WAVESTONE

INSTITUT DES ACTUAIRES

Blockchain Technology

The future of trust ?

June 6th, 2018

Laurence AL NEIMI
Senior Manager
laurence.alneimi@wavestone.fr
(+33) 6 13 49 07 92

AGENDA

- Blockchain, what is it ?
- Potential use cases
- Trust & regulations
- Market view


Blockchain
The current
blockbuster

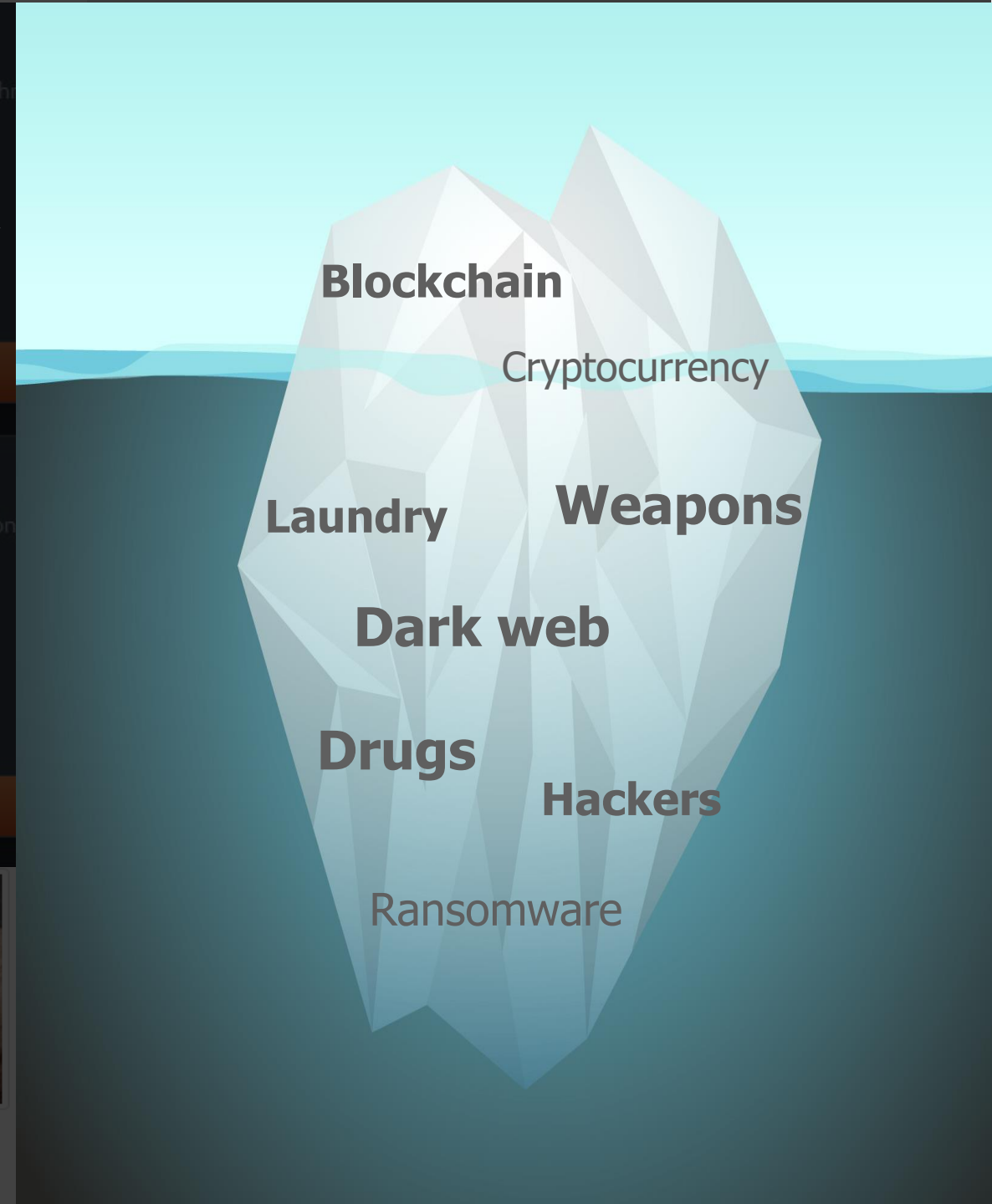
Blockchain

It did not start well…

Bitcoin : the payment medium for Ransomware & dark marketplaces

FBI : the infamous Silkroad marketplace facilitated the sale of $1 billion in drugs

Monero : 200% increase in value one week after AlphaBay support



Blockchain, *the story* of a steady climb to popularity

EMERGENCE OF THE CONCEPT

UNDERSTANDING AND ACCULTURATION

PLAN FOR THE FUTURE

Today

2008
Concept of Blockchain focused on cryptocurrencies

2009
Launch of Bitcoin, the first application of the Blockchain concept
(announcement of the open source software)

2013
First acceptations by establishments of payments with Bitcoin

2014
MT.Gox scandal
(2,4M€ missing)

2015
Evolution of the Blockchain concept with Ethereum and the introduction of *smart contracts*

End 2015
Blockchain hits the headlines of The Economist : « The Trust Machine »

2016
European Commission announce that it plans to include cryptocurrency exchanges in the scope of the anti-laundry directive

July 2017
The AMF (Autorité des Marchés Financiers) supports Blockchain

August 2017
The total market of cryptocurrencies reaches 100 billion dollar

April 2018
French Conseil d'Etat : modification of cryptocurrencies' taxation rate, which becomes more attractive.

In France : 200 000 people invested in Bitcoin ; 3,7 million invested in stocks.

Wait but, **What is** a Blockchain ?

Blockchain is a technology that allows participants to **reliably exchange information without the need of a third party**

A **replicated** ledger

Stored by the agents of the network

Every member of the network stores a **copy of the register**

An **immutable** ledger

Guaranteed by algorithms

Every minor change has to be agreed upon **by the majority**

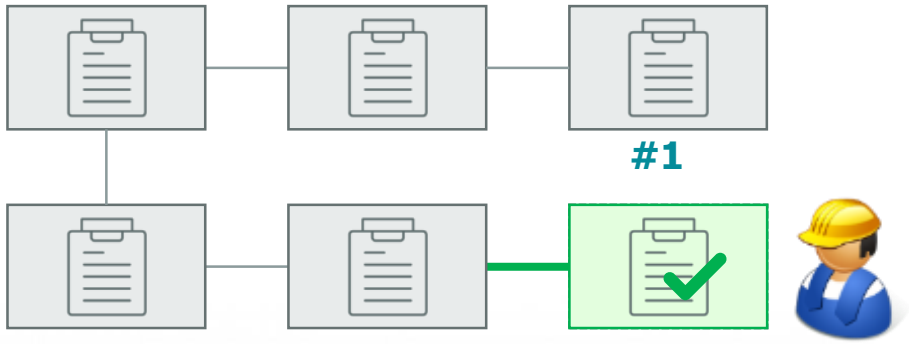
A **self regulated** ledger

Guaranteed by algorithms

No need of **a third party trust**


Brilliant !
But really, how does it work ?

