Blockchain: Myth or Reality?

Systematic
Paris Region Digital Ecosystem
ACKNOWLEDGMENT

This book is the result of an intense collaboration between team members from several key players of the Systematic Paris-Region Cluster. We would like to express our gratitude to all the contributors.

Publication director
Jean-Pierre TUAL: Systematic Paris-Region

Editor and coordinator
Rodrigue GERMANY: Systematic Paris-Region

List of contributors & reviewers
Andra ANOAICA : IRT SystemX
Marine BAUCHERE: Deloitte
Olivier BETTAN: Thales Group
Kei-Léo BROUSMICHE : IRT SystemX
Hervé DEBAR: Institut Mines-Telecom
Roberto DI PIETRO: Nokia Bell Labs
Salma ESSAFI: Systematic Paris-Region
Nicolas FIGAY: Airbus Group
Jean-Yves GUEDON: Safran Morpho
Fabien IMBAULT: Evolution Energie
Waël KANOUN: Nokia Bell Labs
Sebastien KELLER: Thales Group
Ilan MAHALAL: Gemalto
Julien MALDONATO: Deloitte
Adam OUOROU: Orange Labs
Alain ROSET: La Poste
Matteo SIGNORINI: Nokia Bell Labs
David TCHOFFA: Université Paris 8/IUT de Montreuil
Eric THEA: IRT SystemX
Sara TUCCI: CEA List
Michel VOLLE: Institut d’Iconomie
Thierry WINTER: ATOS

Graphic design
Idées fraîches

ISBN: 978-2-9549444-4-9
Date d’obtention : 02/02/2015
BLOCKCHAIN TECHNOLOGIES AND TOOLS

SMART-CONTRACT

ORACLES

DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO)

DATA PRIVACY

INTEROPERABILITY

3/ CURRENT USE CASES, INITIATIVES AND APPLICATIONS

SMART GRID AND SMART ENERGY

IDENTITY MANAGEMENT AND IOT

UPORT

SECUREKEY

SUPPLY CHAIN MANAGEMENT

CHRONICLED & LEDGER

LEDGER

GOVERNMENT SERVICES

HEALTHCARE

FORMALIZED AND SECURE CADASTERS

GUARANTEEING DIGITAL IDENTITIES

MUSIC INDUSTRY

PRICE STABLE TOKEN SYSTEMS

DIGITAL FIAT CURRENCY

CROWD FUNDING

DECENTRALIZED ORGANISATIONS

4/ PERSPECTIVE FOR BLOCKCHAIN

LIMITATIONS & MAIN CHALLENGES

BUSINESS LIMITATIONS

TECHNICAL LIMITATIONS

FUTURE CHALLENGES AND PERSPECTIVES

REGULATORY, LEGAL, GOVERNANCE AND ECONOMY CHALLENGES

STANDARDISATION CHALLENGES
5/ SCIENTIFIC GAP ANALYSIS

51% ATTACKS
DATA MALLEABILITY
AUTHENTICATION AND CRYPTOGRAPHY
WASTED RESOURCES
PRIVACY
COMPRESSION ALGORITHMS
HASING ALGORITHMS
CONSENSUS ALGORITHMS
INTEROPERABILITY
ONLINE VS OFFLINE WALLETS
SMART-CONTRACTS VERIFICATION

6/ SWOT

7/ RECOMMANDATIONS

CONCLUSION

BIBLIOGRAPHY
PREAMBLE

The « Blockchain » topic has quickly raised to the forefront of the digital economy, from the little known bitcoin cryptomoney to one of the major expected building blocks of the digital world. One can attribute this to several factors. On one hand, the bitcoin ecosystem has received in recent months negative publicity, as the vector of ransomware that are plaguing millions of users deprived of their documents, as the victim of the first electronic heist through routing attacks, and as a contributor to climate risk due to excessive mining costs. On the other hand, one has to acknowledge that the technology underlying the bitcoin ecosystem, the bitcoin, seems to be able to deliver new services, such as Smart-contracts or secure software updates, that have been a subject of interest in the past but have largely failed to reach mass usage.

Due to this massive interest, the Blockchain technology has grown from a confidential, for cryptography experts only, scientific contribution published in October 2008 to a buzzword that offers both great potential and great hype. While its significance today ensures that the Blockchain technology is of real importance, myths over what it really can do need to be dispelled. Thus, the “Digital Trust and Security” working group of the Systematic cluster has decided to pool the expertise of its members in order to provide an actual view of the current state of the technology, what it is, what it can deliver and where we expect it will serve our purpose. We hope that you will find this contribution of interest and will be able to leverage this technology to support research interests, product development, new services and possibly more.

We wish you a fruitful reading.
KEYNOTE

To understand the Blockchain and what’s hidden behind its core technology, a quick look back into the history is useful. The Blockchain concept is nothing new in itself and like any other innovation throughout human history, it is built on the top of older concepts or ideas, re-engineered thanks to our modern computing, storage, networking and algorithmic resources.

The earliest form of the Blockchain concept probably dates back from around the 13th century, with the Messari double-entry system of the Republic of Genoa later followed by the modern double-entry system from the Florentine merchant Amatino Manucci, enabling full double-entry bookkeeping and which was largely used by bankers and merchants of Florence, Genoa, Venice and later Lübeck. The underlying concepts were later extended and mathematically formalized for the first time in 1494\(^1\) by Fra Luca Bartolomeo de Pacioli (1445-1517), an Italian mathematician, educator, and Franciscan friar, also a collaborator of Leonardo da Vinci and who is considered to be the «father of accounting and book-keeping». Pacioli’s system included most of the accounting cycle as we know it today. His ledger had accounts for assets (including receivables and inventories), liabilities, capital, income, and expenses, i.e. basically all items that are reported in an organization’s balance sheet and income statement.

In this system\(^2\), “the simple equation is Equity = Assets − Liabilities, and serves as an error detection tool, an important mechanism of logical and mathematical trust, and pillar of the latter Blockchain protocol”.

In very simple terms, Blockchain can be described as a way of storing the information related to all transactions between multiple parties in a trustable and not revocable way. The main difference with most available systems today is that recording, sharing, storing and redistributing of the transaction content is done in a secure (cryptographically protected) and decentralized way. Another noticeable difference is that Blockchain systems are owned, run and monitored by all actors in the system (at least theoretically), without anyone controlling it, hence avoiding modifications or abuses from a central authority.

\(^1\) Fra Luca Boartolomeo de Pacioli: Summa de arithmetica, geometria. Proportioni et proporctionalita (Venice 1494).

\(^2\) Cellabz : Blockchain and Beyond: Report November 2015, version 1.0.
The pioneering work of (pseudonymous?) Satoshi Nakamoto in 2008, followed by the first Open Source implementation of the Bitcoin system, almost immediately raised the attention of the financial community (and of the regulator and governments!) on the potential use of the Blockchain in the financial sector. After some erratic and controversial developments due to some infancy and security problems of the Bitcoin cryptosystem, the potential of Blockchain for the financial sector is now well understood and according to a recent IBM survey, 30 banks expect to have Blockchains in commercial production in 2017. They prioritize first for cost reduction and regulation compliances, but also expect to build new business models for example in trade finance or corporate lending (and finally protecting themselves from the Fintech). The Blockchain subject has been also for the first time at the agenda of the World Economic Forum in 2016.

Conceptually, Blockchain concepts apply to any type of transactions between entities, such entities being humans or machines. Departing from its initial focus on Finance, the potential use of Blockchain in various activity sectors is so heavily prospected, and most SW editors now offer Blockchains solutions on the top of their generic Platforms (e.g. Microsoft Bletchey on the Top of Azure, Google Deepmind, IBM’s Blockchain as a service, aso…). Most application domains are now investigating now the potential of the technology: Defense, Energy, Automotive, IoT, HPC…

The main goal of this White paper, coordinated by the Systematic “Digital Trust and Security” Working Group, is to provide a “vade-mecum” of the Blockchain technology, presenting in a synthetic way all underlying concepts, business data, key application domains outside the financial sector, potential limitations and related research challenges, current regulatory and standardization frameworks.

In this white paper, the security, privacy and performance aspects of the Blockchain technology are especially analyzed, as these concepts are considered in a completely different approach as compared to classical pyramidal systems.

Finally this white paper provides a SWOT analysis of the national Blockchain ecosystem and proposes some recommendations for its re-enforcement.

In this respect, the authors wish it will bring a useful contribution to the current thoughts in the field as well as an easy-access reference for all involved stakeholders (decision and policy makers, innovation actors, users, entrepreneurs…) in order to help them to better align their actions with their objectives.
INTRODUCTION

Mastering cyberspace is without any doubt one of the key aspects of our sovereignty. The continuous digitization of the economy is continuously generating new threats and opportunities, in front of which politics and economics decision makers are not fully prepared to define the most appropriate strategies.

From this perspective, the Blockchain technology is without doubt one of the most disruptive concepts that have emerged in recent years, with increasing awareness and interest from both the financial and technological communities. Initially intimately associated with Bitcoin, the first crypto-currency introduced in 2008 following the initial work of (Pseudonymous?) Sotashi Nakamoto (who also published a first version of the related Open Source SW in 2009), the range of applications of the Blockchain technology has dramatically evolved, as well as its technological basis.

The disruptive nature of the Blockchain resides mainly in the new way it addresses the Trust problem, the most essential value for the development of the digital economy. In very broad terms, Blockchain aims at providing a string answer to one of the most difficult questions related to our digital world "how can you trust people that you don't know?...". In this respect the Blockchain technology moves away from the classical pyramidal approach used in conventional systems.

In such pyramidal systems, a few Roots of Trust are visible enough to be controlled by “the public”.
- Examples (from the IT world) are: OS vendors, CPU designers, CPU manufacturers, AppStores, and of course PKI roots.
- Other examples are of a more organisational nature such as government systems (justice, police, social benefits…), and delegated authorities.

What makes these systems trustworthy is that their reputation prevents them from blatantly endorsing bad guys and that the users can “punish” them in case of failure (democracy, boycott, switch to alternate suppliers, aso…).

The Blockchain introduces a completely different paradigm for Trust, based on a fully distributed approach. The Blockchain approach is based on three founding principles:

- All transactions are recorded in a Distributed Trusted Repository (Distributed Ledger) controlled by “the public”.
- Control comes from the assumption that the good guys are more “powerful” than the bad guys (in Bitcoin, the “power” is the computing power of the “miners”).
- Trust comes from the fact that the content of the repository is publicly validated by “the public itself”, and that this avoids having everyone validating everything.

---

3 Satoshi Nakamoto is the name used by the unknown person or persons who designed bitcoin and created its original reference implementatio.
Many variants of the Blockchain technology have been defined, which differ notably by the definition and the implementation of the three above mentioned “public”, “power”, and “validation” principles.

The structure of this white paper, prepared by the “Digital Trust and Security” Working Group of Systematic Paris-Region with contributions from CEA List, Deloitte, Evolution Energie, Atos, Gemalto, Information System Working Group at Systematic Paris-Region, Institut d’Iconomie, Institut Mines-Telecom, IRT SystemX, Laposte, Nokia Bell Labs, Orange, Safran Morpho, Thales Group and Université Paris 8 is organized around five main chapters aiming at:

– Understanding the value proposal of the Blockchain in key business domains and giving a short term market perspective.
– Presenting all basic technologies and tools supporting the various Blockchains “flavours”.
– Giving an overview of major on-going Blockchain implementations or prototyping activities in non-financial sectors.
– Proposing a future perspective for the Blockchain, analysing the major non-technical challenges to solve for the successful introduction of the technology.
– Providing a technical analysis of current limitations of the technology that require additional research and development work.

Completing this in-depth analysis of the Blockchain, this white paper provides a SWOT analysis of the French ecosystem and proposes some recommendations to enable all involved actors to better understand the business, organisational and operational disruptive potential of the technology.

It is the modest ambition of the authors that this document will be a used as a quick reference for everyone interested in the Blockchain. We welcome in advance any feedback, suggestion or criticism from our readers.
1/ FUTURE ECONOMY TRENDS AND THE BLOCKCHAIN

A society that relies on effectiveness of computing resources creates the root of what we call the future digital economy.

After analyzing the relation between the digital economy and the Blockchain technology, we will provide figures of the Blockchain data market and we will highlight the relationship between Blockchain and three others key technologies which will have a similar impact on the digital society, the Internet of Things (IoT), Artificial Intelligence (AI), and High Performance Computing (HPC).

ECONOMY RELYING ON COMPUTING RESOURCES

The Digital economy is the schema, or model, of a society that, by assumption, effectively relies on computing resources. This model, which highlights the necessary conditions for efficiency, aims in a close future to guide the strategy of companies and institutions.

The perspective of Digital Economy can shed light on the perspectives of the Blockchain itself, while offering a point of view that enables us to disregard current technical debates, e.g., on the optimal size of the blocks, on the choice between proof of work and proof of stake for the remuneration of miners or minters, on the performance of smart-contracts, etc.

The essential features of the digital economy are as follow:\footnote{4}{Claude Rochet et Michel Volle, L’intelligence économique, De Boeck, 2015.}:

- Repetitive physical and mental tasks are automated.
- Each product is diversified according to the variety of needs.
- Each instance of a product is an assembly of goods and services developed by a network of partners.
- Each company aims to acquire a temporary monopoly.

This short description immediately reveals the fields of application of the blockchain technology: cooperation within a network of skills, business engineering around partnerships, cohesion of the assembly of goods and services.

In terms of forecasting, we consider the most advanced Blockchain generation, known as 3.0, which supports smart-contracts and encompasses the functionality of generations 1.0 (realization and retention of payments in digital currency) and 2.0 (storage of traces of transactions relating to assets\footnote{5}{Anuchika Stanislaus, « Les enjeux et défis des infrastructures de données utilisant la Blockchain selon l’Open data institute », LINC, 2 août 2016.}).
NETWORK OF COMPETENCES

The structures found today in open source and, more generally, crowdsourcing structures, are the primer of an organization form that will be frequent in the Iconomy: Decentralized Autonomous Organization or DAO. The Blockchain technology provides the technological foundation of an equilibrium of equals, that was previously lacking and removes an obstacle to cooperation.

Let us illustrate this with an example. When AOL bought the Huffington Post for $315 million in February 2011, people who had contributed to the crowdsourcing diary protested because they believed that some of the added value should have come back to them.

However, to be able to operate, a DAO must not be prohibitively expensive in terms of design and operation, and intelligent contracts must be designed to include the appropriate incentives.

