BLOCKCHAIN
What, Why, Who, When, Where, How

Hồ Tường Vinh
ho.tuong.vinh@gmail.com

Agenda

- What is Blockchain?
- Why to use Blockchain?
- How to implement Blockchain?
- When to use Blockchain?
- Where to use Blockchain?
- Who involves in Blockchain solution?

Notices

This document is created by compilation from various information sources for educational purposes

Digital World

Asset

Anything that is capable of being owned or controlled to produce value, is an asset.

Tangible Assets:

Asset that has a physical form
E.g Machinery, Buildings and Land

Intangible Assets:

Asset that is not physical in nature

- Financial, e.g. bond
- Intellectual, e.g. patents
- Digital, e.g. music

Participants, Transactions & Contracts

Participants, Transactions & Contracts

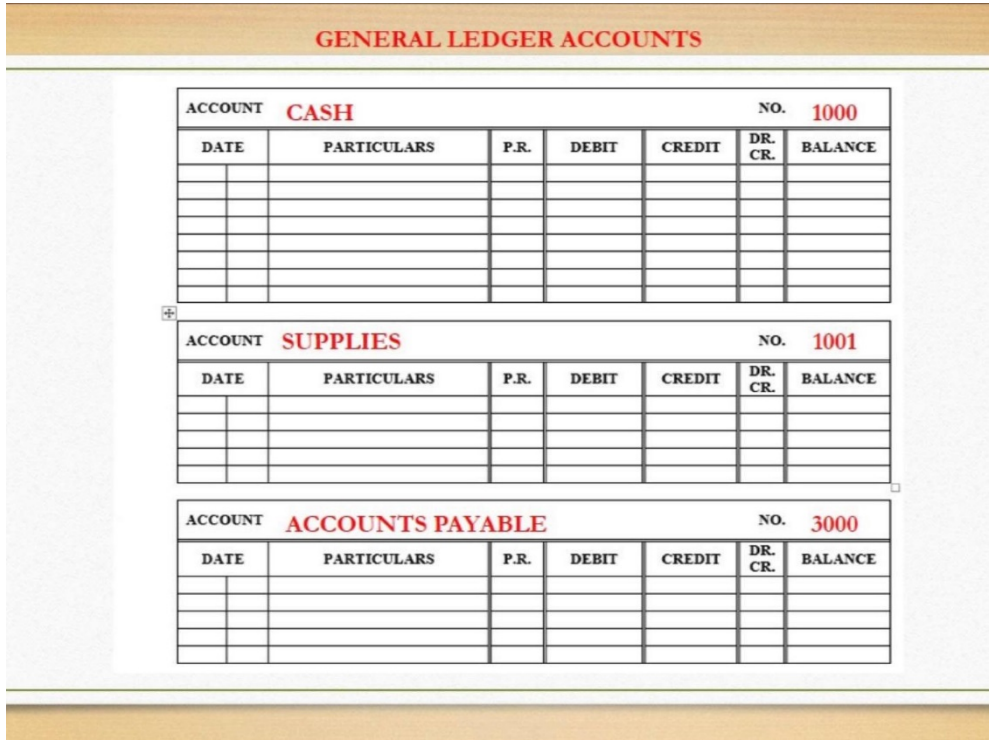
What?

- Participants - members of a business network
  - Customer, Supplier, Government, Regulator
  - Usually resides in an organization
  - Has specific identities and roles
- Transaction - an asset transfer
  - John gives a car to Anthony (simple)
- Contract - conditions for transaction to occur
  - If Anthony pays John money, then car passes from John to Anthony (simple)
  - If car won't start, funds do not pass to John (as decided by third party arbitrator) (more complex)

Ledger

A principal book (or computer file) for recording asset transfer between participants.

Ledger to keep Records



GENERAL LEDGER ACCOUNTS

ACCOUNT CASH NO. 1000

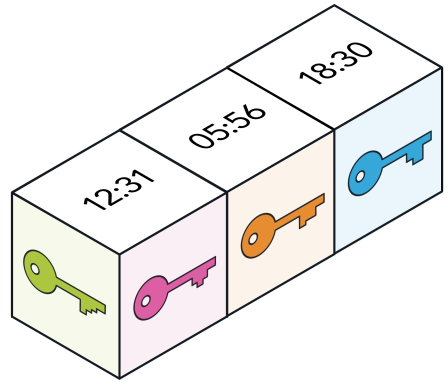
DATE	PARTICULARS	P.R.	DEBIT	CREDIT	DR. CR.	BALANCE

ACCOUNT SUPPLIES NO. 1001

DATE	PARTICULARS	P.R.	DEBIT	CREDIT	DR. CR.	BALANCE

ACCOUNT ACCOUNTS PAYABLE NO. 3000

DATE	PARTICULARS	P.R.	DEBIT	CREDIT	DR. CR.	BALANCE



What is Blockchain?

Blockchain is NOT Bitcoin

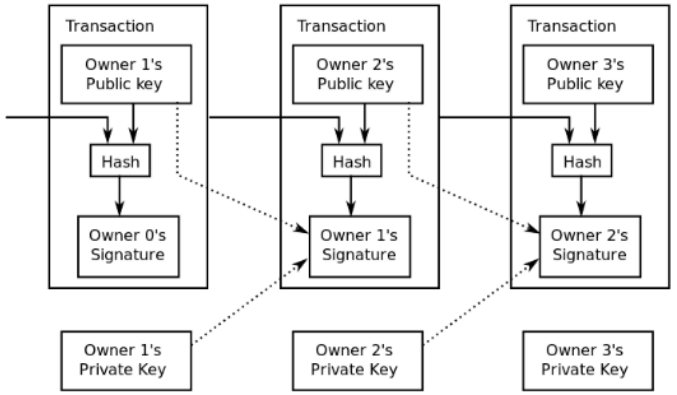
Blockchain underpins Bitcoin . . .

What?

1. bitcoin is unregulated, censorship-resistant shadow currency
2. Blockchain ensures “cash like” coin passing
   - unique,
   - immutable,
   - final
3. bitcoin the first Blockchain application
   - Blockchain is not bitcoin

4. Digital currencies different from cyptocurrency

bitcoin



Blockchain Business

Blockchain for Business

What?

Append-only distributed system of record shared across business network

Shared Ledger

Smart Contract

Business terms embedded in transaction database & executed with transactions

Ensuring appropriate visibility; transactions are secure, authenticated & verifiable

Privacy

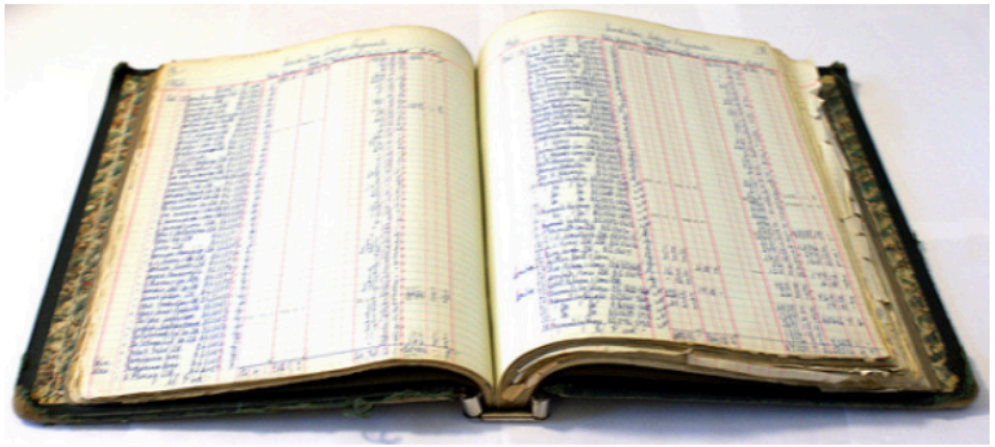
Validation

All parties agree to network verified transaction

Broader participation, lower cost, increased efficiency

Shared Ledger

What?



- Records all transactions across business network
- Shared between participants
- Participants have own copy through replication
- Permissioned, so participants see only appropriate transactions
- THE shared system of record

Blockchain explained as Excel files

	A	B	C	D	E	F
1	Block No	Transaction Time		Transaction	Digital Fingerprint	Previous Block Fingerprint
2	1	2017-Aug-1 3:55:34 PM		(Genesis block)	gsb4z0bf3wbohnbfht8f	
3	2	2017-Aug-2 1:23:35 AM		American Dream purchased by John	iy8ca6e8uip2wo7h2d8z	gsb4z0bf3wbohnbfht8f
4	3	2017-Aug-3 5:45:40 AM		Fifth Harmony purchased by Steve	x1w4tzmwvin5vyzzkwt7	iy8ca6e8uip2wo7h2d8z
5	4	2017-Aug-4 2:25:34 AM		Life Changes purchased by Robert	fpej9w8fy7msljkrsyy6	x1w4tzmwvin5vyzzkwt7
6	5	2017-Aug-5 7:45:24 PM		Luv Is Rage 2 purchased by Timothy	ic2p6ruk6ub6sr6mln1l	fpej9w8fy7msljkrsyy6
7	6	2017-Aug-6 1:52:04 AM		Sleep Well Beast purchased by Mike	639bcwfw9xa0u0i5uzri	ic2p6ruk6ub6sr6mln1l
8	7	2017-Aug-7 9:54:05 PM		Slowheart purchased by Jesse	1gcifrjtqbkz66jh3nig	639bcwfw9xa0u0i5uzri
9	8	2017-Aug-8 8:53:40 AM		Life Changes purchased by Noah	bp6zs6fw5pyyiur2tl60	1gcifrjtqbkz66jh3nig
10	9	2017-Aug-9 11:07:39 PM		Fifth Harmony purchased by Mike	ft616h0ezoq987rfjhzf	bp6zs6fw5pyyiur2tl60
11	10	2017-Aug-10 3:51:01 AM		Evolve purchased by Patrick	0g7scv7ehy8tmczvh4xo	ft616h0ezoq987rfjhzf

- A blockchain is quite literally a chain of blocks.
- Blocks contain data and in our spreadsheet a block is represented by a single row.
- The very first row is called the starting or genesis block.
- The second row/block is attached to the first row.
- The third row/block is attached to the second row and so on and so forth.
- Every new row/block added to the sheet has to reference the row before it.
- This forms the chain in the blockchain.

https://www.linkedin.com/pulse/blockchain-businessperson-rammohan-raja/

Blockchain explained as Excel files

A	B	C	D	E	F
Block No	Transaction Time		Transaction	Digital Fingerprint	Previous Block Fingerprint
1	2017-Aug-1 3:55:34 PM		(Genesis block)	gsb4z0bf3wbohnbfht8f	
2	2017-Aug-2 1:23:35 AM		American Dream purchased by John	iy8ca6e8uip2wo7h2d8z	gsb4z0bf3wbohnbfht8f
3	2017-Aug-3 5:45:40 AM		Fifth Harmony purchased by Cyber Criminal	aijk1rqi5f8mmv9t9ns6	iy8ca6e8uip2wo7h2d8z
4	2017-Aug-4 2:25:34 AM		Life Changes purchased by Robert	gqwhamdn2mjgicbr4tej	aijk1rqi5f8mmv9t9ns6
5	2017-Aug-5 7:45:24 PM		Luv Is Rage 2 purchased by Timothy	afc0nnbroq2qn2gdtn5v	gqwhamdn2mjgicbr4tej
6	2017-Aug-6 1:52:04 AM		Sleep Well Beast purchased by Mike	1jar7waq6wh23l23cazb	afc0nnbroq2qn2gdtn5v
7	2017-Aug-7 9:54:05 PM		Slowheart purchased by Jesse	5m40crqmgtdsa9x2co0w	1jar7waq6wh23l23cazb
8	2017-Aug-8 8:53:40 AM		Life Changes purchased by Noah	4zplopu7ms9k7b2die3r	5m40crqmgtdsa9x2co0w
9	2017-Aug-9 11:07:39 PM		Fifth Harmony purchased by Mike	e4tkvlv84t5qed3b1g14	4zplopu7ms9k7b2die3r
10	2017-Aug-10 3:51:01 AM		Evolve purchased by Patrick	czpbx3mdxu4vfogyxgcz	e4tkvlv84t5qed3b1g14

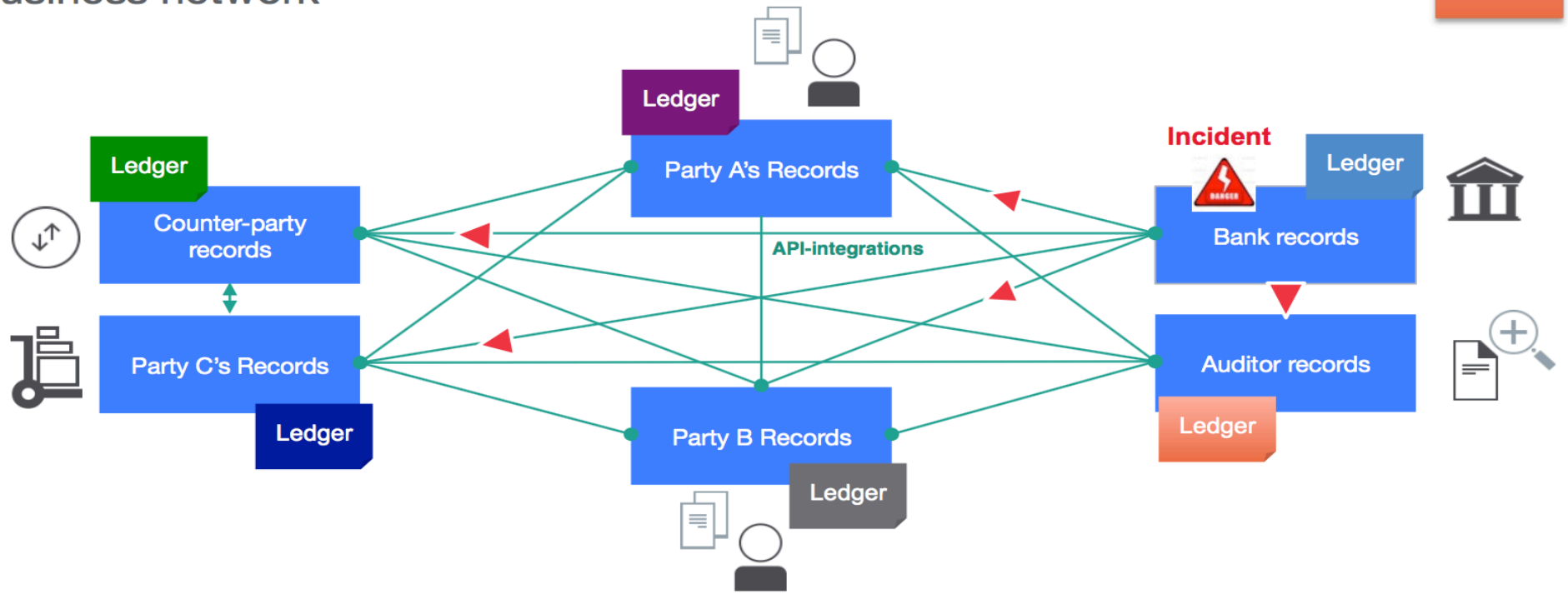
- To keep all copies of the blockchain up to date, each entity who adds a row/block to the spreadsheet is then required to tell the others to also add this new row/block to their own copy of the spreadsheet.
- When a new row is added in this hacked spreadsheet it will use a different Previous Block Fingerprint.
- Now when other organizations/individuals are notified to add this new row they can reject the new block as it is not consistent with other copies.
- This is one of the ways blockchain provides security against data alterations.

https://www.linkedin.com/pulse/blockchain-businessperson-rammohan-raja/

Problem without Shared Ledger

Problem - Difficult to monitor asset ownership and transfers in a trusted business network

What?