No third party trust required



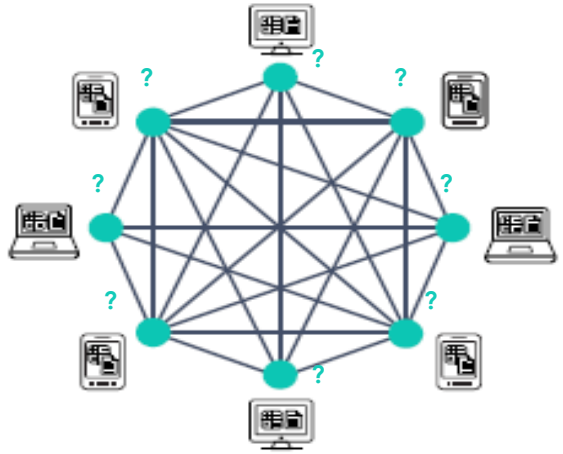
Two possible types of BLOCKCHAIN

Public blockchain

AVAILABLE TO EVERYONE

NO ACCESS CONTROL

DATA AVAILABLE TO ALL

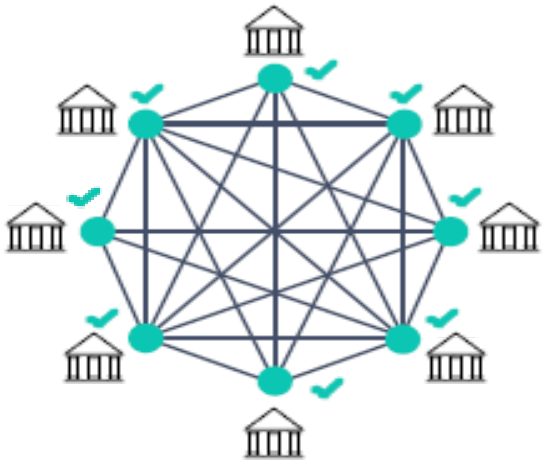


Private blockchain

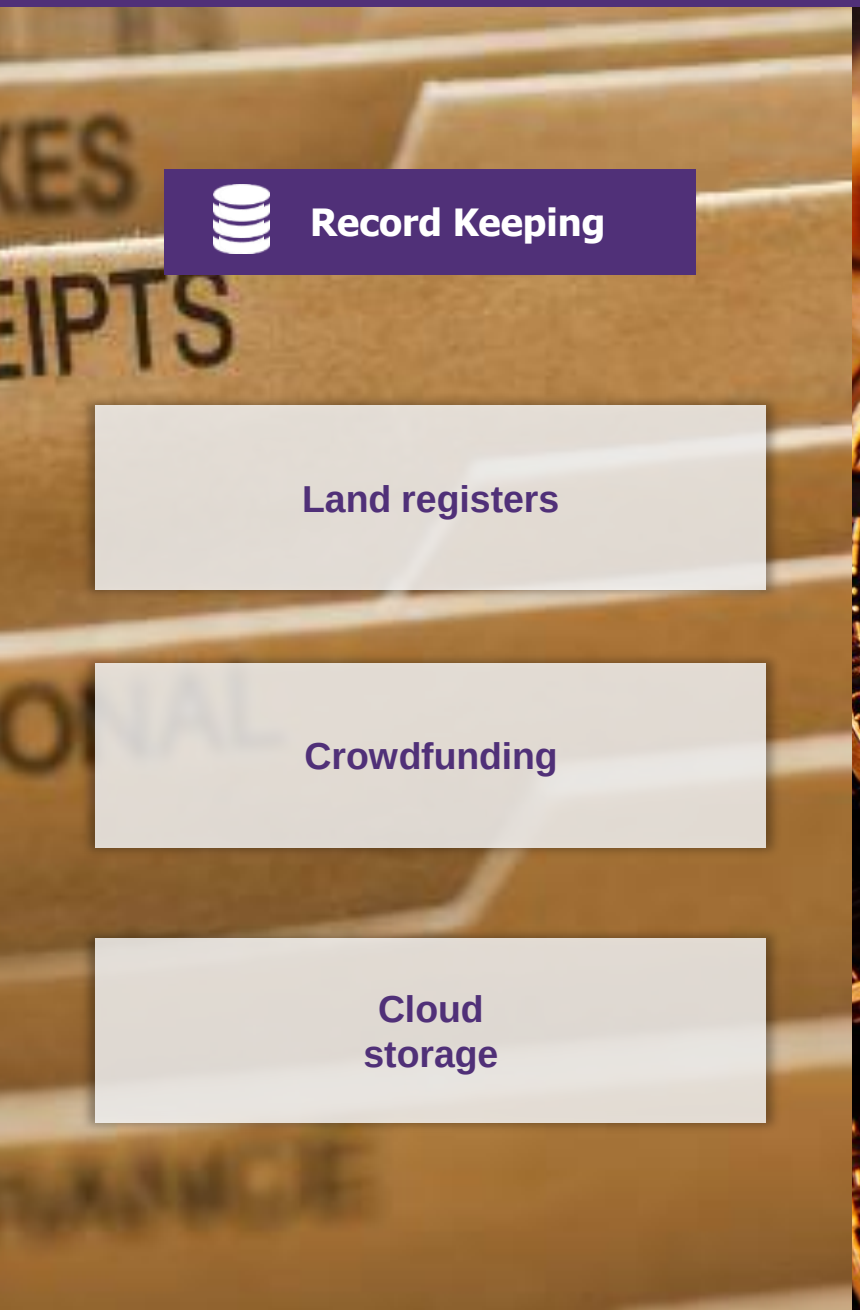
ACCESS CONTROL

USED BY COMPANIES OR CONSORTIUMS (HYBRID BLOCKCHAINS)

