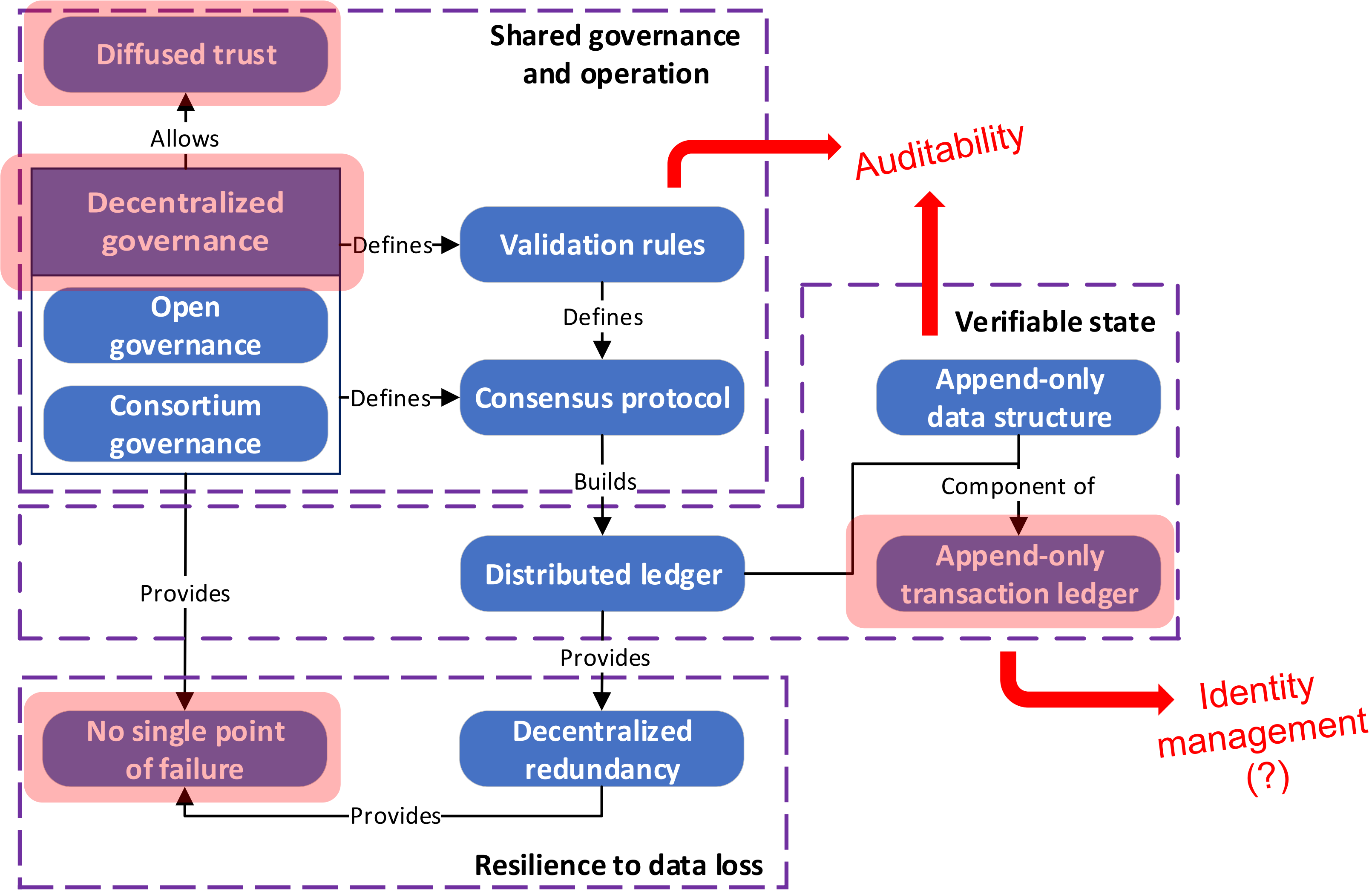

What can I use blockchain for?

Blockchain – What can I use it for?



Ruoti, S; et al. "SoK: Blockchain Technology and Its Potential Use Cases." In submission, 2019.

Blockchain – What can I use it for?



Ruoti, S; et al. "SoK: Blockchain Technology and Its Potential Use Cases." In submission, 2019.

1. **Financial Instruments, Records and Models**
    1. Currency
    2. Private equities
    3. Public equities
    4. Bonds
    5. Derivatives (futures, forwards, swaps, options and more complex variations)
    6. Voting rights associated with any of the above
    7. Commodities
    8. Spending records
    9. Trading records
    10. Mortgage / loan records
    11. Servicing records
    12. Crowd-funding
    13. Micro-finance
    14. Micro-charity
2. **Public Records**
    1. Land titles
    2. Vehicle registries
    3. Business license
    4. Business incorporation / dissolution records
    5. Business ownership records
    6. Regulatory records
    7. Criminal records
    8. Passports
    9. Birth certificates
    10. Death certificates
    11. Voter IDs
    12. Voting
    13. Health / Safety Inspections
    14. Building permits
    15. Gun permits
    16. Forensic evidence
    17. Court records
    18. Voting records
    19. Non-profit records
    20. Government/non-profit accounting/transparency
3. **Private Records**
    1. Contracts
    2. Signatures
    3. Wills
    4. Trusts
    5. Escrows
    6. GPS trails (personal)
4. **Other Semi-Public Records**
    4. Degree
    5. Certifications
    6. Learning Outcomes
    7. Grades
    8. HR records (salary, performance reviews, accomplishment)
    9. Medical records
    10. Accounting records
    11. Business transaction records
    12. Genome data
    13. GPS trails (institutional)
    14. Delivery records
    15. Arbitration
5. **Physical Asset Keys**
    1. Home / apartment keys
    2. Vacation home / timeshare keys
    3. Hotel room keys
    4. Car keys
    5. Rental car keys
    6. Leased cars keys
    7. Locker keys
    8. Safety deposit box keys
    9. Package delivery (split key between delivery firm and receiver)
    10. Betting records
    11. Fantasy sports records (!)
6. **Intangibles (?)**
    1. Coupons
    2. Vouchers
    3. Reservations (restaurants, hotels, queues, etc)
    4. Movie tickets
    5. Patents
    6. Copyrights
    7. Trademarks
    8. Software licenses
    9. Videogame licenses
    10. Music/movie/book licenses (DRM)
    11. Domain names
    12. Online identities
    13. Proof of authorship / Proof of prior art
7. **Other**
    1. Documentary records (photos, audio, video)
    2. Data records (sports scores, temperature, etc)
    3. Sim Cards
    4. GPS network identity
    5. Gun unlock codes
    6. Weapons unlock codes
    7. Nuclear launch codes (!)
    8. Spam control (micro-payments for posting)

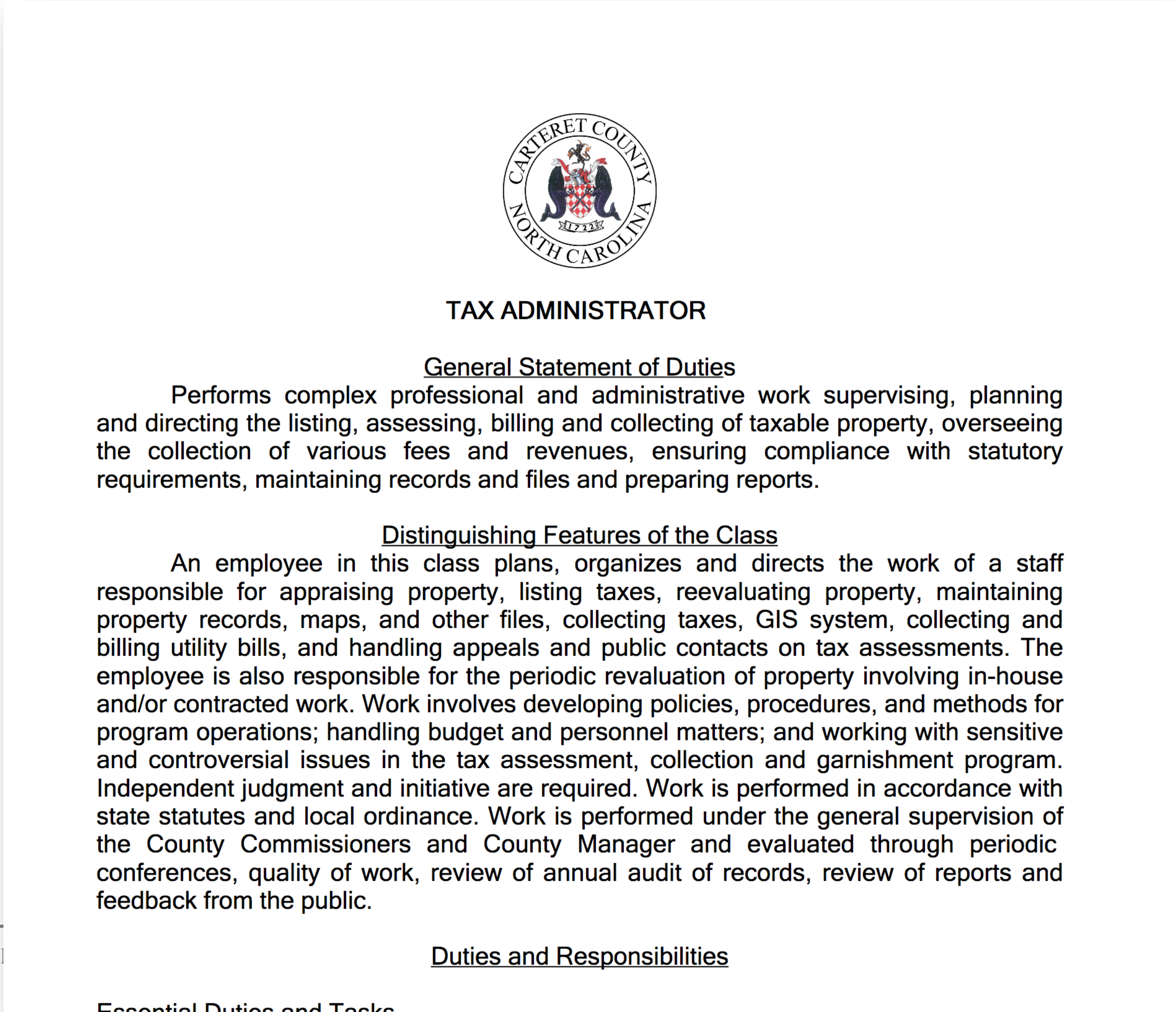
Major relevant use cases – Medical

Use case	Properties
Supply chain management • Medical supplies & equipment • Pharmaceuticals	Auditability, Immutability, Shared governance
Records management • EMR/EHR • Insurance • Research documentation	Auditability, Immutability, Shared governance
Asset management • Device tracking • Drug delivery	Auditability, Immutability, Identity management
Data sharing	Auditability, Decentralized governance, Redundancy

Proposed use cases – Medical

Use Case	Notes
Chain of custody for… • inspection or imports data exchange • labs information	Track data, monitor activity, prevent tampering, audit
State data exchange – authorization and authentication	
HHS Accelerate – Procurement	Press coverage, Demo
CDC/IBM blockchain use case • Information data exchange (CDC: EHR, FDA: Oncology) • Supply chain	
Leidos Health Group document • Opioid chain of custody • Informed Consent	

What the heck is a tax administrator?



