What is Blockchain and how does it work…

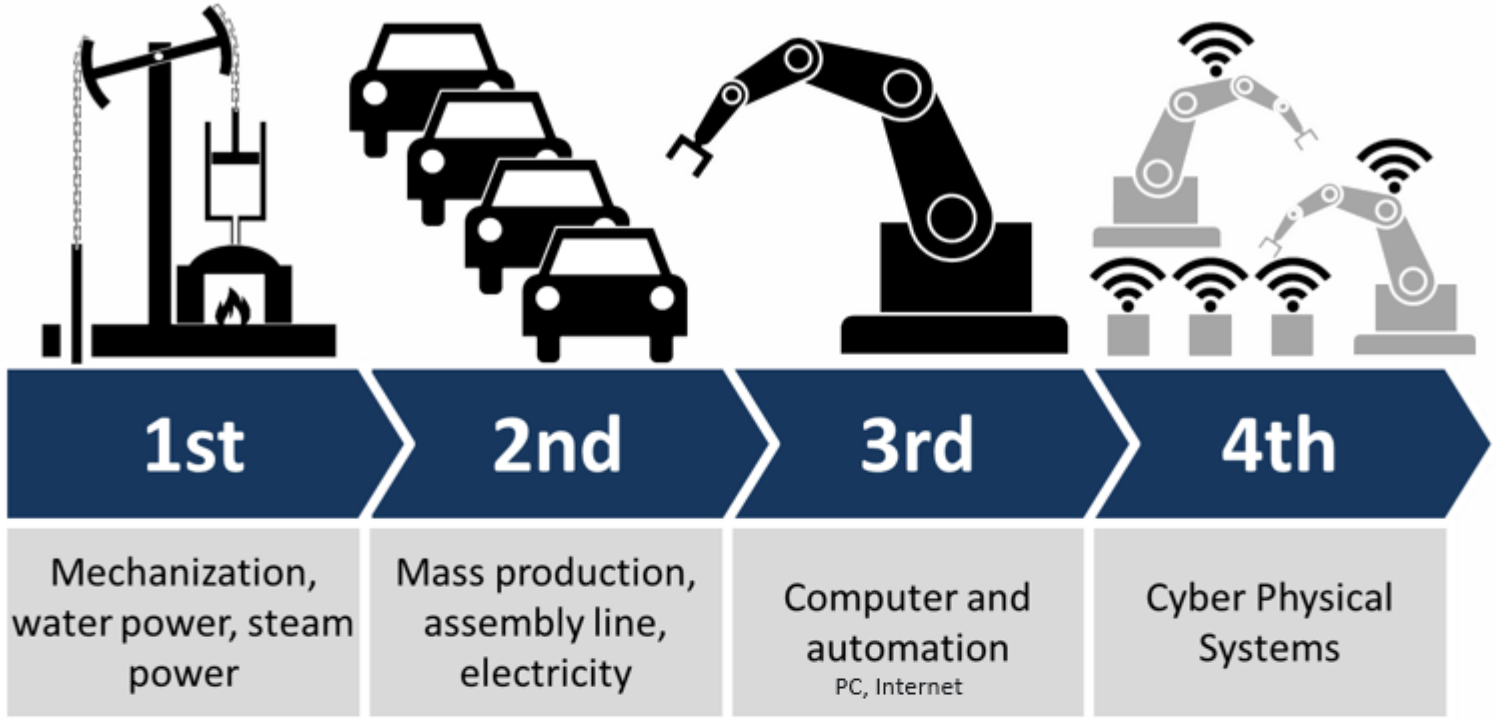
[Χωρίς τίτλο]

George Panou, MBA CBP
Group Digital Innovation Director @Mellon Technologies
Member of the Board @Hellenic Blockchain Hub
Certified Blockchain Instructor IIB Council

What is Blockchain and how does it work

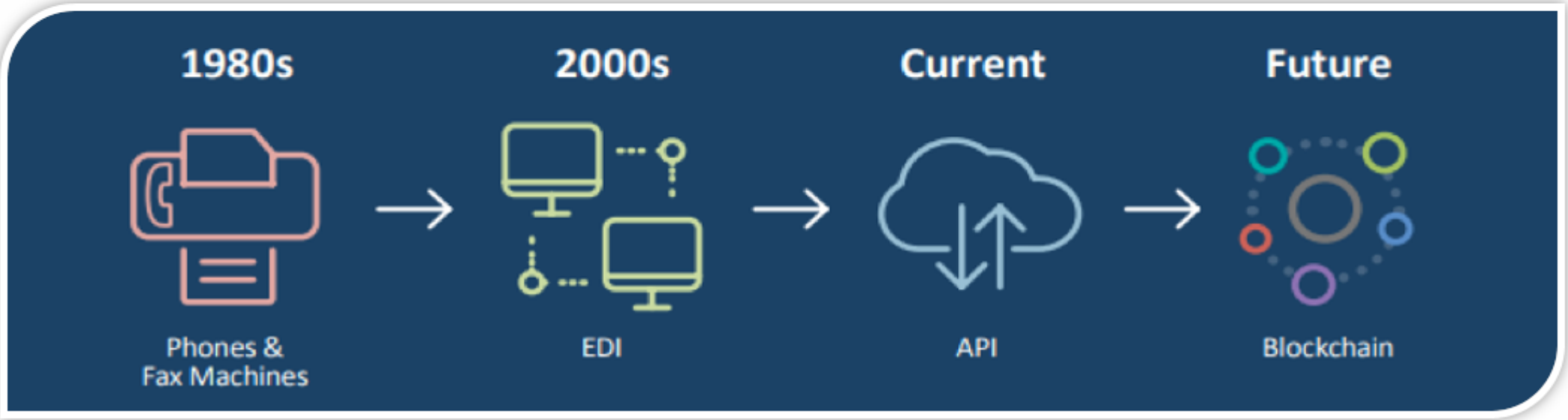
Blockchain, What is and how does it work

Real life blockchain implementations across industries in Enterprise level



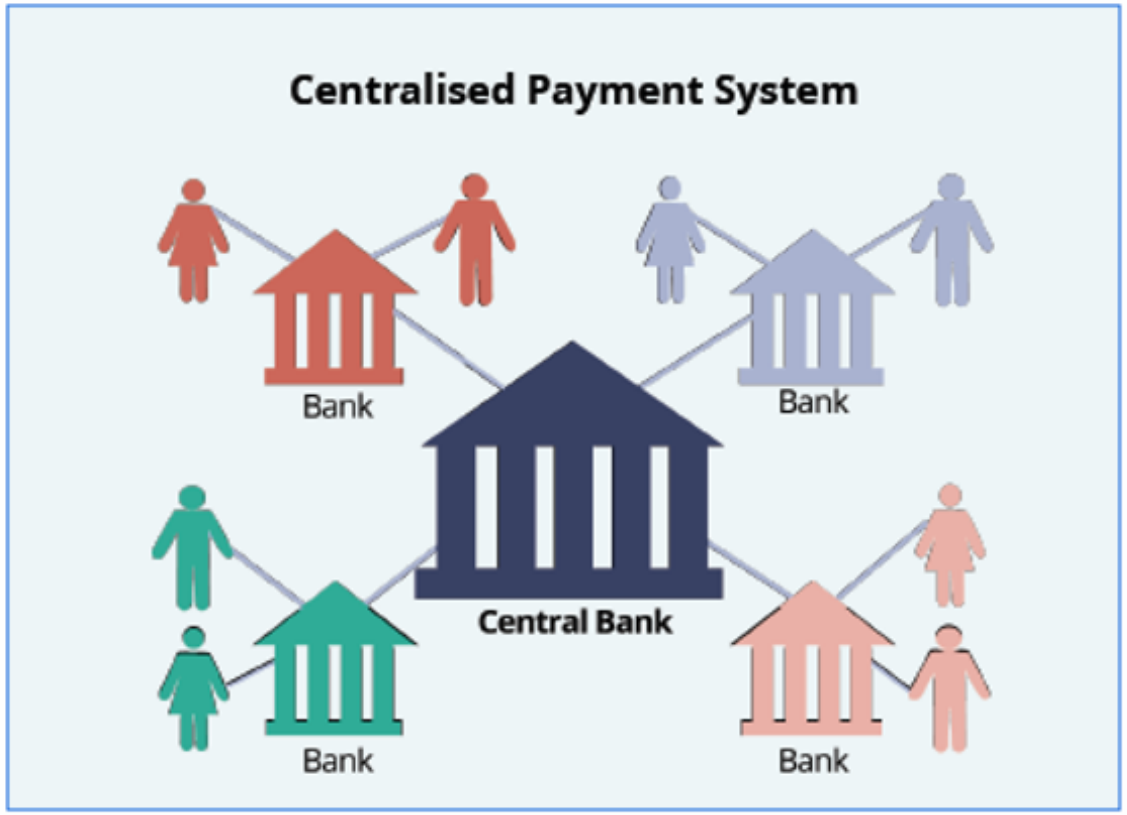
- Robotics,
- Artificial Intelligence,
- Nanotechnology,
- Quantum computing,
- Biotechnology
- The Internet of Things (IoT)
- **Decentralized Consensus**
- 3D printing
- autonomous vehicles

From internet ... to internet of value ...