BUSINESS ENGINEERING

Since repetitive tasks are automated, most of the production cost lies in the fixed cost of the initial investment (sunk cost): product design, automaton design and programming, distribution network design. Nearly all production costs are thus spent before the company receives the first response from the market and competition.

Sharing product development within a network of partners makes it possible to distribute and limit it. This is frequent in today’s industry: automobiles, military aircrafts, airliners, ships, are designed that way. This also exists for services, for example in code-sharing in air transportation, unbundling in telecoms, and logistics operations in distribution. This form of organization tends to replace the contractor / subcontractor relationship, which is often unfair.

Setting up and maintaining a network of partners requires business engineering to define reciprocal mutual commitments and tasks sharing, responsibilities, expenses and revenues. It must also ensure the interoperability of their information systems, which conditions the efficiency of the production process. The cost of business engineering is part of the fixed cost of the initial investment; The contract performance monitoring is also a fixed cost (it hardly depends on the volume produced), but distributed over time.

---


7 Ethereum, widely seen as the most ambitious crypto-ledger project, wants its Blockchain to go beyond transferring value: it should also be able to execute simple tasks such as verifying if a party to a contract has fulfilled its side of the bargain. Its boosters think such a machine could support “smart-contracts”, where a computer can verify or enforce an agreement » (« The next big thing », Special report, The Economist, 9 mai 2015).
An intelligent Blockchain-based contract can meet these requirements: it triggers transactions that split expenses and revenues in an automatic and controllable way. The security and transparency it provides, as well as the reduction in transaction and control costs, are a decisive factor in partnership strength and effectiveness.

Note that while the intelligent contract facilitates the operation of the partnership, and automates a work that would otherwise be done by human beings, the intelligence it involves does not replace the one that is essentially human, which requires the expertise of the organizers and negotiators: notaries, for example, will no doubt lose their mission of archiving but they will retain their advisory role.

COHESION OF GOODS AND SERVICES

In the digital economy, the company seeks to gain a temporary monopoly over a segment of needs. It must differentiate its business model from its competitors’ by endowing its product with qualitative attributes that correspond to this segment: The digital economy is the economy of quality.

The cohesion of the dovetailing of goods and services, or of pure services, requires an information exchange architecture, a traceability, a security for which the Blockchain will be an essential building block. The Internet of Things (IoT) provides solutions for inventory management, supply logistics and remote maintenance; the Blockchain, combined with a distributed computing architecture (edge computing), provides an efficient solution to control the volume of data exchanges and the processing involved.

The cost reduction transaction is likely to give rise to new markets and business models in two layers that involve different companies:

– Blockchain infrastructure offerings (Ethereum, Tezos, etc.) which are distinguished by their technical characteristics, middleware offering (document management with Keeex, vouchers with MoneyTrack, etc.).

– Service solutions offerings targeting final end-users.

---

8 A «smart-contract» is a software, an application of the Blockchain. There is a tendency to assimilate smart-contracts to contracts, but they do not have legal authority in themselves: when a legal contract exists, the smart-contract is merely a technical application of this contract. «Blockchain France, «What is Ethereum?», 4 March 2016.

9 In the case of the Internet of Things, we’re going to need a Blockchain-settlement system underneath. Banks won’t be able to settle trillions of real-time transactions between things » (Don Tapscott, « How Blockchains could change the world », McKinsey Company, mai 2016).

10 We identify two key costs that are affected by distributed ledger technology: 1) the cost of verification; and 2) the cost of networking. Blockchain technology, by allowing market participants to perform costless verification, lowers the costs of auditing transaction information, and allows new marketplaces to emerge. Furthermore, when a distributed ledger is combined with a native cryptographic token (as in Bitcoin), marketplaces can be bootstrapped without the need of traditional trusted intermediaries, lowering the cost of networking » (Christian Catalini et Joshua S. Gans, « Some Simple Economics of the Blockchain », National Bureau of Economic Research, 13 avril 2017).
SERVICE LEVEL

Infrastructure offerings will be diversified but relatively few in number. Their diversification will be similar to the one currently observed in the operating systems domain, about a dozen today. Service offerings, on the other hand, will diversify almost without limits to match the diversity of needs, as today’s web services do, and from a tool-service\textsuperscript{11} to a solution.

Figure 1: Breakdown of Blockchain players by service level (Deloitte)

The chart below confirms this trend: we see a diversification of the uses of the Blockchain, according to various sectors of activity.

Figure 2: Breakdown of Blockchain players by activity manager (Deloitte)

To illustrate the richness of Blockchain use cases in different industrial sectors, we include herein recent examples to illustrate Blockchain uses by domain still under experimentation:

– Financial services: Insurance, Loan, Asset management
– Industry
– Energy

\textsuperscript{11} Document or intellectual property verification (sealX and geniusX, blocksign, Factom); Control of supply chains (EverLedger, Provenance, Skuchain); Peer-to-peer business initiatives (Slock.it, Airlock.me, Lazooz, WeiFund); Governance system (Colony, Freecoin, Boardroom, BitNation); Distribution of dematerialized content (Alexandria, UjoMusic, Blockain).
The following are examples of actors according to their use cases:

**FlightDelay**: Using the power of smart-contracts to automate the compensation of insureds when delaying or canceling an air flight.

**BTCpop**: A platform of reputation-based lending, “BTCpop’s peer to peer lending” is based on reputation, not credit score. Quickly get loans from other members or make some money by loaning money you have. You set the terms. You set the amount.

**Deloitte**: Blockchain for sharing of investment fund. The shares are represented by tokens on a public channel. A Smart-Contracts is used to manage subscriptions and redemptions. Crypto currency is used to allocate tokens to the subscriber after a valorization by the manager.

**Zerochain**: Verification of renewable energy production certificates. The system, which was developed by the energy tech startup Evolution Energie, enables users to track renewable power as it moves through the electrical grid and mixes with energy from other sources. “Using Blockchain, you can sell energy from your renewable sources to your neighbor without the help of a utility managing the process,” says Fabien Imbault, Evolution Energie’s managing director. “You could share your energy with neighbors or even sell it to a parked electric car on your street and get paid securely.”

**Storj**: Decentralized and secure storage cloud device to remove the limitations related to storage capacities of the Blockchain.

**iEx.ec**: Increase the computing power of network members.

**Blockpharma**: Blockchain solution for drug traceability and anti-counterfeiting. The Blockpharma application allows consumers to instantly check the drug authenticity before buying it.

**Bitnation**: Manages the digital identity of all citizens. The First Blockchain-Based Virtual Nation Constitution.

**Augur**: Predict the outcome of real-world events by trading virtual shares: if you think Leonardo DiCaprio will win another Oscar, then buy shares in this outcome. If this prediction comes true, you will earn real money.

**Steem**: The members of the social network post articles, when people appreciates an article they can vote for each writer, which receives money in return based on the number of collected votes.

**Swarm.city**: A decentralized global community of peer-to-peer service providers and consumers. The core technical offering is a decentralized app running on Ethereum.
Ujo Music: Open music-sharing platform built by the startup Consensys, in partnership with the singer Imogen Heap.

Ether: Buying music through crypto-change. Artists record their songs in the Blockchain which are then assigned to a unique identifier. A Smart-Contracts indicates the sale price of the song and the remuneration of the creators of the song (musicians, singer ...). Each transaction (sale - purchase of songs) is recorded in the Blockchain.

The sector of financial services brings together the largest number of players. This could be related to the case of initial use of the Blockchain, namely the exchange of crypto-coin bitcoins. The use of Blockchain in financial services is varied, as can be seen from the graph below:

*Figure 3: Focus on the Blockchain services offered within the financial sector (Deloitte)*

The Blockchain development also leads to a change in the financial services sector in particular through the creation of new services. One example is the development of a new financing method for Blockchain startups like ICO\(^\text{13}\). Funding is obtained through a form of pre-purchasing, not for a product as it is usually the case in conventional crowdfunding, but for digital assets called coin or tokens, in the Blockchain world. The created coins are purchasable in exchange for an amount in crypto-money. Then, if there is sufficient demand, the virtual currency exchange platforms will create a market to allow the exchange of these tokens. Thanks to the ICO, Blockchain startups no longer have to go through investment funds to develop; pre-selling their tokens to early adopters is enough. This funding model, based on the potential that the crowd places in an innovative idea, will likely allow Blockchain startups to lift the development barriers imposed by venture capital.

\(^{13}\) Initial Coin Offering.
This new financing approach, still in its inception, is seen as both a means of decentralizing and disintermediating venture capital, creating new sources of funding for entrepreneurs, and offering them new investment opportunities said Travis Scher\textsuperscript{14}.  

![Layer of the Blockchain (Institut d'Iconomie)](image)

Each business models will specify the form of governance and will include cascaded pay, users paying for the service, paying service itself, tool services, infrastructure and miners or founders who provide the necessary work for the building blocks. The intervention of miners or founders will be the subject of a partnership which construction will require business engineering according to the logic mentioned above.

The number of possible applications is illustrated today by the diversity of service-tools and service-solutions already offered or planned: money transfer, car-pooling, certification of documents, collaborative work, insurance, voting in elections, etc. According to William Mougayar\textsuperscript{15}, the overall taxonomy distinguishes between infrastructure and platforms, services-tools, applications and ancillary services.

The applications’ taxonomy identifies:

3 structuring concepts:
- encrypted currencies,
- Smart-Contracts,
- DAO.

4 application domains:
- finance (processing of transaction flows, asset management, compliance, etc.),
- the public sector with transparency improvement (taxation, social welfare, anti-corruption) and cost reduction,
- the legal sector (proofing of contracts and property rights, automatic contract execution, etc.), and
- the Internet of things (interoperability Equipment, etc.).

\textsuperscript{14} Travis joined DCG in 2015, and supports the firm’s investing efforts. His responsibilities include sourcing, analyzing, and executing venture investments, and helping DCG portfolio companies raise additional capital.

Careful attention is required in the details of Smart-Contracts. When a contract triggers the execution of a computer program, the service comes out of the secure and encrypted world of the Blockchain to enter the more open world of computer programs, subject to all kinds of attacks. The risk may remain limited if the contract involves only a small number of partners who know each other. On the other hand, if the service is open to the wider world, it will be subject to the same temptations and risks as any use of an executable program.

**BLOCKCHAIN MARKET DATA**

**BLOCKCHAIN MARKET INVESTMENT**

A sustained mature evolution.

<table>
<thead>
<tr>
<th>Year</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investments in Blockchain (Millions of USD)</td>
<td>1</td>
<td>93</td>
<td>357</td>
<td>525</td>
<td>550</td>
</tr>
<tr>
<td>Annual growth rate</td>
<td>-</td>
<td>200%</td>
<td>284%</td>
<td>47%</td>
<td>5%</td>
</tr>
</tbody>
</table>

*Source CB Insight*

**BLOCKCHAIN INVESTMENT IN 2015 AND 2016**

Investments in Blockchain players showed exceptional growth in 2014 and 2015, with amount invested in 2015 five times higher than in 2013.

<table>
<thead>
<tr>
<th>Year</th>
<th>2015</th>
<th>2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>Q2</td>
<td>Q3</td>
</tr>
<tr>
<td>Investments in Blockchain (Millions of USD)</td>
<td>226</td>
<td>158</td>
</tr>
</tbody>
</table>

*Source CB Insight*

Blockchain companies attracted $525 million in 2015, largely as a result of a peak in investments in the first quarter of 2015. Investments then decreased until the fourth quarter of 2015 when only $45 million was invested 67% of the fundraising activities carried out between January 1, 2015 and February 18, 2016 concern companies specializing in Blockchain infrastructure and applications. The remaining 33% are companies specialized in bitcoin. (*)

In 2016, there is a concentration of investment in Q1, but investments in this year follow a similar downward curve to that of 2015. Investments are gradually losing momentum in the end of 2015 and 2016, to see if this phenomenon repeats itself on a recurring basis in 2017.
MarketsandMarkets estimates the global Blockchain market size at $210.2M in 2016 with a projection at $2,312.5M in 2021 (an annual growth rate of 61.5%). NB: Calculation assumptions not reported.

The maturity of startups raising funds has increased over the years: the diversity of maturities is highest in 2016. This can be explained in particular by the improvement in investors’ knowledge of Blockchain technology.

Investment rounds legend reflects the level of maturity of a startup:

**Seed capital:** First fundraiser, amounts between 250k€ and 700k€, launch of the startup.

**A Series:** Second fundraiser, enables the startup to acquire a critical mass of users and move towards profitability. Amounts between 800 k€ and 3 million euros.

**B Series:** To allow the startup to internationalize, to facilitate its scale up. Amounts approximately between 3 and 10 million euros.

**C Series:** Accelerates the development of the startup. This is sometimes the occasion of IPOs - 10 to 100 million euros.

**D Series:** And so on, depending on the number of completed rounds.

**BLOCKCHAIN TECHNOLOGIES**

Combining Blockchain with other technologies can create more added value. In some cases, the Blockchain can even be a basis for accelerating the development of another breakthrough technology (for example, Artificial Intelligence). The illustrative examples proposed below are still in phases of experimentation.
**BLOCKCHAIN AND IOT**

In order to extend the scope of the Blockchain, some startups have begun to explore the potential of its coupling with connected objects. One example is Slock.it, a rental platform based on Smart-Contracts in a Blockchain. The specificity of this case lies in the fact that the goods can be leased remotely thanks to an electronic locking system. The renter and the tenant no longer need to meet to exchange the keys.

**The process is as follows:**

– Renters publish, on the Slock.it’ application, the goods they submit for rental and indicate the rental conditions (prices, terms of use ...). It can be any object that can be secured by a lock or a padlock (apartment, bike, warehouse ...). The object must be equipped with the Slock.it electronic lock.

– An electronic key is associated with the lock / padlock of the object subject to the rental. If a client is interested in renting an apartment, he can consult on the application the terms of the property rental (price, duration ...).

– If the validates the rental, the rental amount and a deposit are placed on an escrow account, and Slock.it sends to the landlord an electronic key enabling him to unlock the lock for the duration of the rental. Once the rental period expires, the key becomes invalid. A smart-contract is associated with each property leased. It contains its rental conditions and allows to automate the rental process (receipt of payment, assignment of electronic keys). In this case, the Blockchain, coupled with the connected objects, makes it possible to secure and simplify the rental processes between individuals.

**BLOCKCHAIN AND ARTIFICIAL INTELLIGENCE**

Several players combine the potential of Blockchain and artificial intelligence. Indeed, it seems that these two technologies are complementary: the Blockchain and the Smart-Contracts could be the key to one of the founding pillars of artificial intelligence, namely the constitution of vast databases allowing to train the Artificial intelligence (AI) technology and to make it «intelligent».