CARTERET COUNTY NORTH CAROLINA 1722

TAX ADMINISTRATOR

General Statement of Duties

Performs complex professional and administrative work supervising, planning and directing the listing, assessing, billing and collecting of taxable property, overseeing the collection of various fees and revenues, ensuring compliance with statutory requirements, maintaining records and files and preparing reports.

Distinguishing Features of the Class

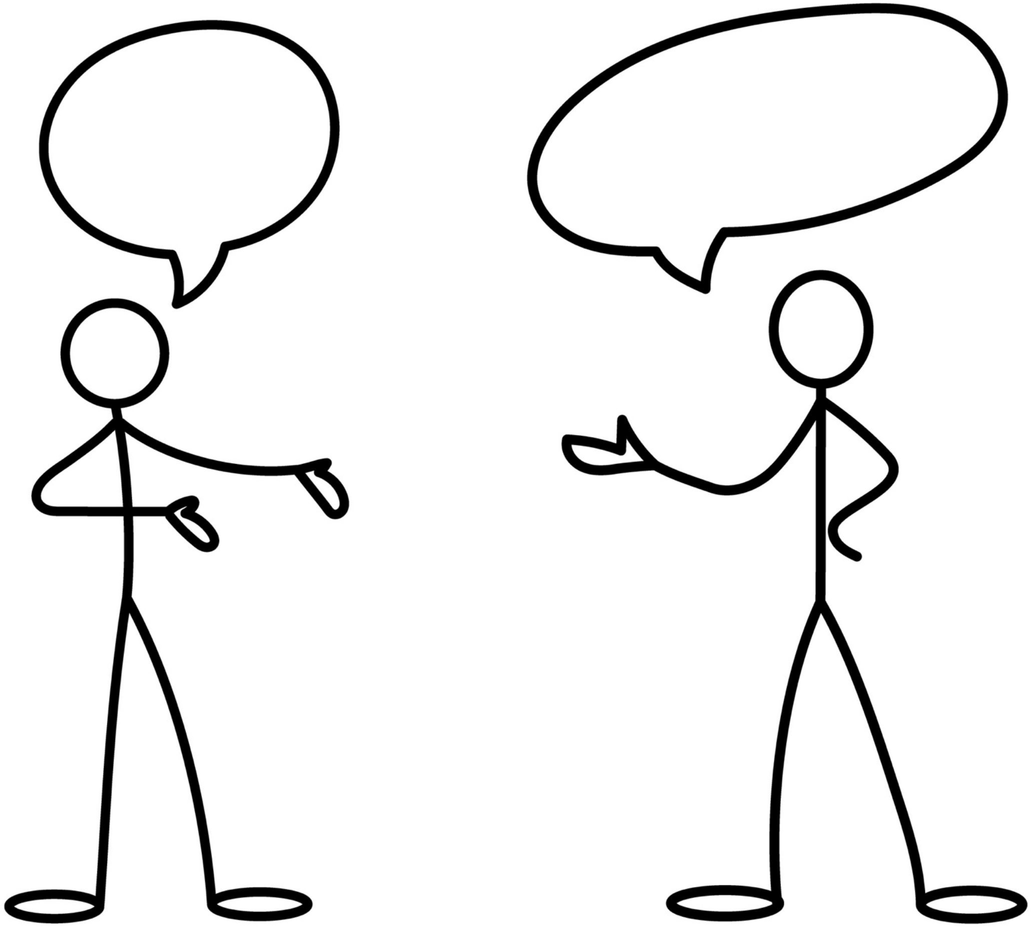
An employee in this class plans, organizes and directs the work of a staff responsible for appraising property, listing taxes, reevaluating property, maintaining property records, maps, and other files, collecting taxes, GIS system, collecting and billing utility bills, and handling appeals and public contacts on tax assessments. The employee is also responsible for the periodic revaluation of property involving in-house and/or contracted work. Work involves developing policies, procedures, and methods for program operations; handling budget and personnel matters; and working with sensitive and controversial issues in the tax assessment, collection and garnishment program. Independent judgment and initiative are required. Work is performed in accordance with state statutes and local ordinance. Work is performed under the general supervision of the County Commissioners and County Manager and evaluated through periodic conferences, quality of work, review of annual audit of records, review of reports and feedback from the public.

Duties and Responsibilities

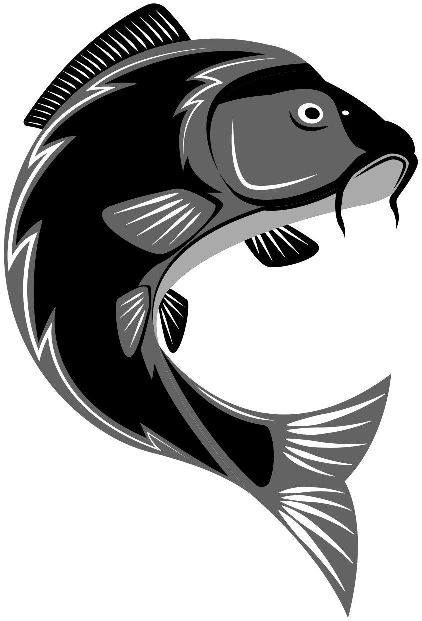
Essential Duties and Tasks

Major relevant use cases – Tax *(proposed)*

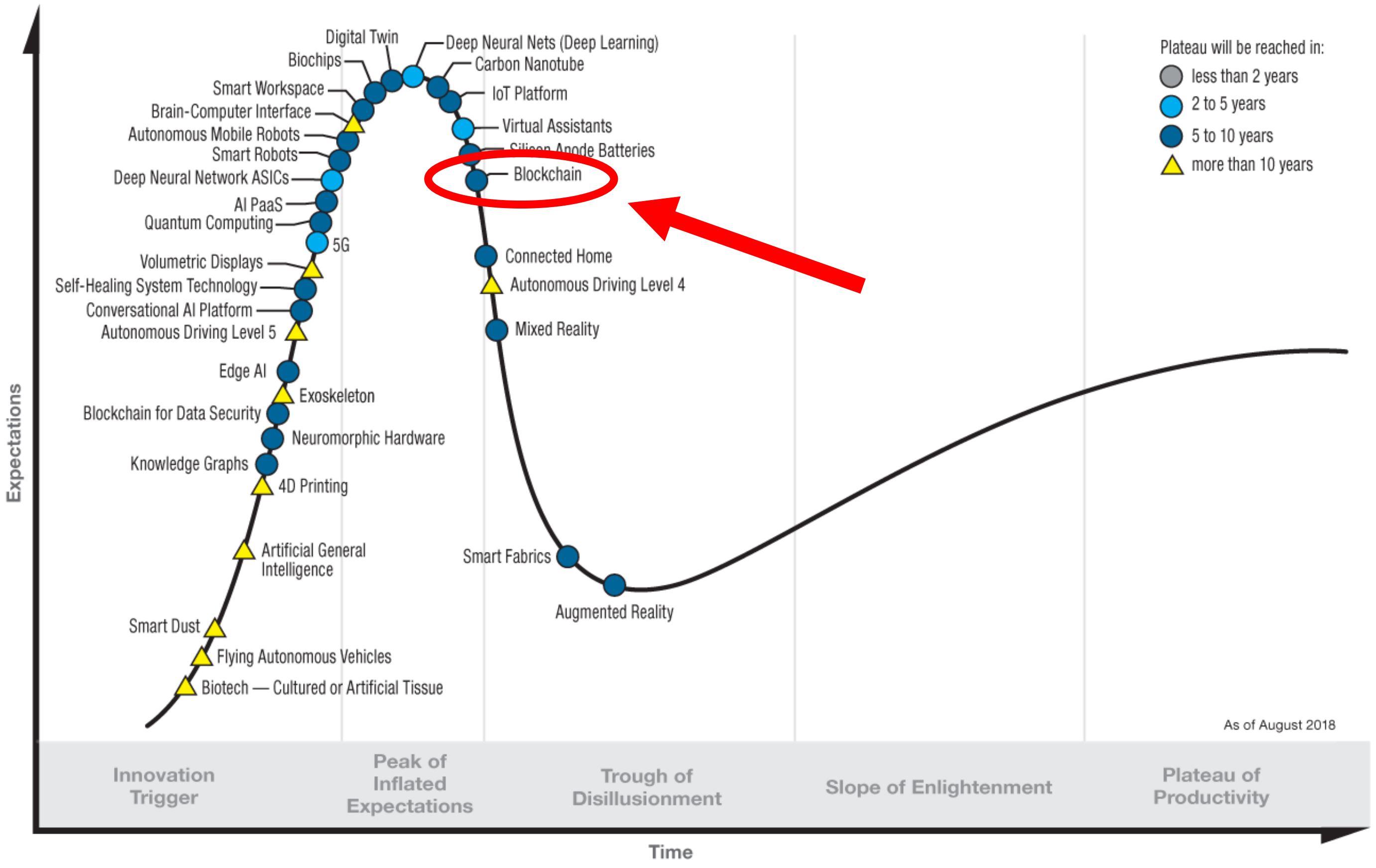
Use case	Properties
Records management - Tax records - Official communications to individuals and companies	Auditability, Immutability, Shared governance, Identity management
Policy dissemination - Internal - Taxpayer - Corporation	Immutability, Identity management
Data sharing	Auditability, Decentralized governance, Redundancy



Who’s used it?