RE-INTRODUCING A THIRD PARTY TRUST



Some Blockchain use cases

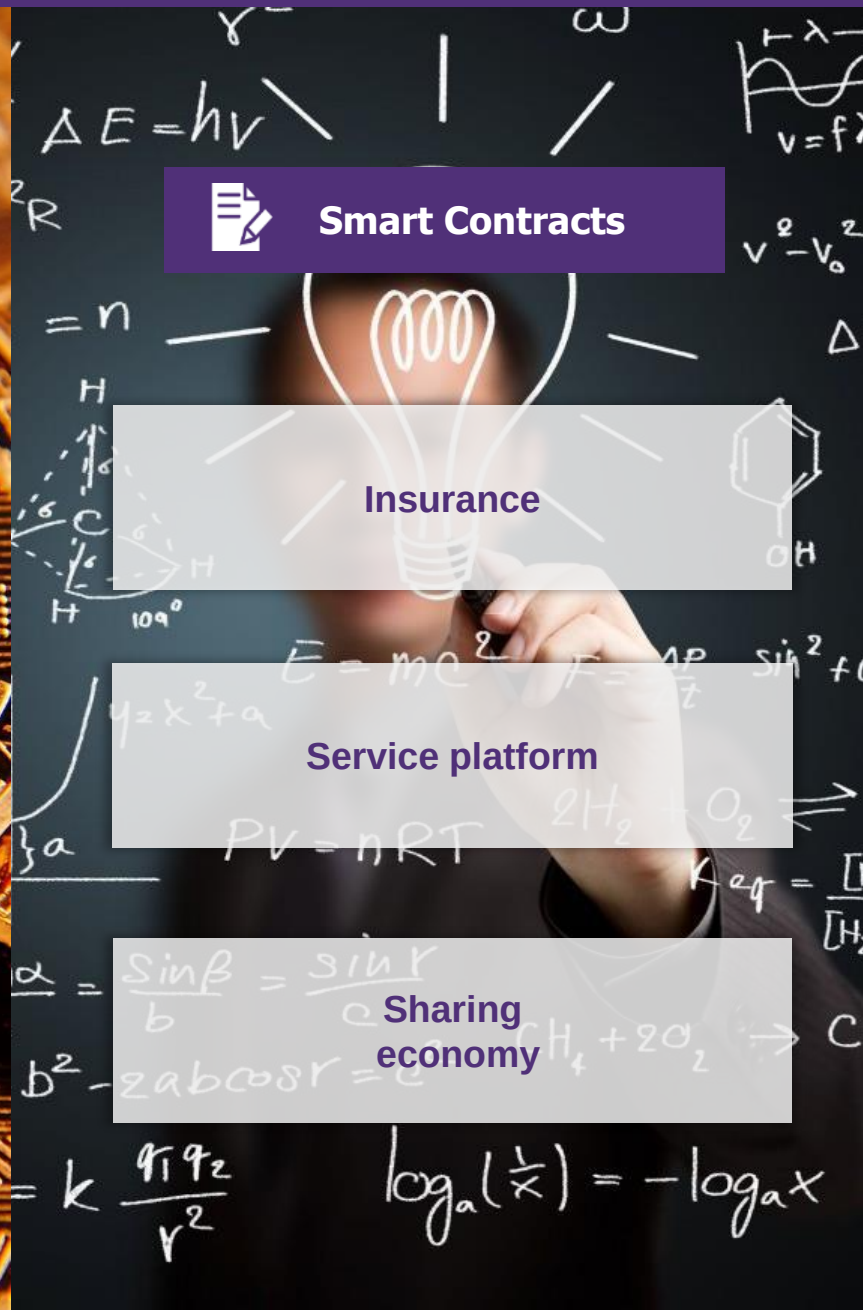


Record Keeping

- Land registers
- Crowdfunding
- Cloud storage

Digital Transactions

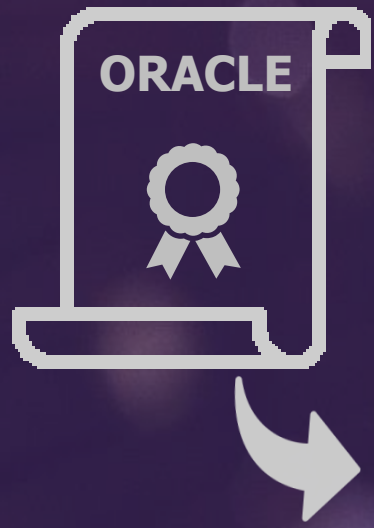
- Crypto currencies
- Digital portfolio
- Initial Coin Offering



Smart Contracts

- Insurance
- Service platform
- Sharing economy

Yes but... **What is** a Smart Contract ?



1

Blockchain members all agree on a piece of code

2

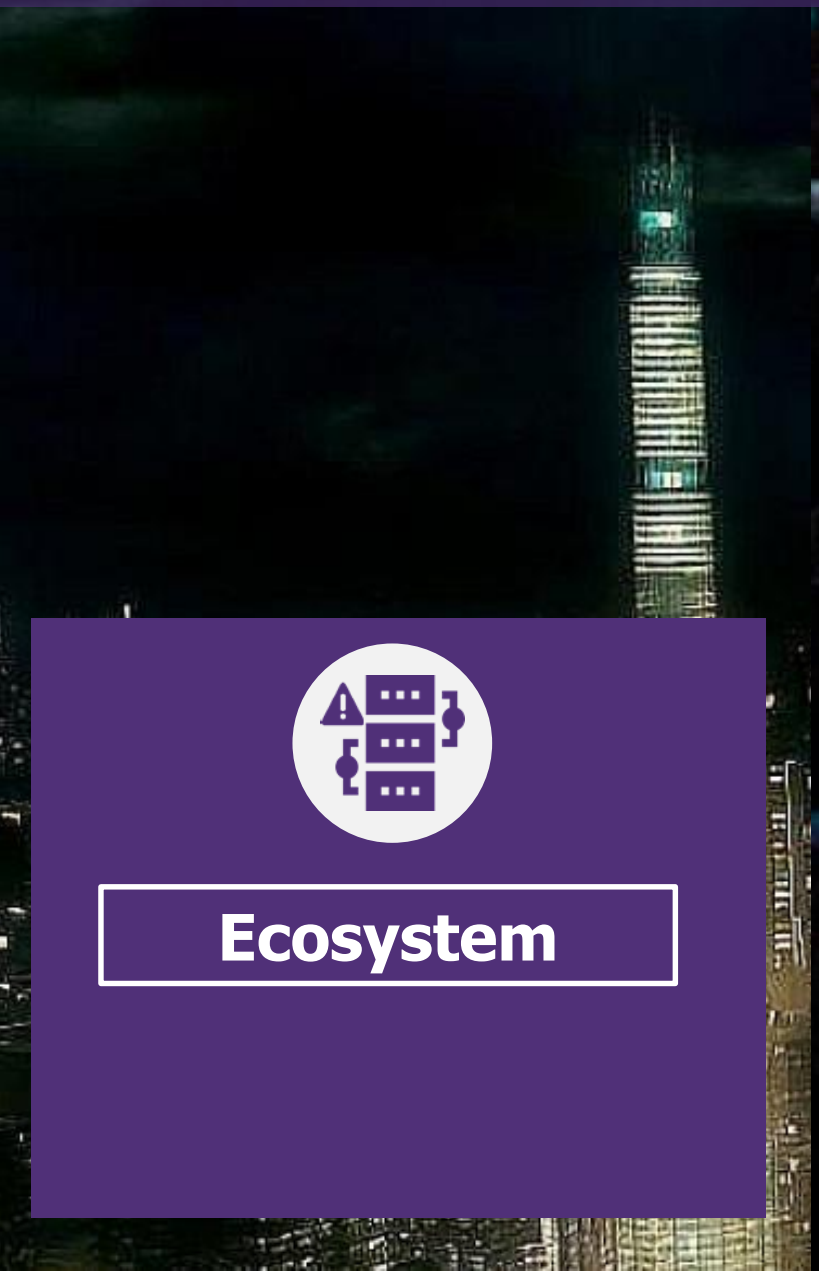
This code is added into the Blockchain by a miner. It becomes inalterable.

