FEDERAL RESERVE BANK *of* ST. LOUIS
CENTRAL TO AMERICA'S ECONOMY®

Blockchain

What it is, what it does, and why you probably don't need one

David Andolfatto

Blockchain Forum, Washington University
January 2018

Individual performance histories

- A database of individual performance histories has value where honesty and trust in future performance is lacking.
    - Individual work histories, customer service records, delivery and receipt histories, credit histories, performance records, etc.
- Obvious incentive to misrepresent/fabricate history.
- Wanted: an honest + immutable database of histories.
- Object: eliminate discordant records, audit costs, promote fair, efficient outcomes.

History as chained blocks of information

- Let *t = 1,2,3*,…, denote time. Let *E(t)* denote a description of events at date *t*.

- A *complete history @ t* is *H(t-1) = { E(t-1), E(t-2),…, E(0) }.*

- Note: *H(t-1)* consists of time-stamped blocks of information, connected in sequence to form a chain of blocks.

- In this sense, any database consisting of a complete history of events can be thought of as a "blockchain."

- In contrast: $H(t-1) = \sum_{j=0}^{t-1} E(j)$ or $H(t-1) = E(t-1)$.

Database Management Systems

- Any DBMS specifies parameters restricting:
  1. Read privileges (who, what and how).
  2. Write privileges (who, what and how).

- Standard (e.g., SQL) protocols can (in principle) accommodate wide range of parameters governing (1).

- But standard protocols must heavily restrict the *who* in (2); only “trusted historians” permitted to write history.

- *Suppose we do not trust delegated historians*. Big problem?

Extending the read privilege

- First, historians *not* “trusted” in present systems (reputations).

- Lack of transparency? Extend the read privilege communally.
  - Implies *de facto* distributed ledger, available in real time.
  - Communal monitoring of historians → “trust, but verify.”

- Shared, replicated, permissioned ledgers of chain-blocked information feasible with current protocols (e.g., SQL systems) → do not need “blockchain” if this is what you want.

- Blockchain only necessary if you do not have faith in standard reputational mechanisms to discipline writers.

Gaming the write privilege

- Replace trusted historian with a set (delegates from different companies, divisions, etc.).

- Have this set play a *validation/consensus game* designed such that the *unique* equilibrium strategy profile chosen by each historian at every date *t = 1,2,3*,… entails:
  1. No tampering with recorded history *H(t-1)*. *Immutability*.
  2. Only true blocks *E(t)* are validated and added to *H(t-1)*.

- Assume *H(t-1)* true. Then *H(t) = E(t) + H(t-1)* is true.
- Trust in historian replaced by trust in algorithm (game).

Definition: *Blockchain*

- A DBMS with: (i) $H(t-1) = \{ E(t-1), E(t-2), \ldots, E(0) \};$ (ii) read privileges (more/less) open; and (iii) write privileges determined by a non-cooperative consensus game at each *t*.

- Blockchain histories are not intrinsically true and immutable; depends on properties of consensus game.

- Because blockchain relies on non-cooperative consensus, it is intrinsically *more costly* than cooperative (trust-based) counterparts.

- Nevertheless, depending on circumstances and application, it may be a cost worth incurring.

Bitcoin: a money and payments system

- Database contains accounts, account balances and account transfer histories (no IDs, no info on objects exchanged).

- Read privilege is open and free, write privilege open and (therefore) costly.
  - WP @ *t* determined by winner of open PoW competition.
  - Historians (miners) compensated in BTC (seigniorage + fees).

- Protocol (which also determines monetary policy) is governed by an observable constitutional code, subject to amendments (code patches) and constitutional crises (forks).

Cryptocurrency mania

- Likely all failures as payment systems. Price appears to be driven by demand for “safe” (not risk-free) crypto-assets.

- Supply of BTC fixed at 21M by algorithm.
  - BCH fork now means 42M “bitcoins.”
  - Supply of cryptocurrencies is potentially infinite.