Hype Cycle for Emerging Technologies, 2018



gartner.com/SmarterWithGartner

Source: Gartner (August 2018)
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Blockchain platforms – "don't blink"

Early 2015

Ethereum

Hyperledger (vaporware)

Apr 12, 2017

BigChainDB

Chain Core

Credits

Domus Tower

Elements Eris:db

HydraChain

Hyperledger Iroha

Hyperledger Sawtooth

Multichain

Openchain

Stellar

Symbiont Assembly

Oct 16, 2018

Cardano

Icon

Aion

Wanchain

Nebilo

Zilliqa

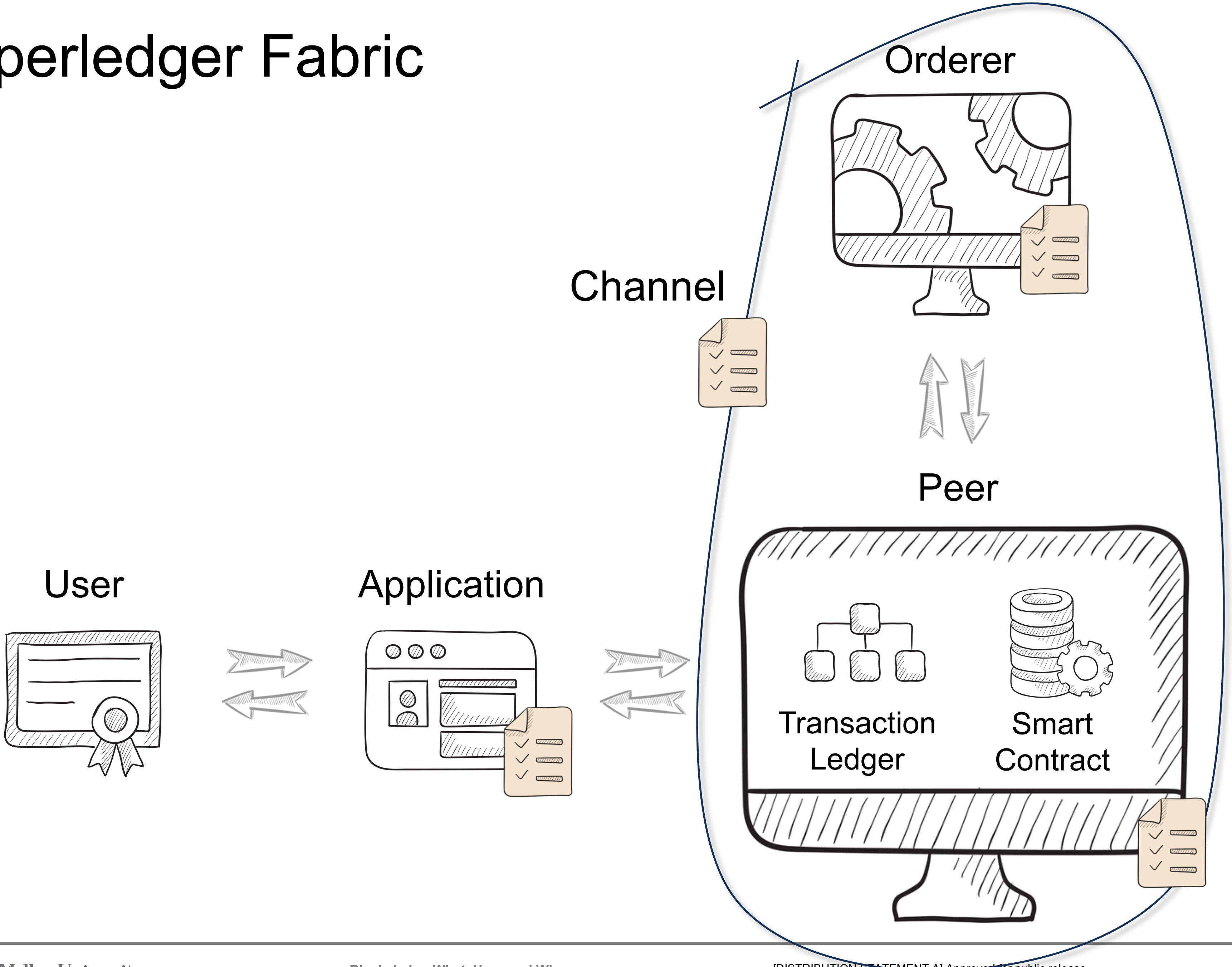
ArcBlock

EOS

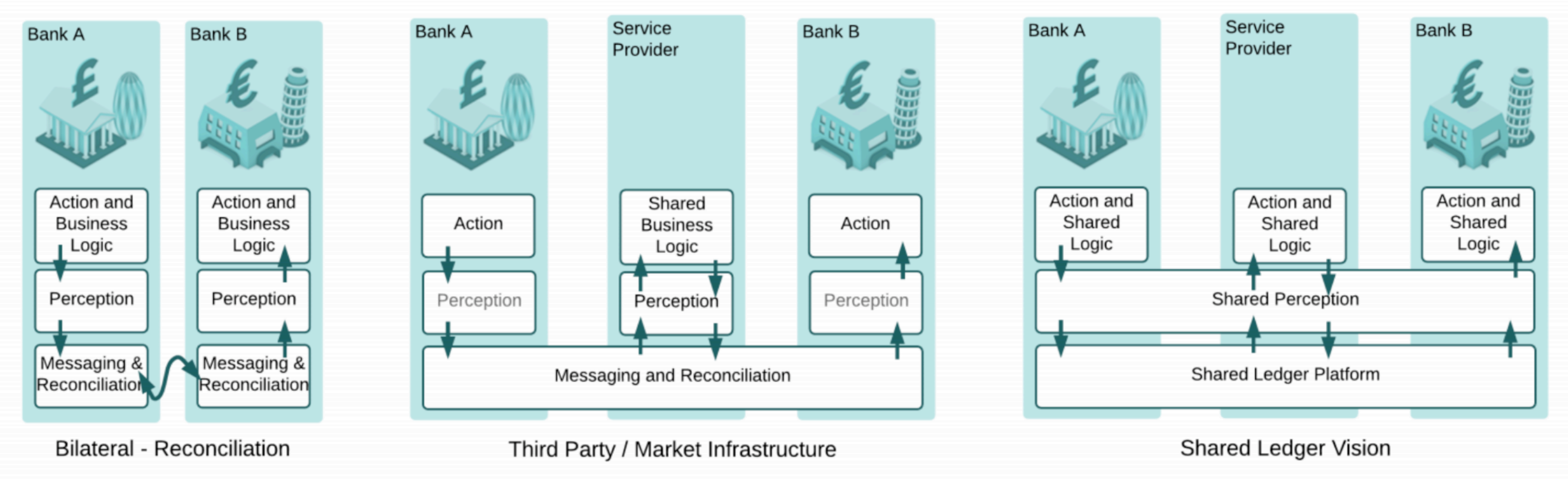
How do I use a blockchain?

The same as any other software!

Hyperledger Fabric

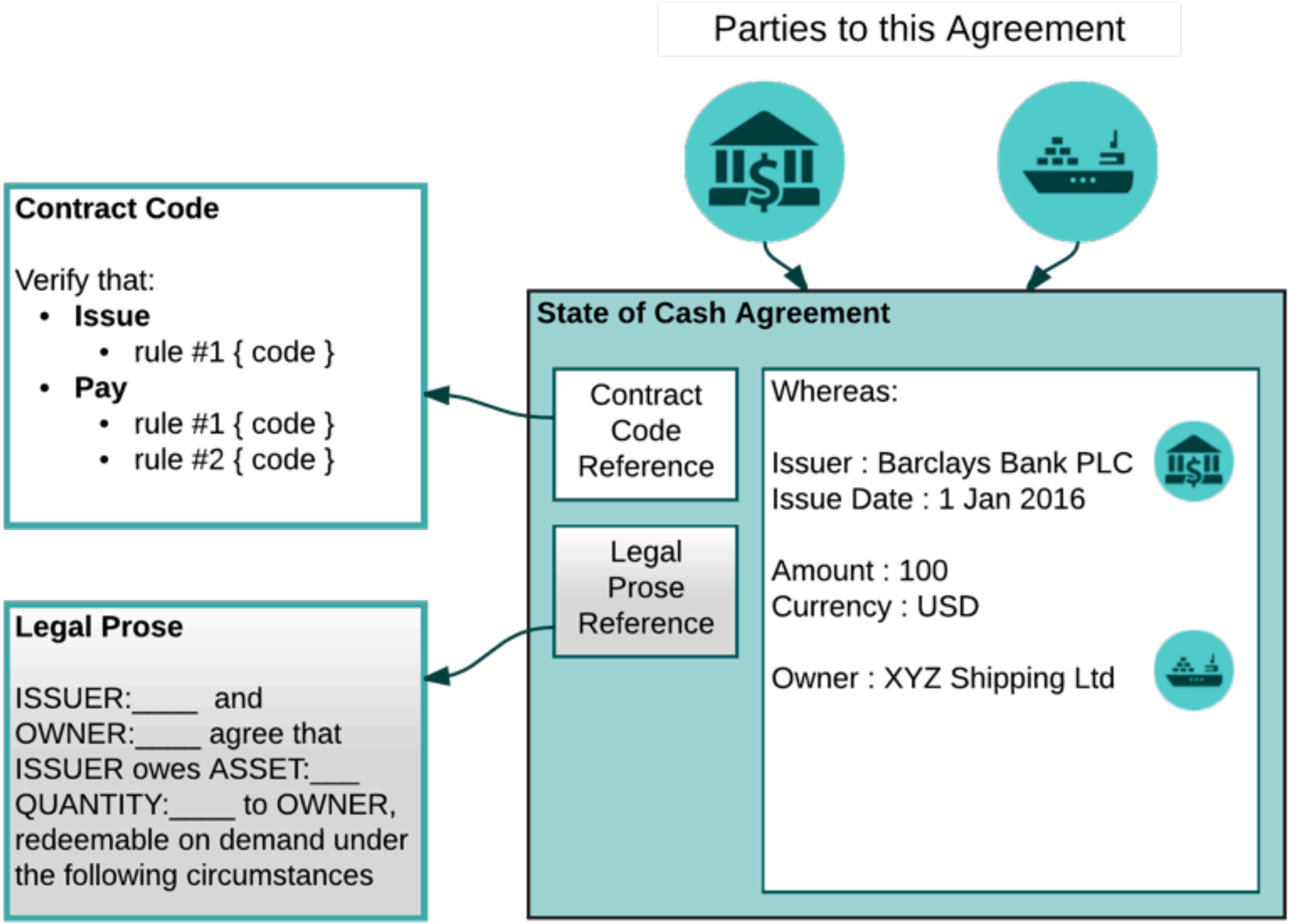


Corda – Blockchain platform



https://www.corda.net/content/corda-platform-whitepaper.pdf, Figure 1

Corda – Blockchain platform



Parties to this Agreement

Contract Code

Verify that:
- **Issue**
  - rule #1 { code }
- **Pay**
  - rule #1 { code }
  - rule #2 { code }

Legal Prose

ISSUER:____ and OWNER:____ agree that ISSUER owes ASSET:___ QUANTITY:____ to OWNER, redeemable on demand under the following circumstances

State of Cash Agreement

Contract Code Reference

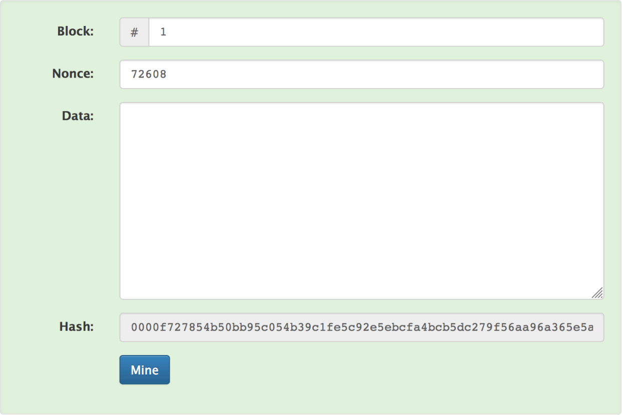
Legal Prose Reference

Whereas:

Issuer : Barclays Bank PLC
Issue Date : 1 Jan 2016

Amount : 100
Currency : USD

Owner : XYZ Shipping Ltd



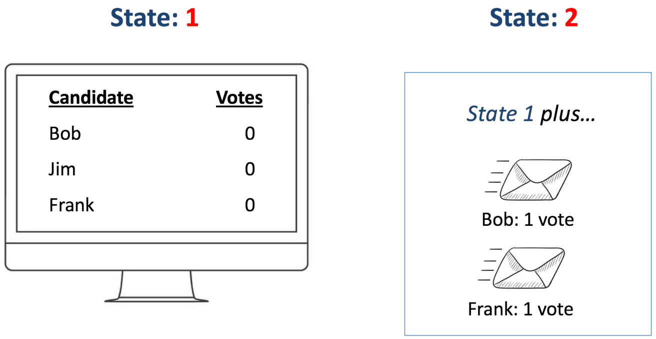
Block: # 1

Nonce: 72608

Data:

Hash: 0000f727854b50bb95c054b39c1fe5c92e5ebcfa4bcb5dc279f56aa96a365e5a

Blockchain basics



State: 1

Candidate	Votes
Bob	0
Jim	0
Frank	0

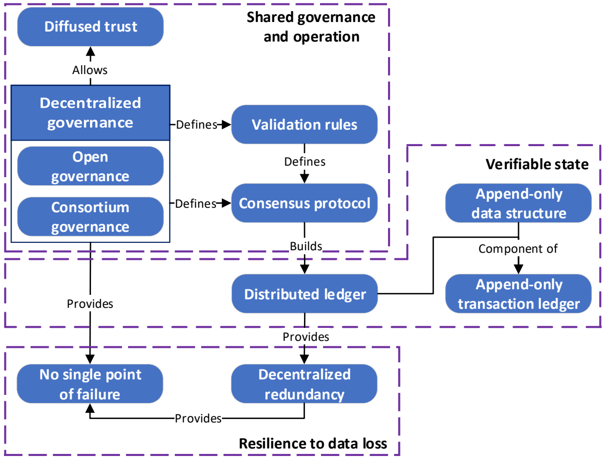
State: 2

State 1 plus…

Bob: 1 vote

Frank: 1 vote

Blockchain-based Applications



Diffused trust

Allows

Shared governance and operation

Decentralized governance

Defines

Validation rules

Defines

Open governance

Consortium governance

Defines

Consensus protocol

Builds

Verifiable state

Append-only data structure

Component of

Append-only transaction ledger

Provides

Distributed ledger

Provides

No single point of failure

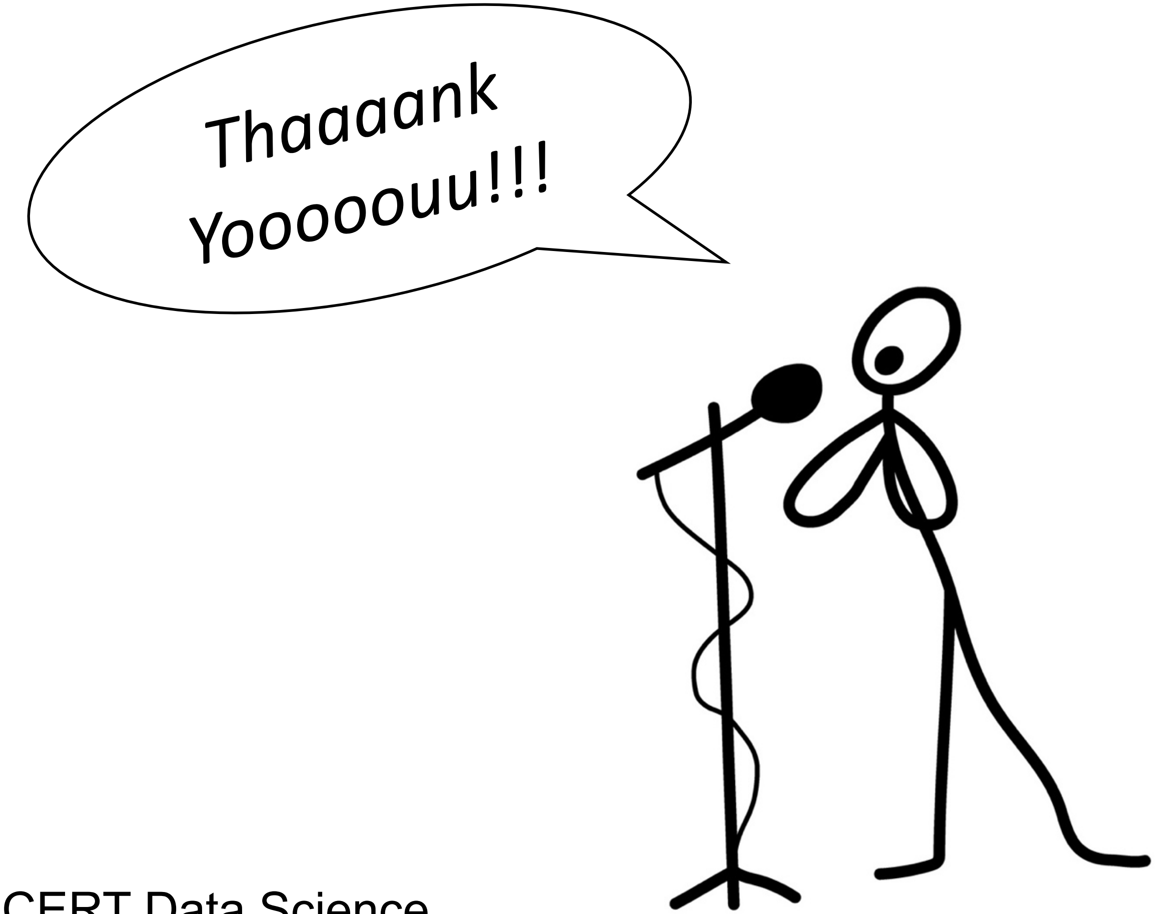
Decentralized redundancy

Provides

Resilience to data loss

Blockchain Use Cases

Implementation Considerations



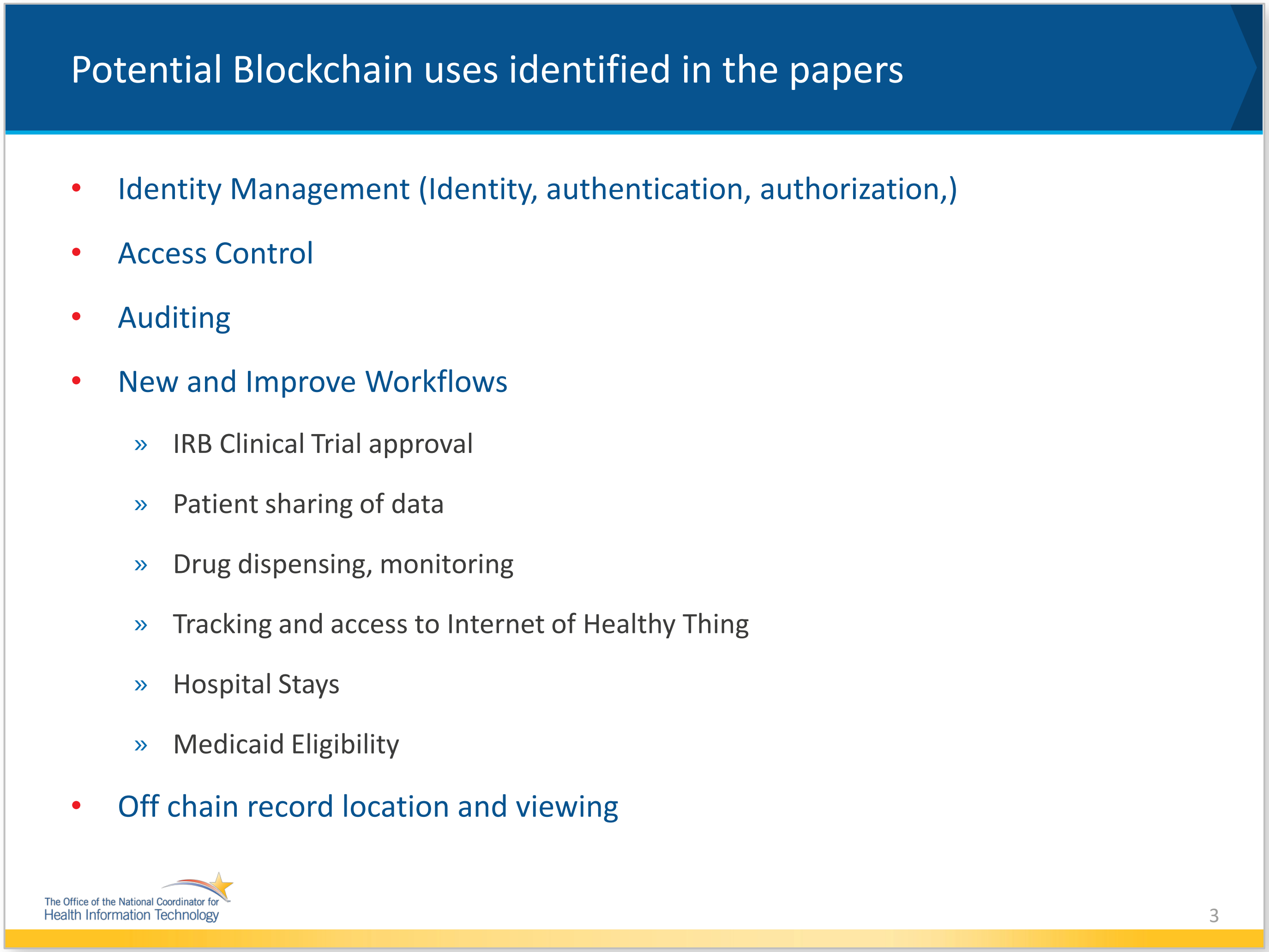
Eliezer Kanal

Technical Manager, CERT Data Science

Telephone: +1 (412) 268–5204

Email: ekanal@cert.org

Backup

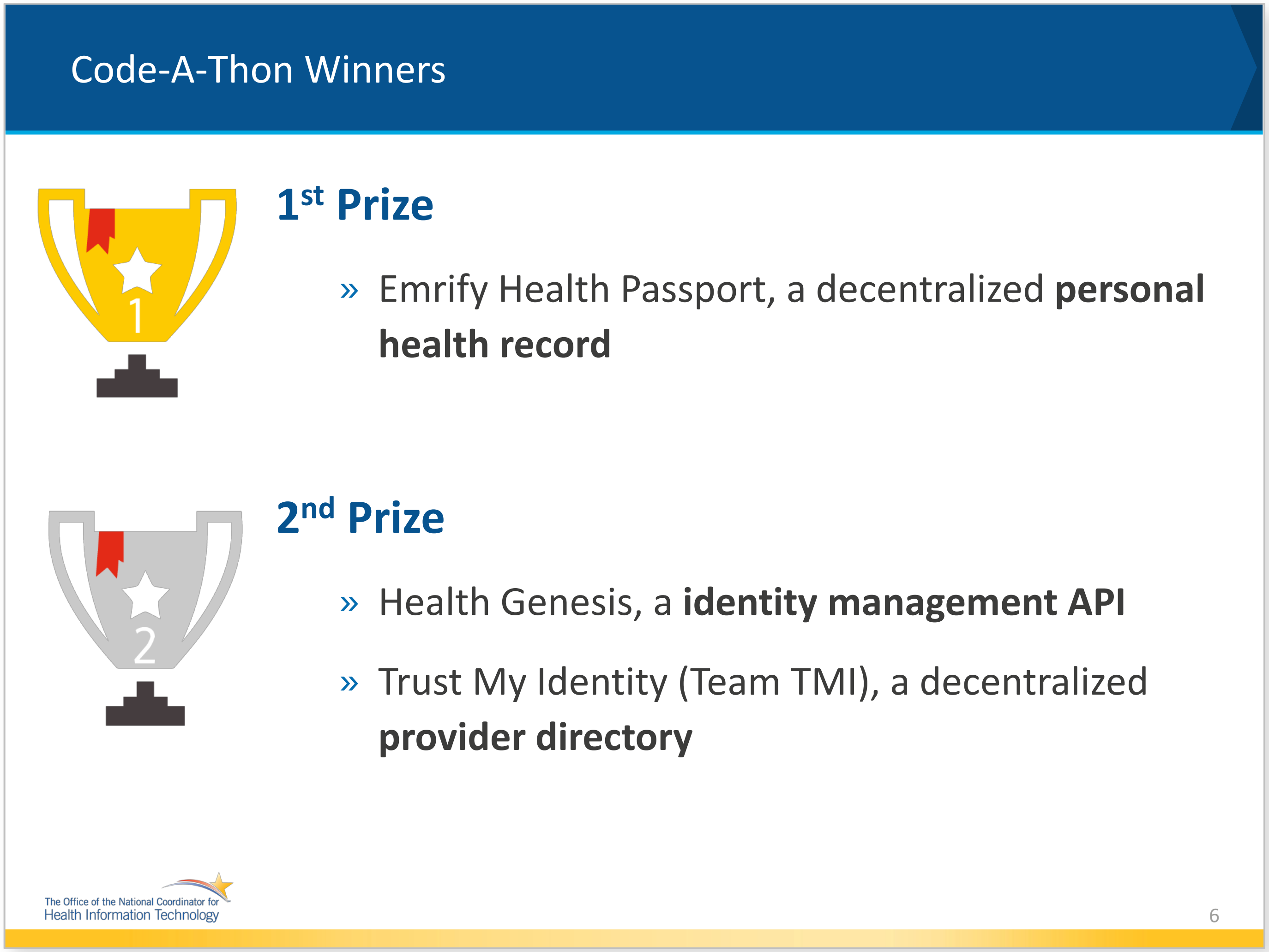


Potential Blockchain uses identified in the papers

- Identity Management (Identity, authentication, authorization,)