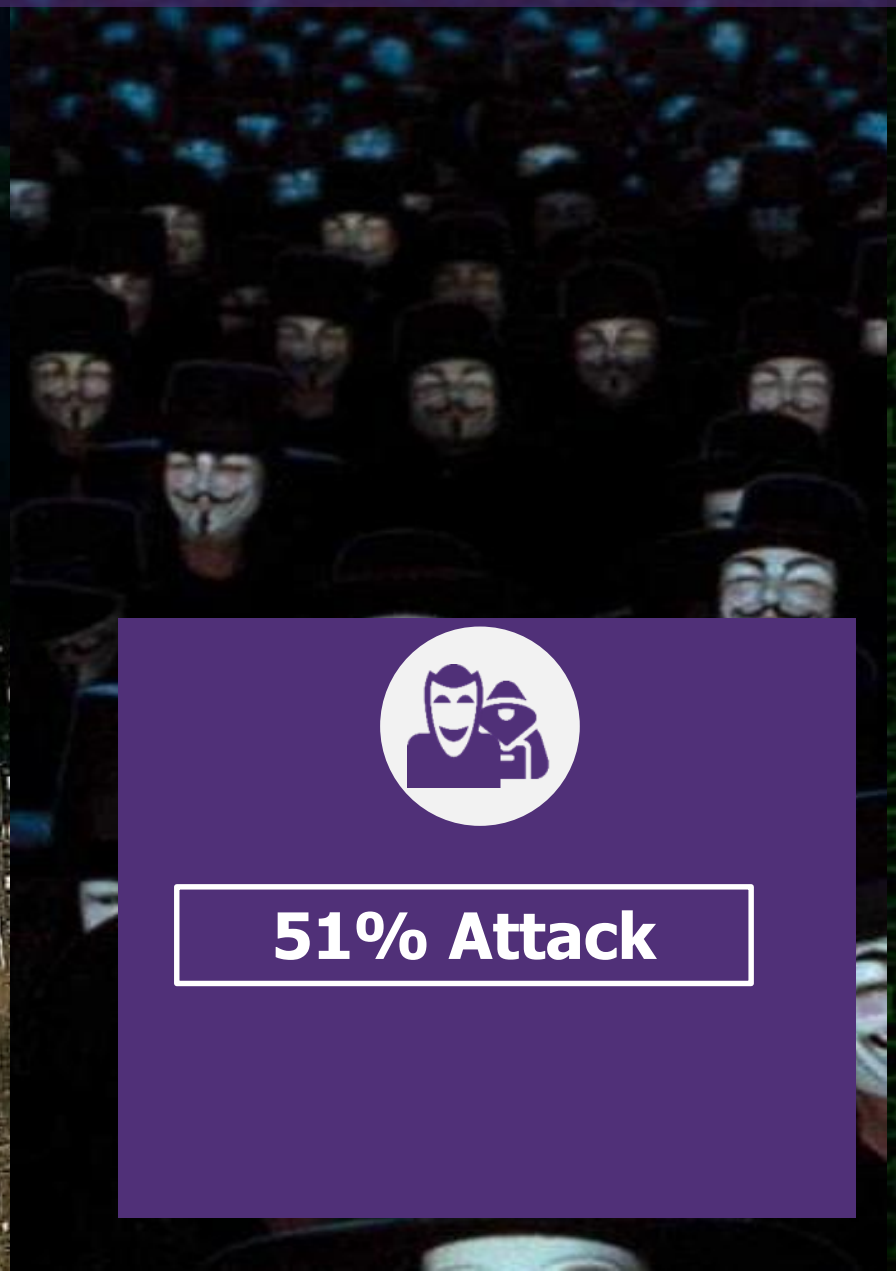
3

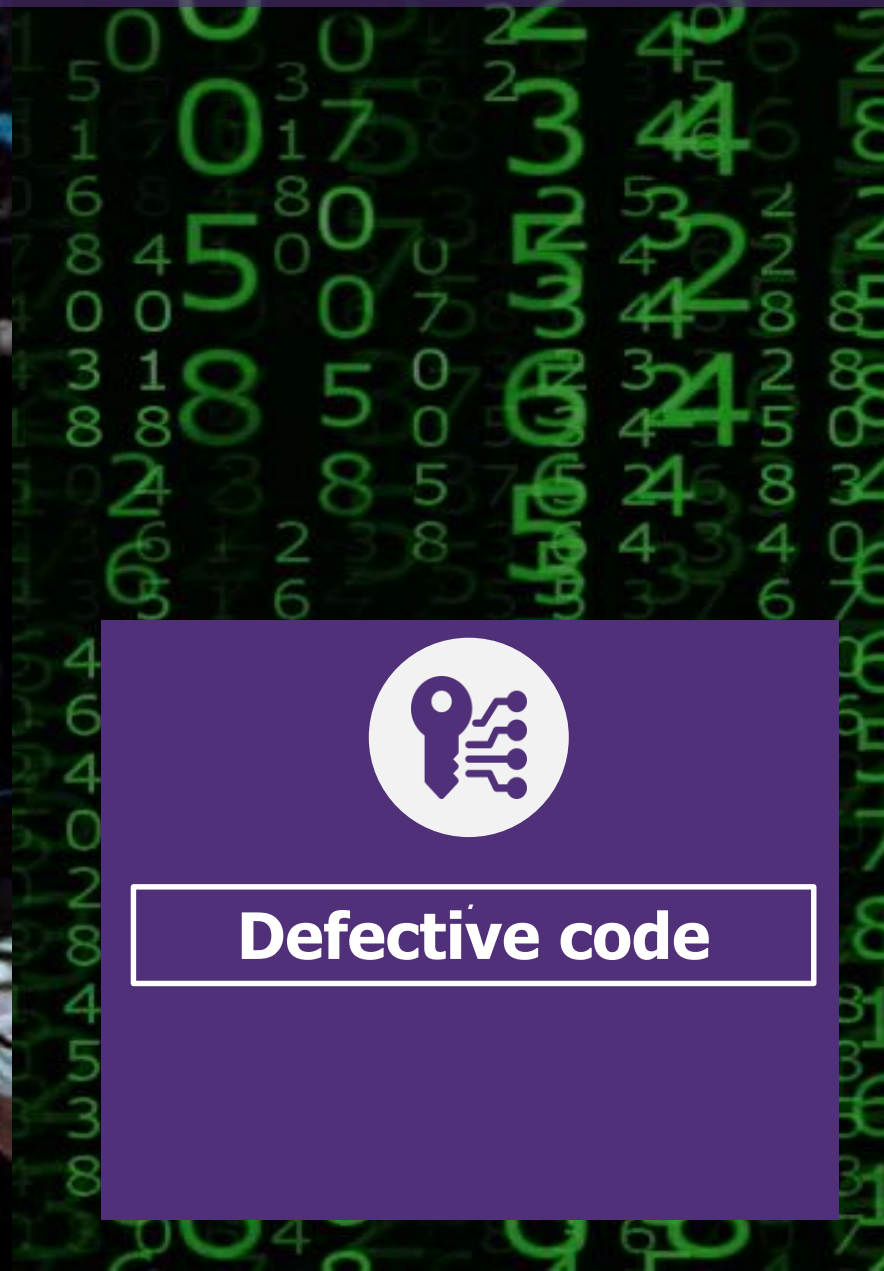
The smart contract is run as expected. External events can cause the code execution (Oracle).


Blockchain:
Can we trust
this technology ?

Major risks associated with a Blockchain







Ecosystem

51% Attack

Defective code

A opportunity for trust, but…

Implement simple rules

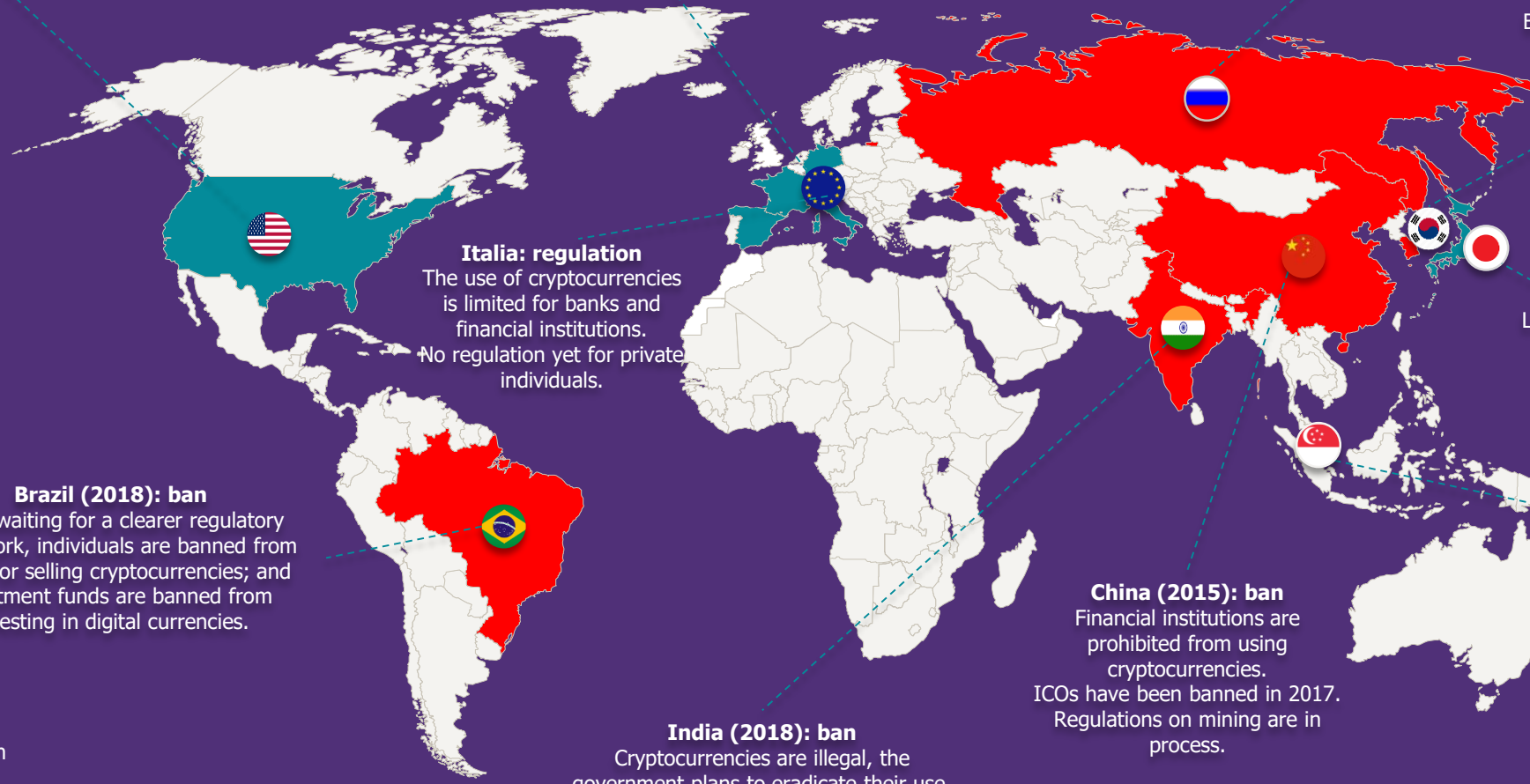
Whether you create your Blockchain or join an existing one

- ❑ Ensure a **secure management of private keys and BC ecosystem**
  Hardening, PKI, cold storage…
- ❑ Trust the governance & the **mining process**
  Developers (hard fork), access, CPU…
- ❑ Don't sign a **contract blindly**
  Code review, devs training, bounties…

➔ **Each blockchain use case is different : systematic risk analysis**


What
about
regulation ?