Although it is necessary to train an AI, building a large and quality database is not easy. Gafa such as Facebook and Google shine in these two tasks, since their users give them free access to a lot of data via their activity on the net (sharing photos and personal data on Facebook, entering keywords into Google search engine ...). They also control the quality of the data they communicate through « likes », shares, tag and other clicks that validate the relevance of the displayed content. Unlike major players such as Facebook or Google, other companies have to pay suppliers and data controllers to build their quality database for artificial intelligence training. They must therefore convince them that they will not be cheated (transparency, use of data, revenues generated by the exploitation of these data...).
Smart-Contracts, which have the power to force all parties to honesty and eliminate transaction costs (sending a token is virtually free), are a solution that can solve these data access questions. Blockchain facilitates the creation and qualification of large databases necessary for training artificial intelligence algorithms. Furthermore, Smart-Contracts ensure that each of the contributors will be paid according to its actual contribution. We can illustrate this concept with a simple example: we want to train artificial intelligence on the recognition of the peculiarities of cars. For this, a Smart-Contracts would propose to all the members of the network to add photos of their personal cars to the biggest multimedia database that contains all world cars. Contributors, whose submitted photos would be validated as car photos, would be paid automatically in tokens (verification of the data quality and payment of the contributors). The controllers, who validate that each photo sent is valid, would also be paid automatically in tokens (Blockchain intrinsic principle, same than the miners in the Bitcoin framework). IA developers who use the database to train their algorithms would pay in token for each use, thus feeding the system.

In this example, the Blockchain appears as an accelerator of the development of artificial intelligence. Indeed, capitalizing on the strength of the Blockchain network to create specific, high-quality databases, accessible to all, would place all artificial intelligence developers on an equal footing in terms of data access necessary for artificial intelligences training.

Blockchain and HPC

Another startup leading active research on the possible alliances of the Blockchain with other technologies is iEx.ec. This Start up started by combining Blockchain and HPC by creating a platform allowing the development of Blockchain-based applications while providing secure, adaptable and simplified access to the computing resources required for their execution (computer computing capacities). This results in the creation of a Blockchain-based market, on which each member of the network can monetize its servers, applications, datasets. This application uses the Ethereum Smart-Contracts capabilities to allow everyone to create their own cloud infrastructure. The iEx.ec solution extends cloud services from traditional solutions such as SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service) to HPC for on-demand services. This new type of Cloud service reconciles Blockchain intrinsic infrastructure solutions with sharing expansion and the peer-to-peer economy conveyed by the Blockchain.

IEx.ec is now studying how to give network members the opportunity to monetize Blockchain applications based on other technologies such as big data, IoT, artificial intelligence or cloud by guaranteeing the degrees of transparency, resilience and Blockchain intrinsic safety.

---

17 Standing for “I Execute”, iEx.ec is a French/Chinese company headquartered in Lyon, France. The platform was first introduced at the Ethereum Devcon2 conference held in Shanghai, China in September 2016. The team also successfully showcased a demo of the platform at the Super Computing Exhibition 2016 held in Salt Lake City, USA.

2/ BUILDING BLOCKS

DEFINING THE BLOCKCHAIN

A Blockchain is a distributed data structure that is shared and replicated among the nodes of a network, and which is secured by cryptographic tools and a consensus mechanism.

DATA STRUCTURE

The data structure corresponds to a linked list of transactions. Each element of the list, a block of transactions, has a pointer to the previous block: each new block $b_i$ that is added has a pointer $p_{b_i}$ that points to the previously added block: $\text{Address}(p_{b_i}) = b_{i-1}$. Moreover, the pointer $p_{b_i}$ of the new block contains the hash of the previous block $\text{PreviousHash}(p_{b_i}) = \text{Hash}(b_{i-1})$ (see figure 5).

This hash is a key element of the Blockchain security. If an adversary tries to modify the content of a block $b_m$, anyone can detect it by computing the block’s hash, $\text{Hash}(b_m)$, and comparing to its hash stored in the next block $\text{PreviousHash}(p_{b_{m+1}})$ to see that there is an inconsistency. In order to avoid this detection, the adversary could change all the blocks and their hashes, from the block $b_{m+1}$ up to the latest block $b_{\text{latest}}$. However, the blocks cannot easily be changed thanks to the protocol defined for adding blocks that we describe in the next section.

DISTRIBUTED NETWORK

Nodes. The participants of the Blockchain are nodes that form a peer-to-peer network. Depending on the implementation of the Blockchain, the network is either public (i.e. anyone can access it) or private / semi-private (i.e. only allowed accounts can participate). Each node has a local copy of the whole Blockchain (or the most recent part of it). When retrieving the Blockchain, a node verifies the integrity of the blocks by computing all the hashes. Every node can send transactions and ask the network to add these transactions to the Blockchain, these pending transactions are then validated by some special nodes called the miners (also known as block generators or validators).

---

19 A hash function takes an input data and outputs a hash, a fixed size data that is specific to the input as a fingerprint.
**Miners.** Miners are nodes that are willing to share their computational power to add blocks to the Blockchain, usually in exchange of crypto-money. The way they are paid depends on the implementation of the Blockchain, however it often involves a fee (i.e. the node who was asking to add a transaction pays the miner to do it) and/or creation of value (e.g. in the case of Bitcoin, the Blockchain creates cryptocurrency and gives it to the miner who has added a block).

**CONSENSUS MECHANISM**

Because (in public Blockchains) they are paid, all the miners are in competition: they all want to add the next block but only one of them will achieve it, in a random way for each new block. This randomness is very important for the security of the Blockchain: since no one knows which miner will be selected, an adversary miner has low probability to be selected, thus has low interest into trying to attack. This leads to the famous 51% attack: if more than half of the validation power of the network is allied with the adversary, there is more chance that the attack succeeds than fails, so the network can be considered under his control.

**Consensus.** There are various ways to enable this random selection among the miners: they are the consensus mechanisms. Public Blockchains usually use a Proof of Work consensus, whereby the more computation power a miner has, the higher the probability that his block will be selected. As computation power is expensive, the cost of acquiring 51% of the network computation power is high. This is a way to secure the network, as the nodes in public Blockchains are unknown and cannot be trusted. Private Blockchains (nodes belong to a same user) or semi-private Blockchains (nodes belong to a consortium of different users) don’t need such a costly consensus mechanism, because the participants are known. In this case, the consensus mechanism is much simpler. Below, we will describe in more details the different consensus mechanisms implementations.

**Forks.** Once a miner’s block has been selected, it is added to the Blockchain and the information is broadcast. Due to network effects, there are cases when multiple miner’s blocks are selected, so there are different versions of the Blockchain in different regions of the network. This is called a fork: the Blockchain splits into branches. The mechanism consensus should be robust enough to account for this kind of scenario. In other words, all honest nodes should somehow converge in the future towards acknowledging a unique and same version of the Blockchain. In practice, the Proof of Work consensus achieves this result by requiring miners to work on the longest branch that they see.

In addition, the miners’ software is sometimes updated to fix bugs or add functionalities. This also can create forks, as different nodes might handle transactions differently depending on their software versions. We usually distinguish:

- “Soft forks” where the transactions considered valid by the new version are also valid for the old version.
– “Hard forks” where the transactions considered invalid by the old version might be valid for the new version.

CRYPTOGRAPHIC TOOLS

Cryptographic tools are used to guarantee the participant identity, the Blockchain integrity, the transactions authenticity and (sometimes) the content privacy.

Identity. An identity is defined by a pair of keys: one private key that is meant to be only known by its owner and a public key aimed to be shared with other users. Technically speaking, these two keys correspond to hexadecimal numbers. In this section, we will take the example of the Ethereum Blockchain. On this Blockchain, private keys are 256-bits numbers, randomly generated. Therefore, it is probabilistically almost impossible to generate two same private keys. This private key is then given to a cryptographic function secp256k1 to generate a 512-bits public key. Finally, this key is hashed to produce a 160-bits address using SHA-3 hash function. These keys are often encrypted by a pass-phrase given by the user and can be stored either on the cloud, on his personal machine or even printed on paper. These keys are used to be identified and to sign transactions.

Signature. When a registered user wants to add a transaction to the Blockchain, he sends it to the network so that some miners can receive it, check it and add it to their blocks. But in order to be checkable, the transactions (data) must be signed so that the miner can identify the sender for sure. The signature is generated by a cryptographic function that takes the data and the private key of the sender. This signature is verifiable by anyone using a function that takes the data, the signature and the public key. Therefore, when sending data, senders also add their signatures and their public keys. In addition, addresses are used to identify the receiver’s account for example.

*Figure 6: Functioning principles (simplified)*
CONSENSUS MECHANISMS

In this section we describe the major consensus mechanisms that are used today in Blockchains. There is no universal consensus mechanism because, as we shall see, different mechanisms have different advantages and drawbacks.

PROOF OF WORK (PoW)

This mechanism ensures that each miner has supplied a substantial amount of computational work before validating blocks, thus preventing denial of service attacks.

To add a block of data into the Blockchain, each miner has to validate the current block’s data and its consistency with the previous blocks and solve a cryptographic puzzle. The puzzle consists of finding a nonce in \( N \) so that the hash of the data combined with the nonce begins with at least \( p \) zeros. Thus the complexity of solving this puzzle is directly function of the number of required zeros \( p \). This enables the Blockchain system to control the difficulty of puzzles according to the fluctuating ratio between the total amount of power available on the network and the number of pending data in order to maintain a stable average mining time (e.g. increase the difficulty when there are too much miners, decrease the difficulty when there are too much pending data etc.). For example, Bitcoin, which uses this consensus mechanism, maintains an average mining time of 10 minutes. Once a miner has solved the puzzle, he can add the corresponding data with its hash and nonce to the Blockchain.

Since this protocol is used on a decentralized network, while the probability is low, multiple blocks containing similar data can be generated for the same block index by different miners. This leads the Blockchain to fork into branches. In that case, it is up to the next miner to validate a block \( Bi+1 \) to choose the branch (i.e. the block) he will increase. Then, the third miner to validate a block will have to choose a branch as well. In general, miners choose the longest branch, thus the \( Bi+1 \) will be chosen and the other branches won’t be increased, making them orphan blocks. It is generally admitted that a branch of approximately 6 blocks can be considered as the main branch. Which means that in order to be sure that a block is valid and won’t be orphaned, it takes 1 hours on Bitcoin (i.e. \( 6 \times 10 \) minutes). The consequence of this consensus mechanism is obvious: it demands a lot of work, thus energy. Indeed, the puzzle requires by design a lot of power from each miner in the network.

PROOF OF STAKE (POS)

This consensus mechanism relies on the idea that the more a user owns a currency on the Blockchain, the less he is likely to attack the system. Thus he would be more likely to be chosen for the next block generation. However, to some people it could be seen as an unfair protocol since a small amount of rich people would dominate the entire network.

\(^20\) A nonce is an arbitrary number that may only be used once.
Therefore, some solutions proposed to combine different selection criteria. For example, Nxt and Blackcoin use a formula, often referenced as randomization, that looks for the lowest hash value in combination with the size of stake (i.e. the balance). Another example of criteria is the coin age based selection which uses the time each coin has been held by its owner. Alternative proposals combine POS with other consensus mechanisms such as the POW as Ethereum would do in its next stable release. While this consensus mechanism is power effective, it has also some limitations. A known issue is called the nothing at stake problem. Indeed, if there is one valid branch A and another B containing a double spending, block generators (i.e. miners) will have to choose between them. However, since it doesn’t cost anything to vote on one or the other, one strategy would be to vote on both branches in order to maximize the chance to earn money for block generation. Different solutions have been proposed to solve this specific issue, usually involving a security deposit that can be forfeited in case of a bad behavior.

**PRACTICAL BYZANTINE FAULT TOLERANCE (PBFT)**

PBFT is a replication algorithm that is able to tolerate Byzantine faults. Put simply, this algorithm ensures the consistency of consensus as long as two thirds of the network’s nodes are safe (i.e. not malicious and not faulty). This is enabled by replicating behaviors (i.e. state machines) of generating nodes (i.e. miners) and applying protocols for choosing a leader among them. However, this method requires that all the generating nodes know each other since they need to communicate. Therefore, the network has to be private and its scale be limited.

**DELEGATED PROOF OF STAKE (DPOS)**

While validators are directly elected according to their stake in POS, in this consensus protocol, rich nodes delegate validations to representatives. In other words, stakeholders elect miners among a small number of nodes. This enables fast mining: on Bitshare, which implements this consensus system, the average validation time is 1 second.

**BLOCKCHAIN TECHNOLOGIES AND TOOLS**

**SMART-CONTRACT**

The concept of smart-contract (also referred as chaincode) has been implemented first by Ethereum. These are computer programs that are executed by the miners. Their deployments and executions are triggered by users through transactions. Like any other transaction, smart-contracts executions also benefit from the properties of the Blockchain: security, integrity, no intermediary, transparency and availability. Thus, one can offer an automated service over the Blockchain through a smart-contract which execution is ensured by the network. For example, a smart-contract could implement an asset representing some kind of ownership that one can sell or buy in an auction manner. Once placed on a market by its owner, some potential buyers place
money on the contract. Then, at a given time, the owner calls the sell function of his asset. This function automatically selects the best offer and gives its ownership to the best buyer. The other bidders are automatically refunded by the smart-contract and the seller receives automatically his money. In this way, all the transactions are secured by the smart-contract and the miners without any third party intervention.

**ORACLES**

In the previous section, we saw that smart-contracts enable the automation of transactions according to programmatically coded conditions. However, the conditions are limited to the internal state of the Blockchain: information about transactions and the smart-contract’s source code. This is where oracles step in. They provide a service that enables communication between the Blockchain and the open-world through Internet. Technically speaking, they allow the smart-contract to call web services using REST. This way, a smart-contract can be aware of the weather, the results of a soccer game, flight information of a specific plane and so on. It is also possible to output data to the real world from the Blockchain. For example, in order to notify some user by email of the execution of the contract.

**DECENTRALIZED AUTONOMOUS ORGANIZATION (DAO)**

A decentralized autonomous organization (DAO) is an organization that relies on rules implemented in smart-contracts. The most famous DAO example was project implemented on Ethereum called “the DAO”, which was meant to crowdfund projects for a profit. What made it so famous is that when launched in May 2016, this project managed to collect roughly 150 million dollars in 28 days. Unfortunately, a bug in the program was exploited to divert part of this money (an estimated 50 million dollars), therefore highlighting the risks and low maturity of the technology. Following this bug, the project was closed and a hard fork on the Ethereum Blockchain reverted the money transfers. Even though this was an unfortunate incident, the general DAO concept still lives on and rightfully represents an interesting perspective for Blockchain applications.

