Introduction to Blockchain and Smart Contracts

Legal IT 2018
March 23, 2018

Laurent Féral-Pierssens

Blockchain Advisory, KPMG Canada

Partner, Inception Block Ventures

linkedin.com/in/pierssens

Agenda for today

What is « blockchain » ?

What are smart contracts?

Use cases

Q & A

What is **BLOCKCHAIN** ?

Five Technological Trends Are Driving Change

ARTIFICIAL INTELLIGENCE

Learning algorithms at the heart of technologies and systems

BIG DATA ANALYTICS

Collecting and analyzing large amounts of data to uncover patterns, correlations and insights
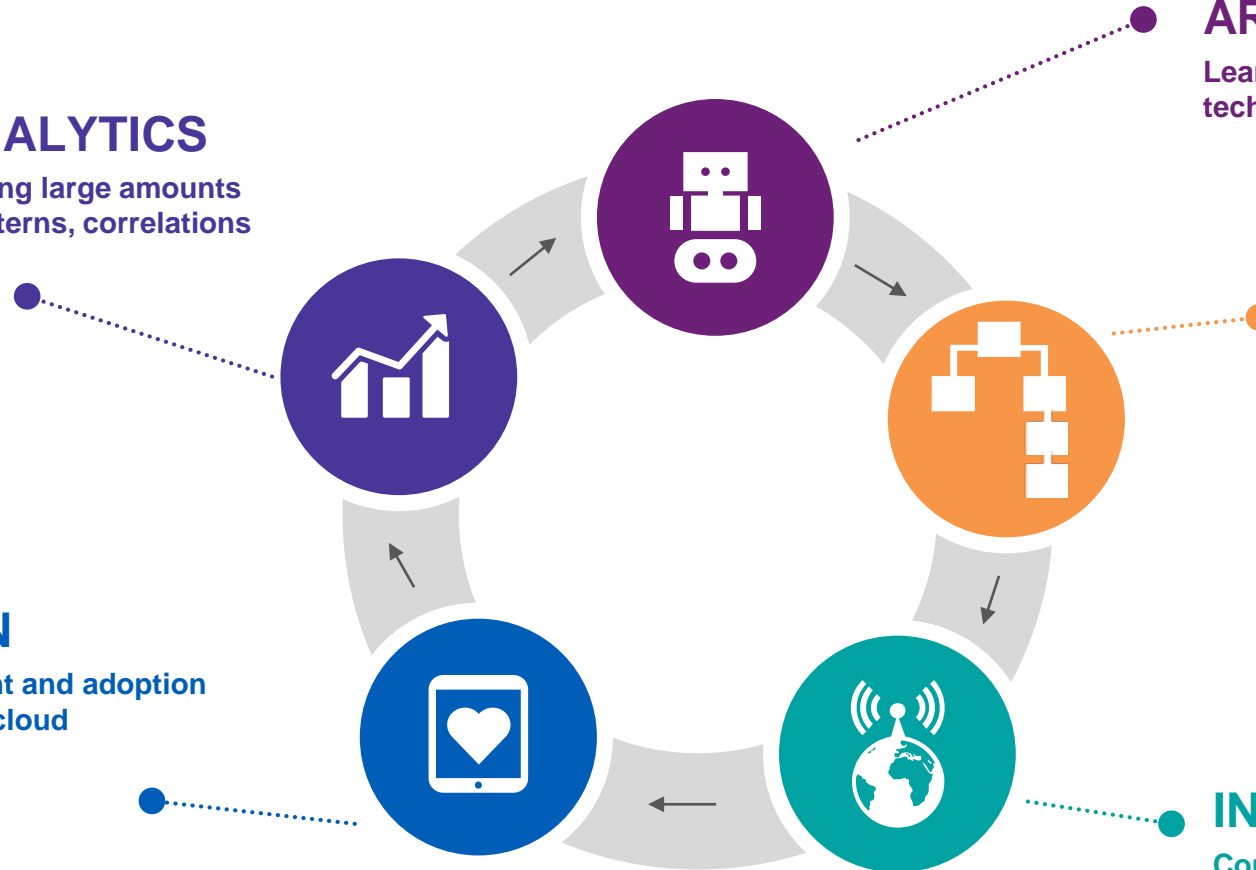
BLOCKCHAIN