At global scale, regulation is focused on cryptocurrencies



United States (2018): tight regulation
of trading platforms.
Regulatory tightening is expected for cryptocurrencies and ICOs

France and Germany (2017): market opening and regulation
Advocating international regulation. Consultations are in progress.
Further regulation is expected, in France, to limit the risks of fraud.

Spain (2018): favorable
Favorable regulation is expected, there is a wish to attract companies with fiscal incentives.

Russia (2014): very tight control
Cryptocurrencies are banned.
The position is shifting toward regulation to better control risks.
Plans to create a national cryptocurrency: the CryptoRuble.

South Korea (2017): ban
Ban on ICOs, and on banks using cryptocurrencies.

Italia: regulation
The use of cryptocurrencies is limited for banks and financial institutions.
No regulation yet for private individuals.

Japan (2017): controlled opening
Legalization of Bitcoin as currency.
Clear framework to regulate cryptocurrencies.

Brazil (2018): ban
While waiting for a clearer regulatory framework, individuals are banned from buying or selling cryptocurrencies; and investment funds are banned from investing in digital currencies.

China (2015): ban
Financial institutions are prohibited from using cryptocurrencies.
ICOs have been banned in 2017.
Regulations on mining are in process.

Singapore (2018): highly favorable
No regulation on cryptocurrencies, only on activities associated with them.

India (2018): ban
Cryptocurrencies are illegal, the government plans to eradicate their use.

Favorable regulation

Unfavorable regulation

France : towards an attractive regulatory framework

2016 | **2017** | **2018**

28 April 2016
France confers a **legal basis to Blockchain**
An order rules the use of a "shared electronic saving device" (a Blockchain), for trading specifics securities.

December 2017
Official authorization of issuing and transferring securities on a Blockchain network.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Ordonnance n° 2017-1674 du 8 décembre 2017

February 2018
The Assemblée Nationale launches 2 information missions of Blockchain and cryptocurrencies.

The French Government makes a former deputy governor of the Banque de France responsible for leading a mission on cryptocurrencies.

ASSEMBLÉE NATIONALE

April 2018
The Conseil d'Etat, considers that cryptocurrencies are tangible personal property and thus non subject to the industrial and commercial profits taxation. Taxation becomes lower.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Ordonnance n° 2017-1674 du 8 décembre 2017

Other initiatives

Caisse des Dépôts

Blockchain Consortium:
Created in 2016

BANQUE DE FRANCE
EUROSYSTÈME

Lab Innovation
Created in 2017

ICO regulation is pending

France will be the **first country in the world** to regulate ICO

Objectives ?

- To set up an **attractive framework** for ICO
- To **protect** investors

How ?

The AMF will be able to deliver an **optional visa** to reliable projects.

It is a guarantee of quality of the project

When ?

This regulation is expected to come into force in early 2019

ZOOM: Is Blockchain compatible with GDPR ?

Blockchain

The immutability of Blockchain make impossible to delete any data written on it.

VS

GDPR

The article 17 guarantees the control of the erase of personal data.

At first glance, it seems impossible to write personal data in Blockchain.

Nevertheless, a solution is used by some startups

3 encryption keys are created

One key for the person whom personal data are kept

One key for the responsible of processing the data

One persistent key

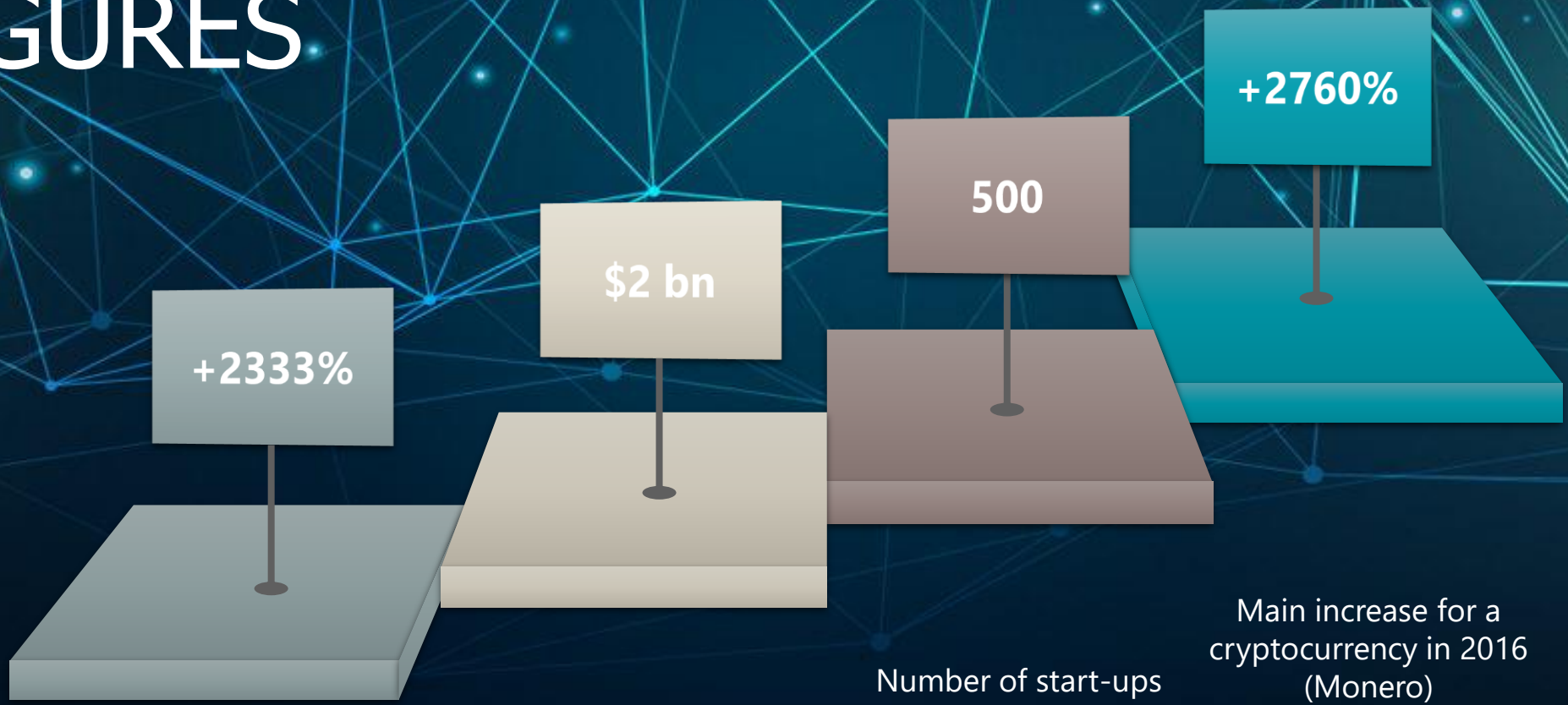
They are used to **encrypt** the personal data written in Blockchain. To access the data, the **three keys are required**.