- Important competitors
  - Litecoin (faster payment process); Ethereum (smart contracts);
  - Zcash (restricts read privileges); Monero (enhanced anonymity);
  - Ripple (cooperative consensus mechanism).

Blockchain: Powering DAOs

- Decentralized Autonomous Organization (DAO).

- DAOs possess no central authority/node and so can offer protocols unencumbered by prevailing laws and regulations.
  - E.g., Bitcoin is a MSB outside the reach of government regulation (of course, not the case with Bitcoin intermediaries).

- Comparative technical advantages.
  - Anonymity, permissionless access and use.
  - Irreversible actions/transactions (Smart Contracts).

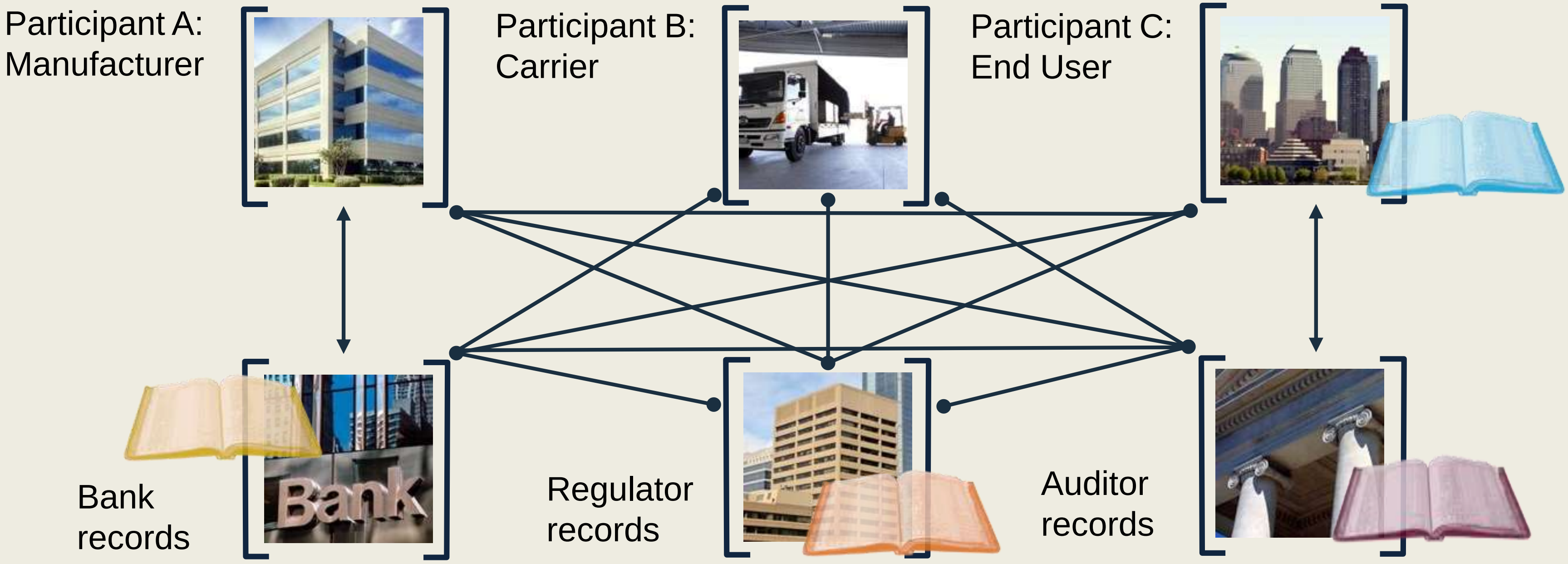
- Not clear (to me) the value for registered businesses.