**DATA PRIVACY**

A transaction is considered anonymous if we cannot identify its owner. Nonetheless, a transaction can have a known initiator and still be private. Indeed, a transaction is called private if the object and the amount of transaction are unknown. Several cryptographic tools can be used to enforce data privacy.

**Homomorphic Encryption.** This technique allows for computation to be done on encrypted data, resulting in an encrypted result. Yet, the decrypted version of the encrypted result still matches the result of computation that would have been performed on the original non-encrypted data. Such a scheme enables the construction of programs that can produce encrypted results without
ever needing to decrypt its inputs, so they can be run by an untrusted party without revealing any information. This would in theory fit perfectly for the Smart-contracts deployed in the Blockchain.

For the moment, Fully Homographic Encryption remains more of a theoretical construct, as it is very costly in terms of computation and thus cannot be used in practice. Additively homomorphic encryption is less computationally intensive and thus can be applied in practice. One cryptocurrency, Monero, which is derived from the Bitcoin, uses this cryptographic method in its algorithm.

**Zero-Knowledge proofs.** One way in which Blockchain information can be secured is through Zero-Knowledge protocols. These protocols are defined as proofs that convey no additional knowledge other than the correctness of the proposition in question. In other words, the challenger verifies that a secret piece of information is truthful, without gaining insight on the actual secret. There are several implementations of Zero-Knowledge protocols over the Blockchain as zk-SNARK (zero knowledge Succinct Non-Interactive Argument of Knowledge). The Non-interactive part implies that there is no necessity of an interaction between prover and verifier.

<table>
<thead>
<tr>
<th>zk-SNARK protocol</th>
<th>Zerocoin (43)</th>
<th>Zerocash (44)</th>
<th>Zcash (45)</th>
<th>ZoE (46)</th>
<th>Project Alchemy (47)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Year Proposed</td>
<td>2013</td>
<td>2014</td>
<td>2013</td>
<td>2014</td>
<td>2013</td>
</tr>
<tr>
<td>Hides origin</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Hides recipient</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Hides value</td>
<td>no</td>
<td>no</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>Blockchain</td>
<td>Bitcoin</td>
<td>Zerocash</td>
<td>Zcash</td>
<td>Ethereum</td>
<td>Ethereum</td>
</tr>
</tbody>
</table>

*Figure 7: Blockchain technics*

The drawback as in case of most of the cryptographic techniques is scalability. Although verification of the signature is computationally efficient, the proofs for the moment take one minute or more to be generated.

**Ring Signatures.** Another protocol that relies heavily on Non-Interactive Zero Knowledge proofs are unique ring signatures. They were introduced by Rivest et al. in 2001. Ring signatures protocol allows one entity to sign a transaction with a key from a set of keys, without revealing which key in the set actually signed the transaction. The transaction is endorsed by someone in the particular group of people. For creating the group, there is no need to have a group manager. Ring signatures work on the principle that the ring can be completed if the one using the signature has the private key corresponding to one of the public keys in the ring. This mechanism can also be used in the case where we want to grant access to a member of a group to a particular information without explicitly identifying the particular member. An example of ring signatures usage is a system where ring signatures are used to ensure the privacy of a transaction by hiding
which specific coins are used in the transaction. Ring Signature Mixing Schemes (RSMSs) allow different sets of Blockchain users to generate groups and signatures on the fly, without requiring any additional trust, at the cost of little added computational time.

An upgrade is the linkable ring signature. The main difference is that a user that signs multiple messages, even if he stays anonymous, can be identified by a tag that links together the signatures. A second attempt to use the same private key can easily be identified by third-parties. The tags can be exploited in use cases where the user has a restricted number of access to a particular information or action. Such a case can be an e-voting scheme, where an entity is only allowed to vote a limited number of times, or the surcharge access to a document. A k-times anonymous authentication (k-TAA) scheme as proposed Teranishi et al. can be put into place.

One drawback of ring signatures is that all participants inside a ring should be honest or incentivised to behave honestly. An example of malicious behaviour is when a user or a group of users reveal their own private key, enabling the inference of the rest of the keys in the ring. A possible workaround could be the use of blind signatures.

**INTEROPERABILITY**

The Blockchain technology can be used in many areas for many services. Each application will have its own requirements, leading to different Blockchain choices and implementations. Therefore, we can easily envision a world where there won’t be a unique Blockchain, but most probably where several Blockchains will coexist and will need to interoperate.

There are 3 known techniques for interoperability:

- Centralized or multisig notary schemes
- Sidechains/relays
- Hash-locking

We see currently some implementations from Blockstream, Cosmos, Polkadot and others.
3/ CURRENT USE CASES, INITIATIVES AND APPLICATIONS

In this chapter, we illustrate several current ongoing applications and services using Blockchain in different domains and beyond the financial sector. These examples mostly highlight the potential of the technology. There are many similar other projects in different stages and on same or additional domains.

SMART GRID AND SMART ENERGY

Energy Web Foundation EWF
The EWF goal is to identify and stimulate the deployment of the most promising Blockchain use cases in the electricity sector. It concerns energy exchanges among small producers (e.g. solar energy), information exchanges between large power generators and independent system operators, regulatory compliance and certifications of renewable energy credits. The Blockchain can automate these tasks by logging the needed information in a secure manner and also embedding an exchange token that is managed by the Blockchain.

The approach of the EWF is to use an Ethereum Blockchain version that is run by a consortium of stakeholders (e.g. producers) and with a dedicated value token (e.g. kwh). Since payment is embedded in the trading process (with the value token) all exchanges can be automated with smart-contracts without the need of a parallel settlement procedures which involve banks or payment processors. The traded token can then be exchanged on token exchange systems (e.g. like bitcoin).

IDENTITY MANAGEMENT AND IOT

UPORT
There are many problems with the current state of identity systems. Digital identity is fragmented and is delivering poor user experience necessitating repetitive registrations and logins with usernames and passwords. The centralized servers of identity providers like Google and Facebook are honeypots of data and they’re economically valuable for hackers to attempt to crack. The upcoming reliance on billions of internet-of-things devices makes it untenable to have all those devices controlled by a centralized identity provider since a breach of this provider would prove catastrophic to not only digital but also physical infrastructure.

Using Blockchains & public/private key cryptography push ownership of identity away from centralized services and to the edges - to individuals - so that the identities themselves are in control. This is commonly referred to as self-sovereign identity. This approach decentralizes data and computation and makes attacks less economically valuable to hackers because it would require a lot of effort to hack so many individual identities one-by-one.
Deploying PKI system proved to be very complex and difficult, especially by managing interconnection between different Certification Authorities (CA). Interestingly the Blockchain can itself help make public-key cryptography more usable and secure by acting as a decentralized public key infrastructure (PKI). The Blockchain can be viewed as a decentralized certificate authority that can maintain the mapping of identities to public keys. Smart-contracts can furthermore add sophisticated logic that helps with key revocation and recovery, lessening the key management burden for the end user.

uPort aims to provide a solution to identity management on top of the Ethereum public Blockchain. It illustrates one approach that is based on self-registration and associated assertions from others who may prove and support one’s identity. These associations, or reputation network, also enables to change public key pairs associated to an identity in case of key lose or key renewal.

SECUREKEY

SecureKey Technologies and a Canadian non-profit coalition have received a grant from a research center funded by the U.S. Department of Homeland Security to help build a digital identity network.

The company uses Blockchain to create a «triple blind» privacy protocol that allows individuals to easily connect to partnering online services using an existing, trusted login credential and at same time limiting the actual amount of data being transmitted for privacy.

The «triple blind» mechanism means a consumer can use their bank credentials to log in, for example, and access their destination service but the bank cannot see where the data is going and the recipient cannot see which bank is used or any bank account information.

SUPPLY CHAIN MANAGEMENT

CHRONICLED & LEDGER

Cold chain monitoring with tamperproof sensor sealing
The transport of certain products (e.g. medicines) is done today via refrigerated transport to ensure that the temperature stays in a safe area. However, from a practical point of view, it is possible to transport these packages in a non-refrigerated environment in certain regions and at certain times (e.g. some countries during winter). The economic gain can be substantial.

In this case it is necessary to be able to ensure that the cold chain is not broken. The use of embedded sealed & secure sensors (i.e. oracles) makes it possible to attest the temperature level over the whole duration of the transport. Each package is associated with a «smart-contract» that binds the buyer and the seller, and whose unbundling is linked to the onboard oracle: upon receipt, the data is unloaded and submitted to the «smart-contract» which will accept or refuse receipt.
The use of a Blockchain allows the automation of the control, payment and insurance processes. It also assures that all data that is transmitted end-to-end cannot be forged. The embedded sealed & secure sensors ensures this at the edges while the Blockchain ensures it when data arrives and integrated in it.

**LEDGER**

**Containers follow-up**
The logistics management of containers is now largely done through paper («bill of lading»), which serves as a real proof of delivery and for the payment of goods. All commodity trading is done through bank financing, which requires the guarantee or sequestration of the transported goods. The supplier will only be paid when the container has been cleared by the port authority and the payment being triggered in practice by receipt of the «bill of lading».

Each element of the chain (carriers, port authority, banks, insurance companies etc.) has a proprietary IT with very little interoperability and the «APIs» are ultimately via the physical flow of “bills of lading” which are retransmitted manually from one IT to another.

This opens the door to many difficulties, both in terms of human error and falsification, with hundreds of millions of euros in permanent risk.

The use of a Blockchain makes it easier to create a bridge between all the actors and to digitize the bill of lading by replacing it with a smart-contract. The interface with the physical world is via oracles (sealed & secure sensors) and personal security devices. Thus, the various states of the «smart-contract» are operated directly by the container when it is unloaded, inspected, cleared or delivered. The Blockchain also provides total traceability of the process and defines the responsibilities of each entity during the different stages.

**GOVERNMENT SERVICES**

**HEALTHCARE**

Guardtime is an Estonian startup that uses technology similar to that underpinning bitcoin to secure public and private data. It has signed a deal with the Estonian government to secure all the country’s 1 million health records with its technology.

Guardtime uses Blockchain technology to verify data and prove that it’s trustworthy. Guardtime technology is distinct from Bitcoin and in fact predates the original white paper on bitcoin… Guardtime technology does not use a network of miners with a consensus algorithm because it’s completely private and is backed by the Estonian government. Yet it guarantees that every update to healthcare records and every access to these records is registered in the Blockchain. This makes it impossible for the government or doctors or anyone else to hide any access or
change to healthcare records. The top hashes that guarantee the integrity of the Blockchain are published continuously in a public journal in order to guarantee that any attempt to change the content of the Blockchain is immediately detected.

Estonia has one of the most digitally advanced societies in the world and helped to incubate Guardtime’s technology. Estonian citizens carry a smartcard that stores their data and gives them access to over 1,000 government services. Guardtime also secures the identity of each citizen by securing this Identity Card with a Blockchain at the backend. Guardtime has contracts with Ericsson, the defense giant Lockheed Martin, and the US military.

**FORMALIZED AND SECURE CADASTERS**

In many developing countries the land is not correctly registered in an official database. Some people often do not even have a real address. In Africa, for example, 90% of rural areas are not registered in a cadaster. A lack of land tenure security leads to fraud and also hampers the investments necessary to the development of agricultural productivity. It is also an obstacle for stimulating borrowing to individuals for construction and other investments.

For example, in Ghana, the Start up Bitland proposes to register land deeds on a Blockchain. In 2015, the government of Honduras has listed its entire territory on a Blockchain thanks to the Epigraph organization to prevent the richest persons from granting themselves properties that they do not own.

**GUARANTEEING DIGITAL IDENTITIES**

Governments can play a crucial role by giving their citizens digital identities, thereby enhancing peripheral trust in all peer-to-peer transactions. A digital identity would be data with provable assertions from a government authority which can then be easily verified (e.g. digital signature).

Such data would not necessarily need to be stored on a Blockchain but only the hashes of such data. Citizens could create public/private-key combinations to release selected personal data to specific recipients. Identity cards with secure token would store the needed keys and interface directly with the Blockchain. Privacy can be handled this way and for example a young person could prove that he or she is old enough to purchase liquor without revealing other irrelevant information.

Over time, legally binding digital signatures, passports, driving licenses, security passes, certificates, log-ins, ownership documentation, voter registration, and various other legal information could be built on that foundation.
MUSIC INDUSTRY

Digital rights management is one of the major issues that the music industry is tackling today. It’s sometimes difficult to clearly trace and implement which performers, songwriters, producers and publishers own the rights to songs and recordings and how royalties should be split between them.

Blockchain is well positioned to bring a change in this domain. For example, the ledger can store a cryptographic hash representing the digital content of new songs including lyrics, musical composition, cover art and other relevant information.

The Blockchain can then automate the way that composers and content creators are being compensated. In a digital world, where music is being downloaded or streamed, royalties are still managed by inefficient and sometimes opaque chain of collection societies. As a reliable peer-to-peer platform, Blockchains establish a direct relationship between artists and consumers, making sure artists are instantly paid for their content and receive near-full payment instead of a small fraction.

This concept is being tested and explored by several startups and nonprofit organizations. One key player is UjoMusic, based on the Ethereum Blockchain, that enables artists to manage their identities, music, and licensing on their own terms.

Mycelia, is another Blockchain-based offering that enables a fair-trade music business that gives artists more control over their songs and associated data.

Other actors are PledgeMusic, BitTunes and PeerTracks, each introducing a complementary approach with a different business model.

Blockchain music solutions will still have to overcome a lot of challenges, including the transfer of old licenses and ownership information to the new platforms and also how to engage the current actors in a new distribution model.

PRICE STABLE TOKEN SYSTEMS

DIGITAL FIAT CURRENCY

At least a half-dozen central banks are considering minting Fiat currency on a Blockchain. There are rumors that the Bank of England would mint “bit£” as digital currency. Unlike bitcoin, bit£ would have a fixed value and be backed by the full faith and credit of the government. The central bank would purchase government securities with bit£ through an interbank-permissioned Blockchain. Commercial banks could then use the bit£ to settle interbank obligations and over time it could be extended to all citizens. Bit£ may then displace physical cash and much of the traditional payments settlement function of commercial banks.
Other projects try to provide Fiat currencies trackers on a Blockchain independently of central banks. This can be done by using smart-contracts where investors place contracts on future value of a currency much the same way it is done with commodities today.

