# Part 7

# Quantum Machine Learning (QML)

- Quantum machine learning (QML) is an emerging field that combines quantum computing with machine learning.

- Machine learning is a subfield of **artificial intelligence that focuses on developing algorithms that can learn from data and make predictions or decisions without being explicitly programmed.**
- Quantum computing is the area of study focused on developing computer technology based on the principles of quantum theory.
- The quantum computer, following the laws of quantum physics, would gain enormous processing power through the ability to be in multiple states, and to perform tasks using all possible permutations simultaneously.

- QML seeks to harness the power of quantum computing to improve machine learning algorithms and solve complex problems that classical computers cannot.
- In QML, quantum computing is used to **perform operations on quantum data, which are represented by quantum states**.
- These **quantum states can encode information in a way that allows for more efficient processing and storage of data**

# Components of QML

The components of Quantum Machine Learning include:

- **Quantum Circuits**: Quantum circuits are the building blocks of quantum algorithms. They are a series of *quantum gates* that operate on *qubits* to perform calculations.
- **Quantum Data**: Quantum data refers to data encoded in quantum states that can be manipulated by quantum algorithms. This data is typically represented as a collection of qubits.
- **Quantum Algorithms**: Quantum algorithms are the algorithms that operate on quantum circuits to solve machine learning problems. These algorithms leverage the power of quantum computing to solve problems that are intractable for classical computers.
- **Quantum Variational Circuits**: Quantum variational circuits are a type of quantum circuit that can be *trained* to solve optimization problems using classical optimization techniques.

- **Quantum Neural Networks**: Quantum neural networks are a type of quantum circuit that can be trained to solve machine learning problems using *backpropagation*.
- **Quantum Support Vector Machines**: Quantum support vector machines are a type of quantum algorithm that can be used to *classify* data into different categories.
- **Quantum Principal Component Analysis**: Quantum principal component analysis is a quantum algorithm that can be used to reduce the *dimensionality* of large dataset

# Advantages of QML

- One of the main advantages of QML is its **ability to perform calculations on a large number of possible inputs simultaneously**, a process known as **quantum parallelism**: *Its ability to perform certain types of computations exponentially faster than classical computers.*
- This is due to the fact that quantum computers can simultaneously compute many different outcomes at the same time. This can make it possible to solve problems that are currently intractable for classical computers.

- Another advantage is the ability of quantum computing *to perform optimization problems more efficiently*, which is useful in fields such as logistics and finance.
- One more advantage of QML is that it can **enable the development of new types of algorithms** that are not possible with classical computers.
- For example, quantum machine learning algorithms could be used to perform computations that are not based on classical probability distributions, or to create new models that can represent complex quantum states.

- QML has the potential to improve a wide range of machine learning tasks, such **as data clustering, classification, and regression analysis**.
- It can also be used for tasks such as **image and speech recognition, natural language processing, and recommendation systems**.

- Another key advantages of QML is its ability to **perform unsupervised learning tasks more efficiently**. *Unsupervised learning refers to the process of finding patterns in data without the use of labeled examples*. This is an important area of machine learning, as it can be difficult and time-consuming to manually label large datasets.

- QML could also have significant implications for fields such as finance, where it could be used to create more accurate models for predicting market trends and optimizing investment strategies.

# Challenges facing QML

• QML is still in its early stages of development, and there are many challenges that need to be overcome before it can be widely adopted. These challenges include **the need for better quantum hardware, improved algorithms, and better understanding of the relationship between quantum computing and machine learning.**

- In addition to that, one of the main challenges is **the difficulty of building stable and scalable quantum computers.**
- At present, quantum computers are still in the early stages of development, and there are significant technical hurdles that need to be overcome before they can be widely adopted.

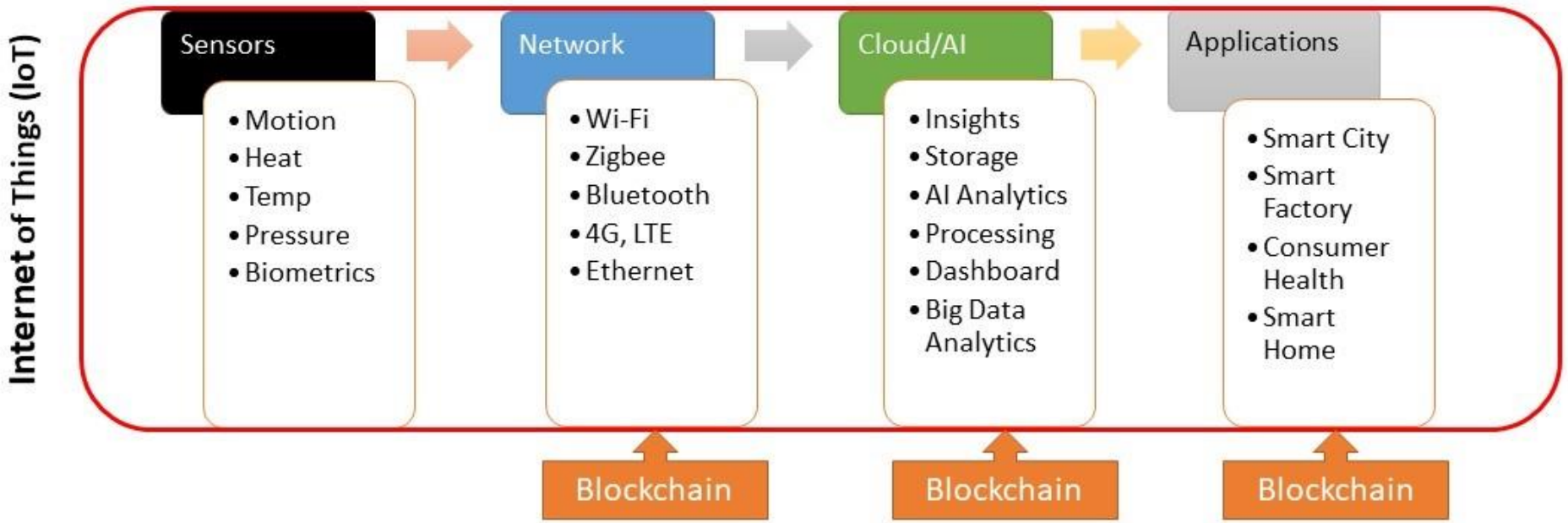
- One of the main challenges in developing QML is **the "quantum-classical gap.**" *This refers to the difficulty of translating classical machine learning algorithms into quantum algorithms, and vice versa*.
- Researchers are working on developing new techniques to bridge this gap and create hybrid algorithms that take advantage of both classical and quantum computing.

- There is currently a lot of interest in developing quantum machine learning algorithms that are "quantum-inspired." These algorithms don't actually run on a quantum computer, but they are designed to take advantage of certain quantum properties to create more efficient machine learning models.

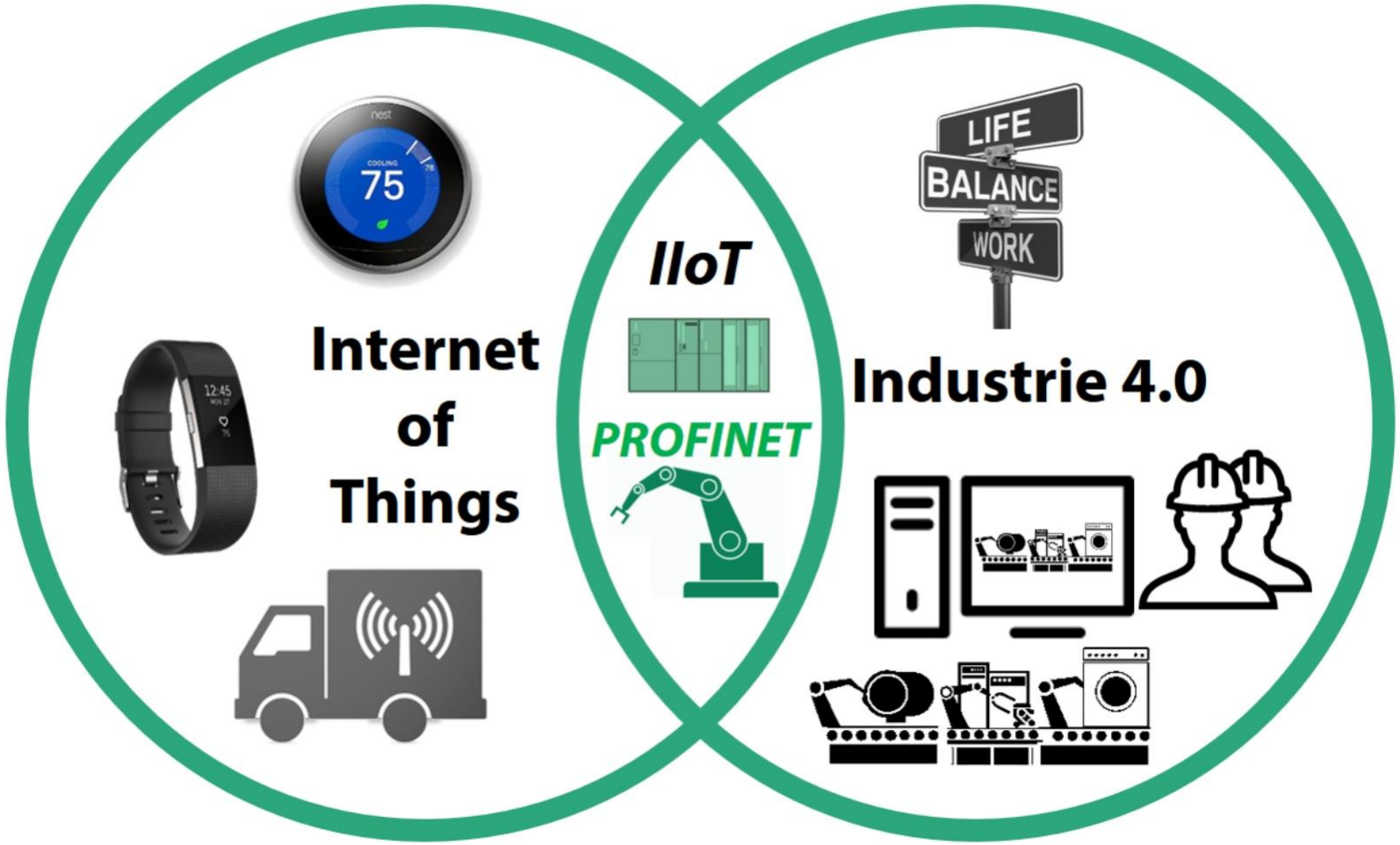
- Despite these challenges, there is a great deal of interest in QML among researchers and practitioners in the field of machine learning.
- As more progress is made in developing stable and scalable quantum computers, and as new algorithms and techniques are developed, we can expect to see significant advances in QML over the coming years.