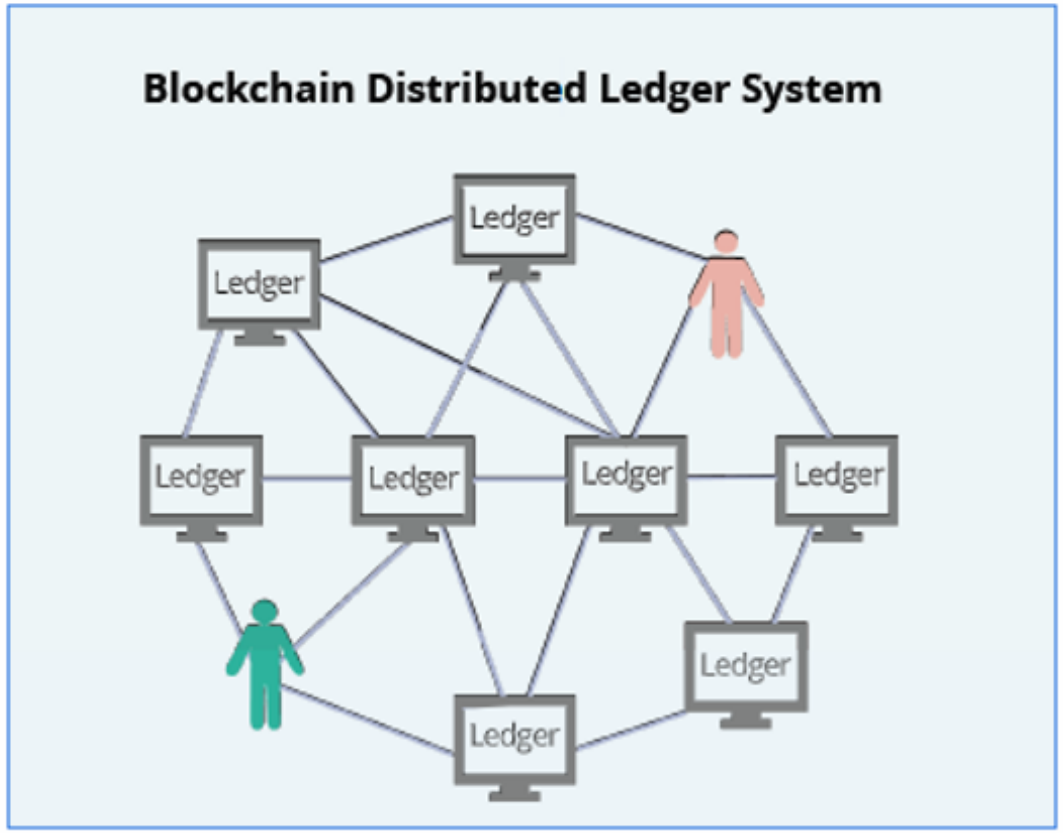
Financial crisis | **trust** | need for transparency & accountability

The Emergence of the Blockchain



http://www.imf.org/external/pubs/ft/fandd/2016/06/adriano.htm

Centralized bank tracks payments between clients

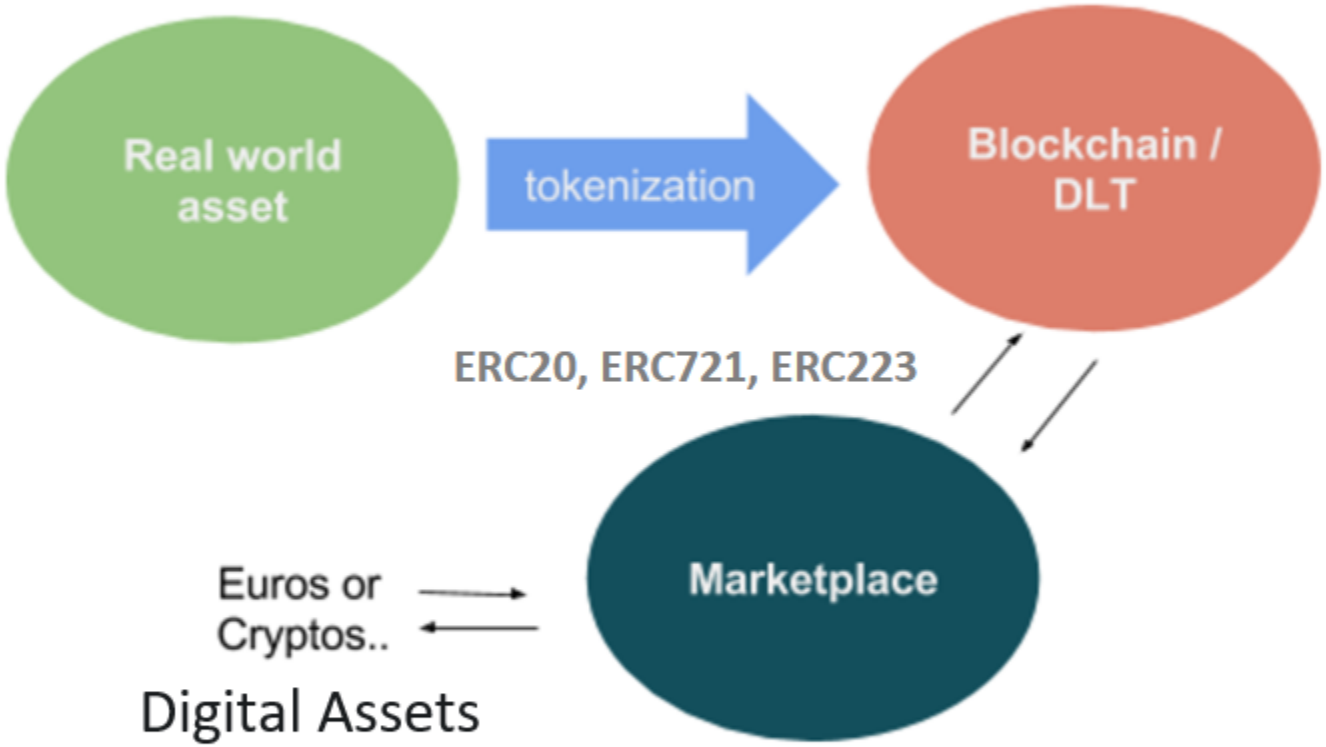


Network nodes store transaction record settled by many individuals

Platform & P2P economy

We live in a "**Platform Economy**"

Token economy



Companies, products and services eventually will become digital. Those who will not turn in to digital will leave a digital shadow behind them and eventually be obsolete and extinct

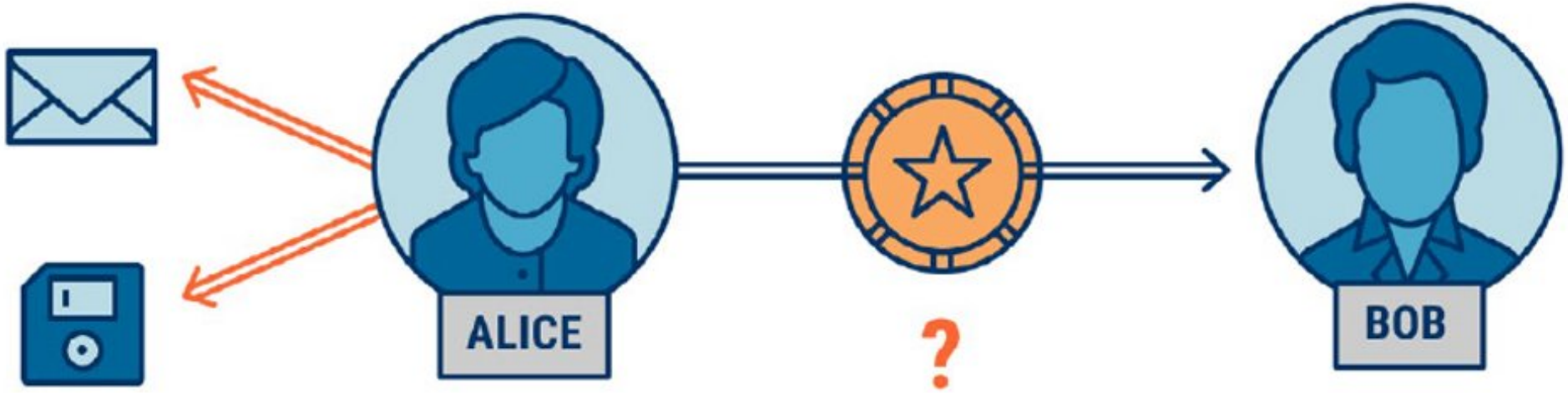
What is Blockchain Technology by WEF

Physical Transaction

Alice can't give Charlie the same token, because she no longer has the token to give — she gave it to Bob. But what if the same transaction were digital?

Source: CBS Insights

Digital Transaction



If Alice and Bob "own" the same string of ones and zeros, who is the true owner of the digital token?

One answer: use a database — a ledger.

Source: CBS Insights

Digital Transaction: Ledger

What if Dave decides to charge a fee that neither Alice or Bob want to pay?

Or, what if Alice bribes Dave to erase her transaction?

Physical Catastrophe? Hacker attack?