A distributed framework to establish trust, transparency and automation

DIGITIZATION

The rapid development and adoption of social, mobile and cloud infrastructure

INTERNET OF THINGS

Connecting the dots…
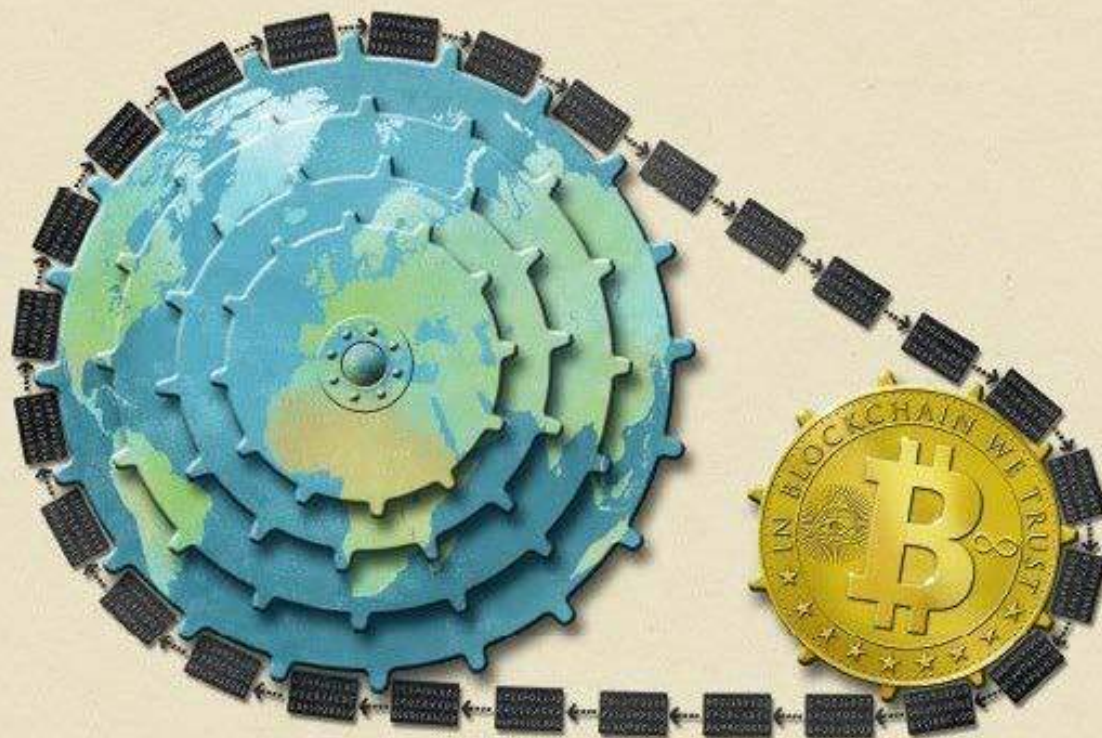
Blockchain has been invented to
DECENTRALIZE TRANSACTIONS

Blockchain has been invented to provide a
SINGLE SOURCE OF TRUTH

First, let's talk about the problem

Sending the digital file

Who has the original?

2 copies of the same picture

Today we solve this very problem
using **TRUSTED** third parties

Blockchain allows to
RECORD AND KEEP TRACK
of the truth

Blockchain uses
UPDATE AND CONSENSUS

Initiate the transaction.