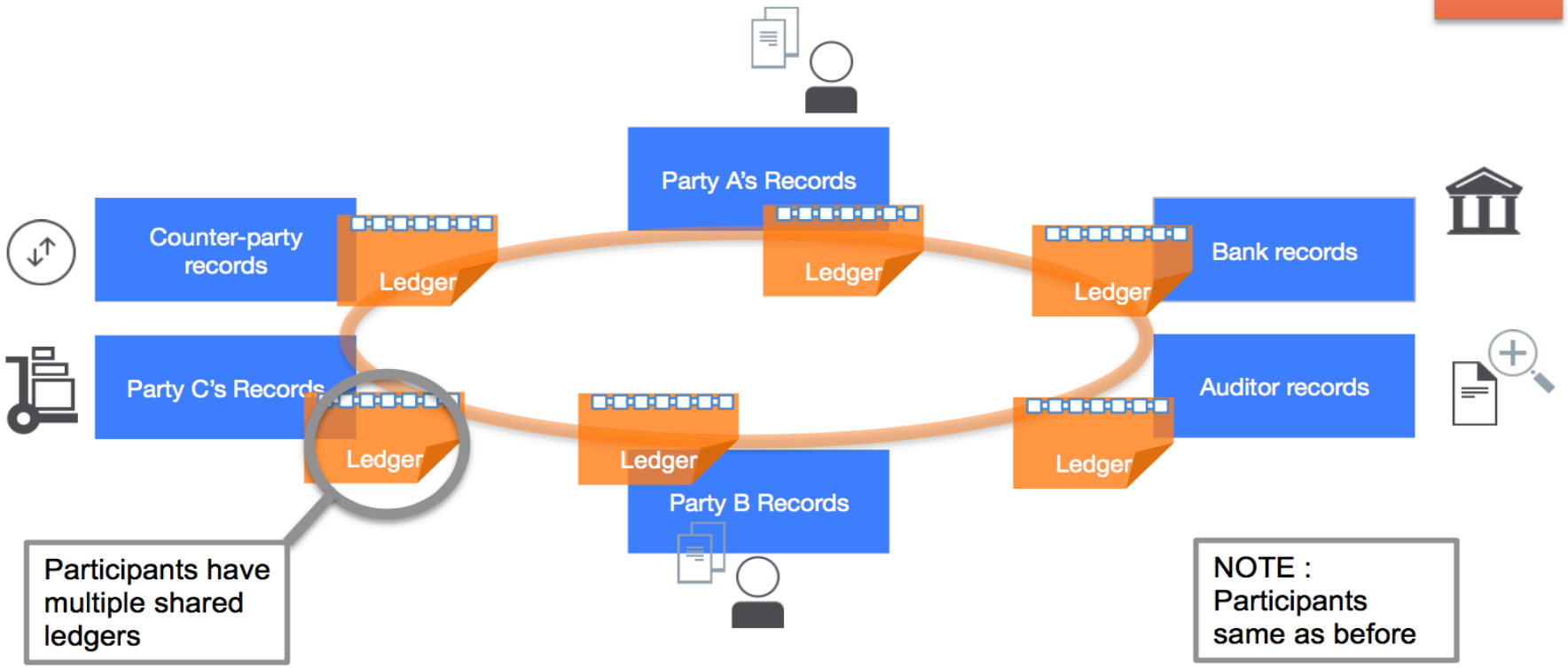


Inefficient, expensive, vulnerable

Solution with Blockchain

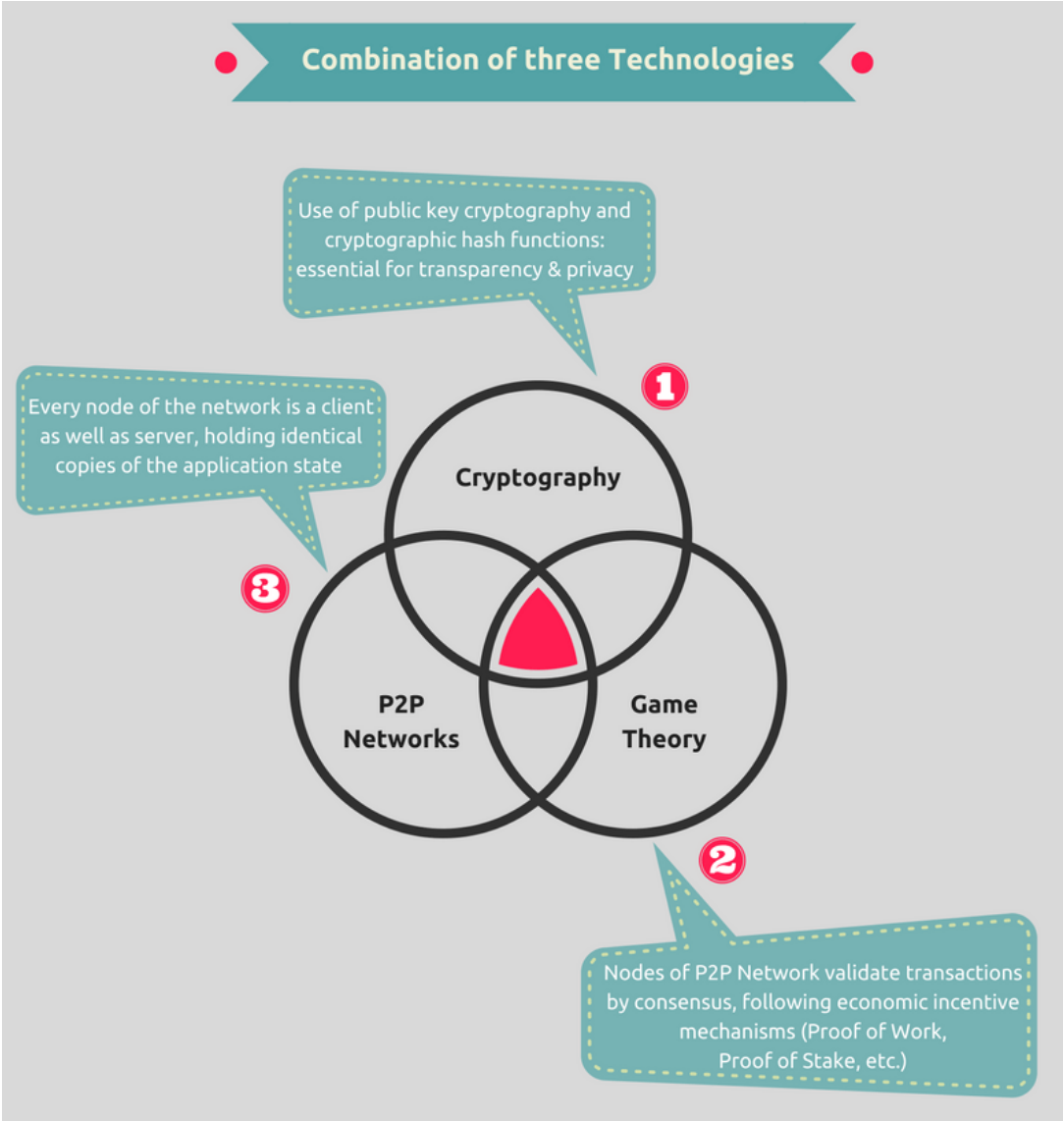
Solution – a permissioned, replicated, shared ledger

What?



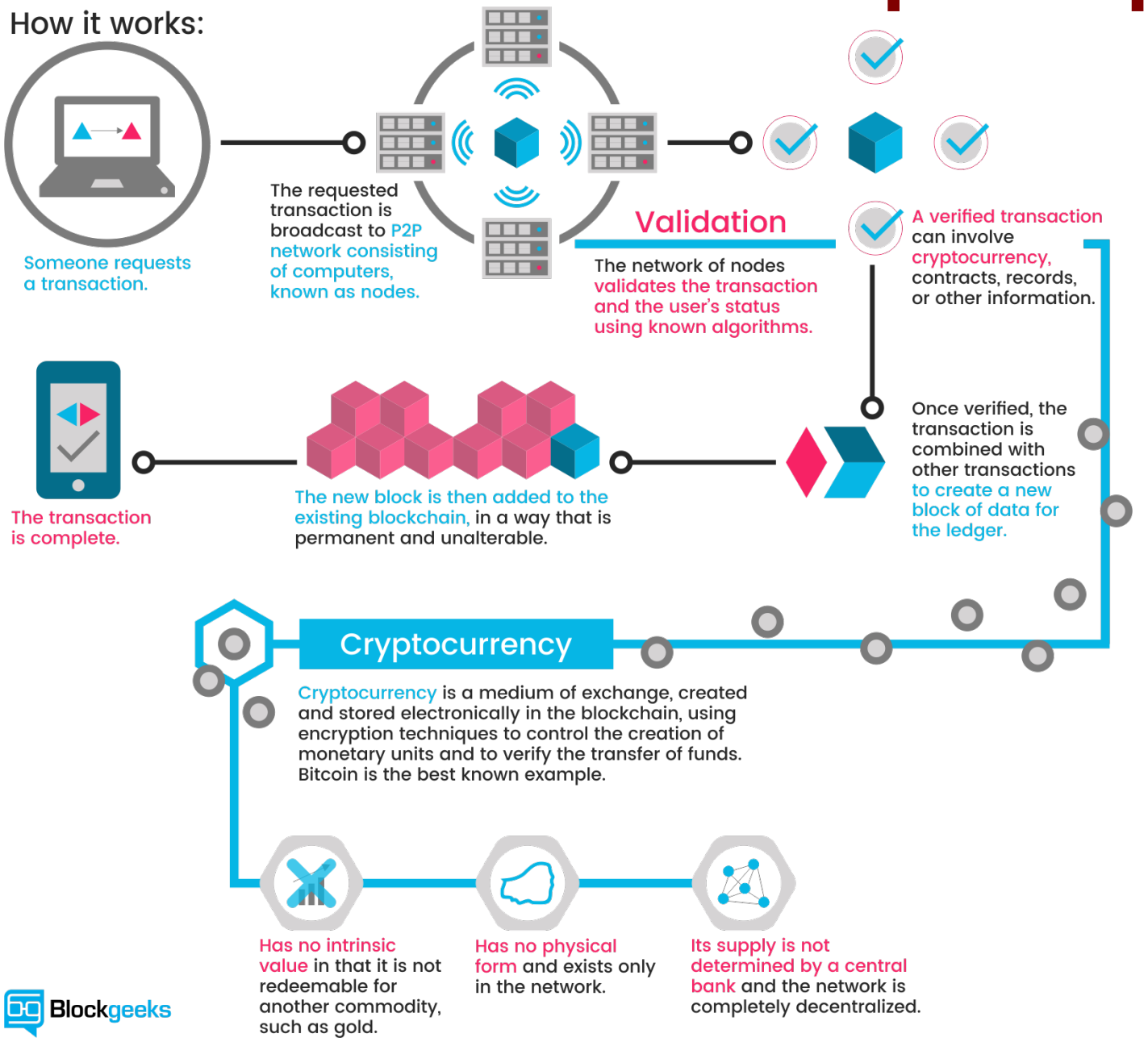
Consensus, provenance, immutability, finality

Blockchain: a combination of 3 technologies



https://blockchainhub.net/blog/infographics/what-is-a-blockchain/

Blockchain: a simple explaination

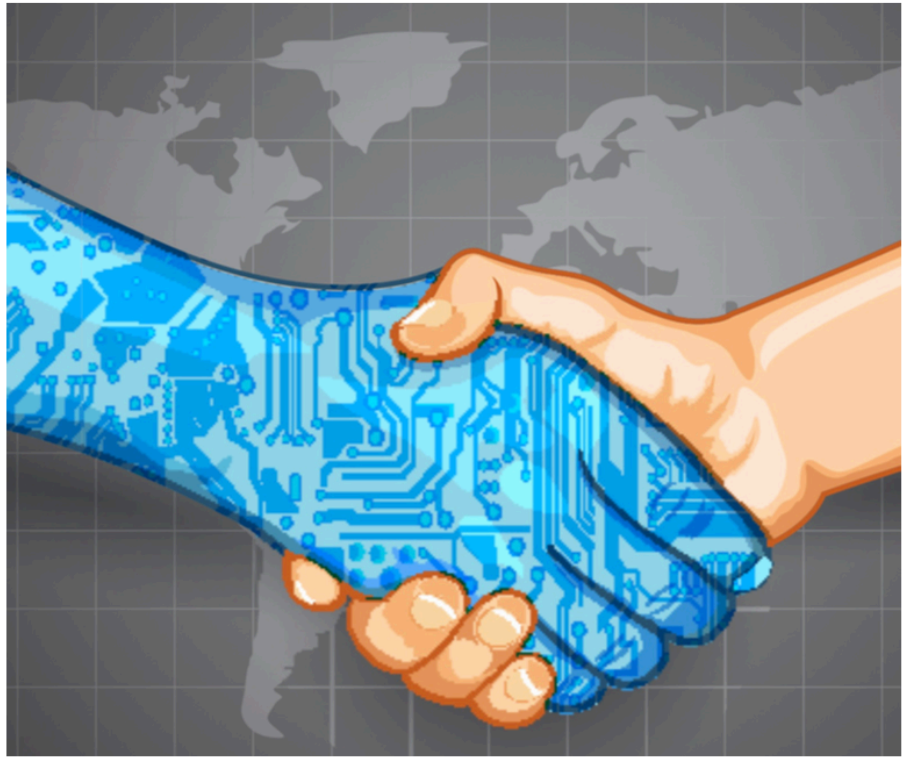


Blockgeeks

Smart Contract

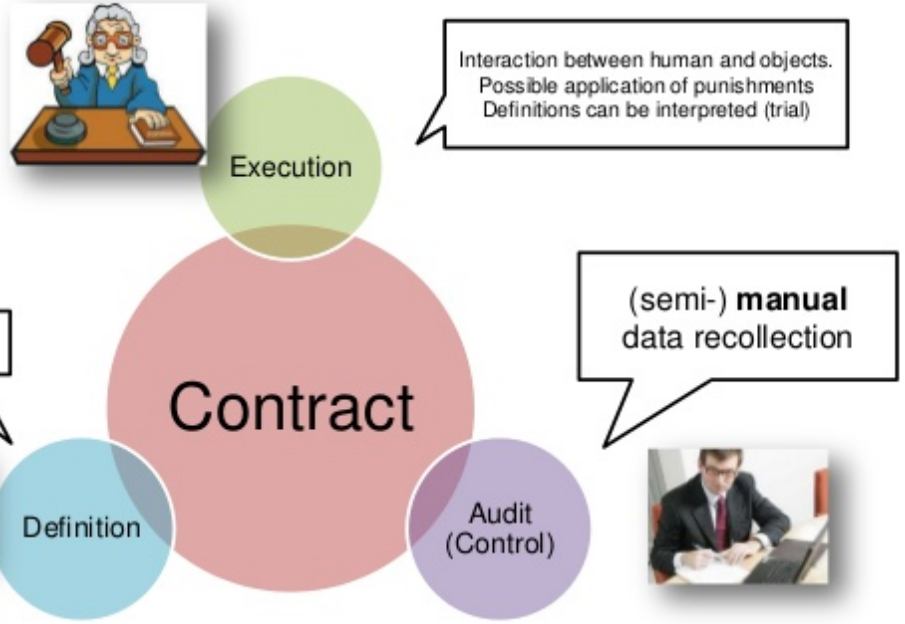
What?