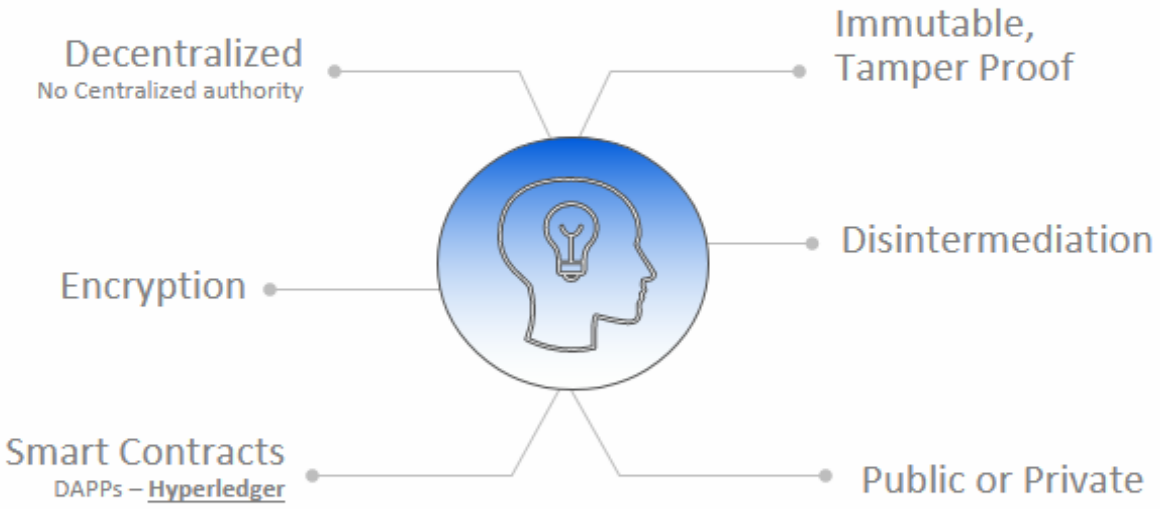
Source: CBS Insights

Decentralized Ledger

When a lot of people have a copy of the same ledger, it becomes more difficult to cheat. If Alice or Bob wanted to falsify a transaction, they would have to compromise the majority of participants, which is much harder than compromising a single participant.

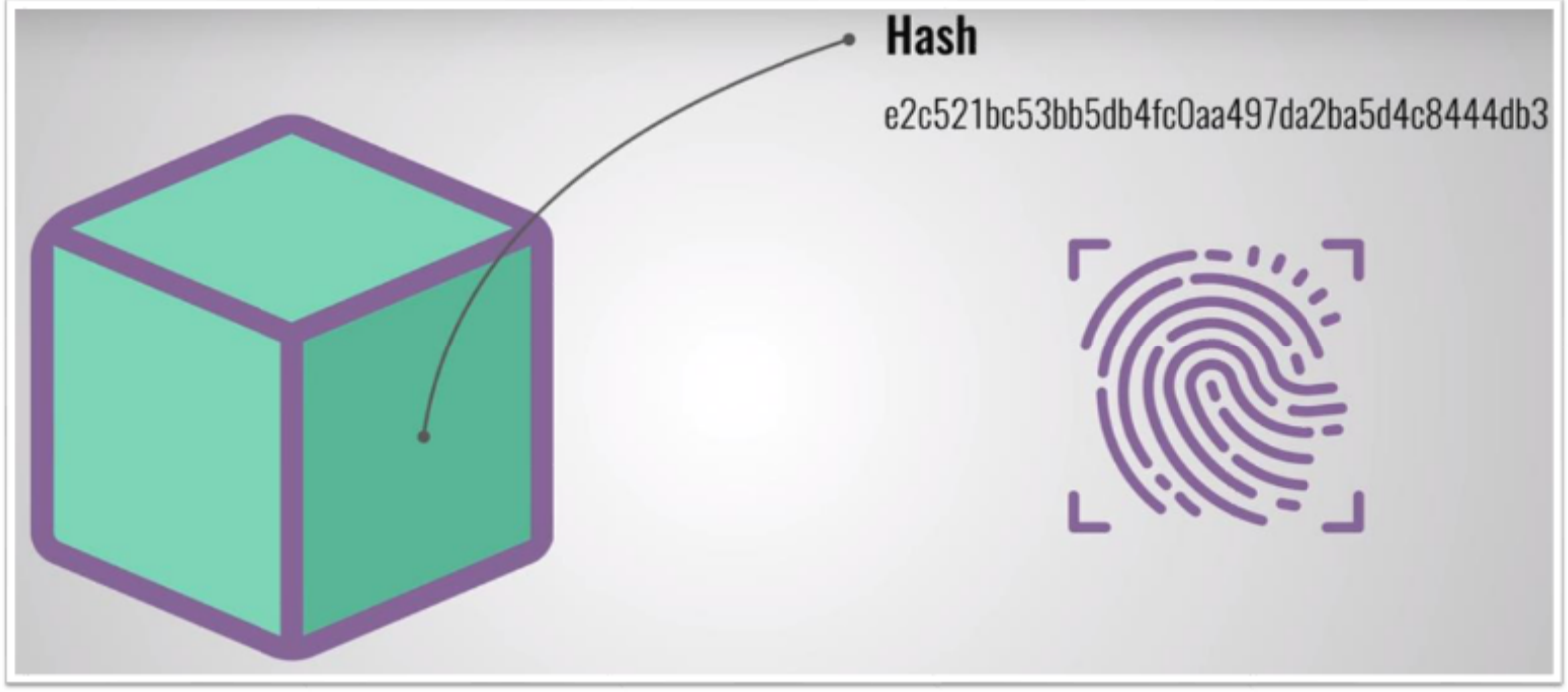
Source: CBS Insights

Blockchain Simplified



...a digital, distributed ledger, public or private, on which transactions or data are interconnected in data blocks. Using math and cryptography they become virtually immutable and undisputable from all distributed nodes that have shared the data...

Block



Hash 32 Bytes or 64 in HEX

d8a928b2043db77e340b523547bf16cb4aa
483f0645fe0a290ed1f20aab76257

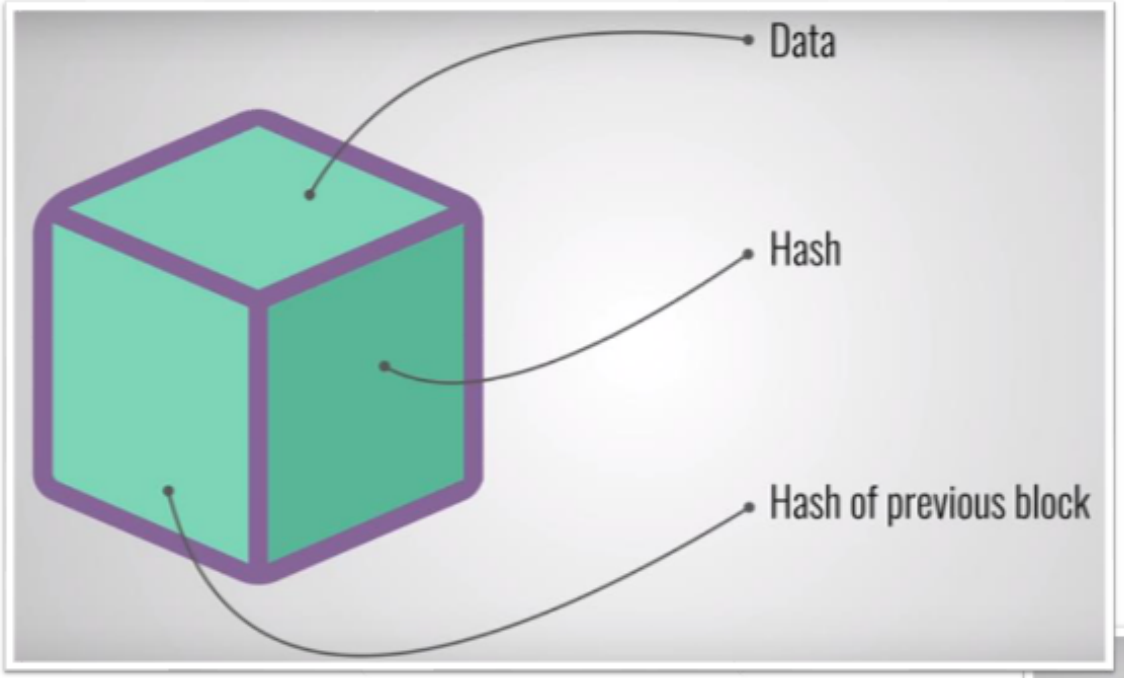
Bitcoin uses double hashing:

- **RIPEMD160**(SHA256(x)) called Hash160 which produces a 160 bit output: Bitcoin addresses
- **SHA256**(SHA256(x)) called Hash256 which produces a 256 bit output

- Once block is created its **hash is being calculated** (unique as fingerprint).
- Changing something inside **block will cause the hash** to change.
- Hashes are useful to detect **data block changes**, if changed so it is not the same block.

