Blockchain Governance and The Role of Trust Service Providers: The TrustedChain® Network

Marcella Atzori, Ph.D.

University College of London - Center for Blockchain Technologies

marcella.atzori@gmx.com

May, 2017

Abstract

Although the blockchain is widely acknowledged as one of the most disruptive technologies emerged in the last decades, many implementation hurdles at the technical, regulatory and governance level still prevent a widespread adoption of services based on open networks. This research discusses the role Trust Service Providers may play in permissioned blockchains, providing a reliable ecosystem in which services can be safely developed and preserved in the long run. As case study, the paper outlines the main features of TrustedChain®, the first blockchain network of European Trust Service Providers specifically designed for highly sensitive sectors, with cutting-edge applications for public administration, e-government, banking, e-health and industry. Emphasis is thus placed on systemic trust, law compliance, adequate technical performance, confidentiality of transactions and long term preservation of data as essential conditions for blockchain networks to thrive and accomplish complex tasks in an effective and reliable way.

Keywords: AI, banking, blockchain, governance, e-government, e-health, eIDAS, smart contracts, Trust Service Providers, TrustedChain®

“Decentralize as much as possible,
regulate as much it is needed.”
G. Paquet

1. The disruptive potential of blockchain and distributed ledgers for digital services. The European Parliament Resolution (2016/2007 INI)

Over the last years, the blockchain technology has come to the forefront of international debate as a new organizational paradigm for decentralized and trustless exchange of value within a network, potentially able to disrupt and re-engineer the way data, processes and digitalized assets are accessed, verified, shared, and preserved over time.

Scholars, technologists, and businesses have explored possible uses of the blockchain - and more generally Distributed Ledgers Technologies (DLT) - in areas as diverse as fintech and banking, e-government, notarial services, healthcare, and industry, including chain supply management, AI, Internet of Things and Machine-to-Machine applications. Depending on the context of use, design and implementation, the advantages of a blockchain-based governance have been recognized as being significant for many classes of services (Blockchain Technologies, 2016; Boucher, 2017; Government Office for Science, 2016; Swan, 2015), in terms of:

- decentralization and reduced reliance of processes on trusted authorities and third parties;
- improved time- and cost- effectiveness of data management and workflows, leading to greater productivity;
- tamper-resistance, verifiability and auditability of digital transactions, with consequent reduction of possible accidental errors, corruption, or fraud;
- improved data security and digital infrastructure resilience;
- enhanced privacy and protection of citizens’ fundamental rights;
- opportunities for value exchange and data sharing between unknown or untrusted participants, reducing counterparty risk;
- tracking of digitalized assets, protection and enforcement of associated rights;
- greater competitiveness, also through the adoption of new business models and applications, such as smart contracts and digital signatures.

Even the European Parliament Resolution (2016/2007 INI) has emphasized the potential of Distributed Ledgers Technology "to contribute positively to citizens' welfare and economic development" (Art. 1). While the Resolution is not binding for Member States or European citizens, it represents nonetheless an important recognition of this technology at institutional level: it established a first conceptual framework for distributed ledger technologies, calling for an adequate regulatory supervision and the development of technical expertise, so to keep up with innovation and ensure timely response to the new challenges at stake (Art. 3).

In particular, the Resolution has acknowledged:

- the potential of DTL to disrupt the way digitalized assets and records are managed and kept, with implications in private and public sector, by means of accelerating, decentralizing, automating and standardizing data-driven processes at lower costs (Art. 5).
- the capacity of DLT to effectively process large volumes of transactions, with innovative applications for fintech industry and beyond, including clearing, settlement, proof of identity and property (Art. B);
- the transformational power of decentralized architectures in terms of efficiency, speed, and also resilience (Art. 6), since they might continue to operate reliably even if the network was to break down in part, due to malfunctioning or malicious attack (Art. 1- c);
- the possibility to use DLT to: protect individual privacy (Art. 1 - d ,e); increase data sharing, transparency and trust between different players, such as governments, citizens, businesses and clients (Art. 8); help institutions to reduce fraud, corruption and money laundering (Art. 11); improve the land registry systems (Art. 12);
- the still unfolding potential benefits of DLT as related to crypto-equity crowdfunding, dispute mediation systems, smart contracts, digital signatures and data security applications for the Internet of Things (Art. 9).

The Resolution has therefore encouraged governmental agencies to test DLT solutions after adequate impact assessment, with a view of improving the quality of e-government and digital services provided to citizens, in accordance with EU data protection rules (Art. 12).

2. Open blockchains and implementation hurdles

In spite of the potential advantages of deployment of the blockchain technology in a great many areas, the adoption of blockchain-based services still appears to be slow and a critical mass of users has not been reached yet. This is surely caused by the many hurdles and trade-offs still existing at the technical, regulatory and governance level, but it is also due to the way the implementation of the blockchain technology is often devised.

So far, practitioners, scholars and blockchain enthusiasts have vigorously insisted on the concept of individual-centricity and decentralization of digital services through peer-to-peer interactions, with the aim to disrupt and re-conceptualize the traditional top-down structure of financial, political, legal and even social powers (Swan, 2015; Wright & De Filippi, 2015). The decentralization of services, however, is often portrayed as a seamless, predictable and linear theoretical process, without properly addressing the complexity of integration mechanisms required at the social, juridical and technical level for effective implementation (Allenby, 2012). At the same time, it is often forgotten that the process of disintermediation may not unfold in an homogeneous way, because every society is different, with different social, cultural and institutional practice, and unpredictable dynamics (Allenby, 2012; Atzori, 2015; Boersma, Meijer & Wagenaar, 2009). A further problem is that the blockchain technology is frequently "picked up and discussed as if it were more mature than it actually is" (Martha Bennett in Earls, 2016).

The question thus remains of *which* blockchain should be used to safely achieving those ambitious, disruptive goals, and how it should be designed, in order to handle the several trade-offs at stake and best make use of this technology.

Open, multipurpose networks such as Bitcoin and its clones have proved highly problematic in this regard. On one side, they are certainly appealing, insofar they aim at fostering innovation and making citizens less dependent on centralized services. On the other side, they still suffer from numerous limitations, related to specific contexts of use, but often overlapping, which may prevent or at least adversely influence a widespread adoption. For the scope of this paper, some of these drawbacks are particularly relevant and can be summarized as follows.

- *Market dynamics and volatility of networks*

Originally designed to achieve disintermediation in the financial sector, permissionless blockchains are generally reliant on voluntary participation of individuals and speculative rewards mechanisms to validate transactions. By their own nature, they are hence exposed to unpredictable market fluctuations, which may endanger their operational capacity over time. While data are permanent in the blockchain, the blockchain is not permanent per se: it can be actually quite volatile, depending on factors such as quality and quantity of nodes, incentive mechanisms and speculation, network effect, and more. Since business continuity is not guaranteed in permissionless blockchains, they may be unsuitable as a permanent store of value and digital data in the long run. This limit adversely affects first and foremost highly sensitive sectors such as e-government, public administration and banking (Atzori, 2015), but many other classes of services as well. Volatility has indeed particular relevance for long-term preservation and notarization of data (namely *proof-of-existence* of data through time), costumer protection and law compliance in both public and private sector, potentially compromising persistence, preservation and future execution of agreements and transactions between parties, as in the case of smart contracts (Atzori, 2015; DuPont & Maurer, 2015). Which suggests that the functionalities of blockchain networks as a store of value and as a medium of exchange exposed to speculative investments should be kept separate, so to minimize systemic risk for sensitive services layered on the top of them (Atzori, 2015).

- *Technical shortcomings*

Services requiring high level of performance are unable to thrive in absence of adequate technical standards. Open blockchains are still at an early stage of development and need to overcome many weaknesses, related for instance to insufficient security, scalability, and capacity of the network, in terms of latency, throughput and bandwidth (Bos et al., 2015; Cortois, 2014; Croman et al., 2016; Ittay & Gün Sirer, 2014; McConaghy et al., 2016). A further problem is caused by irrelevant data (Greenspan, 2015): since open blockchains are typically multipurpose, institutions running their services over such networks would process and store a significant volume of data, which are of no concern to them (Greenspan, 2015), in so also dissipating their computational effort (Monax.io).

Blockchains should rather be streamlined for the domain within which they have been deployed, ensuring high performance, low latency and appropriate level of security, so they can best fit specific purposes (Government Office for Science, 2016; Monax.io).

- *Law compliance and lack of liability*

Open networks are governed by their own technical codes, regardless of geographical boundaries, and this makes it difficult to enforce legal codes issued by state authorities (Government Office for Science, 2016). On one side, regulators have a limited capacity to put in place appropriate safeguards, establish responsibilities and ensure compliance within open peer-to-peer networks - which typically focus on decentralization of services as a way to empower individuals and promote principle of self-organization, with limited or no legal intervention in human affairs (De Filippi, 2014). On the other side, however, the services market and especially the financial industry are highly regulated: businesses and operators are required to provide information to authorities and prove compliance with an extensive set of rules, and transactions executed on a blockchain may not have adequate legal recognition. The lack of liability and regulations governing blockchain services – relating for instance to costumer protection – may also easily undermine users' confidence and discourage them to embrace innovative solutions.

This demonstrates the worth of developing new standards and ensuring effective interaction between technical code and legal code (Government Office for Science, 2016). To mitigate uncertainty and facilitate full compliance with law are in fact essential conditions for businesses and services to thrive.

- *Lack of confidentiality and privacy*

In public blockchains, the nodes of the network have access to each other's data, and transactions are visible to those who explore the ledger. In Bitcoin, a pseudo-identity system allows users to be identified only by the public-keys, but existence, history and flow of transactions are publicly available, so all information associated to users can be retroactively mapped and exposed, if their identity will be revealed at some point in future (Greenspan, 2015; Nakamoto, 2008; Reid & Harrigan, 2011).

To overcome this problem, participants may use different addresses when sending or receiving transactions (Nakamoto, 2008); other solutions such as fully homomorphic encryption (FHE) and zero-knowledge proof are also interesting, insofar they make transaction inputs visible to senders and recipients only, but they are currently still time-consuming, unpractical and inefficient to be widely deployed (Gentry, 2009; Greenspan, 2016; Zyskind, Nathan & Pentland, 2015a).

The transparency of the ledger is often referred to as one of the greatest advantage of the blockchain technology, in line with a new social trend which seems to prioritize transparency over anonymity (Boucher, 2017). Nonetheless, privacy, confidentiality of transactions and data protection are a prerequisite for a wide range of services, especially in sectors such as finance, banking, healthcare, e-government and public administration. Openness and transparency of ledgers usually represent a disadvantage also for firms, because they make it impossible to easily share confidential information or data aggregates with selected users only. Understandably, the risk of losing competitive position or other advantages while making information openly available may prevent many businesses from using public ledgers.

- *Limits of open governance and the problem of democracy*

Peer-to-peer systems like Bitcoin allow anyone to join the community and validate transactions according to a set of rules embedded in a code, with the possibility for each participant to opt-in or out at will. The new forms of direct interaction between individuals enabled by the blockchain technology have led many enthusiasts to challenge the existing political and administrative structures, promoting principles of self-governance based on consensus. In this regard, however, it is important to clarify some important points, and briefly expose the limits which make permissionless blockchains unsuitable for sectors such as public administration and e-government.

The first problem is that open governance can easily turn out to be weak and fragmented. Understandably, the absence of stable, reliable governance structures and traditional safeguards for costumers (European Parliament Resolution, art. 2a,b), along with frequent blockchain forks or even hard forks, may aggravate uncertainty among users and stakeholders, discouraging application in risk-averse sectors.

The second is that, contrary to what is widely believed, open governance and decentralization do not automatically mean fair and democratic governance, nor do they necessarily entail equal opportunities for citizens. While in theory no one owns or controls distributed networks, several factors may prevent open networks from gaining and preserving a true democratic and egalitarian structure over time, such as: digital divide and cognitive entry barriers to digital communities and hackatons; strong asymmetries of information between developers and users; moral hazard and prevalence of economic individualism over common good; core developers' stewardship with special rights in conflict resolution; poor network neutrality and clusters of interests informally acting as centers of steering (Atzori, 2015; Curtois, 2014; Gasser, Budish & West, 2015; Gervais et al., 2013).

The last point is that democracy - as a principle and also as a procedure - cannot be reduce to majority rule and consensus *ex post,* typical of decentralized networks, which entails members of a community to accept (or not) rules already established by developers. Democracy is a much more complex concept, which requires, among other things, adequate quality and extension of participation, consensus *ex ante* and legitimacy of procedures, protection of minority rights, freedom of participants, and again equal opportunities of access to decision-making.

The potential of the blockchain governance and the limits of the mainstream narrative built around it should therefore be critically examined to the light of these concerns.

Thus, for example, the assertion that the blockchain has a sovereign dimension and the constitutional properties of a nation state, and that it is even able to compete against the State (Bitnation.co; Davidson, De Filippi & Potts, 2016) may risk to promote a deeply undemocratic trend in the application of the new technologies at global level. From the standpoint of democratic theory, a group of individuals who cluster around specific interests and temporarily agree on a common set of (algorithmic) rules is nothing more than a private club with no legitimate self-originated sovereign power, and importantly, it represents a relative experience, which cannot "compete" against institutions legitimized by universal suffrage.

Although democratic theory continues to evolve, any exuberant notion of self-organized sovereign community, "private polycentric governance" (Allen, 2016), "authority floating freely" (Swan, 2015) or "algorithmic authority" as a "legitimate power to direct human life" (Lustig & Nardi, 2015) still has to contend with the principle of legitimacy – also considering that algorithms are ultimately human artifacts and they entail assertion of human authority (Atzori, 2015; Musiani, 2013).

Now, the principle of legitimacy is not a trivial issue: it is actually crucial, on both the political and legal level. In fact, it marks the difference between a blockchain governance conceptualized within a democratic framework, and a possible new virtual feudalism, which seeks to justify and advocate the triumph of relativism, alleging technological progress, open innovation, and algorithm-based automatisms.

In this regard, it is important to recall that blockchain networks represent great organizational tools, which can significantly improve the democratic governance, and they should be construed and promoted as such; by their own nature, however, they do not have the properties of stand-alone, entirely self-sustainable political systems (Atzori, 2015), able to represent a viable democratic alternative to institutions and their constitutional principles.

It is true that in the network age, we cannot rely on too rigid, permanent rules (Paquet, 2005); however, if networks only consist of "a loose web of agreements" (Guéhenno, 1993; Paquet, 2005) and they are not anchored to stable and democratically shared principles, the risks is to deconstruct our socio-political dimension and transform it into what is was defined as *spectralitè* (Guillaume, 1984 ; Paquet, 2005): a new form of interaction where “spectres who do not know one other meet” (Baudrillard & Guillame, 1994; Paquet, 2005), giving rise to “a society of phantom-like nomads” (Paquet, 2005), where relationships are disembodied, coordination is difficult, and anonymous market-type linkages are the only ones feasible (Paquet, 2005).

Risks and drawbacks of open governance and permissionless blockchains must therefore be carefully assessed with particular reference to their possible undemocratic development, before promoting forms of “do-it-yourself public administration” (Swan, 2015) or other essential services on the top of them. As Kiviat (2015) rightly noted, “the blockchain technology can support different kinds of dreams”: but precisely because there are so many different legitimate interests and stakeholders in society deserving protection, the main challenge of the blockchain governance is still to achieve a balance between innovation, individual ethos, and the broader public interest.

3. Permissioned blockchains and systemic trust: the role of Trust Service Providers

Technical structure, functionality and coordination of distributed ledgers can be streamlined for specific sectors and purposes, through controlled access permissions, different verification systems and visibility of data. While such permissioned blockchains are inevitably more closed and less transparent than those organized in fully-decentralized manner, they may bring other significant advantages, overcoming some of the limitations of public blockchains. For example:

- ledgers can be designed as tokenless, keeping data safe from speculative rewards mechanisms;
- security, scalability, capacity and general performance of the network can be optimized and adapted to specific functionalities;
- law compliance, consumer protection and confidentiality of transactions can be achieved as needed, through an adequate degree of centralization and even further regulation, if necessary.

Compared to open networks, thereby, permissioned networks enable a more effective and complex governance, suitable for complex tasks.

Even permissioned blockchains, however, may present significant challenges. The main problems lie with volatility and business continuity, since there may be no guarantee that networks will still be operative or even exist in some distant future. The question may thus arise of which entities can be sufficiently reliable as nodes of a blockchain, so to ensure long -term preservation of transactions, without exposing data to market fluctuations or token speculation.

To anchor the blockchain to something stable is of crucial relevance, since so far volatility has been an obstacle preventing the adoption of blockchain-based services in many sectors. The problem also shows that although the blockchain performs trustless transactions through algorithmic protocols, trust is anything but a resolved issue and it actually assumes an even greater relevance at the systemic level. This is why we should better focus on the concept of "increased verifiability" of digital transactions, rather than completely distributed and "trustless" environments (Monax.io).