– Multiple parties transact.
– All transactions are recorded, including the transaction's date, time, parties, and amount wants to do a transaction.
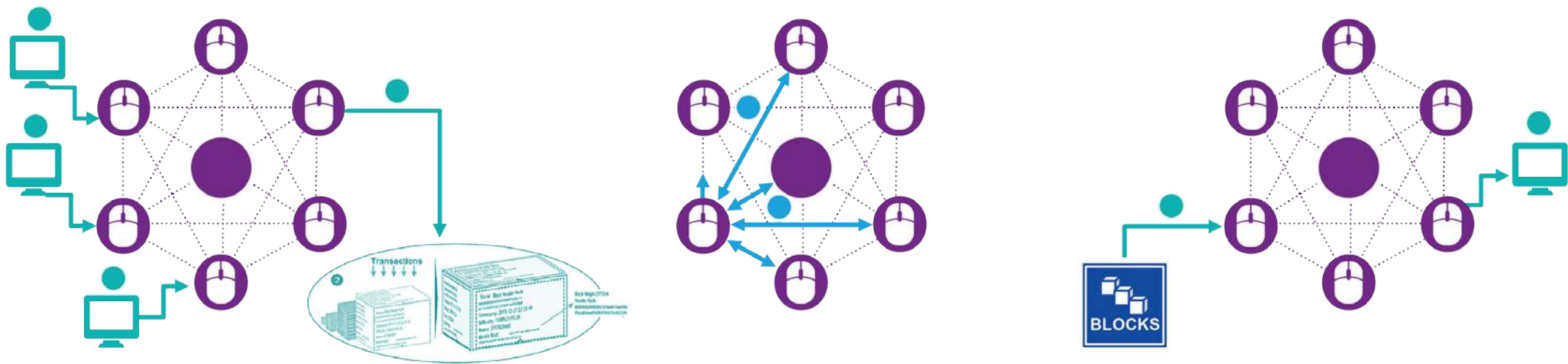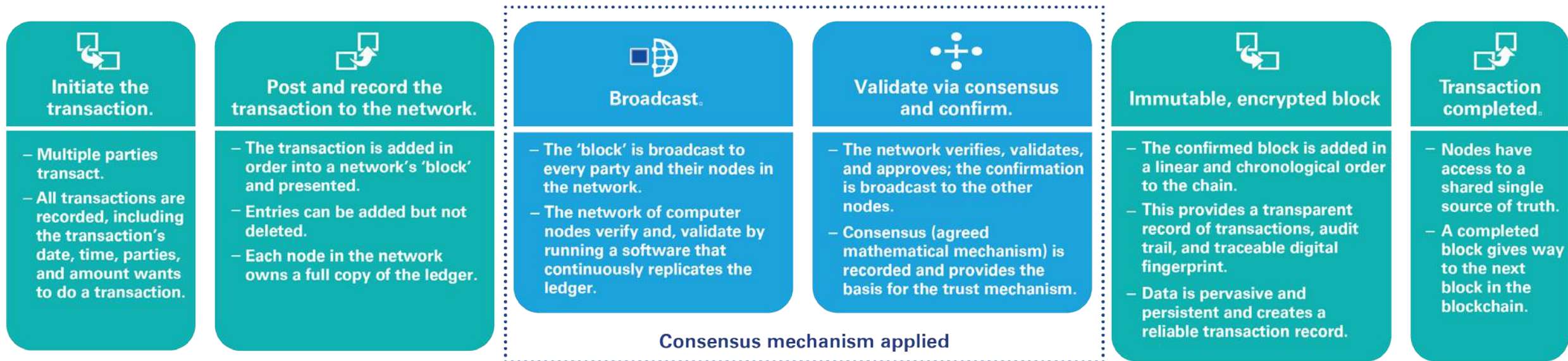
Post and record the transaction to the network.

– The transaction is added in order into a network's 'block' and presented.
– Entries can be added but not deleted.
– Each node in the network owns a full copy of the ledger.

Broadcast.

– The 'block' is broadcast to every party and their nodes in the network.
– The network of computer nodes verify and, validate by running a software that continuously replicates the ledger.

Validate via consensus and confirm.

– The network verifies, validates, and approves; the confirmation is broadcast to the other nodes.
– Consensus (agreed mathematical mechanism) is recorded and provides the basis for the trust mechanism.

Consensus mechanism applied

Immutable, encrypted block

– The confirmed block is added in a linear and chronological order to the chain.
– This provides a transparent record of transactions, audit trail, and traceable digital fingerprint.
– Data is pervasive and persistent and creates a reliable transaction record.

Transaction completed.

– Nodes have access to a shared single source of truth.
– A completed block gives way to the next block in the blockchain.

