



# DEMYSTIFYING THE BLOCKCHAIN

NCJA, Fort Worth, July 24, 2018

Kay Chopard Cohen  
Iveta Topalova



**Blockchain  $\neq$  Bitcoin**

# Definitions

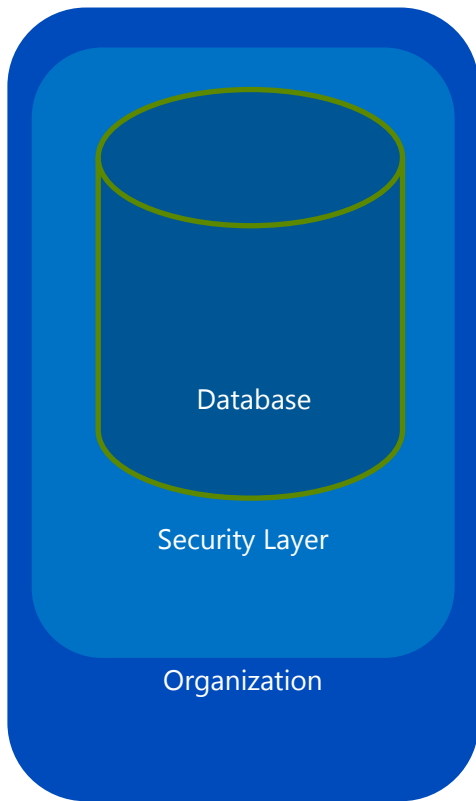
---

- A Blockchain is a secure, digital, distributed ledger that uses public/private signature technology to validate and record transactions in real-time.
- Blockchain = anything of value, where duplicates matter: money, ideas, music, art, land, identity (my 'background' check / record / identity), promises (contracts)
- “The first native digital medium for value, just as the internet was the first native digital medium for information.”—Don and Alex Tapscott | HBR