- Access Control
- Auditing
- New and Improve Workflows
  - » IRB Clinical Trial approval
  - » Patient sharing of data
  - » Drug dispensing, monitoring
  - » Tracking and access to Internet of Healthy Thing
  - » Hospital Stays
  - » Medicaid Eligibility
- Off chain record location and viewing

The Office of the National Coordinator for
Health Information Technology

3



Code-A-Thon Winners

1st Prize

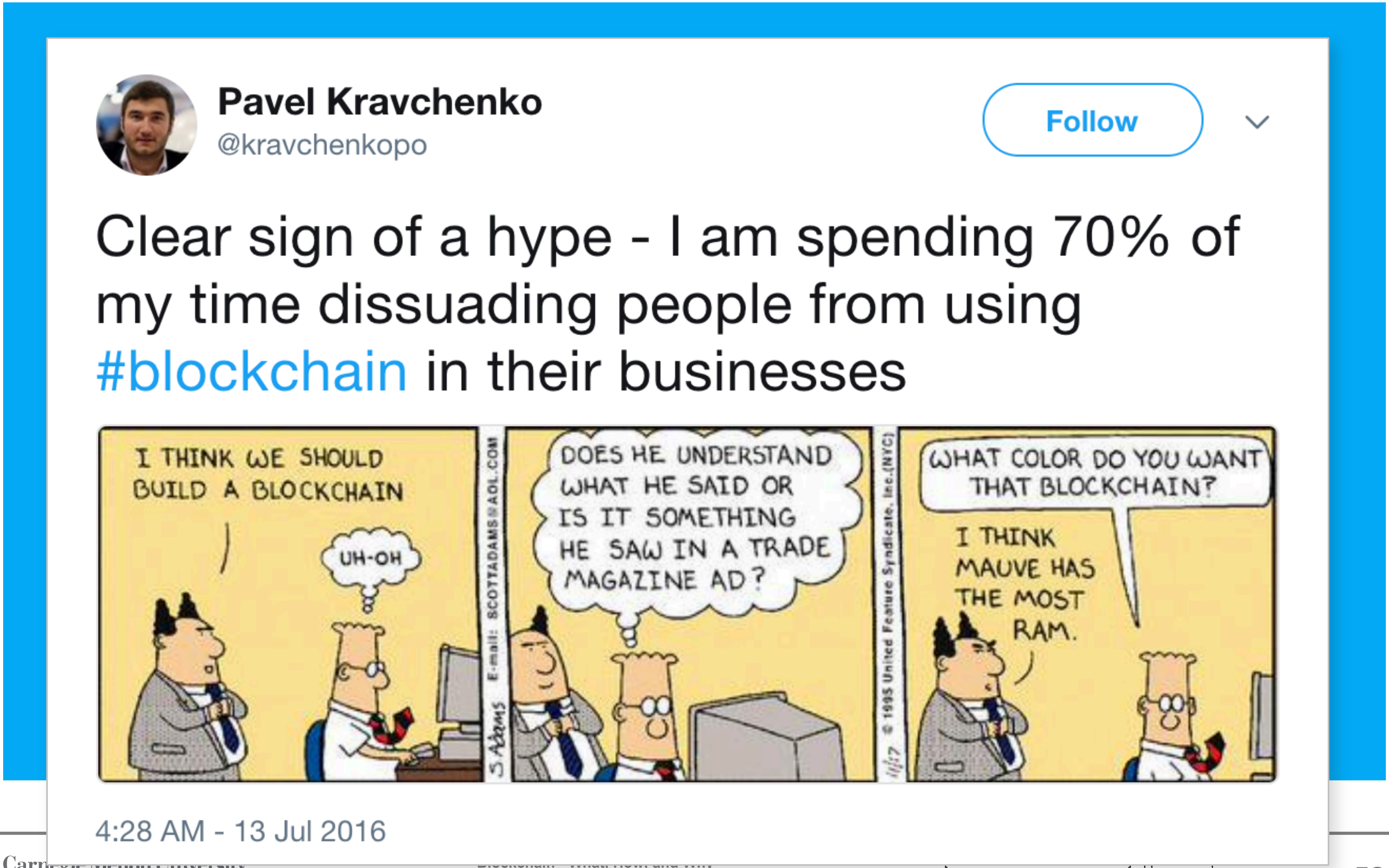
- Emrify Health Passport, a decentralized **personal health record**

2nd Prize

- Health Genesis, a **identity management API**
- Trust My Identity (Team TMI), a decentralized **provider directory**

The Office of the National Coordinator for
Health Information Technology

6



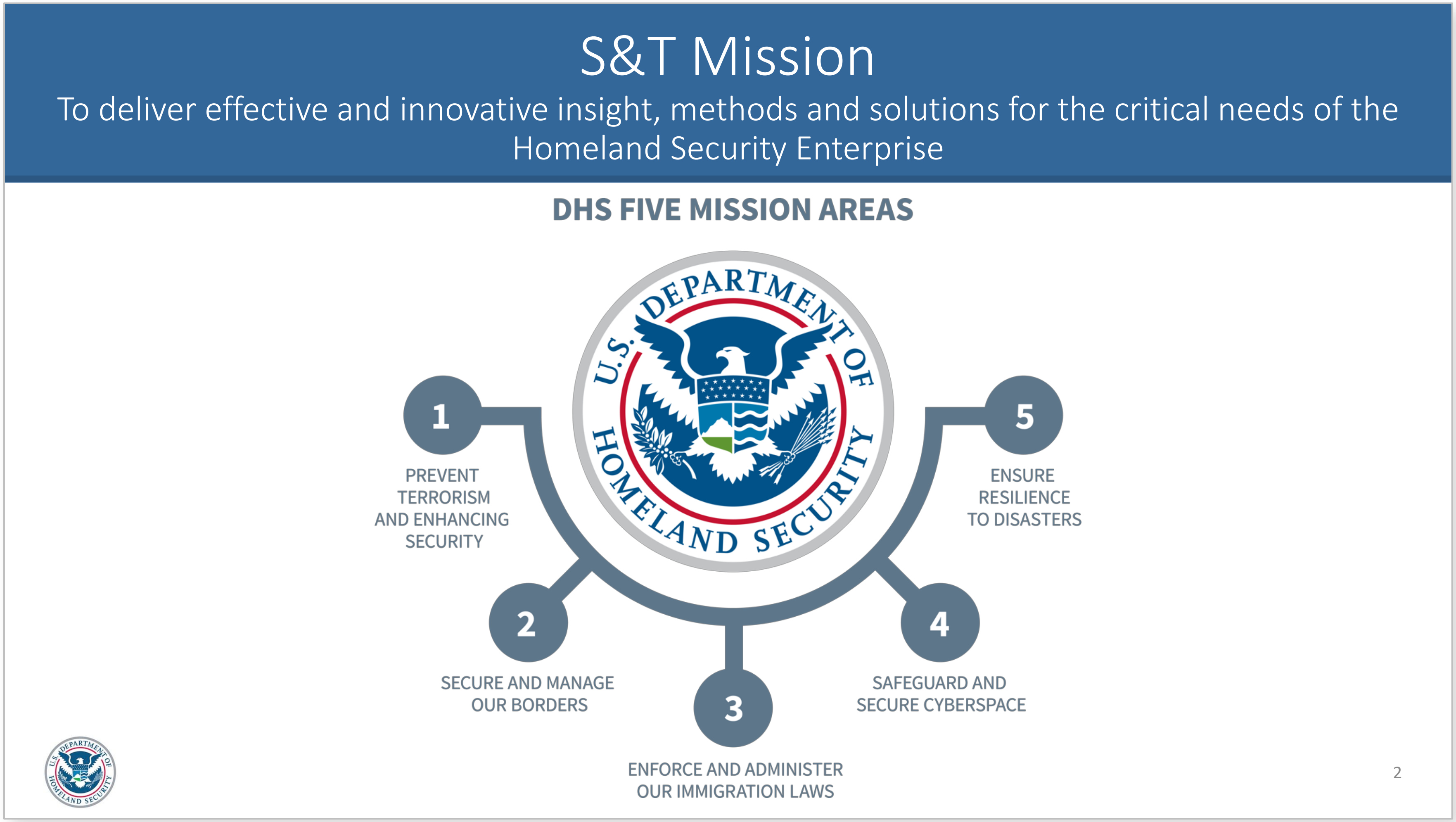
Pavel Kravchenko
@kravchenkopo

Follow

Clear sign of a hype - I am spending 70% of my time dissuading people from using #blockchain in their businesses

4:28 AM - 13 Jul 2016

I THINK WE SHOULD BUILD A BLOCKCHAIN
UH-OH
E-mail: SCOTTADAMS@AOL.COM
S. Adams
DOES HE UNDERSTAND WHAT HE SAID OR IS IT SOMETHING HE SAW IN A TRADE MAGAZINE AD?
© 1995 United Feature Syndicate, Inc.(NYC)
11/17
WHAT COLOR DO YOU WANT THAT BLOCKCHAIN?
I THINK MAUVE HAS THE MOST RAM.



