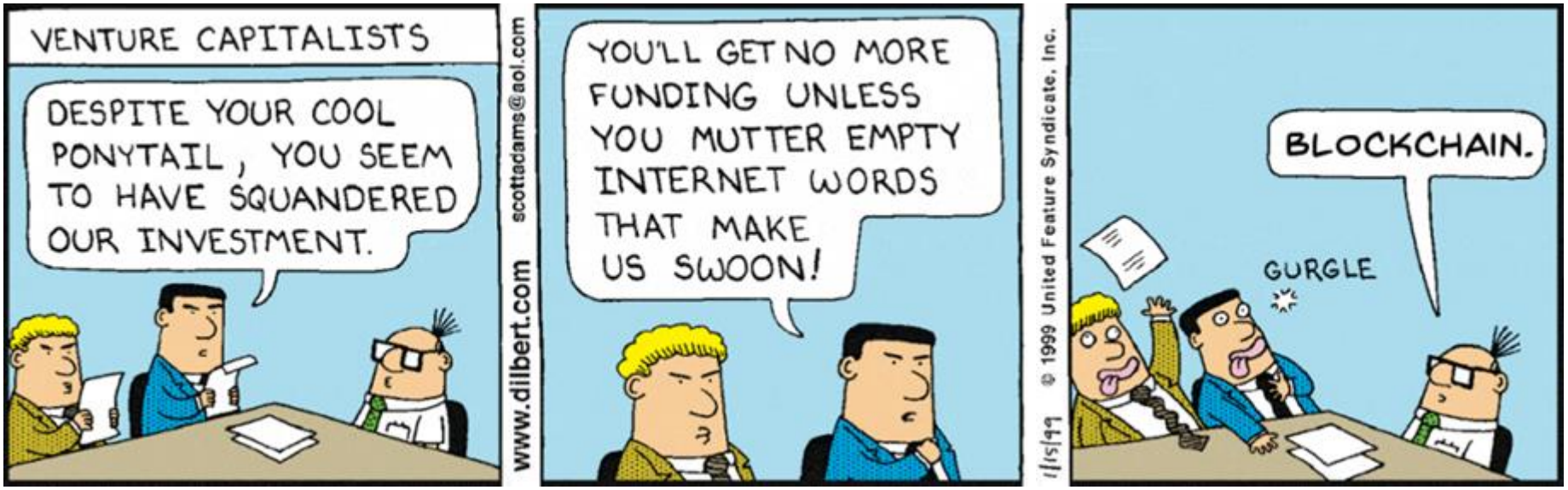
Blockchain overview

Portland State
Computer Science

Why?

- To avoid this…

- …and maybe take advantage of this? (circa 2017-2018)



MENU CNBC MARKETS BUSINESS NEWS INVESTING TECH

Salaries for blockchain engineers are skyrocketing, now on par with AI experts

- Blockchain engineers are making between $150,000 and $175,000 in annual salaries on average.
- Blockchain engineers are the top paid roles in software development, on par with specialists focused on artificial intelligence.
- Demand for blockchain engineers has increased by 400 percent since late 2017 on Hired, a firm that helps clients recruit tech candidates.

But...

- Unlike other courses…
  - Skills learned here might never be used again…

MIT Technology Review

Connectivity

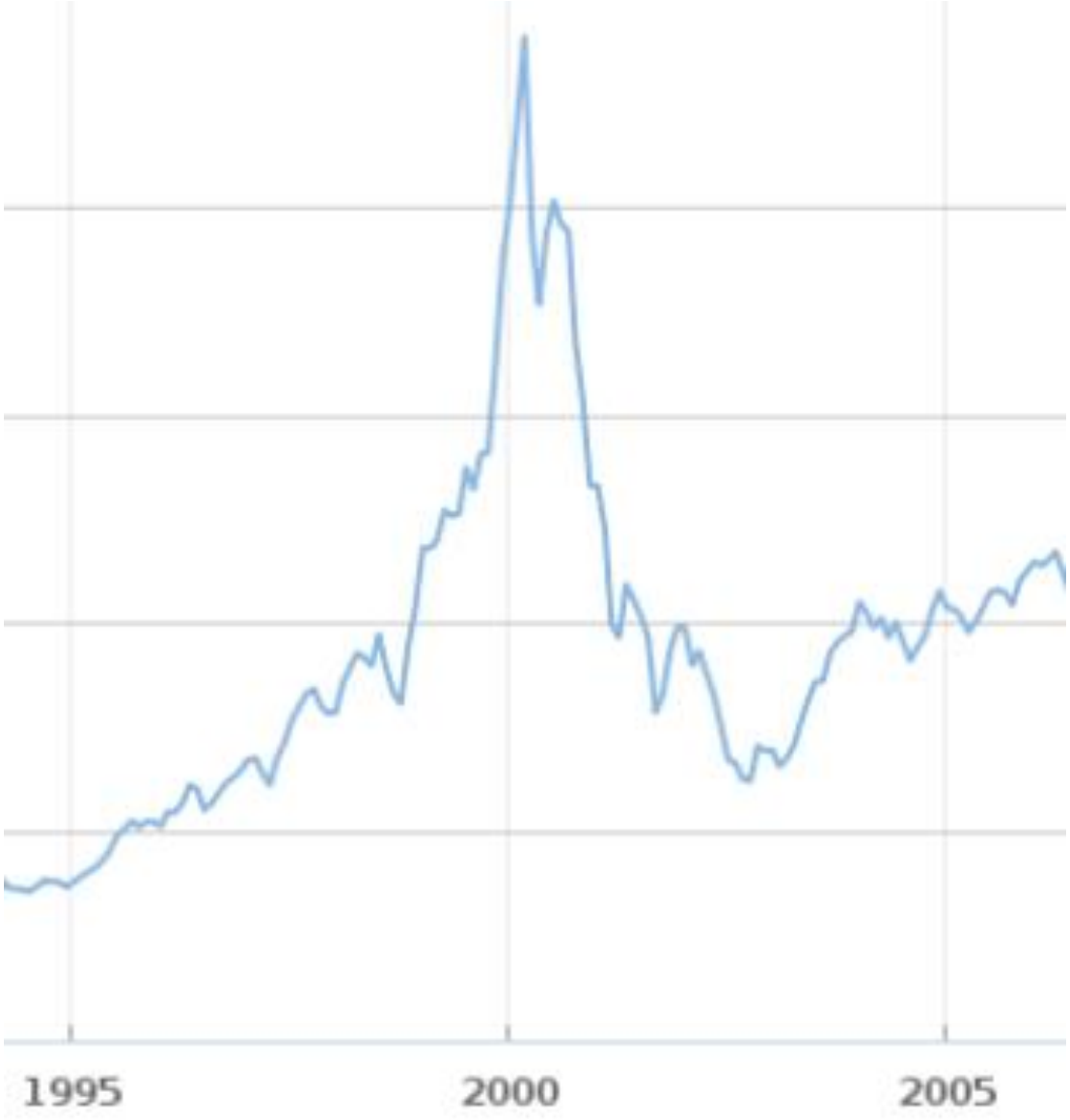
Ethereum thinks it can change the world. It's running out of time to prove it.

The blockchain system has daunting technical problems to fix. But first, its disciples need to figure out how to govern themselves.

by Mike Orcutt December 13, 2018

  - Might be applicable elsewhere (hopefully)

Play the long game?