**A Blockchain can be described as a secure, immutable, sharable spreadsheet in the cloud!**

# Today Data is the Center of Gravity

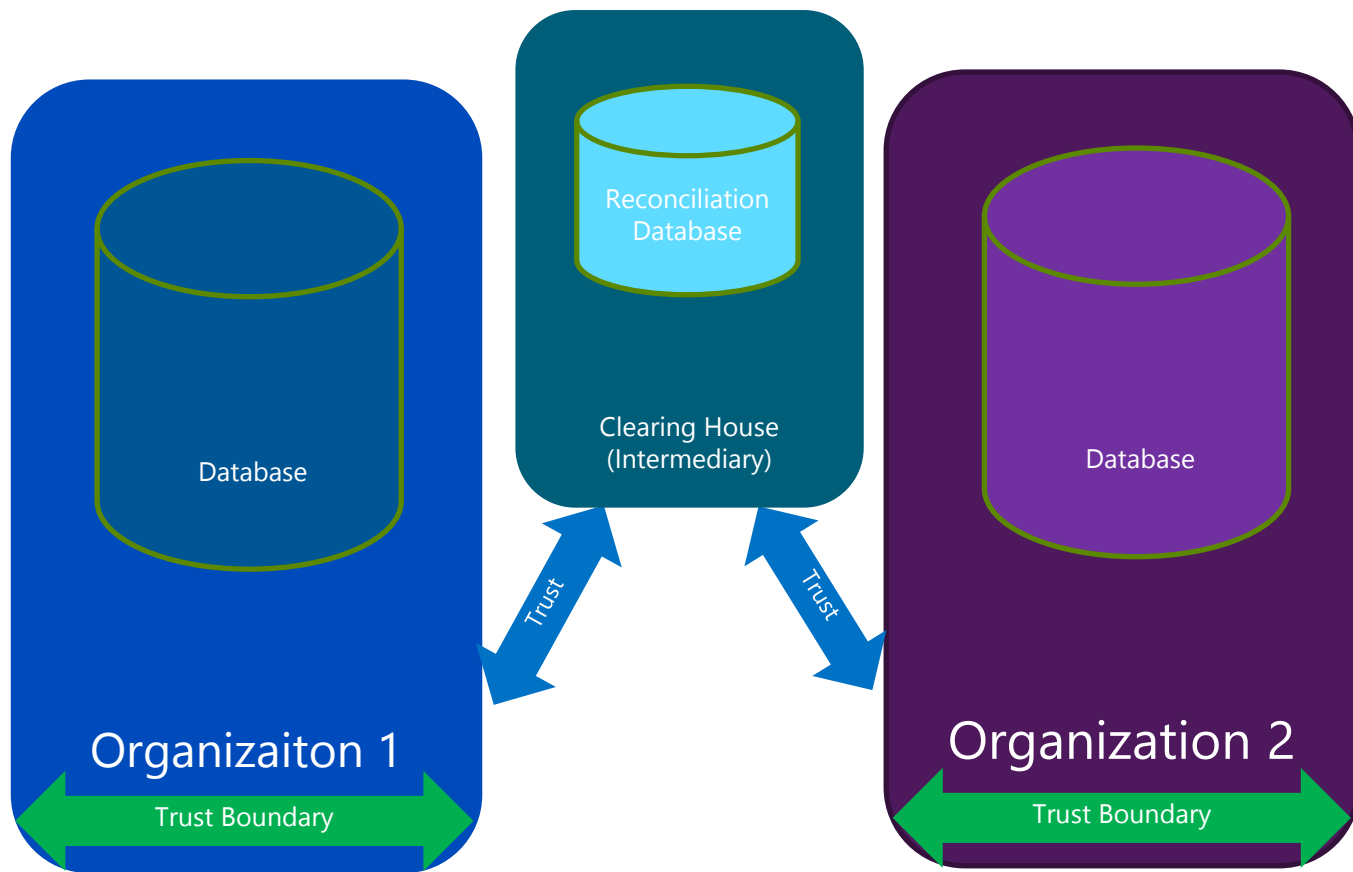
---



- We store all of our key information in databases as records in a container.
- We invest a lot of money to surround these databases with layers of security.
- If a cyber attack can penetrate these layers, typically that would expose all of the information.