The nature of the **RECORD** can be very different

transaction · vote · contract · data

Each blockchain is a global NETWORK

The most important innovation since the **INTERNET**

Adoption
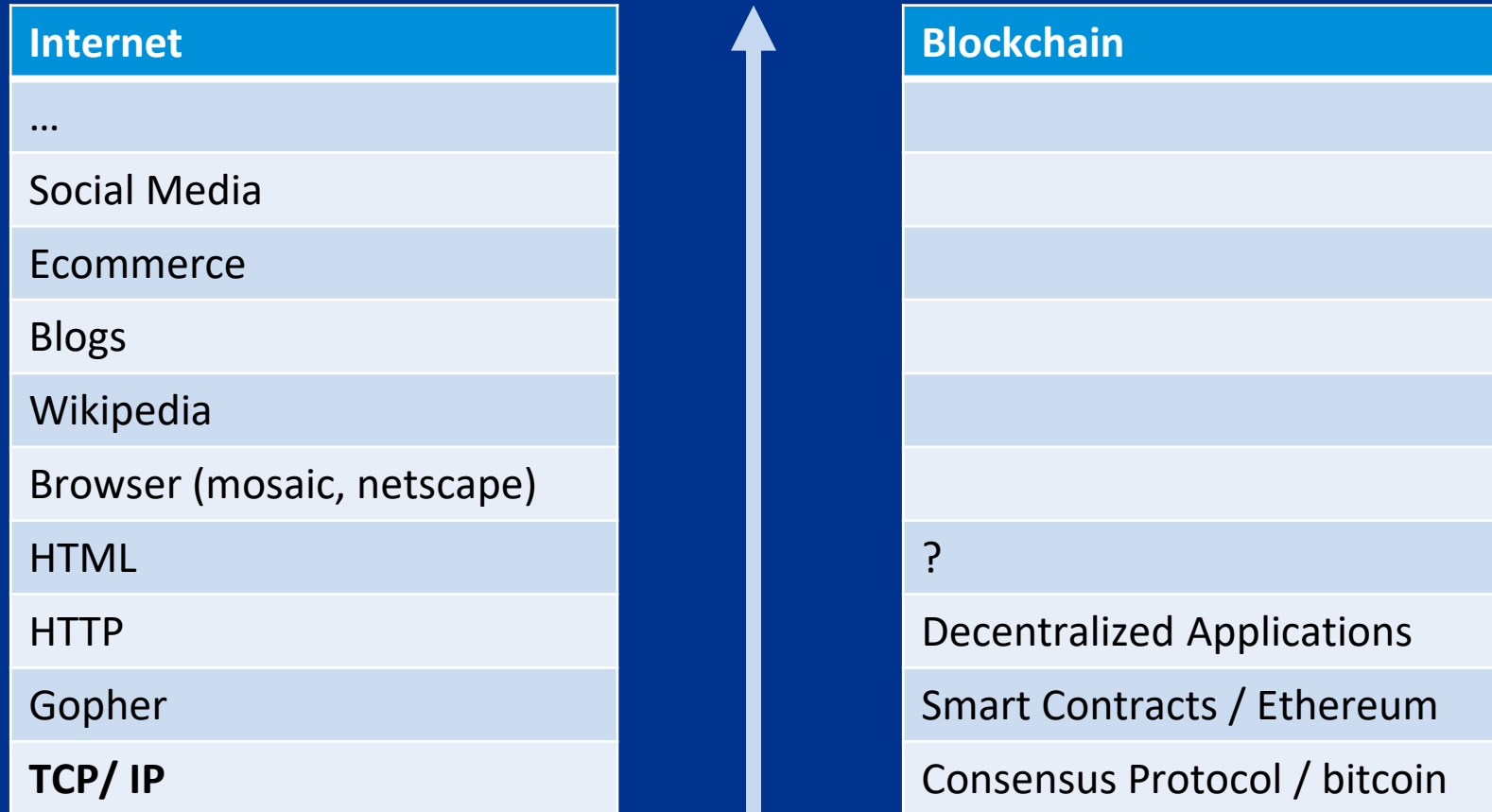
Internet
…
Social Media
Ecommerce
Blogs
Wikipedia
Browser (mosaic, netscape)
HTML
HTTP
Gopher
TCP/ IP

Blockchain
?
Decentralized Applications
Smart Contracts / Ethereum
Consensus Protocol / bitcoin

Key Components

Distributed Ledger Technology
DLT is a write-once database so it registers an immutable record of every transaction that occurs.

→ Database

Cryptoasset
Blockchains have underlying cryptographic currencies, they can tokenize any asset and track digitally and securely.

