# Blockchain as an event source

## The utility of bitcoin

ACT-IAC Blockchain Working Group
Friday October 27, 2023

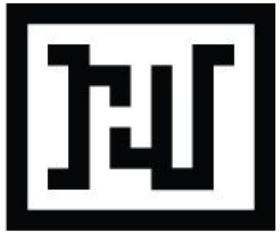
# Goals for today

- To share my **personal** experience related to using blockchains
- To share system development concepts that will impact IT organizations
- To get you thinking a bit
- To entertain you a bit
- Foster good conversations about moving adoption forward

# Hi, I’m Ryan Wold

Disclaimers:

This is a personal presentation.
Not the opinions of my clients or employer.
Does not imply endorsements.
Not financial advice.
Not legal advice.
Do your own research.
Think for yourself.



TEACHTHECONTROVERSY


Source: https://www.reddit.com/r/gpumining/comments/7xquql/felt_like_sharing_my_milk_crate_miner/


r/bitcoin
MAGIC
Internet
money
Join us

# Ethereum × Solidity

HACKED!

Ethereum × Solidity

HYPERLEDGER


HYPERLEDGER


SO EXPENSIVE 😬

# bitcoin

bit · coin

information · value


SLAPS ROOF OF CAR
PROCESSES 7 TX PER SECOND


C'mon,
do something...

# (at least) 3 flavors of bitcoin

# (at least) 3 flavors of bitcoin

**Bitcoin**
**BTC**

**Bitcoin Cash**
**BCH**

**Bitcoin SV**
**BSV**

# (at least) 3 flavors of bitcoin

**Bitcoin Core**

**1 MB blocks**

**Bitcoin Cash**

**32 MB blocks**

**Bitcoin Satoshi Vision**

**large blocks (4GB+)**

Public 👏

Scalable 👏

Blockchain 👏

# Bitcoin as a scalable public ledger

| | |
|---|---|
| Blockchain | made of immutable transactions and blocks |
| Scalable | Web-scale ~ Global scale ~ Bitcoin Scale |
| Public ledger | No cryptography required in bitcoin transactions. Auditable by many. |

Proof of Work (SHA256)

UTXO model

# Bitcoin Script

A Forth-like language that has more than 90 OP_CODES.

Could this thing be a global computer?
A Bitcoin computer?

# ESSAYS

# HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH*

LAURIE LAW
SUSAN SABETT
JERRY SOLINAS

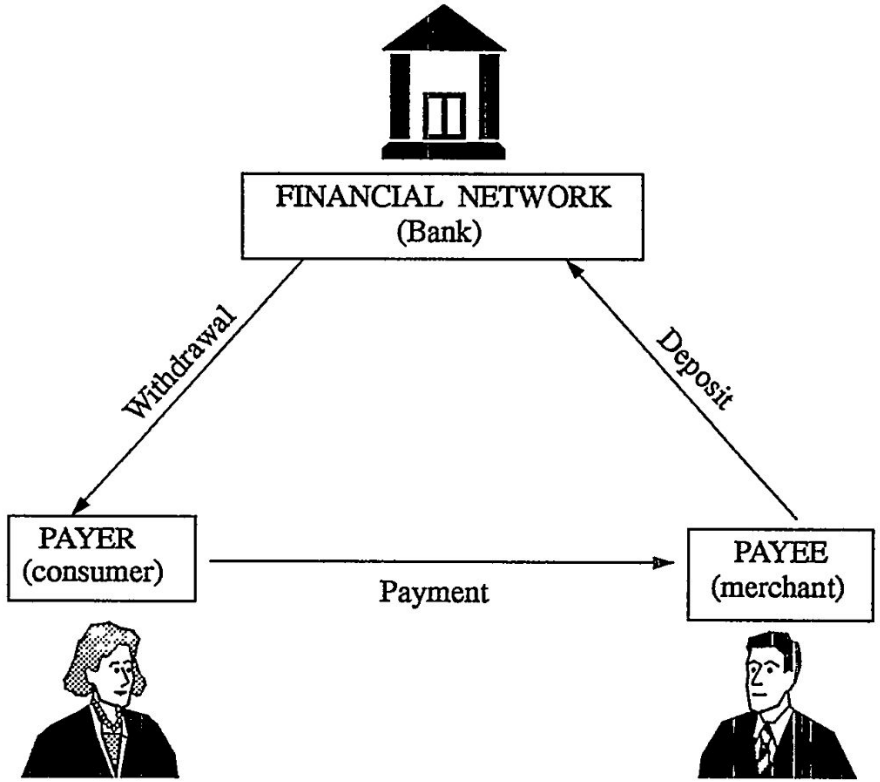


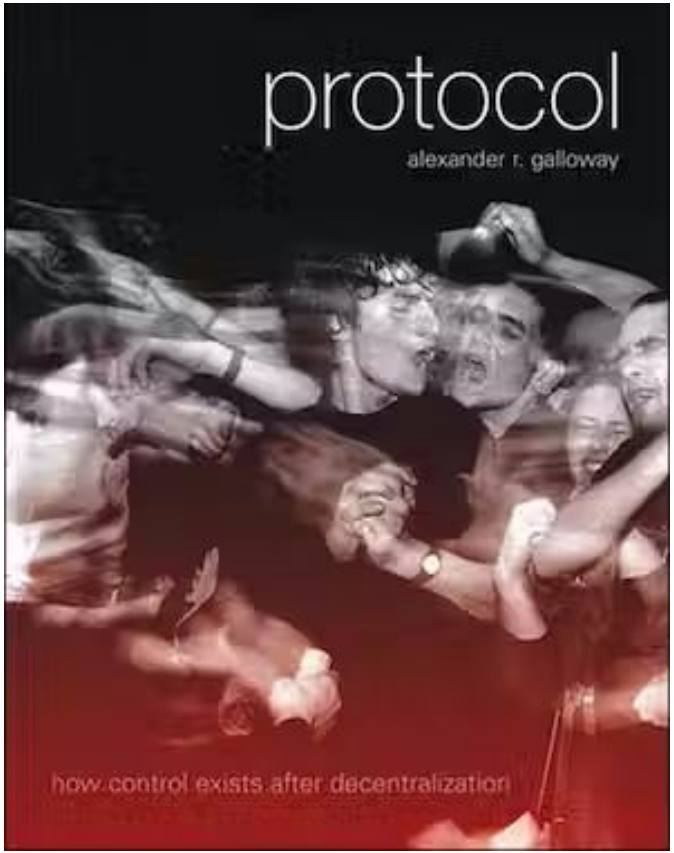

Figure 1. The three types of transactions in a basic electronic cash model.

# THE QUANTIFICATION OF INFORMATION SYSTEMS RISK

## A LOOK AT QUANTITATIVE RESPONSES TO INFORMATION SECURITY ISSUES

by

Craig S. Wright




Source: https://mitpress.mit.edu/9780262572330/protocol/

# SOFTWAR

## A Novel Theory on Power Projection and the National Strategic Significance of Bitcoin

a thesis by

**Major Jason P. Lowery**

United States Space Force
Massachusetts Institute of Technology

# Implications for enterprise adoption

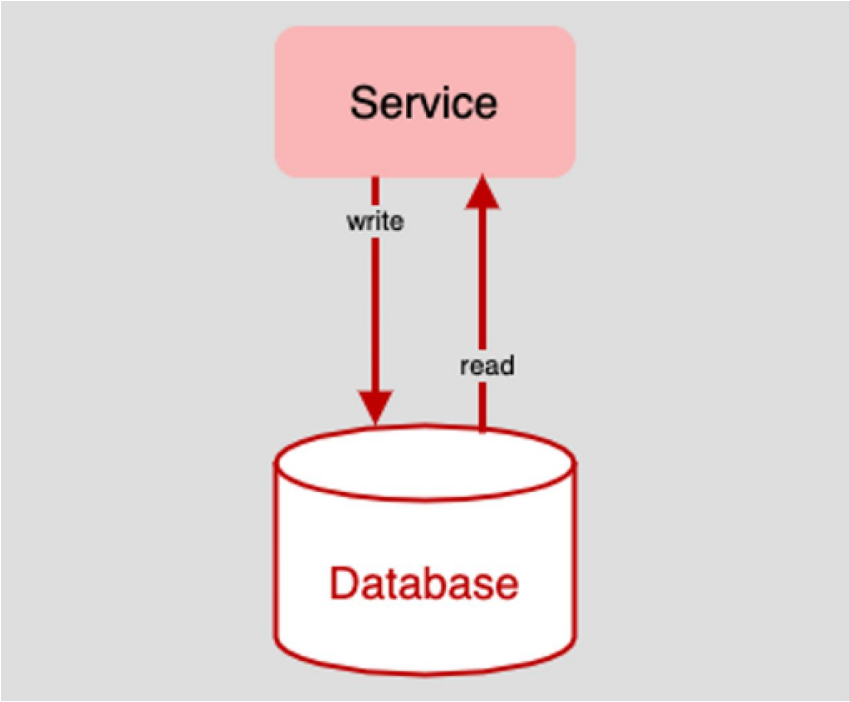
# Blockchain implications for enterprise adoption

1. CRUD apps become Event-sourced apps
2. Value moves toward interfaces and experiences atop signed data
3. Adopting wallets and supporting strong identity
4. Economic considerations for socio-technical systems

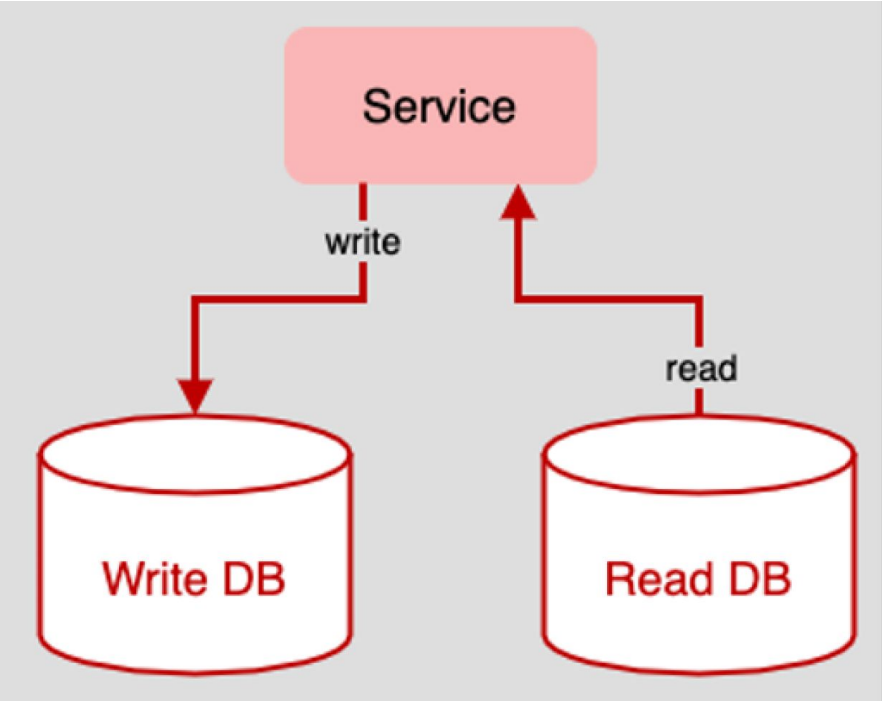
# CRUD apps become Event-sourced apps

- Blockchain acts an event-source
- A blockchain is an addition to existing infrastructure; not a replacement.
- Objects are not merely CRUD'd, but a rollup function of a stream of events
  - Think: debits and credits tallying to a current balance, as opposed to editing the balance directly
- Odds are, your application is no longer *the* source of truth, but rather, a replicated copy, or cache with a reference
- Existing applications listen to and/or post (broadcast) data to a blockchain