# Traditional Information Exchange Transaction

---



## Challenges

Slow Processing

Everyone has their own database

High risk of errors

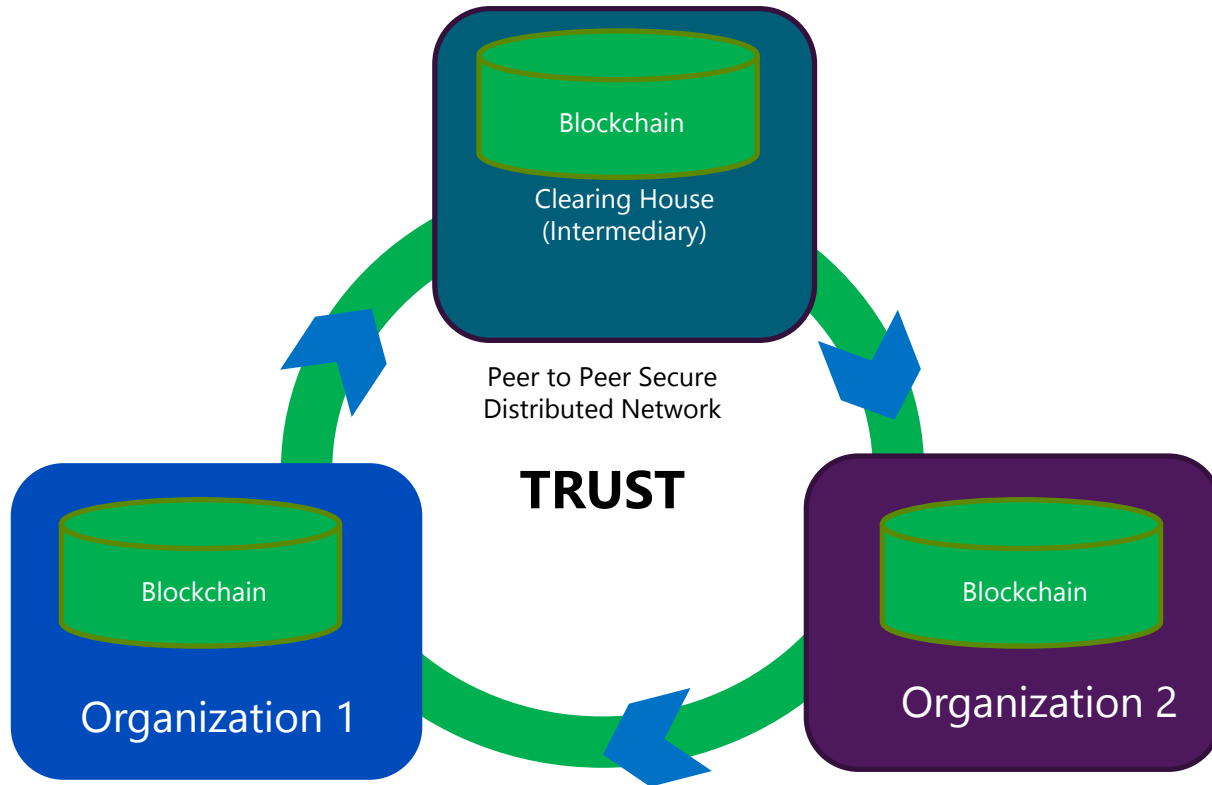
Security

High Compliance Overhead

# What if?

---

Everyone could have a 'Single Version of the Truth'