→ Incentive

Smart Contracts
Some blockchains can store and execute both data and logic (code). Can enforce the code to make payments, update blockchain, transfer ownership, etc.

→ Automation

Key Components

Distributed Ledger Technology
DLT is a write-once database so it registers an immutable record of every transaction that occurs.

Cryptoasset
Blockchains have underlying cryptographic currencies, they can tokenize any asset and track digitally and securely.

Smart Contracts
Some blockchains can store and execute both data and logic (code). Can enforce the code to make payments, update blockchain, transfer ownership, etc.

Crypto Economy
Describes the nature of the decentralized ecosystem being created: stakeholders, incentives, ethics, governance, monetary distribution.

Liquid Market
Ability by participants to transact peer to peer creating a fluid market with properties that have more in common with commodities than foreign exchange.

Blockchain is a distributed ledger

Authenticated. Every transaction is associated with an identity.

Transparent. It enables transparent audit trails, has the ability to require specific types of content based on the user, and transaction authorization based on permissions.

Auditable. The entire history of the blockchain is stored on multiple nodes and is easily viewable by an auditor, thus creating a highly transparent system.

Tamper-proof. The cryptographic underpinnings make the system resistant to tampering with historical data. No single participant can affect the data, and advances are regularly being made to ensure that the data cannot be changed once logged.

What are **SMART CONTRACTS** ?

DATE 1915	ITEMS	Folio	√	DEBITS	DATE	ITEMS	Folio	√	CREDITS
Nov 2	Barten Contract			40 —	Nov 13	Salary	1		9 50
2	Strong Curio Co			11 50	13				35 —
13		1		4 50					11 50
				56 —					56 —
13	Btn Bal.			35 —	20	"	2		9 50
13	WaB "			11 50					30
30		2		4 50					11 50
20	Btn "			30 —	27		3		9 50
20	WaB "			11 50					25
27		3		4 50					11 50
27	Btn "			25 —	Dec 4		4		9 50
27	WaB "			11 50					
Dec 4		4		4 50					
4	Btn "			20 —	11		5		9 50
4	WaB "			11 50					
11		5		7 75					
11	Btn "			15 —	18		6		9 50
11	WaB "			14 75					10 —
									10 25
18	Btn "			10 —	25		7		9 50
18	WaB "			10 25					5 —
									5 75
				20 25					20 25

```
contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

    /* Initializes contract with initial supply tokens to the creator of the contract */
    function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

    /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

Source: Ethereum.org

Smart Contract

Ethereum Account Type (Just like User Account)

Address — 0x16E0022b17B...

Balance — 0 Ether

Code

State

```
contract Counter {
    uint counter;