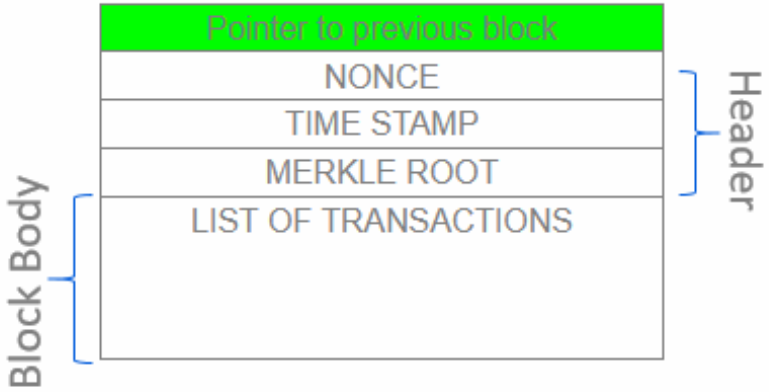
- They are collision resistant – almost impossible for two different inputs to have the same output
- They are non-reversible – output → input only by trial-and-error
- Bitcoin mostly uses SHA-256

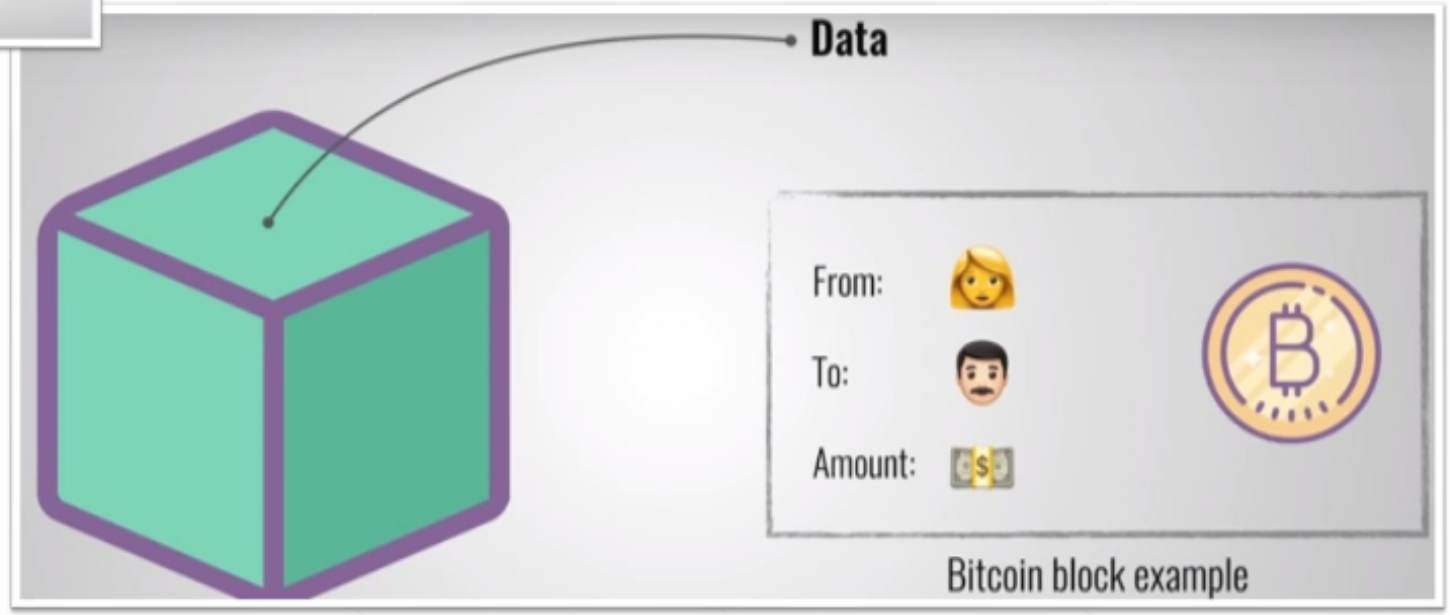
Block



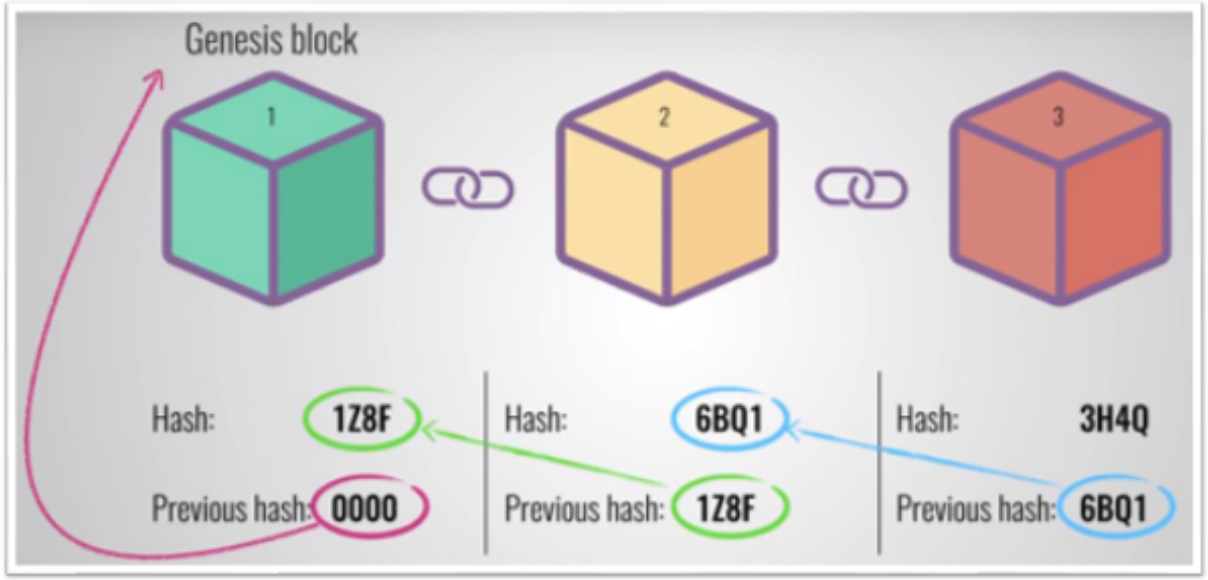
- Data stored in blocks connected to other blocks

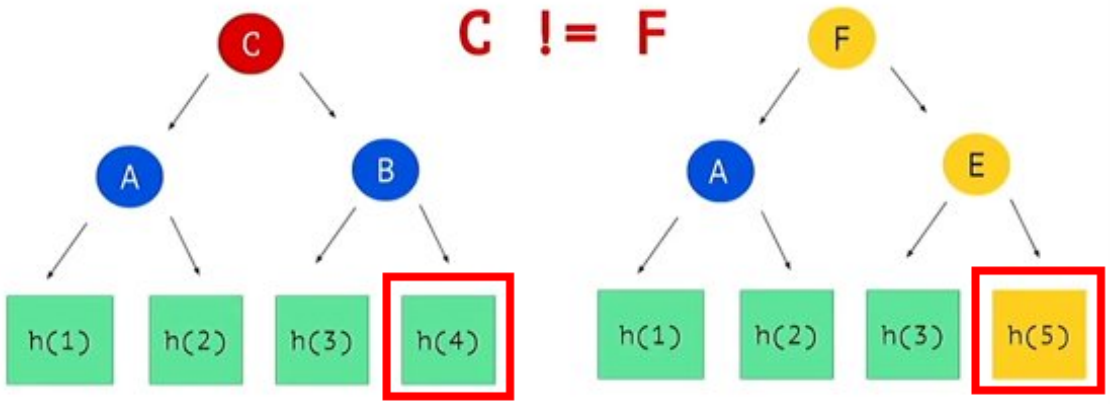
Bitcoin uses double hashing:
- **RIPEMD160**(SHA256(x)) called Hash160 which produces a 160 bit output: Bitcoin addresses
- **SHA256**(SHA256(x)) called Hash256 which produces a 256 bit output