## Attributes

Trust

Shared

Tamper Proof

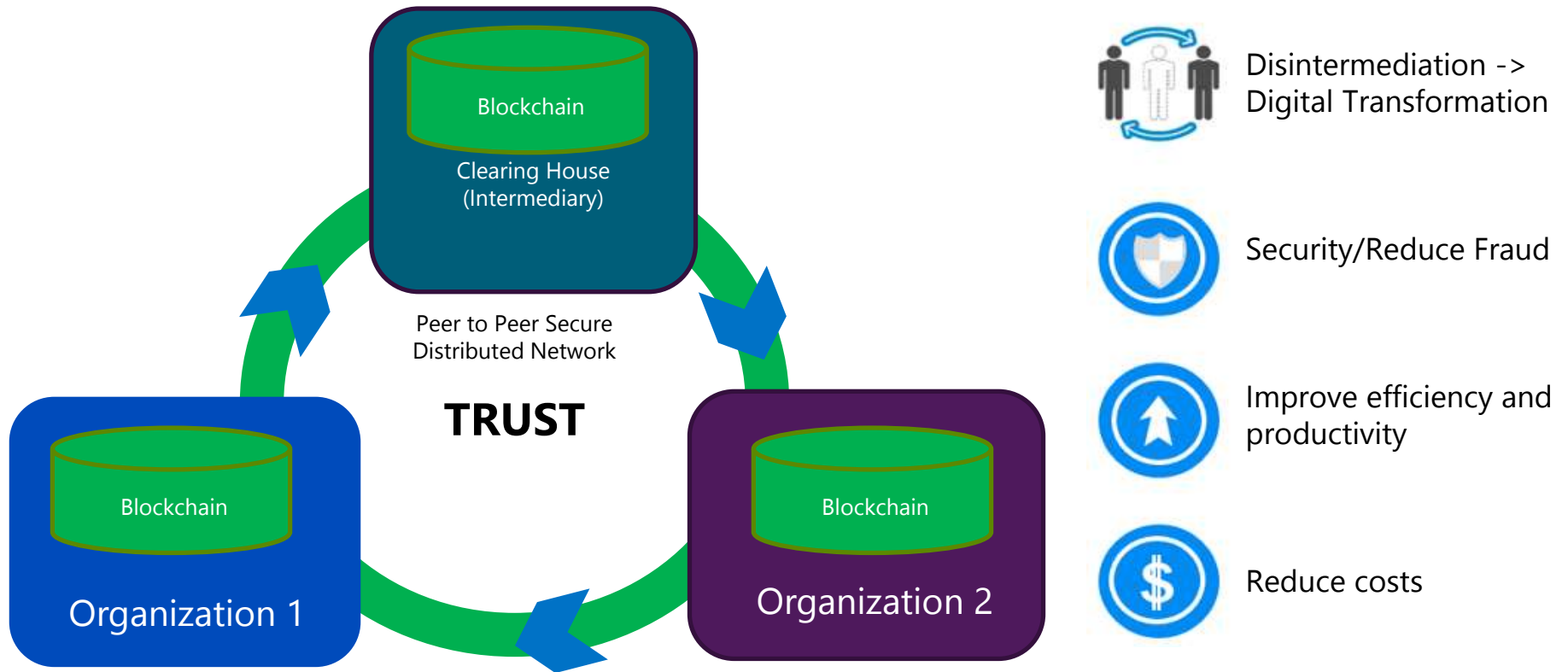
Security

Traceability

# What if?

---

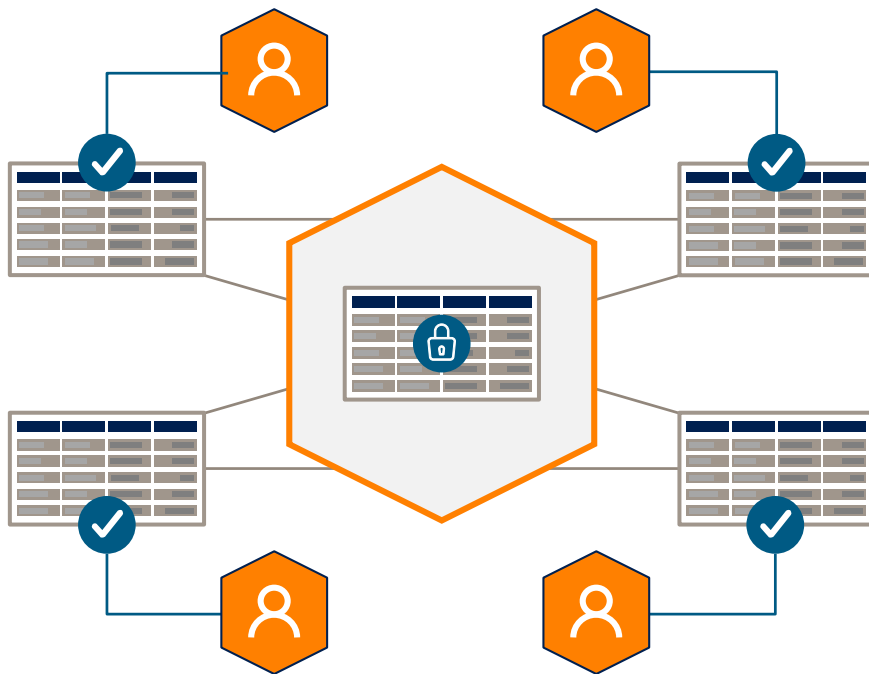
We can take Intermediaries out of the process?





# Blockchain establishes a secure, shared source of truth

---

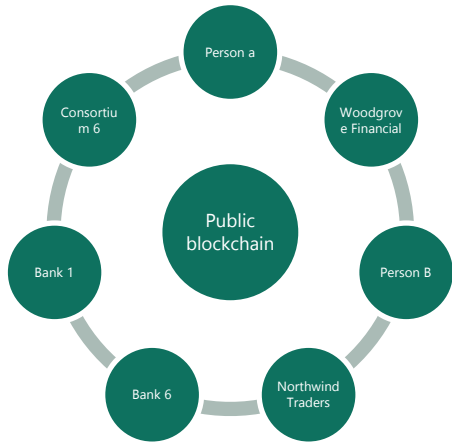


- | Data is stored in a ledger— a record of every transaction
- | Everyone in the network has an individual, identical copy
- | The ledger can only be updated by network consensus, and information can't be altered or deleted without the knowledge of the whole network.