    function Counter() public {
        counter = 0;
    }
    function count() public {
        counter = counter + 1;
    }
}
```

Smart Contracts

A smart contract benefits from the blockchain's features: irrevocable, immutable…

Pre-written logic in the form of computer code

Stored and replicated across the distributed ledger

Executed by a network of computers

Updates the ledger itself

Smart contracts – simple to complex

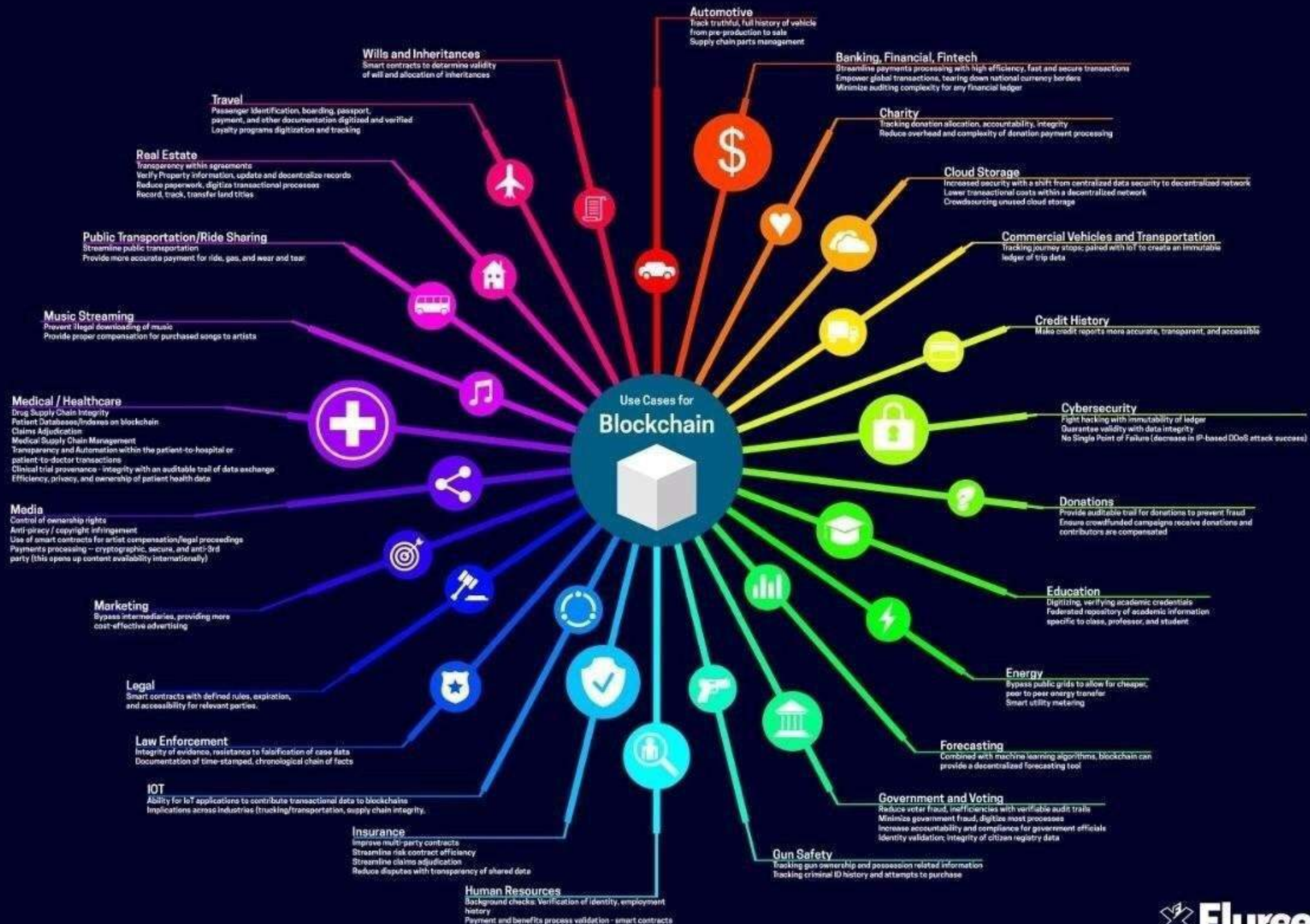| Digital value exchange	Smart right and obligation	Basic smart contract	Multiparty smart contract	Distributed autonomous business unit	Distributed autonomous organization	Distributed autonomous government	Distributed autonomous society
A family member sends some bitcoin to another family member	Consumer buys a digital content stream	Landlord remotely locks nonpaying tenant out of apartment	Seller lends buyer funds to buy a house	Unit of a corporation issues its own bonds, and buyers monitor payments via a shared ledger	Self-driving trucks make P2P deliveries, pay local toll road fees, and buy local electricity	Settlers of a previously uninhabited area code their own self-enforcing government services	Groups of settlers from different areas establish self-enforcing trade agreements

Use case examples

Simple ← → Complex

Blockchain **DISRUPTS** business processes

Where there is:

- A network with third parties who introduce cost, complexity, and latency

- A need for a common version of the truth between multiple stakeholders

- A divergence of stakeholder incentives

- A regulatory environment

- An audited environment

Blockchain in the **REAL WORLD**

Use Cases for Blockchain

Automotive
Track truthful, full history of vehicle from pre-production to sale
Supply chain parts management

Banking, Financial, Fintech
Streamline payments processing with high efficiency, fast and secure transactions
Empower global transactions, tearing down national currency borders
Minimize auditing complexity for any financial ledger

Charity
Tracking donation allocation, accountability, integrity
Reduce overhead and complexity of donation payment processing

Cloud Storage
Increased security with a shift from centralized data security to decentralized network
Lower transactional costs within a decentralized network
Crowdsourcing unused cloud storage

Commercial Vehicles and Transportation
Tracking journey stops; paired with IoT to create an immutable ledger of trip data

Credit History
Make credit reports more accurate, transparent, and accessible

Cybersecurity
Fight hacking with immutability of ledger
Guarantee validity with data integrity
No Single Point of Failure (decrease in IP-based DDoS attack success)

Donations