Blockchain abstraction

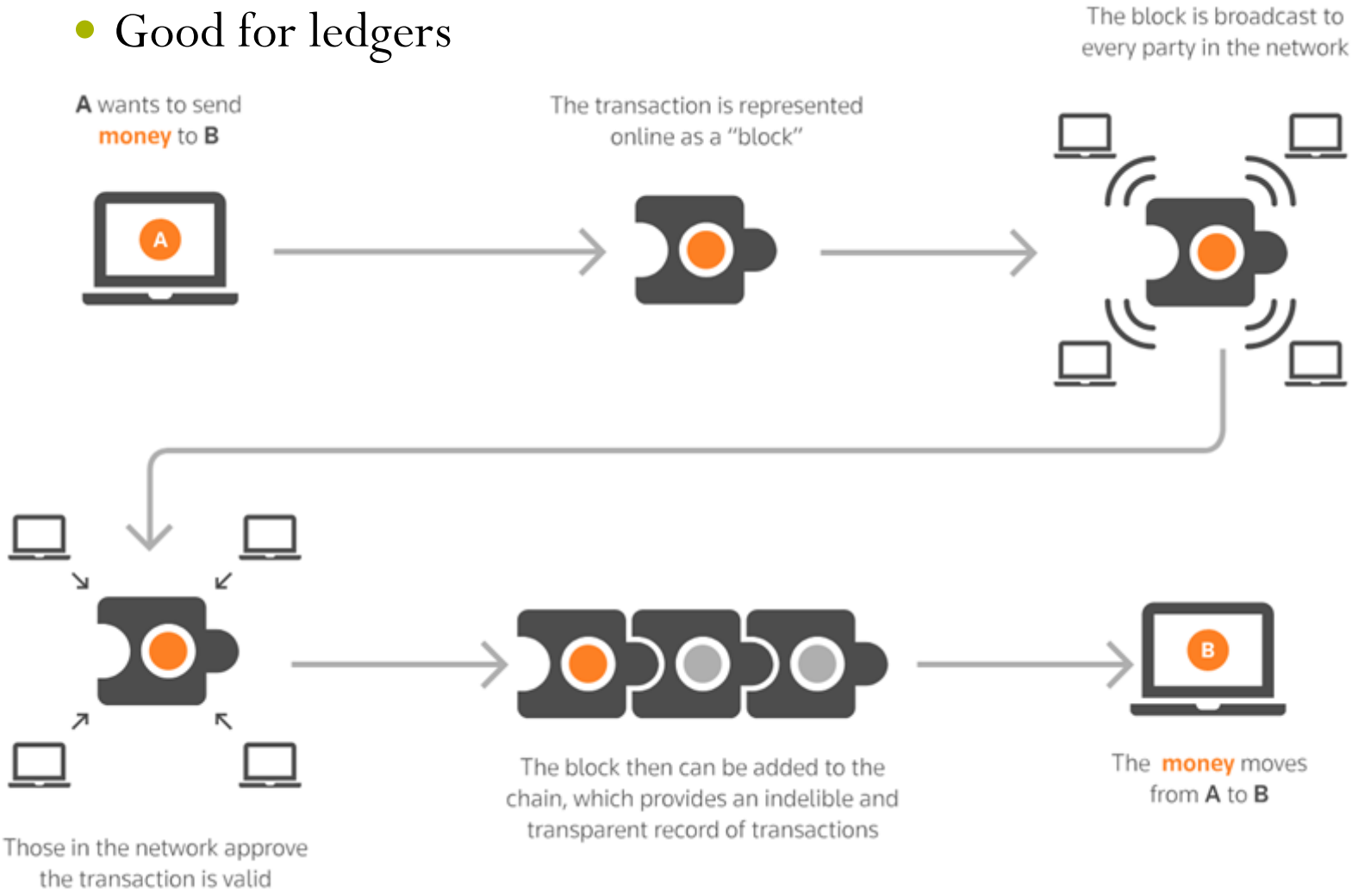
- Definition #1
  - A shared database stored in multiple copies on computers throughout the world
  - Potentially maintained without the need for a central authority (e.g. a bank, a government, Google, etc.)
- Definition #2
  - Replicated and consistent, immutable, append-only data storage system resistant to tampering
- Definition #3
  - A write-only, decentralized, state machine that is maintained by mutually untrusting actors, secured by economic incentive
    - Cannot delete data
    - Cannot be shut down or censored
    - Supports defined operations agreed upon by participants
    - Participants may not know each other (public permission-less blockshains)
    - In actors' best interests to play by the rules

How?

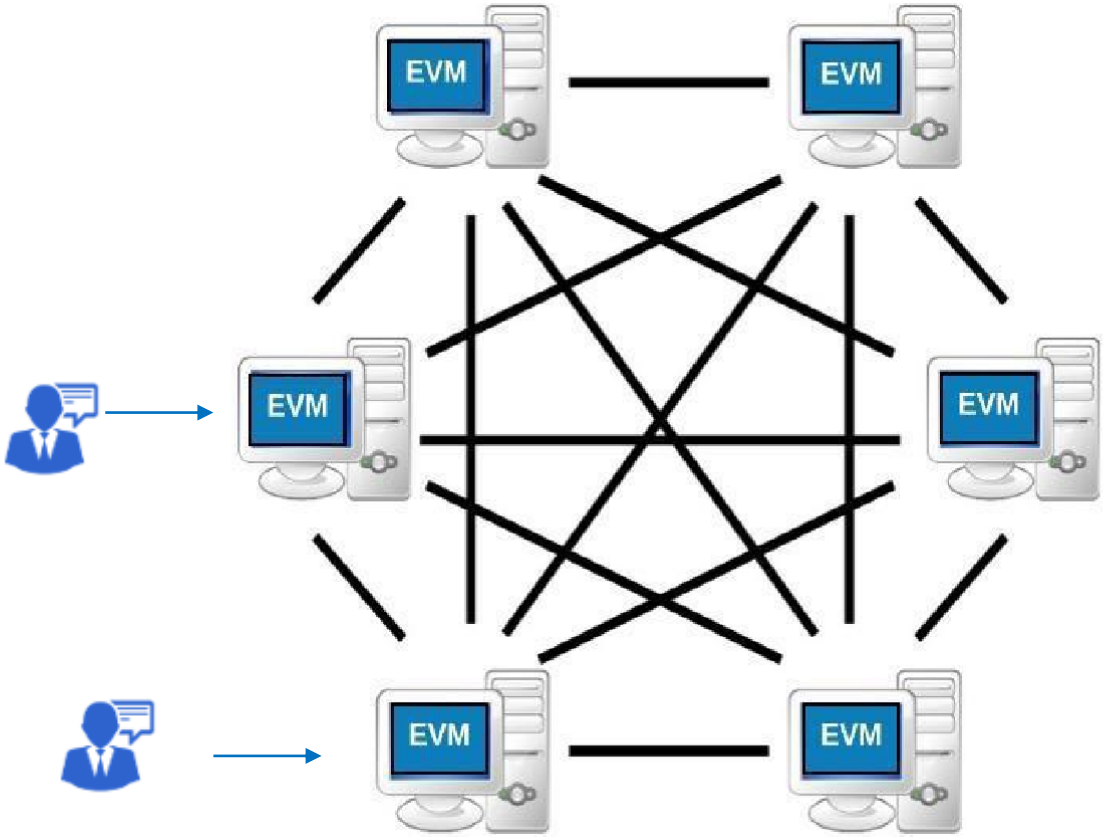
- Digital signatures (e.g. public-key cryptography)
  - Provides authentication
- Cryptographic hash functions (e.g hash chains of data transactions)
  - Provides tamper-resistant immutability
- Replication (e.g. full copies stored everywhere)
  - Provides availability and censorship resistance
- Distributed consensus amongst mutually trusting or distrusting replicas
  - Provides integrity and decentralized control

Kinds of blockchains #1

- Transaction log (Bitcoin)
  - Limited computational functionality
  - Good for ledgers



- Turing-complete (Ethereum)
  - Treats blockchain and its nodes as a single, global, replicated, consistent computer
  - Entire state machine, its code, its input/output, and its history executed and replicated in a consistent manner



Kinds of blockchains #2

- Permissionless
  - No permission to join
  - Everyone allowed to use
  - Everyone untrusted and potentially malicious
  - No central authority* (-ish)
  - Bitcoin, Ethereum
- Permissioned
  - Only selected and authenticated users can participate (via consortium or central authority)
  - Support information sharing and immutability as in permissionless
  - But also data privacy
    - Transactions visible only to authorized parties

Why not...