# Types of Blockchain Networks

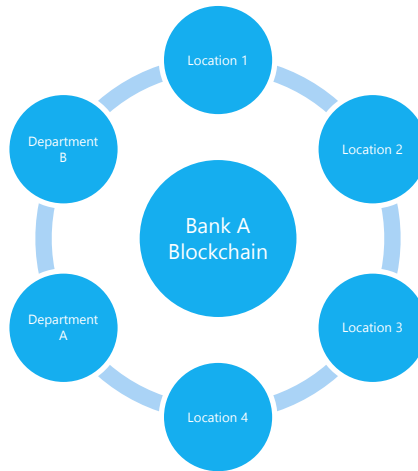
---

## Public



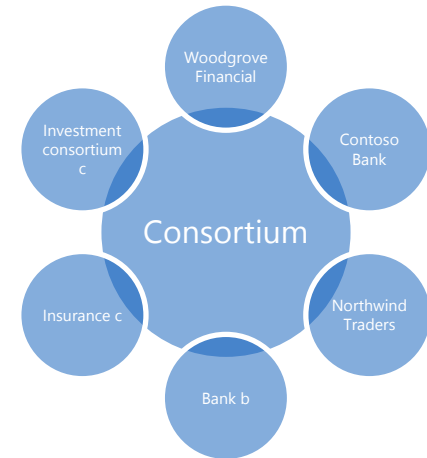
- Many, unknown participants
- Writes by all participants
- Reads by all participants
- Consensus by Proof of Work

## Private



- Known participants from one org
- Write permissions centralized
- Reads may be public or restricted
- Multiple algorithms for consensus

## Consortium



- Known participants from multiple orgs
- Writes require consensus of n participants
- Reads may be public or restricted
- Multiple algorithms for consensus

# Smart Contracts

- Smart Contracts are objects available on some blockchains (Ethereum)
- They allow agreements between parties to be reduced to code, variables and properties, that can be published to a blockchain
- Promising for multi-party contracts, and processes

YEAR	2007	MAKE	FORD	MODEL	Focus ZX4 S	VIN	45045
USED	21K484						
<p>The dealer here "has sold" the title to the credit lender at the closing, as is usual in this contract. We will pay the motor vehicle described above on credit. The annual percentage rate is 7.99% (variable) or 9.99% (fixed) (whichever is the better rate) in order to be fully disclosed to you. This rate is subject to change in the future. We are not responsible for all or part of this contract. SEE OTHER PAPERS FOR ADDITIONAL TERMS AND CONDITIONS.</p>							
ANNUAL PERCENTAGE RATE:		FINANCE CHARGE		Amount			
21.99%		\$2,853.34		The cost of your credit in a year's time.			

B.	YOUR PAYME
Number of Payments:	Amount of Pa
One Payment of	\$500.00
One Payment of	
One Payment of	
47	\$156.83
One final payment	

C.  
**SECURITY:** You are giving a security interest. any payment is more than 10 days late you r  
**PRE-PAYMENT:** If you pay early, you may be contract for any additional information abou the scheduled date and prepayment refund:

  
 David K. Sullivan  
 [Signature]  
 [Signature]

Smart Contract Package`

Variable

Percentage Rate

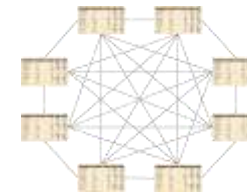
Payment Amount

Static

Signatures	Assets or Security
Payment Date	Amount Financed
Late Date	Term
Total Sale	

Monthly Payment	Interest Rate	Term
Monthly Payment	Interest Rate	Term
Late Fee	Late Fee	Late Fee
Term	Total Sale	Term

Date	Payment	Late Fee
12/1/2019	\$500.00	30
1/1/2020	\$500.00	30



# Considerations

---

## **Appropriateness**

- Right technology for the right scenario
- Alternative technologies

## **Cost**

- Environmental impact
- Complexity

## **Performance/Scale**

## **Immutability**

- 'Write Only'
- No delete or update

## **Policy / Regulatory**

- Time to market
- Sharing data across states
- Data retention

## **Stakeholder Engagement**

- Usability
- Change management

## **Interoperability**

## **Security and Privacy**

# What are the Opportunities in Justice

---

- Criminal History, Prosecution and Disposition Matching
- Expediting Protection Orders Execution
- Securing Chain of Custody for Digital Evidence
- Recognizing illegal transactions conducted as part of standard processes
- Decentralized Data and Analysis
- Availability of Historic Data