- Business rules implied by the contract . .
- . . embedded in the Blockchain &
- executed with the transaction
- Verifiable, signed
- Encoded in programming language
- Example:
  - Defines contractual conditions under which corporate Bond transfer occurs



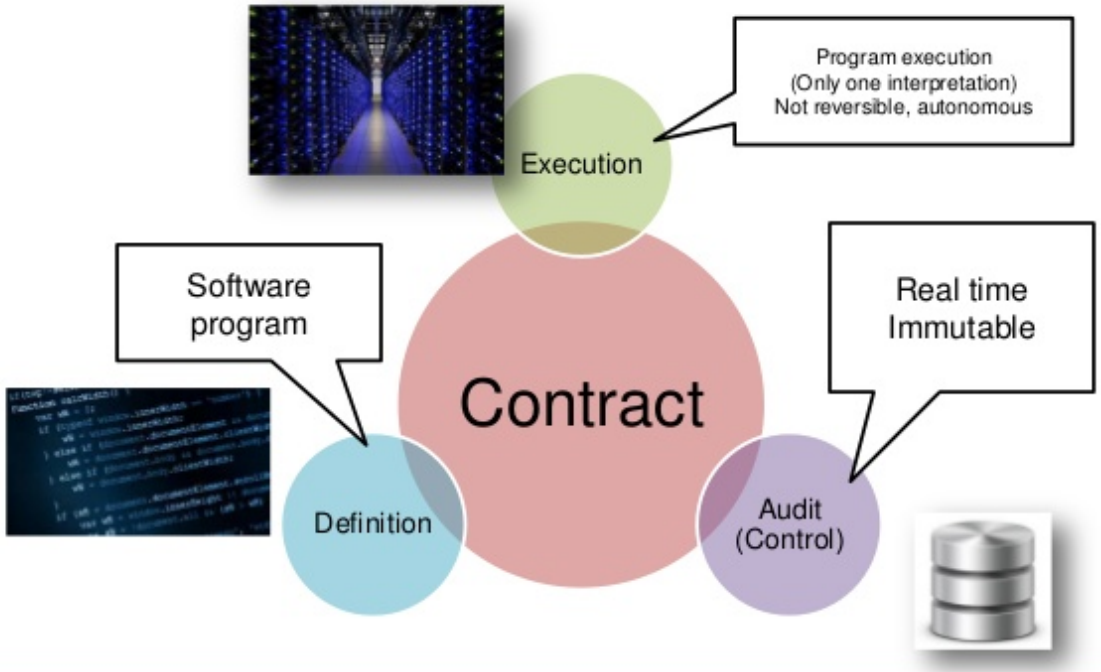
Smart Contract

«Traditional» contract



4

Smart contract



5

"Smart contract": is not really smart, should be "digital contract" because no AI applied.
Other name is "Chaincode".

https://www.slideshare.net/philippecamacho/smart-contracts

Smart Contract

Smart Contracts are Awesome!

Autonomy

1

You're the one making the agreement; there's no need to rely on a broker or lawyer

2

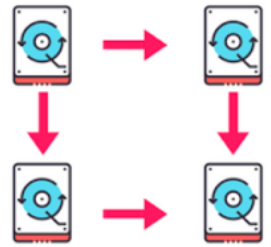
Trust

Your documents are encrypted on a shared ledger

Backup

3

On the blockchain,Your documents are duplicated many times over



4

Savings

Smart contracts save you money since they knock out the presence of an intermediary

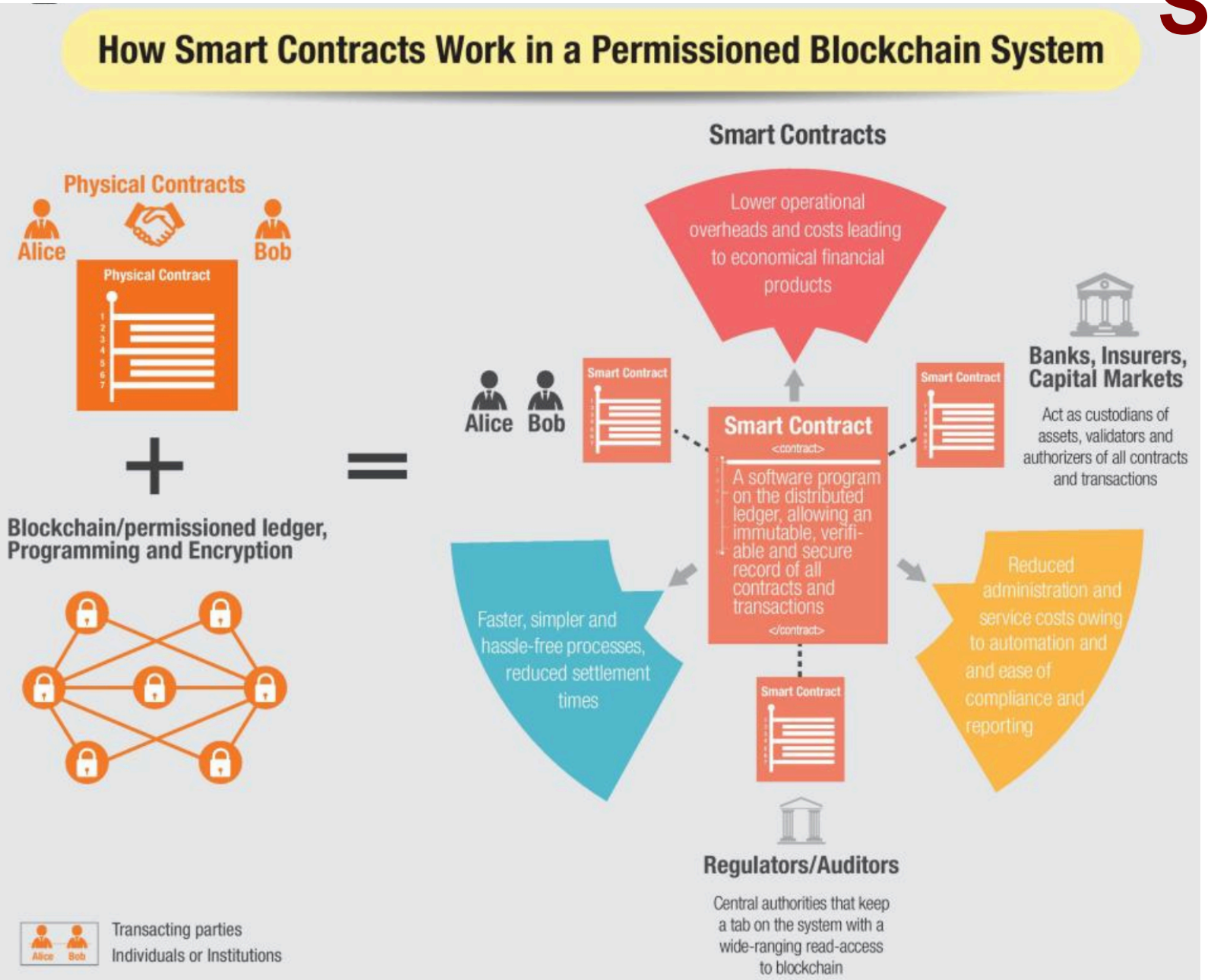
Accuracy

5

Smart contracts are not only faster and cheaper but also avoid the errors that come from manually filling out heaps of forms.

https://steemit.com/ethereum/@khalid177/what-is-ethereum-explained

Smart Contract



https://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts

Privacy

What?

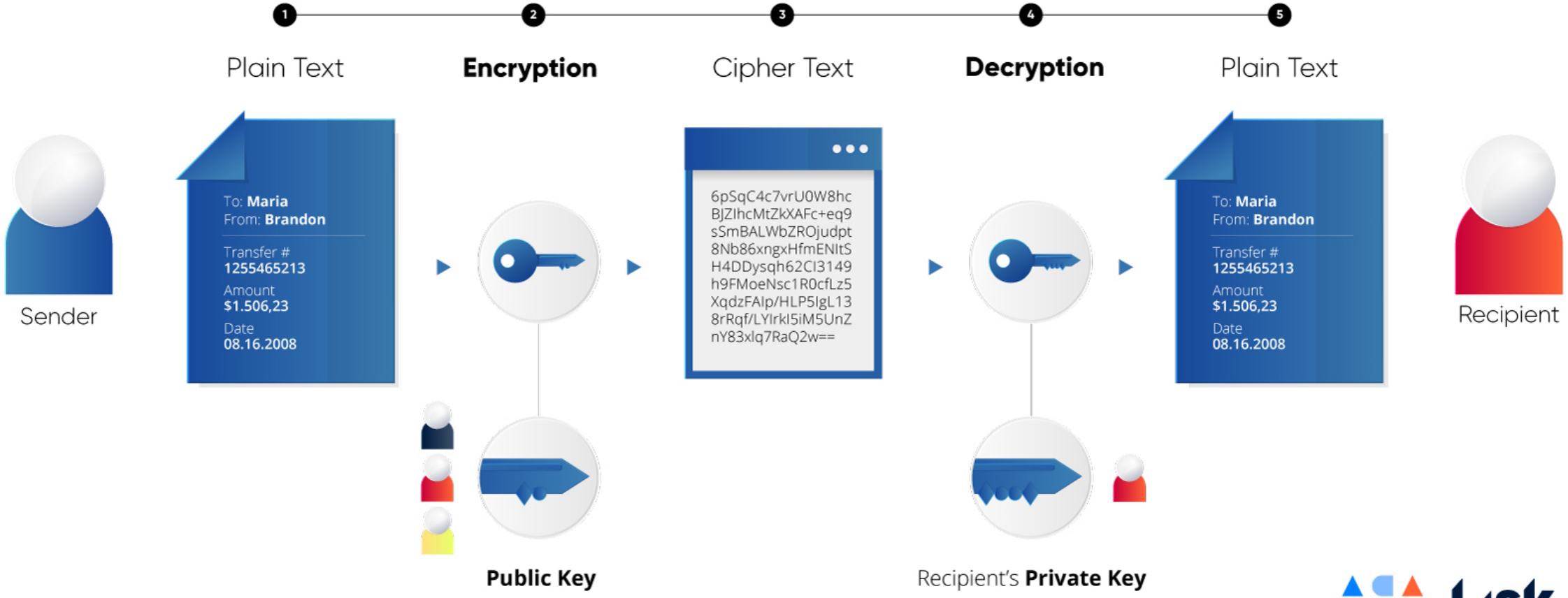
- Ledger is shared, but participants require privacy
- Participants need:
  - Transactions to be private
  - Identity not linked to a transaction
- Transactions need to be authenticated
- Cryptography central to these processes

Privacy

Public-key cryptography

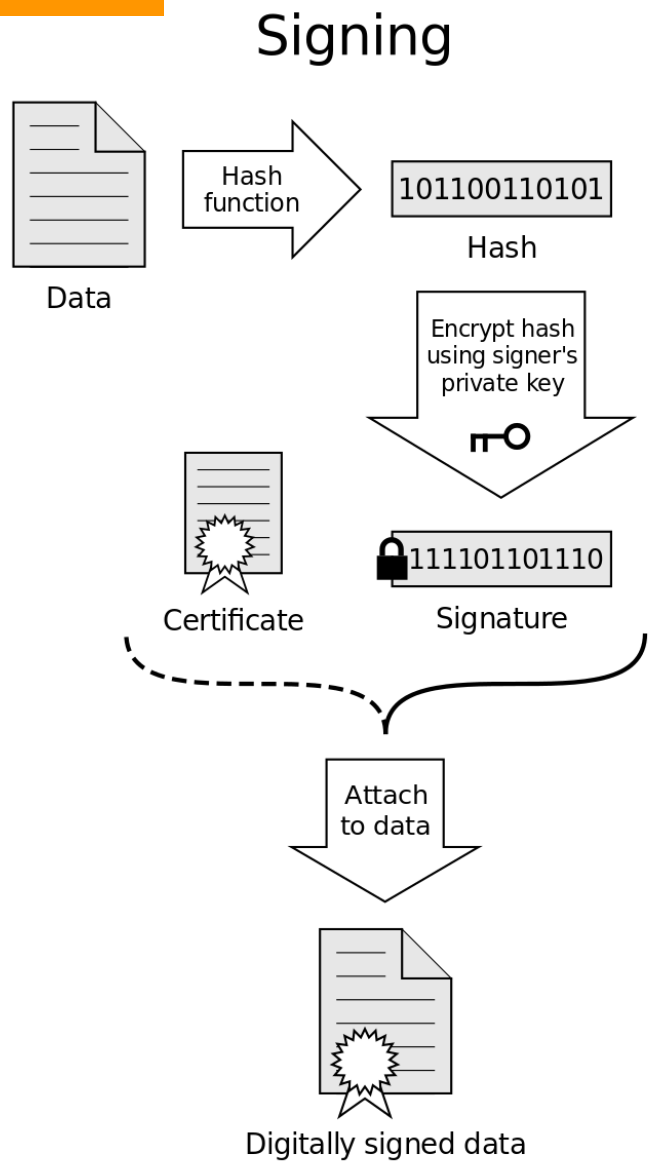
In blockchain, **cryptography** is primarily used for two purposes:

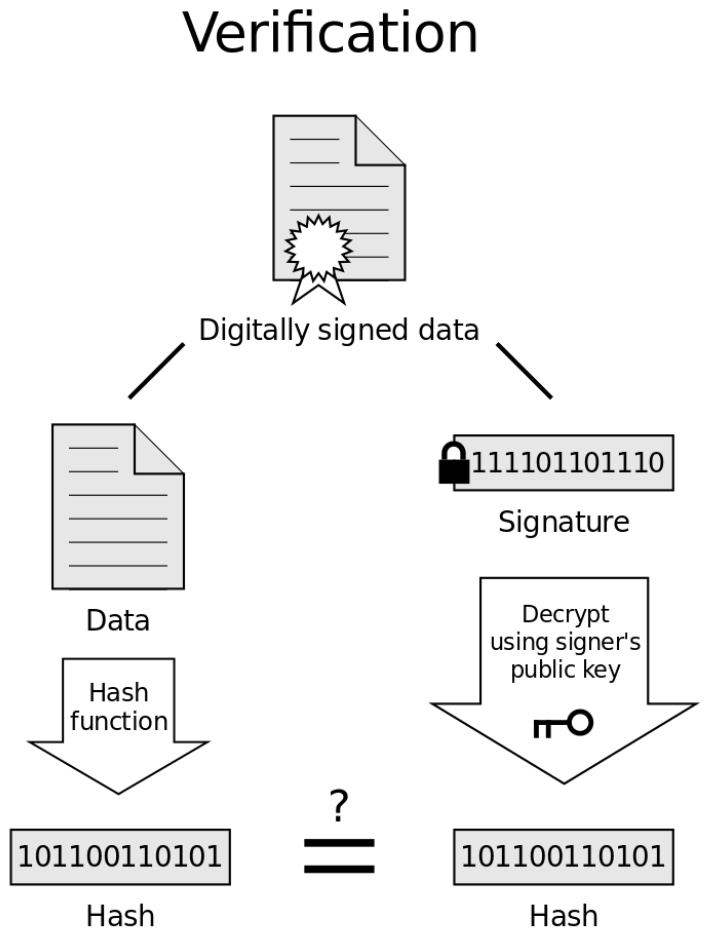
- Securing the identity of the sender of transactions (Digital signature)
- Ensuring the past records cannot be tampered with.



https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/blockchain-cryptography-explained

Digital Signature





Other ref: https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/digital-signatures

Validation is realized based on Consensus Protocols

Validation

What?