Thank you

david.andolfatto@stls.frb.org

http://andolfatto.blogspot.com/2017/12/my-perspective-on-bitcoin-project.html

Problem



Participant A: Manufacturer

Participant B: Carrier

Participant C: End User

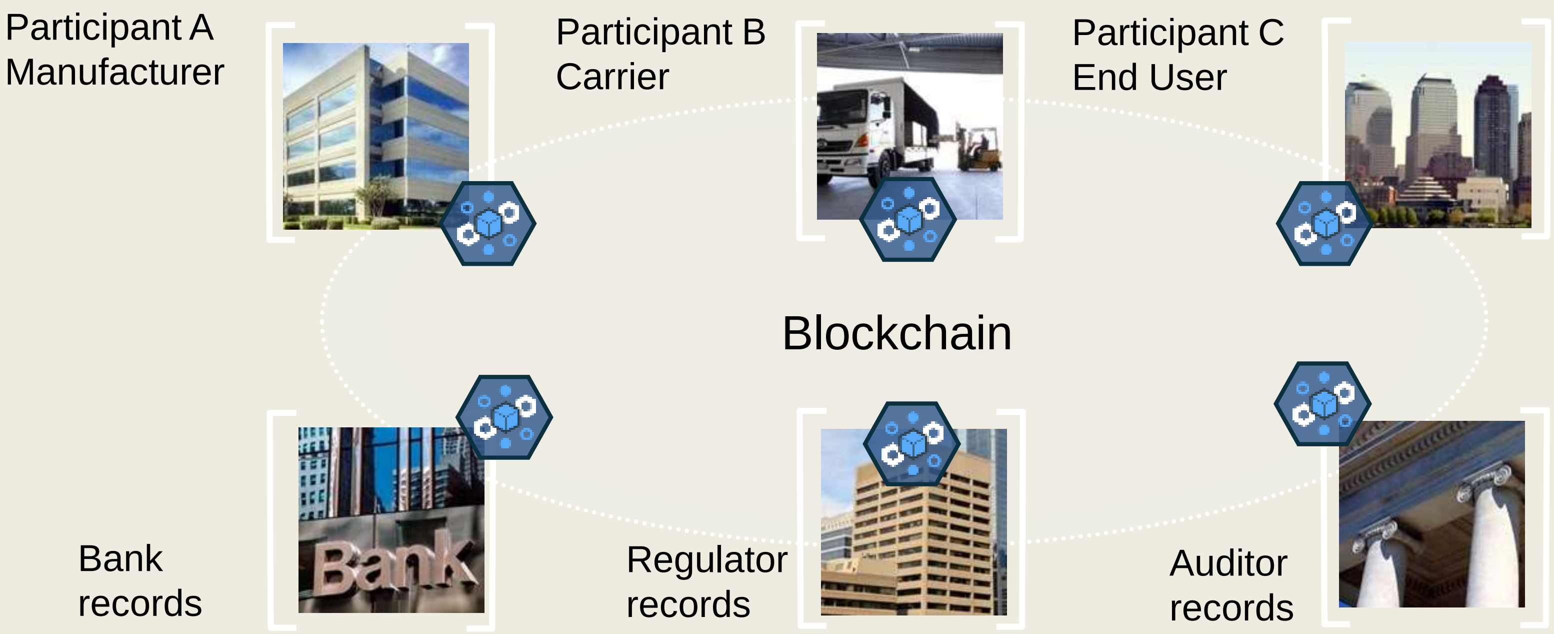
Bank records

Regulator records

Auditor records

Inefficient, Expensive, Vulnerable

Solution: Shared, replicated, permissioned ledger …



Participant A
