Workshop FPDAPP
H 14,00-14,45 -Room F2

Decentralized Applications : The CEFRIEL Experience

Turin, August 28th

Cefriel
POLITECNICO DI MILANO

Background: (if is it possible) I will try to define blockchain…

- **Blockchain is** a system (not service) able to create, keep and enable the circulation of digital value, without “middle man” and centralization.

- In Bitcoin and other networks are based on chronologically timestamped ledger of transactions, secured by a collaborative distributed “consensus” mechanism, based on combination of computer science, probability and economics concepts.

- Blockchain may also run self-executing programming logics (called **smart contracts**) for conditioning the exchange of value to triggers like events or actions.

REMARKS

- The paradigm of blockchain may be potentially applied to every human field where there is an exchange of a digital asset with value
- Blockchain is lacking formalization so
  - It is better to start from real world problems rather than trying to force the application of blockchain to use cases

Background: (if is it possible) I will try to define blockchain…

- Blockchain is a technology but also a cultural change. The “constitutive” self executing and deterministic logic imply “reflections” beyond technology
- Smart Contracts for instance poses some huge problems: how to manage exception? What about immutability?
- It can be applied to any digital exchange where there is a value and without third party
- It is hard because it is a balanced systems which involves Computer Science (Network), Game Theory and Cryptography
- The hype is a consequence of a need for a paradigm change. But will the hype conduct to standards?
- In some context, like Finance, it is a radical change