**CROWD FUNDING**

WeiFund is a crowdfunding portal built on Ethereum. Along with the portal interface, WeiFund offers a Standard Campaign sample contracts that allow anyone to rapidly assemble a crowd fund offering. Alternatively, campaigns are allowed to roll their own smart-contract code.

WeiFund enables the implementation of various types of crowdfunding, depending on product, service or proposed remuneration. A crowdfunding campaign can embed a remuneration token that can eventually be traded on exchange portals. Being on the Ethereum Blockchain the fund raising is done with ether and can then be converted to the project remuneration or participation token. The smart-contracts embed the functions for funds reimbursement in case of fund raising failure (not enough funds raised) or the level and type of participation in case of fund raising success.

WeiFund campaign rollout readiness provides a template for campaign release best practices. A campaign readiness means readiness assessment as a measure of security assessment with the goal of creating an environment for secure contract system rollouts.

**DECENTRALIZED ORGANISATIONS**

Backfeed ([http://backfeed.cc](http://backfeed.cc)) provides the infrastructure for decentralized cooperation and without the rigidities of hierarchical structures. Backfeed’s infrastructure comprises decentralized management tools, equity-sharing schemes, crowdsourcing mechanisms, and instruments for the collaborative evaluation and management of content. Its goal is to enable the bootstrapping of decentralized organizations on top of the Blockchain as easily as one would deploy a website today…

The Backfeed protocol rewards individual contributors through the distribution of tokens and the reallocation of individual influence or reputation within a given community, based on the perceived value of their contributions to that community.

The specific rewards granted to contributors and their corresponding influence in the community are calculated automatically by the workings of the protocol (Proof of Value) and do not require any kind of central administration. The score comprises several elements including reputation, Value distribution and Accommodating Diversity.

This approach goes in line with the philosophical value perceived by the Blockchain… If Bitcoin was aiming to avoid the centralized control of central banks and governments on money issuing and its associated value then Backfeed tries to apply it on the organization hierarchy itself by inventing a new type of distributed enterprise. Time will tell if this approach can be effective or not…
4/ PERSPECTIVE FOR BLOCKCHAIN

In January 2017, Bitcoin Magazine\textsuperscript{21} published that: “\textit{Many experts predict that blockchain technology will be the most disruptive technology since the creation of the internet. Given the amount of industries that face disruption by the distributed ledger technology, it is starting to look like this prediction will come to fruition}”. It is interesting to highlight that the financial industry is already testing and implementing blockchain technology while different other sectors are facing disruption as well. Bitcoin magazine has identified seven keys sectors for 2017.

This amazing disruption shows that the technology is mature enough to envision its use in many domains, some of them unexplored as of today. This chapter explores the different issues that need to be addressed to have an exploitable technology implementation, legal aspects and standardization.

For the implementations, it is important to know where we stand, to distinguish the mature parts from the ones requiring further work in the software development life cycle.

Legal aspects, will take into account the foreseeable profound transformation of society and human relationships. Will they be followed by economic actors who, step by step, build solutions to the problems faced by the previous generation? Will encryption and decentralization impact the role of digital trusted third parties? What will be the dominant players of this new technology? Will a new legal realm be build to supervise, manage socially these technologies?

The standardisation challenge is to help organizations adopt the blockchain and foster the development of a community of economic actors in the Blockchain area able to consolidate the confidence in the technical and business designs, as well as the corresponding legal or regulatory frameworks.

\textbf{Implementation challenges}

Bitcoin is the perfect example of a successful implementation of Blockchain technology and has motivated different kinds of actors to analyze this technology and to understand how to use it. Innovation, driven by this technology, was developed by imaging new use cases, starting from cryptocurrency (Bitcoins) with their transactions to various business domains like health or transportation.

In 2016\textsuperscript{22}, in order to foster innovation for the Blockchain, Gartner has published a list of featured use cases that leverage the Blockchain technology. This list contains two tabs, the first one, “Industry-Led Developments”, lists the use cases which have a clearly identified end-user organization. The second one, “Startup-Led Developments”, lists different use cases which are

\textsuperscript{22} https://www.gartner.com/doc/3267717/toolkit-overview-Blockchain-use-cases.
still in testing phases and do not have a clear end-user organization involved. This User Centric driven approach is very interesting for people aiming to innovate in various vertical systems.

This complete list of use cases and all associated available implementations demonstrates that Blockchain has reached a good maturity level. It is actually possible to define a Blockchain-based system, to design it and to implement it. In this chapter, we discuss Blockchain-based architectures, their maturity, and we identify the main limitations that make it difficult to reach enough maturity for the future innovative systems.

LIMITATIONS & MAIN CHALLENGES

BUSINESS LIMITATIONS

Over the last 3 years, multiple initiatives in the field of the Blockchain were conducted to identify new innovation capabilities and that span multiple business domains. Considering all the work performed Blockchain architectures have already reached a first level of maturity. Recent publications, based on this status, have proposed an architecture taxonomy for Blockchain-based systems and a design process.

Even if the design principle of a Blockchain-based system are clear now, the main current limitations are related to the software and hardware implementations and the expected business model.

TECHNOLOGY PROVIDERS

In the previous section, a design process for a Blockchain-based system was presented highlighting the main aspects of the Blockchain. This approach is mature enough but should be followed by guidelines for its implementation. Currently, different hardware and software implementations exist, but several key aspects are not fully addressed. These aspects are detailed in this section.

Source code access for the different components

One of the best ways to establish trust between the different Blockchain actors is to provide a direct access to the source code. It allows to check the quality, the conformity and the lack of vulnerability. It is a sign of confidence even if, in reality, it is very rare that someone verifies the code of the components supplied. In the case of a public Blockchain, this need often leads to release the different components with an open source license.

Components certification

To release the components under an open source license is not sufficient to provide enough guarantees regarding their implementation, their security and to trust the whole Blockchain-based system. For example, a company, aiming to use Ethereum for developing a business solution,

---

This work will focus on providing common definition of the main terms (e.g. what is a Blockchain from a technical standpoint? from a legal perspective?)
needs assurances regarding Ethereum implementations. It needs to be sure that the Blockchain is trustworthy and that no one is able to modify the implementations for his interest. Certification is a good option and could offer this kind of assurance.

Confidentiality management

Bitcoin has opened the door of Blockchain-based system guaranteeing anonymity and integrity by publishing all transactions in public Blockchains. All new systems aiming to guarantee different security attributes need other Blockchain implementations restricted to authorized users (Permissioned Blockchain) and managing data confidentiality (for example Enigma\textsuperscript{24} combined with multi-party computation).

Sustainability of platforms

Every day, new platforms are proposed and then suddenly disappear. These platforms, managed by different groups having very different motivations (startup, academic, professional associations for example), never offer sufficient guarantees for their sustainability. To answer this problem, recently, software editors groups joined to support a Blockchain platform (Blockchain as a service in Azure\textsuperscript{25}). This kind of support gives some reassurance on the Blockchain platform sustainability but other aspects need to be addressed (especially for life cycle management) to provide assurance regarding security because these groups are acting as a trusted third party.

Monitoring

How to monitor miners’ activity and to trust the results? How to be sure that no one control more than 2/3 of the nodes? This information is mainly delivered now by the Blockchain platform provider but without strong assurances.

These 5 aspects are not specifically limitations but open points where the future mature implementations should provide clear answers.

BUSINESS MODELS OR ECONOMIC CONSTRAINTS

Today, thanks to the various implementations and the already running platforms, different services can be provided to end users without important investments. It comes particularly true in the case of public Blockchain where a company could deliver a service paid by the end users, including the platform funding. For example, this company could only develop and deliver a smart-contract, using Ethereum platform. The end user would pay the service usage including a contribution for Ethereum platform. In this case, the revenue model is simplified but the cost model is more complex and must include the platform cost.

In the case where a group of business actors would like to set up a restricted Blockchain platform, for example with a private Blockchain, the question about the infrastructure to deploy and the cost model is crucial. What kind of incentives would be relevant? Proof of work consensus wouldn’t be

\textsuperscript{24} http://www.enigma.co/

\textsuperscript{25} https://azure.microsoft.com/fr-fr/solutions/Blockchain/
applicable here due to large amount of work to be performed. This consensus is relevant in the case where miners are paid for mining, as it gives a good way to select the miner receiving the money. In the case of private Blockchain, this kind of consensus is not well-adapted because the goal is only to fund the infrastructure providing the service, not more. In this case, the Blockchain-based system has only to guarantee that there are enough miners and that no miner has more 2/3 of the node. When a group of actors want to deploy a private Blockchain-based system, they need that all actors contribute to the mining, in this context, the proof-of-stake consensus is very promising.

Nevertheless, the funding remains a difficulty for these different cases especially when the Blockchain-based systems are not handling financial elements (for instance private data, sensitive data, …).

FUTURE INNOVATION PATHWAYS

In the Gartner publication26, the approach, with 2 use case lists, is very interesting. The first one lists the use case supported by the industrial companies and they can be considered as the current challenges validated for their business interests. The second one gives the use cases promoted by different startups. These use cases are very promising and could address the near future challenges. Considering only the main domains (illustrated by at least 6 use cases in industrial list and 10 use cases in startup list), the difference between the 2 lists are that 2 domains almost disappear (Banking and Government). However, the domains Media and Legal, are emerging in the use cases promoted by the startups.

The main domains mentioned in Gartner’s lists are still very influenced by banking transactions (especially payment transactions) or by the financial assets handling. They are always very close to the Bitcoin cryptocurrency and its implementation. The use of smart-contract is also highlighted very often. Another consolidated axe is the legal axe with different usage for Government (voting system for instance) or for Media (management of copyrights management for example). The current challenges aligned with this trend (described in section 3) are:

– Confidentiality management: The legal approaches run often into problems of privacy and accountability. The existing R&D activities developing permissioned Blockchain solutions (without anonymity) and providing different way to manage the confidentiality (Enigma for example) are totally in this scope.

– Sustainability of platforms: To guarantee the sustainability of BC platform, the initiative of Azur27 is a first solution (Blockchain as a service) in that way.

– Business models or economic constraints: The Proof of stake consensus is being developed in different implementation.

26 https://www.gartner.com/doc/3267717/toolkit-overview-Blockchain-use-cases
27 https://azure.microsoft.com/fr-fr/solutions/Blockchain/
TECHNICAL LIMITATIONS

LIMITATIONS OF CURRENT BLOCKCHAIN TECHNOLOGIES

Despite its first application in 2014 with Bitcoins (Nakamoto, 2008), the Blockchain industry is still in its early stages and presents both internal and external open challenges or limitations which span from technical issues, government regulations and mainstream adoption. Erreur ! Source du renvoi introuvable. sketches the actual state of research on the Blockchain technology (Jesse, Deokyoon, Sujin, Sooyong, & Kari, 2016) and shows how some of the limitations have not yet been analyzed from the research community.

![Figure 8: Bitcoin transactions per second](image)

THROUGHPUT

The first limitation regards the rate at which Blockchain-based applications can process transactions. In the Bitcoin Blockchain, this rate reached 2.75 transaction per second (for short, tps) in November 2016, with a theoretical current maximum of 7 tps. Comparison metrics in other transaction processing networks are typical 2,000 with peaks of 10,000 tps. It is then clear that in order to compete with such well-established processing networks the Blockchain throughput has to be increased while also taking into account collateral side effects such as storage capabilities and computational power.

LATENCY

Together with throughput, the latency in blocks validation is another big challenge in the Blockchain technology. This limit is not due to implementation issues but rather to security requirements. Taking as a toy example the Bitcoin network, it take roughly 10 minutes to validate a block and to write it within the next block. Furthermore, in order to be trusted by the community (such as by online vendors) transactions are required to be 6 blocks old, which makes the acceptance

---

delay 1 hour long. This high latency is required to outweigh the cost of the double spending attack, which is the result of successful accepting the same transaction more than once (Karame, Androulaki, & Capkun, 2012). Again, as the comparison metric for payment transactions, other payment platforms usually take seconds at most.

Figure 9: Bitcoin Blockchain size

SIZE AND BANDWIDTH

In November 2016 the bitcoin Blockchain measured roughly 92GB (with 2,075 transactions per block (see Figure 9). With latency and throughput limitation solved, its size could grow 214PB each year (if assumed to be as fast as other traditional payment platforms). Furthermore, this prediction is based on the actual size of Bitcoin blocks (1MB). If the Blockchain-based application needs to control more data (as for smart-contracts or any other digital assets written within the Blockchain), this growth can be even faster. In the Bitcoin community, this problem is known as «bloat» and is usually solved by reducing the size of the Blockchain. However, whilst this is a valid short term solution, it will not scale to huge networks such as for application targeting the Internet of Things (for short, IoT). In this case, the long-term solution is rather to design a faster and more efficient way to manage large Blockchains.

Figure 10: transactions per block
SECURITY

The Blockchain technology is usually seen as an inherently secure technology. However, there is no formal proof that the three classical security properties (confidentiality, integrity, and availability---CIA) are enforced by Blockchain technologies. The Blockchain technology, in its bitcoin version, offers great availability and confidentiality features but a fragile integrity. In fact, whilst transactions are immutable once committed to the Blockchain (not taking into account the double-spending attack), the veracity of each transaction within the blocks only rests on who controls the private keys of those accounts; keys being used to sign transactions. This limitation is not evident now as clients are installed within personal devices such as smart-phones or laptops (thus being supervised for the whole time) but in the IoT, un-managed and un-supervised devices could be running on top of Blockchain technology thus being exposed to key theft or information stealing attacks.

USABILITY

The API for working with Bitcoind (the full node of all code) is far less user-friendly than the current standards of other easy-to-use modern APIs, such as widely used REST APIs. The usability open challenge in Blockchains was first defined by Swan in his book (M., 2015). Even though usability in Blockchain mainly refers to design APIs which can allow easier and seamless interactions with this technology, another big usability issue is the analysis of the information contained within the Blockchain. In fact, it is usually hard to browse the blocks to check what is inside and people usually rely on online services for this task. It is therefore important to develop support tools for the user which have their devices running on top of the Blockchain and which want to analyze the activity of their devices and the connections with other devices over time. For the Bitcoin network, this is already happening with solutions such as BitConeView (Di Battista, et al., 2015), which helps in tracking the coin flows within the Blockchain, and BitIodine (Spagnuolo, Maggi, & Zanero, 2014) which parses different flows belonging to different addresses from the same user and allows complex transaction analysis. Solutions for general purpose Blockchains which differ from the ones implemented for Bitcoin are still missing.