S&T Mission

To deliver effective and innovative insight, methods and solutions for the critical needs of the Homeland Security Enterprise

DHS FIVE MISSION AREAS

1 PREVENT TERRORISM AND ENHANCING SECURITY

2 SECURE AND MANAGE OUR BORDERS

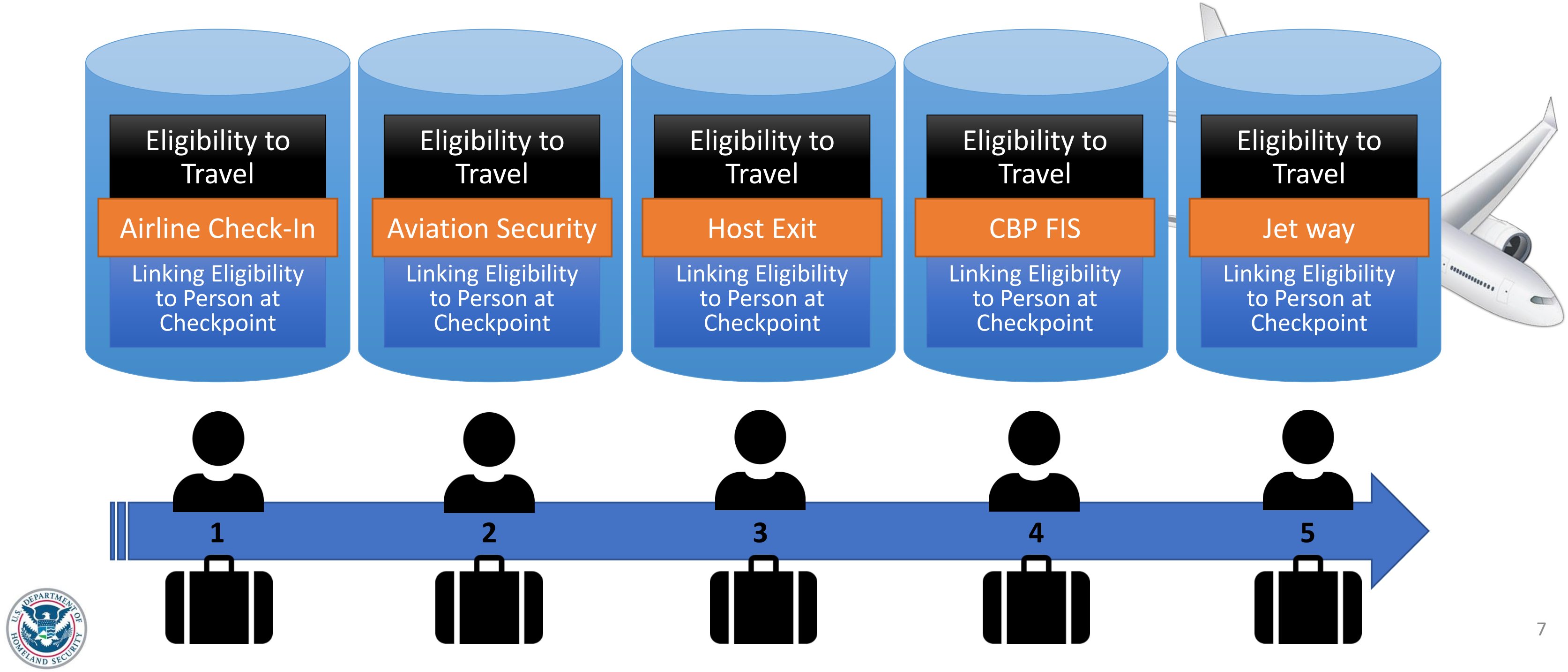
3 ENFORCE AND ADMINISTER OUR IMMIGRATION LAWS

4 SAFEGUARD AND SECURE CYBERSPACE

5 ENSURE RESILIENCE TO DISASTERS

2

Improving International Passenger Processing



Eligibility to Travel | Airline Check-In | Linking Eligibility to Person at Checkpoint | 1

Eligibility to Travel | Aviation Security | Linking Eligibility to Person at Checkpoint | 2

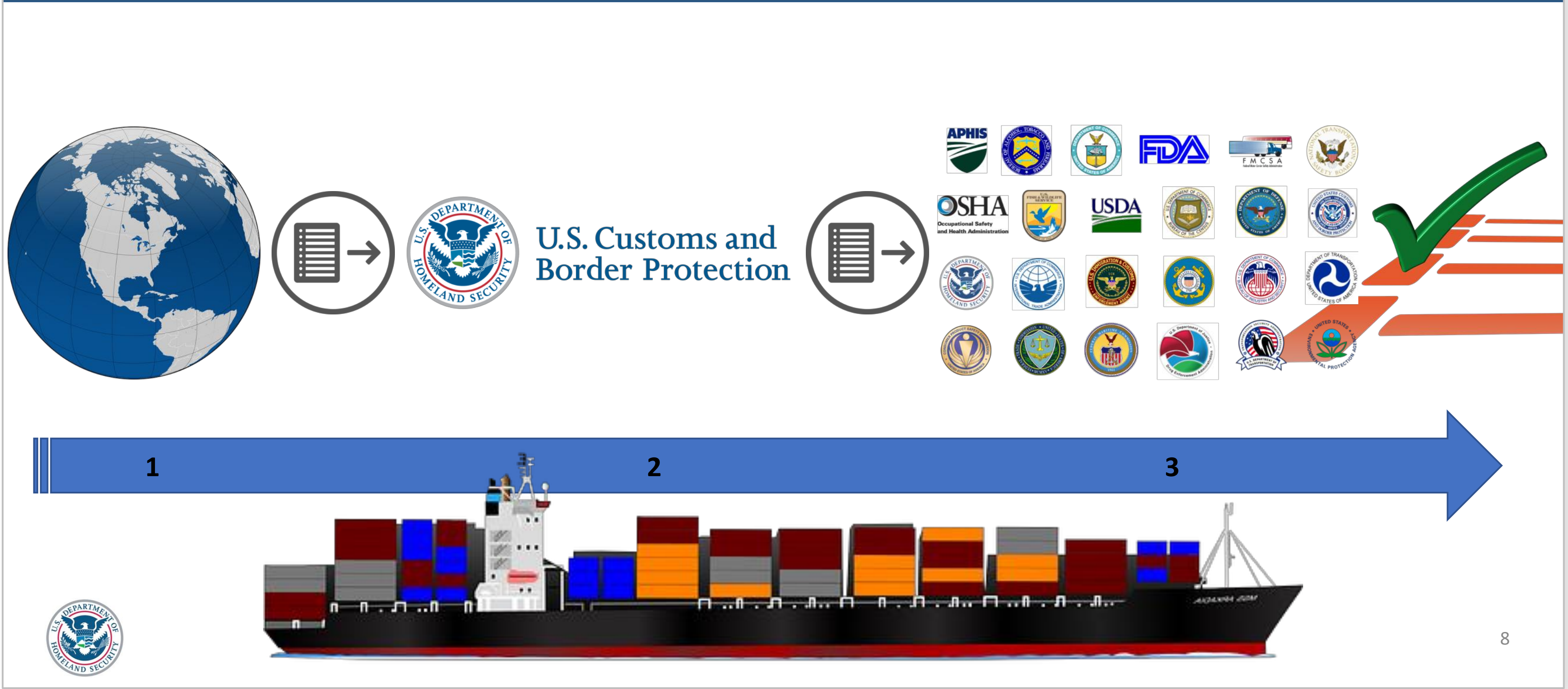
Eligibility to Travel | Host Exit | Linking Eligibility to Person at Checkpoint | 3