- Regular databases?
- Distributed databases like Cloud Spanner, Amazon Aurora?
- Hosted data warehouses like BigQuery, Amazon Athena?
- Append-only (ledger) databases? (AWS QLDB)
- git repositories?
- Internet time machine?

An easier solution might exist...

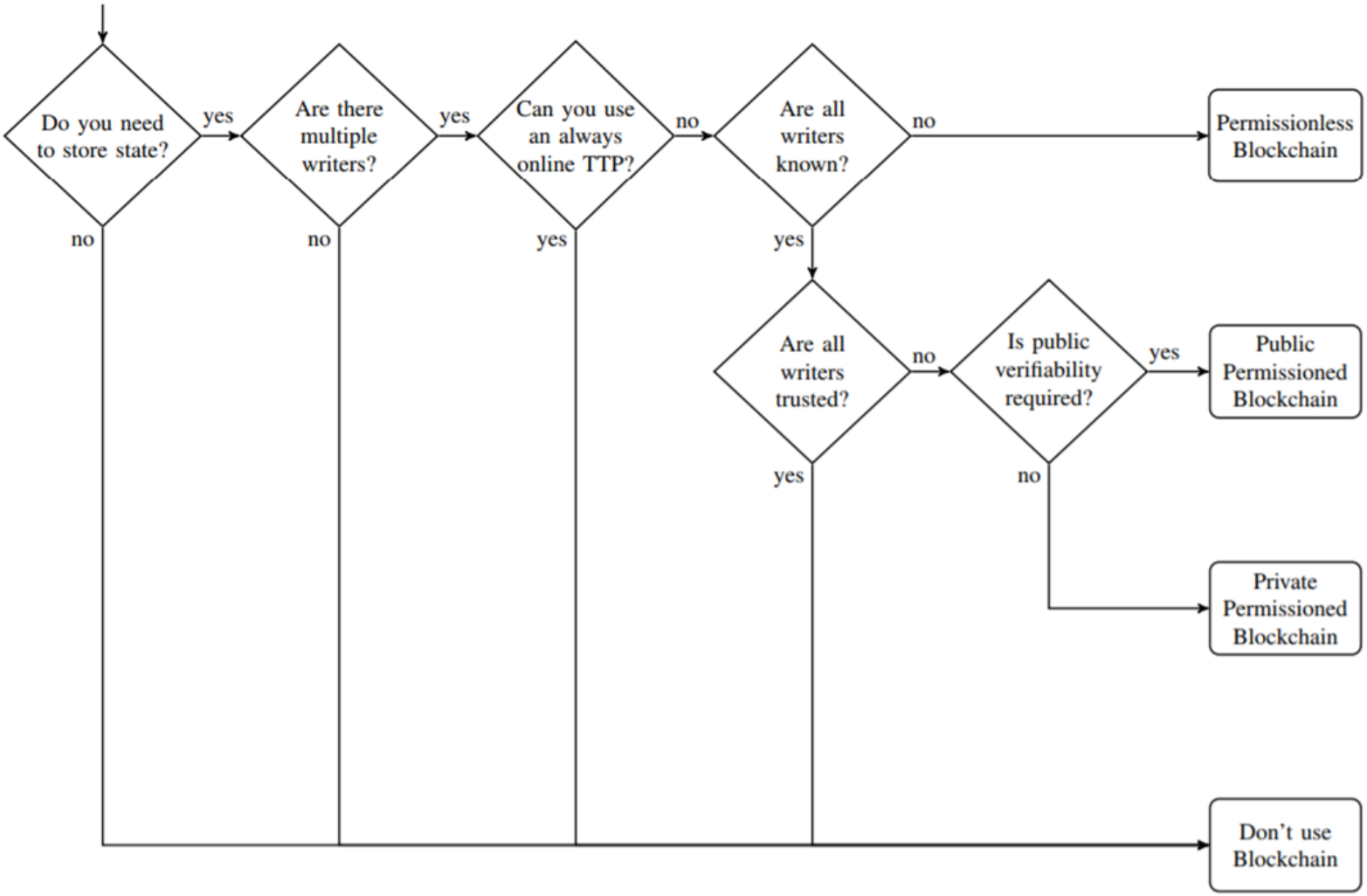
- If all parties are *known* and *trusted*, DO NOT use a blockchain
  - Use any number of databases
  - Many proposed uses of blockchains for business applications fall in this category!
- If all parties are *known* and *trusted*, but you also need *immutability* DO NOT use a blockchain
  - Use databases augmented with cryptographic hash-chains (e.g. AWS QLDB, Kafka)

But...

- If all parties are *known* but *untrusted*
  - Then, if public verification needed?
    - Use a Public Permissioned Blockchain
  - Otherwise
    - Use a Private Permissioned Blockchain
- If you *need to store a state* and there are *multiple, anonymous* writers and they *cannot agree* on an *online trusted third-party*,
  - Use a **permissionless** Blockchain (e.g. Bitcoin and Ethereum)