INFRASTRUCTURE

The Blockchain technology relies on the broadcast model which is well known to be unreliable in real networks, and this also applies to the Blockchain (Decker & Wattenhofer, Information propagation in the Bitcoin network, 2013). This means that in the real world, peers do not send their messages directly to the network but rather to some special devices acting as gateways which represents a bridge to the outside world. As a result, the global
Blockchain network (i.e. the global network participating in an application such as the global Bitcoin network) should not be seen as a single network but rather as a fragmented network composed by many sub networks.

These networks are much smaller in size, which makes them less resilient to the 51% attack while making easier for an attacker to eclipse (Kartik, Srijan, Andrew, & Elaine, 2016) one or more peers.

**VERSIONING**

If Blockchain-based applications are split for administrative or versioning purposes, there is no easy way to merge or cross-transact on forked chains. This is mainly due to the fact that current applications use one single Blockchain and get rid of forks generated over time. Other directions such as the ones proposed in Multichain (Gareth & Guy, 2016) or Blockstream (Back, et al., 2014) are trying to design a Blockchain technology which relies on different chains. However, their solution has to be taken as a whole and merges among different Blockchain are not yet supported.

*Figure 11: Classification of the actual research on the Blockchain technology listing the actual number of published works on security related topics [2]*
FUTURE CHALLENGES AND PERSPECTIVES

It is surprising to find that the main verticals involved in the Gartner’s use case list constitute a short list. The main ones (healthcare, banking, transportation, administration, Energy) are hardly mentioned and often in a use case including payment or financial assets handling.

If we compare the dynamism of the Blockchain ecosystems with the growth of IoT, we are surprised to see so little interaction between them. The IoT-based systems, distributed by nature, should take advantages of BC for sharing sensitive and critical information. The main brake we can imagine is that, till today, the most part of running systems are too isolated (under the authority of one single organization) without interactions between them. The future of the systems will be with the opening and the interconnection of the systems. 5G landscape and IoT growth are the first step to build new systems based on existing systems devoted to their domains. This opening raise new security challenges and the main one will be how to share critical and sensitive data without a central authority. Today, a few initiatives exist but they remain under-developed.

To summarize, the future challenges to develop Blockchain applications will be, regarding the ones identified in section 3:

– To have a complete, certified, sustainable solution and being able to be deployed in private area.
– To guarantee the collaborative and independent verification operated by the miners in private (or restricted) Blockchain with different incentive not only financial ones.
– To demonstrate new innovation pathways, not addressing an existing need but opening the door to new application domains and functionalities.

REGULATORY, LEGAL, GOVERNANCE AND ECONOMY CHALLENGES

After 20 years of rapid and unrestrained development, Internet has succeed in reshaping social connections, transforming communication between humans. Economic breakups in the newspapers, television or advertising sectors are now visible. If this phenomenon had been, perhaps, anticipated by some gurus since the beginning of the launch of the TCP/IP protocol, it was especially built step by step by the actors themselves throughout mix of technical innovations, new uses and disruptive business models: the main business model, theorized by Jean Tirole, is built around platforms with double faces. This development is organized mainly around the dissemination, the consultation of textual, audio or visual data and interpersonal exchanges (mails). Intermediation platforms, quickly in a monopolistic position, are built around the concept of trusted third party to overcome the native defects of basic technical protocols and offer value added services. Currently, spam, fake news, phishing etc… demonstrate the fragility of the underlying technical system.
The proposal of a Bitcoin protocol in 2008 presents a judicious blend of technological blocks based on cryptography research (Diffie and Hellman, Turing price 2015) and distributed computing (Butler Lampson Turing price 1992, Leslie Lamport, Turing price 2013). Will it build a rupture in the information technology a few decades later, the evolution of the human interrelationship or between human and complex automated systems? Will the Blockchain format the transactions between economic agents by providing the missing elements of the first wave of innovation of the TCP/IP protocol?

Here, too, visionaries have promised a profound transformation of society and human relationships. Will they be followed by economic actors who, step by step, build solutions to the problems faced by the previous generation? Will encryption and decentralization impact the role of digital trusted third parties? What will be the dominant players of this new technology? Will be build a new legal realm to supervise, manage socially these technologies?

The elements of discussion below focus on the public Blockchain, a paragraph deal quickly with the Blockchain with consortium.

**Blockchain in the society**

Major developments of Information technology since the middle of the 20th century resulted in a societal transformation: the architecture of information systems “impresses” its mark on the surrounding social organization. The first steps have remained confined to businesses, but the emergence in 1980 of personal computers has integrated the private and social life in this transformation. The Blockchain by its potential impact on transactions with proven and certified values, will necessarily impact the relationships of citizens with the State and its general interest services and/or with companies.

For example, the Ukrainian demonstrators waved posters with a bitcoin address to raise funds from viewers with total anonymity; indeed the example is anecdotic, but it demonstrates the impact of new technologies like the Blockchain on the social life.

The first impacts will be visible in areas where either organizer of the service or the guarantor of benefits or the trust service provider doesn’t properly fulfills its role: high transactions costs, heavy and binding interfaces, lack of transparency in its operating rules, or conversely, an over-quality compared to the real needs. This impact will be quickly visible in consortia of professional users (some sectors such as banking and insurance are already accustomed to working together to collectively ensure consistent and interoperable services); in a second phase less structured economic sectors will benefit from the impacts of Blockchain technology. Blockchain technology is needed to question the silos of data, the limits of the company information system, imposes an opening on global value chains and the competitive business environment.
The public sector will be largely affected by this technology as the direct or ultimate guarantor of the citizen identities, the important assets, of the organization of the interactions between all stakeholders of the society. Politicians began to study technology to understand its social, economic, legal and regulatory dimension (parliamentary seminars in France in 2016, European Parliament report). Overall, the following important strengths and weaknesses are identified:

- **Strengths**: reducing banking costs, banking inclusion, resilience of systems, respect for private life, micropayments, transparency of information areas are in the European parliamentary report.
- **The current weaknesses**: lack of governance, the volatility of the crypto currencies, legal uncertainty, lack of formal guarantees on the functioning of the system.

A consensus emerges in European and North American countries for a period of observation with limited regulation (for example law No. 2016-1691 from December 9, 2016 relating to transparency, the fight against corruption and the modernization of economic life called the ‘Law Sapin 2’). In most cases, the political power provides a simple formulation of caution to the actors to let technology evolve and mature before, perhaps, then to formulate new rules and/or adapt existing regulations.

Then, new features can appear based on the strengths of the Blockchain technology (transparency, auditability, non-repudiation, security, resilience) as for example the electronic votes that could evolve towards more complexity of choices today limited by the physical support for the choices of the citizen.

The sharp decline in transaction costs (see following paragraph) will asks the limits of the companies as they have been studied by Olivier Williamson and Ronald Coase, in reviewing the arbitration between the employment relationships and contractual commercial relationships (customer or supplier).

However, transactions automation promised by the Blockchains will be limited by the lack of empathy and awareness that are essential to life in society; algorithmic consensus technology does not solve all conflicts between people, the State, remaining the only legitimate guarantor of coordinating the actors of society and of the arbitration of conflicts.

Finally, will the idyllic schema described by the visionaries of the Blockchain be actually implemented such as drawn? TCP/IP, 20 years ago, promised to transform the citizen into a producer of its own information. This is now formally true, but the search tools for relevant information on the web have become a new form of domination by some platforms. Will the players of the ecosystem Blockchain (developers, minor) become the dominant players of the future market global transactions?

**Legal aspects of a Blockchain**

If Blockchain technology is too recent to find clear references in law, we may nevertheless present a few rules that will evolve into new regulations and case law developments.
First, we find of course the traditional characteristics of the legal issues in connection with automated digital treatments:

- Identification of the actors and the link between the physical actor and its identification in the digital universe. Blockchain brings a quite widespread use of asymmetric encryption based on a public key and private key that, in a first approach, allows a clear identification of the digital actor unambiguously, but it does not link this digital identity with his alter ego physical representative: physical, economic or administrative person. This lack of a link has not been a problem for the development of the Internet but appears now crucial in the realm of the transactions. The resolution of the problems of identification of the actors of the transactions by implementing appropriate services with certainly the implementation of «oracles» of digital actors, new form of trusted third party identification provider, is essential for the development of the new ecosystem.

- The continuous streaming of the content of the register between the stakeholders, in general, stabilizes the common basis of information, shortens discussions about these factual elements, reduces the debates and disputes between stakeholders on the individual analysis of these data.

- Digital items in an appropriate Blockchain can provide evidence (time stamp of a digital content, signature and notarization of a contract, etc.). However, this evidence must be supported by a complementary technical expertise because a judge is not taking as evidence the young technology. Moreover, Blockchain technologies do not support the same strength for evidence (the settings conditions of implementation may largely influence the strength of the evidence). Currently, no legal provision raises records in a Blockchain to a level of simplified recognition or de facto and, similarly, no standard or equivalent document allows characterizing the strength of a record in a Blockchain.

In addition, highly distributed computing and the proposal of ‘smart-contract’ creates new legal questions:

- The strong distribution of treatment brings both a strength and a resilience in the chain increasing its legal appeal but, conversely, a problem of territoriality and location of the treatment, the data and thus, of the legality (if the network is cross-border) and identification of responsibilities because of the extent of the treatment network not included in a single entity legally responsible for its governance and bearer of its purpose. This lack of overall responsibility contradicts the current trend of the European laws mandating a clear identification of the trust service providers (see eIDAS Regulation) and of their responsibilities.

- Several initiators of Blockchain launched the notion of ‘smart-contract’. A more accurate definition of this concept would be an «agent of autonomous processing inside a Blockchain, running specific software activated by messages or other transactions, and producing output by transactional exchanges with accounts or other agents of this Blockchain». These applications are perhaps still marginal today, but they will be able to multiply with the introduction of connected objects in everyday life that can be managed by Blockchain-based tools. They bring with them an improvement of process automation and therefore reduce costs while improving quality. However, their legal status remains unclear due to the distributed nature of the computation, the lack of assignment of responsibility to the author of the software, and the interactions between multiple transactions.
Furthermore, Blockchain technologies must pay attention at the following points:

– Pseudonymisation and encryption of the identities, that are metadata available for all, are likely to be susceptible to re-identification as are all traces of activity on a digital network.

– The irreversibility of personally identifiable records must be analyzed precisely to not contravene the new law to forgetfulness of personal information.

– Acceptance of rules of use of a Blockchain is implicit as well as their evolution according to exchanges between miners, developers without always taking into account users of such systems.

– Many sectors with specific regulations organizing the relations between the companies, operators and individuals (housing, banking, insurance, e-commerce, etc.) will have to change their regulations when stable Blockchain technologies are implemented.

– The use of ‘coins’ associated with some Blockchain is considered as a currency and so must be administered as such on accounting and tax realms.

– Large generic regulations (anti money laundering, anti-fraud, anti-terrorism) cannot be overridden by this new technology even if in this case, the lack of overall responsible actors pushes these legal responsibilities on the players positioned at the Blockchains boundaries.

The irruption of a transactional computing that can «write» the laws in a formal language with self-processing opens potential of rigor and impartiality. That annoys, however, the law experts. They want to keep a certain vagueness and maintain the freedom for actors to override the established rules because of special characteristics not initially planned, allowing the improvement of these rules by successive advances.

But without waiting for a specific status of the transactions managed by a Blockchain, most of the States have ruled on the tax system of crypto-currencies: the France stated in 2014 the tax status of capital gains by using encrypted currencies and their valuation in the wealth tax or inheritance. The European Court of justice ruled on the tax nature applicable for encrypted currency, confirming its character as an instrument of financial exchange not subject to VAT.

In conclusion, the Blockchain technology brings a concept opposing, in first appearance, a law formalized in computer language for global performance and the national and international legal systems based on the traditional right and legitimate violence of the State (with the sense of Weber 1917). The technical and legal developments may help to restore consistency these two approaches.

Economy of the Blockchains

The economic dimensions of the Blockchain are multiple and evolve quickly:

– ‘Coins’ at the base of the mining becomes sometimes convertible into common fiat values, giving this token monetary value used as a medium of payment, money exchange. The overall capitalization of the crypto currencies is still low compared with the major world currencies, its value is often fluctuating (example Bitcoin) becoming a tool for speculation. It is certain that an increase in these valuations pushes the need of control, with an unpredictable impact on the values of the ‘coins’.
– The ‘coins’ can also remain a simple means of payment by the user, for the miners for their audit work, control of transactions (memory and processor consumption).

– These ‘coins’ have been used as seed funds for a few months (ICO: initial corner offering) to support the entities in charge of the development of software that will be implemented by miners. This new form of financing transforms the usual methods of launch of startups by an innovative tool without (yet) legal framework.

– Automation of the transaction process tends to reduce the unit costs and the marginal costs allowing the multiplication of the transactions associated with frequent use. The arrival of these micropayments will certainly revolutionize markets where the pay-as-you-go unit will become the rule (music, video, software, etc.). Blockchain coupled with connected objects will open new markets, for the management and sharing of data generated by these objects.

– The security of a Blockchain is proportional to its size and the number of miners contributing to its coherence; this property will tend to promote monopolistic or oligarchic positions of major Blockchain attracting uses within the technical limits of the scaling. The first Blockchains may win this run to the biggest chain.

– The risk reduction by automatization, and by simultaneous execution of complex relationships between various stakeholders, will structurally reduce the number of intermediaries and thus their costs; air or maritime logistic may benefit from this approach.

– The revision of business processes between companies: the Blockchain, by creating the need for a transversal approach to the current entrepreneurial structures, allows ‘discovering’ processes between companies that remain based on less productive procedures. This modernization could not occur because of the rivalry between the parties involved or because of negative externalities if one stakeholder invests first to modernize the collective process. The technological neutrality of the Blockchains without leadership of one of the parties facilitates this approach of co-investment with profit sharing.

– The auditability of Blockchain transactions can reduce the workload of the finance division in the companies or among regulators: the transparency of the register allows this continuous and exhaustive audit.

– Software blocks are generally available under an open mode source. This method eliminates the purchase of the software or the payment of licenses fees, but versioning of the multiple Blockchains is currently still very fast, posing a problem of stability of the applications built on top of these software blocks.

A company that provides trust services and transactions must address Blockchain technologies in its markets by looking at what would be easy to disintermediate between the company and its customers. How the business model will change if a Blockchain is introduced and so where should be the new value of the business, how to build new offers (contribution of the micro payment for example) and how to operate this shift to the new value chain (independently or in collaboration with competitors, customers or suppliers of infrastructure of Blockchain).
Governance of the Blockchains

The internet players have built products and services by inventing adapted governance and managed by the stakeholders: the Linux Foundation, the Internet governance with the ICANN, ISOC and IETF organizations, the open source software licenses for example. This work has to be implemented for the Blockchains. For any functional changes, groups of miners, the «core developers» are communities of independent actors associated step by step according to the subjects.