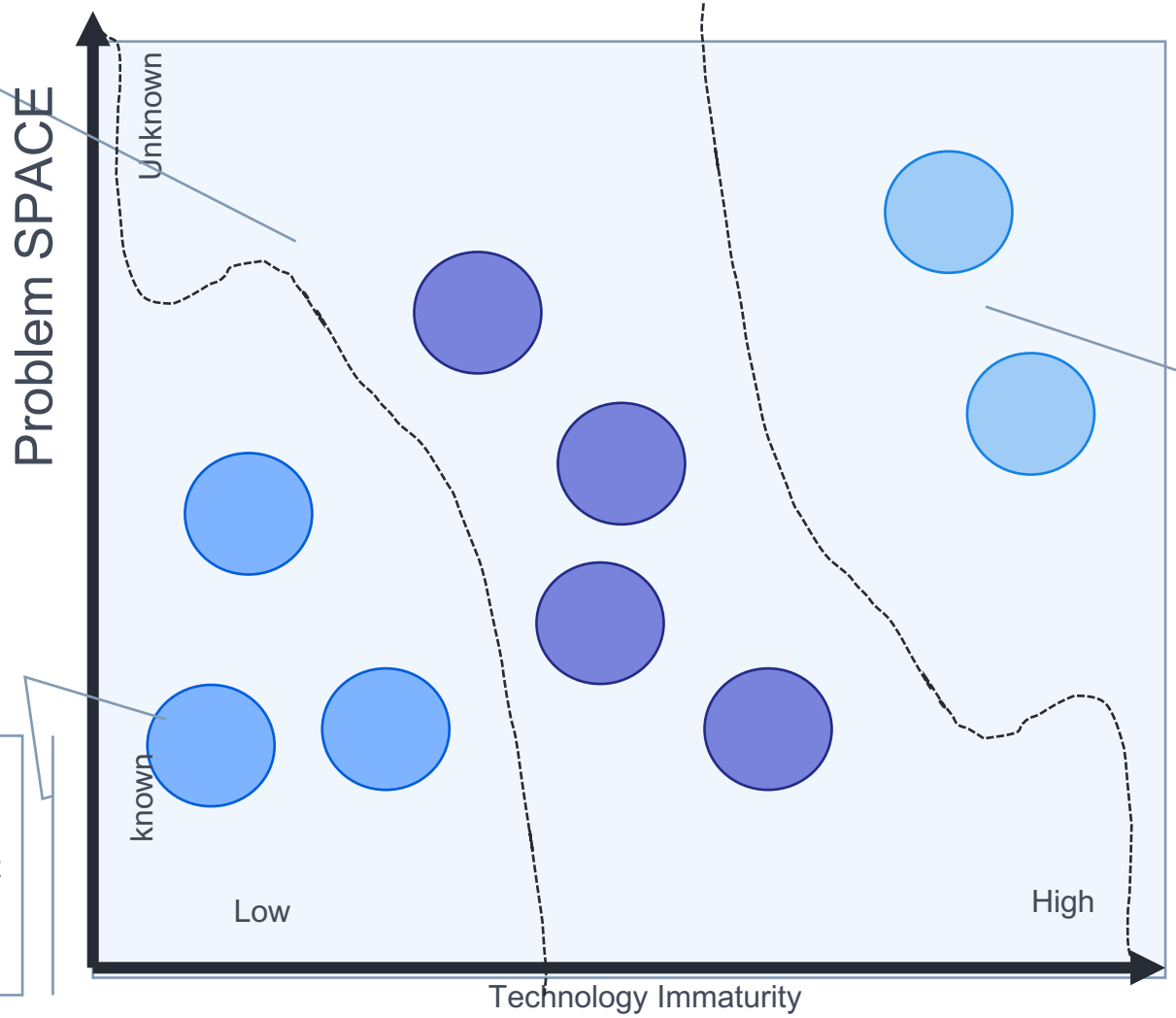
KEY FACTS ABOUT BLOCKCHAIN

It has the **potential to reshape any intermediated business or sectors**, in health in particular for simplifying the supply chain of drugs for clinical trials and intermediated processes, and replacing third parties.

1. Blockchain is **core infrastructural solution** to ensure a chronologically reliable exchange of digital assets which we want to be reliable, transparent and traceable;
2. There is **huge diversity in term of market readiness** and use cases among blockchain platforms;
3. Unfalsifiable timestamping information (**Proof of Existence**). Once a piece of information is stored, it is forever; it is a proof that the data existed at the time in the timestamp;
4. May have self-executing logic capabilities (**Smart Contracts**)
5. Decentralized nature of the infrastructures: the ecosystem made up by the actors that participate in the network have the consensus power, there is **no intermediation power**
6. For public blockchains, the model is based on **reward** (crypto) for network maintenance (mining)
7. For **private blockchains**, some of the features above are limited

What about the experience of developing decentralized applications?

Complex Project
Strategy: Learn and Adapt!
- Short Cycle Time
- Agile Tools
- Inspect, Adapt & Transparency



Chaos!
Strategy: Get out from it or …!
1. Replan with another technology?
2. Leave out
3. Lean and Lean Startup

Non complex projects
Strategy: Plan-Do-Check Act
- gressive Elab

"The Growth Mindset"

What about the experience of delevoping decentralized applications?

- High Rate of changes/ Low Degree of Maturity Uncertainty of external conditions
- Challenges (Motivation)
  - Forced to adopt agile mindset and lean start up methods
  - Necessary to increase or **discover** capabilities by **empirical** approach

- **Challenges (Technical)**
  - Volatility of cryptocurrencies poses a limit to the public adoption in industrial/ecosystems contexts
  - The overall technology readiness (i.e Smart Contracts) is not yet satisfying, due to lack of standards and lack of rules and regulations (Sustainability of Applications)

BRIEF STORY

- **TEN YEARS SINCE THE INVENTION OF BITCOIN**
- **TODAY SEVERAL BLOCKCHAINS AND APPROACHES**

- 2008 the paper of Satoshi, 2009 the first transaction
- The ever-increasing popularity of blockchain began with cryptocurrencies like bitcoin during the financial crisis of 2013
- Finance and banking sectors were the fist to experiment and invest , so these industries now represent the first wave of a mass decentralization
- Blockchain helps distribute the cost of running a platform to its various participants, but rewards them for it in equal measure.
- Beyond the Financial aspects, this decentralized model is already relevant for blockchain-based solutions such as tracking of sources, payment processing, self execution of contracts, authorization processes and many others.

Ethereum as first case of smart contracts system (2013)

- The concept originate by Nick Szabo paper in 1995 but took nearly 20 years to come to light with the introduction of Ethereum project in 2013

- They are essentially an **”if-then-else” automated SW that can be executed over a a blockchain**, that can store data in themselves and that can use external data if and only by a single source (oracle)

- Ethereum is an **open-source, public, blockchain-based** distributed computing platform featuring smart contract (scripting) functionality.[