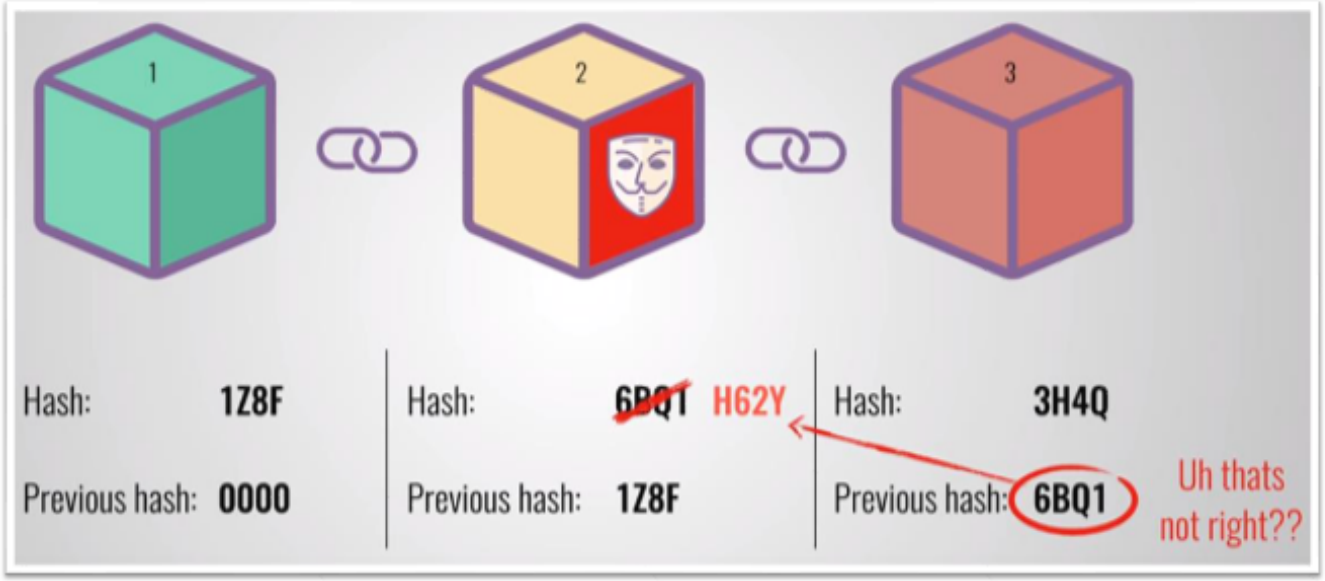




Block connection and tamper proof protection

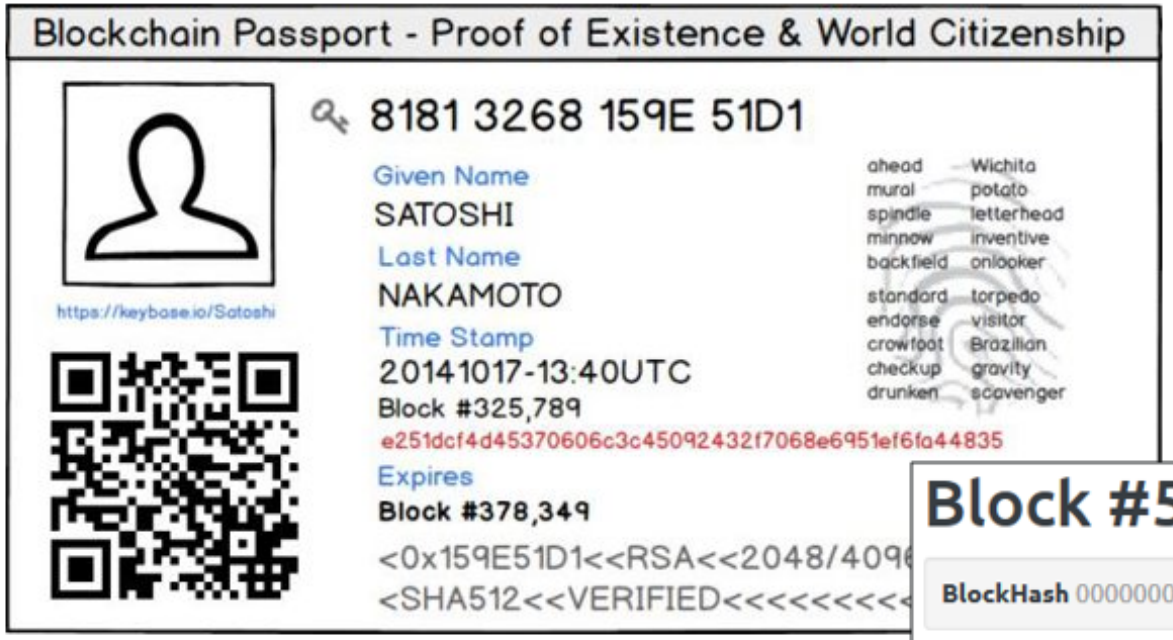






Talk is cheap.
Show me the blockchain

Blockchain identification



My Public Key Identifier :

JwDfJJPGguVWe9N6vkPAqYBovoVCYgobj

Bitcoin Transaction

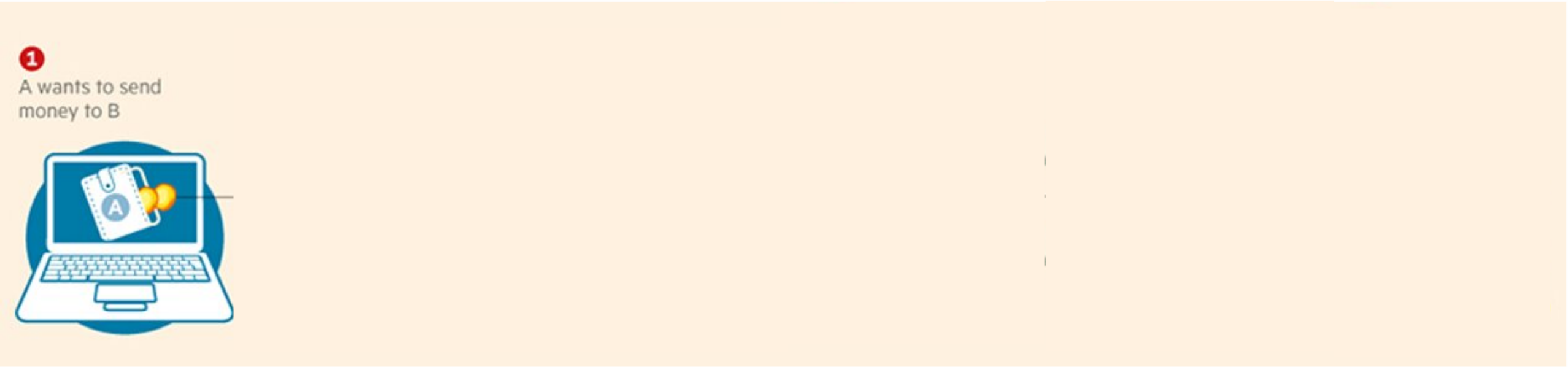
Block #568109

BlockHash 0000000000000000000bc077150030875daa008e83fc96e875de5ea0d5906401

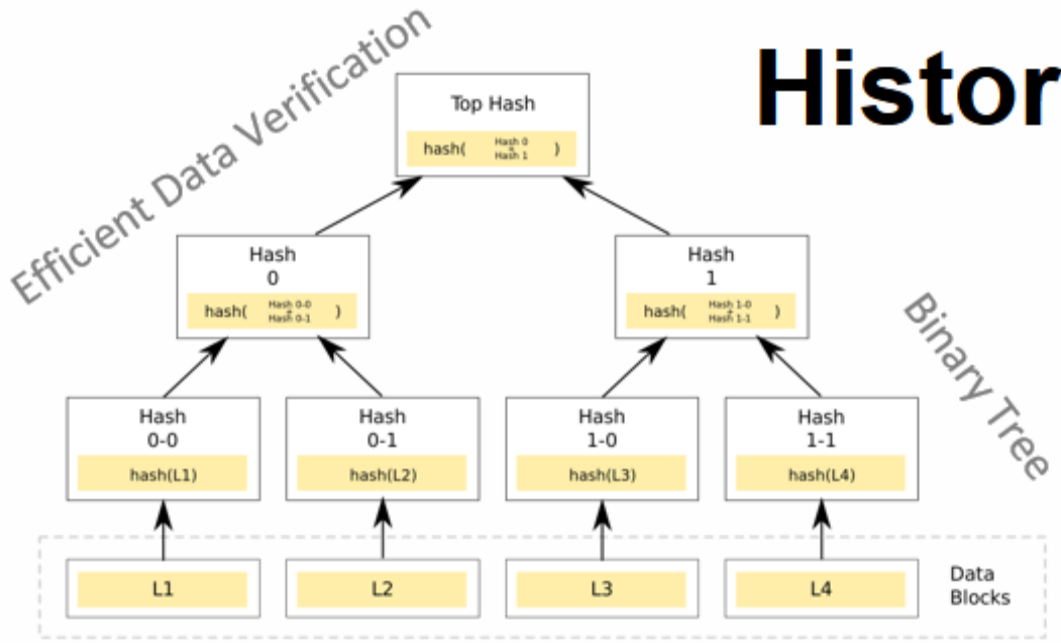
Summary

Number Of Transactions	3226	**Difficulty**	6068891541676.553
Height	568109 (Mainchain)	**Bits**	172e6117
Block Reward	12.5 BTC	**Size (bytes)**	901644
Timestamp	Mar 21, 2019 11:52:57 AM	**Version**	536870912
Mined by		**Nonce**	1212005713
Merkle Root	898d61fd8cf7aa3cd8884bc...		
Previous Block	568108		

Sending Money Using Blockchain Tech



History of Blockchain



Merkle Trees

hash( ) ->

```
2cf24dba5fb0a30e26e83b2ac5
b9e29e1b161e5c1fa7425e7304
3362938b9824
```

One Way encryption to 32 bytes
Similar data cannot have the same hash output
+ salt

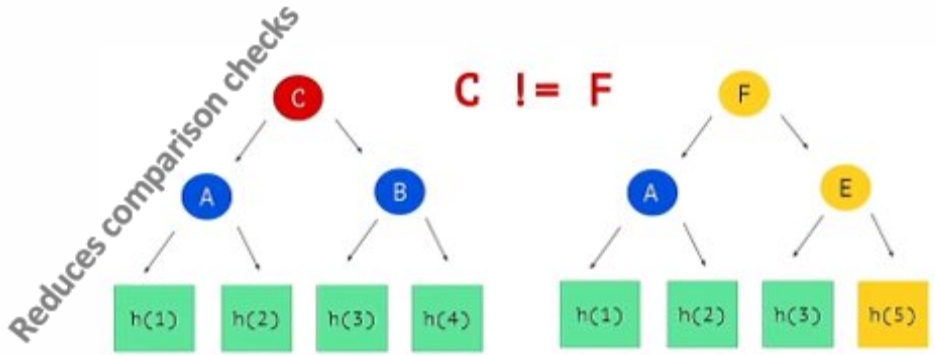
2008

Satoshi Nakamoto
Bitcoin

Proof of Work (POW)

1991

Tamper-proof doc system Habert & Stornetta



Blockchain Adoption

2015

Exploration & Investment

- Initial capability & use case assessments
- Early adoption likely for internal reconciliation

2016–2017

Early Adoption

- Leading-edge banks see the value of blockchain and begin deployments for asset classes that are bilaterally traded and/or have no central clearing authority
- Regulatory certainty drives adoption for external uses
- Regulatory authorities realize the benefits of blockchain for auditing and compliance, and rule-making begins

2018–2024

Growth

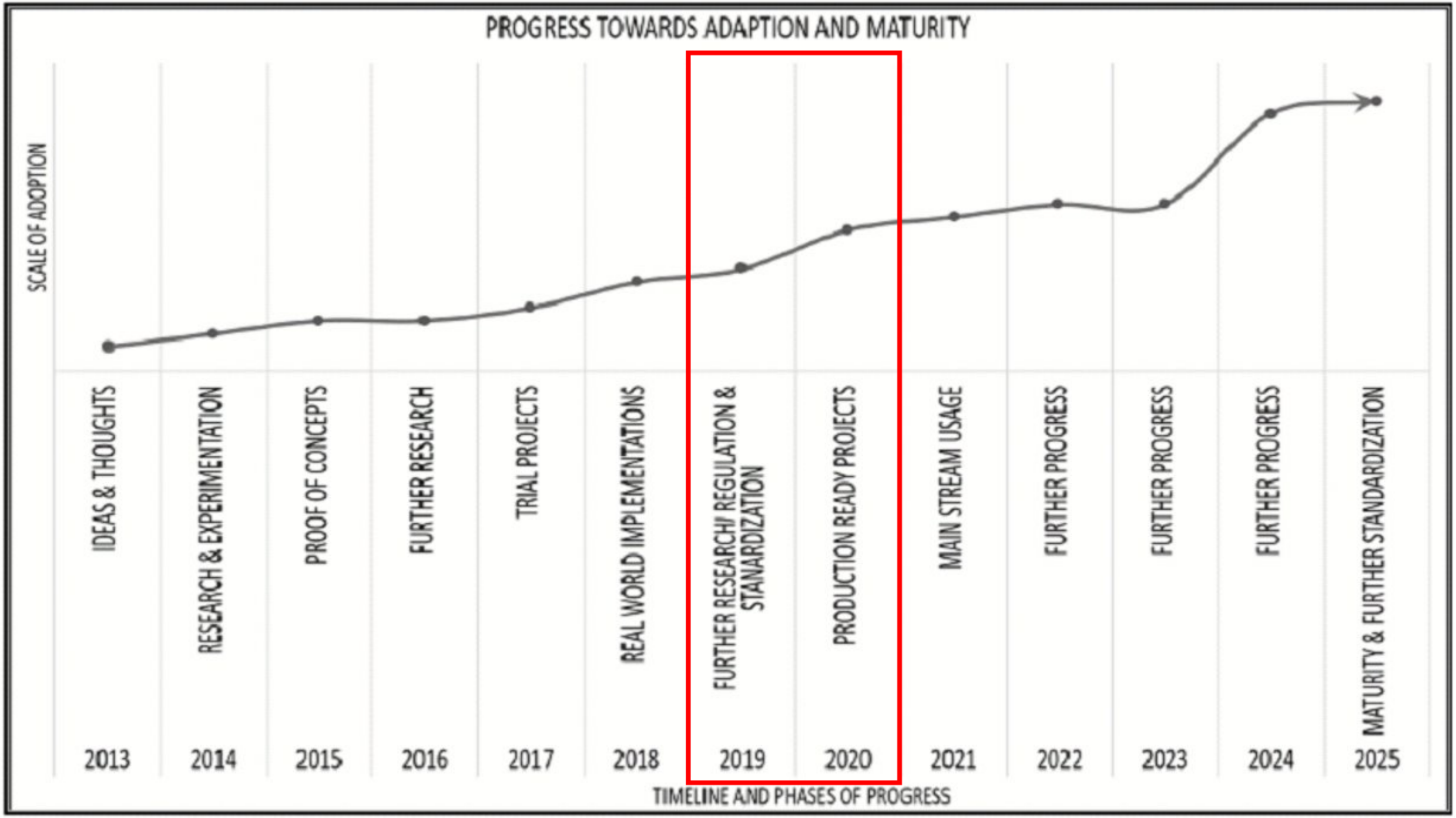
- Banks begin to see the benefits accorded to early adopters and – combined with regulatory guidance and certainty – the network effect takes hold
- New service providers and models emerge
- Deployments go viral across numerous asset classes
- New products and services are created; incumbent processes and services are discarded

2025

Maturity

- Blockchain adoption is considered mainstream and integral to the capital markets ecosystem

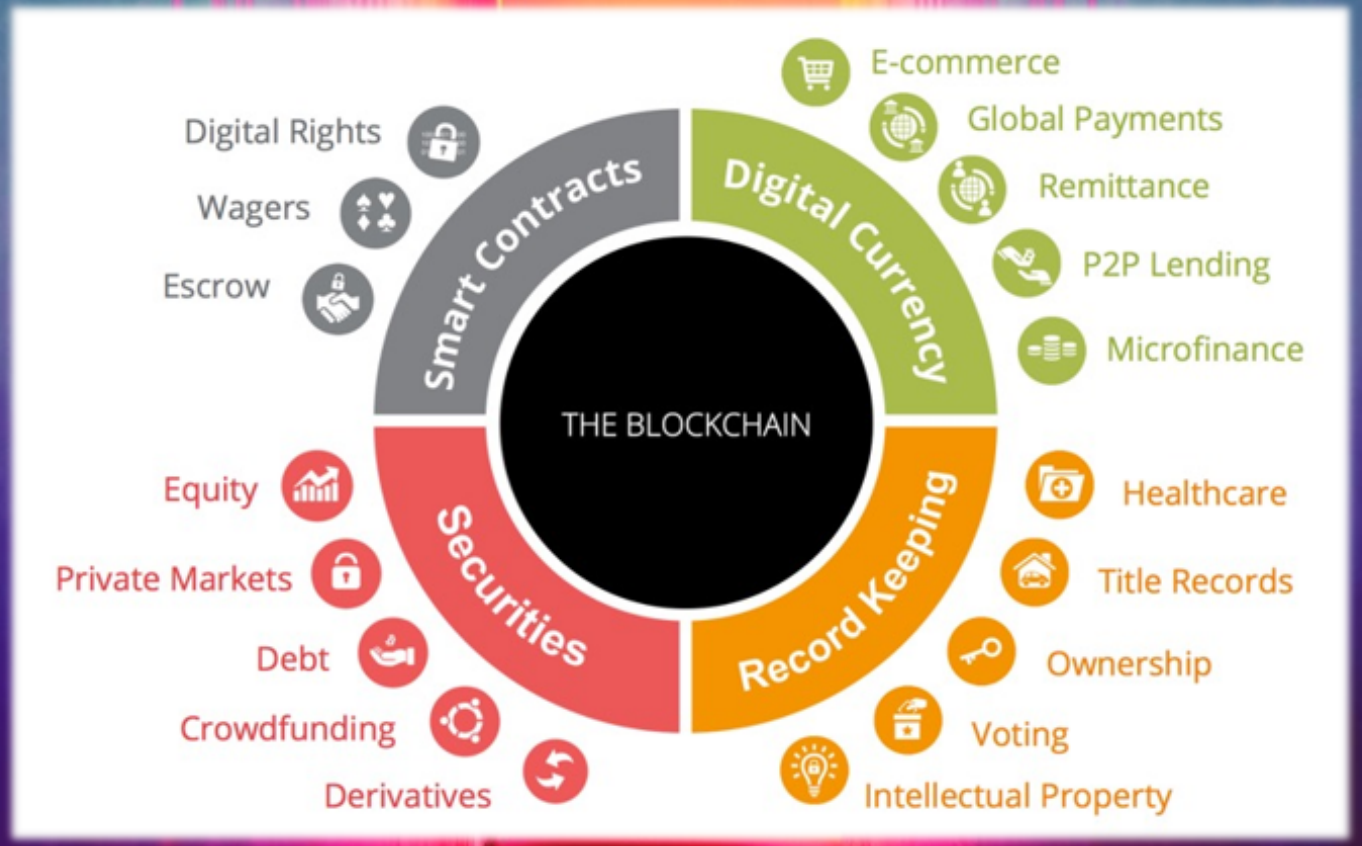
Source: Accenture Research


PROGRESS TOWARDS ADAPTION AND MATURITY
SCALE OF ADOPTION
IDEAS & THOUGHTS
RESEARCH & EXPERIMENTATION
PROOF OF CONCEPTS
FURTHER RESEARCH
TRIAL PROJECTS
REAL WORLD IMPLEMENTATIONS
FURTHER RESEARCH/ REGULATION & STANARDIZATION
PRODUCTION READY PROJECTS
MAIN STREAM USAGE
FURTHER PROGRESS
FURTHER PROGRESS
FURTHER PROGRESS
MATURITY & FURTHER STANDARDIZATION
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
TIMELINE AND PHASES OF PROGRESS