Provide auditable trail for donations to prevent fraud
Ensure crowdfunded campaigns receive donations and contributors are compensated

Education
Digitizing, verifying academic credentials
Federated repository of academic information specific to class, professor, and student

Energy
Bypass public grids to allow for cheaper, peer to peer energy transfer
Smart utility metering

Forecasting
Combined with machine learning algorithms, blockchain can provide a decentralized forecasting tool

Government and Voting
Reduce voter fraud, inefficiencies with verifiable audit trails
Minimize government fraud, digitize most processes
Increase accountability and compliance for government officials
Identity validation; integrity of citizen registry data

Gun Safety
Tracking gun ownership and possession related information
Tracking criminal ID history and attempts to purchase

Human Resources
Background checks: Verification of identity, employment history
Payment and benefits process validation - smart contracts

Insurance
Improve multi-party contracts
Streamline risk contract efficiency
Streamline claims adjudication
Reduce disputes with transparency of shared data

IOT
Ability for IoT applications to contribute transactional data to blockchain
Implications across industries (trucking/transportation, supply chain integrity)

Law Enforcement
Integrity of evidence, resistance to falsification of case data
Documentation of time-stamped, chronological chain of facts

Legal
Smart contracts with defined rules, expiration, and accessibility for relevant parties.

Marketing
Bypass intermediaries, providing more cost-effective advertising

Media
Control of ownership rights
Anti-piracy / copyright infringement
Use of smart contracts for artist compensation/legal proceedings
Payments processing -- cryptographic, secure, and anti-3rd party (this opens up content availability internationally)

Medical / Healthcare
Drug Supply Chain Integrity
Patient Databases/Indexes on blockchain
Claims Adjudication
Medical Supply Chain Management
Transparency and Automation within the patient-to-hospital or patient-to-doctor transactions
Clinical trial provenance - integrity with an auditable trail of data exchange
Efficiency, privacy, and ownership of patient health data

Music Streaming
Prevent illegal downloading of music
Provide proper compensation for purchased songs to artists

Public Transportation/Ride Sharing
Streamline public transportation
Provide more accurate payment for ride, gas, and wear and tear

Real Estate
Transparency within agreements
Verify Property information, update and decentralize records
Reduce paperwork, digitize transactional processes
Record, track, transfer land titles

Travel