# IoT

*The Internet of Things (IoT)* is the network of physical objects accessed through the Internet. These objects contain embedded technology to interact with internal states or the external environment.

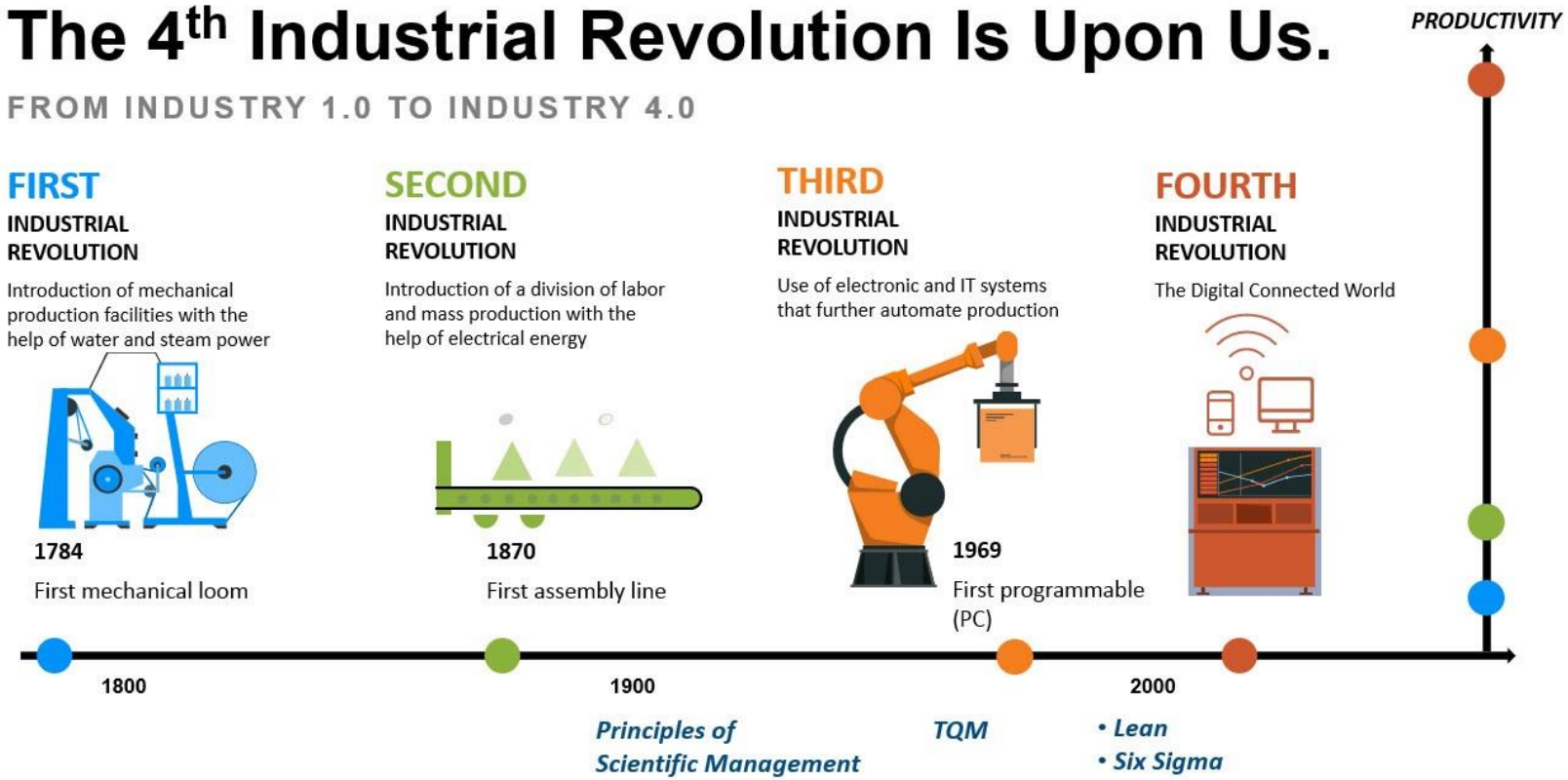



Source: Prof. Ahmed Banafa's Book "Blockchain Technology and Applications", 2020


nest
COOLING
75
78
12:45
MON 27
Internet
of
Things
IIoT
PROFINET
LIFE
BALANCE
WORK
Industrie 4.0

# The 4th Industrial Revolution Is Upon Us.

FROM INDUSTRY 1.0 TO INDUSTRY 4.0



Factfile

## History of industrial revolution

**1.0**

**1780 – Mechanisation**
Industrial production based on machines powered by water and steam

**2.0**

**1870 – Electrification**
Mass-production using assembly lines

**3.0**

**1970 – Automation**
Automation using electronics and computers

**3.5**

**1980 – Globalisation**
Offshoring of production to low-cost economies

**4.0**

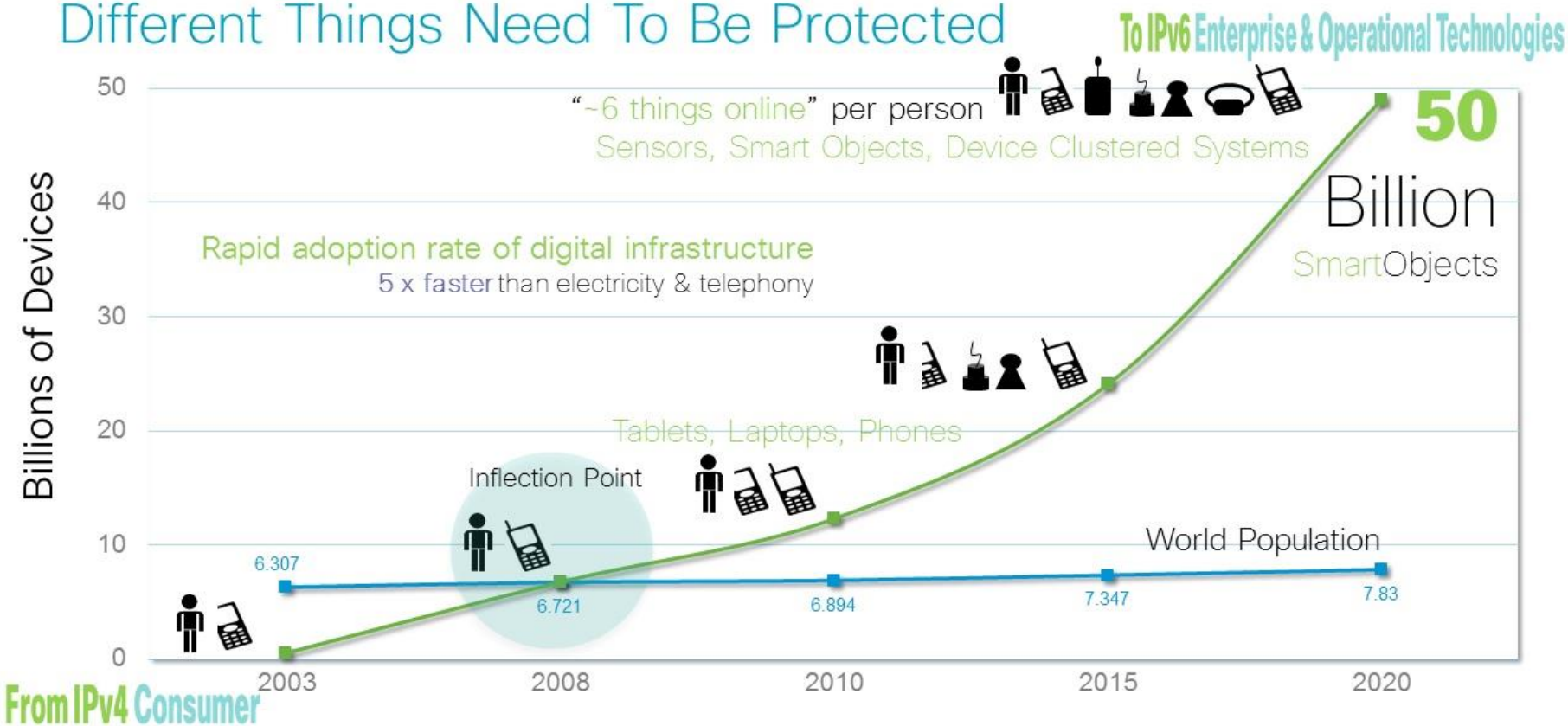
**Today – Digitalisation**
Introduction of connected devices, data analytics and artificial intelligence technologies to automate processes further