From this week's reading

- Do you need a Blockchain?
  - https://eprint.iacr.org/2017/375.pdf

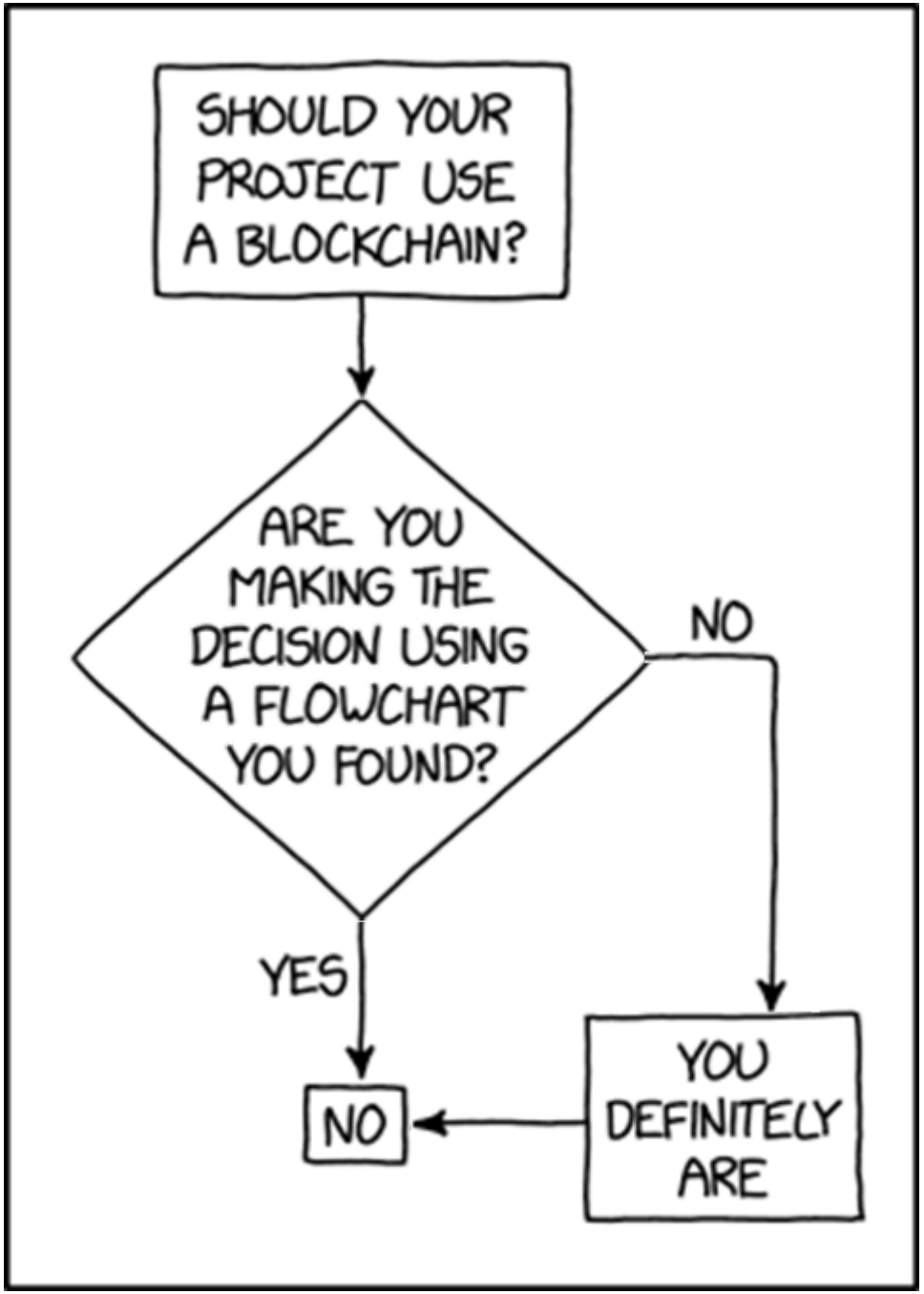


Other considerations

- Not good if all you need is a signature
  - Statement authenticity guarantee application
    - e.g. certificate of completions
  - Can be solved by digital signatures alone
    - Unless…Blockchain being used as a reliable timestamping method
    - Hash committed to a block with a known timestamp
- Not good if you still need a regulatory piece
  - Land registry
    - Must have regulatory agencies with authority to modify ownership
    - Centralized authority can not be removed
      - Use distributed database managed by agency instead
  - ICOs
    - Holding a startup accountable to its investors
    - Need a regulatory mechanism to keep companies from taking $ and running

Or for the cynical...

- https://xkcd.com/2267/



Applications

Portland State
Computer Science

Targets for Blockchain

- Applications that require shared common, append-only database with limited capacity
- Applications with multiple participants with varying degrees of trust amongst them
- Applications that must run in a distributed manner
- Applications that require a settlement process with a trusted third party
- Applications needing integrity, authentication, and non-repudiation
- Applications governed by precise rules that do not change and are simple to encode
- Applications requiring transparency (as opposed to privacy)

Currency

- Alternative to fiat currencies (Bitcoin)
  - Fiat currencies decouple supply from a physical good (i.e. gold)
  - Blockchain systems typically tie supply to a bounded, virtual good (e.g. cryptographic collisions)
  - Blockchain implementation records and verifies transfers of currency
  - Breaks status-quo where
    - Only government issues money, defines issuing procedures
    - Central authorities (banks) decide which transactions are valid and which are not
      - Main reason why criminals use it

Loans and finance

- Lending bank, borrower's bank and the loan applicant see transparent processing of loans
  - Strong identity and consensus of blockchain reduces fraud
  - Use of blockchain reduces time over manually processing and issuing a loan.
- Twiga Foods and IBM microfinancing
  - Pilot of 220 small food kiosks across Kenya.
  - 220 loans with the average loan around $30 (3,020 KES)
  - Loan duration four and eight days with an interest rate of one and two percent, respectively.
  - Increased the order size by 30 percent and profits for each retailer, on average, by six percent.

Currency transfers (e.g. real $ xfer)

- International bank transfers
  - Sending money to friend overseas can involve a third bank unless your two banks have a direct agreement
  - Many hops and long transaction times.
- Solved via distributed ledger in which only banks are writers (Permissioned Blockchain)
  - Transactions happen only between the bank and the ledger
  - Currency can be homogenous for a single network

- Recent example (1/2019)

U.S. LEGAL NEWS JANUARY 14, 2019 / 9:41 AM / UPDATED 5 HOURS AGO

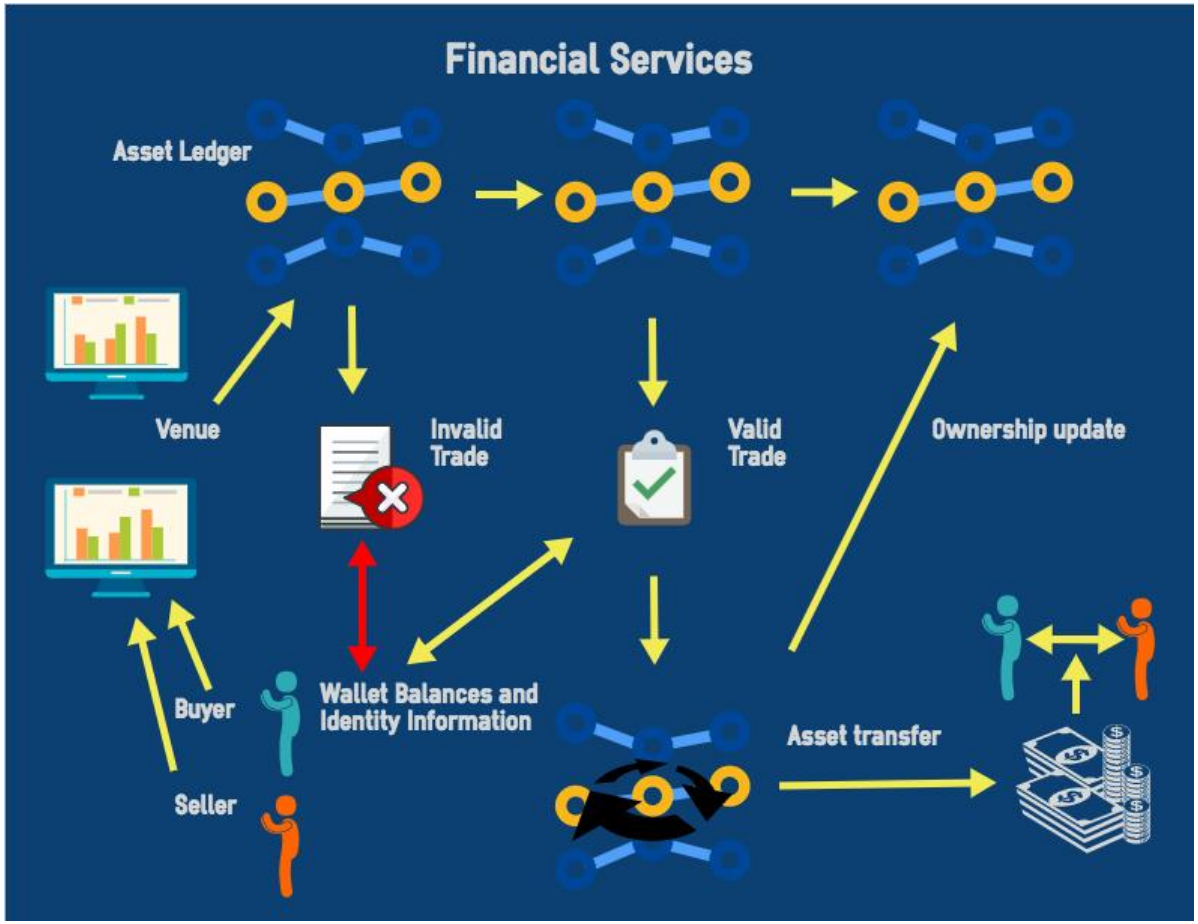
HSBC settles FX deals worth $250 billion on blockchain in last year

Blockchain is a shared database that can process and settle transactions in minutes. Originally conceived to underpin the cryptocurrency bitcoin, the technology does not require third-parties for checks and its entries cannot be changed, making it highly secure.