Passenger identification, boarding, passport, payment, and other documentation digitized and verified
Loyalty programs digitization and tracking

Wills and Inheritances
Smart contracts to determine validity of will and allocation of inheritances

Intellectual Property Rights

Spotify acquires blockchain startup Mediachain to solve music's attribution problem

Posted Apr 26, 2017 by *Sarah Perez* (*@sarahintampa*)

Next Story

ADVERTISEMENT

AdChoices

Crunchbase

Spotify   −

Spotify has acquired the Brooklyn-based blockchain startup Mediachain Labs, whose

New Insurance Products

AXA Is Using Ethereum's Blockchain for a New Flight Insurance Product

Sep 13, 2017 at 17:50 UTC by Stan Higgins

Record Keeping

Delaware Blockchain Legislation to Revolutionize Corporate Record Keeping

By IncNow | Published July 31, 2017

Delaware corporations are now able to store corporate records on a blockchain, thanks to legislation passed this week by the Delaware General Assembly and signed by Governor John Carney.

This innovative legislation allows Delaware companies to finally toss the stacks of paper stock ledgers collecting dust on shelves, and provides a secure and immutable electronic record of share activity that eliminates opportunity for bookkeeping errors and costly ownership disputes.

With the current paper-based system, tracking stock ownership in a corporation as it grows and changes produces a nightmare for many companies. It is a challenge to reconstruct the stockholders at any given point in time, including the exact number of shares held and any restrictions or agreements that apply to

FedEx Moves Forward With Blockchain Logistics Plans

Nikhilesh De ✉ 🐦 🔊

🕐 Feb 1, 2018 at 03:18 UTC | Updated Feb 2, 2018 at 02:23 UTC

FedEx, which is part of BiTA's standards board, launched a pilot program using blockchain to store data for dispute resolution, said vice-president of strategic planning and analysis Dale Chrystie. The project hopes to establish what data would be needed for a permanent ledger to ease disputes between customers sending and receiving goods through FedEx.

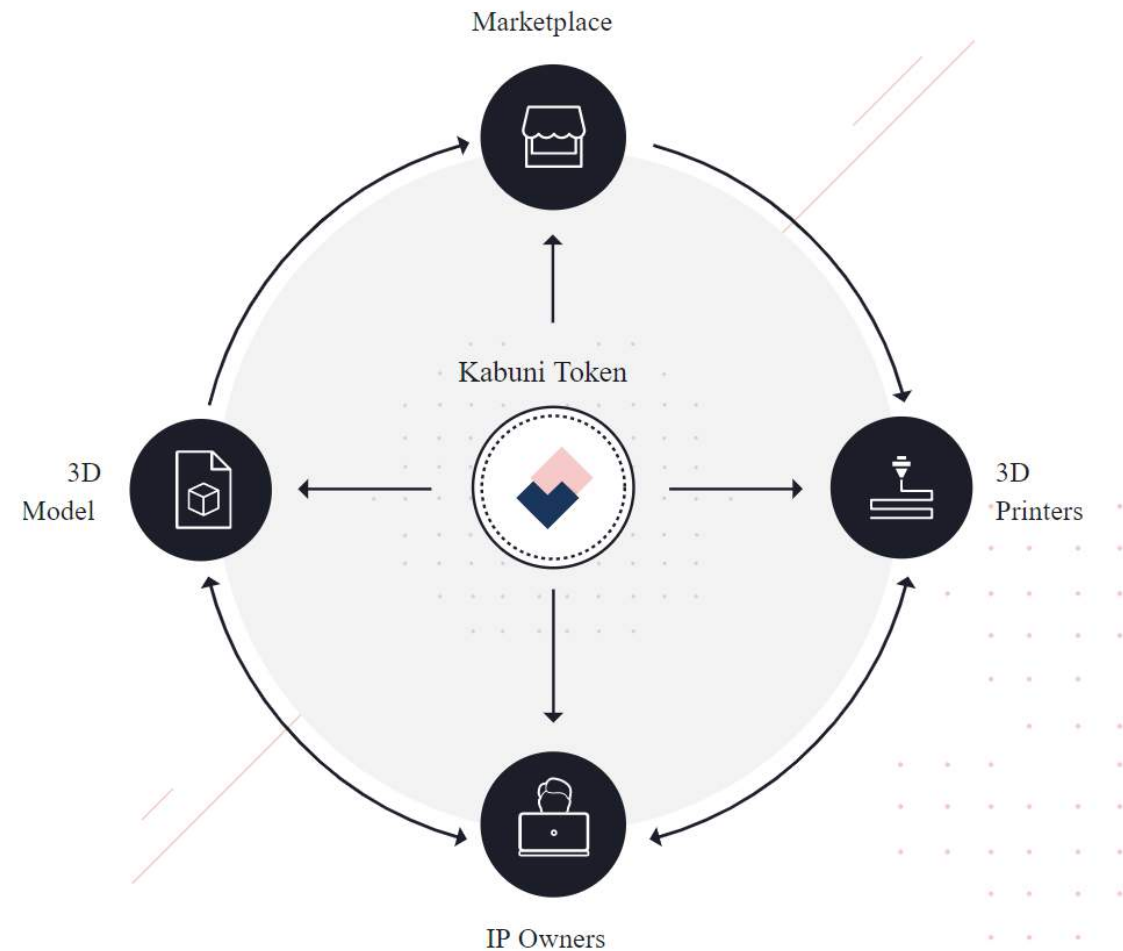The shipping giant also wants to use blockchain to store its records, he said, expanding:

> "We have millions of records a day in our system, and we think of blockchain as a secure chain of custody that could transform the logistics industry. We believe it holds a lot of promise in that space and would streamline all that data exchange in a very secure way."

Manufacturing

Blockchain is a **GREAT OPPORTUNITY** for our economy, for our society

Thank you!

Laurent Féral-Pierssens

Blockchain Advisory, KPMG Canada

Partner, Inception Block Ventures

in linkedin.com/in/pierssens