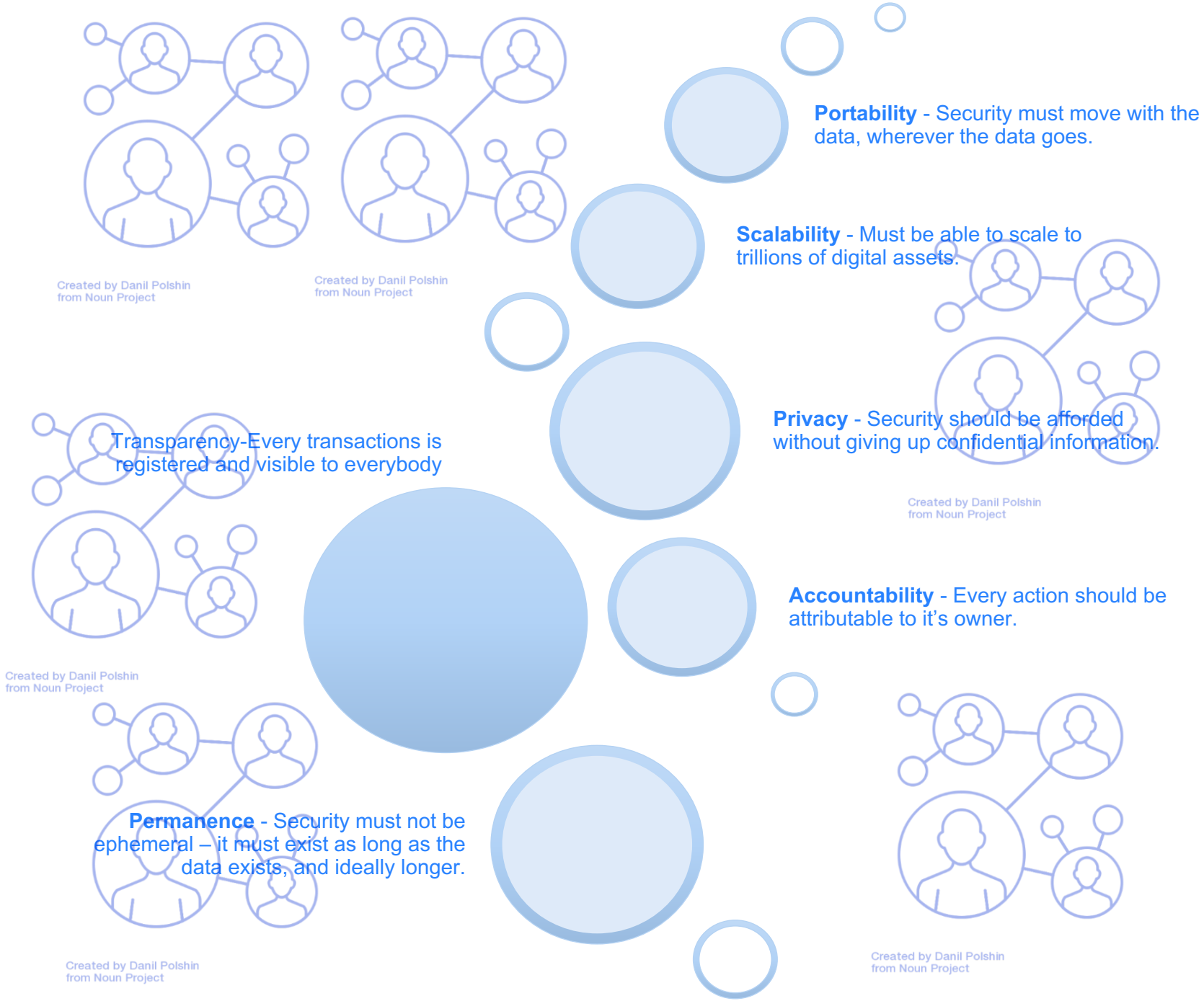
- It provides a **decentralized Turing-complete virtual machine, the Ethereum Virtual Machine (EVM)**, which can execute scripts using an international network of public nodes.

- Ethereum also provides a **cryptocurrency token called "ether",** which can be transferred between accounts and used to compensate participant nodes for computations performed.

- **"Gas",** an internal transaction pricing mechanism, is used to mitigate spam and allocate resources on the network