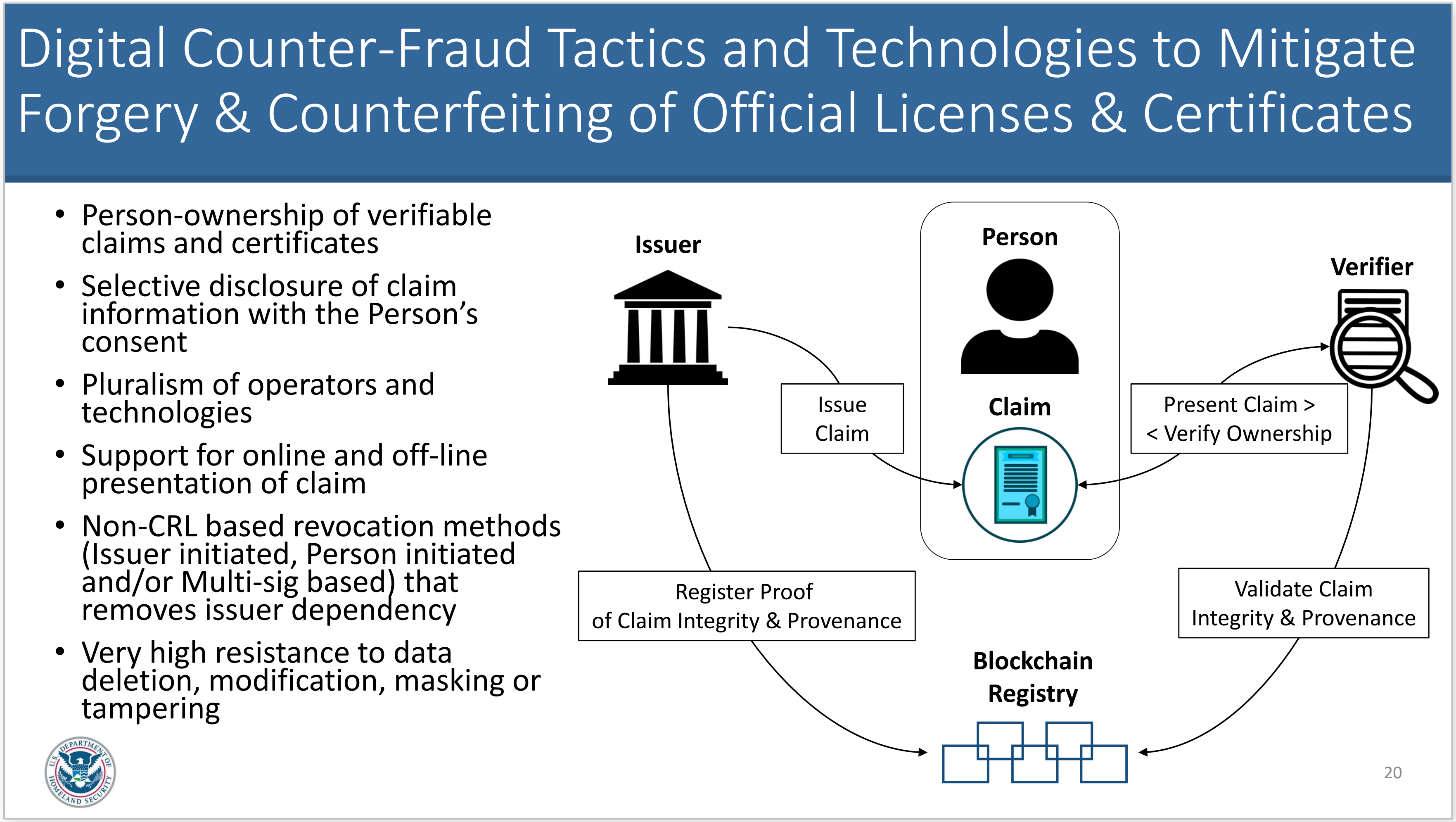
Eligibility to Travel | CBP FIS | Linking Eligibility to Person at Checkpoint | 4

Eligibility to Travel | Jet way | Linking Eligibility to Person at Checkpoint | 5

7

Streamlining and Enhancing International Trade Facilitation


U.S. Customs and Border Protection
APHIS
FDA
FMCSA
OSHA
Occupational Safety and Health Administration
USDA
1
2
3
8



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

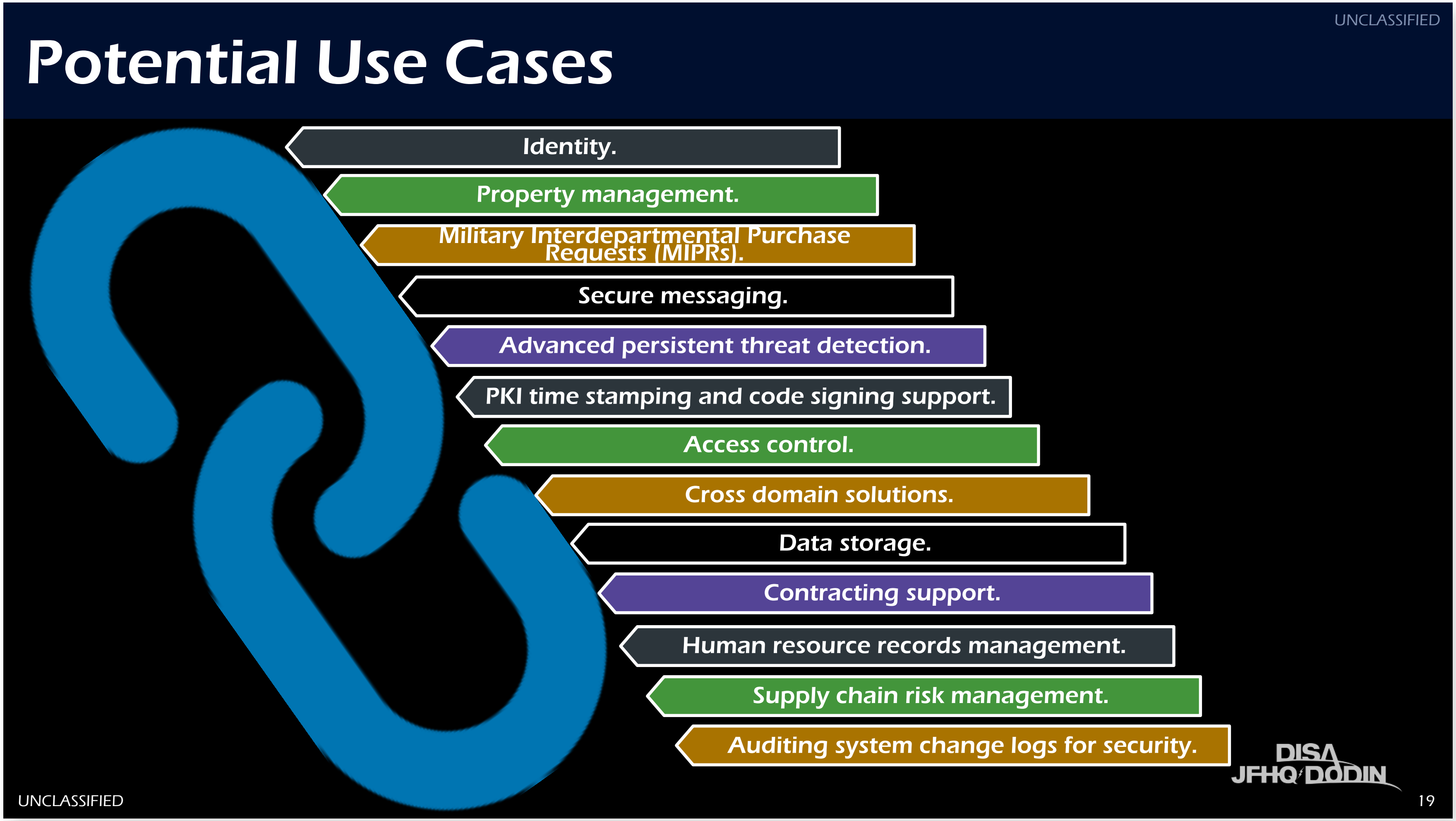
20

UNCLASSIFIED / FOUO

Leveraging Blockchain Solutions

DISA
JFHQ DODIN

Defense Information Systems Agency
Joint Force Headquarters – DOD Information Networks



UNCLASSIFIED

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.

DISA JFHQ-DODIN

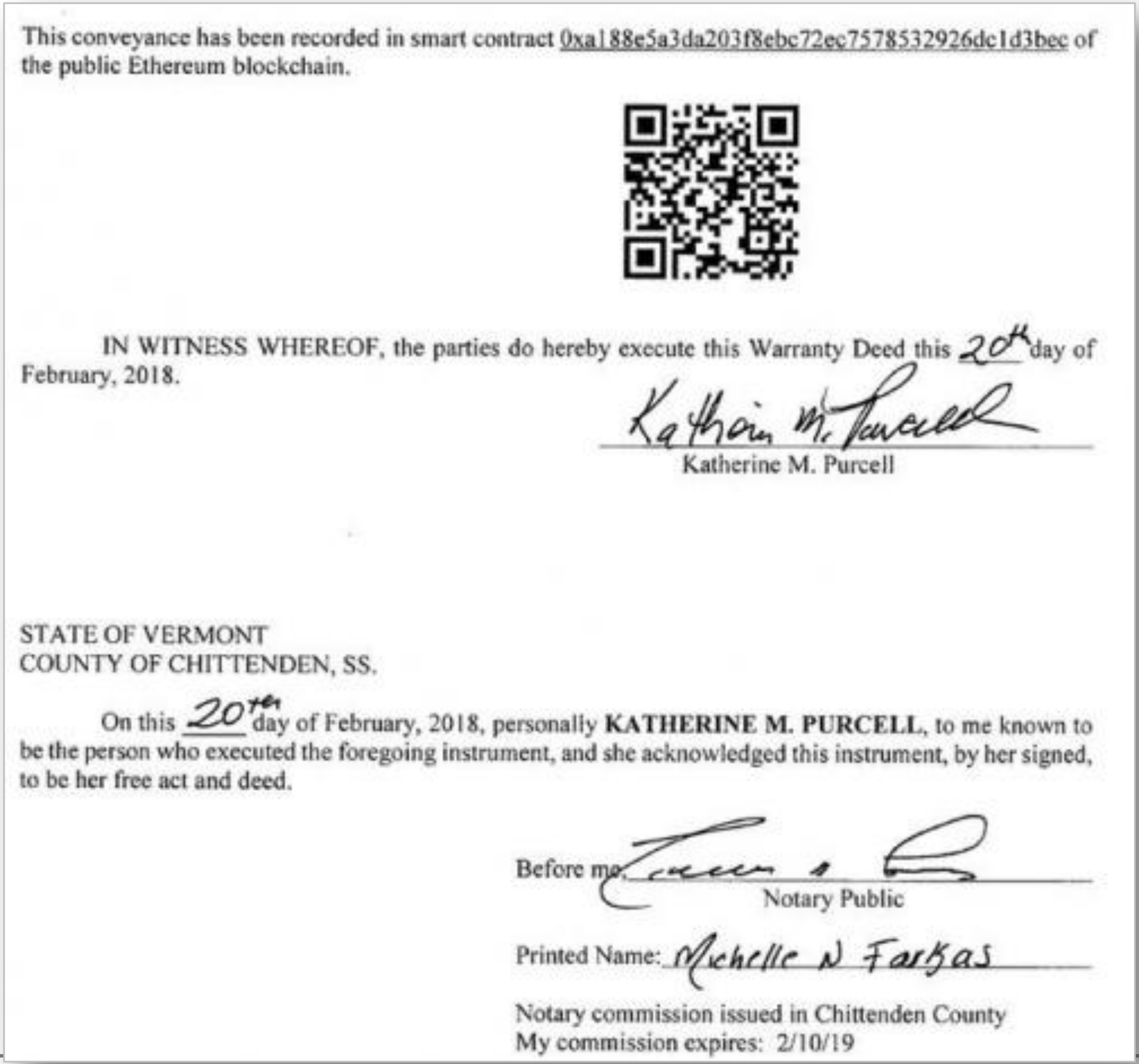
UNCLASSIFIED

19

More Blockchain in Government

DoD	Secure data files for Additive Manufacturing (3D printing) of parts
CDC	Attributable, distributed information dissemination
FDA	EMR replacement
GSA	“…automate the FASt Lane process for IT Schedule 70 contracts.”
DHS	Exploratory (air travel, international trade, anti-money laundering)
Treasury	Asset management
Illinois Blockchain Initiative	“Give me some of that blockchain goodness”

Unofficial and definitely incomplete list



This conveyance has been recorded in smart contract 0xa188e5a3da203f8ebc72ec7578532926dc1d3bec of the public Ethereum blockchain.