Banks and other financial firms have invested hundreds of millions of dollars in the technology, hoping it will simplify and slash costs in processes from settlements to payments.

Asset transfers

- Similar to currency transfers
- Stock ownership and trading



- Real-estate, fine art, equity, investment funds

Harbor raises $28M to bring blockchain to real estate, fine art

By | April 17, 2018 | No Comments

- Deeds to property put on blockchain to provide public verification
- Provides a safer way to transact with property owners
  - Buyer can directly check for ownership!

Intellectual Property ownership

- Digital content owner hashes content together with their identity and commits to the blockchain.
  - If nobody else can prove they published it prior to that commitment, this is evidence that they own it.
  - More convenient than a patent office and allows for you to not have to disclose details of the digital object.

Provenance and supply-chain

- Auditing to track provenance and chain of custody for materials and products
  - Conflict diamonds (e.g. blood diamonds) that fund civil war

COMMERCE

IBM will use blockchain to verify diamond and gold jewelry authenticity

DEAN TAKAHASHI @DEANTAK APRIL 26, 2018 3:00 AM

IBM said the TrustChain Initiative will use blockchain to trace the provenance of finished pieces of jewelry and provide increased transparency across the supply chain.

- Retail goods

IBM Crypto-anchors and blockchain will save up to $600 billion per year from fraud

brian wang | March 19, 2018 2 comments

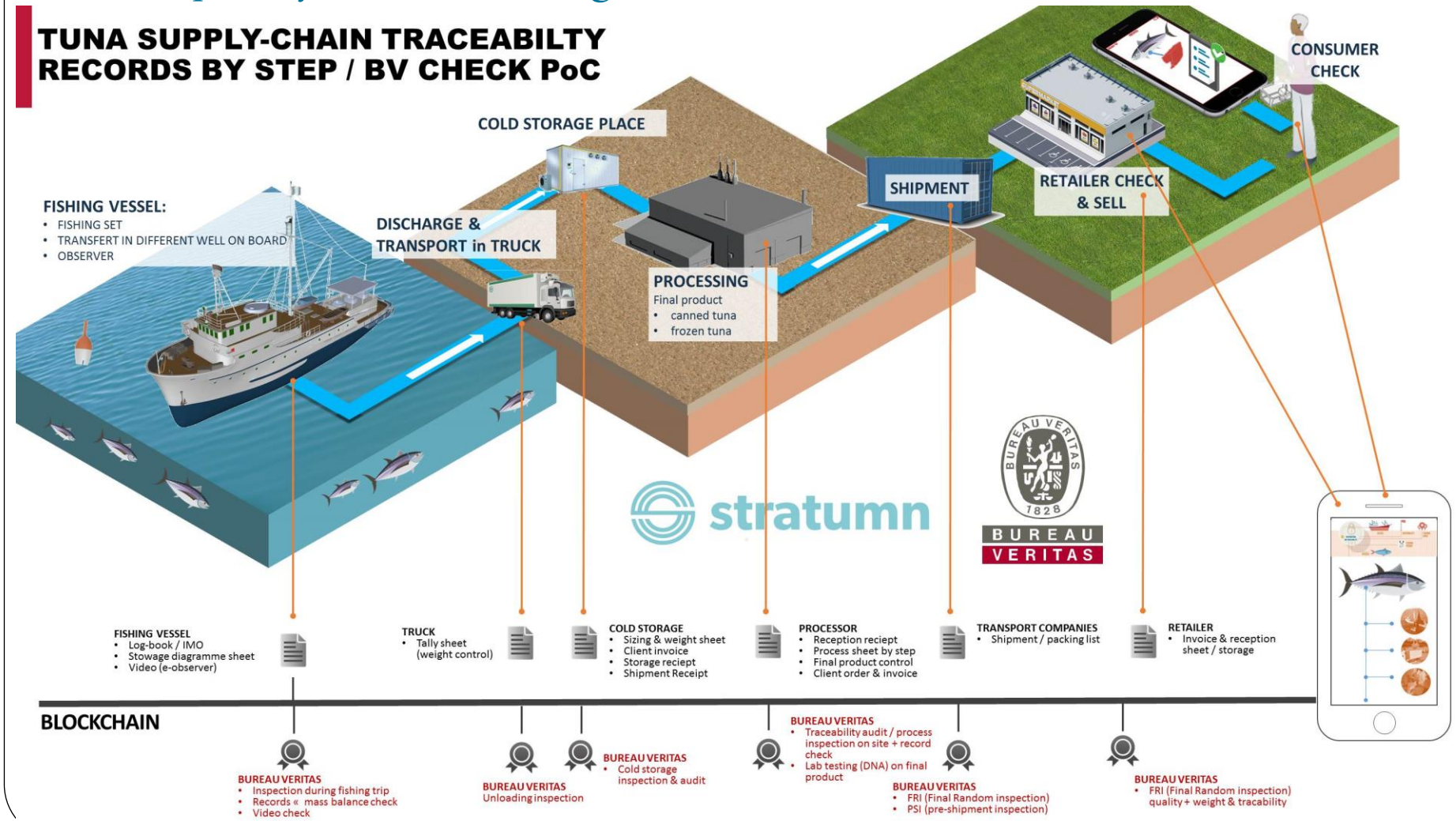
06.03.16

How Sneaker Designers Are Busting Knock-Offs With Bitcoin Tech

Shoe counterfeiters are notoriously difficult to stop, but an unlikely solution is emerging–and it's inspired by cryptocurrencies.

- Fishing
  - Restaurants can view and verify chain of custody for fish
  - Sensors attached to fish can log location/temperature/humidity

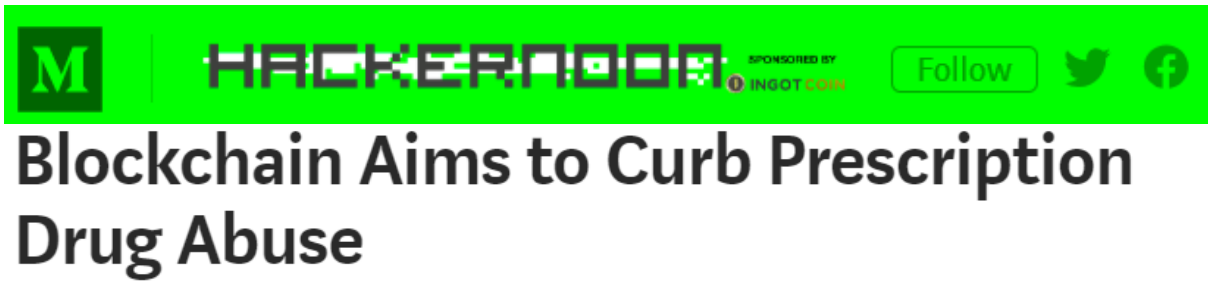
https://youtu.be/Buw3g8oNG74



Healthcare

- Transparent medical claims processing
  - Enable insurance providers to audit care providers and claims to remove fraud (e.g. multiple claims for same procedure)

- Prescription drug fulfillment to prevent "doctor shopping", audit individual doctors, detect prescription drug abuse



- Tamper-resistant storage of medical records

Censorship circumvention

- COVID-19 censorship (3/2020)

6,512 views | Mar 31, 2020, 08:46pm EDT

Chinese Netizens Use Ethereum To Avoid China's COVID-19 Censorship

Roger Huang Contributor ⓘ

Crypto & Blockchain

I write about the social impact of blockchains.