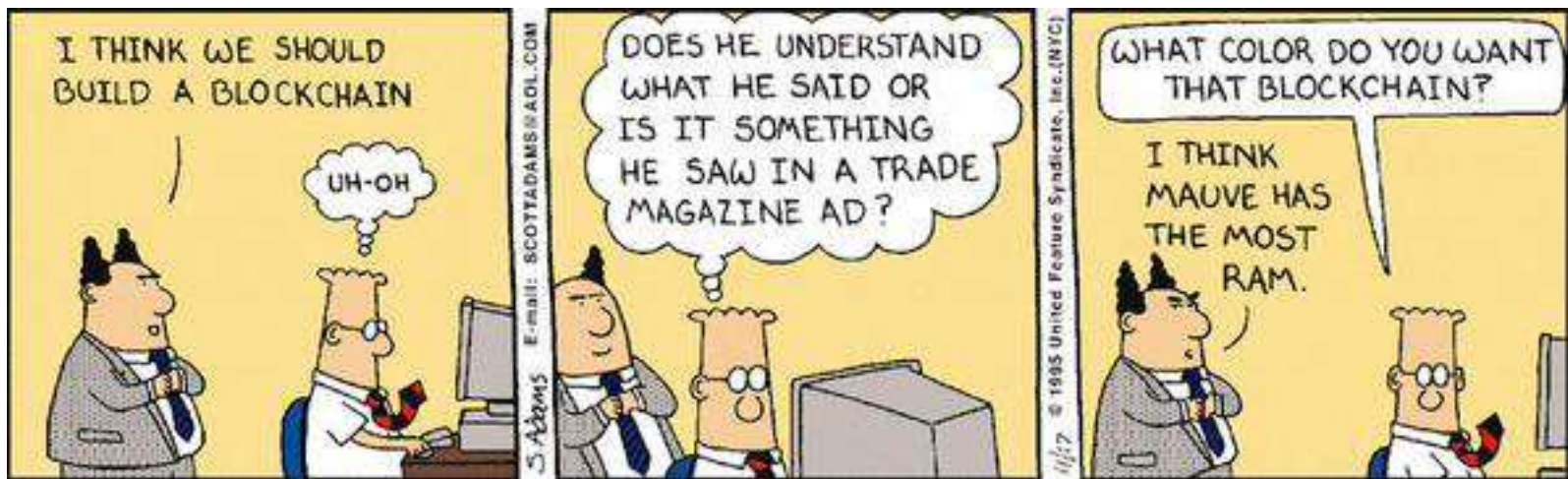
## What is Next

---

- Digital assets: validation of associated metadata and transactions
- Arrest warrants: issue to dissemination
- Protection orders: issue to dissemination
- Criminal history: disposition recording
- Criminal history: validation of data as part of dissemination
- Law enforcement: sharing of officer testing and certification
- Dispatch: resource sharing between agencies
- Information sharing: API for digital notarization of documents
- Law enforcement: interagency de-confliction

# Blockchain—so what?

---



# In Summary

---

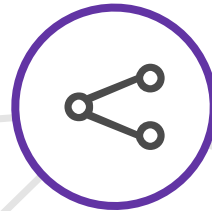
## Secure and Transparent

Uses cryptography to create transactions that are impervious to fraud and establishes a shared truth as well as real time transparency and auditability.



## Shared

Blockchain value is directly linked to the number of organizations or companies that participate in them. That creates a system with no single point of failure.



## Ledger

The database is "write once" so it is an immutable and programable record of every transaction that occurs.



## Distributed Consensus

There are many replicas of the blockchain database. In fact, the more replicas there are the more authentic it becomes.