PUBLIC

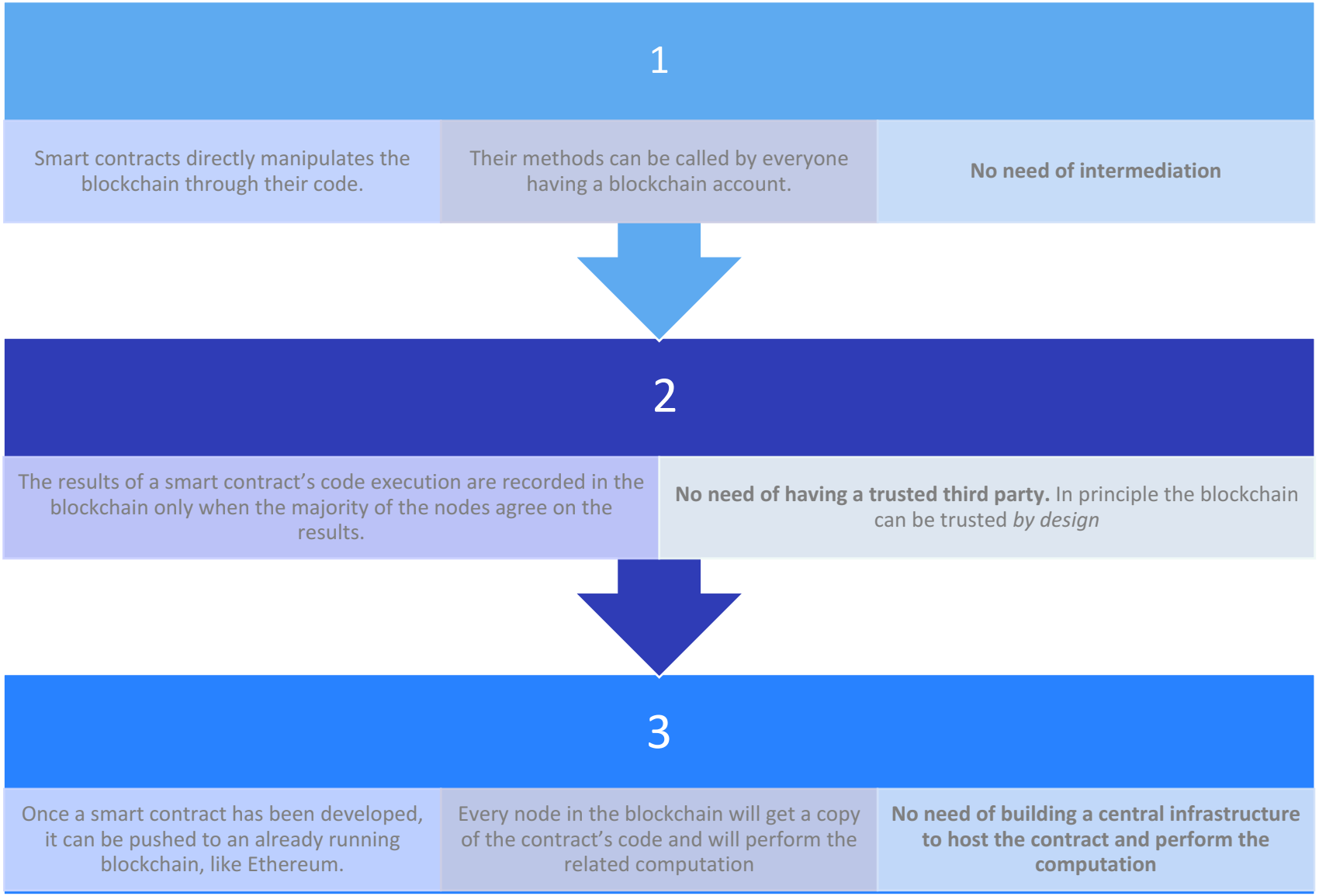
PUBLIC Blockchain is a chronologically timestamped ledger of transactions, maintained secured by a collaborative distributed “consensus” mechanism, based on combination of game theory algorithms and statistics, and able to replace the third party (the agreement, the contract, the notary) in intermediation processes.



WHAT BLOCKCHAIN CAN DO

Cut off Third Party in intermediation processes

Store timestamped signatures associated with small pieces of information like author name, place, dates



TRADITIONAL BLOCKCHAIN APPROACH

- Smart Contracts are not like Web applications!

- Blockchain are not database that can store big volumes of data!

Contacting external services (i.e.: API calls)

Idea: Have a smart contract's computation depending on values coming from external API calls.	**Problem:** Every node in the blockchain performs the same computation (in an asynchronous way) and they have to agree on the result.	**Question:** What happens if the API call returns different values to different nodes?

Enforcing on-chain payments (i.e.: Smart bonds)

Idea: Put bonds' funds on the blockchian. A smart contract will manage them, guaranteeing the buyer will get her money back at due time.	**Problem:** Funds managed by the smart contract in the blockchain can be used only by it.	**Question:** What good is bond's funds if you cannot invest it?