- Transaction verification & commitment
- When participants are anonymous
  - Commitment is expensive
  - bitcoin *cryptographic mining* provides verification for anonymous participants but at significant compute cost (proof of work)
- When participants are known & trusted
  - Commitment possible at low cost
- Multiple alternatives
  - proof of stake where fraudulent transactions cost validators (e.g. transaction bond)
  - multi-signature (e.g. 3 out of 5 participants agree)
- Industrial Blockchain needs "pluggable" consensus

Validation

Consensus Algorithms have Different Strengths and Weaknesses

Proof of work

Require validators to solve difficult cryptographic puzzles

PROs: Works in untrusted networks

CONS: Relies on energy use; slow to confirm transactions

Example usage: Bitcoin, Ethereum

Proof of stake

Require validators to hold currency in escrow

PROs: Works in untrusted networks

CONS: Requires intrinsic (crypto)currency, "Nothing at stake" problem

Example usage: Nxt

Proof of Elapsed Time

Wait time in a trusted execution environment randomizes block generation

PROs: Efficient

CONS: Currently tailored towards one vendor

Example usage: Sawtooth-Lake

Validation

Consensus Algorithms have Different Strengths and Weaknesses

Solo

Validators apply received transactions without consensus

PROs: Very quick; suited to development

CONS: No consensus; can lead to divergent chains

Example usage: Hyperledger Fabric V1

PBFT-based

Practical Byzantine Fault Tolerance implementations

PROs: Reasonably efficient and tolerant against malicious peers

CONS: Validators are known and totally connected

Example usage: Hyperledger Fabric V0.6

Kafka/
Zookeeper

Ordering service distributes blocks to peers

PROs: Efficient and fault tolerant

CONS: Does not guard against malicious activity

Example usage: Hyperledger Fabric V1

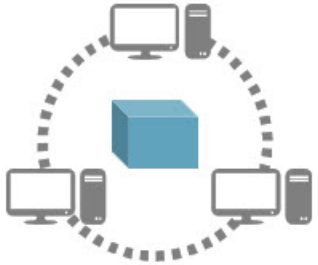
Public/Private Blockchain

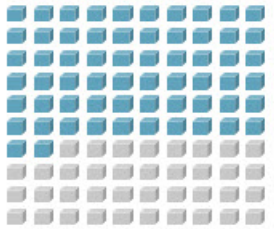
‘Public’ (Open) vs ‘Private’ (Closed) Blockchains: Generalized Features Comparison

	Public	Private
Access	Open read/write access to database	Permissioned read and/or write access to database
Speed	Slower	Faster
Security	Proof-of-Work/ Proof-of-Stake	Pre-approved participants
Identity	Anonymous/ pseudonymous	Known identities
Asset	Native assets	Any asset

Note: some features can vary form platform to platform.
Sources: Chain, Chris Skinner’s blog

Blockchain Process Steps





P2P Network ⇨ **Communication** ⇨ **Validation** ⇨ **Verification** ⇨ **Confirmation**

1

Someone in the Peer to Peer network requests a transaction.

2

The requested transaction is broadcast to the P2P network consisting of computers, known as nodes.

3

The network of nodes validates the transaction and the users status using algorithms.

A verified transaction can involve cryptocurrency, contracts, records or other information.

4

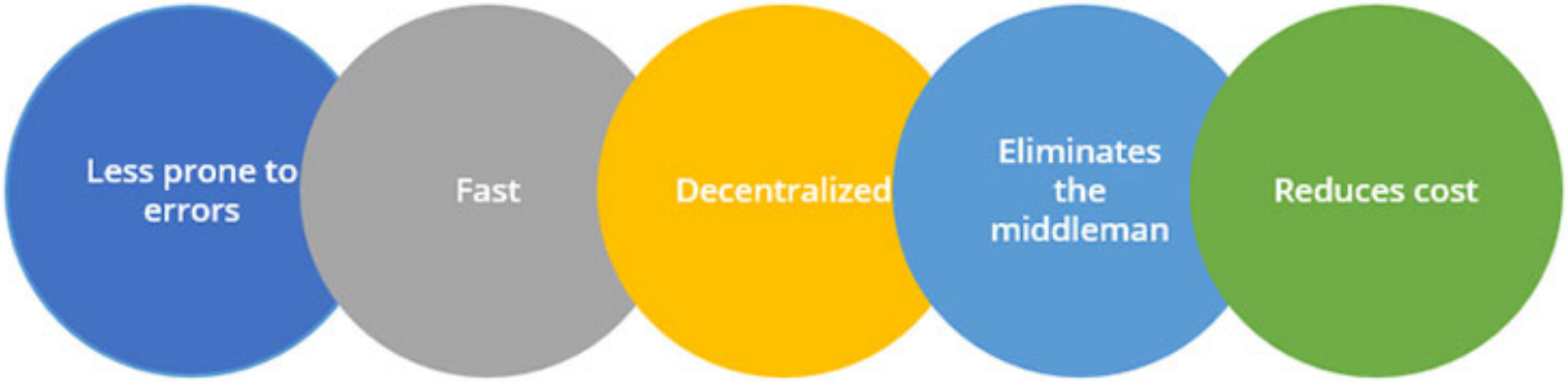
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger.

5

The new block is then added to the existing blockchain, in a way that is permanent and unalterable.

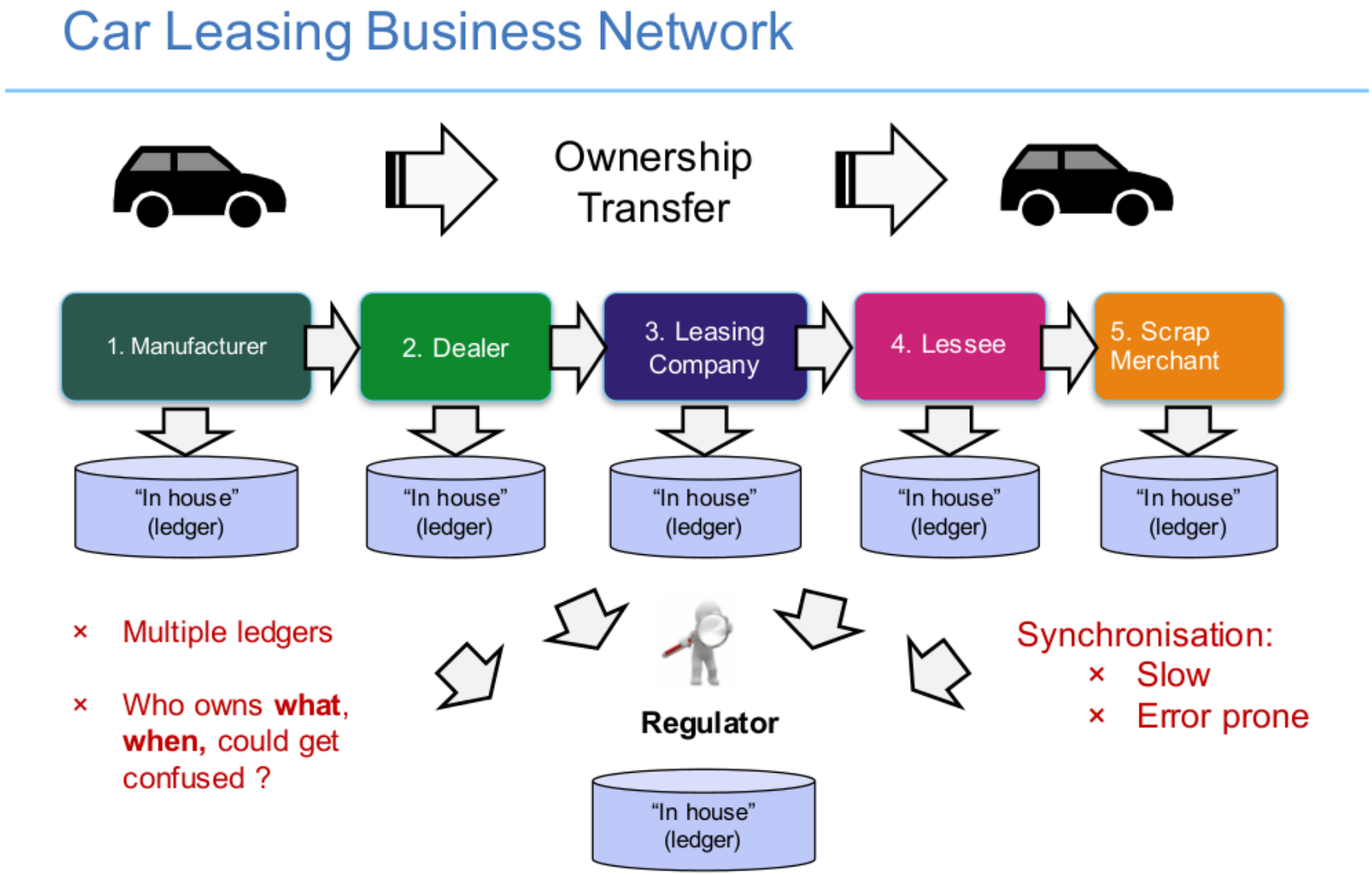
The transaction is complete.

https://www.msg-global.com/blog-item/blockchain-moving-beyond-bitcoin



Why to use Blockchain?

Exemple 1: Why do we need Blockchain?



Exemple 1: Why do we need Blockchain?

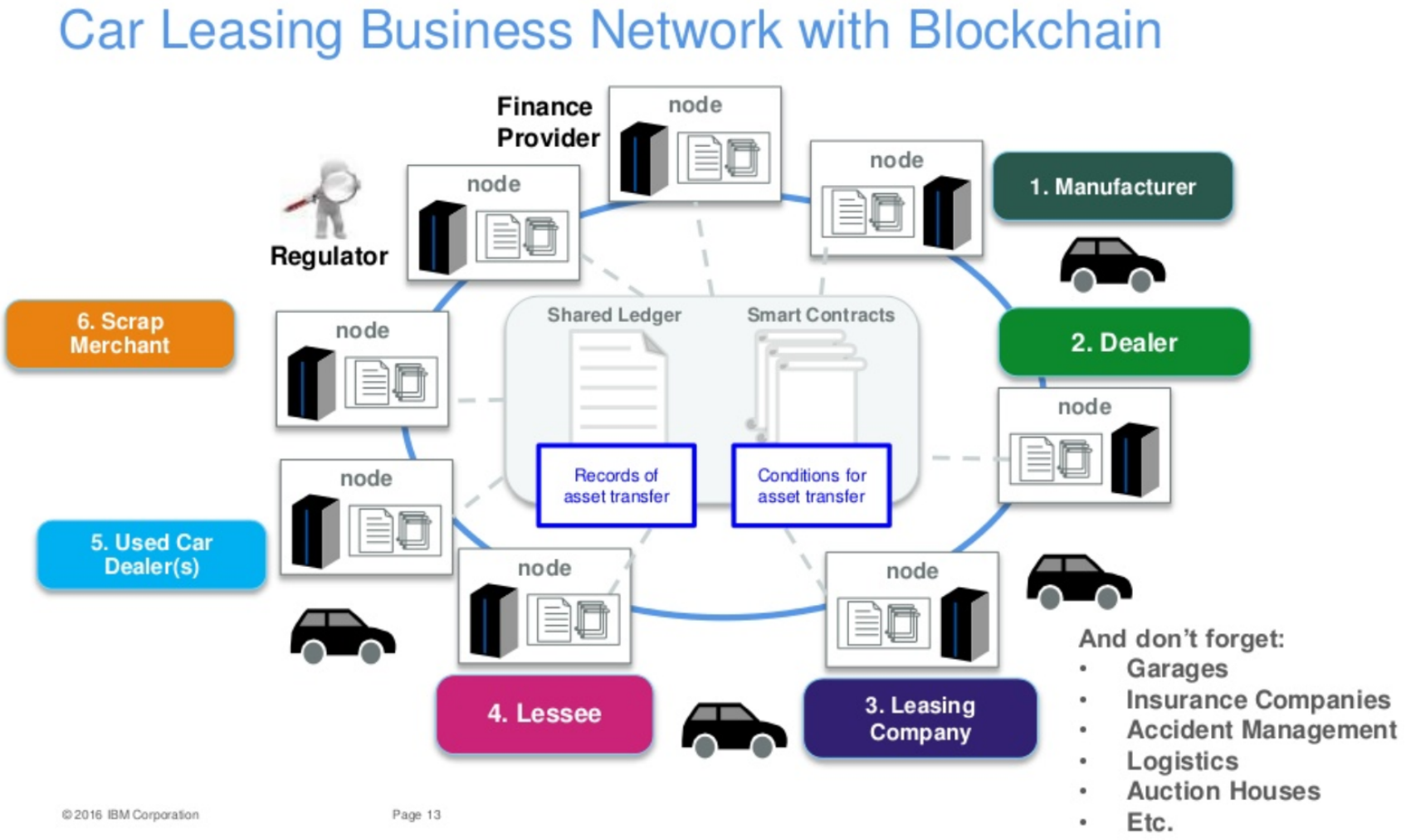
Benefits

Time savings:

- Transaction times for complex, multi-party interactions take minutes versus days.
- Transaction settlement is faster because it doesn't require verification by a central authority.