So, understanding the point of view and the strategies of the stakeholders, analyzing the positions of miners, monitoring their numbers and their geographical distribution, understanding the visions of developers are essential to build a Blockchain service, on which we wish to support a business development.

The distribution of the process, by imposing a coherence of the applications of each mining node, is a fundamental difference with free software where it is generally possible to diverge with successive changes and implement its own version stabilized without impact on other users.

Several cases of divergence in vision of the public purposes of the main Blockchain have occurred: forks were detected in July 2016 for Ethereum, in March 2017 for Bitcoin. Every time, two resulting chains emerge with, indeed, very different valuations of the ‘coins’ between the two chains and between the computing power of the mining (and thus between the security of managed transactions).

Beside the large Blockchain public, we note the approach of the Hyperledger consortium, which is organized within the Linux Foundation. This governance based on the rules for Linux helped to attract the big names of IT industry such as IBM to cooperate and build a commercial service on this particular technology of Blockchain.

The stability of chains based on consensus methods different of proof of work algorithms cannot be assessed, due to a lack of maturity. This issue is addressed within the objectives of the Tezos project, which should provide innovative solutions. However we need to understand its implementation to evaluate this new governance.

Special cases of the private or consortium Blockchains

The consortium or private Blockchains avoid the legal difficulty of governance.

In such case, entities work together for the creation of such Blockchain; they agree on the purposes of the consortium and generally write all the details in a conventional contractual relationship to deal with the various points, the responsibilities, the allocation of costs, etc.
The collective approach between several companies operating in the same market should be perfectly mastered to comply with competition laws. The collective work within official bodies of standardization enables the definition of technical protocols over a clear legal framework between competitors.

The profitability of such a project is still based on the same general principles set out in the paragraph above:

– Private chains within a single company look for a reduction in the costs of information system: open source software, distributed resilient architecture implementing rustic technologies, ease use of the cloud with the encryption of information, etc.

– The profitability of a chain for a consortium of several companies will be based mainly on the reduction of inefficiencies of inter-company transactions. Bypassing a centralized, under optimized trust service will result in an improvement in the quality of the interfaces (reduction of delays, reduction of claims). However, new services will seldom be created in this context for reasons of competition among the parties involved.

– However, limits remain due to the difficulty of joint work between actors which also are often competitors. For example, even with encryption, part of the data or metadata remains accessible to all the partners of the Blockchain.

Conclusions

The legal context and the governance are important elements to address in any project using Blockchain technologies. They should be address from the very beginning of prototyping because these elements are more critical for his deployment than the technical aspects. Looking for a maximum distribution of treatments, the project must implement cooperation with actors external to the company; this new method of project management will allow, hopefully, better coordination among the value chain for the benefit of customers.

The societal impact of the Blockchain technology, announced by several visionaries, is not immediate and its current form will require a lot of back and forth between technology, its developers and all stakeholders (customers, States, citizens).

The use of Blockchain by companies needs an estimation, and then, an effective realization of the financial gains by reductions of costs or new commercial developments, projects emerge with:

– A digitization of procedures, that could certainly be developed previously in the traditional way, but Blockchain and the collaborative approach allow the focus on these procedures.

– New services also based on the new economy of the Blockchains.
STANDARDISATION CHALLENGES

An international working group has been recently established as part of the International Standards Organization, with a first meeting being held in April 2017. The group is labelled as ISO TC 307 “Standardization of Blockchain technologies and distributed ledger technologies”.

The challenge is to help organizations adopt the Blockchain and foster the development of a community of economic actors in the Blockchain able to consolidate the confidence in the technical and business designs, as well as the corresponding legal or regulatory frameworks.

The group will therefore be responsible for designing the next voluntary standards to enable a greater level of interoperability and fasten the diffusion of innovations.

The initial scope of work covers more particularly:

**Terminology (leader to be defined)**
This work will focus on providing common definition of the main terms (e.g. what is a Blockchain from a technical standpoint? from a legal perspective? etc.).

**Reference Architecture, Taxonomy, and Ontology (led by USA)**
This work will conceptualize the development of Blockchain architecture, check that the model allows all existing representations for the use cases, allow the definition of a functional model between the actors and the interfaces for information exchange.

**Use cases (led by Japan)**
This work will consider the most common types of use cases and applications and their potential implications.

**Security and privacy (led by Russia)**
This work will assess the requirements for security and privacy in relation to Blockchain and distributed ledger technologies, and explore relationships with already existing standards.

**Identity (led by Korea)**
This work will Identify the types of identities and entity types needed for data and functionality within Blockchain, as well as the identity management requirements needed outside a Blockchain, upon which the operation of the Blockchain depends, such as for data integrity and for access control.
Smart-contracts (led by Germany)

This work will consider interoperability with the law, including but not limited to the verification, enforcement, and life cycle of smart-contracts. The study group will also consider the transfer of the concept of smart-contracts including transactions to other domains such as Cyber Physical Systems or IoT systems. Further the work will consider the application of programming methodology, domain specific language to also enable non-programmers to express conditions.

French experts are welcome to participate via AFNOR and strengthen the industrial strength of France on the subject and value the know-how of technological clusters such as Systematic and its members. France is also considering a new work item proposal on the governance of the Blockchain. Lastly it is important to make sure European stakes are taken into consideration (for instance the EU Regulation project on Privacy and Electronic Communications), so that European organizations may use the Blockchain to solve their practical business issues.

ISO: International Organization for Standardization

Other initiatives are currently being launched by bodies such as IEEE\textsuperscript{29} and IETF\textsuperscript{30}. European companies are encouraged to participate and make sure their stakes are being taken into account.

Conclusion

Blockchain has reached such a significant level of maturity that the question of its software production in industrial systems arises. This is the very reason these new challenges for this emerging technology are coming from implementation maturity, legal and standardization perspectives.

With these additions, the Blockchain technology will continue to be a disruptive technology but with enough maturity to join the base of operational systems. Each time a system needs a trusted third party, Blockchain will be the alternative solution modifying the trust relationship between the actors. Depending on the requirements analysis, this alternative could replace the previous one based on trusted third party. This emerging technology opens the way for new systems based on the inter-connection between separate systems. For example, the 5G area gathering many different telco operators is a good experimenting field for Blockchain to support the sharing of sensitive or critical data. The IoT landscape is another experimenting field for allowing interactions between the different devices.

\textsuperscript{29} https://www.secureidnews.com/news-item/ieee-launches-standards-program-focused-on-Blockchain-and-identity/
5/ SCIENTIFIC GAP ANALYSIS

Similar to the rising of the internet, the Blockchain technology has the potential to disrupt multiple industries and make processes more democratic, secure, transparent, and efficient. However, many limitations prevent a broad adoption of this technology. In this chapter, we analyze the main limitations, giving links to solutions which already solved them (or at least tried to do so) and describing whether these solutions can work on general purpose Blockchain-based applications or only in the Bitcoin network. At the end of the chapter we also describe the open challenges both from a theoretical and a practical point of view.

RESEARCH CHALLENGES

The interest on Blockchain technology has been drastically increased since 2013. The cumulative number of papers is increased from 2 in 2013 to 41 in 2015 (Jesse, Deokyoon, Sujin, Sooyong, & Kari, 2016). A majority of the studies has been focused on addressing the aforementioned challenges and limitations, but there still exist many issues without proper solutions.

51% ATTACKS

Applications running on top of the Blockchain technology assume that honest nodes control the network (Nakamoto, 2008). If malicious nodes collectively control the majority of computational power within the network (e.g. with botnets) then the network is said to be vulnerable to the 51% attack. In 2015, Beikerdi et al. (Beikerdi & Song, 2015) showed that, although the Bitcoin application has been designed as a fully distributed system, peers gathered within pools are making it more and more centralized over time (26% of centralization in 2011 and 33% of centralization in 2014), thus increasing the chances for successful 51% attacks. Furthermore, other studies showed that the assumption made on the necessity to have at least half of the network computational power is not enough for the security of the network, as the adversarial computational power needed to perform the attack decreases as the network desynchronizes (Garay, Kiayias, & Leonardos, 2015). Even the more recent smart-contract systems, such as Ethereum (I. Eyal, 2016), can suffer from this attack.

Luu et al. (Luu, Teutsch, Kulkarni, & Saxena, 2015) presented a new attack named verifier’s dilemma in which miners are forced into skipping certain transaction verifications where the verification process requires a huge amount of computational power. To solve this problem, the authors proposed a new consensus model which limits the complexity in block verification, thus decreasing the work required by miners. However, this approach cannot be applied to non-financial Blockchain-based application, thus requiring the design and formalization of additional consensus models.
DATA MALLEABILITY

Data integrity is one of the main limitations in a Blockchain based application as it is required that transactions exchanged among peers and verified by the peers have not been altered or tampered with. The lack of strong integrity properties in the Blockchain has been proven in the Bitcoin application with malleability attacks (Decker & Wattenhofer, Bitcoin Transaction Malleability and MtGox, 2014). These attacks are really powerful as they allow malicious users in pretending that one or more transactions in the Blockchain never happened. This is mainly due to the fact that transaction signatures, embedded within transactions, do not provide any integrity guarantees of the signatures themselves (Decker & Wattenhofer, 2014). Trying to solve the malleability issue, Meiklejohn at al. (Andrychowicz, Dziembowski, Malinowski, & Mazurek, 2015) proposed a deposit-based protocol. Their solution uses a timed commitment scheme to enable a malleability-resilient refund transaction as a solution to the malleability problem. However, this approach is tied to the Bitcoin application and cannot be applied to non-financial Blockchain-based applications.

AUTHENTICATION AND CRYPTOGRAPHY

Authentication in Bitcoins and other Blockchain-based cryptocurrencies is based on controlling peers self-certification, and it has been subject to attacks in the past (Decker & Wattenhofer, 2014). Probably the most well-known example is the one that involved Mt.Gox and which saw many customer’s private keys to be stolen. Furthermore, in the last years, different studies tried to analyze the weaknesses in the authentication protocol being used in Blockchain-based application and to propose alternatives. As an example, Bos et al. (Bos, et al., 2014) showed that the use of elliptic curve cryptography (for short, ECC), used in Bitcoin to compute addresses within wallets, is not enough secure as it does not provide enough randomness.

WASTED RESOURCES

The Bitcoin mining process and any mining process which is based on the proof of work or any other brute-force and random-based approach require a high amount of energy to be accomplished. However, this open challenge has not been deeply investigated in the research community. So far, only few papers have been published and all of them were only focused on the Bitcoin network. As examples, Paul et al. (Paul, Sarkar, & Mukherjee, 2014) and Anish (J, 2014) proposed improved Bitcoin schemes for more efficient Bitcoin-like cryptocurrencies whilst Wang and Liu (Wang & Liu, 2015) suggested an economic model for getting high economic returns in consideration of the use of mining hardware with high computation-overpower efficiency and electricity price. Studies on wasted resources are missing for Blockchain technologies not based on the PoW.
PRIVACY

In the Bitcoin network transactions are validated by simply referring to the previous output transactions which are then spent as inputs in new transactions (Nakamoto, 2008). All of this is accomplished by using pseudo-random addresses as transactions sources and destinations without revealing the identity of the users behind them. So far, this approach has been used by many other Blockchain-based applications (either running on PoW or on top of other mining algorithms) and all of them claimed to have good privacy properties because of the original Bitcoin Blockchain design. However, studies such as the traffic analysis done by Koshy et al. (Koshy, Koshy, & McDaniel, 2014) and the framework proposed by Feld et al. (Feld, Schnfeld, & Werner, 2014) both proved the possibility to have transactions linked to the addresses and in some cases even to the users behind the addresses.

To improve privacy, services built on top of transaction mixing algorithms have been defined. A mixing transaction allows the users to randomly move digital assets (coins in the example of the Bitcoin network) between peers thus making it hard to follow the traffic of each digital assets and to link peer activities. Valenta and Rowan (Valenta & Rowan, 2015) proposed a system named Blindcoin which modifies the Mixcoin (Bonneau, et al.) mixing protocol by using blind signatures and public append-only logs which make it possible for a third party to verify the validity of accusations when blind signatures are used. As for Blindcoin, other solutions such as CoinParty (Ziegeldorf, Grossmann, Henze, Inden, & Wehrle, 2015), CoinShuffle (Ruffing, Moreno-Sanchez, & Kate, 2015) and ZeroCoin (Androulaki & Karame, 2014) have been proposed all focused on the Bitcoin version of the Blockchain. To the best of our knowledge, no studies have been published so far on other Blockchain technologies.

COMPRESSION ALGORITHMS

As already introduced, Blockchain size and bandwidth open issues force nowadays applications in either restrict the number of information stored within the Blockchain or to reduce the number of transactions which are accepted and written within the Blockchain. Both these two limitations will not fit in the Internet of Things thus requiring a different approach. This might be the opportunity to innovate new kinds of compression algorithms that would make the Blockchain (at much larger future scales) still usable and storable while retaining its integrity and accessibility.

HASING ALGORITHMS

Since storage in Blockchains is permanent, and storing large amounts of data on a Blockchain is not economical, the practical way to store data on a Blockchain is to store a fixed (and normally smaller) size representation of the data called the hash of the data. Hashing is extensively used with Blockchains, examples are the bitcoin addresses computed by hashing public keys or signatures, computed from a hash of data to be signed and a private key. The Bitcoin protocol
uses the SHA2-256 algorithm but different Blockchain-based application might need different properties and require different algorithms. As an example, Litecoin and other cryptocurrencies use scrypt, which is at least slightly faster than Bitcoin. Furthermore, other yet unknown hashing algorithms could be innovated and designed to support different/improved Blockchain properties.