**5.0**

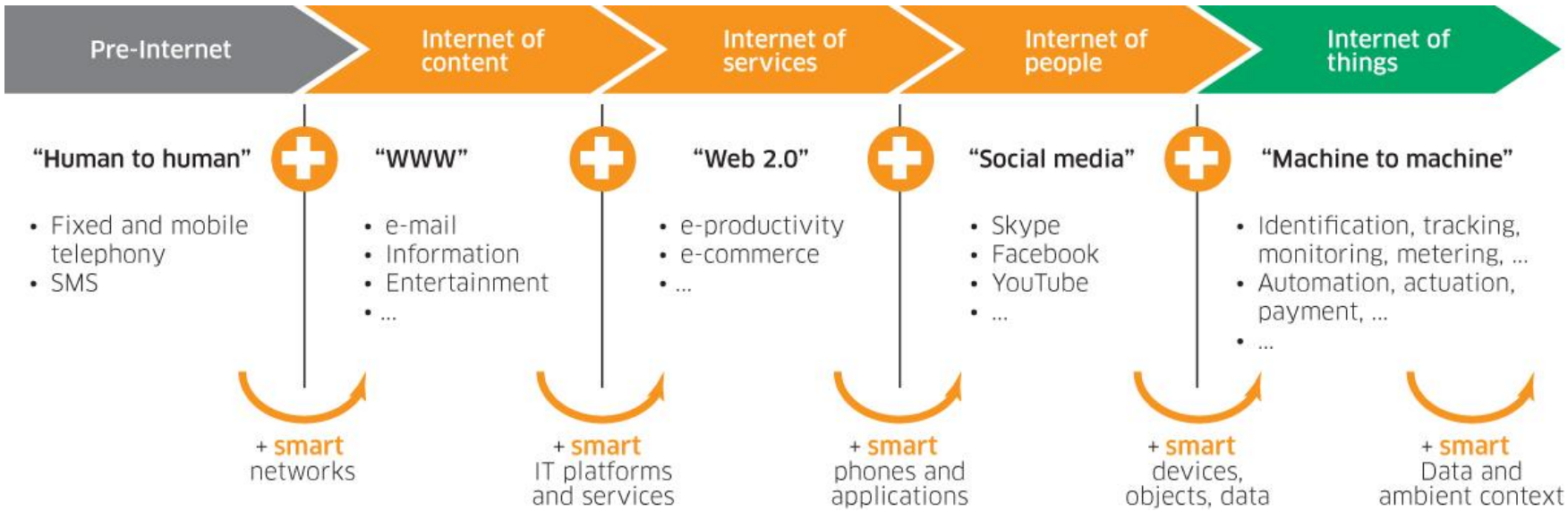
**Future – Personalisation**
The fifth industrial revolution, or Industry 5.0, will be focused on the co-operation between man and machine, as human intelligence works in harmony with cognitive computing. By putting humans back into industrial production with collaborative robots, workers will be upskilled to provide value-added tasks in production, leading to mass customisation and personalisation for customers

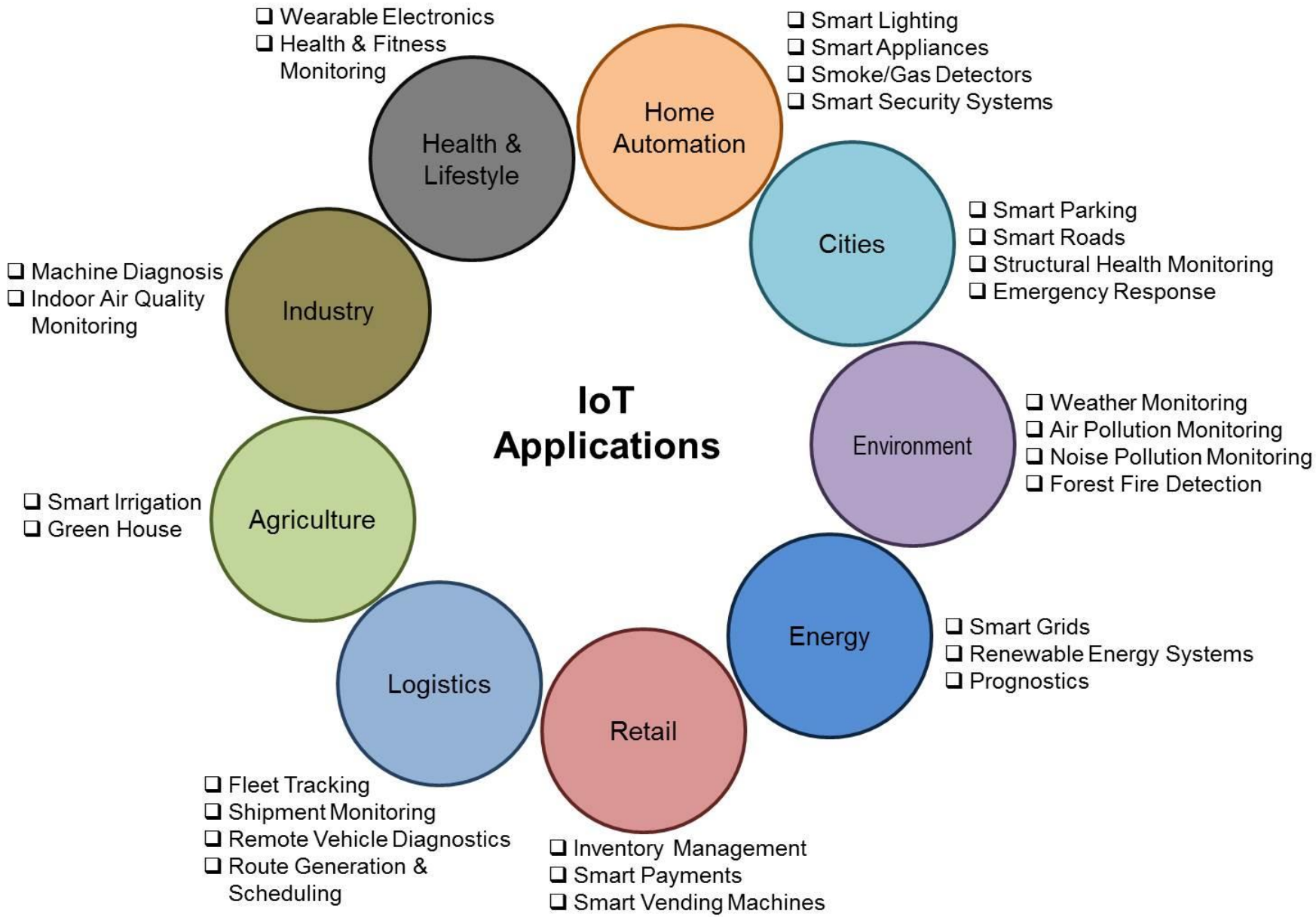
# How big is IoT ?

# Different Things Need To Be Protected




Source: Cisco IBSG projections, UN Economic & Social Affairs http://www.un.org/esa/population/publications/longrange2/WorldPop2300final.pdf


Pre-Internet
Internet of content
Internet of services
Internet of people
Internet of things
"Human to human"
• Fixed and mobile telephony
• SMS
+ smart networks
"WWW"
• e-mail
• Information
• Entertainment
• ...
+ smart IT platforms and services
"Web 2.0"
• e-productivity
• e-commerce
• ...
+ smart phones and applications
"Social media"
• Skype
• Facebook
• YouTube
• ...
+ smart devices, objects, data
"Machine to machine"
• Identification, tracking, monitoring, metering, ...
• Automation, actuation, payment, ...
• ...
+ smart Data and ambient context


IoT Applications
Health & Lifestyle
❑ Wearable Electronics
❑ Health & Fitness Monitoring
Home Automation
❑ Smart Lighting
❑ Smart Appliances
❑ Smoke/Gas Detectors
❑ Smart Security Systems
Cities
❑ Smart Parking
❑ Smart Roads
❑ Structural Health Monitoring
❑ Emergency Response
Environment
❑ Weather Monitoring
❑ Air Pollution Monitoring
❑ Noise Pollution Monitoring
❑ Forest Fire Detection
Energy
❑ Smart Grids
❑ Renewable Energy Systems
❑ Prognostics
Retail
❑ Inventory Management
❑ Smart Payments
❑ Smart Vending Machines
Logistics
❑ Fleet Tracking
❑ Shipment Monitoring
❑ Remote Vehicle Diagnostics
❑ Route Generation & Scheduling
Agriculture
❑ Smart Irrigation
❑ Green House
Industry
❑ Machine Diagnosis
❑ Indoor Air Quality Monitoring

# Factors helping IoT ?

A number of significant technology changes have come together to enable the rise of the IoT. These include the following:

- *Cheap processing*
- *Smartphones*
- *wireless coverage*
- *Big data*
- *IPv6*


INDUSTRIAL
internet of Things
CONSUMER
internet of Things
Heavy Machinery
Transportation
Smart Cities
Automation
Factories
Healthcare
NETWORK CONNECTIVITY
Powered by Software
Wearables
Phones
TVs
Appliances
Home Monitoring
Home Automation
Graphic thanks to Vector Software
Antonio Grasso - @antgrasso

The challenges can be divided into 4 categories; Platform, Connectivity, Business Model and Killer Applications

- **Platform :** This category includes , form and design of the products (UI and UX) , analytics tools used to deal with the massive data streaming from all products in a secure way , and scalability which means wide adoption of protocols like IPv6 in all vertical and horizontal markets .

- **Connectivity:** Connectivity includes all parts of the consumer's day and night using wearables, smart cars, smart homes, and in the big scheme smart cities. From the business prospective we have connectivity using IIoT (Industrial Internet of Things) where M2M communications dominating the field.

- **Business Model:** The bottom line is a big motivation for starting, investing in, and operating any business, without a sound and solid business models for IoT we will have another bubble , this model must satisfied all the requirements for all kinds of e-commerce; vertical markets, horizontal markets and consumer markets.

- **Killer Applications**: Three functions needed in any killer applications, control “things”, collect “data”, analyze “data”.

# Quantum Computing and IoT

# Quantum Computing and IoT

- Consumers, companies, and governments will install **40 billion IoT** devices globally.
- Smart tech finds its way to every business and consumer domain there is—from retail to healthcare, from finances to logistics—and a missed opportunity strategically employed by a competitor can easily qualify as a long-term failure for companies who don’t innovate.

- Moreover, the 2020’s challenges just confirmed the need to secure all four components of the IoT Model: Sensors, Networks (Communications), Analytics (Cloud), and Applications
- One of the top candidates to help in securing IoT is Quantum Computing, while the idea of convergence of IoT and Quantum Computing is not a new topic, it was discussed in many works of literature and covered by various researchers, but nothing is close to practical applications so far.

- To understand the complexity of this kind of convergence, first, you need to **recognize the security issues of IoT**, second, comprehend the complicated nature of Quantum Computing.
- IoT system’s diverse security issues include

- *Data breaches* – IoT applications collect a lot of user data, and most of it sensitive or personal, to operate and function correctly. As such, it needs encryption protection.

- *Data authentication* – Some devices may have adequate encryption in place but it can still be open to hackers if the authenticity of the data that is communicated to and from the IoT device cannot be authenticated.

- *Side-channel attacks* – Certain attacks focus on the data and information it can gain from a system's implementation rather than vulnerabilities in the implementation's algorithms.

- *Irregular updates* – Due to the rapid advances in the IoT industry, a device that may have been secure on its release may not be secure anymore if its software does not get updated regularly. Add to that the famous SolarWinds's Supply Chain attack of 2020 which infected over 18,000 companies and government agencies using updates of office applications, and network monitoring tools.

- *Malware and ransomware* – Malware refer to the multitude of malicious programs that typically infects a device and influences its functioning whereas ransomware has the capabilities to lock a user out of their device, usually requesting a “ransom” to gain full use back again paid by cryptocurrency “Bitcoin”.

# Quantum Computing and IoT

• With its capabilities, quantum computing can help address the challenges and issues that hamper the growth of IoT. Some of these capabilities are ：

- *Optimized complex computation power*: With Quantum Computing the speed is incredibly high, IoT benefits from this speed since IoT devices generate a massive amount of data that requires heavy computation and other complex optimization.

- *Faster validation and verification process*: Quantum computing addresses that concern as it can speed up the verification and validation process across all the systems several times faster while ensuring constant optimization of the systems.

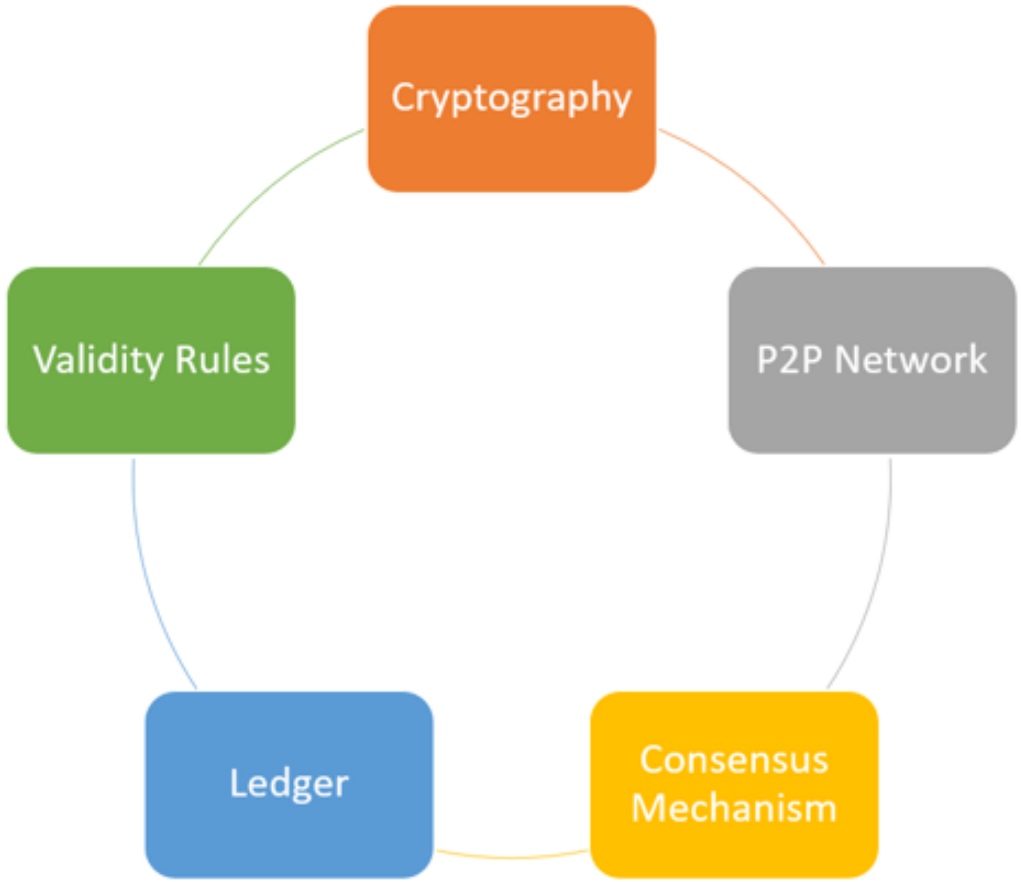
- *More secure communications*: A more secure communication is possible through *quantum cryptography* as explained before. The complexity serves as a defense against cyberattacks including data breaches, authentication, and malware, and ransomware.

# Blockchain

# Blockchain is a software

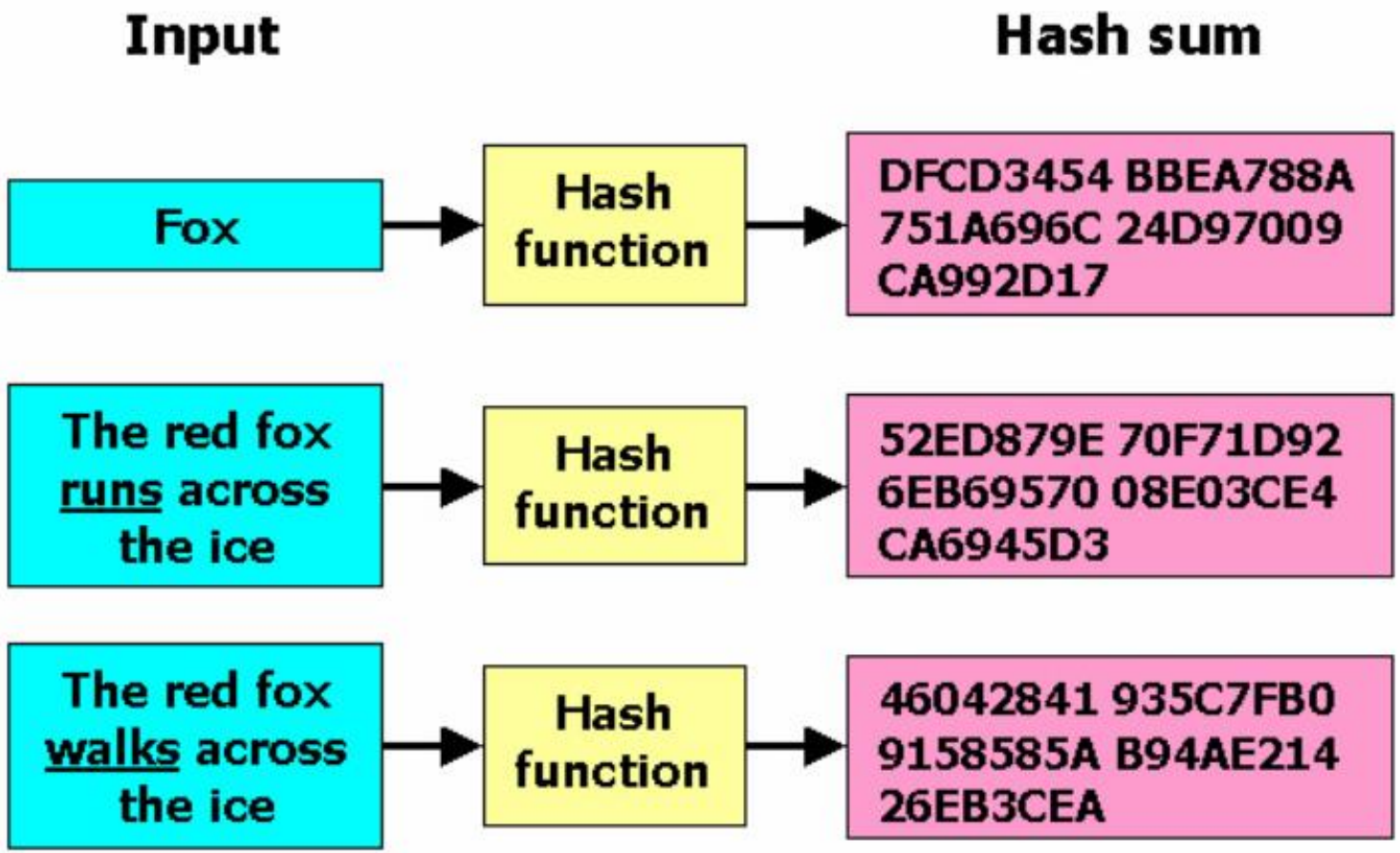
# Best Definition of Blockchain?


Dr. Abel Sanchez -MIT



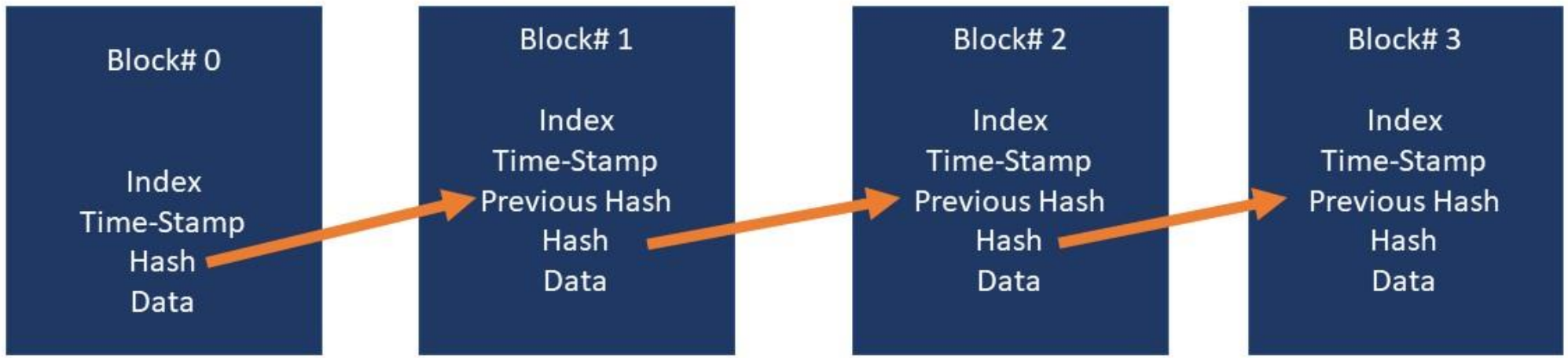

# Components of a Blockchain

Source: Prof. Ahmed Banafa's Book "Blockchain Technology and Applications", 2020




A cryptographic hash function, Image from Wikipedia

Node # 1




Node # 2

Node # 3

Node # 4

Other Nodes with same copy of Data,
they sync using *gossip protocol*

```
class Block {
        constructor(timestamp, transactions,
        previousHash = '') {
        this.previousHash = previousHash;
        this.timestamp = timestamp;
        this.transactions = transactions;
        this.hash = this.calculateHash();
        this.nonce = 0;
        }
}
```

```
1  contract MetaCoin {
2    mapping (address => uint) balances;
3
4    function MetaCoin() {
5      balances[tx.origin] = 10000;
6    }
7
8    function sendCoin(address receiver, uint amount) returns(bool sufficient) {
9      if (balances[msg.sender] < amount) return false;
10     balances[msg.sender] -= amount;
11     balances[receiver] += amount;
12     return true;
13   }
14
15   function getBalance(address addr) returns(uint) {
16     return balances[addr];
17   }
18 }
19
```

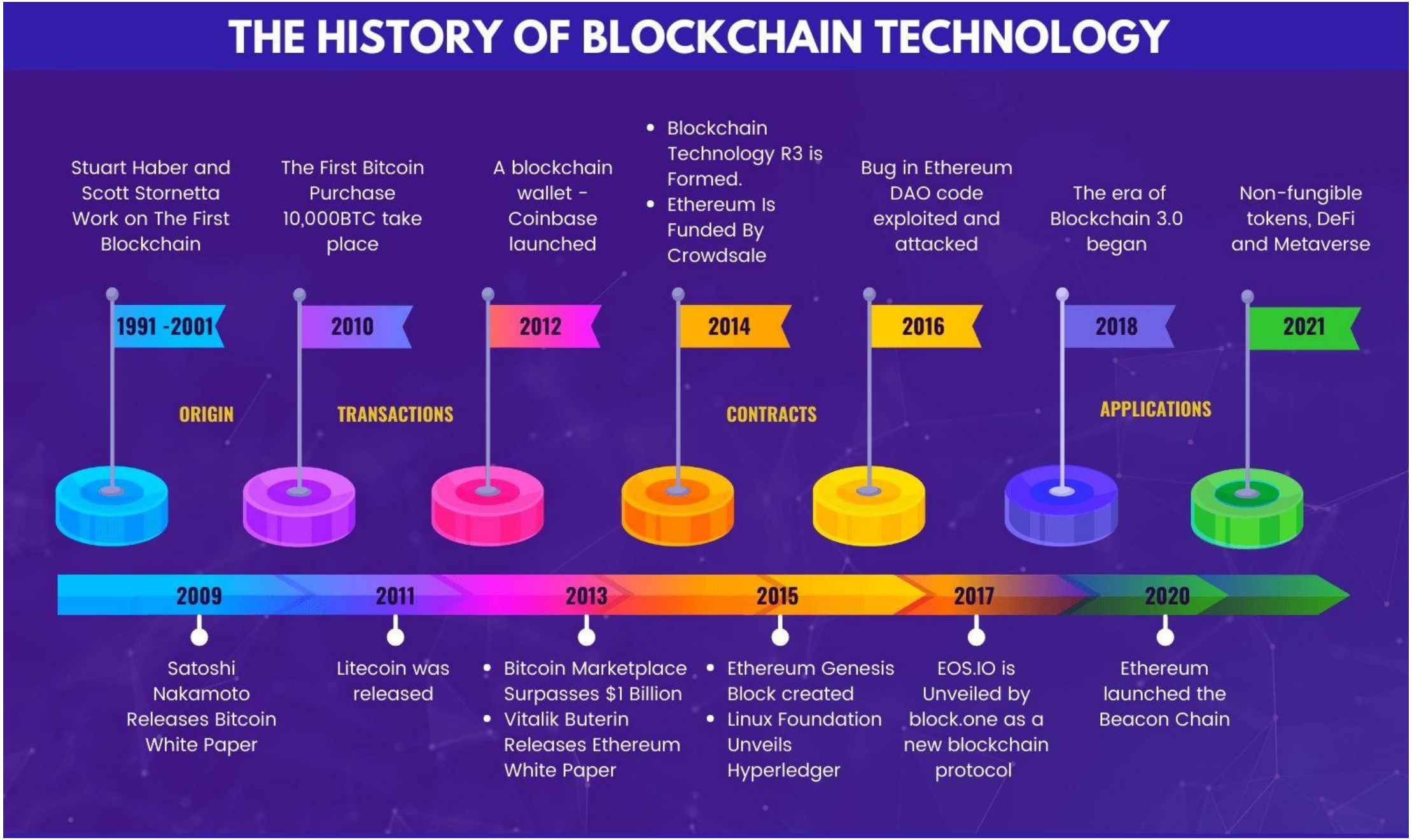
Example of a Smart Contract written in Solidity

Smart contracts are perhaps the most powerful aspect of blockchain-enabling technologies.

**They add dynamic behavior to transactions**

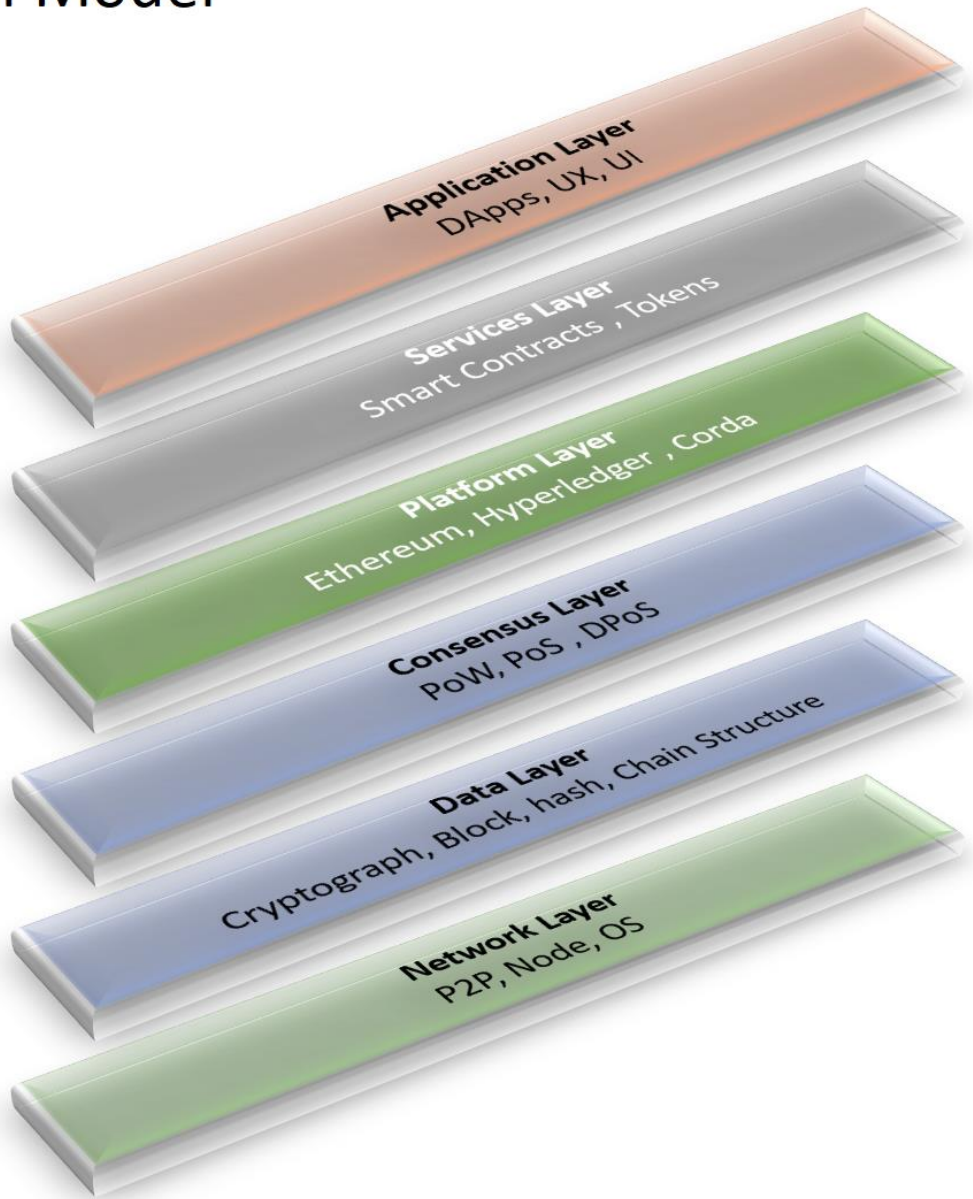
# Blockchain Programming Language

- C++ (Bitcoin)
- Python
- JavaScript
- Solidity (Smart Contract)
- Java
- Go

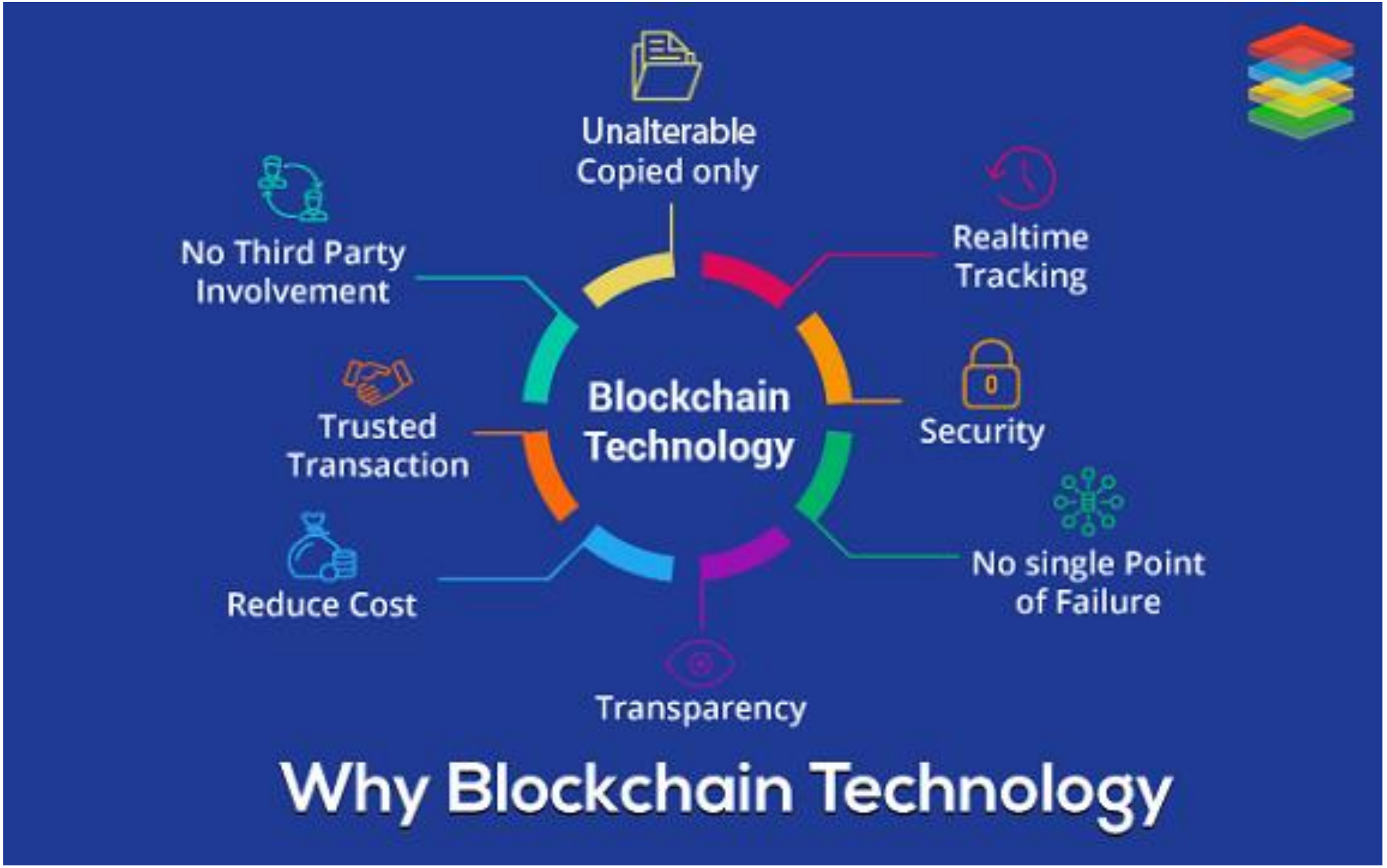



101Blockchain

# Blockchain Model

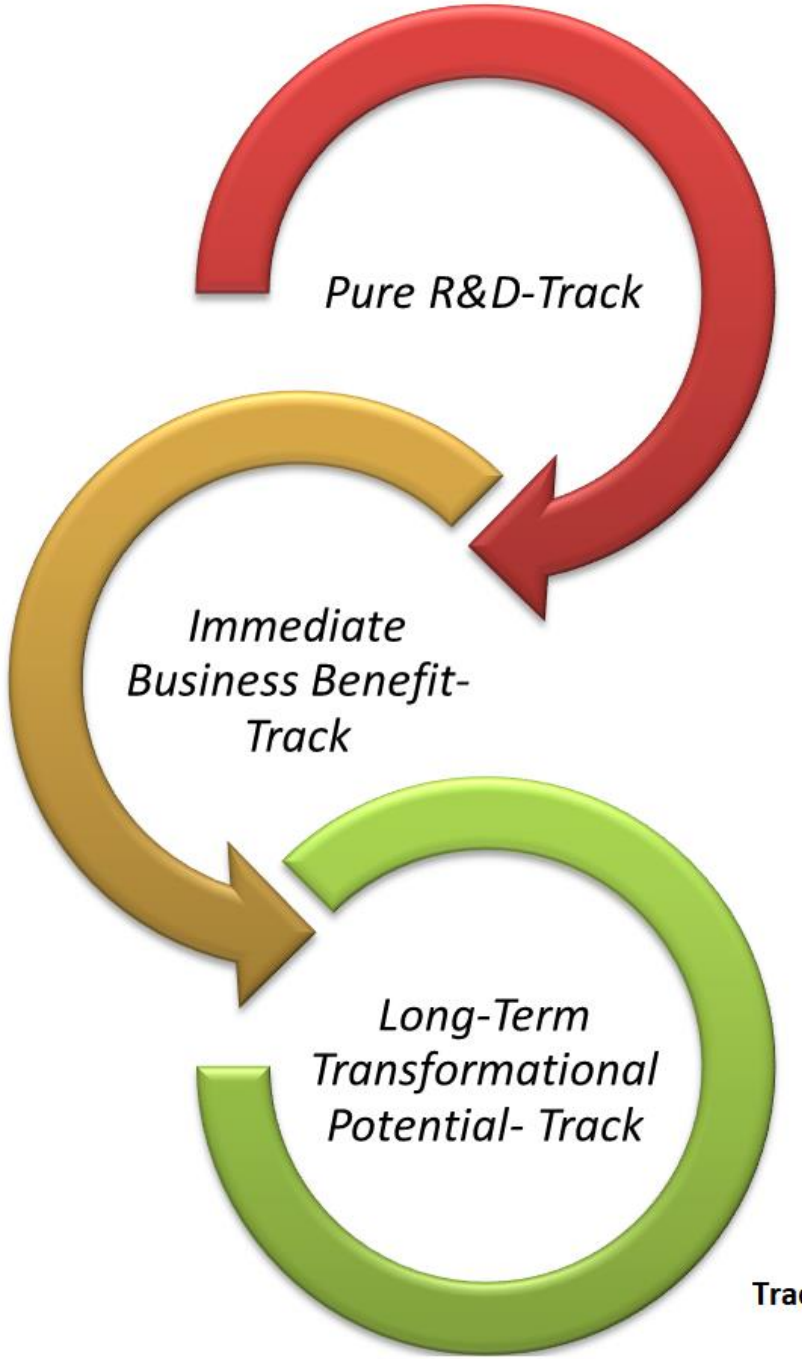



Source: Prof. Ahmed Banafa's Book "Blockchain Technology and Applications" 2020


Unalterable
Copied only
Realtime
Tracking
Security
No single Point
of Failure
Transparency
Reduce Cost
Trusted
Transaction
No Third Party
Involvement
Blockchain
Technology
Why Blockchain Technology

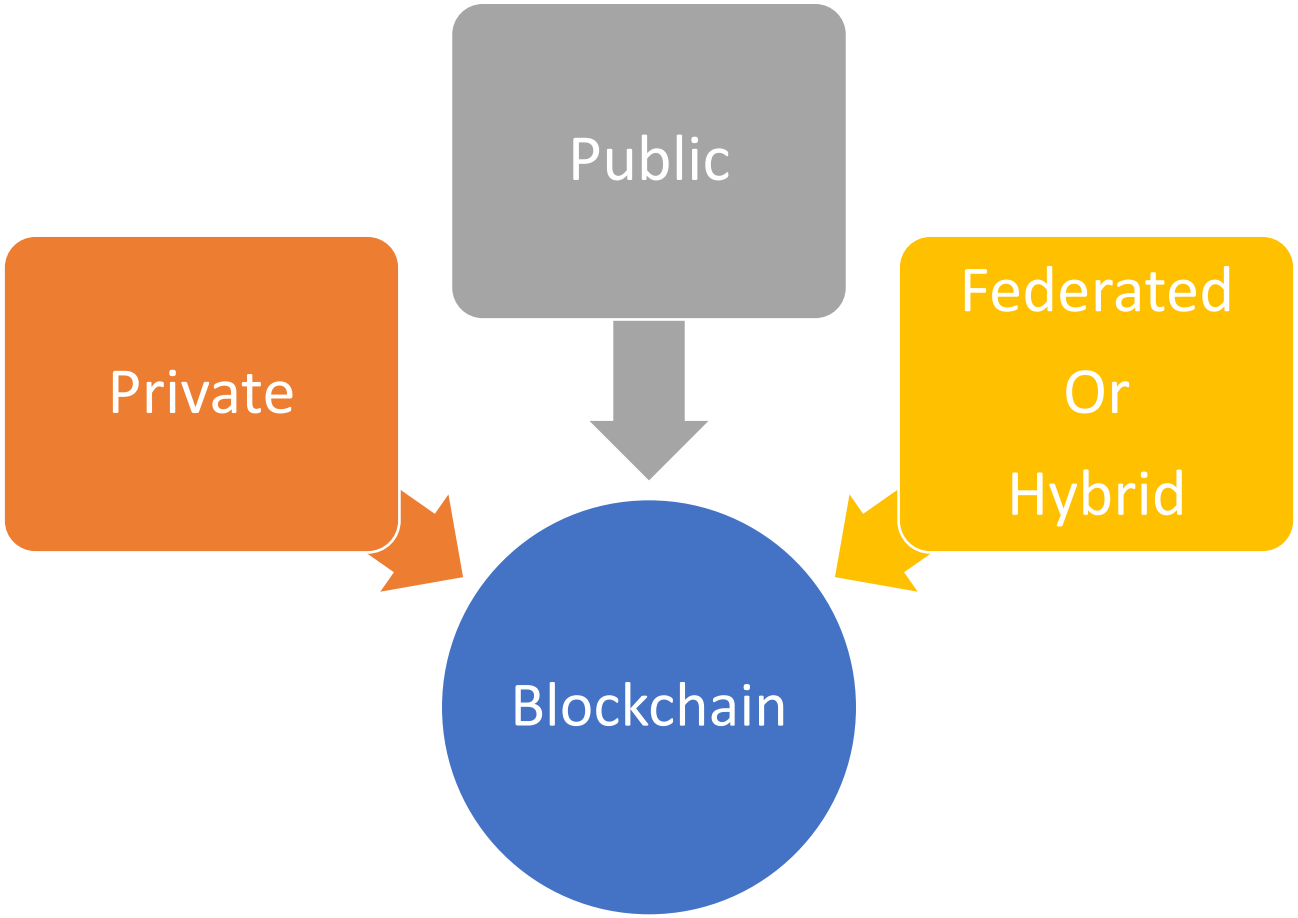
# Blockchain Tracks

To understand the direction of Blockchain technology in 2019 and beyond, we need to recognize the three tracks of blockchain technology:

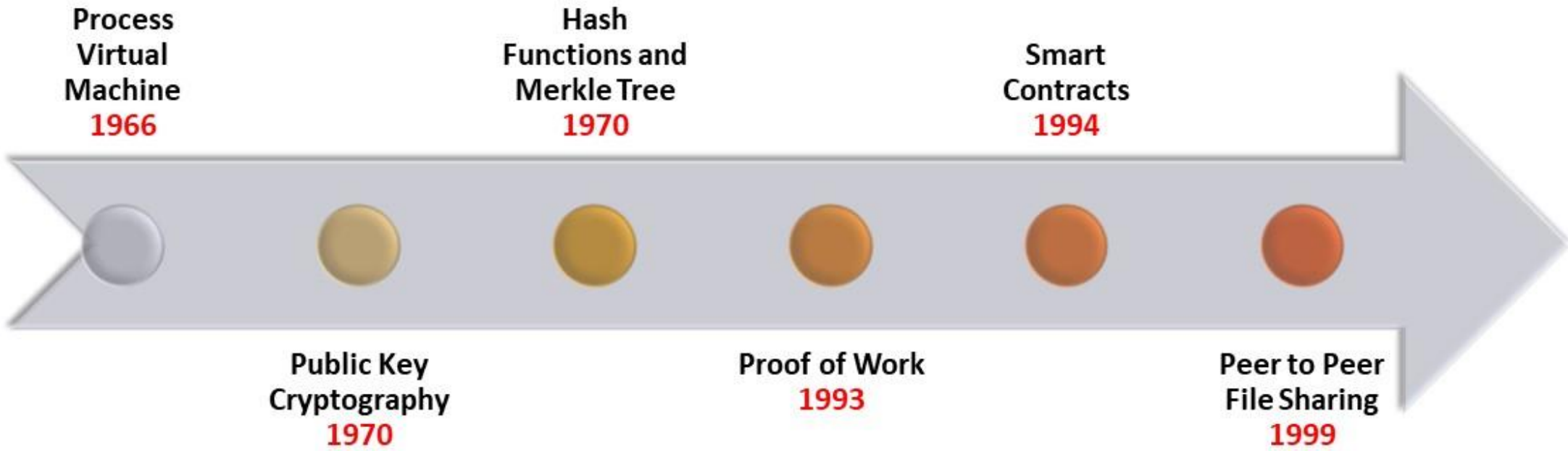



**Tracks of Blockchian Technology**

# Types of Blockchain



Its not a new technology!




**Blockchain built on the above Technologies**

# Blockchain vs. Database

| Blockchain vs. Traditional Database | | |
|---|---|---|
| **Characteristics** | **Blockchain** | **Database** |
| **Authority** | Decentralized | Centralized and controlled by the admin |
| **Architecture** | Distributed | Client-server |
| **Data Handling** | Read and Write | CRUD (Create, Read, Update, Delete) |
| **Integrity** | High | Can be altered by hackers |
| **Transparency** | High | Controlled by the admin |
| **Cost** | High | Low |
| **Performance** | Slow | Very fast |