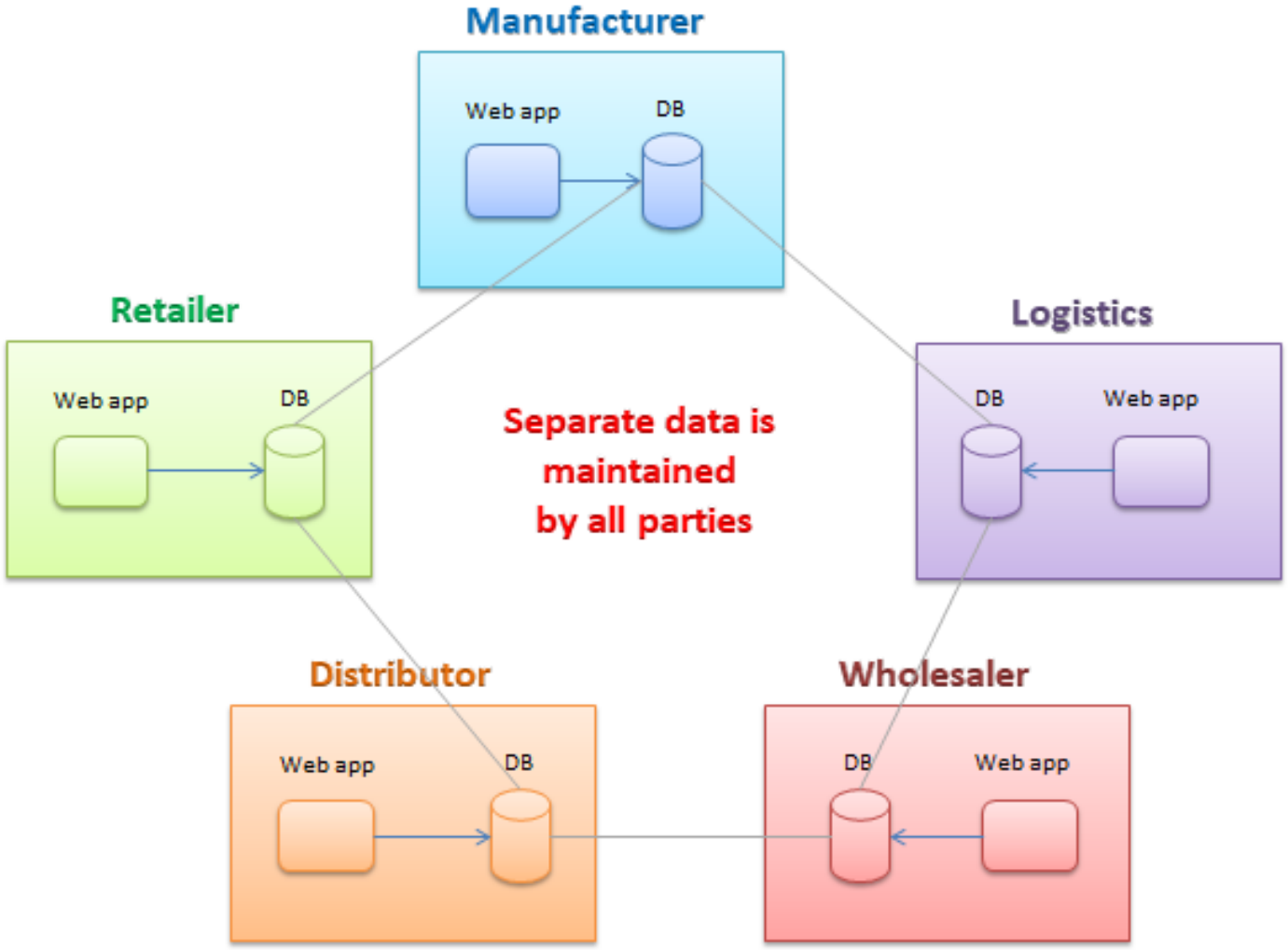
Cost savings:

- Less oversight is needed (network is self-policed by participants, all of whom are known on the network).
- Intermediaries are reduced because participants can exchange items of value directly
- Duplication of effort is eliminated because all participants have access to the shared ledger.



Exemple 2: Why do we need Blockchain?

Business Scenario Implemented Using the Database

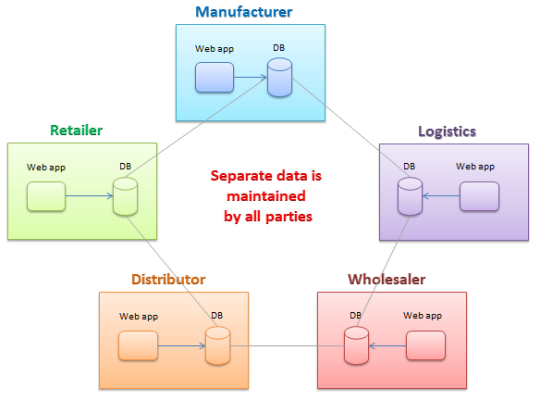


https://dzone.com/articles/why-do-we-need-blockchain

Exemple 2: Why do we need Blockchain?

Business Scenario Implemented Using the Database

Problems



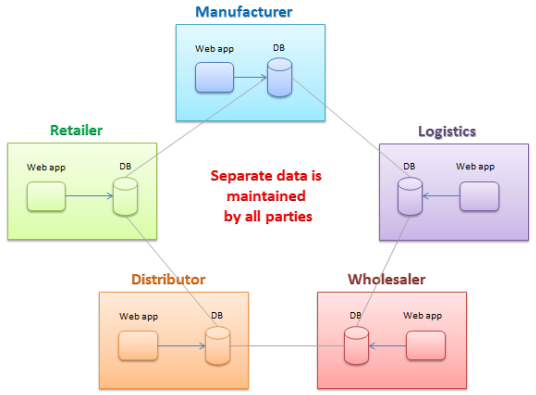
- **Multiple sources of truth**: At any point of time, all the databases may not have the same data, as it depends on the organizational process involved in updating the database or the delay in propagating the data across all the parties.
- **Human error**: The data in one or more of the databases may not sync up due to human error or application issues. This would lead to a dispute between parties.
- **Fraudulence**: This provides the possibility for parties to modify their database for business benefits and claim that their data is true.

https://dzone.com/articles/why-do-we-need-blockchain

Exemple 2: Why do we need Blockchain?

Business Scenario Implemented Using the Database

Problems

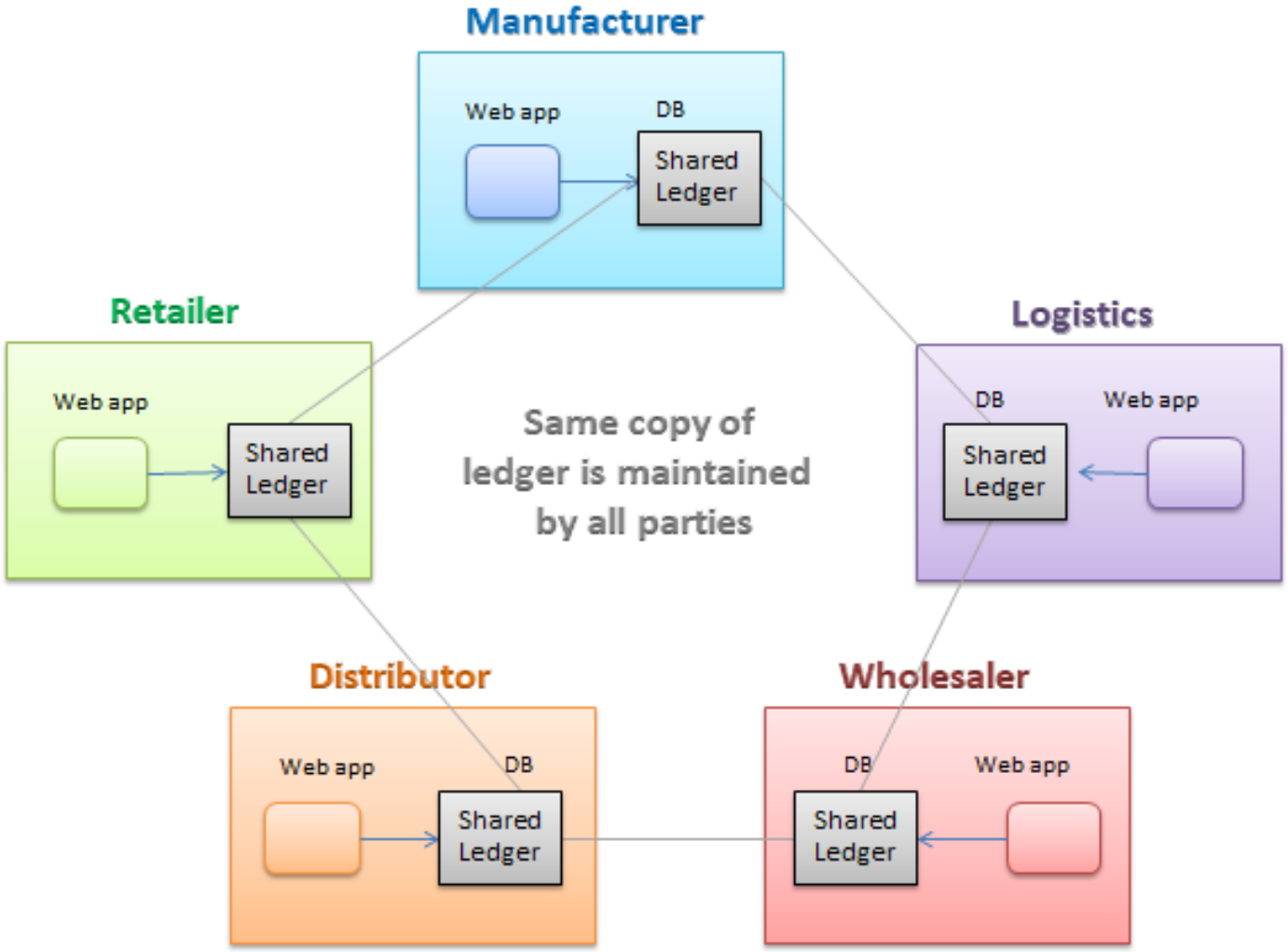


- **Reliance on intermediaries**: Depending on brokers or agents increases manufacturing costs and increases inefficiencies.
- **Vulnerability**: Due to the involvement of intermediaries and multiple copies of data, the manufacturer is unable to control fake products being introduced into the chain or genuine products distributed into the black market.
- **Lack of customer focus**: The customer finds it extremely difficult to identify whether the product is genuine.

https://dzone.com/articles/why-do-we-need-blockchain

Exemple 2: Why do we need Blockchain?

Business Scenario Implemented Using the Blockchain

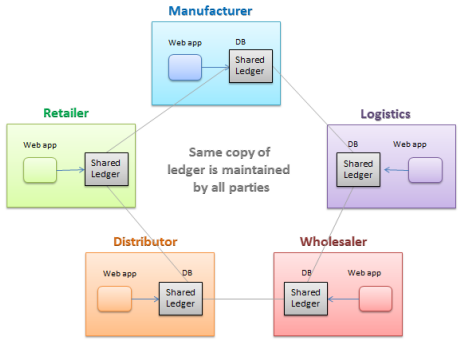


https://dzone.com/articles/why-do-we-need-blockchain

Exemple 2: Why do we need Blockchain?

Business Scenario Implemented Using the Blockchain

Benefits



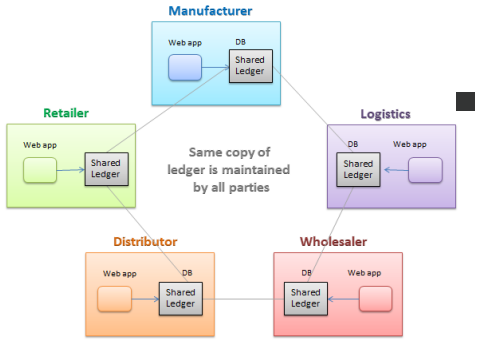
- **Single source of truth:** At any point in time, all the parties will refer to the same data due to a single shared ledger.
- **Early detection of human error:** Since all parties need to give consensus, any human or application errors will be caught early in the chain.
- **Security**: Treachery by any of the parties will be immediately identified by comparing the ledger copies of the other parties.
- **Safety**: The manufacturer can ensure that the quality of their products is not comprised.

https://dzone.com/articles/why-do-we-need-blockchain

Exemple 2: Why do we need Blockchain?

Business Scenario Implemented Using the Blockchain

Benefits



- **Disintermediation:** Elimination of intermediaries is one of the biggest benefits of the BLOCKCHAIN. It enables the manufacturers to reduce the overall cost and facilitates to connect the manufacturer directly with the customer.
- **Customer centric supply chain**: Since BLOCKCHAIN provides the opportunity to connect the manufacturer directly with the customer; the manufacturer is able to provide a better customer experience.
- **Regulatory compliance:** BLOCKCHAIN improves regulatory compliance through transparent audits.

https://dzone.com/articles/why-do-we-need-blockchain

Key Benefits of Blockchain

Harvard Business Review

INFORMATION & TECHNOLOGY

The Promise of Blockchain Is a World Without Middlemen

by Vinay Gupta

MARCH 06, 2017

- Greater transparency
- Enhanced security
- Improved traceability
- Increased efficiency and speed
- Reduced costs

https://www.ibm.com/blogs/blockchain/2018/02/top-five-blockchain-benefits-transforming-your-industry/

HOW to use Blockchain?