- Irony?

- Example: Bitcoin ransom (2019)
  - Group attempting to get paid to release damaging papers
  - Payment mileposts in BTC determine which documents are released
  - Banned from mainstream social media platforms
  - Messaging via Steemit to prevent censorship (must block entire blockchain)

EDITOR'S PICKS JANUARY 04, 2019 19:28 EST

Bitcoin Ransom: Hacker Group Releases Layer 1 Of "Damaging" 9/11 Papers

Twitter has suspended their account. They moved to Steemit, a blockchain-based censorship-resistant social media platform. Since their initial announcement, they have received more than 3 bitcoins from the public. The first "level" and a few "checkpoints" are now publicly available.

steemit beta

How does Steemit work?

Steemit.com is one of the many websites (including Busy.org, DTube, and Utopian.io) that are powered by the Steem blockchain and STEEM cryptocurrency. All of these websites read and write content to the Steem blockchain, which stores the content in an immutable blockchain ledger, and rewards users for their contributions with digital tokens called STEEM.

National ID systems, elections

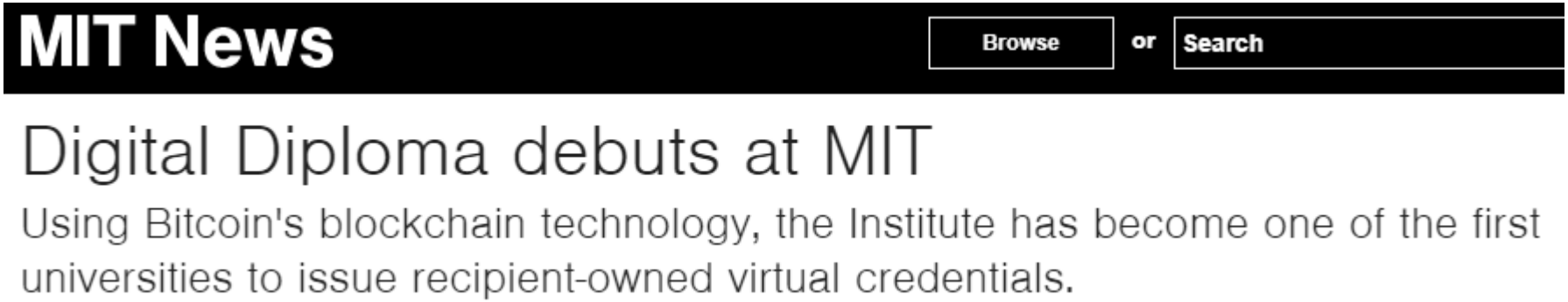
- Voting logs, travel documents, and citizenship records
  - Absentee voting for overseas military

By Aaron Wood NOV 17, 2018

West Virginia Secretary of State Reports Successful Blockchain Voting in 2018 Midterm Elections

Certificates

- Recording certifications, licenses, degrees (e.g. AWS certs)



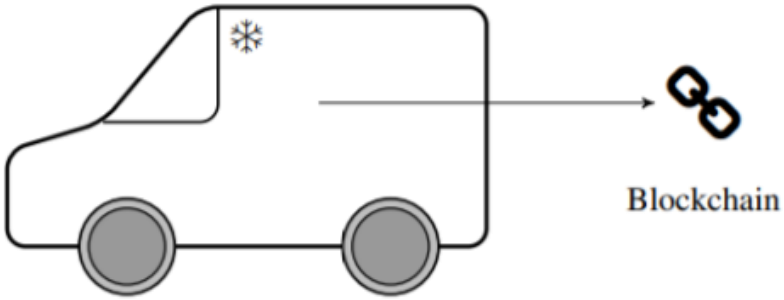
Naming services

- Trustless DNS
  - string:value mappings without a central authority (e.g. ICANN)

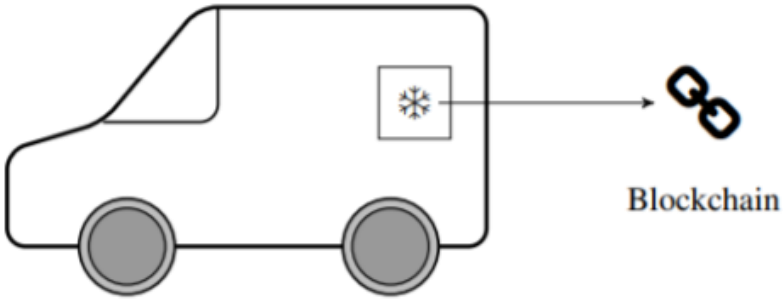
'aardvark.eth' instead of **'0x4cbe58c50480...'**

But..no substitute for security

- Garbage-in, garbage-out



(a) Intended Scenario: The supply truck is refrigerated.



(b) Attack Scenario: The trusted sensor is in a cooled compartment, while the rest of the truck is unrefrigerated.

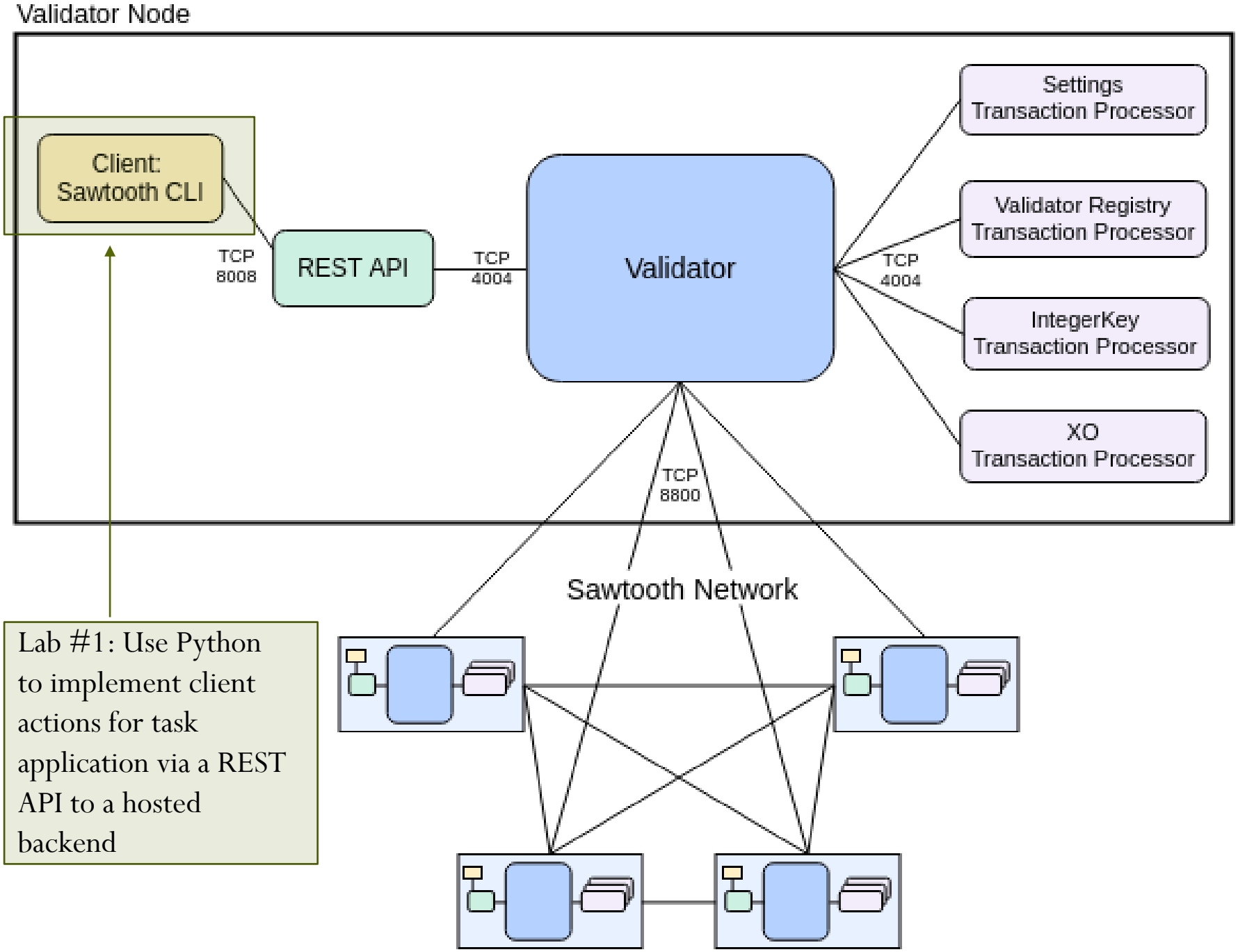
  - Expensive wine bottle emptied of contents and refilled with cheap wine – still tracked in the supply chain