To make **impossible to access** personal data, one key should be destroyed.

With this mechanism, personal data aren't erased, but their access becomes **impossible** and **illegible**.


What about the
Blockchain market
today ?

KEYS FIGURES



Investment growth in Blockchain between 2012 and 2017

Cumulative Blockchain investments in 2017

Number of start-ups worldwide developing Blockchain-based solutions in 2017

Main increase for a cryptocurrency in 2016 (Monero)

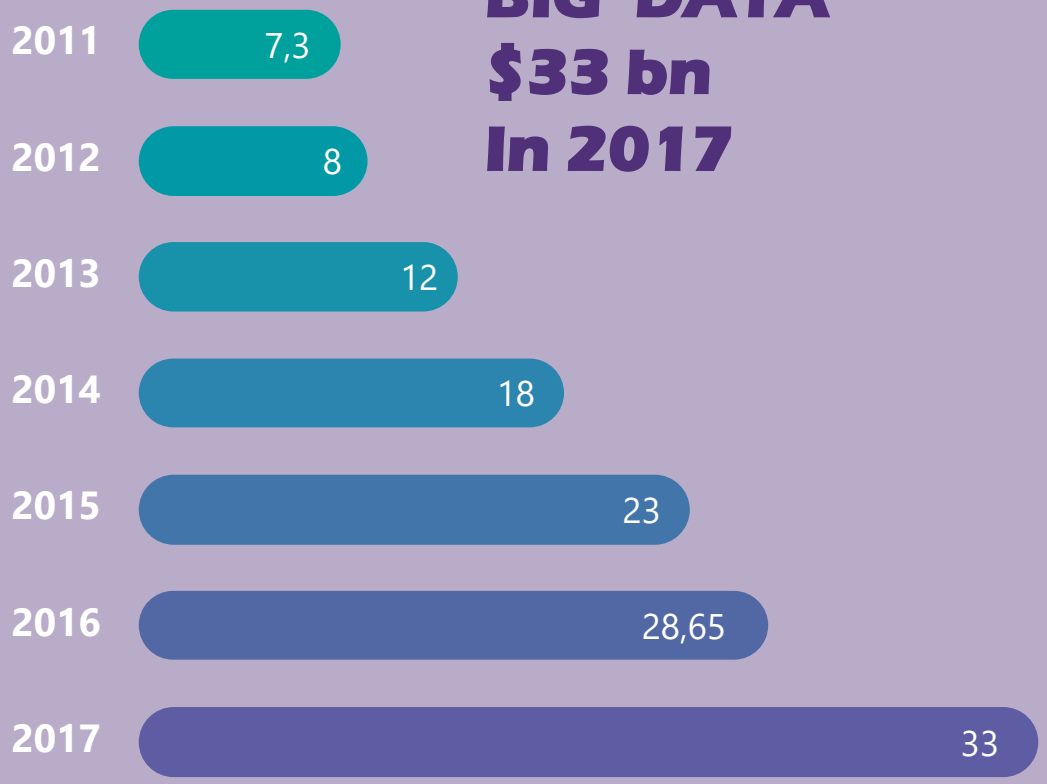
Larguillière Finance

Investments in Blockchain are seeing significant growth

but

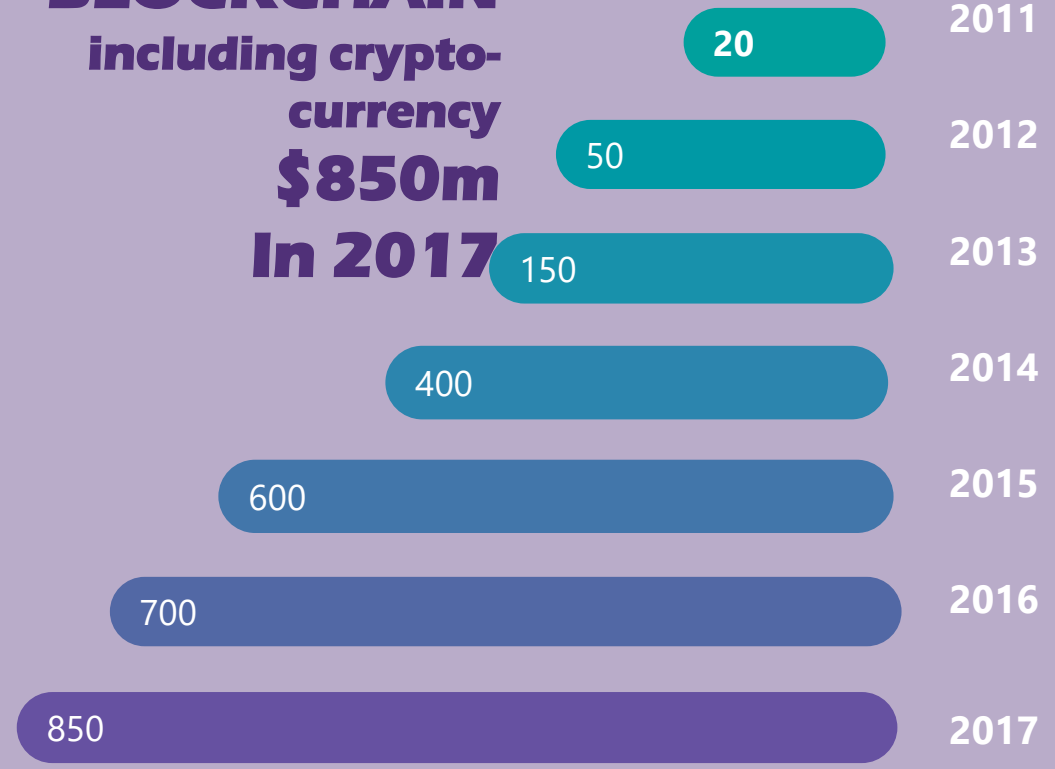
REMAIN FAR BEHIND MORE MATURE TECHNOLOGIES

BIG DATA
$33 bn
In 2017



Total level of investment in Big Data ($ bn)

BLOCKCHAIN
including crypto-currency
$850m
In 2017



Total level of investment in Blockchain except cryptocurrencies ($ m)

Larguillière Finance

but HOW ABOUT START-UPS ?