Potential Blockchain Use Cases

Financial Institutions

- International payments
- Capital markets
- Trade finance
- Regulatory compliance & audit
- Anti-money laundering & know your customer
- Insurance
- Peer-to-peer transactions

Corporates

- Supply chain management
- Healthcare
- Real estate
- Media
- Energy

Governments

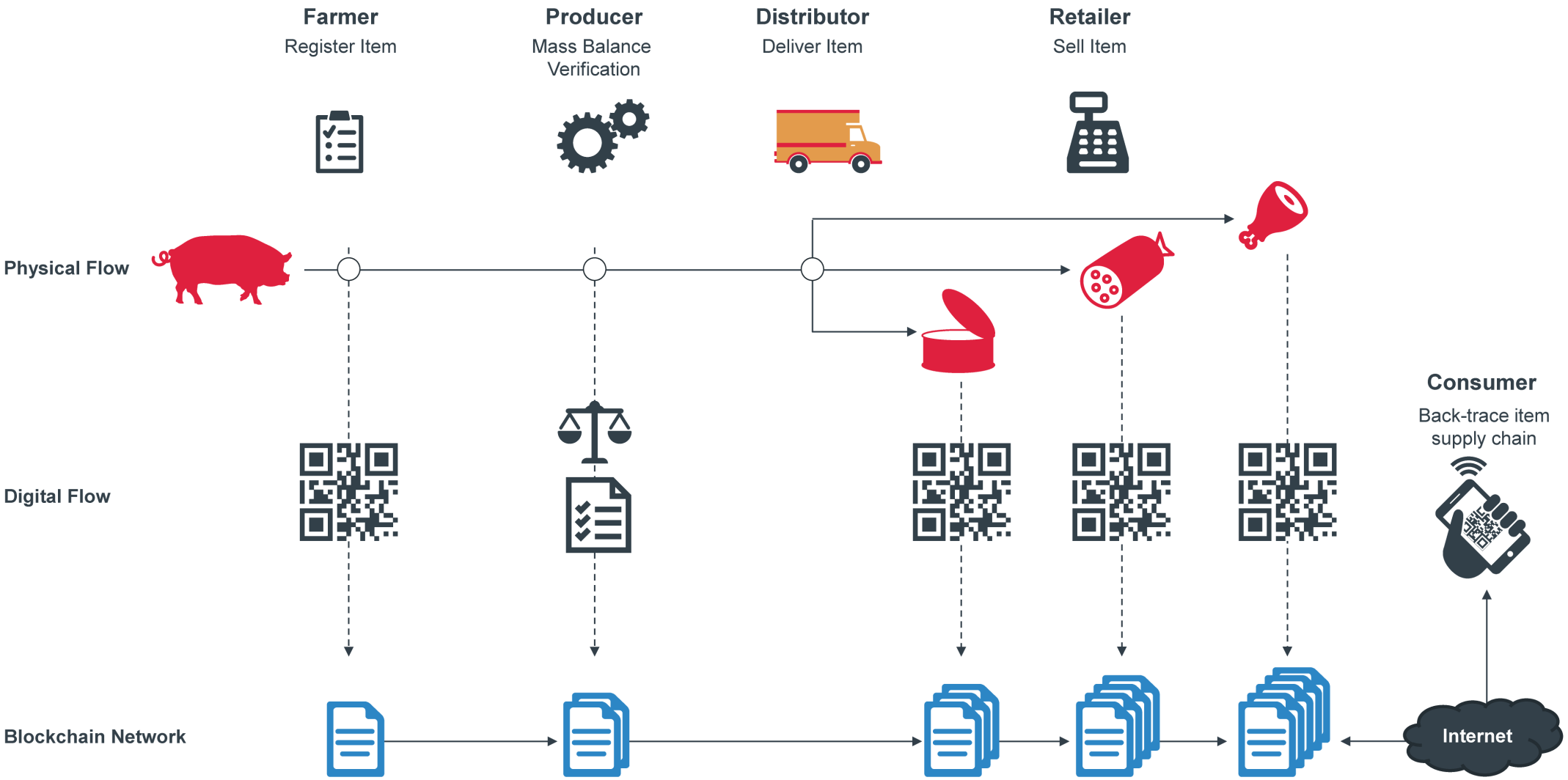
- Record management
- Identity management
- Voting
- Taxes
- Government & non-profit transparency
- Legislation, compliance & regulatory oversight

Cross-industry

- Financial management & accounting
- Shareholders' voting
- Record management
- Cybersecurity
- Big data
- Data storage
- Internet of Things

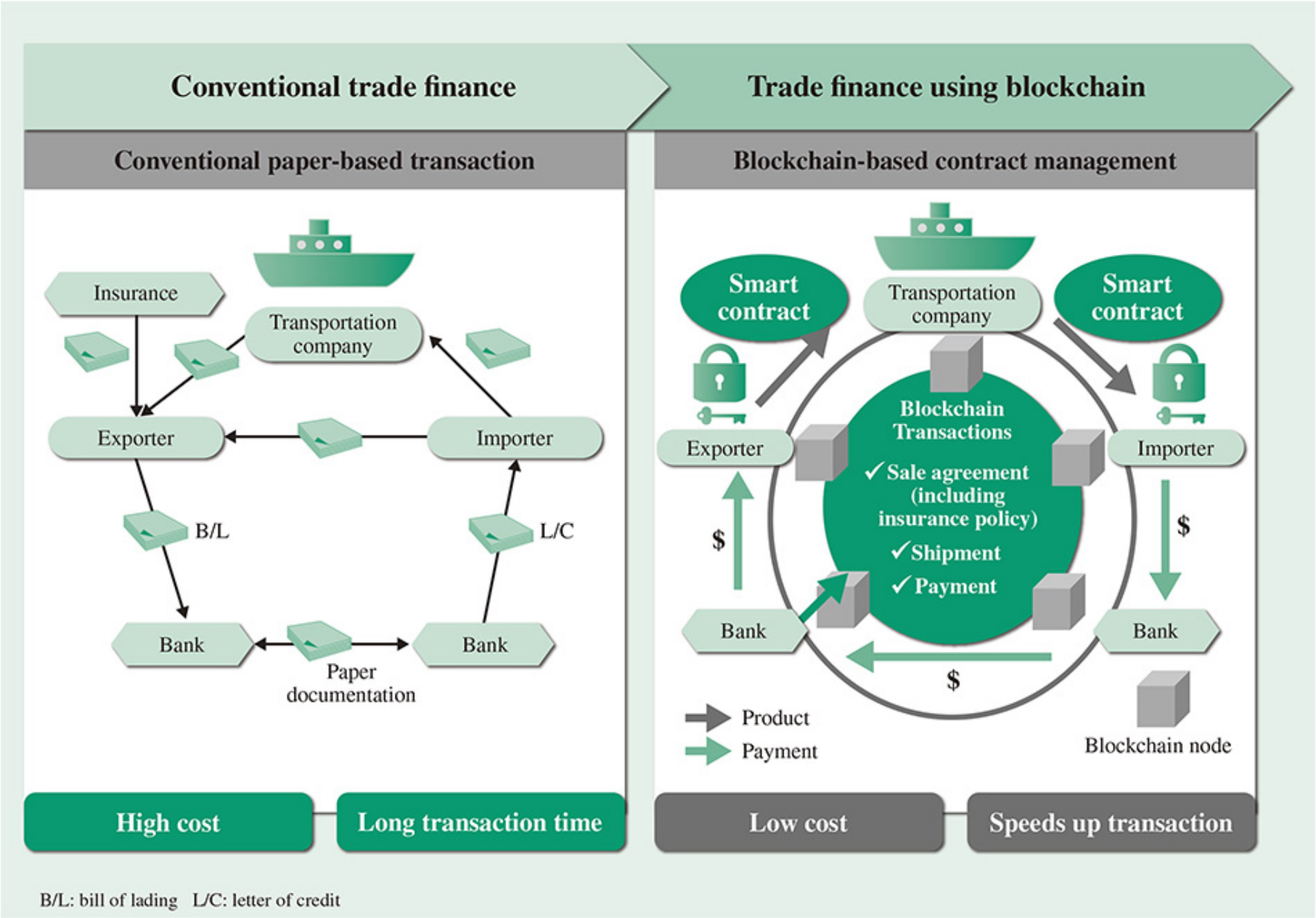
Source: Moody's Investors Service

Blockchain for Supply Chains



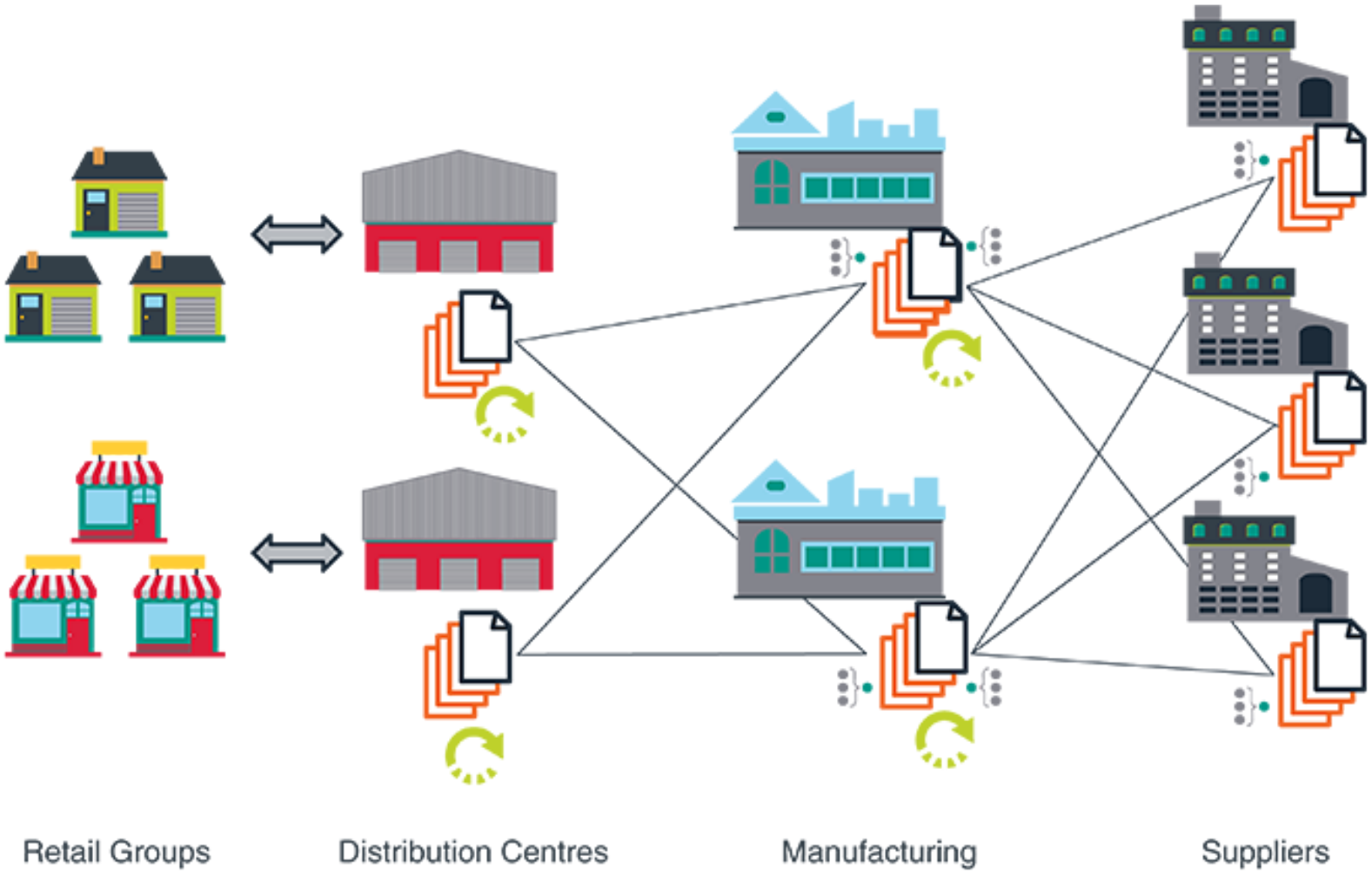
http://resolvesp.com/blockchains-supply-chains-part-ii/

Blockchain for Finance



http://www.hitachi.com/rev/archive/2017/r2017_01/103/index.html

Blockchain for Retails



Identical encrypted distributed ledger via the Internet

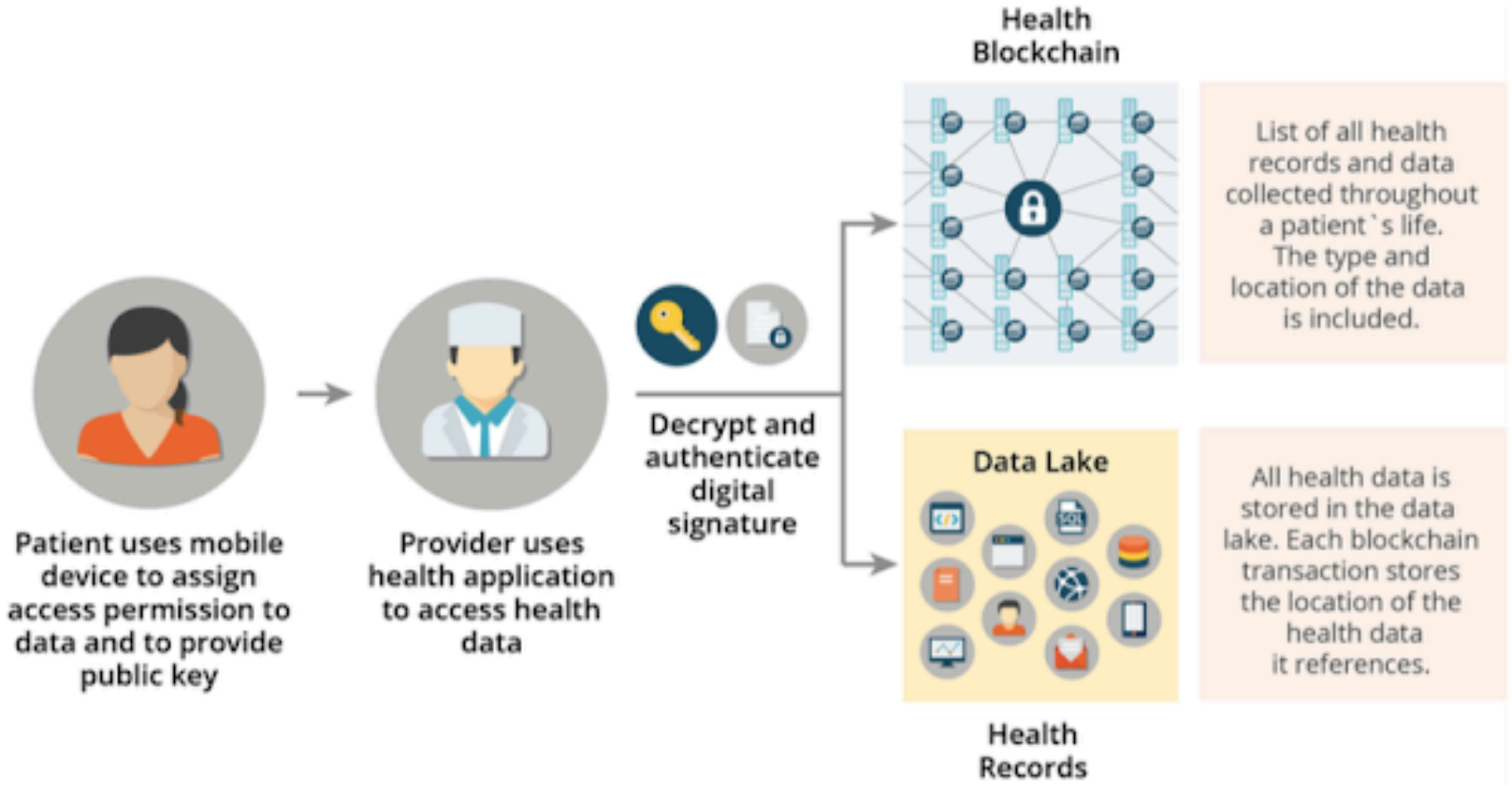
Dis-aggregator, automatically exploding product demand signal into constituent bill

Aggregator, automatically combining demand signals into one.