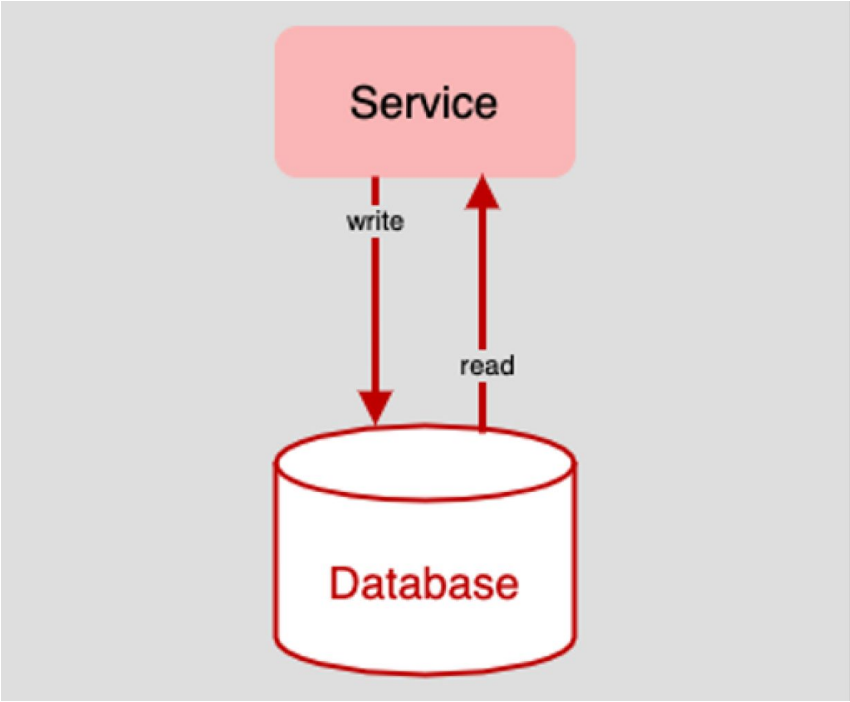
**Today:** CRUD



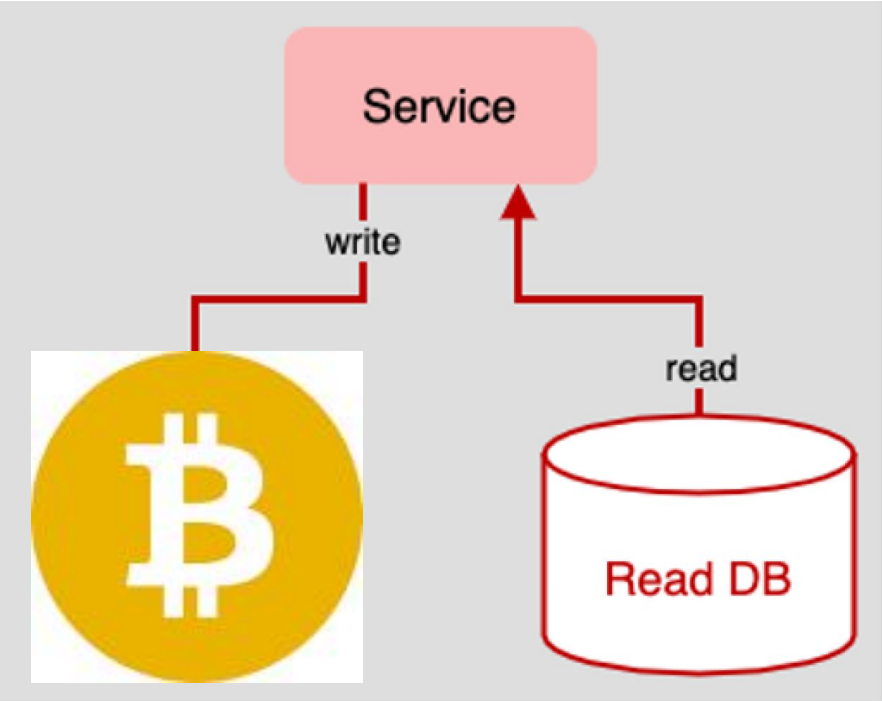

**Tomorrow:** Event-sourced CQRS

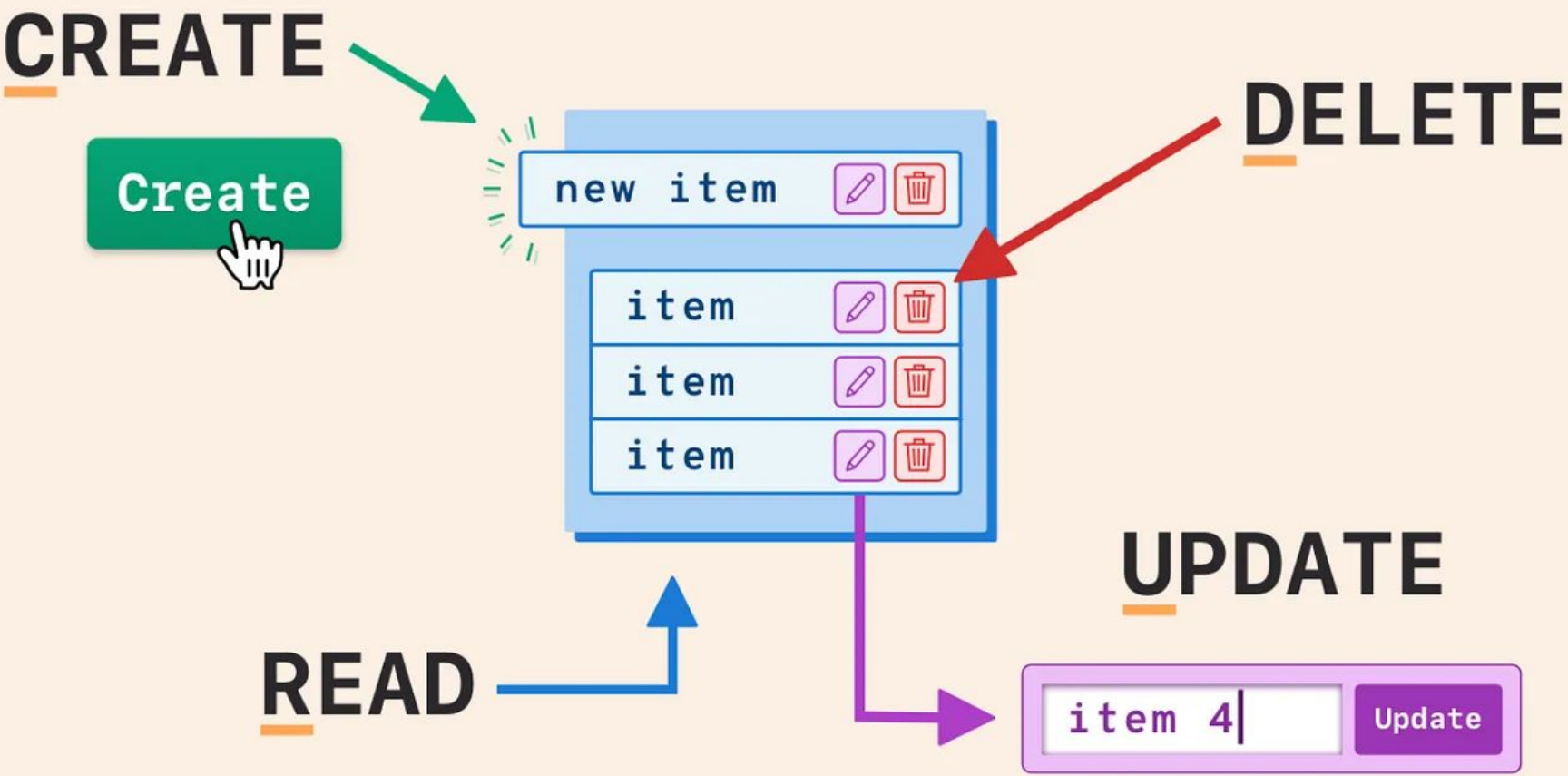


**Today:** CRUD




**Tomorrow:** Event-sourced CQRS

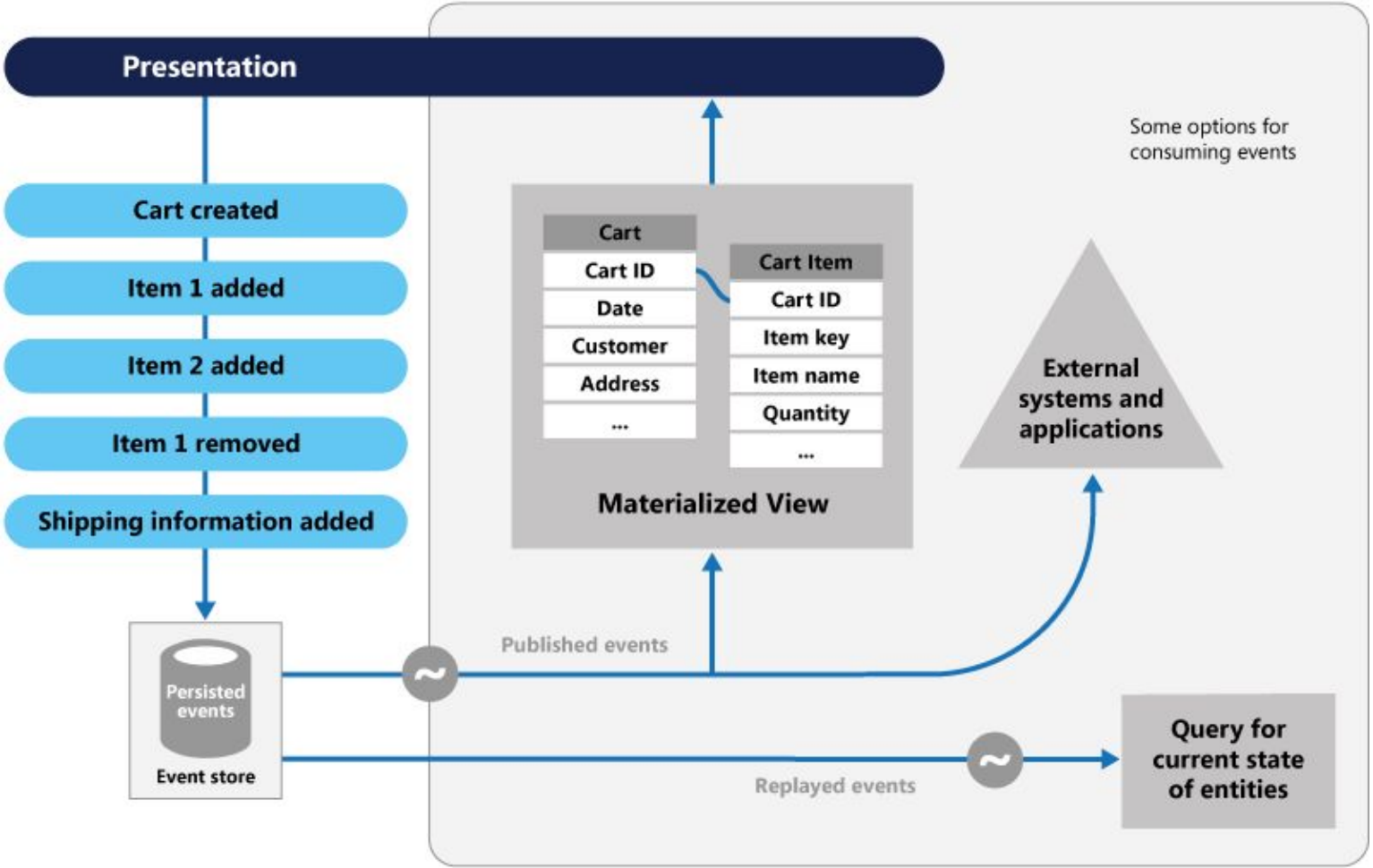




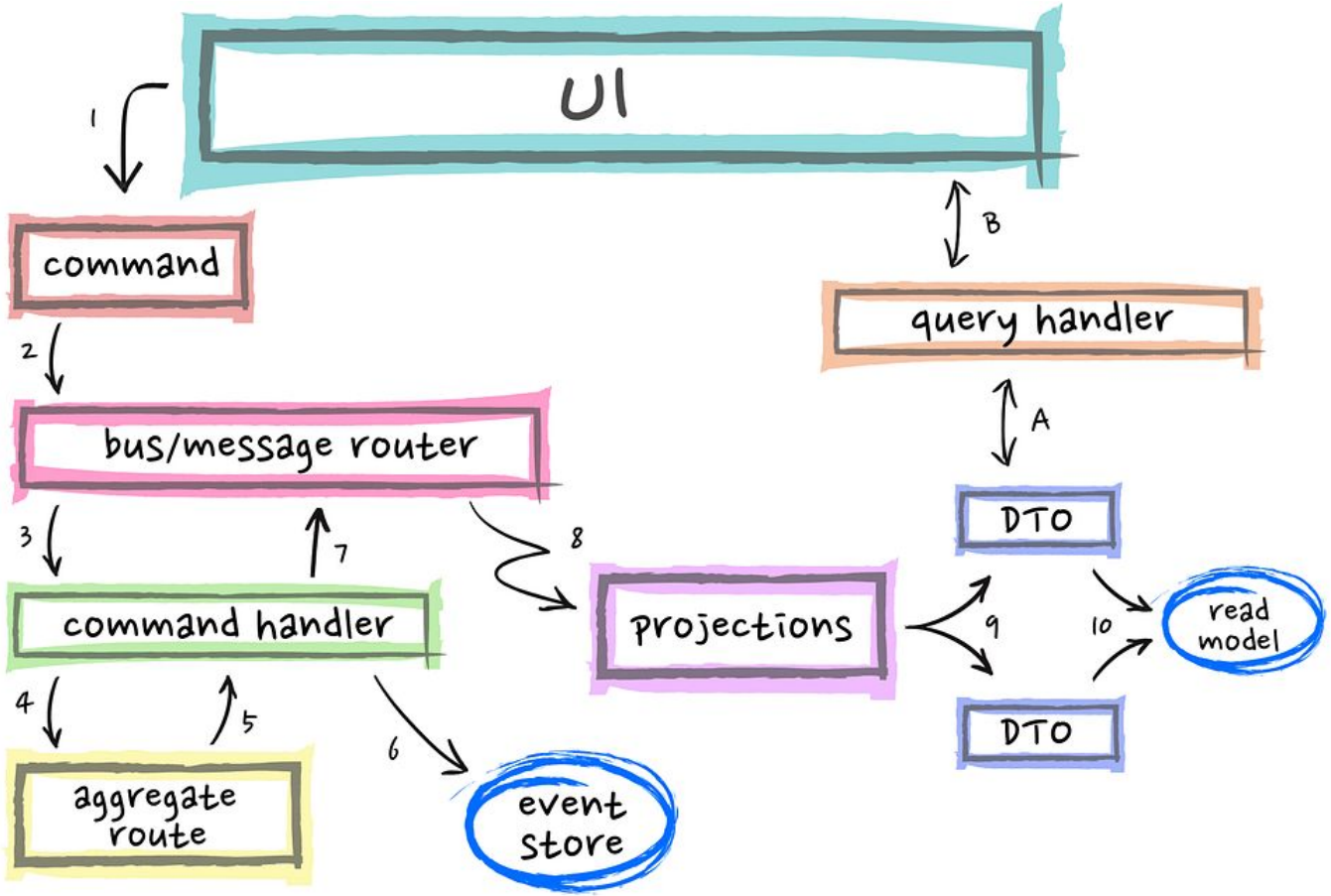

Source: https://medium.com/geekculture/crud-operations-explained-2a44096e9c88

| HTTP Method | CRUD operation | SQL query |
| --- | --- | --- |
| POST | CREATE | CREATE |
| GET | READ | SELECT |
| PUT | UPDATE | UPDATE |
| DELETE | DELETE | DELETE |

Source: https://www.forestadmin.com/blog/build-a-crud-app-for-your-database/




Source: https://learn.microsoft.com/en-us/azure/architecture/patterns/event-sourcing




Source: https://danielwhittaker.me/2020/02/20/cqrs-step-step-guide-flow-typical-application/

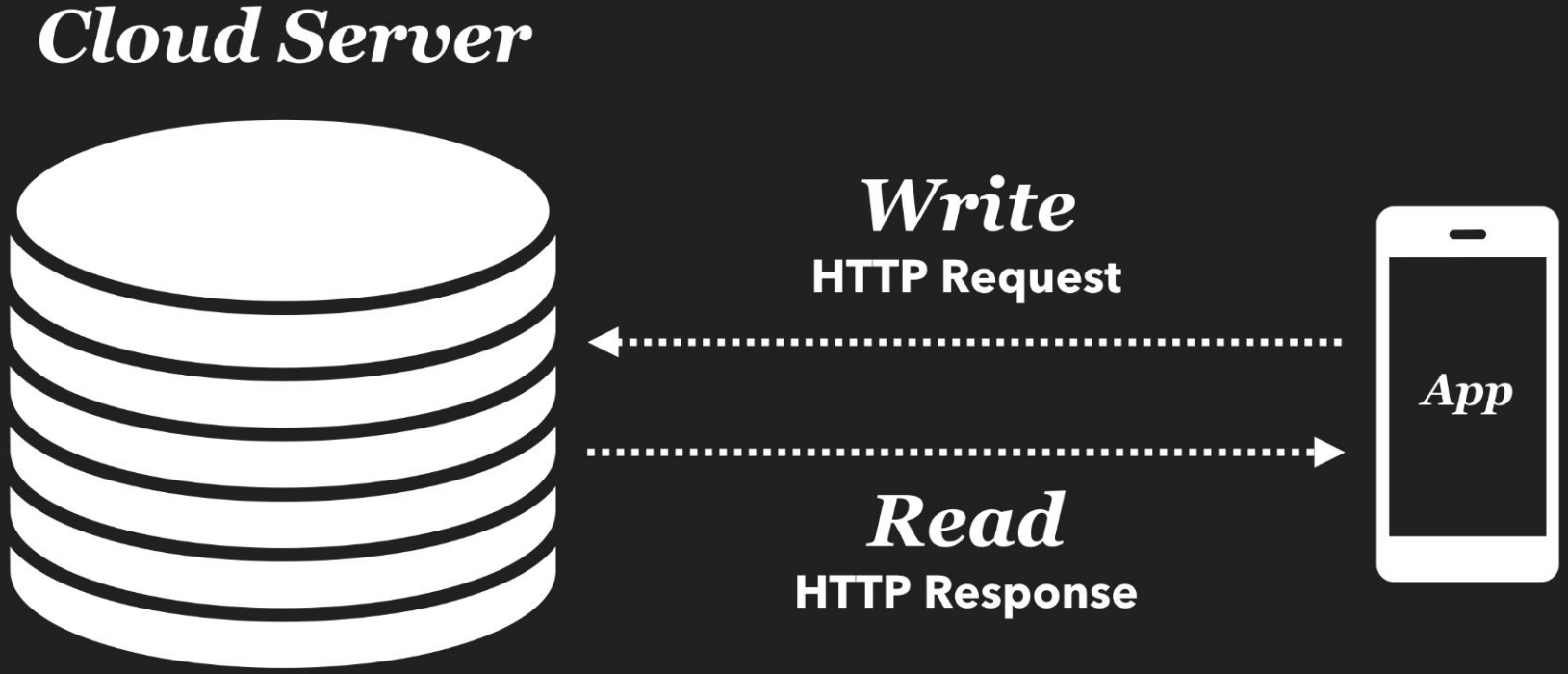
# Value streams shift

# 402 - Payment Required

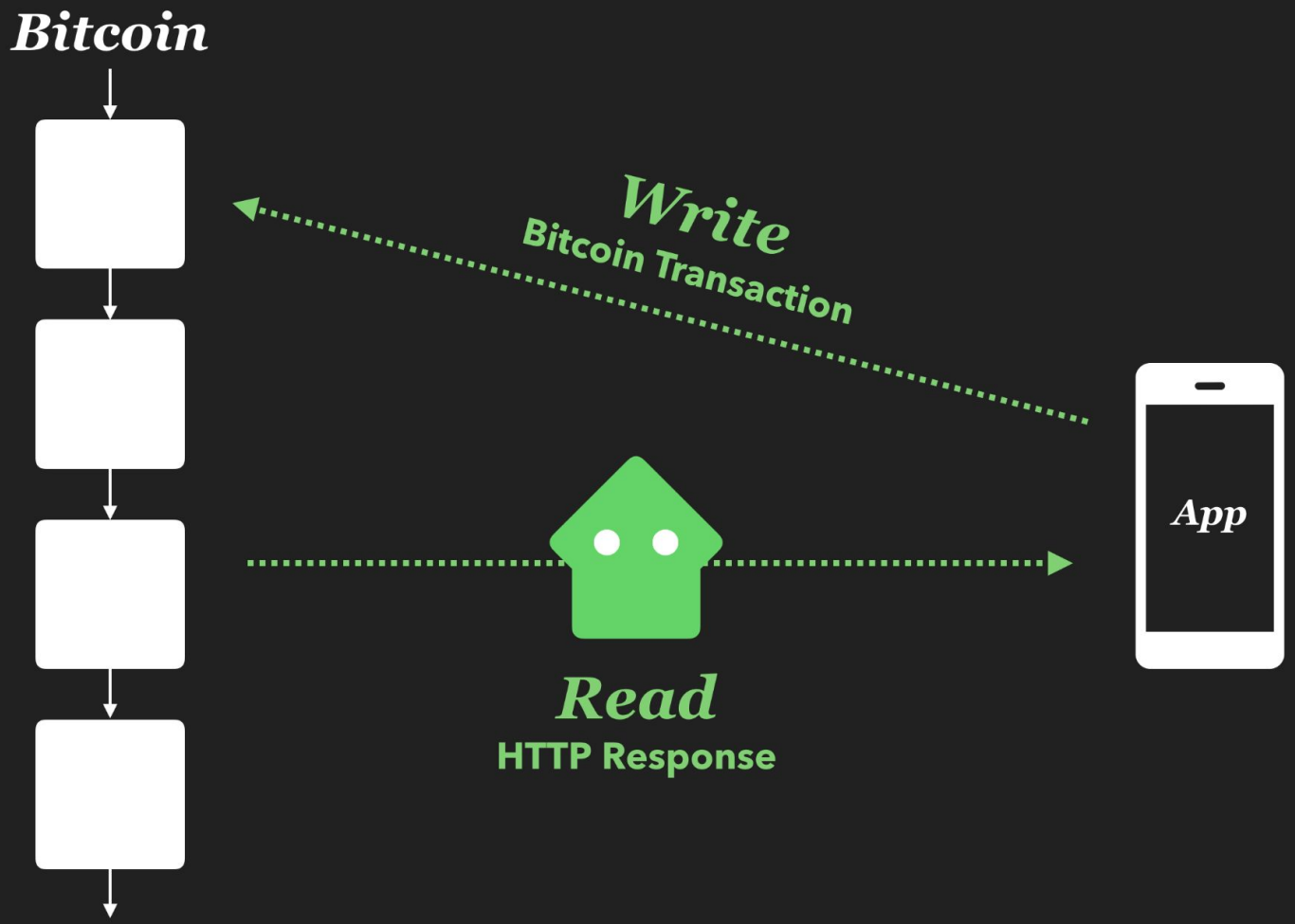
# HTTP Code 402 - Payment Required

- Every application taking payments on the internet today requires a third-party payment processor
- There is an existing, lower-bound to internet payments - about 25 cents + ~3% fees
- “A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution.”

# The Great Unbundling




Source: https://docs.planaria.network/#/intro


Bitcoin
Write
Bitcoin Transaction
App
Read
HTTP Response

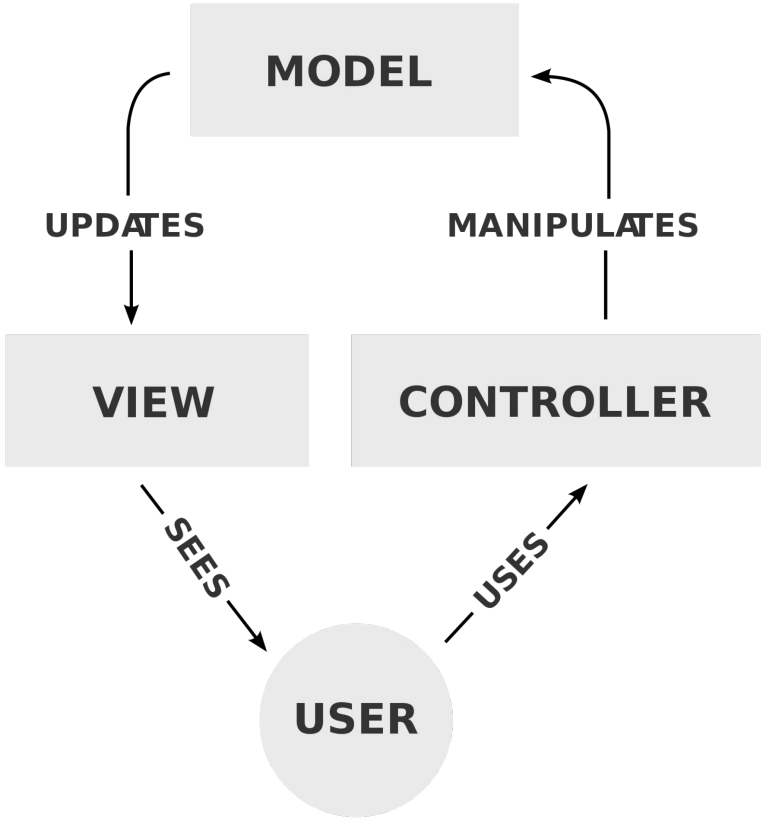
# Value moves from data silos to distributed interfaces

- The last 20 years of internet business will not be like the next 20
- Blockchains become a source of truth. Organization databases become caches.
- Value moves toward utility and the (people) services built atop systems.
- Value moves downward: from interface to objects to protocol
- Business models shift around a new, higher caliber data transactions
  - Users get paid for data
  - Users pay each other directly; no middlemen
  - Users pay for service and are less a (by)product of “free” web services
- The digital begins to mirror the physical world
  - eg: Digital twins and Augmented realities

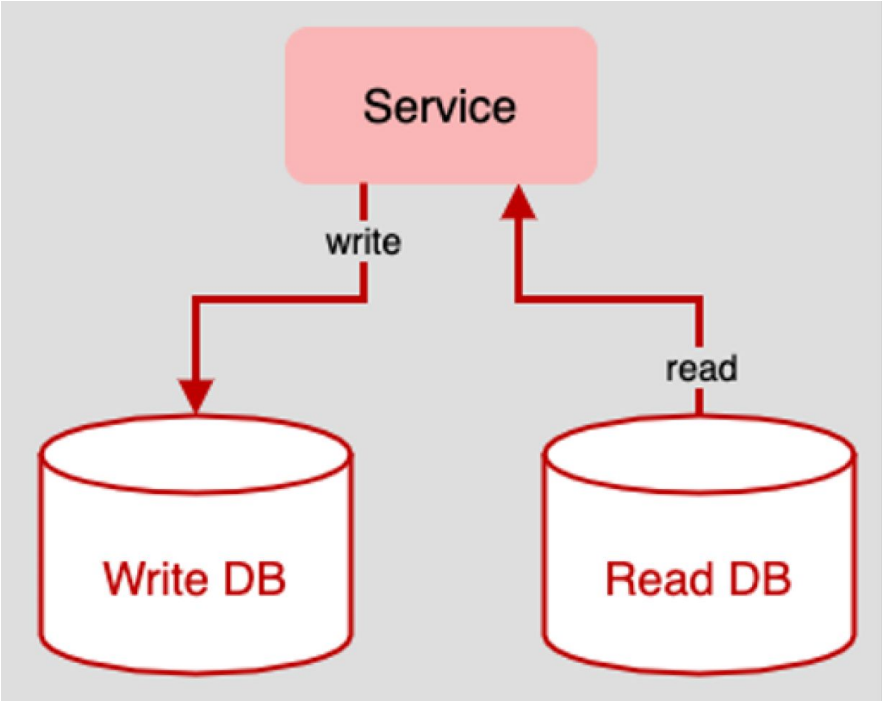
# The DRY Principle

Every piece of knowledge must have a single, unambiguous, authoritative representation within a system.

Source: https://www.slideshare.net/EvalKenig/dry-or-die




**MVC (Model View Controller)** is a *very* common pattern used in software,
where a single data source (database) is used to generate many views based on defined business logic



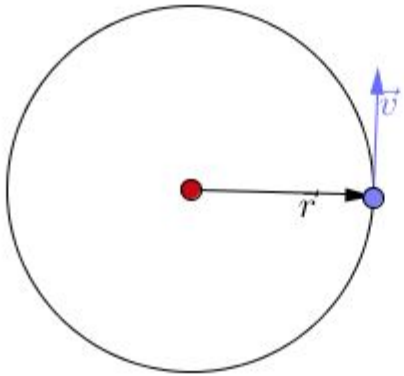

Odds are, your system will NOT be an originator of unique data,

but will reference a sea of existing, verifiable data

# The systems beyond your system

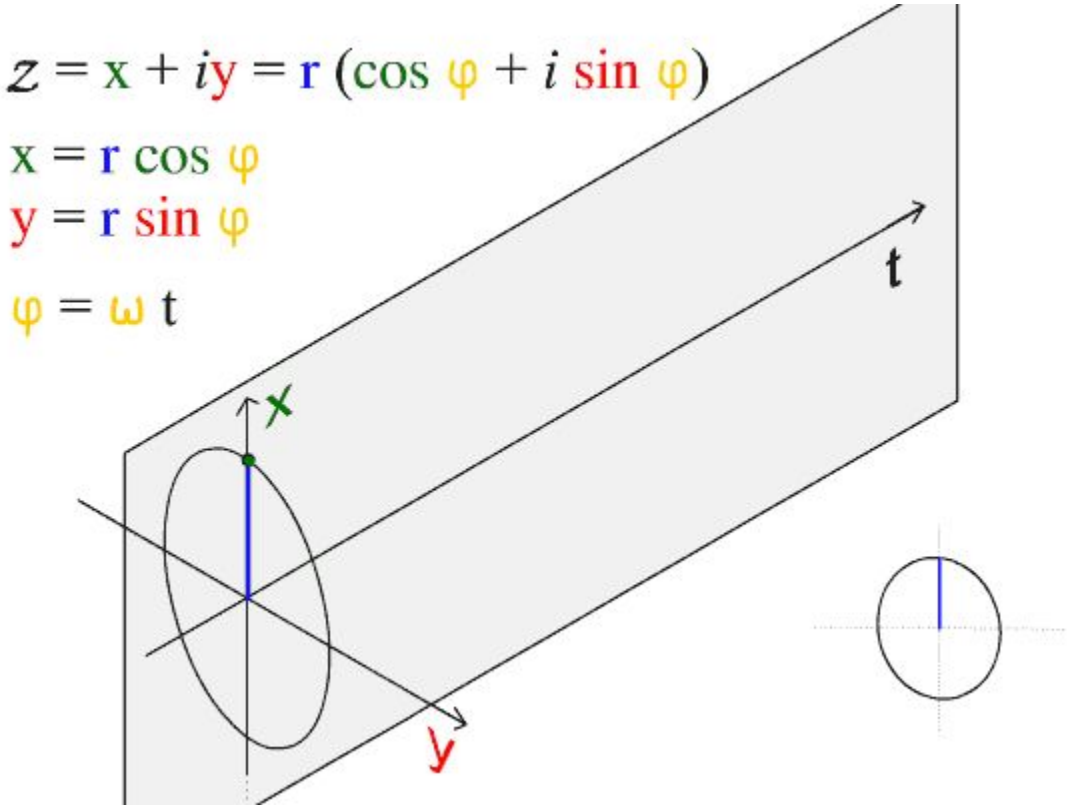
# Bitcoin

Let's think of Bitcoin as a perpetual rotating machine, an infinity motor.

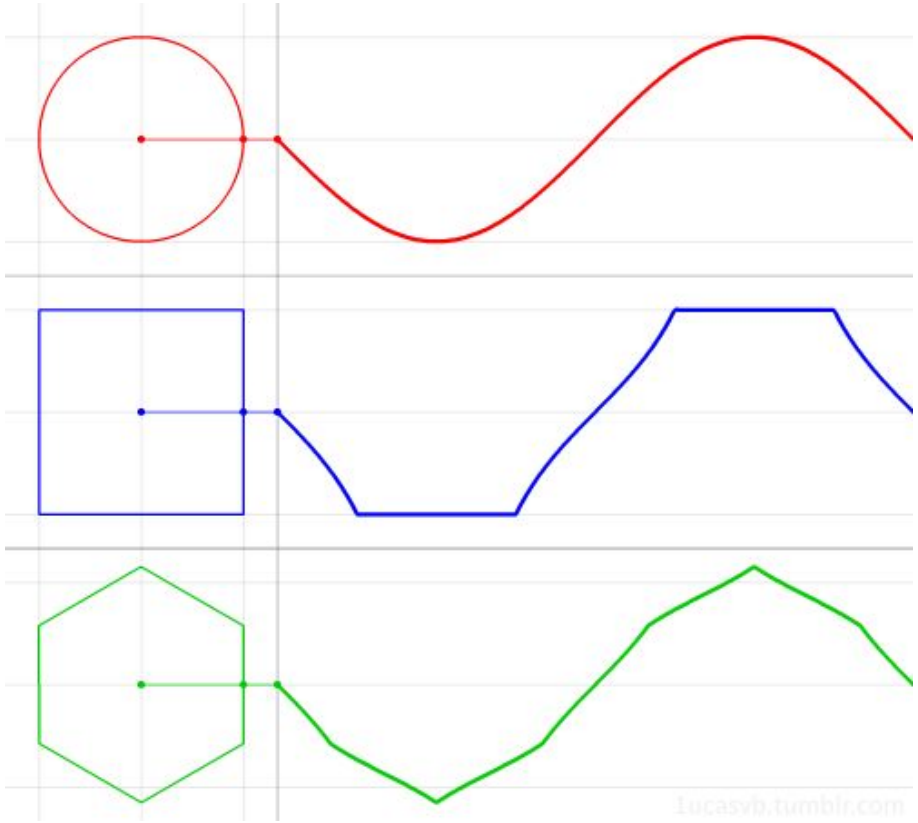



This "motor" travels through time and collects all the events (**transactions**) that happen through each rotation and takes an immutable snapshot (**a block**).

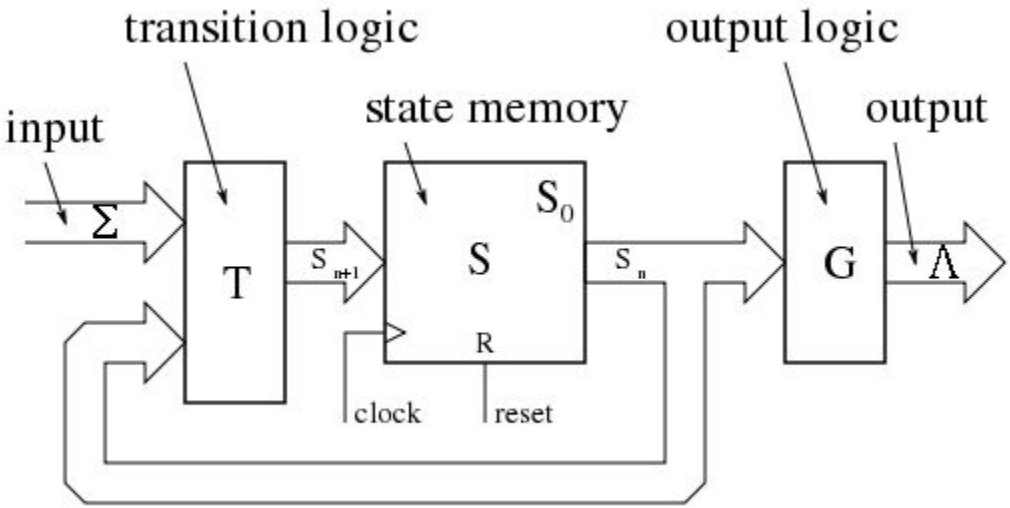
Source: https://docs.planaria.network/#/intro




Bitcoin's algorithms are deterministic and secure (powered by Proof of Work), making it a stable piece of technology to power all kinds of useful machines.

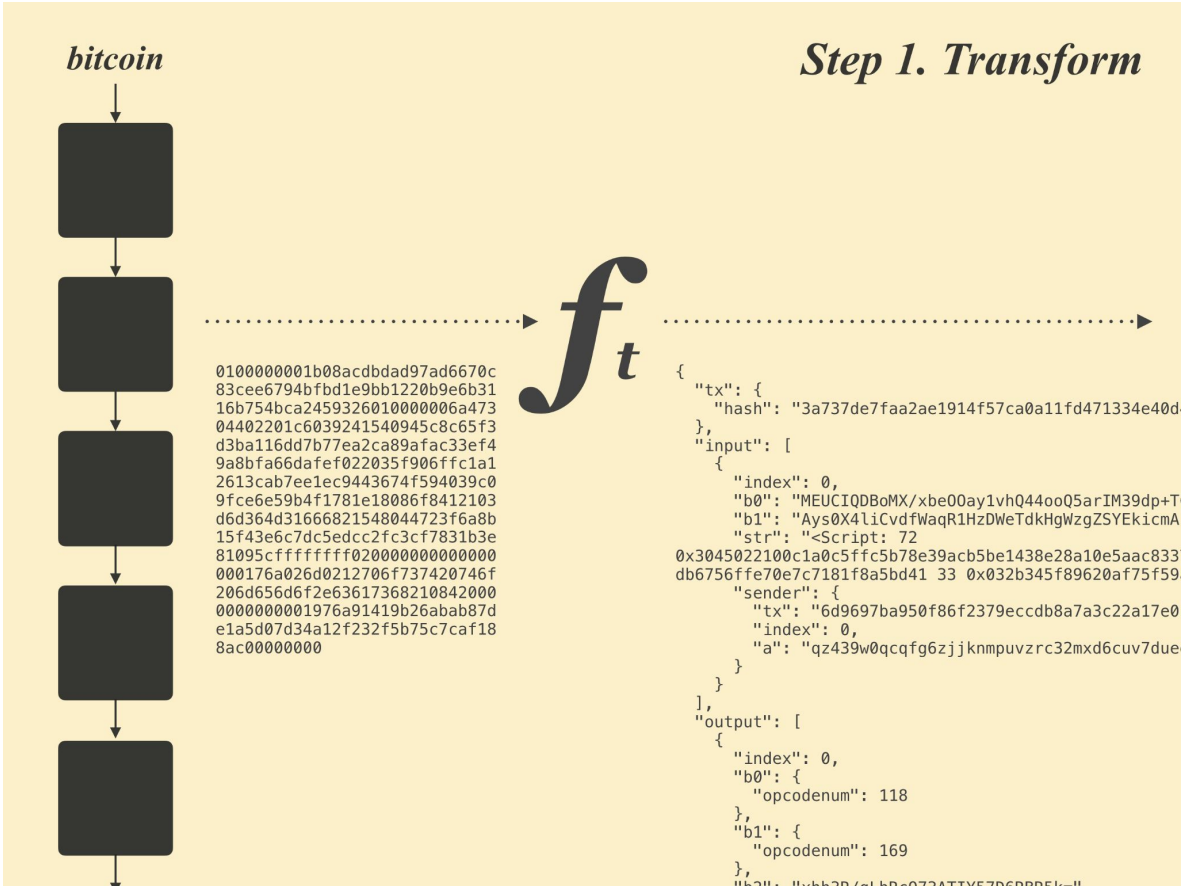



You can create infinite number of "machines" from a single reliable source



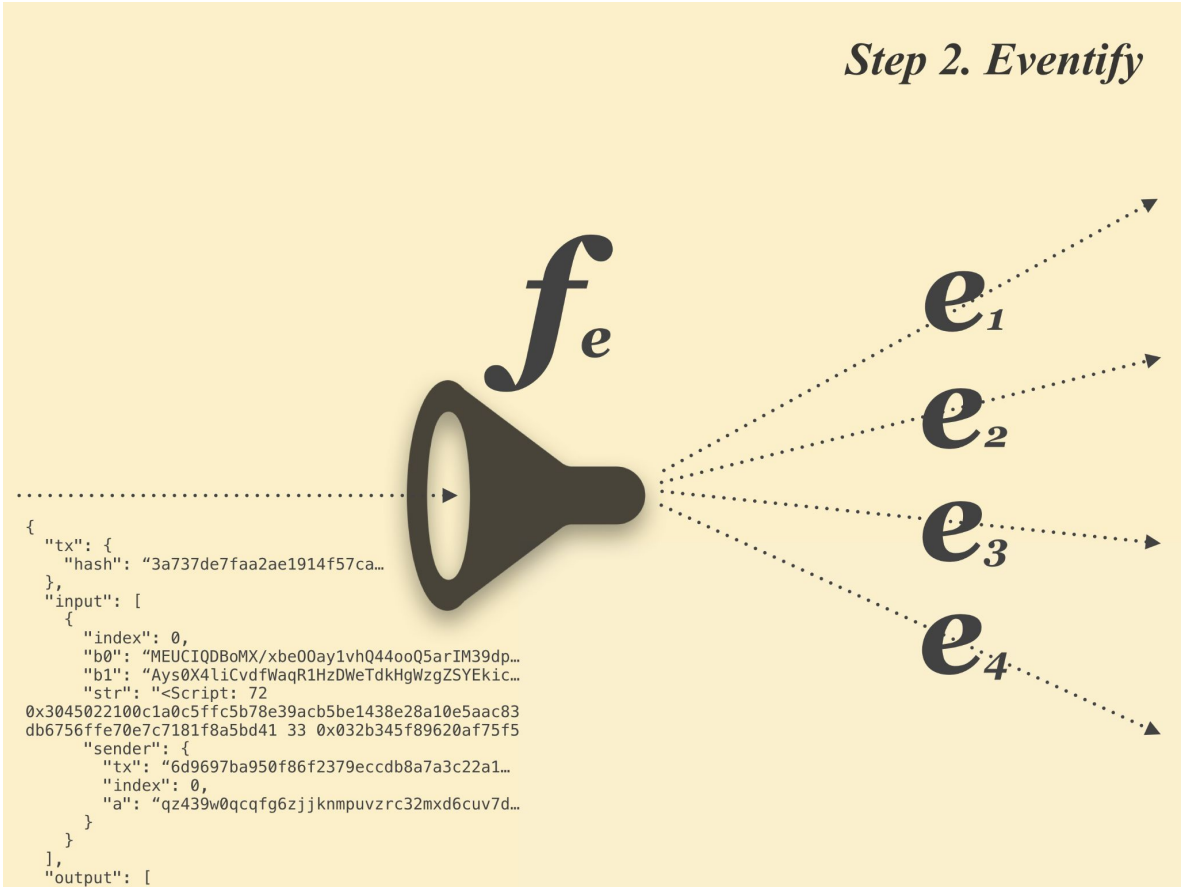

State machines.