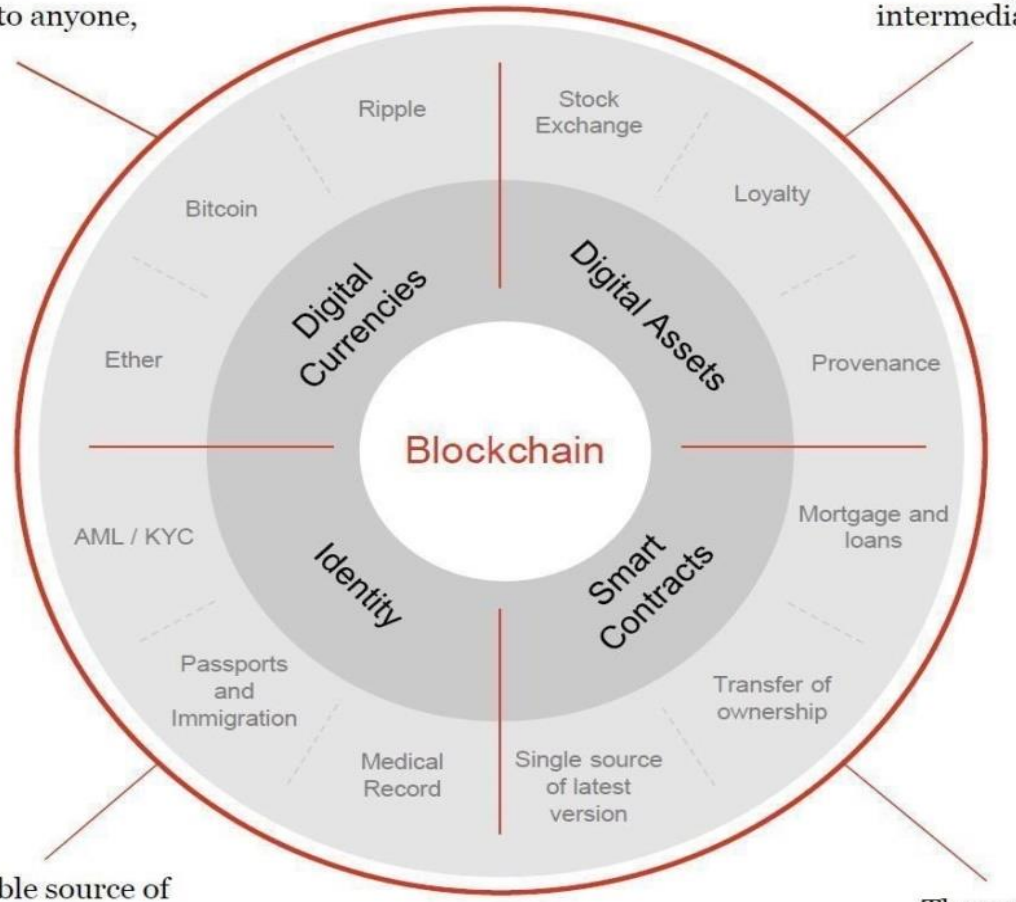
**Table 1.1:** Blockchain vs. Traditional Database

Source: Prof. Ahmed Banafa's Book "Blockchain Technology and Applications", 2020

# 4 Areas for Blockchain Applications

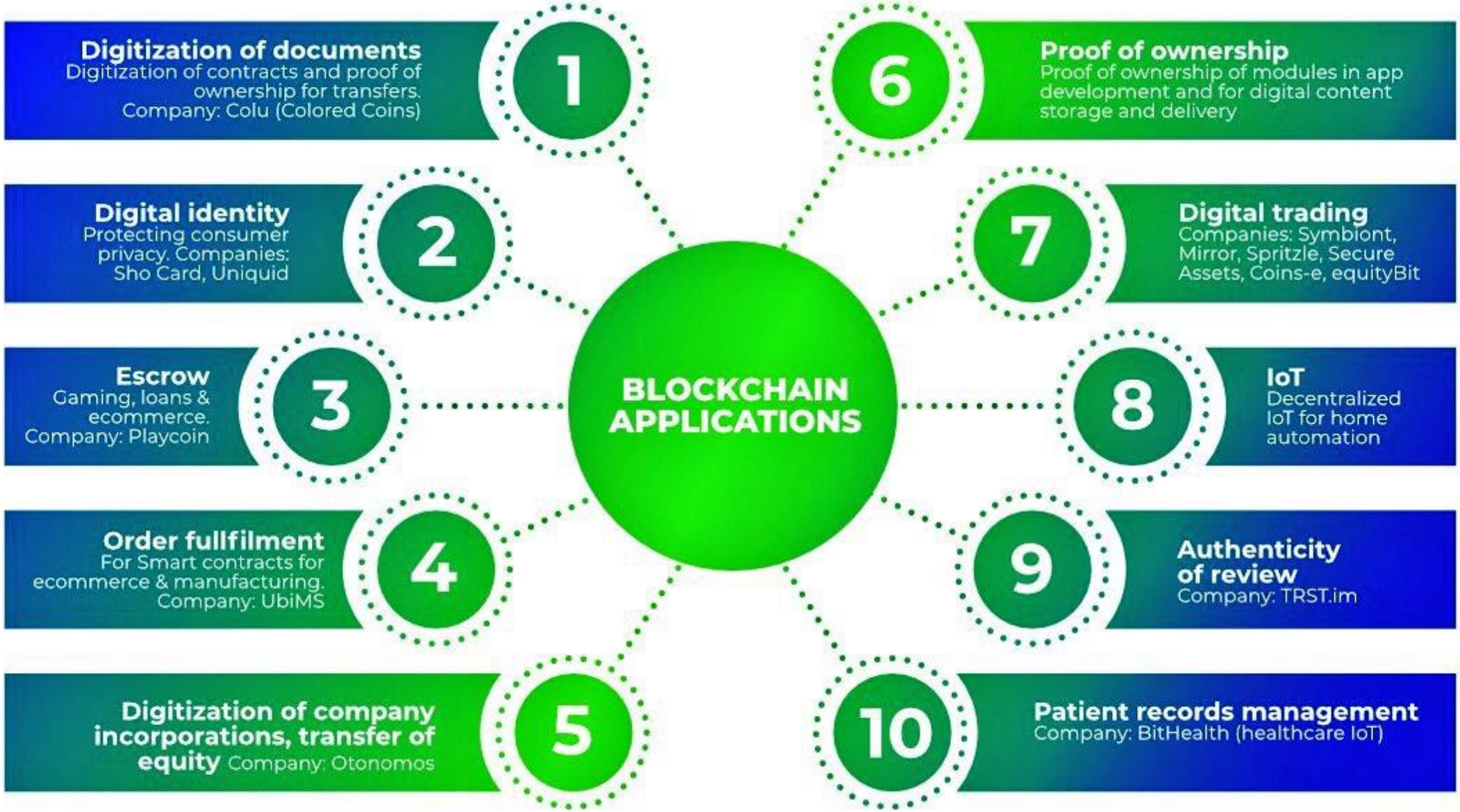
Digital currencies can be transferred almost instantaneously to anyone, anywhere

Faster and cheaper settlement of trade by removing slow intermediaries




An always available source of true identity will remove increasing problems such as forged documents

The potential to digitize and automate existing paper contracts


BLOCKCHAIN APPLICATIONS
1
Digitization of documents
Digitization of contracts and proof of ownership for transfers.
Company: Colu (Colored Coins)
2
Digital identity
Protecting consumer privacy. Companies: Sho Card, Uniquid
3
Escrow
Gaming, loans & ecommerce.
Company: Playcoin
4
Order fullfilment
For Smart contracts for ecommerce & manufacturing.
Company: UbiMS
5
Digitization of company incorporations, transfer of equity Company: Otonomos
6
Proof of ownership
Proof of ownership of modules in app development and for digital content storage and delivery
7
Digital trading
Companies: Symbiont, Mirror, Spritzle, Secure Assets, Coins-e, equityBit
8
IoT
Decentralized IoT for home automation
9
Authenticity of review
Company: TRST.im
10
Patient records management
Company: BitHealth (healthcare IoT)

# Quantum Computing and Blockchain: Myths and Facts

- The biggest danger to Blockchain networks from quantum computing is its ability to break traditional encryption

- Google sent shock waves around the internet when it was claimed, had built a quantum computer able to solve formerly impossible mathematical calculations–with some fearing crypto industry could be at risk .
- Google states that its experiment is the first experimental challenge against the *extended Church-Turing thesis* — also known as computability thesis — which claims that traditional computers can effectively carry out any “reasonable” model of computation

**What is Quantum Supremacy ?**

• Google claims to have successfully built the world's most powerful quantum computer. What that means, according to Google's researchers, is that calculations that normally take more than **10,000 years** to perform, its computer was able to do in about ***200 seconds,*** and potentially mean Blockchain, and the encryption that underpins it, could be broken.

- **Asymmetric cryptography** used in crypto relies on key pairs, namely a private and public key. Public keys can be calculated from their private counterpart, but *not* the other way around.
- This is due to the impossibility of certain mathematical problems. Quantum computers are more efficient in accomplishing this by magnitudes, and if the calculation is done the other way then the whole scheme breaks

- It would appear Google is still some way away from building a quantum computer that could be a threat to Blockchain cryptography or other encryption.
- "Google's supercomputer currently has **53 qubits**,"

- "In order to have any effect on bitcoin or most other financial systems it would take at least about **1500 logical qubits** and the system must allow for the entanglement of all of them,"
- Meanwhile, scaling quantum computers is "a huge challenge,"

- Blockchain networks including Bitcoin’s architecture relies on two algorithms**: Elliptic Curve Digital Signature Algorithm** (ECDSA) for digital signatures and **SHA-256** as a hash function.
- A quantum computer could use Shor’s algorithm to get your private from your public key, but the most optimistic scientific estimates say that even if this were possible, it won’t happen during this decade.

- “A 160 bit elliptic curve cryptographic key could be broken on a quantum computer using around ***1000 qubits*** while factoring the security-wise equivalent 1024 bit RSA modulus would require about ***2000*** *qubits*”.
- By comparison, Google's measly 53 qubits are still no match for this kind of cryptography. According to research paper on the matter published by Cornell University.

- But that isn’t to say that there’s no cause for alarm. While the native encryption algorithms used by Blockchain’s applications are safe for now, the fact is that the rate of advancements in quantum technology is increasing, and that could, in time, pose a threat.
- "We expect their computational power will continue to grow at a double exponential rate," Google researchers.