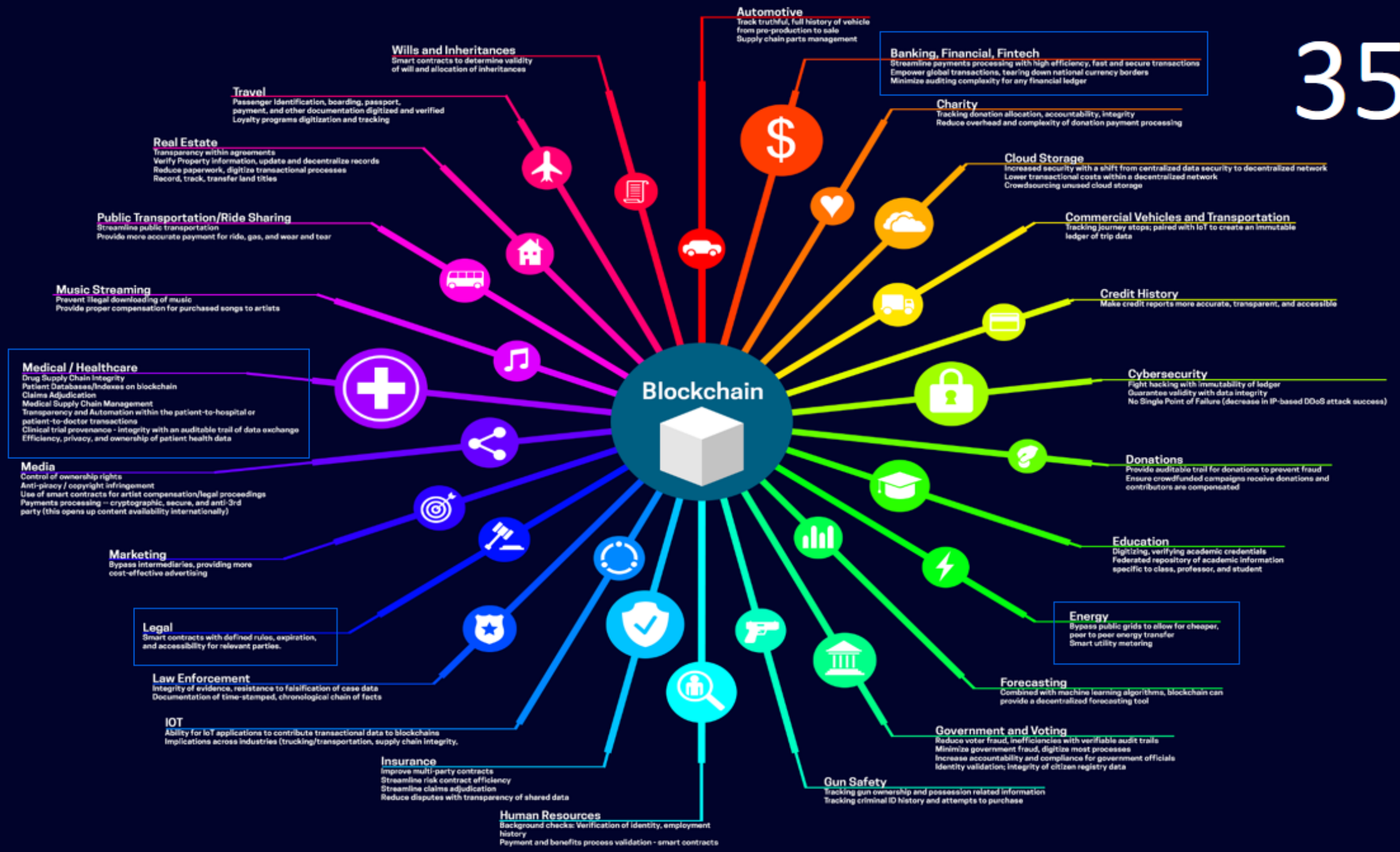
Fast – Removes Cost - Decentralized - Secure

Blockchain Everywhere Securing Digital Currency - Data - Securities providing Trust

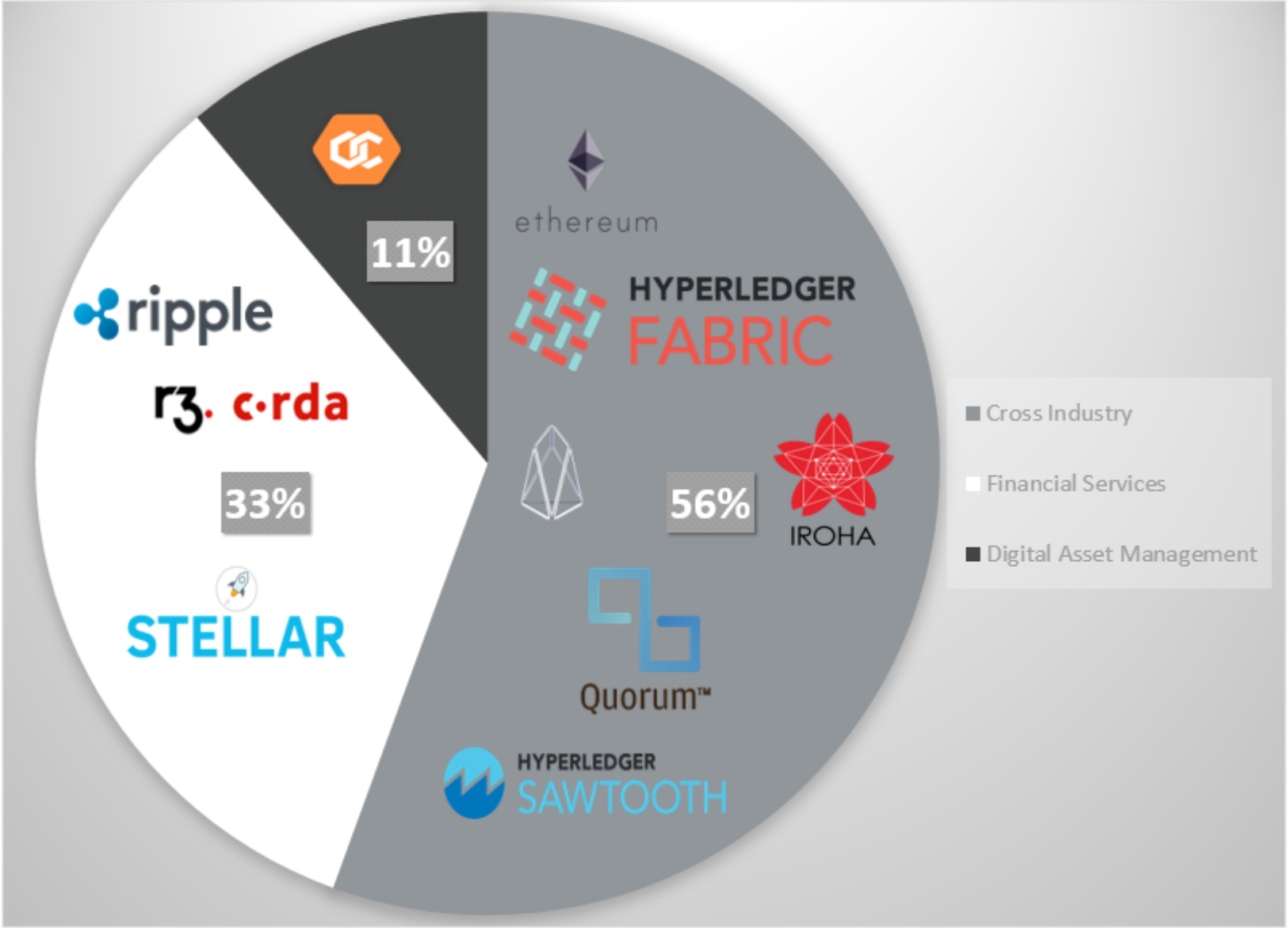
A technology that disrupted the IT landscape in a manner that was not witnessed since the advent of the Internet.



BLOCKCHAIN APPLICATIONS



Blockchain Platforms Landscape



Ledger Type

Permissionless
Permissioned
Both Public & Private

Consensus Algorithms

Proof of Work
Delegated Proof of Stake
Majority Voting
Pluggable Framework
Chained Based Byzantine Fault Tolerant
Stellar Consensus Protocol
Partitioned Consensus

Smart Contracts

Programmable actions
on most of the ledgers

Source: LeewayHertz

Blockchain Platforms

Indicative Selection

Cross Industry

Hyperledger Fabric is another project of Hyperledger, intended for building blockchain based solutions or applications using a modular architecture.

Blockchain companies prefer building enterprise-grade applications using this *blockchain platform*.

Cross Industry

Founded in late 2013, Ethereum is an open-source and blockchain based distributed computing platform proposed by Vitalk Buterin.

Ether is a native cryptocurrency of Ethereum, used for fueling the Ethereum ecosystem.

Financial Services

Built on the advanced blockchain technology, XRP is more scalable and faster than other blockchains. Ripple uses probabilistic voting to reach the consensus between nodes.

Big brands like **Santander**, American Express, **MoneyGram** International, SBI Holdings, and Deloitte are testing the potential of Ripple's Blockchain and planning to integrate it to make the existing payment processes secure and faster.