Back to basics.



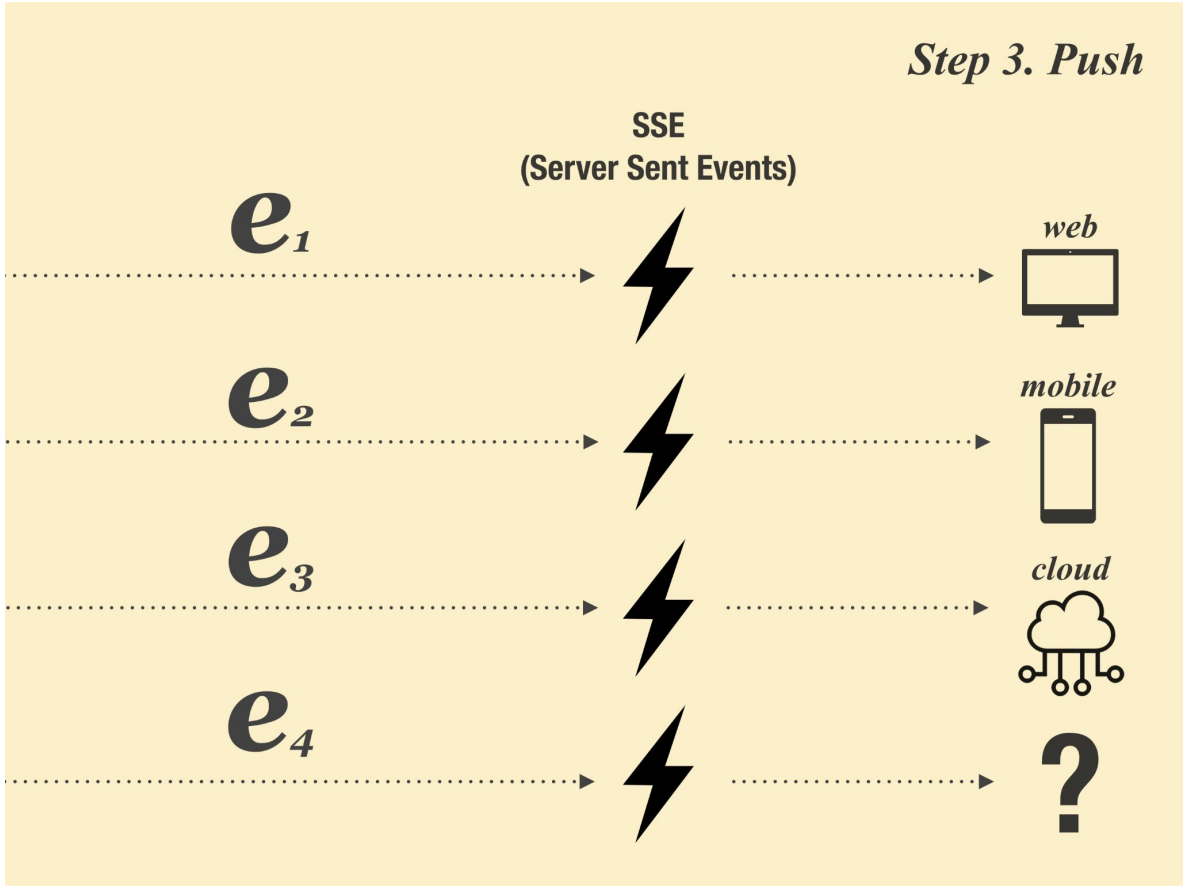

Currently, few blockchains can be queried directly.

A supporting system needs to exist to be queried. (These systems are being developed)



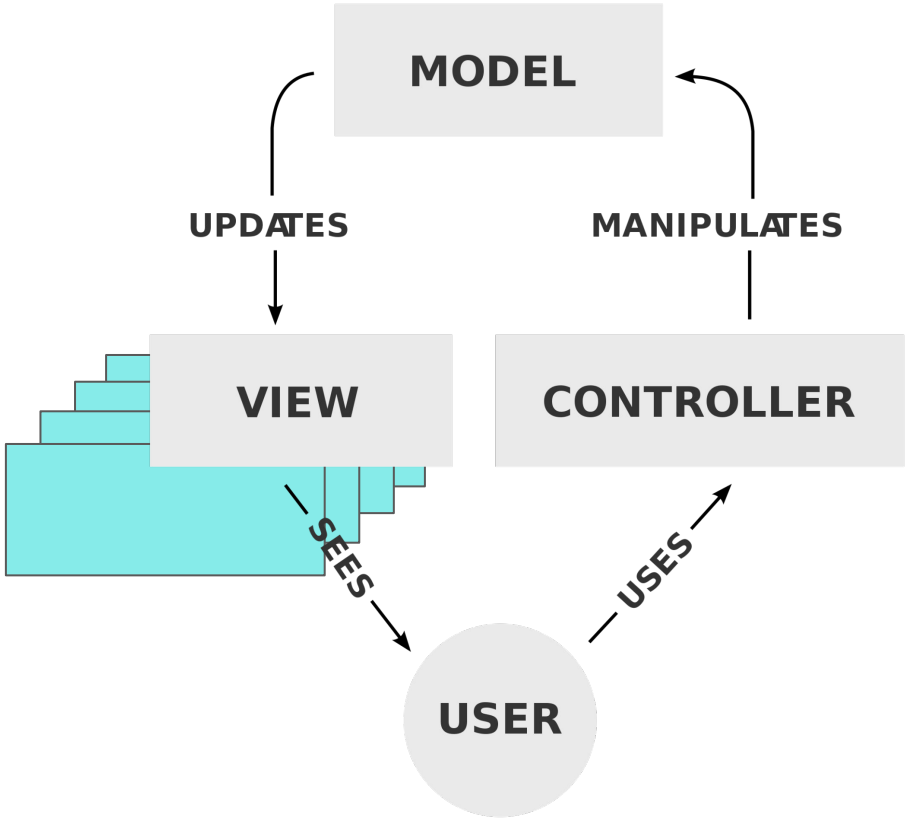

Based on your use case and the events in your business domain,

your app can **tune into specific events** happening on chain

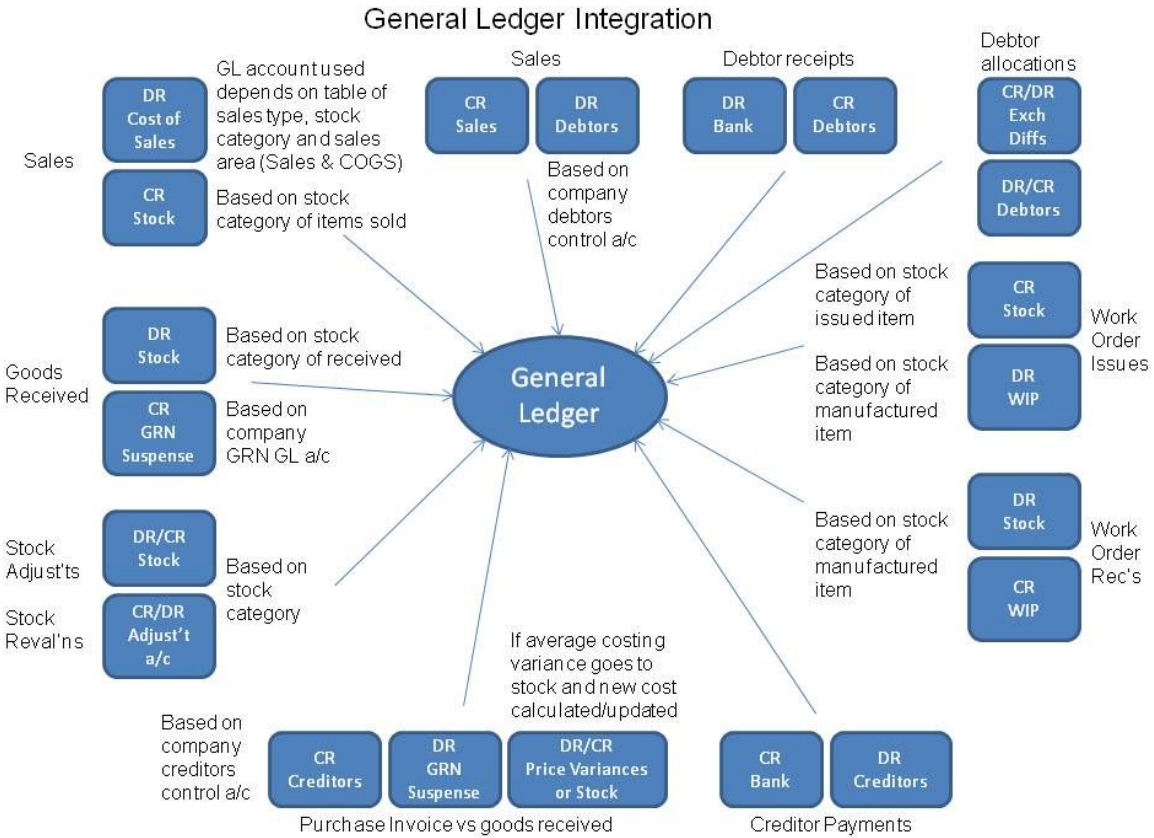



The same data can be projected into multiple  interfaces, based on user needs

Source: https://docs.planaria.network/#/socket




**MVC (Model View Controller)** is a *very* common pattern used in software,
where a single data source (database) is used to generate many views based on defined business logic