Smart Contracts orchestrating money flow based on codified parameters, process triggers and algorithms.

http://resolvesp.com/blockchains-supply-chains/

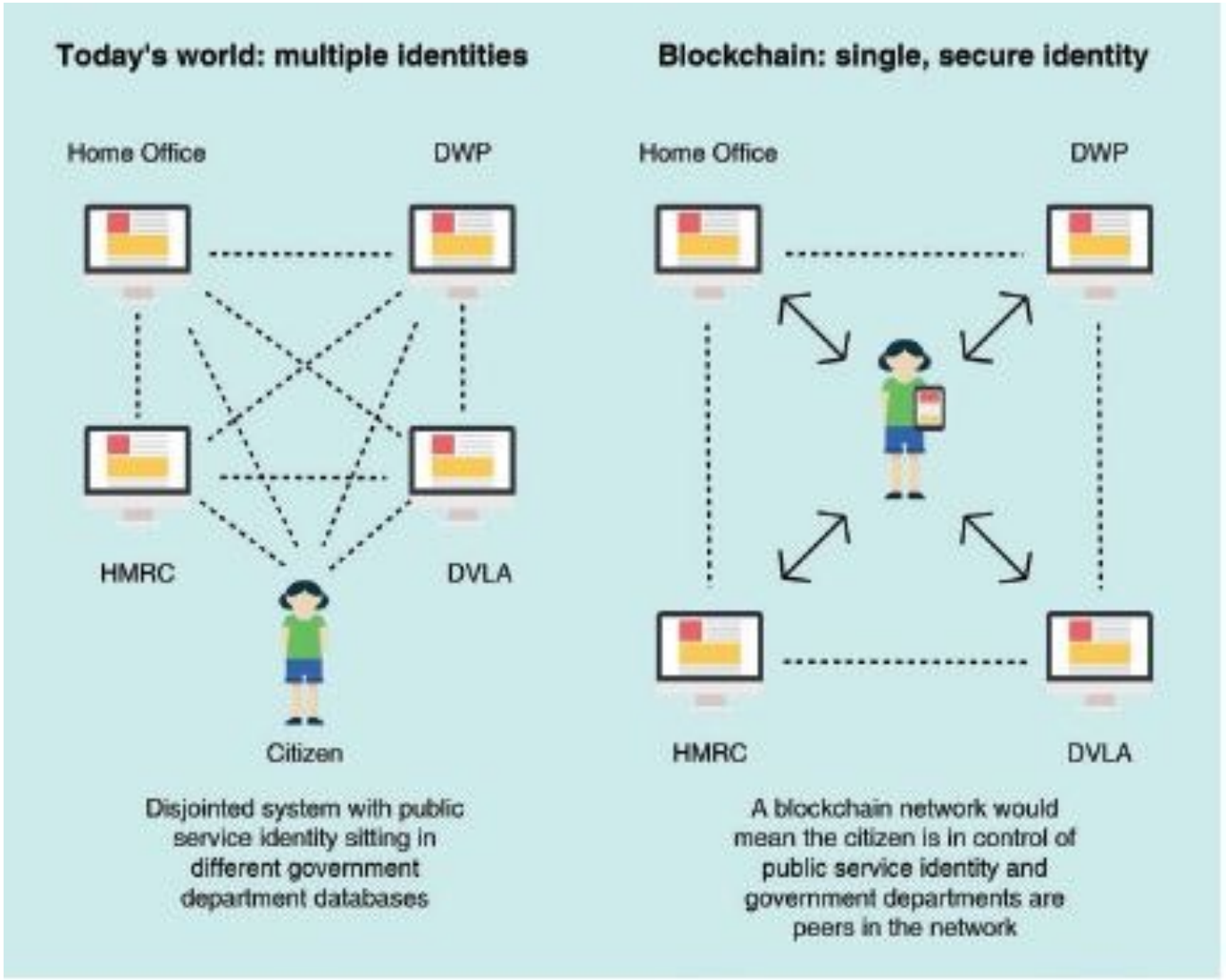
Blockchain for Healthcare



Identity authentication would follow the best practices established by financial institutions and regulators. Ideally, biometric identity systems would be utilized as they offer enhanced security over password and token (smartcard) based methods for identity authentication.

https://blog.hcitexpert.com/2017/10/blockchains-in-healthcare-by-msharmas.html

Blockchain for Identity in Public Services



Source: *Reform* interviews.

https://social.shorthand.com/reformthinktank/ngAikKvXau/the-future-of-public-service-identity-blockchain

Blockchain Platforms for Enterprise

Summary of Features of top 5 Blockchain Platforms for Enterprises

	Ethereum	Hyperledger Fabric	R3 Corda	Ripple	Quorum
Industry-focus	Cross-industry	Cross-industry	Financial Services	Financial Services	Cross-industry
Governance	Ethereum developers	Linux Foundation	R3 Consortium	Ripple Labs	Ethereum developers & JP Morgan Chase
Ledger type	Permissionless	Permissioned	Permissioned	Permissioned	Permissioned
Cryptocurrency	Ether (ETH)	None	None	Ripple (XRP)	None
% providers with experience[1]	93%	93%	60%	33%	27%
% share of engagements[2]	52%	12%	13%	4%	10%
Coin Market Cap[3]	$91.5 B (18%)	Not applicable	Not Applicable	$43.9 B (9%)	Not Applicable
Consensus algorithm	Proof of Work (PoW)	Pluggable framework	Pluggable framework	Probabilistic voting	Majority voting
Smart contract functionality	Yes	Yes	Yes	No	Yes

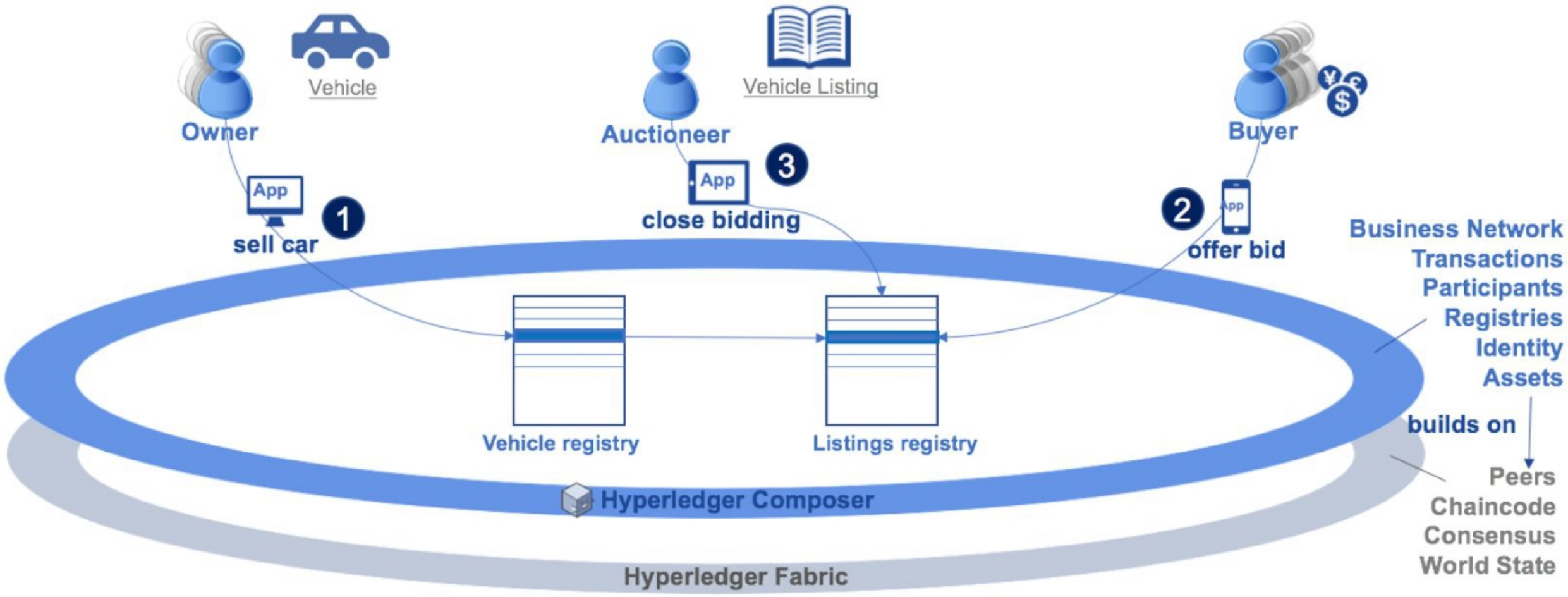
1. *Based on responses from 15 leading blockchain service providers*
2. *Based on a random sample of set of 50 enterprise blockchain engagements across multiple industries*
3. *Coinmarketcap.com as of Feb 20, 2018, 6:20 PM UTC*

Source: HfS Research, 2018

HfS

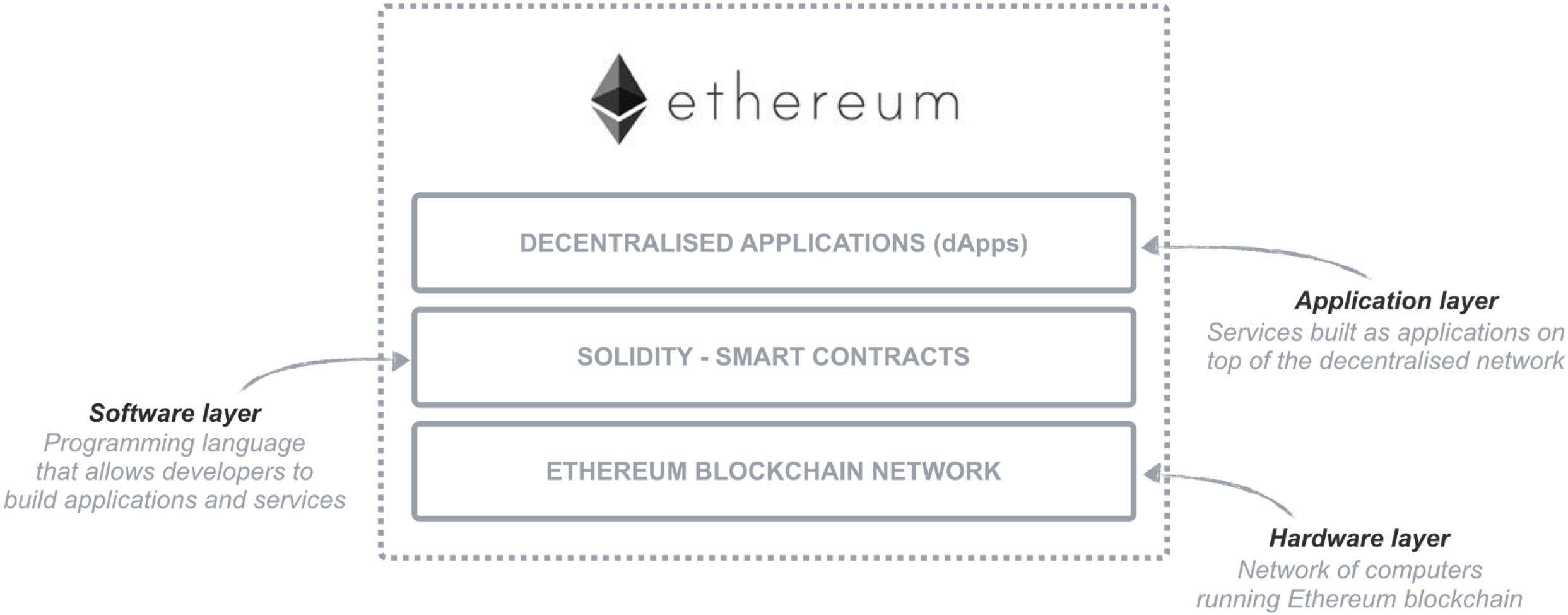
https://www.horsesforsources.com/top-5-blockchain-platforms_031618