BLOCKCHAIN

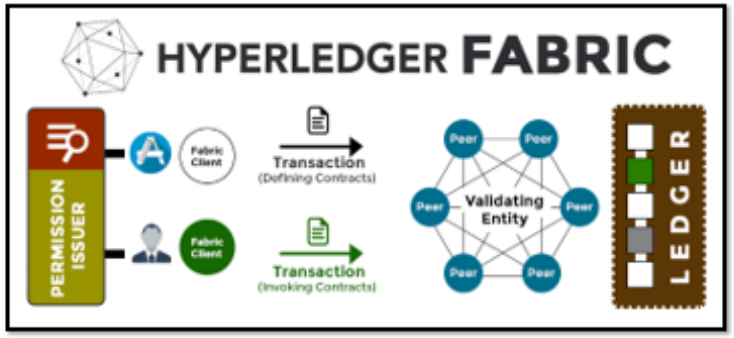
2

Blockchain Real World Examples

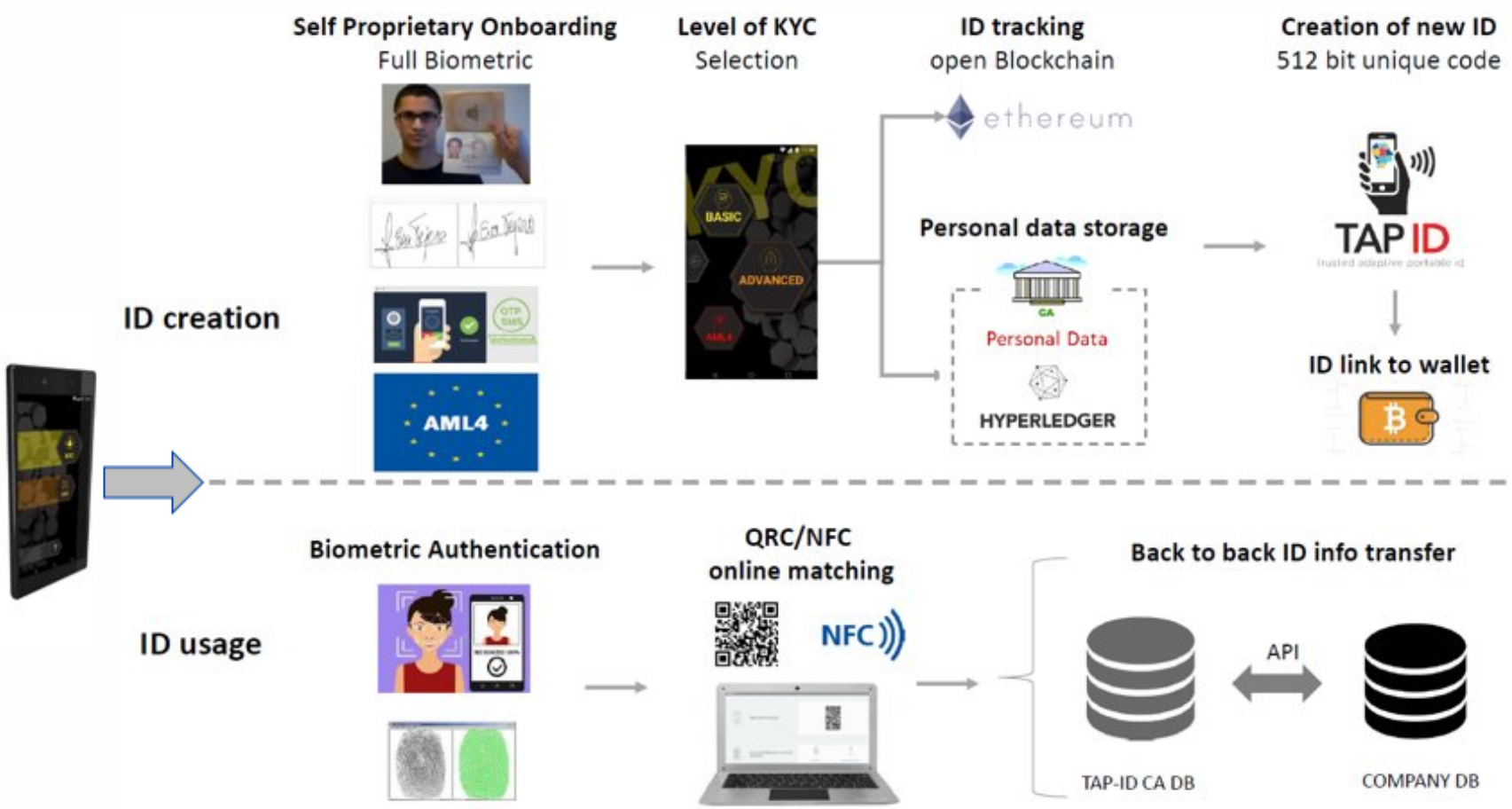
Land Titles
University Degrees
Supply Chain
Birth Certificates

Blockchain Real World Examples

Real life blockchain implementations across industries in Enterprise level



Self-sovereign Identity / KYC Digital Onboarding



1. REQUEST
   New client visits institution's portal from his smartphone and starts the onboarding
2. PERSONAL DATA
   users has to fill in their personal data
3. CREDENTIALS
   An OTP is sent to user's email and phone
4. OCR
   Take a picture of the document. Document validity is verified and the OCR reads the personal information
5. FACE BIOMETRIC MATCHING
   To prove his identity, the client receives the instructions to take pictures of himself. The biometrics of the face are compared to the pictures on the documents
6. PROOF OF LIVENESS
   Users has to prove their liveness blinking, and voice recording
7. SIGNATURE
   Users upload a photo of their signature or they sign in real-time
8. PROOF OF ADDRESS
   For example using a utility bill
9. AML verification
10. ONBOARDING COMPLETE
    The client is registered in the institution's system

GDPR and AML4 compliant

Jordan refugee camp that runs on blockchain.

Blockchain helps solve unsolvable problems in authentication and privacy

Building Blocks

Source: MIT Technology Review

Though Bassam may not know it, his visit to the supermarket involves one of the first **uses of blockchain for humanitarian aid**.

By letting a machine scan his iris, he confirmed his identity on a traditional United Nations database, queried a family account kept on a variant of the Ethereum blockchain by the World Food Programme (WFP), and settled his bill without opening his wallet.

PROVENANCE

A Blockchain Platform for Business

91% of business leaders believe that transparency builds trust. Provenance makes it easy for your business to bring trustworthy information to the point of sale, helping you to build brand trust now and into the future.

Source: The Consumer Goods Forum & Futerra Report, 2018

HEALTH & NUTRITION
Vegetarian

ANIMAL WELFARE
Pasture Raised

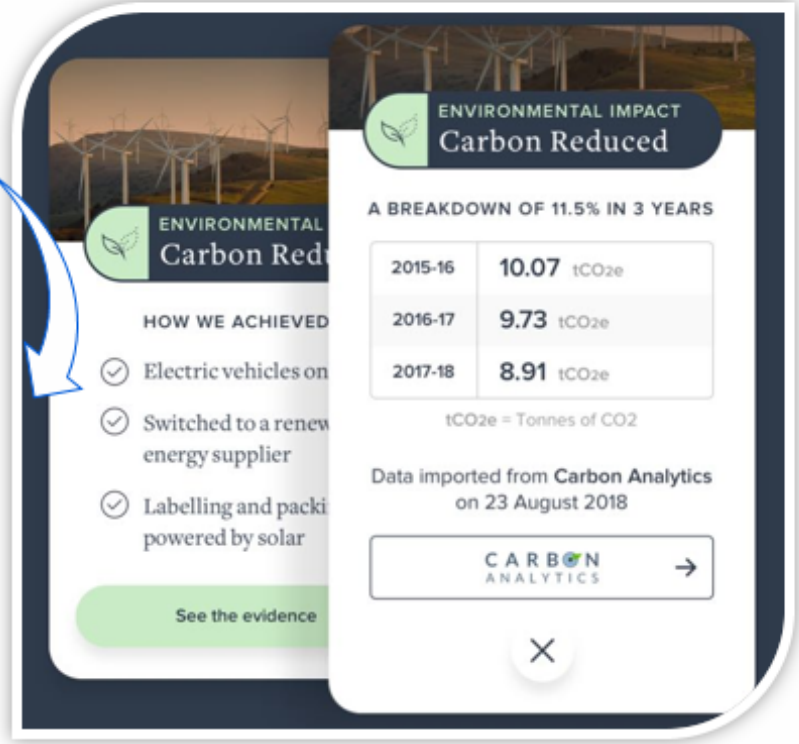
SAFETY & QUALITY
Sulfate-free

SOCIAL IMPACT
Fair Payment

ENVIRONMENTAL IMPACT
Carbon Reduced

"We've reduced our carbon footprint by 11.5% in 3 years."

See how →

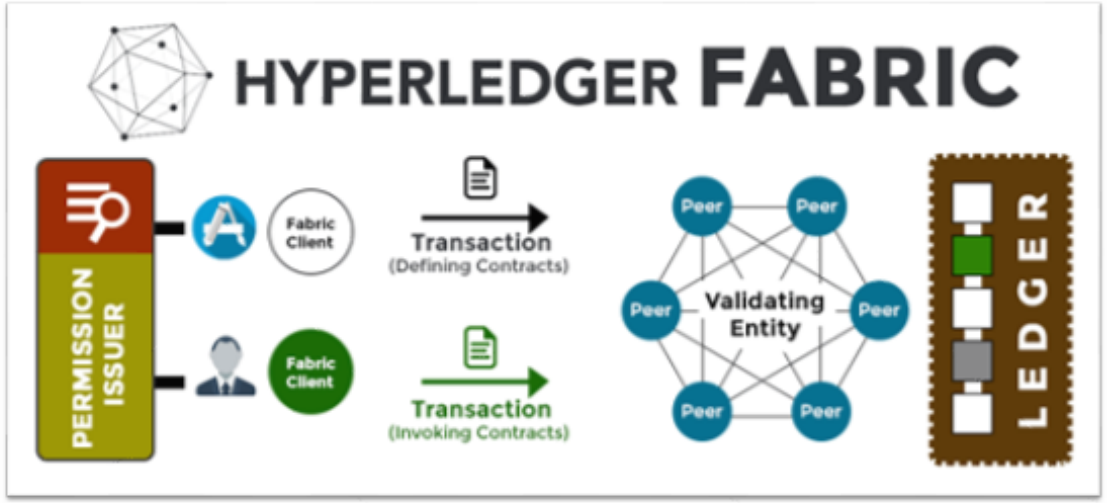


Removing paperwork
by using blockchain to create a tamper-proof "master ledgers" between trading parties

Creating "smart contracts"
that check when new records are written, ensure there are no out of balance conditions, and remove the existence of 'bad' invoices

Having a single system of record
replicated across all partners to a transaction, which enables the impartial enforcement of contract terms

French Court Clerks to Use IBM Blockchain Platform for Corporate Registry



It will be used to record and share information related to:
- the exchanges of regulatory information related to companies' difficulties
- the changes of status of the company registered on the French territory (change of court office in which a company is registered; change of corporate names; the addition of a new branch office; or even dissolution of the business, etc…)

PARIS, March 14, 2019 /PRNewswire/ -- IBM (NYSE: IBM) and the National Council of Clerks (NCC)

https://newsroom.ibm.com/2019-03-14-French-National-Council-of-Clerks-of-Commercial-Courts-announce-the-deployment-of-a-blockchain-network-developed-by-IBM-to-streamline-the-management-of-commercial-and-corporate-registry

THANK YOU

George Panou

3 DECEMBER 2019