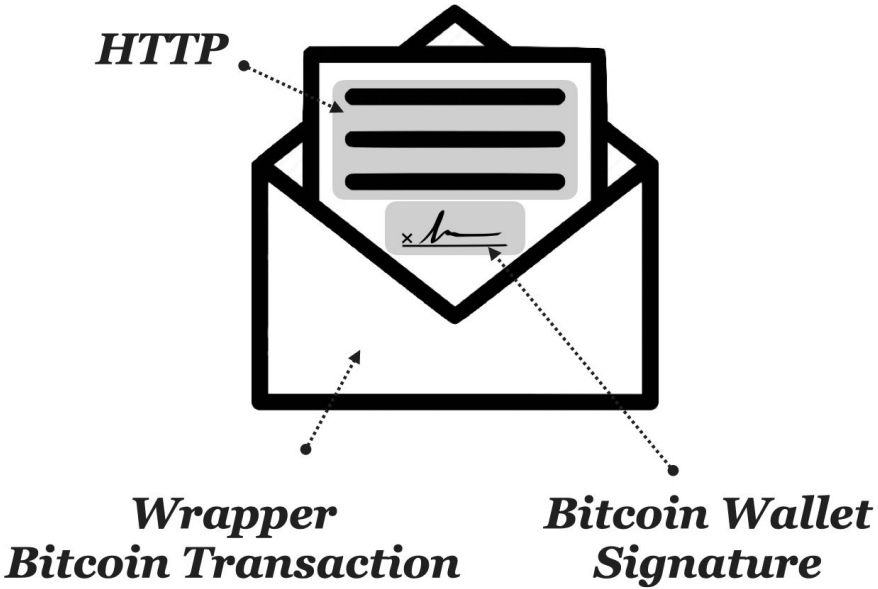

**How a single Model can generate many Views based on business needs**

Source: https://active-technologies.com/book/export/html/561

# Managing identity, Creating transactions

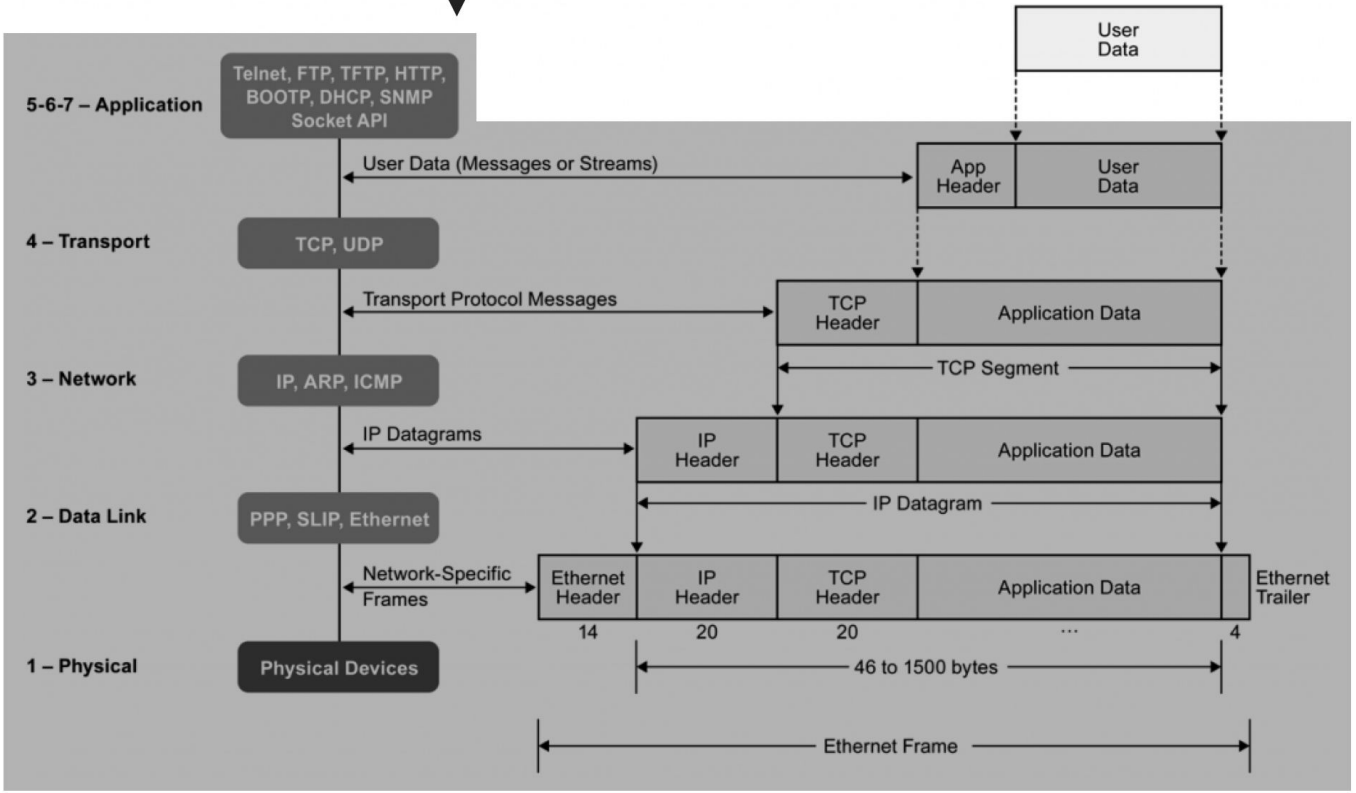
# Adopting wallets and supporting strong identity

- Identity (as opposed to anonymity) increases accountability and grounds online actions in existing bodies of law
- Blockchain transactions are immutable and can be treated as evidence
- DID (Decentralized Identifiers can be created cheaply then attested to by a public authority or delegate)
    - DIDs can be verified remotely, or revoked

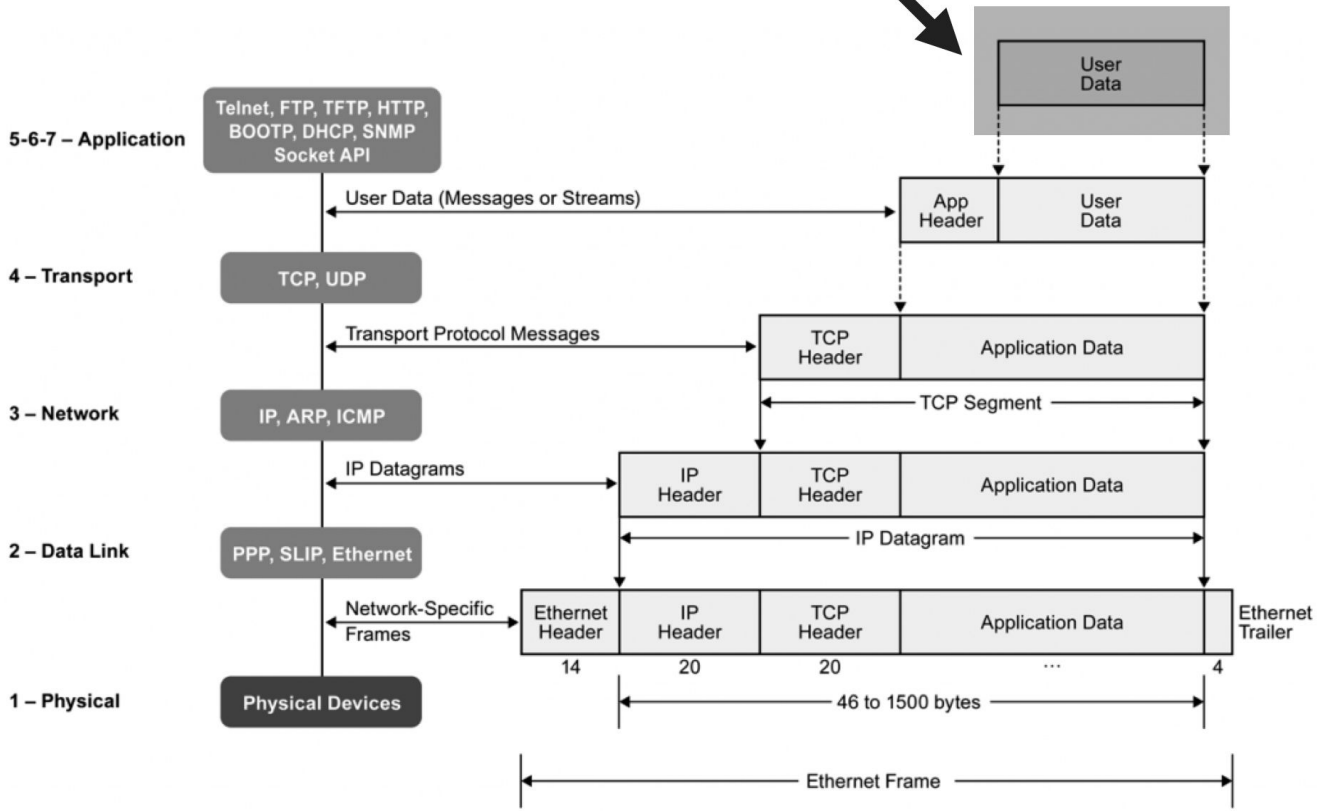


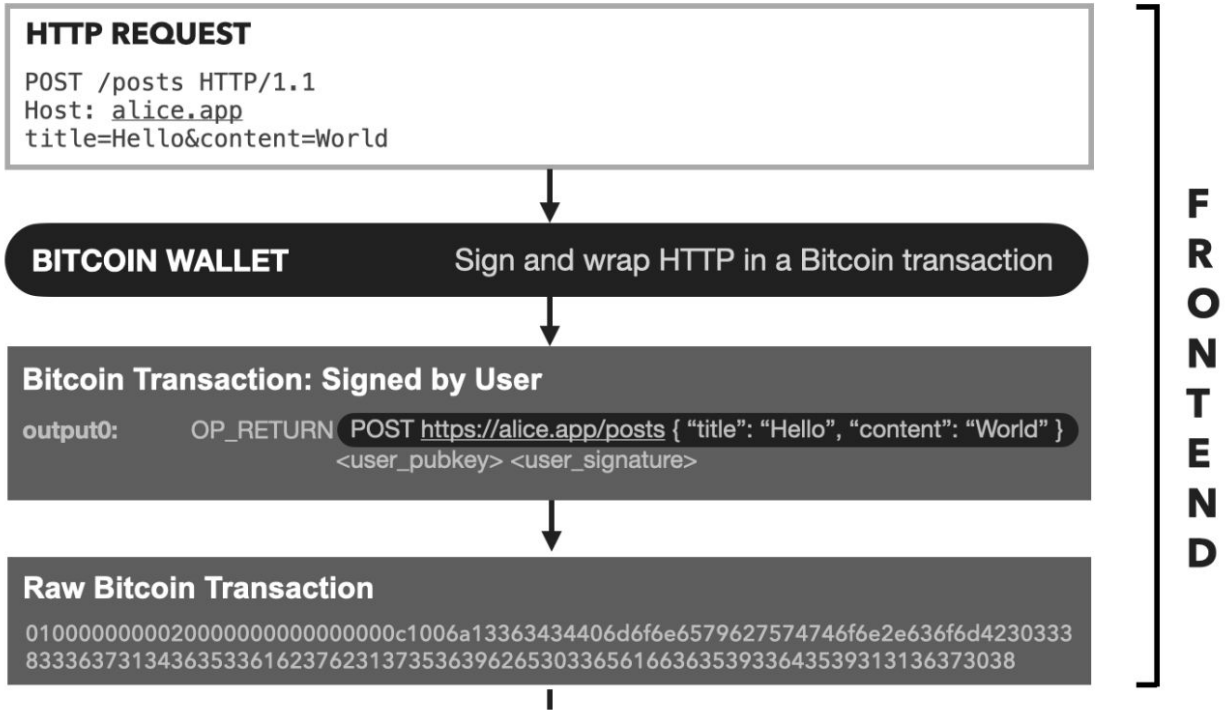

Source: https://vapor.network/

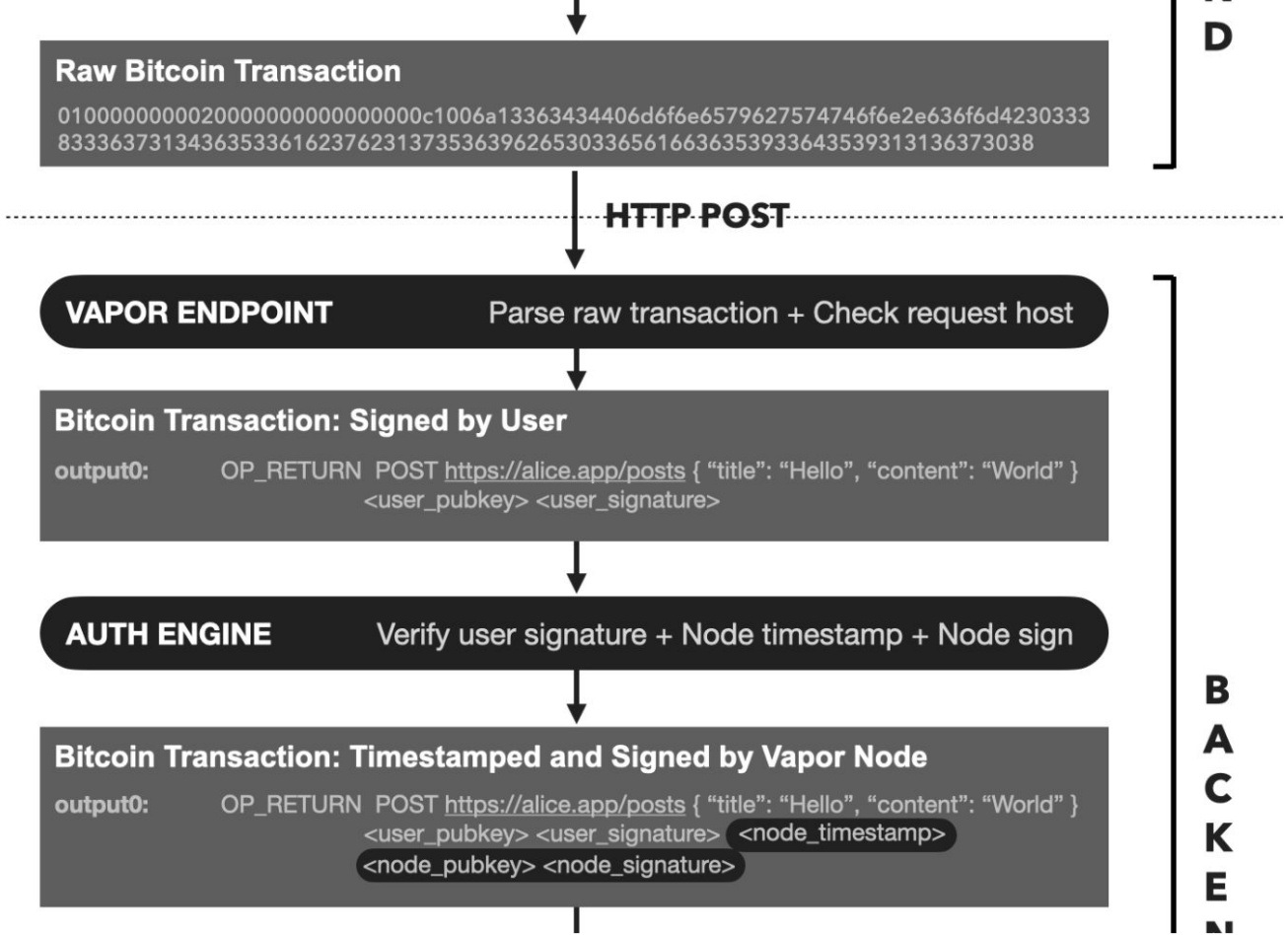
Most “Decentralized Web” projects try to **decentralize the networking stack.**