Manufacturer

Participant B
Carrier

Participant C
End User

Blockchain

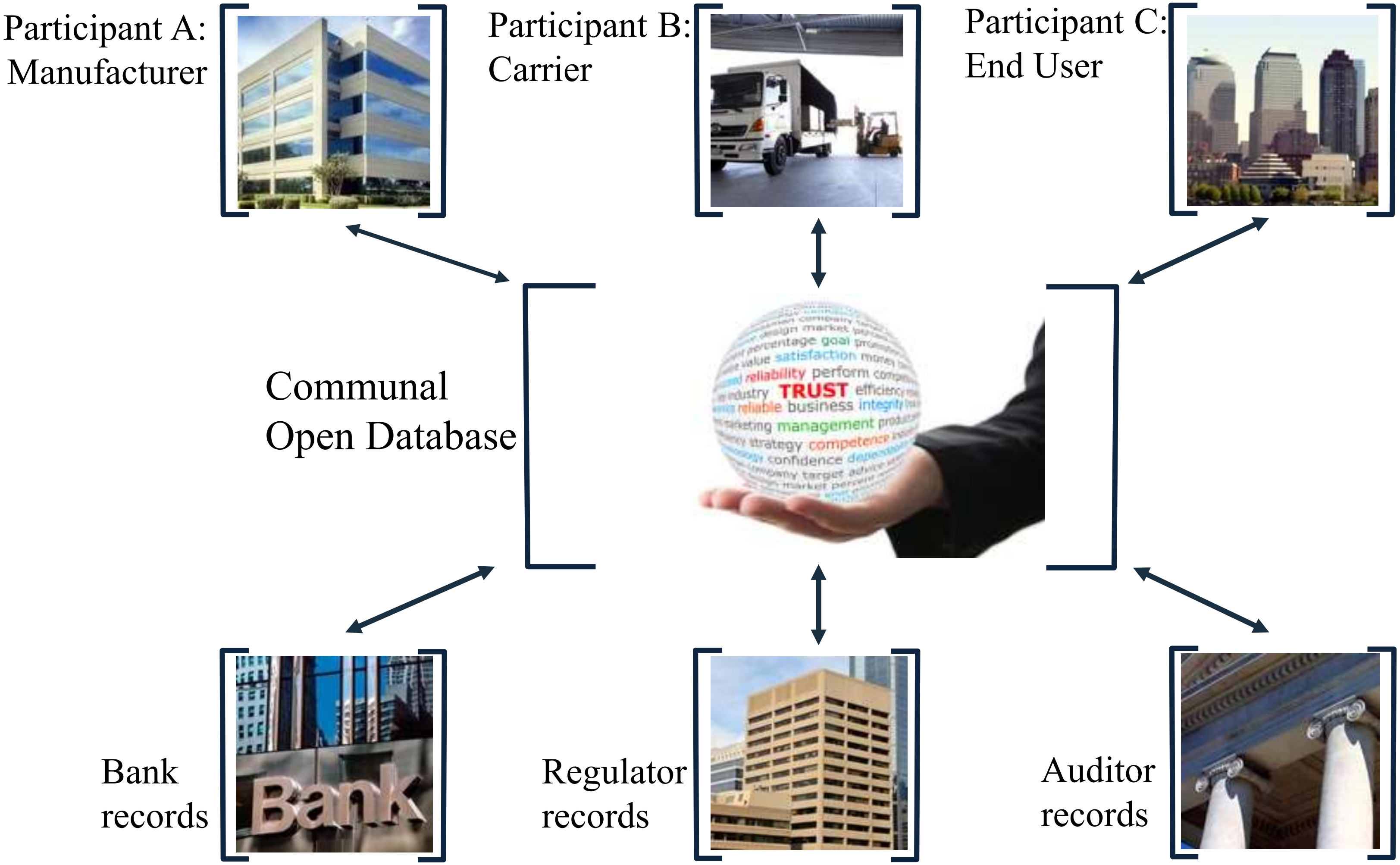
Bank
records

Regulator
records

Auditor
records

… with consensus, provenance, immutability and finality

Client-Server Model with Communal Database



Participant A:
Manufacturer

Participant B:
Carrier

Participant C:
End User

Communal
Open Database

Bank
records

Regulator
records

Auditor
records