GLOBAL BLOCKCHAIN

2011	20
2012	50
2013	150
2014	400
2015	600
2016	700
2017	850

2016 Bitfinex attack:
Theft of private keys from the Bitcoin platform which enabled 120,000 Bitcoins—with a value of just over €64m—to be stolen

START-UPS

2011	20	
2012	50	
2013	104	150
2014	326	400
2015	476	600
2016	455	700
2017	600	850

- 4%

Total level of investment in Big Data ($ bn)

Larguillière Finance

Total level of investment in Blockchain except cryptocurrencies ($ m)

Total level of investment by startups in Blockchain ($ m)

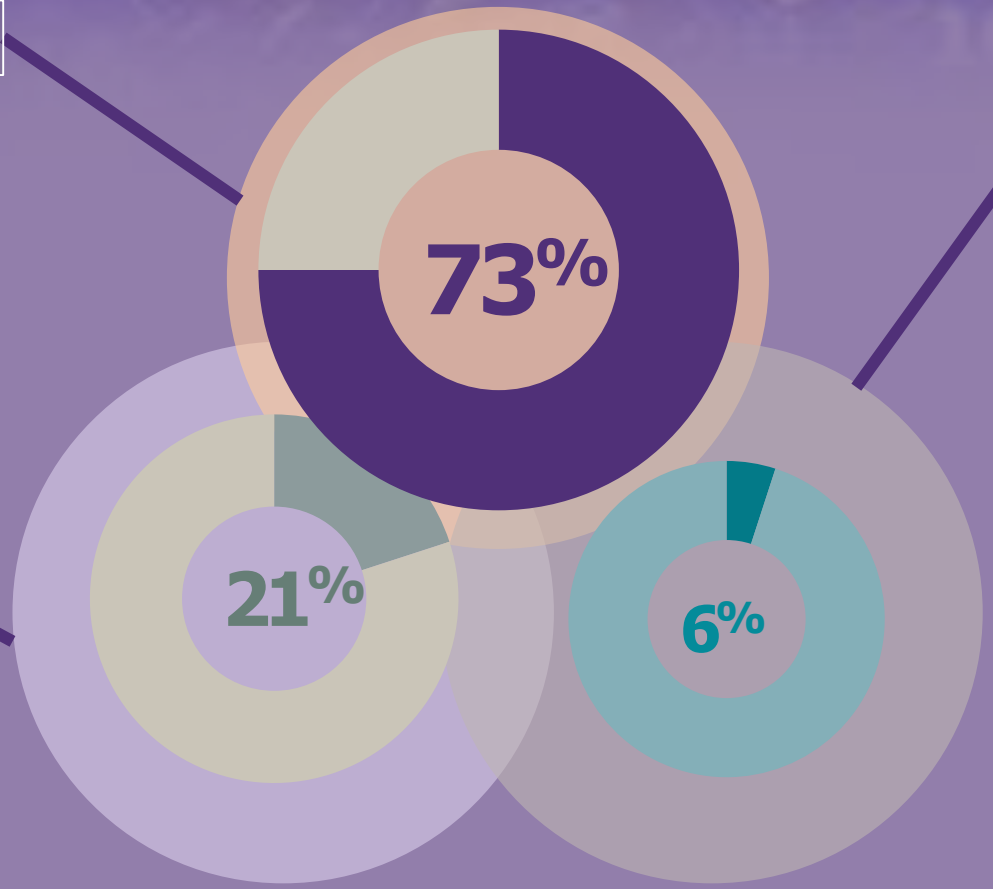
A market mainly in observation, *(except crypto-currencies)* waiting for results and a regulatory framework

Observation and acculturation

Raising awareness, decoding the trend
Technological and regulatory monitoring

Ideation

Search for use cases, opportunity study, R&D financing study
Mixed innovation approach: business and technical



Experimentation

Choice of technical solution, Proof of Concept, Proof of Value

Risk analysis and security audit

Creation of a Research Tax Credit file

Wavestone's double filter ® help assess the relevance of Blockchain Business Cases

1/Are Blockchain characteristics obstacles to business transformation?

Are intrinsic blockchain characteristics (retail consensus, unicity and incorruptibility) dragging blockchain implementation in some business cases?

Distribution

Information is shared with all stakeholders involving transparency

Unicity

Blockchain technology ensures unification of rules and information

Incorruptibility

Information can't be changed nor deleted

2/Is Blockchain Technology the best solution available at the time?

The enthusiasm generated by Blockchain must be tempered by 3 factors of uncertainty which can lead to a complex implementation

Level of participation

Blockchain resilience is proportional to its level of participation and activity

Distrust towards third parties

A power transfer towards an algorithmic system conceived by developers

Economic Incentive

Contrary to centralized systems an investment is also needed for participation

Let's discover

THE MOST PERTINENT BLOCKCHAIN USES

Financial Services

Crowdfunding

SMARTANGELS

Real-time payment
E-certificates
Secured distributed platform for Start-ups

KYC

Compliance platform where KYC statements are stored

Foreign Exchange

BARCLAYS

Speed up processes accross multiple banks

Insurance

Smart Contracts

fizzy

By AXA

Flight parametric insurance

Proof of Process

Fédération Française de l'Assurance

A secured database available for a consortium of 14 insurers

Energy : Green Energy !

Habitat Marseille Provence

BROOKLYN MICROGRID

A peer-to-peer green energy solution based in Brooklyn neighborhood where the energy demand is met thanks to solar panels

Mass Retail : Supply Chain !

Alibaba Group 阿里巴巴集团

End-to-end AUS Farm Production in China

BlockChain

End-to-end chicken supply chain tracability


WAVESTONE
PARIS
LONDON
NEW YORK
HONG KONG
SINGAPORE *
DUBAI *
BRUSSELS
LUXEMBOURG
GENEVA
CASABLANCA
LYON
MARSEILLE
NANTES
* Partenaires stratégiques