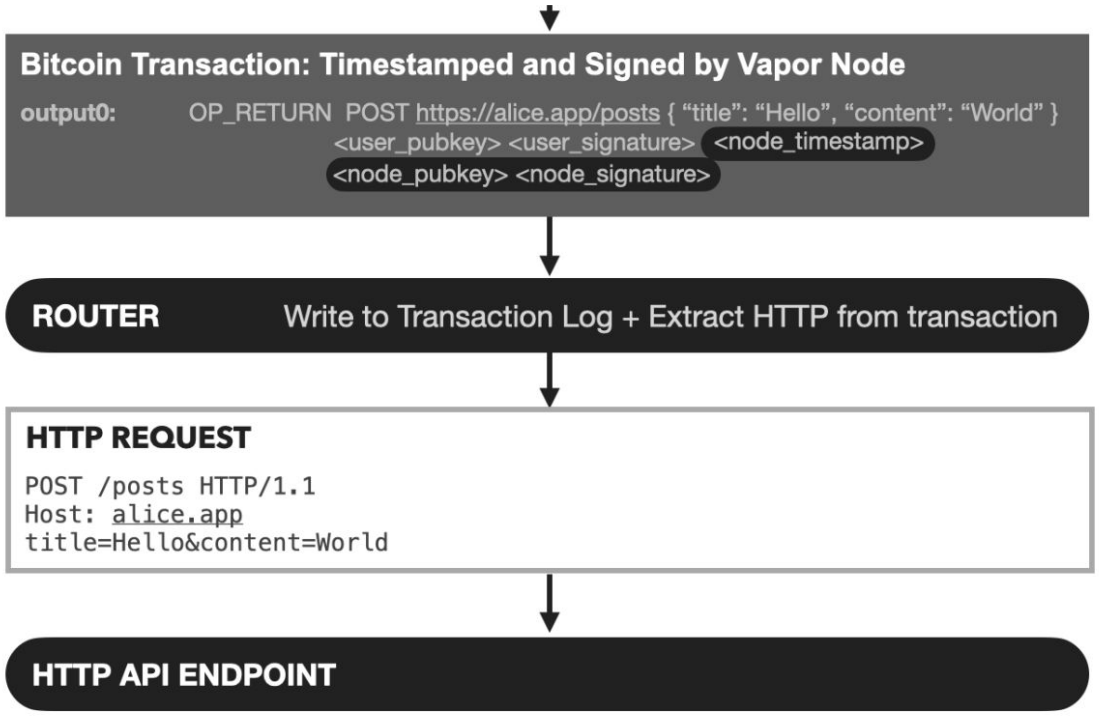


VAPOR **decentralizes the data layer** instead of the networking stack.

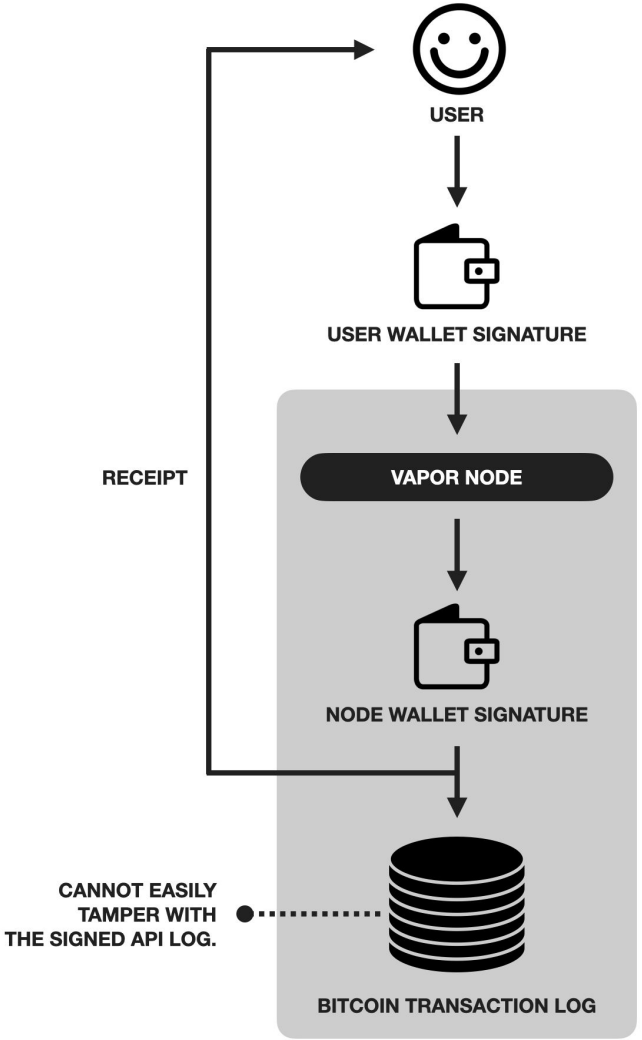


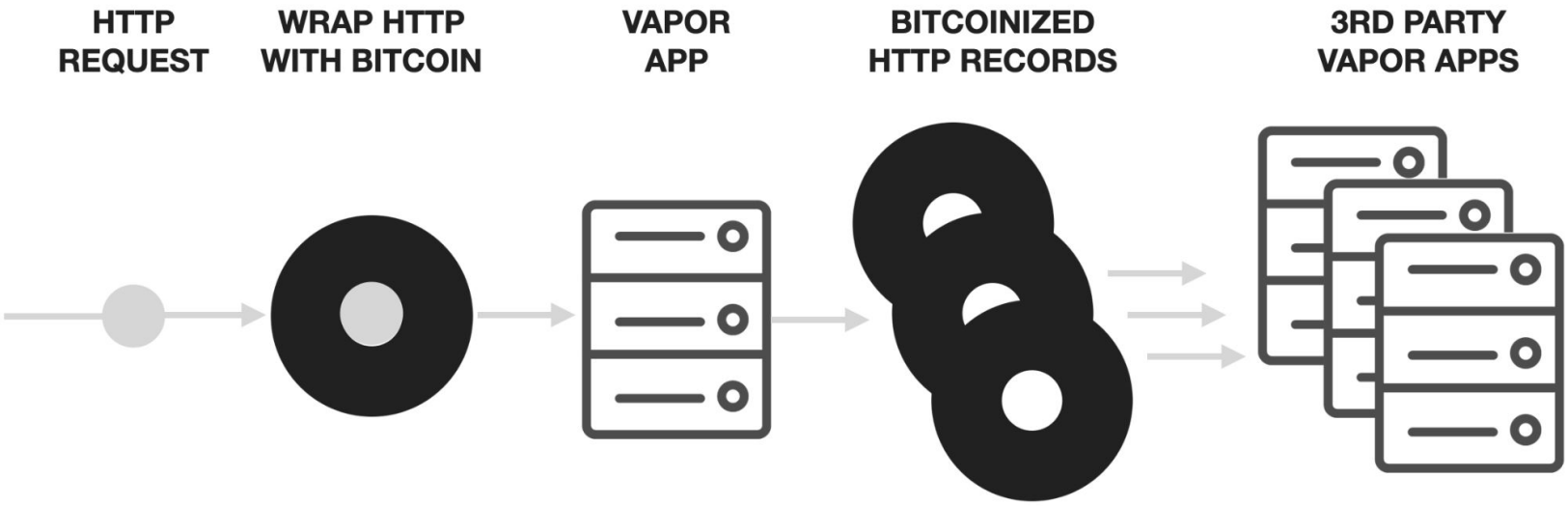

HTTP REQUEST
POST /posts HTTP/1.1
Host: alice.app
title=Hello&content=World
BITCOIN WALLET
Sign and wrap HTTP in a Bitcoin transaction
Bitcoin Transaction: Signed by User
output0:
OP_RETURN
POST https://alice.app/posts { “title”: “Hello”, “content”: “World” }
<user_pubkey> <user_signature>
Raw Bitcoin Transaction
0100000000020000000000000000c1006a13363434406d6f6e6579627574746f6e2e636f6d4230333
8333637313436353361623762313735363962653033656166363539336435393131363730 38
FRONTEND


Raw Bitcoin Transaction
0100000000020000000000000000c1006a13363434406d6f6e6579627574746f6e2e636f6d4230333
8333637313436353361623762313735363962653033656166363539336435393131363730 38
HTTP POST
VAPOR ENDPOINT
Parse raw transaction + Check request host
Bitcoin Transaction: Signed by User
output0:
OP_RETURN POST https://alice.app/posts { “title”: “Hello”, “content”: “World” }
<user_pubkey> <user_signature>
AUTH ENGINE
Verify user signature + Node timestamp + Node sign
Bitcoin Transaction: Timestamped and Signed by Vapor Node
output0:
OP_RETURN POST https://alice.app/posts { “title”: “Hello”, “content”: “World” }
<user_pubkey> <user_signature> <node_timestamp>
<node_pubkey> <node_signature>
B
A
C
K
E
N
D


Bitcoin Transaction: Timestamped and Signed by Vapor Node
output0: OP_RETURN POST https://alice.app/posts { “title”: “Hello”, “content”: “World” }
<user_pubkey> <user_signature> <node_timestamp>
<node_pubkey> <node_signature>
ROUTER
Write to Transaction Log + Extract HTTP from transaction
HTTP REQUEST
POST /posts HTTP/1.1
Host: alice.app
title=Hello&content=World
HTTP API ENDPOINT

BACKEND


USER
USER WALLET SIGNATURE
RECEIPT
VAPOR NODE
NODE WALLET SIGNATURE
CANNOT EASILY
TAMPER WITH
THE SIGNED API LOG.
BITCOIN TRANSACTION LOG