To overcome volatility and ensure systemic trust of platforms - especially in sensitive sectors such as public administration, e-health or finance, which are not tolerant of service disruptions - one solution would be to engage Trust Service Providers (TSP) as the only full nodes, able to verify the transactions of the network.

The TSP are highly qualified market operators with EU trust mark, appointed by European governmental agencies after a strict conformity assessment, in compliance with Regulation EU No. 910/2014 -eIDAS. They typically provide services such as: the creation, verification and validation of electronic signatures, seals, time stamps or digital certificates; and the management of electronic storage and archiving for documents.

The eIDAS Regulation establishes a general legal framework for digital services provided to the public and having effects on third parties (21). It forces TSP to meet specific requirements in the provisioning of services, relating to high-level security standards (Art. 19), use of trustworthy systems (Art. 24), performance audit (Art. 20), legal certainty and costumer protection (Art. 13.2; Art. 19.2), with a view to ensuring trustworthiness of services and long-term preservation of information (61). Importantly, the Regulation provides for the liability of TSP in the case of non-compliance with due diligence (37) (Art. 13).

The deployment of blockchain-based services by TSP may be facilitated by Art. 62, which allows TSP to introduce new technologies and advanced methods to perform their duties, until they can provide an equivalent level of security and fulfil the obligations laid down in the Regulation.

Compared to other permissioned networks, the development of blockchain networks by TSP under eIDAS Regulation may have a strong added value, leading to significant benefits for sensitive services, such as:

- *Systemic trust, technical performance and privacy*

Long-term preservation of data, business continuity, high-level of security standards, privacy and confidentiality of transactions are essential factors for users, public administration and businesses, in order to develop reliable services and fully benefit from new technologies. Unlike other market operators which may run permissioned networks, the TSP are the only certified entities legally required to fulfil those conditions. Being highly regulated, they have a unique market position, with a unique kind of added value in terms of reliability, security and operative capacity over time. They can hence develop a clearly defined and robust blockchain governance, minimizing hazards and compensating possible market failures caused by volatility and proliferation of hit-and-run services, in so countering the possible gamification of essential services. TSP are also obliged to protect confidentiality of data. Such a high level of reliability can affect positively the general perception of users, institutions and investors about blockchain-based services, leading to a safer and faster adoption.

- *Automatic law compliance, liability and legitimacy*

Unlike other market operators which may need further regulation, the TSP blockchain networks directly apply the EU strict provisions already existing for digital services under eIDAS Regulation, which already harmonizes TSP behavior, liability and procedures. EU follow-up measures and decisions by national regulatory authorities about the blockchain services can be automatically transposed into the TSP network and then applied in many areas, effectively combining legal and technical code, and easily establishing and enforcing responsibilities (Government Office for Science, 2016). Law compliance has the effect to anchoring the blockchain to stable principles set out by legitimate institutions, serving the broader public interest. If well-balanced by the principle of "decentralize as much as possible, regulate as much it is needed" (Paquet, 2005), common international standards and regulation automatically implemented in the TSP networks can be the source of technological development rather than just a constraint, speeding up the adoption of blockchain solutions, and fostering moral progress and innovation.

In turn, even TSP may gain significant benefits from the adoption of the blockchain technology. The digital services they typically provide– such as timestamps, electronic seals, document storage and archiving – can be managed in a cheaper and more effective way with the blockchain technology, improving security and efficiency across industry, but also ensuring privacy and technological neutrality. The blockchain would prevent indeed TSP to indiscriminately gain and collect sensitive information of the citizens, especially relating to online authentication services – an issue which has already raised the legitimate concerns of The Council of European Professional Informatics Societies (CEPIS) for possible risk of user monitoring, profiling and tracking (Hölbl, 2016).

4. The TrustedChain® network: overview

TrustedChain® is the first permissioned blockchain network of European Trust Service Providers currently in operation. Designed by Ifin Sistemi in partnership with Monax Industries, TrustedChain® is engineered to meet the needs of highly sensitive services, both within public administration and private sector. It only accepts TSP as verifiers of transactions and it leverages their high technical standards required by the law, in order to provide a trustworthy and reliable blockchain-based ecosystem, which ensures long-term preservation of data, along with adequate security, scalability, reliability, continuity of service and law compliance.

TrustedChain® is currently the biggest permissioned blockchain of its kind in Europe, both for quality and number of nodes, as well as for number of transactions.

Leveraging the experience and the long-established market positioning of some TSP in specific sectors, the TrustedChain® eco-system allows to develop applications in different vertical sectors, such as public administration, healthcare, banking and industry (*infra* § 5), also supporting the use of smart contracts and AI functionalities. Processing data of several Italian public institutions, such as municipalities and regional governments, the network also introduces the blockchain technology in the Italian public administration for the first time.

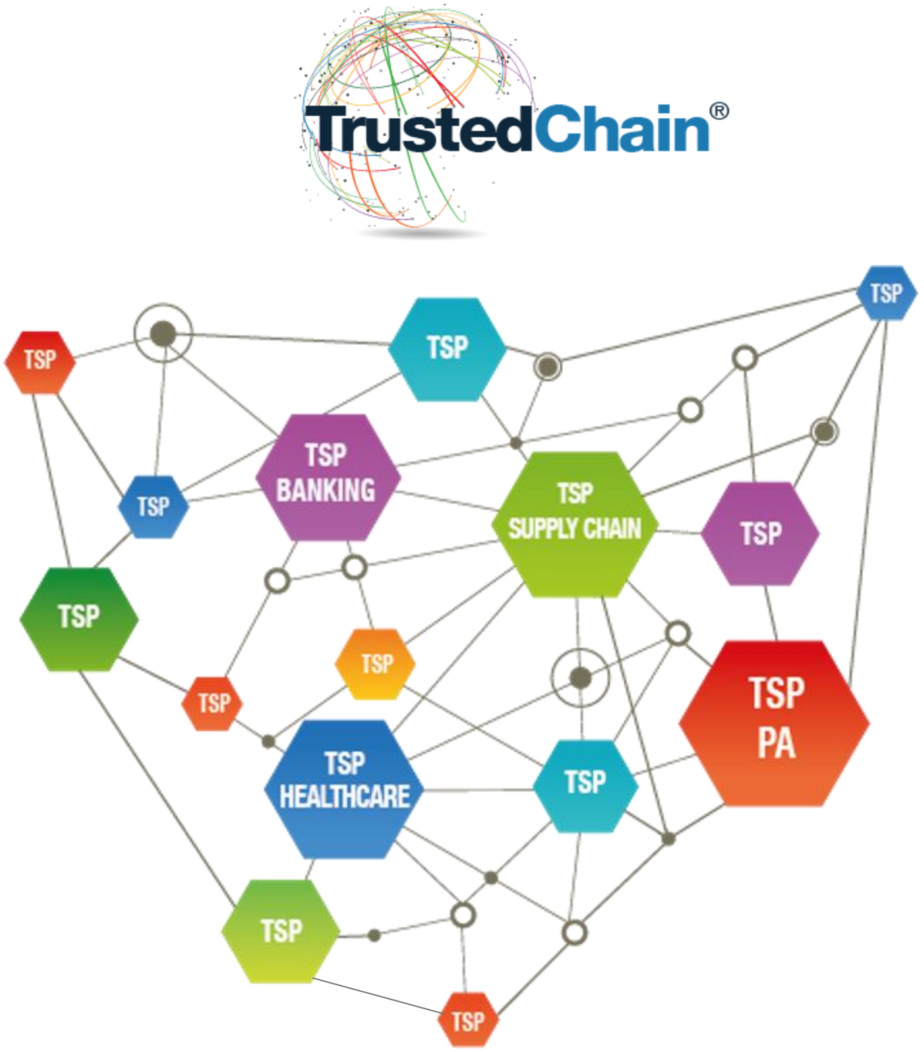


Fig. 1 – The TrustedChain® Ecosystem

- *From inertial data to "green data": the new ecology of digital services*

The TrustedChain® network allows TSP to share and extract value from the data they manage.

So far, the mission of TSP was to ensure digital information to remain accessible and usable over time. Albeit of crucial importance, the digital preservation of TSP has kept data in an inertial condition, since it was not possibile to share them without affecting confidentiality and legitimate interests of their owners.

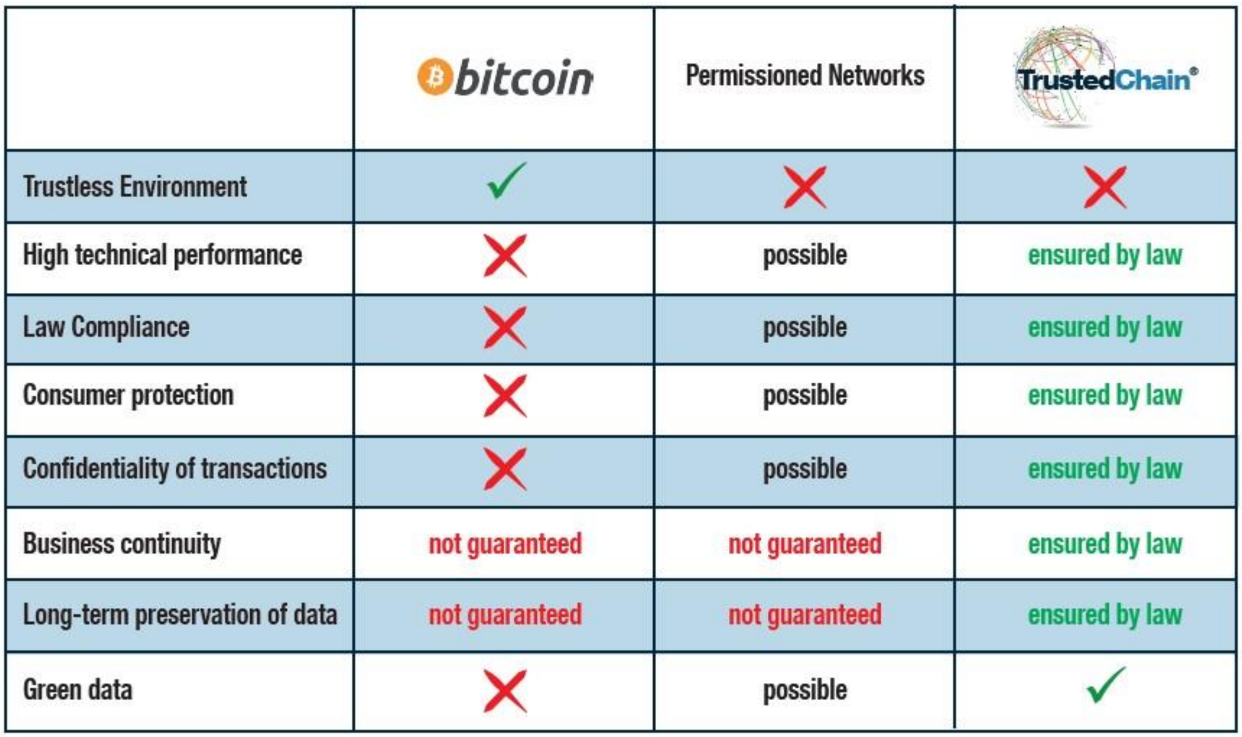
TrustedChain® is conceived as a secure eco-system, which enables all participants to safely share sensitive data and extract value from them for mutual advantage, without compromising confidentiality of transactions: privacy is indeed enforced *by-design* (Zyskind, Nathan & Pentland 2015a,b), namely automatically and in a decentralized fashion, throughout the engineering process. Thanks to the off-blockchain data storage and the use of blockchain as a trustless access-control manager, data queries and calculations are processed off-chain only and in a completely distributed way (Zyskind, Nathan & Pentland 2015a,b). Thereby, through different layers of control, permission and visibility of data, the blockchain makes possible to safely remove the barrier of sharing data with untrusted sources or even competitors, reducing friction and meeting different market and management needs across many industries. Businesses, for example, may hide sensitive information and only share those data that do not endanger their competitive position in the market – especially when a wide array of unknown stakeholders and competitors are involved.

This *ad hoc* algorithmic governance ushers in a new ecology of digital transactions and services, based on *green data*: these are data which are *generated, managed and shared between untrusted or unknown participants for different purposes – for example of a commercial, statistical or scientific nature – and create value for the stakeholders involved and the whole ecosystem, but always in the full respect of sector-specific regulations and without compromising confidentiality, privacy, interests and will of data owners.*

Green data may also be viewed as opposite to Big Data (Zyskind, Nathan & Pentland 2015b), which are often generated by platforms lacking in adequate privacy policy. Especially through ubiquitous computing and IoT applications, “the atomic age of data” (Goodman, 2015) has fuelled public concern about security and privacy of digital platforms, since users may be exposed to several threats, such as identification, localization, monitoring, tracking, surveillance, manipulation, profiling, targeted advertising, data linkage, data breach and even social engineering (Langheinrich, 2001; Ziegeldorf, Morchon & Wehrle, 2013; Zyskind, Nathan & Pentland 2015b).

Thanks to the principle of *privacy-by-design*, a creative engineering and deployment of *green data* may boost research, innovation and the development of new business dynamics in different sectors, to the benefits of many stakeholders. The more the data shared in the ecosystem, the bigger the value generated. This triggers a virtuous circle and a network effect, attracting new participants with increasingly variegated and complex combinations of data sharing, and new models of economic incentives as well. AI and machine learning patterns with both reactive, proactive and predictive functionalities can also be used to extract value from data even more effectively.

In this regard, it should be recalled that it is not possible to generate *green data* with open blockchains such as Bitcoin: *green data* require off-blockchain heavy computation on private data, namely on data with permissioned visibility; Bitcoin transactions instead are completely visible to the nodes and to those who explore the ledger, and the system cannot properly handle heavy computation (Zyskind, Nathan & Pentland, 2015b).



	bitcoin	Permissioned Networks	TrustedChain®
Trustless Environment	✓	✗	✗
High technical performance	✗	possible	ensured by law
Law Compliance	✗	possible	ensured by law
Consumer protection	✗	possible	ensured by law
Confidentiality of transactions	✗	possible	ensured by law
Business continuity	not guaranteed	not guaranteed	ensured by law
Long-term preservation of data	not guaranteed	not guaranteed	ensured by law
Green data	✗	possible	✓

Fig. 2 - Basic features of Bitcoin, permissioned networks and TrustedChain®

5. *TrustedChain® main fields of application*

TrustedChain® supports applications in sensitive sectors, such as:

- *Document storage and archiving* - The application of the blockchain technology can have particularly relevant effects on the traditional TSP storage services. The tamper-resistant, non-repudiable timestamp enabled by the algorithmic protocols can automatically certify the existence and the exact content of any file at a certain date and time (Swan, 2015), ensuring data integrity, accuracy and reliability, and thus complementing the traditional TSP function of long-term preservation of data. "Rather than simply storing the documents, as is done today, a shared ledger system would record proof of the state of those documents" (Government Office for Science, 2016). Importantly, the *proof-of existence* can have several applications in the legal field, since it can demonstrate the existence of any digital asset at a certain date and time, without showing its contents, and keeping confidentiality (Swan, 2015).

- *e-Government and public administration* - The blockchain technology can offer immediate advantages for public institutions through different applications: from the resistance to tampering and protection of document integrity, to the automation and effectiveness of tax collection and administrative workflows. The blockchain has the potential to transform the delivery of public service, improve governance, reduce fraud and also foster the confidence of citizens in institutions and digital services (Government Office for Science, 2016).
  To this aim, TrustedChain® applications include:

- the tamper-resistant, decentralized and efficient management of digital identities and public records, such as fiscal information, judicial data, information concerning immigration flows, etc. Among the many applications of the blockchain technology for public administration, record keeping represents one of the most immediate (Boucher, 2017): it allows for a reduction of redundant data, cost, time and need for infrastructure, and it may lead to a significant saving in public expenditure;
- interoperability and notarization of permissioned ledgers developed within public administration: TrustedChain® is compatible with any blockchain framework and it can preserve other ledgers over time;

- smart contracts and multi-signature transactions: these features may improve effectiveness of tax collection, and also manage and keep track of both public and private funds, with provable transparency and traceability (Government Office for Science, 2016; Swan, 2015);
- data cross analysis and AI: they can be used to improve public governance, reporting anomalies or predicting future problems based on machine learning patterns, while always protecting citizens personal information and privacy.

▪ *Finance and banking* - The blockchain technology can be effectively applied to: reduce cost, time and complexity of the payment, clearing and settlement infrastructures; secure data and transfer of digital assets; gain competitiveness, also through the adoption of new business models and applications, such as smart contracts and multi-signature transactions.

  TrustedChain® provides financial services with a trust-by-design platform, overcoming the typical risks of open networks, and ensuring security, confidentiality of data and law compliance. It also supports smart contracts, for the purpose of reducing transaction time, costs and risks, as well as AI applications. While the latter are already being used by banks, they can be significantly enhanced by the integration within the TrustedChain® ecosystem, since it allows data to be shared between untrusted participants. Indeed, AI models can become much more accurate and efficient if they can access the data of several banks within the same system, instead of only one. In turn, a more accurate AI response can lead to a reduction of workflows and hence greater savings (e.g.: banks may detect frauds or identify unworthy borrowers more quickly).

▪ *Healthcare* - The health sector typically generates, manages and stores big volumes of sensitive data, often causing understandable concern about security, protection of privacy and anonymity of patients. As a consequence, patients may often be refrained from sharing their clinical data and trials for scientific or statistical purpose. The insufficient consent of patients for data sharing may generate significant social and management costs, since it can adversely affects: the quality of scientific research and statistics, due to lack of updated and/or crossed data records; the adequate understanding of costs and benefits of therapies and treatments, due to under-reporting; the prompt response to particular diseases, such as epidemics (Chamber of Digital Commerce, 2016).

  TrustedChain® applications aim at eliminating friction and ensuring privacy, security and systemic trust within e-Health systems.

In particular:

- the algorithmic protocols allow patient identities to be safely verified and tracked;
- data can be collected, shared and analysed for scientific, statistical or commercial purpose, always protecting the privacy of patients *by-design* (i.e. *green data*);
- the procedures to obtain patient consent for data sharing can be automated in a time- and cost-efficient way through smart contracts;
- the exchange of clinical data between medical infrastructures and research institutions can be safely enabled, improving scientific research to the benefit of the entire industry and patients themselves; database can be created for specific problem or purposes (e.g. for transplant) and updated in real-time, without disclosing personal information of patients involved;
- AI applications can be used for automatic diagnosis, medical image processing, prediction of future pathologies, personalized management of care pathways and therapies, and the creation of a broader clinical picture of the patient, including data from wearable devices.

▪ *Industry (and other services)* - TrustedChain® aims at simplifying and improving the efficiency of complex industrial workflows, for example through the traceability of products of an entire production chain from raw materials, in so preventing and combating counterfeiting. But the fields of application of TrustedChain® also include insurance and energy sectors. Smart contracts can be used to automatize and make transactions seamless and more efficient; AI applications can also be deployed to analyse data and support the decision-making phase of workflows, with reactivity but also proactively, pointing out and predicting potential hazards and risks. The technological solutions implemented within TrustedChain® are expected to be a starting point for even further industrial applications, arising from the daily confrontation of developers with the experiences of users.

6. Conclusions

Fully-decentralized blockchains represent one of the many possible models of blockchain governance. Because of its many limits, however, it should not be assumed that such model is always effective for any field of application, or the only *true* way to deploy the blockchain technology - as it was endowed with an undisputed and superior worth. Permissioned blockchains are often perceived as a suboptimal solution or a major brake on innovation, but that view is rather simplistic. The blockchain must be fit for purpose. Accordingly, technical trade-offs, regulation and the plurality of values of the stakeholders involved should always be carefully evaluated, choosing the best model of blockchain governance which satisfies functional requirements of specific usage areas, and serves sustainability in the long run.

In this context, it must also be recognized that a *perfect* blockchain governance may not exist in practice. Compromises are possible and necessary in a multi-stakeholder framework: there may be many possible alternatives for action, and the appropriate mix of centralization and decentralization should be tailored to specific use cases, applying creativity, multi-disciplinary knowledge and technical skills.

Trust Service Providers can play a fundamental role in the blockchain governance, validating the transactions of highly sensitive sectors and providing an ecosystem in which services can safely thrive. Systemic trust, clearly defined governance, law compliance, adequate technical performance, confidentiality of transactions and long term preservation of data are indeed essential conditions for blockchain networks to accomplish complex tasks in an effective and reliable way, and promote sustainable innovation.

TrustedChain® is the first cutting-edge network of European TSP, which captures the benefits of the blockchain technology and offers a reliable and risk free infrastructure upon which public administration and private sector can run specific, decentralized applications. The TrustedChain® ecosystem also allows for AI functionalities and data sharing between unknown parties or competitors, giving rise to a new ecology of data, enabled by privacy-preserving computation techniques. This shows that innovation is not only a prerogative of open networks: even permissioned blockchains may have a strong innovative capacity, and the benefits of a relatively centralized governance can thus be significant.

The active involvement of TSP and the implementation of networks such as TrustedChain® may be highly useful to the faster development of blockchain-based services; additional legislation and standardization at the international level may then facilitate the seamless integration of blockchain services into specific sectors.

References

Allen, D. W. E. (2017). Blockchain Innovation Commons. Available at *SSRN*: https://ssrn.com/abstract=2919170

Allenby, B.R. (2012). *The Theory and Practice of Sustainable Engineering* (1st ed.). Upper Saddle River, NJ: Pearson Prentice Hall

Atzori, M. (2015). Blockchain Technology and Decentralized Governance: Is The State Still Necessary?. Available at *SSRN*: http://dx.doi.org/10.2139/ssrn.2709713

Baudrillard, J. & Guillaime, M.(1994). *Figures de l'altérité*. Paris: Descartes & Cie

Bitnation.co. Governance 2.0. Available at: https://bitnation.co

Blockchain Technologies (2016). What are Blockchain Applications? Use Cases and Industries Utilizing Blockchain Technology. Available at: http://www.blockchaintechnologies.com/blockchain-applications

Boersma, K., Meijer, A., & Wagenaar, P. (2009). Unraveling and Understanding the e-Government Hype. In A. Meijer & al., *ICTs, Citizens and Governance: After the Hype!* (1st ed., pp. 256-265). IOS Press

Bos, J., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., Wustrow, E.,(2014). Elliptic Curve Cryptography in Practice. In Nicolas Christin & Reihanen Savafi- Naini, (Eds.), *Financial Cryptography and Data Security. 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers* (1st ed., pp. 157-175)