Hyperledger platform

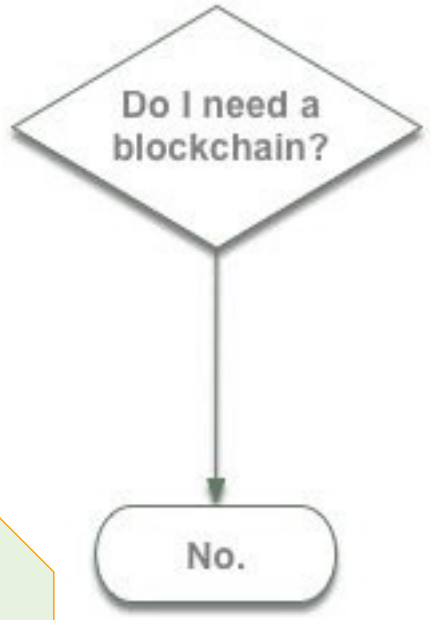


https://www.infoq.com/articles/blockchain-poc-hyperledger

Ethereum platform

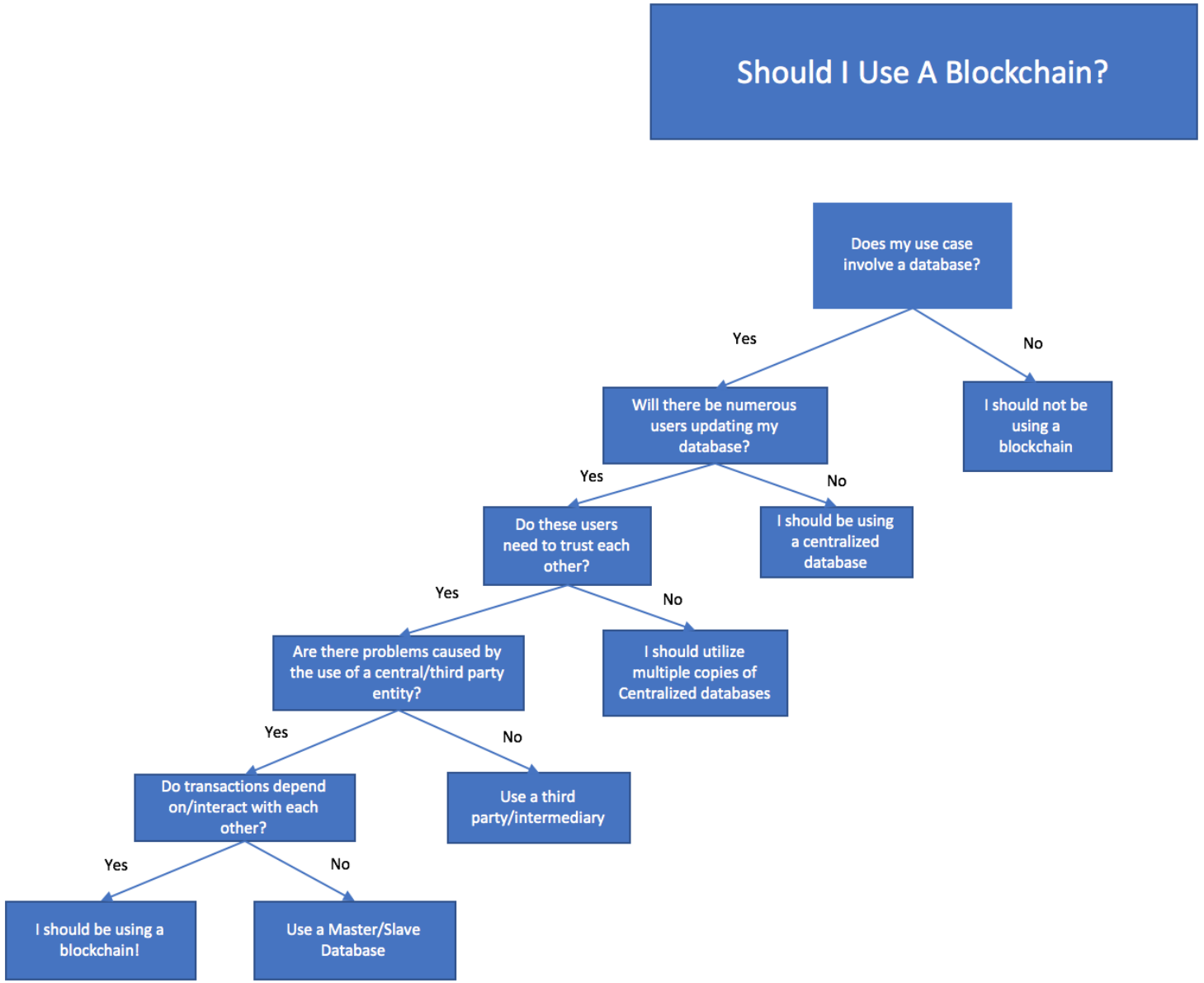


https://medium.com/@micheledaliessi/how-does-ethereum-work-8244b6f55297



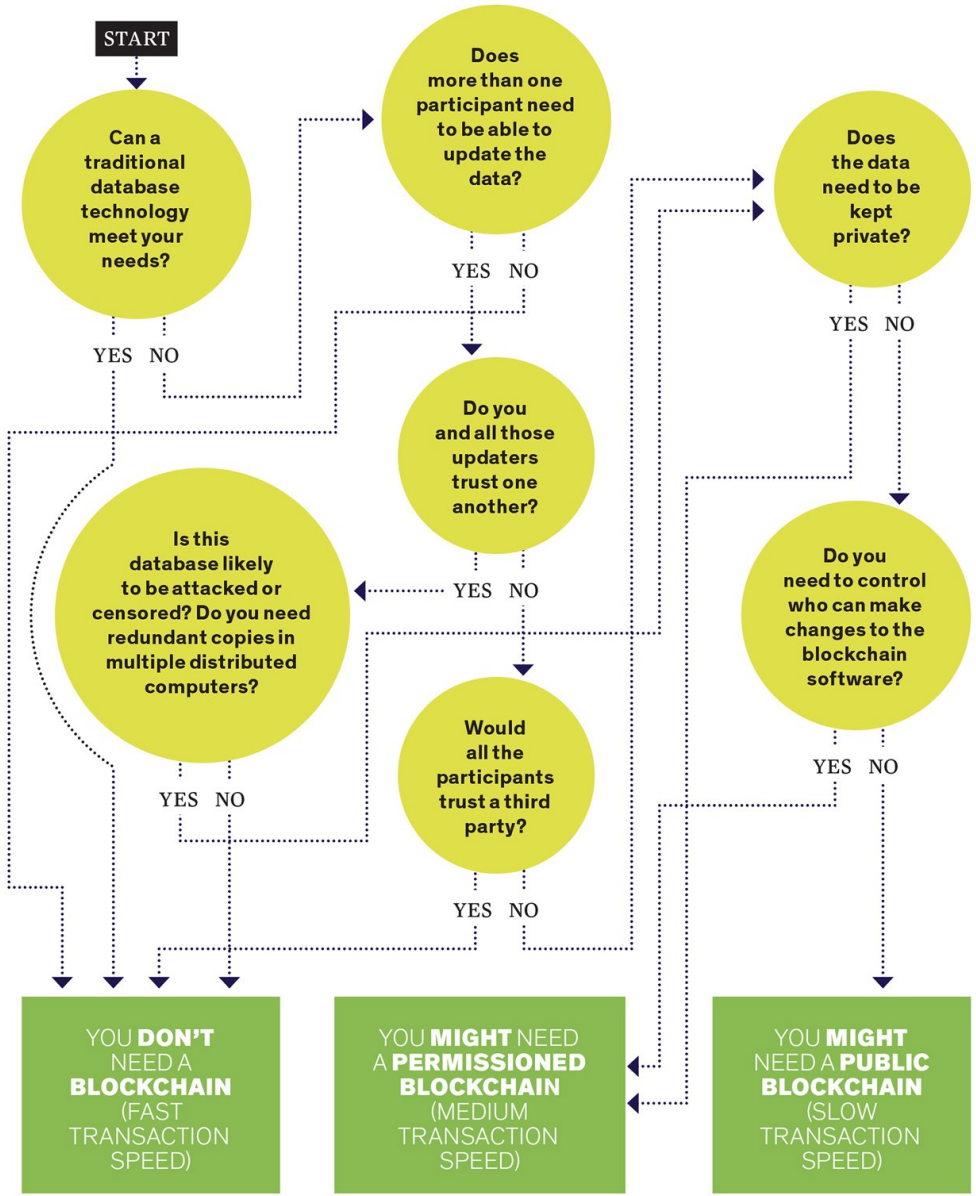
When to use Blockchain?

Do you even need Blockchain?



https://blockchainatberkeley.blog/building-it-better-a-simple-guide-to-blockchain-use-cases-de494a8f5b60

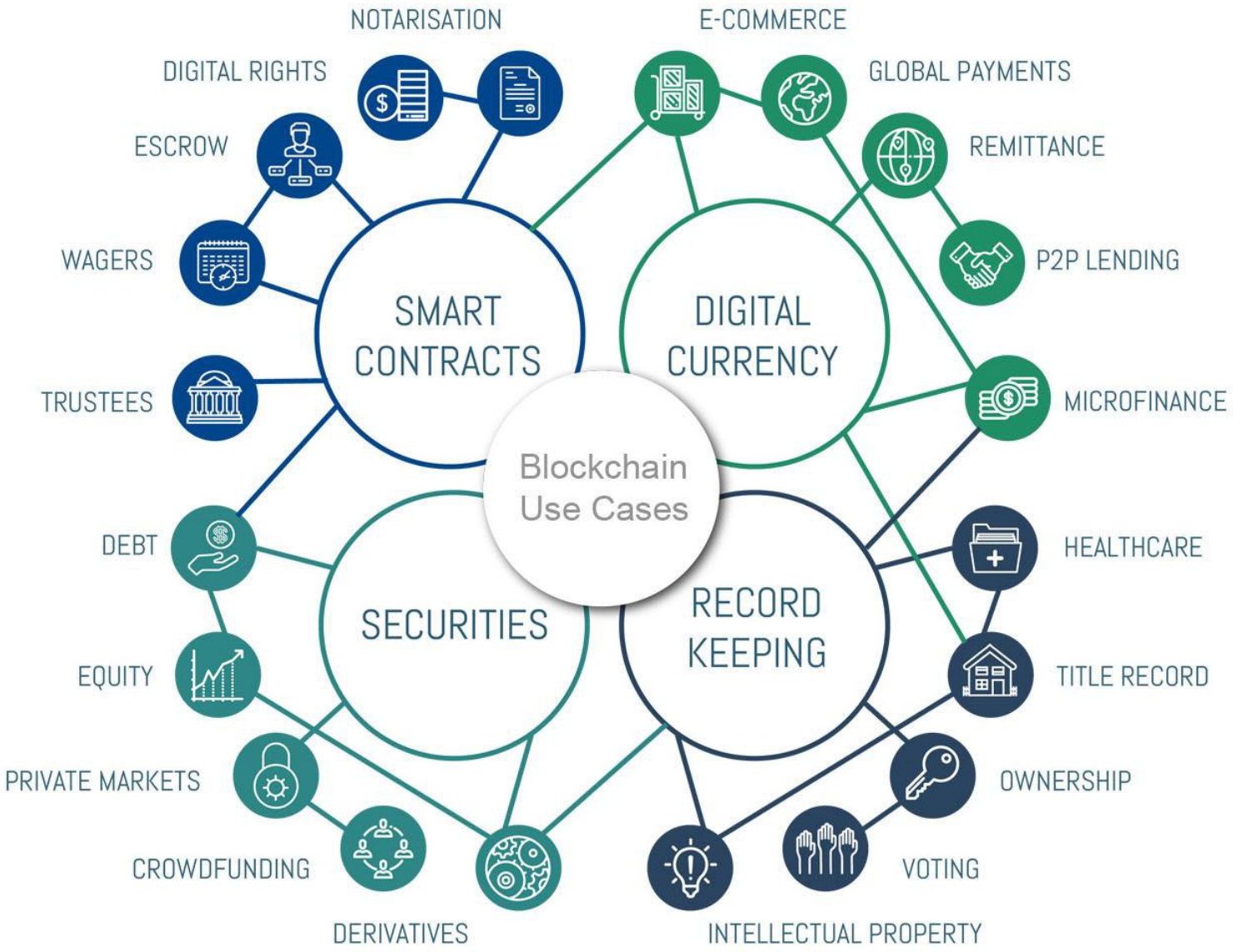
Do you need Blockchain?



https://medium.com/@sbmeunier/when-do-you-need-blockchain-decision-models-a5c40e7c9ba1

Where to use Blockchain?

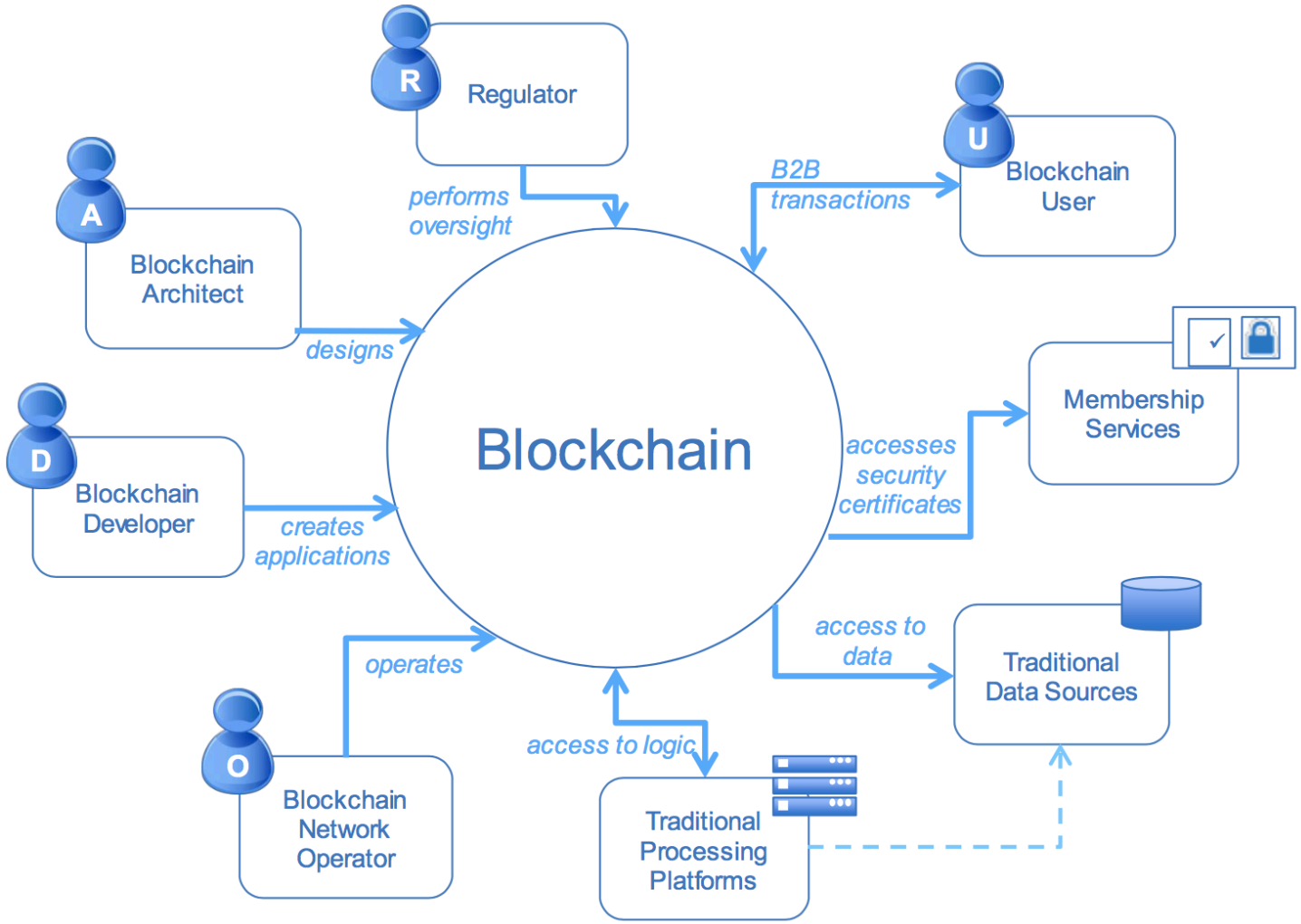
Blockchain



https://medium.com/@sergiomarrero/6-emerging-categories-for-blockchain-use-cases-4650f824d130

Who involve Blockchain solutions?

Actors in Blockchain Solutions

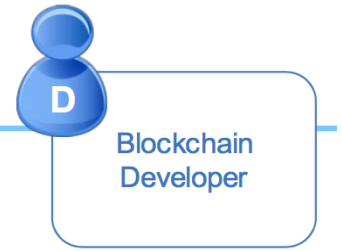


Actors in Blockchain Solutions

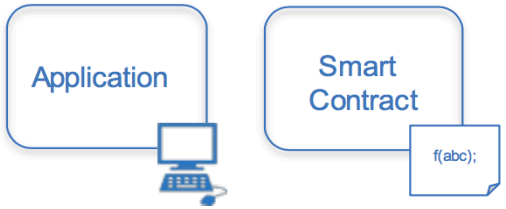
Blockchain Architect		Responsible for the architecture and design of the blockchain solution
Blockchain User		The business user, operating in a business network. This role interacts with the Blockchain using an application. They are not aware of the Blockchain.
Blockchain Regulator		The overall authority in a business network. Specifically, regulators may require broad access to the ledger's contents.
Blockchain Developer		The developer of applications and smart contracts that interact with the Blockchain and are used by Blockchain users.
Blockchain Operator		Manages and monitors the Blockchain network. Each business in the network has a Blockchain Network operator.

Blockchain Developer

The Blockchain Developer



Blockchain developers' primary interests are…



…and how they interact with the ledger and other systems of record:

They should NOT have to care about operational concerns, such as:

X Peers Consensus Security

Blockchain challenges?

References

IBM Blockchain courses:

- Blockchain essentials
- IBM Blockchain foundation developer
  https://developer.ibm.com/courses/all/category/blockchain/

And other online documents

- Searching with keywords: Blockchain, Blockchain Explained, Blockchain Consensus, Blockchain Platforms, etc