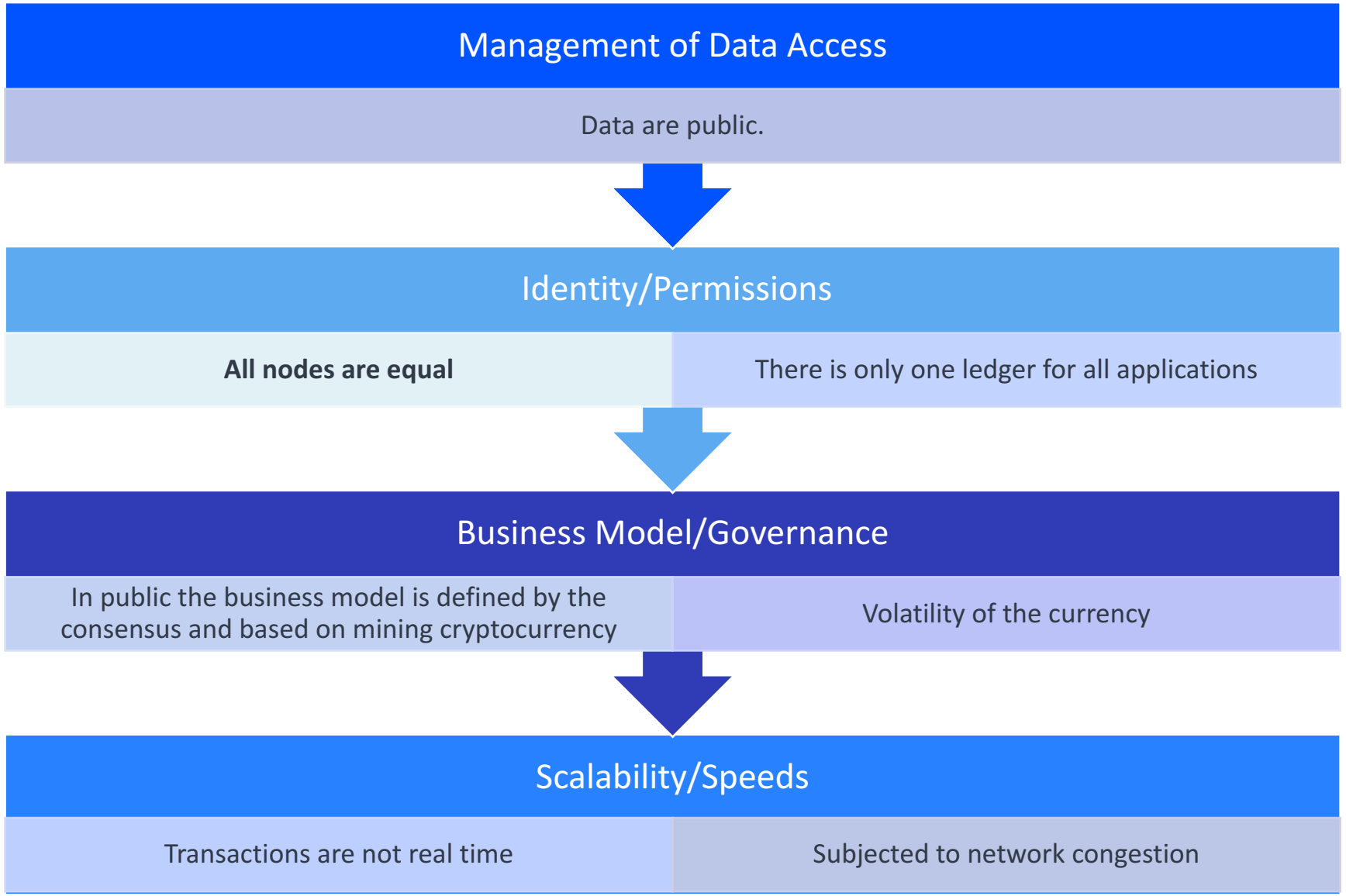
Hiding confidential data (work in progress)

Idea: Every smart contract has its own DB, over which it has full control. No other contract can access it. So let's use it to store confidential information.	**Problem:** The DB is replicated on *every single* node participating in the blockchain.	**Question:** What good is a confidential DB if it is stored on hardware we do not own and control?

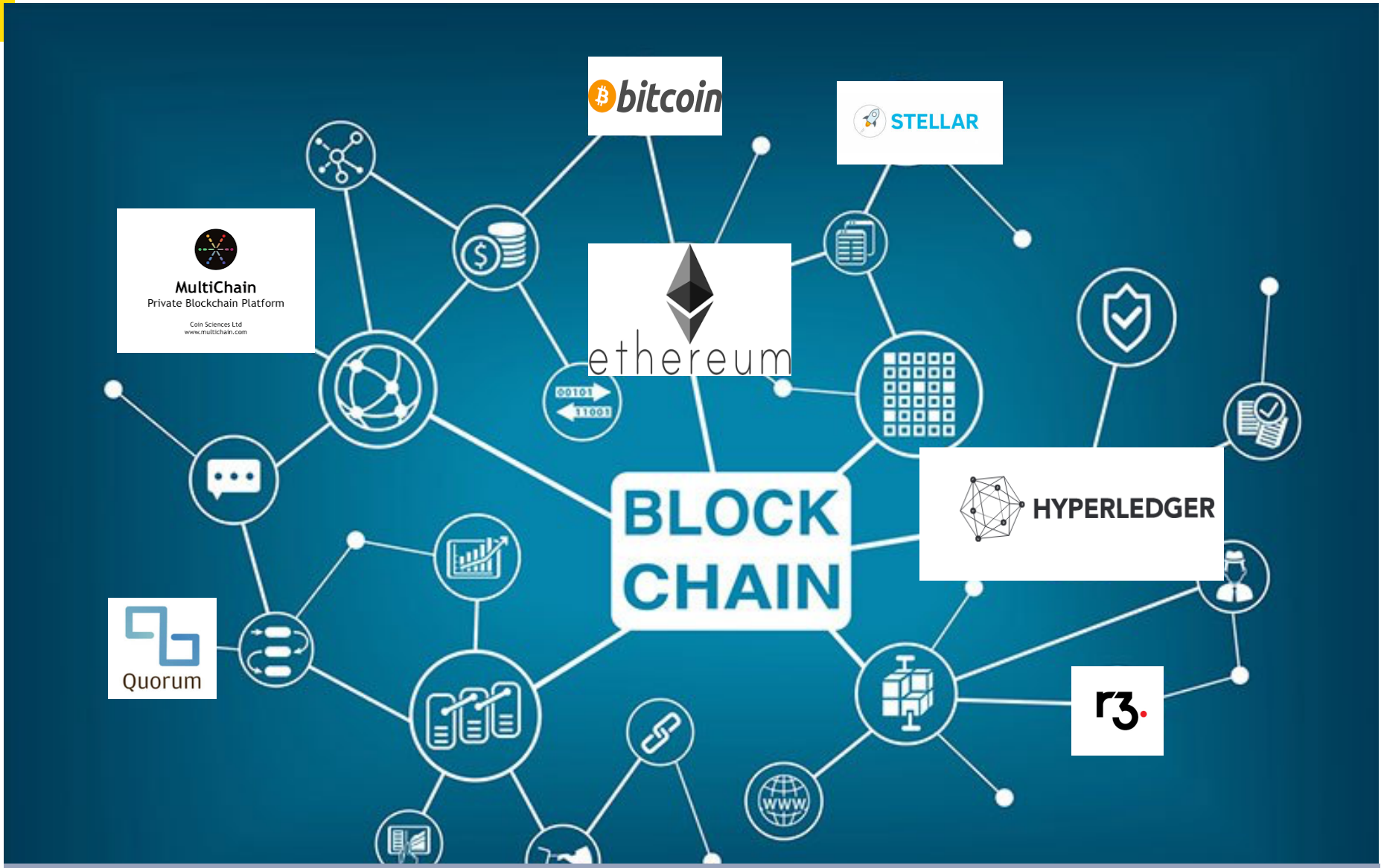
Main ISSUES with Public Blockchain

Enterprise blockchains have been launched in the last two years.

They are an effort of industrial consortium or service provider to combine blockchain capabilities with the need for assuring privacy and avoiding to use cryptocurrencies



Pre-Selection of potential blockchain architecture



- **Readiness/Maturity & Installation requirements in banking** sector might imply the exclusions of some technologies

DLT for Invoice Discounting

ELAPSED

12 months

PROJECT OBJECTIVE

Ideation, design, development and evaluation of an end-to-end prototype for a invoice discounting solution for the Italian Banks Ecosystem. The solution potentially allow to manage through the blockchain the entire process

MAIN PARTNER

GFT

Fondazine Bruno Kessler

CEFRIEL

ELAPSED

Currently ongoing
(Sept 2017 – Sept 2019)

PROJECT OBJECTIVE

Distributed Ledger Technologies and smart contracts may allow to enhance efficiency and reduce costs in complex ecosystem. In IN2DREAMS we are automating specific use cases related to the management of railways assets

MAIN PARTNERS

Evolution Energie

RFI RETE FERROVIARIA ITALIANA GRUPPO FERROVIE DELLO STATO ITALIANE

KU LEUVEN

UNIVERSITÀ DEGLI STUDI DI GENOVA

Main Goal

Create a system able to digitally manage interactions and workflows between the different actors that participate to the railways asset management ecosystem

IN2DREAMS

Shift2Rail

European Commission

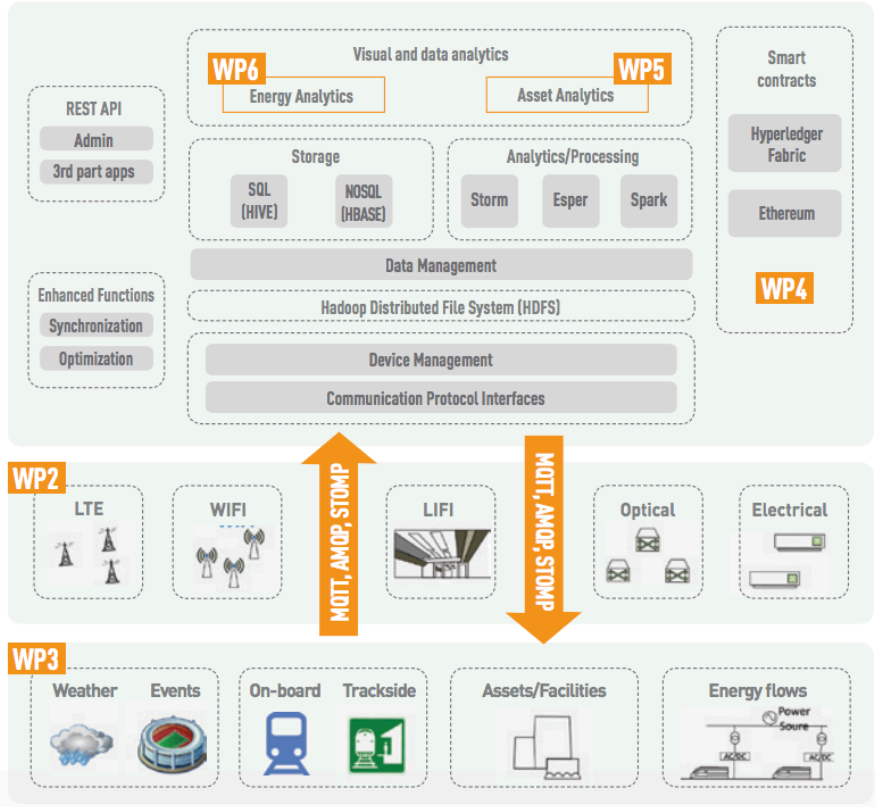
MAIN OBJECTIVES OF IN2DREAMS

Work Stream 1 – Management of Energy-related Data

WS1 aims to remove the current and anticipated limitations of REMS, by making these capable of supporting a much wider array of requirements than it is currently the case.

Work Stream 2 – Management of Asset-related Data

WS2 will address some of the challenges related to a specific Technology Demonstrator (TD3.6) outlined in the Shift2Rail Multi-Annual Action Plan. This TD focuses on interfaces with external systems, maintenance-related data management as well as data mining and data analytics, asset degradation modelling covering both degradation modelling driven by data and domain knowledge and the enhancement of existing models using data/new insights.



CEFRIEL Vision on Blockchain for the Health Ecosystem

Some Areas of Applications
Personal Health Record Management
Medical Devices and IoT Security
Supply Chain for Drugs and Medical Devices
Tracing and Tracking for Clinical Trials
Care Delivery

Key Benefits in Health Ecosystems

- *Integrity*
- *Reconciliation*
- *Transparency*
- *Patient Engagement*

An example

End-to-end clinical trials delivery and return process may be decentralized and developed over a **network of independent nodes**, so that allowing **the simplification** of process, **automation and cost reduction**

Challenges

- Exploit business opportunities and impact of blockchain-based solutions
- Investigate use cases and develop prototypes
- Be ready for future large scale development

Cefriel Approach

- From ideation to demonstration of end-to-end proof of concepts
- Technology evaluation and comparison
- Lab with state of the art of technology (Fabric, Stellar, Ethereum, and others)
- Experience lab and Education activities
- Support to blockchain lab creation
- Know-how transfer
- Collaboration with IoT Lab and SW Development Competence Centers

VIDEOSIGN

Project VIDEO SIGN

Elapsed: June-Nov 2016

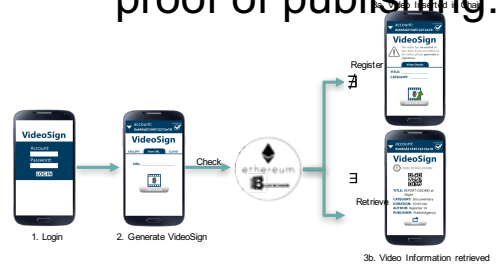
DIGITAL NEWS INITIATIVE

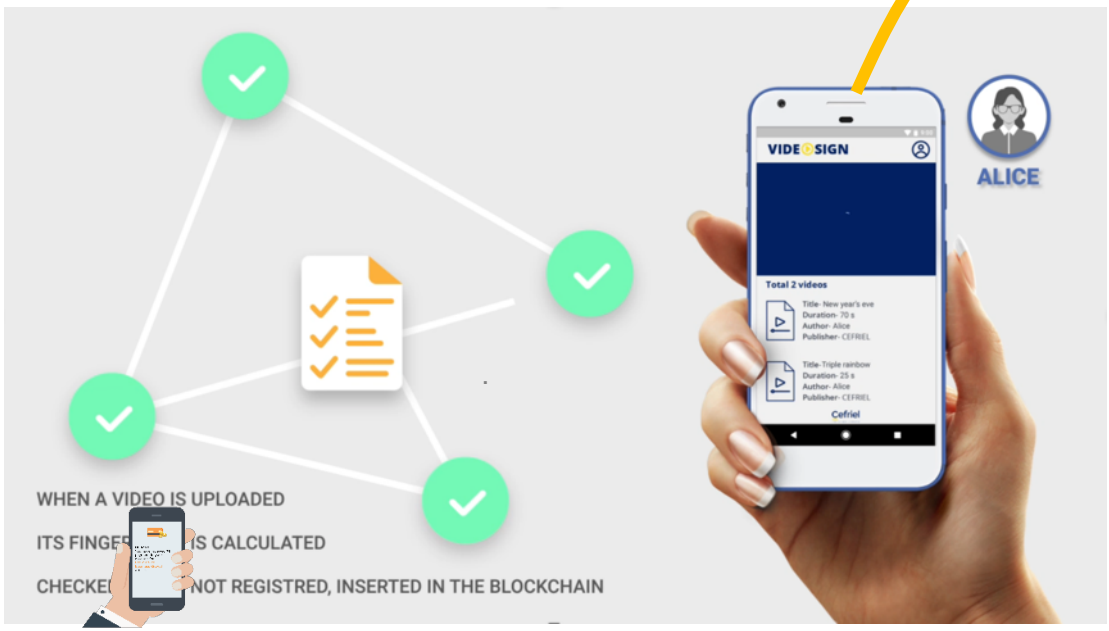
Sustainability

Innovation Fund

By applying advanced blockchain framework, we arrived at a Proof of Publishing PoC based on smart contract logics.

Blockchain can be used in the digital news for proof of publishing.





The journalist can prove the authorship without using frustrating locking system.

The model is based on Sharing Economy scenario

Blockchain in Digital Media

Potential Advantages and Motivation

- Cross site infrastructure
- Sharing Economy model
- Register is trusted by “users” by definition
- Low cost of implementation and maintenance
- Country-independent

ReaderWallet Project

Cefriel
POLITECNICO DI MILANO

Google
DIGITAL NEWS INITIATIVE

- PROJECT OBJECTIVE

The goal of the project is to study the feasibility, define an architecture and develop a Proof of Concept for a peer2peer micro-payment system based on the blockchain technology aimed at allowing users to buy news content on websites

- Motivation

Nowadays micropayments represent a limit for the news & media ecosystem. High transaction costs and lack of friendly user experiences do not allow business model based on acquiring of single content.

- Blockchain technology can be applied for micropayments.

With the adoption of blockchain it is possible to use cryptocurrencies to establish **direct peer2peer payments**, which have lower transaction costs if compared to traditional payment systems.

Moreover, using smart contracts features, it is possible also to implement the business logic aimed at tracking payments and managing access control to news, creating a standard interoperable method to manage access to content.

The infrastructure is maintained in a **decentralized way**, therefore there is no need of a central authority for managing information exchange. In this **sharing economy scenario** any user and any website news can use the technology and benefit trust and security intrinsic in the blockchain.

Potential benefits of Blockchain in Digital Media

- Reduce transaction costs, avoiding banks
- Cross site infrastructure
- Sharing-economy model
- Low cost of implementation and maintenance
- Country and website independent

READERWALLET

Project P2P PAYMENTS
(On-going project)

Jan-Jun 2017

Google | DIGITAL NEWS INITIATIVE

Sustainability

Application for micropayments in the Digital News Ecosystem

Blockchain mobile p2p payment are opening new scenarios for news ecosystem in long term.

The new approach

- Cross-site
- Sharing Economy model

1. **Alice is a free-lance** journalist. She has just finished her investigation piece, but she believes local news agencies won't pay her fairly for it. She then **decides to sell the article personally to each person who wish to read it**.
Alice connects to her ReaderWallet, which is like a "digital wallet mobile app"

2. She uploads the article on the website with a locking mechanism.
A QR code with her address for payment is automatically generated and displayed on her article's presentation page

3. **Bob wants to read Alice's article**. He is logged into the ReaderWallet and scan the article's related QR code present on the website.
A micropayment is due to Alice's for accessing the article.
Alice's wallet "receives" the money directly from Bob's wallet.

4. The **"smart " contract acts like an agent** and automatically gives Alice's a payment.
No transactions fees are due to the "Visa-like" third party.

Figure. Reference scenario for basic implementation.

SCOPE OF THE LAB

UNDERSTANDING THE TECHNOLOGY

Blockchain is a **complex technology**: in order to be ready it is necessary to understand how it works on relevant use cases.

A good learning strategy is starting with design and develop of **end-to-end prototypes** with multiple technologies, allowing to validate feasibility and providing **short-term results** aimed at supporting decision making for solutions.

BE READY FOR FUTURE LARGE SCALE ADOPTION

Blockchain is a disruptive technology: it is foreseen that in the next few year will introduce a revolution in several business processes. **Companies need to be ready for this change.**

Studying pragmatic use cases and suggesting the right approach and technologies to support companies in blockchain business evolution.

Nadia Fabrizio, Blockchain Expert and Agile Coach
nadia.fabrizio@cefriel.com
Twitter @nadyfabri
Skype:nadia.fabrizio
Viale Sarca 226, 20133 Milan
Web site www.cefriel.com

Any Questions?