Chamber of Digital Commerce (2016). Smart Contracts: 12 Use Cases for Business & Beyond. Available at https://digitalchamber.org/resources/chamber-reports/

Croman, K., et al. (2016). On scaling decentralized blockchains. In *International Conference on Financial Cryptography and Data Security*. (pp. 106-125). Springer Berlin Heidelberg. Available at: http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf

Curtois, N. (2014). On The Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies. http://arxiv.org/abs/1405.0534

Davidson, S., De Filippi, P., & Potts, J. (2016). *Economics of Blockchain.* Available at *SSRN*: http://dx.doi.org/10.2139/ssrn.2744751

De Filippi, P. (2014). Bitcoin: a regulatory nightmare to a libertarian dream. *Internet Policy Review*, 3(2). DOI: 10.14763/2014.2.286

DuPont, Q. & B. Maurer, (2015). Ledgers and Law in the Blockchain. *KR*. Available at: http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/

Earls, A. (2016). Blockchain not a panacea for supply chain traceability, transparency. *TechTarget*. Available at: http://searchmanufacturingerp.techtarget.com/feature/Blockchain-not-a-panacea-for-supply-chain-traceability-transparency

European Parliament Resolution (2016). European Parliament Resolution of 26 May 2016 On Virtual Currencies (2016/2007(INI)). Available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2016-0228+0+DOC+XML+V0//EN

Gasser, U., Budish, R., West, S. M., (2015). Multistakeholder as Governance Groups: Observations from Case Studies. Berkman Center Research Publication No. 2015-1. Retrieve from http://ssrn.com/abstract=2549270

Gentry, C. (2009). Fully homomorphic encryption using ideal lattices. In *STOC*, vol. 9 (pp. 169–178).

Gervais, A., Karame, G., Capkun, S., & Capkun, V. (2013). Is Bitcoin a Decentralized Currency?. *IACR Cryptology ePrint Archive*, 2013, (p. 829).

Goodman, E. (2015). The Atomic Age of Data: Policies for the Internet of Things. Available at *SSRN:* http://ssrn.com/abstract=2605201

Government Office for Science (2016). *Distributed Ledger Technology: Beyond Blockchain*. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

Greenspan, G. (2015). MultiChain Private Blockchain — White Paper. Available at: http://www.multichain.com/download/MultiChain-White-Paper.pdf

_____(2016). Understanding zero knowledge blockchains. *MultiChain.com*. Available at: http://www.multichain.com/blog/2016/11/understanding-zero-knowledge-blockchains/

Guillaume, M. (1984). *Crise et Chuchotements*, Graduate Institute Publications, 1984. DOI: 10.4000/books.iheid.3357

Guéhenno, J.M. (1993). *La fin de la démocratie.* Paris: Flammarion.

Hölbl, M. (2016). Position on the Electronic identification and trust services (eIDAS). Council of European Professional Informatics Societies (CEPIS). Available at: http://www.cepis.org/media/Position%20on%20the%20Electronic%20identification%20and%20trust%20services%20(eIDAS).pdf

Ittay E., & Gün Sirer. E., (2014). Majority is not Enough: Bitcoin Mining is Vulnerable. In Nicolas Christin & Reihanen Savafi- Naini (Eds.), *Financial Cryptography and Data Security. 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers* (1st ed., pp. 436-454). Available at: http://www.cs.cornell.edu/~ie53/publications/btcProcArXiv.pdf

Kiviat, T. I. (2015). Beyond Bitcoin: Issues in Regulating Blockchain Transactions. *Duke Law Journal*, *65*, pp. 569- 608. Available at: http://www.the-blockchain.com/docs/Beyond%20Bitcoin-%20Issues%20in%20Regulating%20Blockchain%20Transactions.pdf

Langheinrich, M. (2001). Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems. Presented at International conference on Ubiquitous Computing. Available at http://cs.gmu.edu/~jpsousa/classes/699/papers/privacy%20Langheinrich.pdf

Lustig, C., & Nardi, B. (2015, January). Algorithmic authority: The case of Bitcoin. In *System Sciences (HICSS), 2015 48th Hawaii International Conference on System Science* (pp. 743-752). IEEE.

McConaghy, T., et al. (2016). BigchainDB: A Scalable Blockchain Database. Available at: https://www.bigchaindb.com/whitepaper/bigchaindb-whitepaper.pdf

Monax.io. Explainer | Permissioned Blockchains. Available at https://monax.io/explainers/permissioned_blockchains/

Musiani, F. (2013). Governance By Algorithms. *Internet Policy Review*, 2 (3). DOI: 10.14763/2013.3.188

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Available at: https://bitcoin.org/bitcoin.pdf

Paquet, G. (2005). *The New Geo-Governance. A Baroque Approach*. (1st ed). Ottawa: The University of Ottawa Press.

Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services For Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC

Reid, F. & Harrigan, M. (2011). An Analysis of Anonymity in the Bitcoin System. Available at: https://arxiv.org/abs/1107.4524

Swan, M. (2015). *Blockchain. Blueprint For a New Economy*. Sebastopol, CA: O'Reilly

Wright, A. & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. Available at *SSRN*: https://ssrn.com/abstract=2580664

Ziegeldorf, J., Morchon, O. & Wehrle, K. (2013). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, 7(12), (pp. 2728-2742). Available at https://arxiv.org/ftp/arxiv/papers/1505/1505.07683.pdf

Zyskind, G., Nathan, O. & Pentland, A. (2015a). Decentralizing Privacy: Using Blockchain to Protect Personal Data. *IEEE Security and Privacy Workshops (SPW)*, (pp.180–184). Available at: http://web.media.mit.edu/~guyzys/data/ZNP15.pdf

_____(2015b). Enigma: Decentralized Computation Platform with Guaranteed Privacy. Available at: http://arxiv.org/pdf/1506.03471v1.pdf