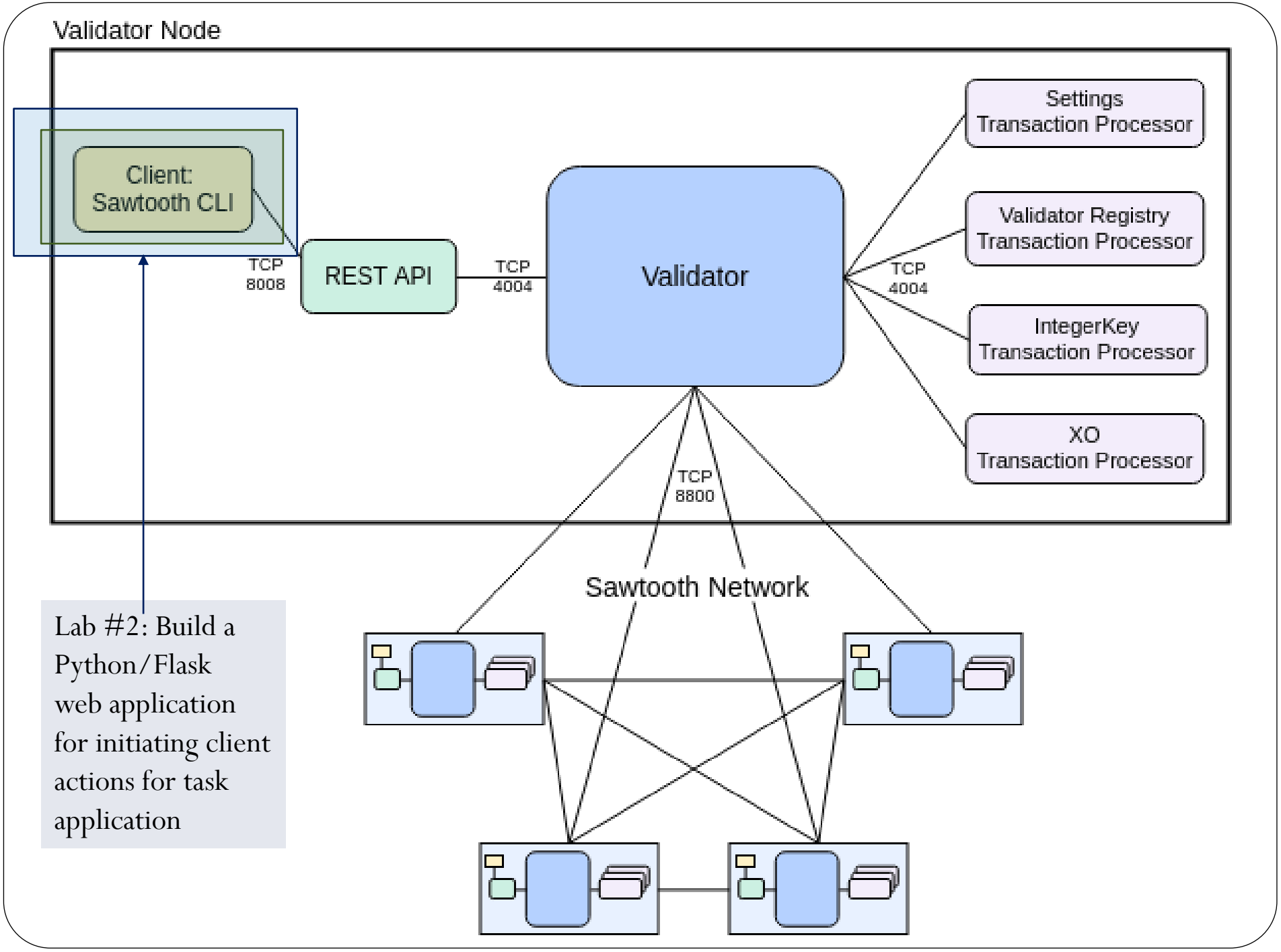
Hyperledger Sawtooth Python Labs

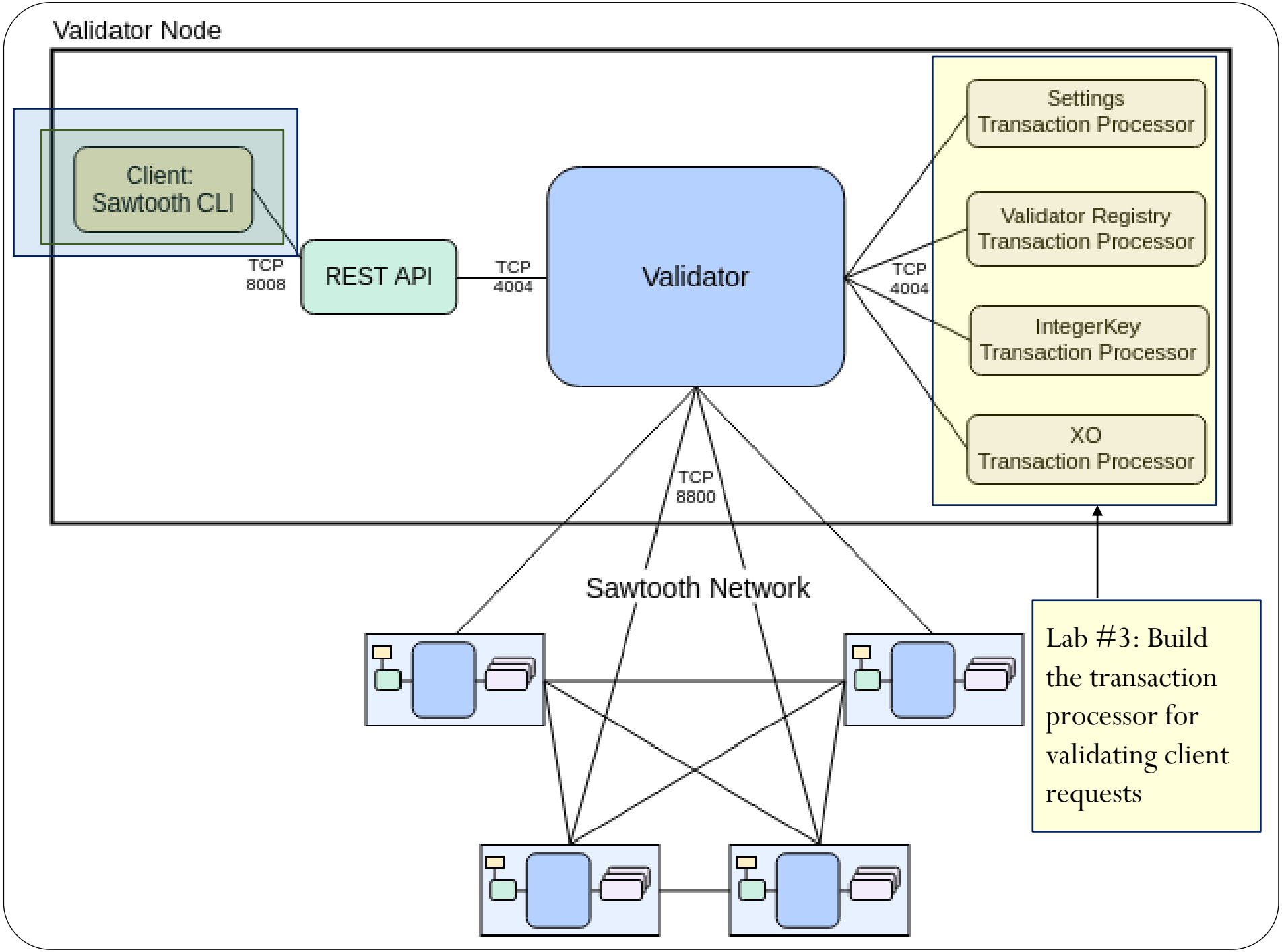
Labs 1.1-1.4

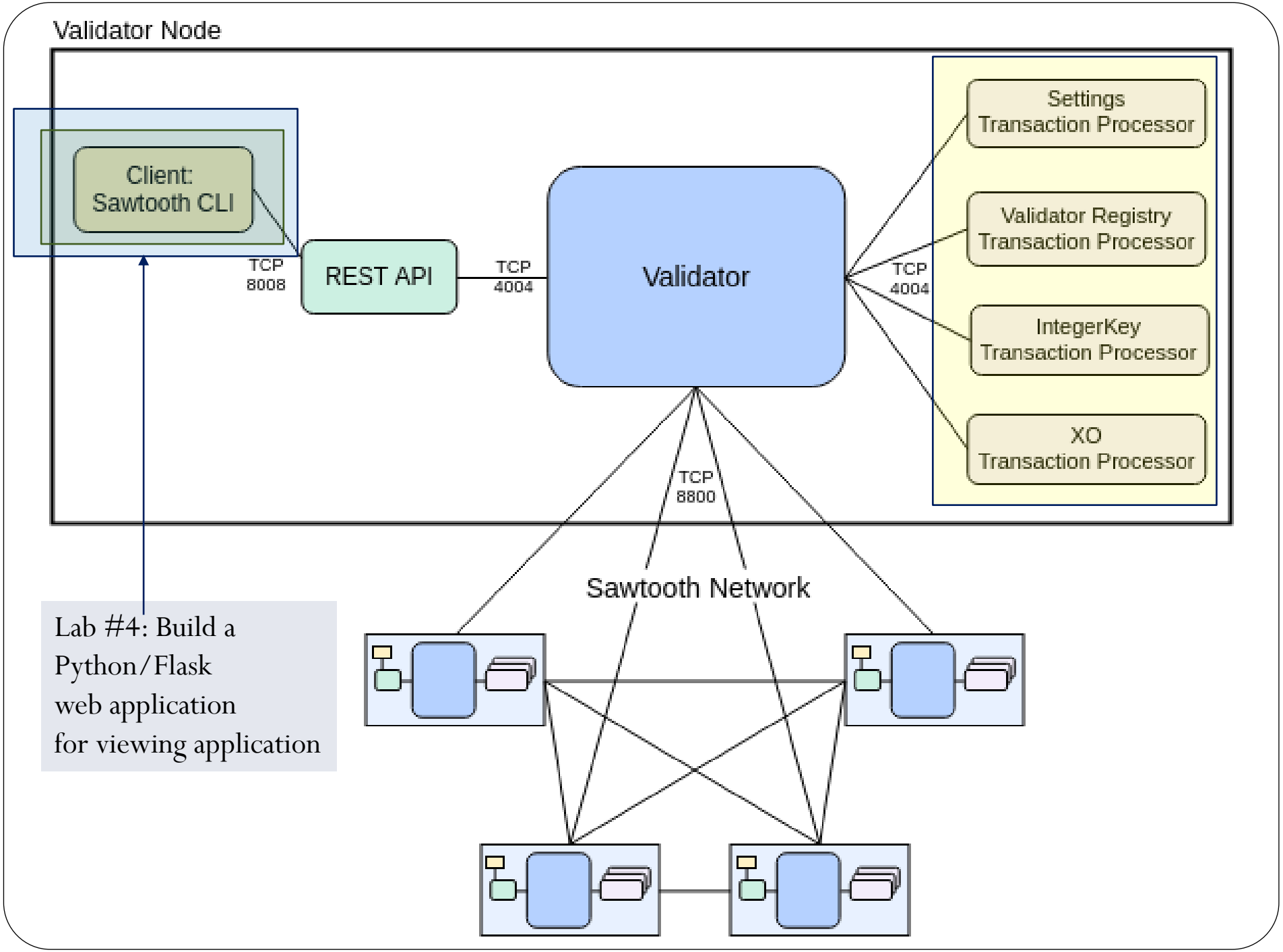
Application

- Create the frontend and backend implementations of a task-list application on a popular permissioned blockchain framework
- Task list (e.g. Trello)
  - Create project
  - Create task
  - Add authorized users/contributors
  - Edit task
  - Progress task
- Write to Sawtooth APIs to construct application on top of its blockchain implementation
  - Note: For steps of the codelab requiring code, a corresponding commit to git repository should be included upon completion of step


Validator Node
Client:
Sawtooth CLI
TCP
8008
REST API
TCP
4004
Validator
TCP
4004
Settings
Transaction Processor
Validator Registry
Transaction Processor
IntegerKey
Transaction Processor
XO
Transaction Processor
TCP
8800
Sawtooth Network
Lab #1: Use Python to implement client actions for task application via a REST API to a hosted backend


Validator Node
Client:
Sawtooth CLI
TCP
8008
REST API
TCP
4004
Validator
TCP
4004
Settings
Transaction Processor
Validator Registry
Transaction Processor
IntegerKey
Transaction Processor
XO
Transaction Processor
TCP
8800
Sawtooth Network
Lab #2: Build a Python/Flask web application for initiating client actions for task application


Validator Node
Client:
Sawtooth CLI
TCP
8008
REST API
TCP
4004
Validator
TCP
4004
Settings
Transaction Processor
Validator Registry
Transaction Processor
IntegerKey
Transaction Processor
XO
Transaction Processor
TCP
8800
Sawtooth Network
Lab #3: Build the transaction processor for validating client requests


Validator Node
Client:
Sawtooth CLI
TCP
8008
REST API
TCP
4004
Validator
TCP
4004
Settings
Transaction Processor
Validator Registry
Transaction Processor
IntegerKey
Transaction Processor
XO
Transaction Processor
TCP
8800
Sawtooth Network
Lab #4: Build a
Python/Flask
web application
for viewing application