*“Record and Play”*

# Server-side Auth

Centralized Auth DB


Bitcoin
Built-in Auth
A Bitcoin Transaction itself is an "Auth"
App
Wallet

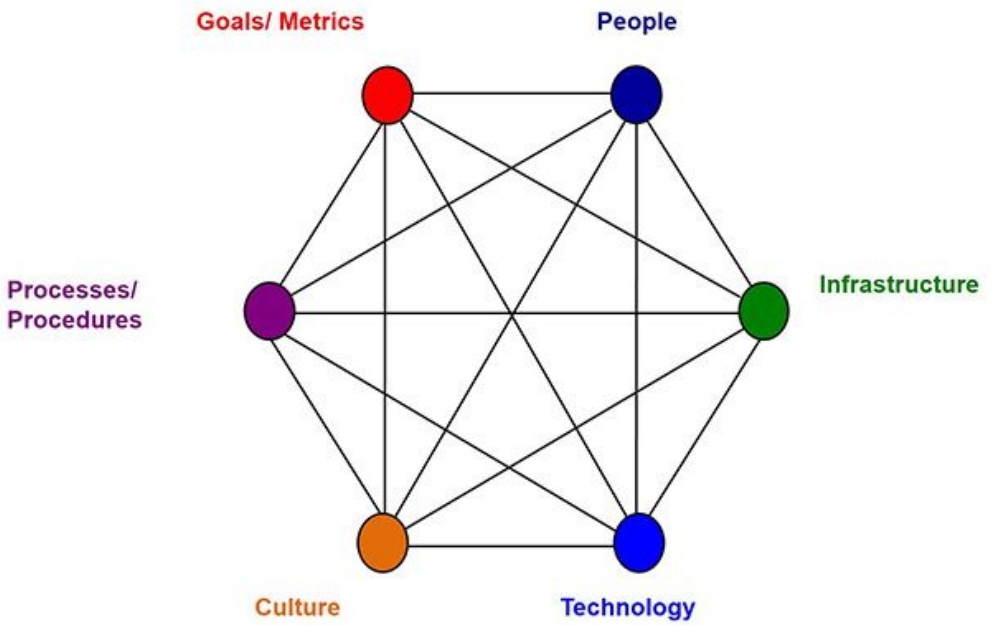
# Economics

# Economic considerations for socio-technical systems

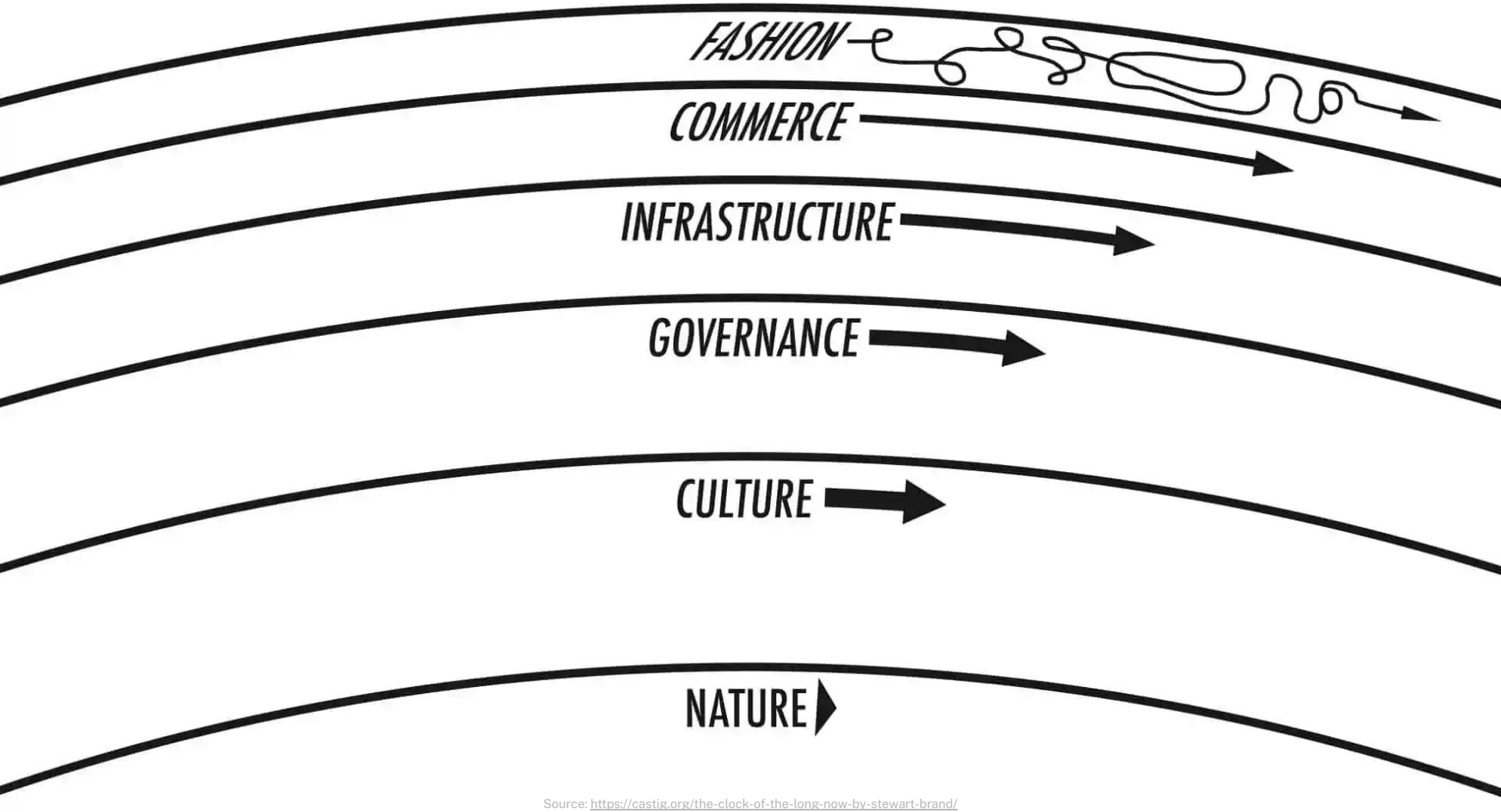
- Software is not a “solution”, software is a tool
- People + software create and transmit value

## Social + Technical

# Social + Technical considerations




Source: https://business.leeds.ac.uk/research-stc/doc/socio-technical-systems-theory



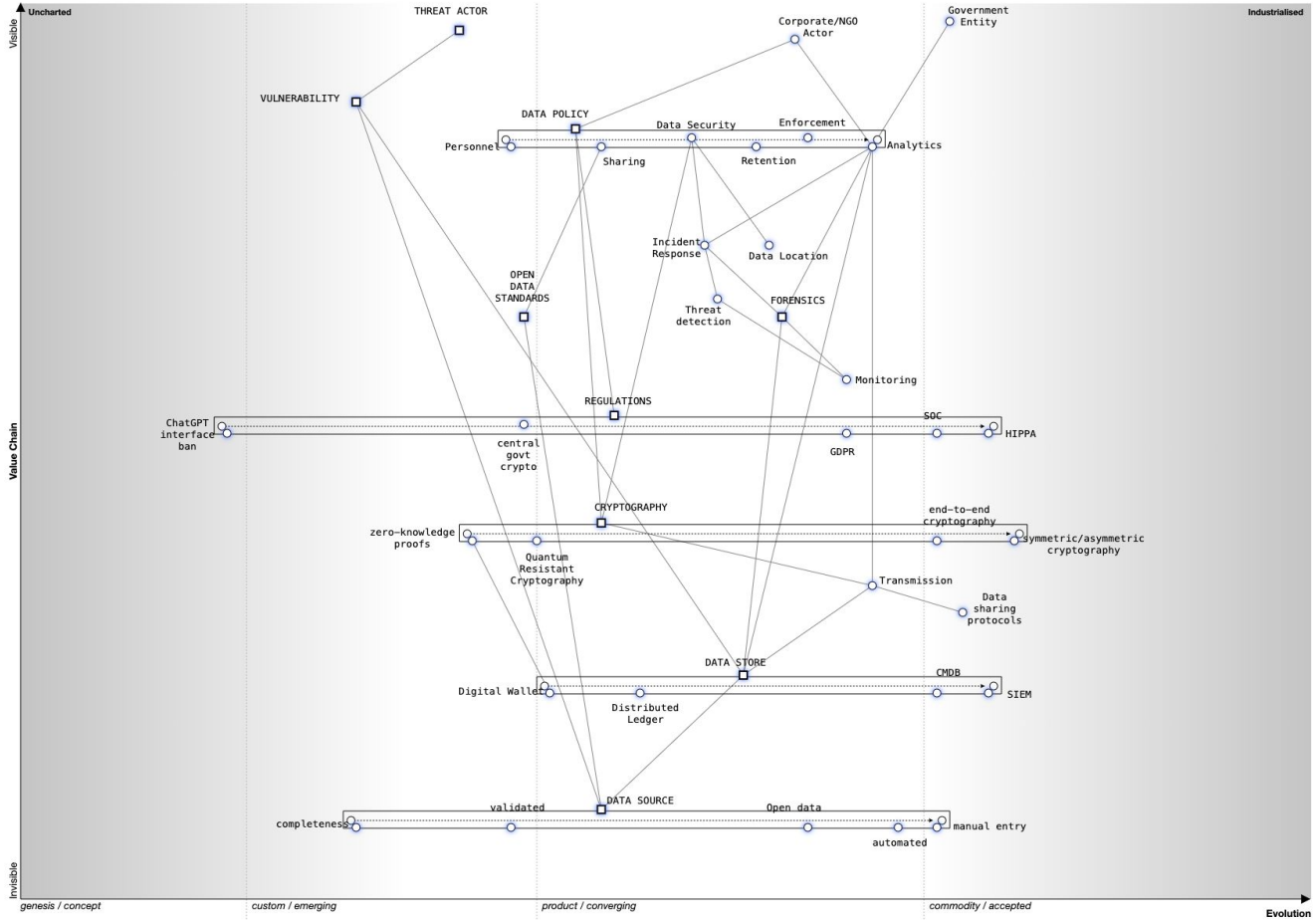

Source: https://castig.org/the-clock-of-the-long-now-by-stewart-brand/

# Economic considerations for socio-technical systems

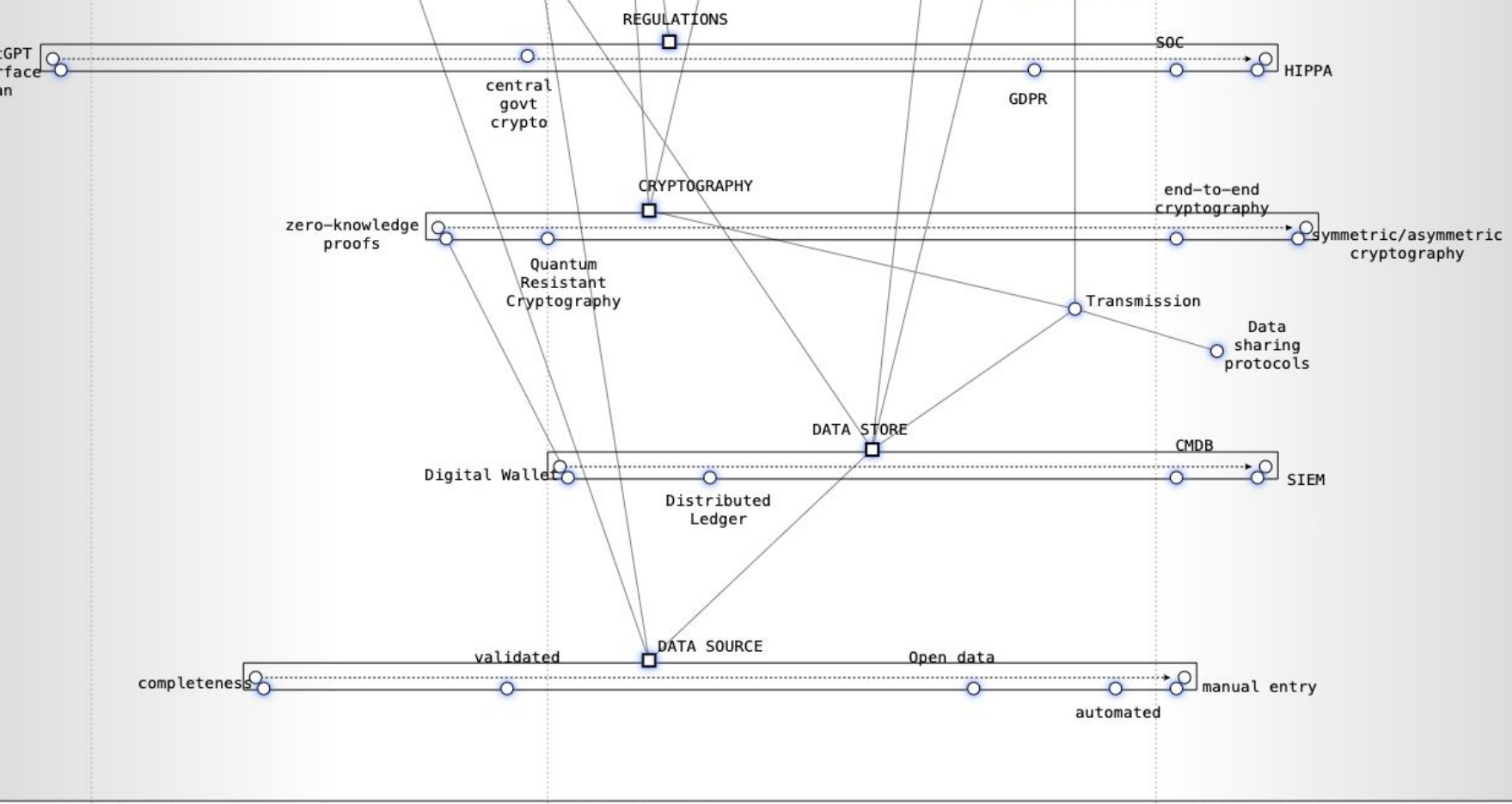
- Coordination costs
- Coordination costs
- Coordination costs
- Sound network economics
- Major implications for existing tech business models
- Major implications for workforce. Value streams shift.

Reference: https://www.brightstorm.com/math/geometry/reasoning-diagonals-angles-and-parallel-lines/number-of-handshakes-at-a-party-problem-1/

Data (organizations), MAY 2023




Source: http://blog.gardeviance.org/2015/02/an-introduction-to-wardley-value-chain.html


REGULATIONS
SOC
HIPPA
central
govt
crypto
GDPR
CRYPTOGRAPHY
end-to-end
cryptography
zero-knowledge
proofs
symmetric/asymmetric
cryptography
Quantum
Resistant
Cryptography
Transmission
Data
sharing
protocols
DATA STORE
CMDB
Digital Wallet
SIEM
Distributed
Ledger
DATA SOURCE
validated
Open data
completeness
manual entry
automated
custom / emerging
product / converging
commodity / accepted

# Economic foundations

- Security is an economic function
- Bitcoin’s block reward is a subsidy
  - The subsidy is phased out over time
- Miners will compete for transaction fees
- Transaction fees are cheap, but voluminous (millions of tx/second)
  - Think: cans of soda
- It is more costly to attack the network than to support it
  - harness the unattractive human tendency toward greed

# Security

Bitcoin reduces human politics.

Because of the Proof of Work system that powers Bitcoin, there is little room for human politics. Bitcoin operates at scale with this model. Everything else is or has moved to utilizing a concept called "Stake", also known as politics.

# Bitcoin is (primarily) an economic breakthough

Security is an economic function.

Blockchains already existed by 2000.
Sarbanes-Oxley (2002) led to increased adoption of WORM (write once read many) drives.
Many (hundreds) of electronic cash projects had been tried by 2008.
Bitcoin was designed with deep knowledge of the history of currency.
Bitcoin was designed with considerations for law, evidence, and chain of custody.
Bitcoin's block subsidy, transaction fees, and competitive miner network are well-considered.

Public 👏

Scalable 👏

Blockchain 👏

# **Action** items to consider

- Get a public blockchain ATO'd at an organization
- Support experimentation of wallet technologies
  - In a browser, and at the operating system level
- Support research for identity systems
  - PIVs, DIDs, and Active Directory
- Wardley Map your systems
  - Make the value streams visible and focus on the **economics** involved between players
- Move existing systems toward event-sourcing patterns
- Consider digital currency friendly legislation
  - Reduce burden and improve public service delivery

# References

- Bitcoin
  - docs.planaria.network
  - unwriter.net
  - vapor.network
  - en.bitcoin.it
  - wiki.bitcoinsv.io
  - craigwright.net/blog
- CQRS & Event-sourcing
  - Greg Young
- Domain-driven Design
  - Albert Brandolini
- Wardley Mapping
  - Simon Wardley

# Questions?

# Thank You

ryanwold.net
github.com/afomi