IN WITNESS WHEREOF, the parties do hereby execute this Warranty Deed this 20th day of February, 2018.

Katherine M. Purcell

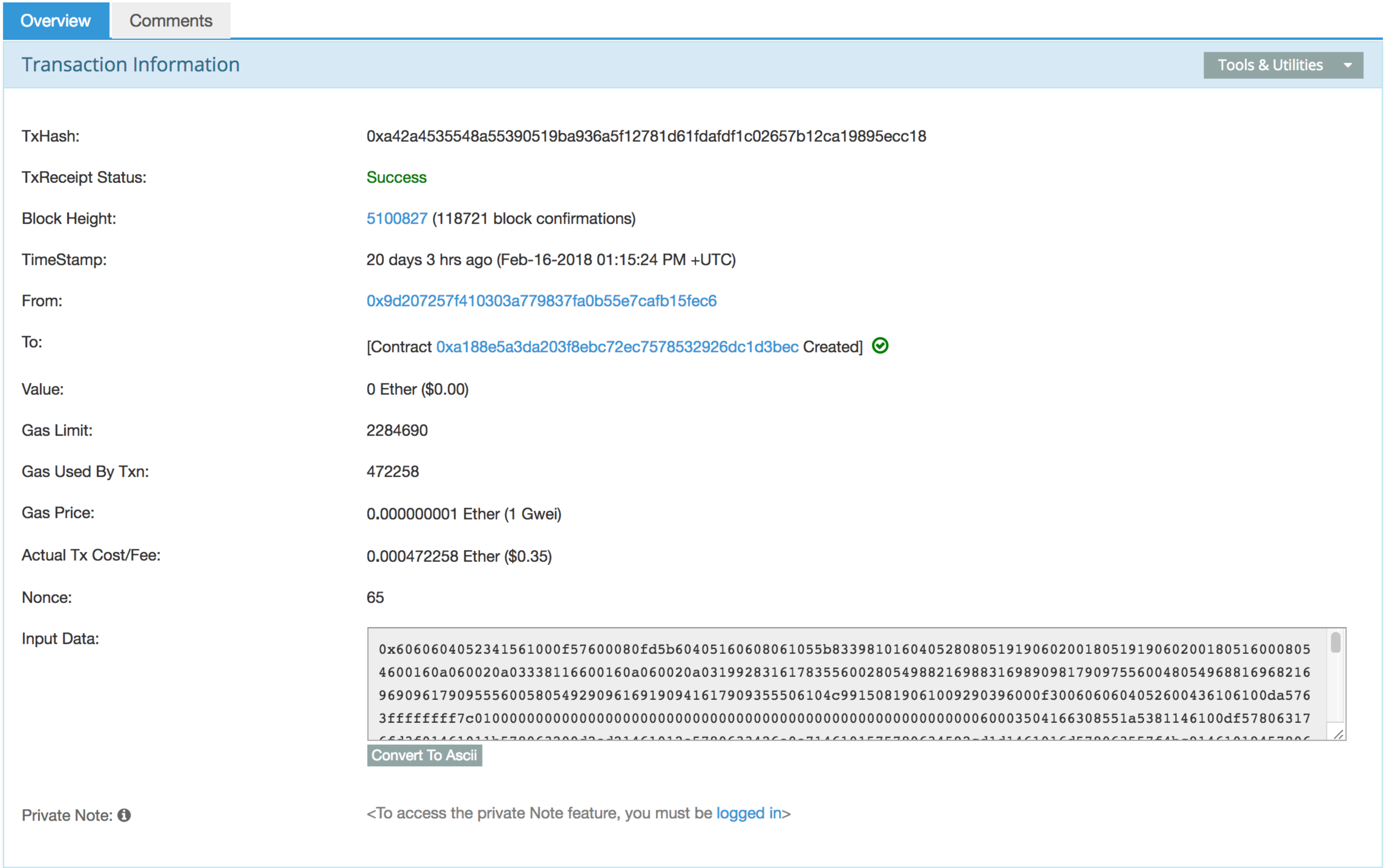
STATE OF VERMONT
COUNTY OF CHITTENDEN, SS.

On this 20th day of February, 2018, personally **KATHERINE M. PURCELL**, to me known to be the person who executed the foregoing instrument, and she acknowledged this instrument, by her signed, to be her free act and deed.

Before me, ______________
Notary Public

Printed Name: Michelle N Farkas

Notary commission issued in Chittenden County
My commission expires: 2/10/19



Transaction Information

TxHash:	0xa42a4535548a55390519ba936a5f12781d61fdafdf1c02657b12ca19895ecc18
TxReceipt Status:	Success
Block Height:	5100827 (118721 block confirmations)
TimeStamp:	20 days 3 hrs ago (Feb-16-2018 01:15:24 PM +UTC)
From:	0x9d207257f410303a779837fa0b55e7cafb15fec6
To:	[Contract 0xa188e5a3da203f8ebc72ec7578532926dc1d3bec Created] ✓
Value:	0 Ether ($0.00)
Gas Limit:	2284690
Gas Used By Txn:	472258
Gas Price:	0.000000001 Ether (1 Gwei)
Actual Tx Cost/Fee:	0.000472258 Ether ($0.35)
Nonce:	65

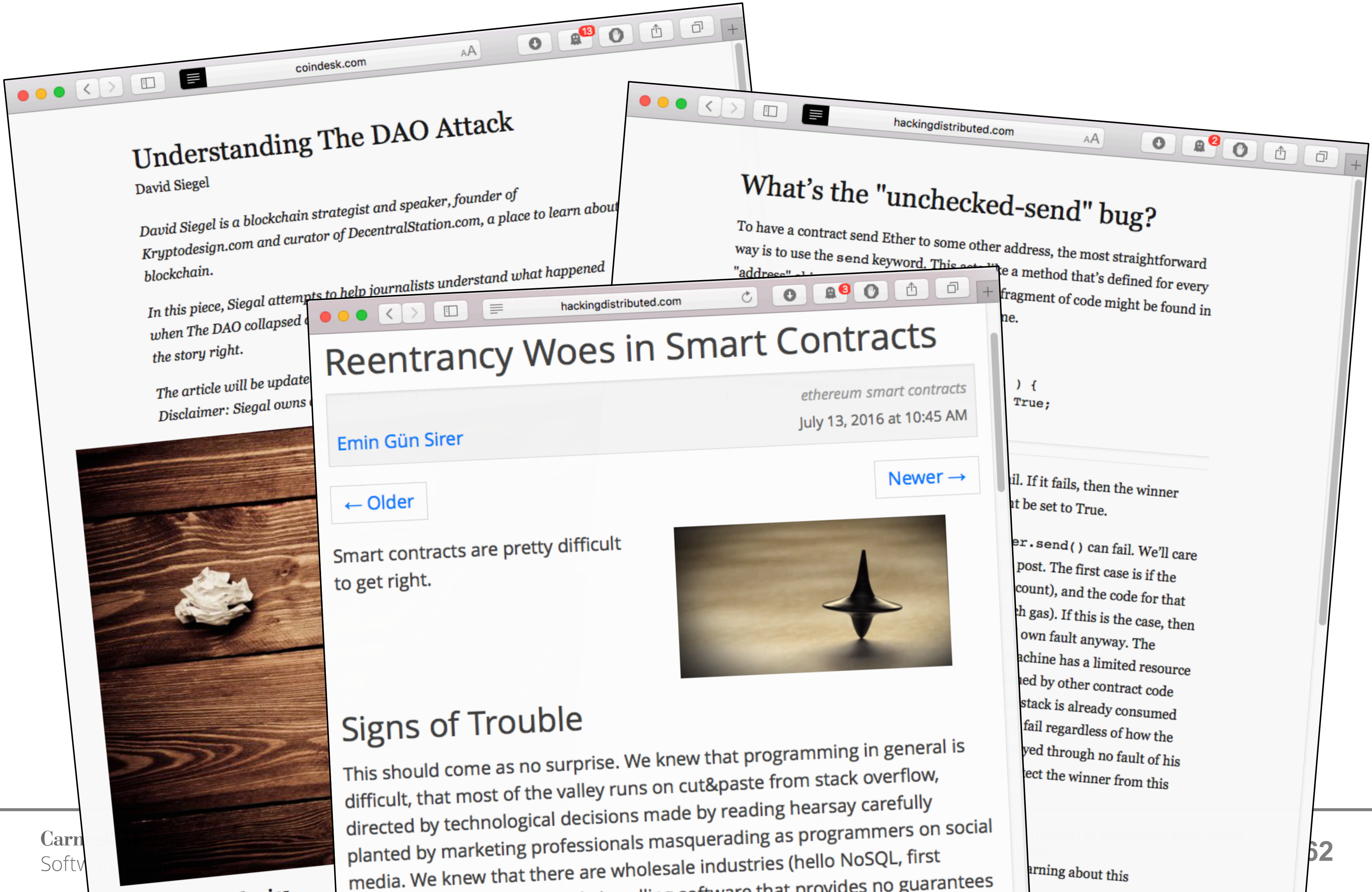
Input Data:

```
0x6060604052341561000f57600080fd5b6040516060806105 5b83398101604052808051919060200180519190602001805160008 05
```

```
0x6060604052341561000f57600080fd5b60405160608061055b833981016040528080519190602001805191906020018051600080 5
4600160a060020a03338116600160a060020a0319928316178355600280549882169883169890981790975560048054968816968216
969096179095556005805492909616919094161790935550610 4c991508190610092903960 00f3006060604052600436106100da576
3ffffffff7c0100000000000000000000000000000000000000000000000000000000600035041663085 51a5381146100df57806317
```

Private Note: ℹ <To access the private Note feature, you must be logged in>

Still in infancy!



Understanding The DAO Attack

David Siegel

David Siegel is a blockchain strategist and speaker, founder of Kryptodesign.com and curator of DecentralStation.com, a place to learn about blockchain.

In this piece, Siegal attempts to help journalists understand what happened when The DAO collapsed

the story right.

The article will be update

Disclaimer: Siegal owns

What's the "unchecked-send" bug?

To have a contract send Ether to some other address, the most straightforward way is to use the send keyword. This acts like a method that's defined for every "address"

e a method that's defined for every fragment of code might be found in ne.

```
) {
True;
```

il. If it fails, then the winner nt be set to True.

er.send() can fail. We'll care post. The first case is if the count), and the code for that h gas). If this is the case, then own fault anyway. The achine has a limited resource ed by other contract code stack is already consumed fail regardless of how the yed through no fault of his ect the winner from this

arning about this

Reentrancy Woes in Smart Contracts

ethereum smart contracts

July 13, 2016 at 10:45 AM

Emin Gün Sirer

Smart contracts are pretty difficult to get right.

Signs of Trouble

This should come as no surprise. We knew that programming in general is difficult, that most of the valley runs on cut&paste from stack overflow, directed by technological decisions made by reading hearsay carefully planted by marketing professionals masquerading as programmers on social media. We knew that there are wholesale industries (hello NoSQL, first