**CONSENSUS ALGORITHMS**

Under the hood, block-chain technologies rely on a set of replicas, containing a copy of the ledger and a distributed consensus protocol among replicas to establish a unique history of data updates for consistency. However, popular implementations (e.g. BitCoin and Ethereum) provide a weak form of consensus, guaranteeing only eventual consistency. Eventual consistency states that eventually the transaction will be part of a same stable prefix at each peer, but the point in time in which the prefix become stable for a transaction is unknown. In other words, no explicit commit of transactions is provided to the application. Recently, several attempts to make the consistency of the block-chain stronger appeared in the literature (I. Eyal, 2016), (C. Decker, 2016), (E. Kokoris-Kogias, 2016). All of them propose to give additional power to miners, by coordinating their view of the Blockchain through Byzantine-tolerant consensus protocols. Unfortunately, (E. Anceaume, 2016) showed that these solutions have serious limitations. Beyond the complexity introduced by the consensus executions, the main issue comes from the fact that all important decisions are solely under the responsibility of (a quorum of) peers, and the membership of the quorum is decided by the quorum members. This magnifies the power of malicious peers. As already pointed out by Nakamoto (Nakamoto, 2008), if consistency were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs (Sybil attack). The Proof-of-Work mechanism is a barrier for the Sybil attack, however system conditions for Sybil attack prevention without central authority are still under investigation (Douceur, 2002).

Additional work is then needed to assess the security and consistency of mechanisms alternative to Proof-of-Work, such as Proof of Stake, Proof of Activity, Proof of Memory, and related consensus algorithms built upon, such as Practical Byzantine fault tolerance protocols used in Tendermint and Hyperledger.

**INTEROPERABILITY**

In the upcoming Internet of Things, interoperability is of paramount importance in order to have a homogeneous ecosystem rather than multiple heterogeneous ones. As such, even for Blockchain-based applications, interoperability is a key point. Blockstream is a FinTech company working to accelerate the innovation and the adoption of the Blockchain technology by means of improved cryptocurrencies, open assets and smart-contracts. The final goal is to have a platform with sidechains (i.e. different Blockchain implementations with distinct properties) that rely on a central Blockchain which makes all of them able to communicate and cooperate. However, right now this central chain is the bitcoin Blockchain which makes this solution only interesting for financial services or applications.
There are 3 known techniques for interoperability:
– Centralized or multisign notary schemes
– Sidechains/relays
– Hash-locking
Currently, several implementations exist, from Blockstream, Cosmos, Polkadot and others.

**ONLINE VS OFFLINE WALLETS**

In the bitcoin network, wallets are used to store private keys which are needed to access bitcoin addresses and spend their funds. In other Blockchain-based applications, wallets do not contain funds. However, they are still needed to sign transactions exchanged among peers. Wallets can come in different forms and can be designed for different types of devices. The main distinction among wallets is online vs offline. Online (i.e. web-based) wallets store private keys online and some of them are synchronized with mobile and desktop applications, replicating bitcoin addresses between different devices. The main advantage of web-based wallets is that they can be easily accessible from anywhere. However, they also have one major disadvantage: unless implemented correctly, they can put the organization running the website in charge of private keys belonging to the wallets owner – essentially taking control of the wallet itself. The other option is to use an offline (i.e. hardware) wallet. This kind of wallet is actually limited in number and composed by dedicated devices that can hold private keys in a secure way. The major disadvantage of this approach is that wallets cannot be accessed remotely.

**SMART-CONTRACTS VERIFICATION**

Smart-contracts in Ethereum, or chain codes in Hyperledger, are programs executed by the block-chain in an actively replicated fashion. Software replication allows to deliver a great level of fault-tolerance, i.e., execution is guaranteed despite the failure of one or more nodes in the network. While the distributed consensus protocol can tolerate a certain fraction of the nodes affected by a Byzantine behavior (arbitrary deviation from the expected behavior), it is of utmost importance to assure that the program is “bug-free” before execution. Today the verification of those programs poses several challenges. First of all, smart-contracts are expressed in general-purposes Turing-complete languages as Java for HyperLedger and Solidity for Ethereum that are hard to verify. A second problem derives from the very specific mechanisms used in the block-chain related to the cryptocurrency management and payments due to execute “writes” in the block-chain. In Ethereum, for instance, to execute a function changing the block-chain state, the caller must pay some “gas”, where the amount of gas depends on the complexity of the function executed. However, the context of the call can change the amount of gas required in a priori-unknown manner, leading to execution uncertainty. Third problem relates to the distributed nature of the execution. Active replication mimics the execution of a program as if it was sequential, however, in an asynchronous system with at least one process that can fail it is impossible to guarantee sequential consistency (Michael J. Fisher, 1985). Viable consistency semantics must then be established and taken into consideration for program verification.
6/ SWOT

<table>
<thead>
<tr>
<th>STRENGTHS</th>
<th>WEAKNESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical strengths of French environment</strong></td>
<td><strong>Structures</strong></td>
</tr>
<tr>
<td>Many new applications with the only limit of the imagination thanks to the advantages of the Blockchain solution:</td>
<td>– National markets (France and other European countries) are too small.</td>
</tr>
<tr>
<td>– Excellence in mathematics and algorithms</td>
<td>– French players in the Blockchain small and not well known</td>
</tr>
<tr>
<td>– Strong and demonstrated capacity for innovation</td>
<td>– Integration of complete offers (Large Groups + SMEs) still insufficient</td>
</tr>
<tr>
<td>– Powerful but insufficiently exploited ecosystem of freeware</td>
<td></td>
</tr>
<tr>
<td><strong>Ecosystem</strong></td>
<td><strong>Skills</strong></td>
</tr>
<tr>
<td>– Dynamic structures in R &amp; D &amp; I</td>
<td>– Need of more Blockchain specialists, specific cursus to be developed in engineer universities and schools, training curricula to be also developed</td>
</tr>
<tr>
<td>– Many incubators of very innovative SMEs</td>
<td></td>
</tr>
<tr>
<td>– Large international groups with high potential to use the Blockchain as a supplier or as a user (SSII, banks…)</td>
<td></td>
</tr>
<tr>
<td>– Public/private ecosystem working together thanks to the actions of CoFIS</td>
<td></td>
</tr>
<tr>
<td><strong>Public action</strong></td>
<td><strong>Public action</strong></td>
</tr>
<tr>
<td>– Public promotion and support to the innovation and research: FrenchTech, BPI France..</td>
<td>R&amp;D funding landscape</td>
</tr>
<tr>
<td>– Digital domain at the forefront of the priorities of the new government</td>
<td>– Too complicated with a multiplicity of instruments,</td>
</tr>
<tr>
<td>– Some initiatives to support Blockchain development (IRT projects, …)</td>
<td>– Financial support spread over a lot of small projects, not</td>
</tr>
<tr>
<td></td>
<td>sufficiently focused on the real innovations of the sector</td>
</tr>
<tr>
<td></td>
<td>or critical technologies to be developed</td>
</tr>
<tr>
<td></td>
<td>– Funding rates too low, not adapted to the level of</td>
</tr>
<tr>
<td></td>
<td>potential technological risks</td>
</tr>
<tr>
<td></td>
<td>– No funding for projects close to the markets</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPPORTUNITIES</th>
<th>THREATS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New markets</strong></td>
<td><strong>Public action</strong></td>
</tr>
<tr>
<td>Many new applications with the only limit of the imagination thanks to the advantages of the Blockchain solution:</td>
<td>– No large government initiatives launched at this stage</td>
</tr>
<tr>
<td>– Light solutions for the users</td>
<td><strong>Image / acceptability</strong></td>
</tr>
<tr>
<td>– No central repository</td>
<td>– Potential poor perception of the Blockchain in case of issues regarding the Bitcoin. For instance, no ANSSI endorsement of this technology in France.</td>
</tr>
<tr>
<td>– Guarantee of the data integrity</td>
<td>– Uncertain acceptability of Blockchain by large companies and operators</td>
</tr>
<tr>
<td><strong>Business environment</strong></td>
<td><strong>Competition</strong></td>
</tr>
<tr>
<td>– Only emerging standards at this stage for Blockchain, opportunity for Europe to define leading standards which help to mature the market</td>
<td>– Easy financing of SMEs in the US</td>
</tr>
<tr>
<td>– The definition of a Blockchain certification process would help reassuring users and would foster the market development</td>
<td>– Risk of domination by large US Blockchains: Ethereum, Hyperledger and by Chinese miners pools who control Bitcoin.</td>
</tr>
<tr>
<td>– Opportunity to leverage existing demonstrators as Arcade city</td>
<td></td>
</tr>
</tbody>
</table>
7/ RECOMMANDATIONS

This document shows that Blockchain has a strong potential to reinvent the domain of transactions. From this promising prospect, our country should not be set apart but instead should support initiatives aiming at investigating the capabilities of this technology, and identifying its limits, both technical and legal, as well as its ethical and social implications.

Institutional and community involvement

After the first proofs of concept already done with Blockchain technology, the following actions would help move on to more concrete understanding of Blockchain potential:

– Reinforce the relationships between the industrial and the academic teams and scientific societies (such as « Société Mathématique de France », « Société de Mathématiques Appliquées et Industrielles », « Société Française de Statistique », « Société Informatique de France »), to develop joint activities aimed at bridging the scientific gap exposed in this white paper (e.g. through immersive workshops, new ANR projects,...).

– Following this white paper, set up dedicated trainings on Blockchain applications for executives and developers.


– Set up one or several ambitious demonstrators in line with the roadmap of the French Committee of the Industrial Security Sector (CoFIS), in order to increase trust in this technology, to facilitate its adoption and to check its interoperability across organizations and fundamental industries.

– Promote national actions or results related to Blockchain at European level (e.g. through joint contributions between Systematic and the French National Cybersecurity Agency (ANSSI) at the European Cyber Security Organization (ECSO)).

– Establish close relationships between Systematic Digital Ecosystem and other ICT clusters along with the French Data Protection Authority (CNIL) to analyze Blockchain compliance with the General Data Protection Regulation (GDPR).

– Take an active part in the standardization challenges, including security by design and privacy aspects, to influence at least ISO TC 307 working group on Blockchain and distributed ledger technologies (for instance through the French AFNOR. Standardization Association).

– Establish close relationships between Systematic, other ICT clusters and national or European organizations monitoring the development of major public Blockchains, to assess the necessity to develop new national initiatives for public or private applications.

– Encourage sharing best practices around Blockchains, through well-designed community tools and publication of implementation guidelines. Follow in particular the feedback from the French Blockchain Fintech activities.
Organizations’ check list

Each use case should be cautiously investigated to avoid “Blockchain washing” that advocates the use of Blockchain without preliminary study of its applicability. Reasons that justify this technology should be clearly defined beforehand. Other solutions indeed can be simpler and more appropriate. Considering only hype promises brought when introducing any new technology can cause a risk of disillusion and early abandon.

Before jumping into Blockchain, organizations should:

– Analyze the problem that has to be solved, and assess in a challenging approach which/if technical aspects of Blockchain can deliver quantitative/qualitative benefits versus classical solutions.

– Involve all business stakeholders, thus the Blockchain approach is not only handled by R&D. Apart from technology, commercial and regulatory requirements must be analyzed too.

– Analyze the addressable market, for any new solution, but scrutinizing more particularly the ability and willingness of customers to subscribe to the foreseen Blockchain framework. This means validating technical and non-technical aspects, such as ability to deploy, scalability, ease of use, privacy-keeping…

– Get C-level executives as sponsors. They need to be educated about what Blockchain can and cannot do, in a realistic way. This high-level sponsorship will create the first elements of trust in the technology by the consumers.

– Address legal aspects, considering national and international regulations, as well as cross-border interoperability and potential liability issues. Demonstrating the benefits brought by a Blockchain-based solution and the way it copes with non-technical challenges is key to get acceptance.

– Build a long-term vision offer, in order to take into account scalability and resilience requirements, and more importantly, so that the evolution of the operational costs and expected revenues are correctly estimated from the solution launch up to the long term.
The Blockchain can be seen as the ultimate solution to most of our trust problems in the increasingly digitizing global economy. This is demonstrated for example by the amount of investment engaged in startups during the last two years, the announcements of major to care vendors to develop Blockchain offers, the high number of pilots running or in preparation in almost every economic sectors, and also the relatively high visibility of the subject in the agenda of the governments.

Nevertheless, it seems that we still need to be cautious and that in spite of its promises, the Blockchain technology needs to be fully proven in the field before we can really talk about a revolution. Bitcoin was a significant breakthrough – but it is only one part of the story; while it was supposed to revolutionize the money, its major effect has been to raise the attention on the Blockchain itself. One of the key value of Blockchain is its disintermediation proposal, aimed at removing intermediaries thanks to its distributed-ledger architecture. This is for sure a high value proposal, largely overpassing the field of the finance industry.

In order to stimulate mass adoption, the Blockchain will have to demonstrate its ability to solve key issues such as real time processing capabilities, energy consumption, peripheral trust management, to name a few. This will also require joint work between enterprises and regulators, to create a fair business ecosystem and to avoid creating new monopolistic situations.

If all these hurdles are overcome, then Blockchain will not only have created a revolution, it will have succeed in becoming an essential tool in an ever-changing world.
In spite of the questions it raises, the Blockchain technology coupled e.g. with Artificial Intelligence has the potential to revolutionize a lot of application domains by cleverly crossing borders with trust, agility and efficiency. By questioning our governments about their essential roles on regulation and standardization, it could foster a simplification of the notion of trusted-third-parties over time, removing excessive administrative constraints and increasing the confidence than citizens might have in the digital world. In this respect, Blockchain potential on maintaining transaction traceability and non-revocability could be a powerful tool to reinforce digital trust and fight against corruption.

The technology could nevertheless appear as a disturbing paradigm for those who do not wish to see mathematical algorithms replacing human consciousness (observe, capture, integrate, format, analyze, compare, decide, share and memorize… learn from errors).

Beyond this technological upheaval are hidden questions for our philosophers and human science specialists. Society must find its way to reconcile recognized freedom while accepting to be observed. Blockchain announces the premises of in-depth ethical debates at a time when Artificial Intelligence shows up. This should create the foundations for a renewed debate to define the place and acceptance of new technologies in the digital society.
BIBLIOGRAPHY


ABOUT SYSTEMATIC PARIS-REGION

With its Open Innovation focus, the Systematic Paris-Region international competitiveness cluster is there to bring together and promote an ecosystem of excellence that counts over 800 members. Systematic connects stakeholders from software, digital and industry, and boosts digital projects through collaborative innovation, SME development, networking and business sourcing, across a range of strategic sectors: energy, telecoms, healthcare, transport, information systems, factory of the future, digital city, and security. The cluster is also there to promote its members, its region and its innovation projects, with the aim of raising their profile and enhancing the attractiveness of the geographical territory and ecosystem.

The cluster and its projects are especially supported by the European Regional Development Fund (ERDF), the French State (Direccte) and Paris Region.

www.systematic-paris-region.org
@pole_systematic - Systematic
WHITE PAPER

Blockchain: Myth or Reality?

The cluster is supported by:

Honoured partner:

Key partners: