RBPD
Revista Brasileira de Planejamento e Desenvolvimento
ISSN: 2317-2363

https://periodicos.utfpr.edu.br/rbpd

Innovation policy design to scalable crypto-assets in urban public services

Armando N.G.L. Martins
armandomartins.phd@gmail.com
Universidade Federal do Rio de Janeiro.
Rio de Janeiro. Rio de Janeiro. Brasil.

ABSTRACT

This article examines the suitability of crypto-assets in IoT solutions for smart cities from the perspectives of top-down and bottom-up innovation models, discussing the risks and conditions for a secure implementation in accordance with the Precautionary Principle. The emerging technology of the Internet of Things (IoT) promises to solve urban problems through data collection and processing for effective decision-making, which is essential for smart cities. Challenges such as data security, interoperability, and hacking risks persist. Crypto-assets, with their decentralization and security, emerge as potential solutions to these challenges. After discussing the taxonomy of urban innovation policies and associated risks, the study investigates cases of crises in global smart cities, exploring how crypto-asset-based initiatives seek to address these risks. It is found that the distributed nature of crypto-assets addresses typical problems of smart cities, but operational risks, as seen in the cases of IOTA and VEChain, require caution regarding the system's security, indicating a better compatibility with the bottom-up innovation model. The results propose ways to integrate this new technology into urban services, aiming to increase well-being and robustness to prevent failures in the implementation of these services.

KEYWORDS: Smart Cities; Crypto-assets; fat-tailed risk; Precautionary Principle.

1 INTRODUCTION

The objective of this paper is to identify, among top-down and bottom-up models of innovation promotion, which is better suited (following the Precautionary Principle) for risk management related to the use of crypto-asset platforms for urban infrastructure. The growth of cities and intensified urbanization create a need for innovative solutions to address urban issues, such as traffic congestion and pollution.

Global urbanization, and notably Brazilian urbanization, has undergone significant expansion. Brazil saw its urban population grow from 46% in 1960 to 86% in 2016 (WORLD BANK, 2016). Cities, through exchanges of experiences and education, become attractive to individuals seeking benefits from urban networks. However, these metropolises face challenges, such as heavy traffic and pollution.

Cities can be viewed as innovative systems, as proposed by Bjorn Johnson (2008). The author, inspired by the ideas of Schumpeter (1942) and Hall (1998), suggests that cities, in their discontinuous development, can be cradles of innovation to solve their own structural problems and imbalances. Urban innovation can be a crucial tool for the survival and evolution of modern metropolises.

In the context of seeking technological solutions, the Internet of Things (IoT) emerges as an essential integrator for public and private services in cities, promoting better coordination and decision-making related to collective and public goods. This technological advancement paves the way for discussions about Smart Cities, or intelligent cities, which seek to address negative urban externalities through technology.

Despite the potential of IoT, its implementation brings challenges. The need for a unified platform, the processing of large volumes of data, cybersecurity, and ethical issues related to privacy are fundamental concerns. These key elements should guide discussions on the implementation of IoT in cities, especially when it comes to the use of crypto-assets for urban services.

Crypto-assets, as recent and decentralized technologies, seek to address problems associated with Smart Cities and IoT. By exploring the policies of urban innovation systems and observing precautionary principles, this article seeks to analyze the contribution of crypto-assets, their limitations, and usage recommendations in Smart Cities.

The analysis does not assume that crypto-assets automatically drive innovation in urban services. Instead, this study aims to explore crypto-assets as a specific vector in this complex process, observing their suitability in solving urban problems identified in case studies and evaluating the risks associated with their implementation.

The methodological strategy of this work begins with a conceptual discussion about innovation in urban infrastructure and the taxonomy of relevant risks. Then, four case studies are conducted in smart cities to identify risks, followed by an analysis of two scalable crypto-assets (Iota and VEChain). These are studied with the aim of understanding how they address the risks identified in the cities in question. After filtering out the persistent risks, the paper concludes that the bottom-up diffusion model is better suited to minimize the risks observed in the

studied cases, meeting the precautionary needs necessary for a safe and effective implementation of IoT technologies in cities.

2 CONCEPTS

2.1 Innovation Policy Models

The analysis of the technological phenomenon of innovation (that is, the creation of new processes and products in a given sector) and diffusion (the spread of innovation in the market) and the design of policies to promote these activities encompasses a broad research program inspired by the writings of Schumpeter (1942), with notable expansion since the 1980s. Generally, this research program views itself as an approach that studies specific sector contexts and their innovation without necessarily forming a generalizing theory (EDQUIST, 2001). Different taxonomies of innovation policy approaches have been proposed in this research program, focusing specifically on two in this work: the one proposed by Ergas (1987) and the one recently addressed by Schot and Steinmueller (2018).

According to Ergas (1987), the generation of innovation and the survival process of diffusion in the capitalist system heavily depend on market forces, but this system has interacted with the public sector in two ways: harnessing technological strength for public interest and shaping the system to the social context in which it is embedded, be it the institutional or educational standard of the social environment.

In this sense, for Ergas (1987), different models of innovation promotion can be divided into “mission-oriented policies” and “diffusion-oriented policies.” Mission-oriented policies are seen as focused on radical innovations necessary to achieve public interest goals, which are established, implemented, and assessed centrally. On the other hand, diffusion-oriented policies focus on spreading technological capabilities throughout the productive structure, providing facilities for incremental adaptations for structural change. The fundamental aspect of this policy is decentralization instead of centralized goal setting. The focus is on providing public goods for the development of facilitated diffusion structures, with the author presenting three main areas: the expansion of education to form human capital, the development of productive capabilities that facilitate adaptations, production standardization to reduce transaction costs, and the establishment of a cooperative system between production agents, such as industry-university linkages or cooperative laboratories, to facilitate technology transfers and focus on research that benefits multiple actors.

Schot and Steinmueller (2018) see an evolution in the way science, technology, and innovation policies are perceived, starting with three frameworks: promoting innovation through incentivizing research and development sectors for economic growth, the innovation systems approach, and the so-called "transformative change approach." The first framework, stemming from the 1950s, focused on the state's role in developing R&D centers to create innovations that would directly or indirectly benefit the private sector, leading to changes in the productive structure that would bring economic growth. Considering the incompleteness of reducing innovation to R&D leads to the development of the Innovation Systems framework, broadening the scope of involved social actors

(integrating university, public and private initiative, civil society) and bringing transdisciplinary elements of demand and social context to the innovative process, with a non-linear approach. Finally, Schot and Steinmueller describe the conceptualization of a third framework of innovation policies called "transformative change." For the authors, transformative change arises from understanding demands that go beyond the productive focus and enter the social, cultural, and environmental spheres. Transformative change emphasizes the bottom-up process of innovation and seeks to promote this process not only by improving the existing productive system but also taking into account the change in so-called "socio-technical" systems, involving social habits and customs that change the productive system and also the ways of interaction in society.

2.2 Precautionary Principle

Amidst the discussion on the advantages of technological policies for implementing IoT in urban systems, the debate on the precautionary principle brings significant contributions. Originating from environmental law, its concept involves the action of law in the face of damage uncertainty. According to the principle, "a public policy should include measures to prevent or reduce morally unacceptable harm that may result from human actions" that can be "scientifically plausible" (STEELE,2006).

However, this principle is widely debated regarding its potential negative impacts on public policy decision-making. For instance, Cass Sunstein (2003) argues that if understood strongly, the principle is overly paralyzing. According to the author, the concept of precaution involves imposing the burden of proof on the proponent of the activity; there will be cases where the permanent absence of activity may cause more welfare loss than assuming an extremely low risk of a systemic risk event.

On the other hand, Taleb and coauthors (2014) propose a risk typology: the "normal" risk and the "fat-tailed" risk. For "normal" risk, mitigation measures would be available given its estimable magnitude and frequency. However, the "fat-tailed" risk would be of very large or incalculable proportions, and its occurrence would not be estimable, making remedial measures impossible. In this vein, Sunstein's approach would be flawed since it would assume that it is possible to infer the magnitude of the harm that might occur in environmental activities or quantify the likelihood of their occurrence. There might be a chance of risk accumulation that would interact and trigger a chain reaction, contaminating the entire system with disastrous results.

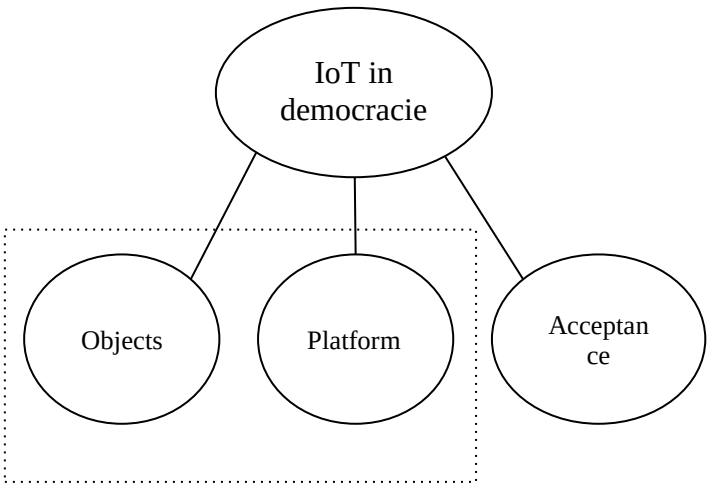
In the case of IoT, one might also argue that, unlike environmental activities, network damage is known: hacker attacks that would take down or manipulate linked activities, or data theft. In this sense, the wrongdoers' volition and severe damages to the urban environment could suggest that the "probability distribution" may have recognized ruinous effects and would warrant a careful look from the precautionary principle's perspective (MARTINS E CIVITARESE, 2018).

2.3 Internet of Things

The Internet of Things (IoT) faces its initial challenge in its own conceptualization. According to Atzori, Iera, and Morabito (2017), the definition of IoT has transformed as related technologies evolved. Broadly speaking, a minimal concept is assumed wherein IoT deals with the interaction between devices capable of capturing or processing data, creating a continuous flow of information production and exchange. Typically, these devices are everyday objects, yet internet-sensitive. For clarity in this paper, a more in-depth discussion of the concept should consider the formation of ontological relationships of necessity and sufficiency that enable an Internet of Things in a democratic environment. In this brief definition, we know, for instance, that the internet is a sine qua non condition for the IoT.

Following Gary Goertz's (2006) methodology for designing the concept of the Internet of Things, the constituent elements of IoT in democracies will be treated here as threefold: applications (or more literally, Things), connection platform, and user acceptance; this structure can be observed in Figure 1. The first two conditions are geared towards technological aspects and industrial organization issues (see Shy 2001), but the third suggests a more cultural analysis than a market-based one, even though it deals with the acceptance of a product. Consensual acceptance is a minimal prerequisite for the IoT to be desirable and, in fact, an internet to navigate. Otherwise, the technological structure is reduced to an imposed monitoring structure. These components, therefore, require separate analyses.

Figure 1 -Formulating the necessary conditions for a democratic structure of the Internet of Things (IoT)



The two technical components required for the Internet of Things (IoT) seem to already be the subject of specialized technological research and development when one considers projections about the phenomenon. On one hand, the number of objects and applications related to IoT is in the billions; on the other, there is currently strong mobile internet coverage in various places around the world, making it possible to assert that there is a latent market for data transfer in countries still without access to these objects. Enabling a platform architecture

that can process this large and growing volume of data is a strategic topic for any development of an Internet of Things network.

What determines technical feasibility is, ultimately, a matter of pricing - or of incentive for adoption in the broader sense. Signal processing and sending technologies are rapidly developing; in this case, adoption becomes a function of supply and demand phenomena. Thus, the issue can be segmented on two fronts. The first is whether the demand is valuable enough to motivate market entry. The second is whether the supply costs of the Internet of Things are low enough for this demand and enterprise to be worth implementing, as opposed to continuing with the current technology without major demands.

Regarding demand, there is significant evidence of the desirability of IoT technologies. The gains in terms of task efficiency and service enjoyment comfort - among other reasons - are notable, and the ever-increasing demand for these services indicates a strong market. However, there might be a moral hurdle concerning consumption. Numerous studies indicate valid constructs of privacy concerns, yet meta-analyses reveal, for instance, a robust non-correlation between these measures and the use of atomized social network platforms (BARUH, SECINTU e CEMALCILAR, 2017). There is what is called the "privacy paradox," where consumers claim to be concerned about the use of their data, but do little to ensure their security when subscribing to a service in the market (BARTH e DE JONG, 2017).

Regarding the Internet of Things, the results are similar, albeit less robust. It has been studied that, for instance, metrics related to the benefit of being on a network dominate the use of technology, making privacy-related metrics less significant (HSU e LIN, 2016). Consequently, it might be hypothesized that privacy may not be, from a market perspective, a barrier to technology adoption, and since consumers disregard the sensitive nature of the technology, the question boils down to an analysis of how many advantages IoT adoption will bring given a cost.

From the supply perspective, there's currently the cost of producing the object itself and a platform for data from that object to travel. These two elements are mapped in the concept but articulate differently. Thinking in an environment of competition from "atomized" platforms, if an object can have an individual production cost, with each unit having unique expenses related to material, a well-designed platform can be repurposed and generate economies of scale. These gains, however, are associated with the formation of monopolies. An open IoT structure may represent, therefore, more than just an application possibility for governments; their incentive also counts as a public policy instrument against market concentration. In this context, there isn't just the technical and business decision of the Internet of Things but also room for government-driven actions in the platform dimension.

The third component of the concept of acceptable IoT in a democracy is how socially desirable the Internet of Things is. As argued here, individual privacy concerns become weak in the face of the advantages of using new technology. However, this individual decision may hide some flaws from the perspective of aggregate well-being. There might be the so-called "commons problem": with everyone only concerned with individual benefit in a process that is not purely market-driven, there's a loss of aggregate well-being and long-term harm to all individuals. Even knowing risks about the future, market participation is subject to

network externalities. In this way, one agent amplifies the cost of non-participation for another, leading to a situation where the immediate network benefits always dominate potential future risks.

Beyond dysfunctional incentives for individual matters, there's also a discussion on the dimension of externalities. It's arguable that delegating the decision on a phenomenon with considerable risks to a relatively uninformed public and with the biases discussed above might even bring harm to individuals who rejected participation in the system. When there's a breakdown of an urban service due to a network failure decided individually by the majority that did not consider the tail risk, those who wouldn't have joined suffer losses. However, if the risk can be estimated, that is, not associated with ruin, one must weigh whether the adoption of restrictive regulations unnecessarily hinders freedom of action in terms of production and acquisition of IoT services.

2.4 Smart Cities

The very delimitation of the concept of Smart Cities is a challenging task, open to debates. To get an overview of the different approaches to what Smart Cities might be, Albino, Berardi, and Dangelico's (2015) work provides an extensive compilation of various notions. In general, one notices that the most comprehensive definitions tend to emphasize either the purpose of smart cities in terms of better outcomes in urban well-being or highlight technological integration as the specific means to this end.

A notable example of a teleological conceptualization of smart cities can be found in Caragliu, Del Bo, and Nijkamp (2011). According to them, a city is smart when investments in human and social capital, and traditional (transport) and modern (telecommunications) communication infrastructure catalyze sustainable economic growth and a high quality of life. This comes with intelligent management of natural resources through participatory governance.

Contrasting this outcome-focused conceptualization, the present study will use a means-focused analysis as a guide to constructing a smart city. Drawing from Chen (2010), who conceives a smart city as one that takes advantage of sensor resources and communications present in the city's infrastructure to optimize logistical operations underlying everyday activities (such as the electrical and transport systems). Thus, there would be improvements in the population's quality of life.

3 INCENTIVES TO SMART CITIES: DIFFERENT APPROACHES

As recognized by Mundula and Auci (2012), the smart cities literature points to various governance operational models. Among those highlighted by the authors are the notions of open cities (PARTRIDGE, 2004), emphasizing transparency through data collection and the transmission of public acts, as well as the mobilization of collective campaigns; sentient cities (SHEPARD, 2011), focusing on the efficiency of urban infrastructure (energy, environment, public transport) by identifying priority care areas; wiki cities (CALABRESE, 2009), aiming at informing urban agents about data for everyday decision-making; and cities 2.0

(CHADWICK, 2008) which underscore the roles of citizens in the city's governance decision process, through e-citizenship and public discussion forums.

Concretely, the existence of different smart city models showcases the possible applications of the Internet of Things in urban systems, as presented in the public consultation to the Brazilian Ministry of Science and Technology (2016): public transport tracking to optimize traffic, electronic surveillance for public safety, measurement of consumption and production to reduce failures and downtime in electric power networks, digitization of hospital goods in public health service, monitoring of water and air quality through electronically connected sensors, aiming to optimize the focus of repair decisions in more urgent areas. Synthesizing from innovation systems, Komninos and coauthors (2019) argue that smart city planning occurs in "innovation circuits" from which the innovative process emerges: the first innovation circuit would be the agglomeration of software and hardware, public administration databases, and electronic services addressed to each city domain; the second circuit pertains to improving decision-making in public and private investments in the city, and the third circuit would be the more efficient behavior of citizens in urban daily life through intelligent systems.

Regardless of the operational model, authors like Kuk and Janssen (2011) indicate two ways a city can evolve to acquire the smart cities status. The first involves the initiative of companies and non-governmental sectors to modernize their existing services and integrate them intelligently to the public, as well as introducing new services under this perspective; the second form stems from the government's initiative to form a technological infrastructure that encourages the shift in business practices to include these in the platform.

For the aforementioned authors, the first model enjoys faster implementation of technologies and lower costs, while in the second model, although more costly and slower for private sector implementation, it would enable greater innovations in the long term, given the greater flexibility and lower service maintenance costs.

Regarding the different emphases on what can develop as smart cities, Komninos et al. (2019) argue an evolutionary view of the development of these cities. In their rationale, the authors borrow from Nelson and Winter (1977) the idea that innovation is an intentional yet stochastic action, which is guided by an external selection that determines how different technologies are selected and changed over time. They also reference Rosenberg (1982), who claims that the evolutionary process is characterized by essential diversification in societies' capabilities to generate technical innovations compatible with their needs. Moreover, in an urban context, they concur with Lambooy (2010) that urban regions provide effective contexts for the development of competencies influenced by environmental selection formed by institutions, market, and spatial structure. However, the uniqueness of regional and urban growth paths is perceived once the competitiveness of a region depends on intangible and non-marketable assets grounded in a knowledge base immersed in the region's own institutional structure (BORSCHMA, 2004).

The role of a smart city formation plan is prone to controversy given the risk of ignoring the city's complex dynamics and the vertical implementation of the plan "killing" aspects of the city's functioning. Insights from information economics suggest that distributed decision-making systems encourage agents to freely

obtain information about their own preferences and stimulate the search for solutions that meet the preferences of demanders. Opting for a centralized system would not only pose problems in processing information scattered among people but would also be an obstacle to the agents' own heuristics in formulating their preferences given everyday choice dilemmas (GREENFIELD, 2013). In an approach termed "quadruple helix governance," both Selada (2017) and Komninos et al. (2019) emphasize the importance of civil society and bottom-up initiatives in building the innovation environment of smart cities, beyond the State-Enterprise-University triplet. In a case study by Komninos et al. for the city of Thessaloniki, the authors found this fourth entity and the technological push encouraged by related organizations a relevant determinant for the development of the city's intelligent infrastructure. In this sense, a model that doesn't seek to shape markets and communities but allows citizens to make decisions in an open manner would tend to offer better results.

3.1 Challenges in Implementing Smart Cities: Four Case Studies

3.1.1 Las Vegas

One of the most notable cities in the implementation of smart city infrastructure is Las Vegas, in the United States. The city, located in the desert areas of Nevada, developed a strong tourism sector driven by the casino industry, has approximately 650,000 inhabitants and receives around 42 million visitors annually. In March 2016, the information systems company Cisco began testing smart infrastructure in Las Vegas "innovation districts". In June 2017, the City Hall closed a deal with Cisco to participate in the Smart+Connected Digital Platform program, implementing city-wide infrastructure of sensors and data collection systems for traffic (mainly), pollution, water consumption, public safety, public parking, waste collection, and public lighting (REICHERT, n.d.). The project was already part of the city's plan to become a Smart City by 2025 and had already invested amounts in the order of US$500 million up to that point. However, the project encountered notable data processing limitations. In 2018, the RootMetrics report by IHS Markit found that the city's Internet of Things networks could not adequately handle large-scale data collection and traffic for basic smart city solutions (AKHTAR e HASLEY, n.d.).

3.1.2 San Francisco

San Francisco, located in the state of California, is the thirteenth most populous city in the United States, with 883,305 residents in 2018 (US CENSUS BUREAU, 2018) and was considered the forty-ninth best city in the world to live in by The Global Liveability Report 2015 (THE ECONOMIST, 2015). In 2012, the San Francisco city government established a department dedicated to "civic innovation". Projects subsequently created by the department involved technological solutions for optimizing police and fire department phone support, the creation of an online portal for accessing subsidized housing purchases and rentals, incentives for voluntary services from private sector professionals, and care for the homeless population (MAYOR'S OFFICE OF INNOVATION SAN

FRANCISCO, n.d.). Other initiatives included smart metering of public water consumption and optimizing parking space offers on the streets. The institutional initiative for innovation in urban services and the pioneering in green solutions earned the city the title of the second most intelligent city in North America, according to Fast Company magazine (COHEN, n.d.). However, the city suffered from a significant crisis due to the hacking of the smart transportation system. In 2016, the city's railway system was captured by hackers who demanded a ransom of 70,000 dollars in bitcoin for its restoration. At the time of the attack, it was estimated that 2000 company servers were affected and sensitive data from 4800 company employees may have been compromised (POREMBA, n.d.), in addition to a loss of 50,000 dollars in uncollected fares due to the halt in activities (NIEPOW, n.d.).

3.1.3 Toronto

Toronto, located in the state of Ontario, is the most populous city in Canada, with 2,731,571 residents in 2016 (CANADA, 2016) and was ranked as the fourth-best city in the world to live in by The Global Liveability Report 2015 (THE ECONOMIST, 2015). In 2017, it was announced that the city would be the first in the world to host a smart city project from Sidewalk Labs, a subsidiary of Google established in 2015. The project entailed the creation of the Quayside district in the city, which would introduce advanced models of physical and digital integration in urban infrastructure (TONAR E TALTON, 2019), involving digital traffic, logistics, and public space management, transportation sharing, and affordable housing solutions, among others (SIDEWALK LABS, n.d.). According to the company, the project anticipates the creation of 93,000 direct and indirect jobs by its completion in 2040, with an annual GDP increase of 14.2 billion dollars (SIDEWALK LABS, 2019). The design of the public-private partnership, however, caused reactions among Toronto's population due to concerns about the privacy of data to be managed by Google, which led to the development of the #BlockSidewalk movement (https://www.blocksidewalk.ca/). In 2019, the Canadian Civil Liberties Association (2019) wrote an open letter to the then Prime Minister, Justin Trudeau, and filed a lawsuit against the project manager, Waterfront Toronto, the municipal government of Toronto, the state government of Ontario, and the federal government of Canada to halt Sidewalk's progress (SMARTCITIESWORLD, 2019a). In June 2019, Sidewalk Labs released the master plan for the project (SIDEWALK LABS, n.d.), addressing, among other things, the disputed data privacy issues; however, Waterfront Toronto criticized the plan's vagueness regarding critical aspects of the proposals and the feasibility of digital innovation, suggesting that data management should be conducted by Waterfront Toronto and the governments. Doubts about Waterfront Toronto's commitment to data protection regulation led to the resignation of its members (SMARTCITIESWORLD, 2019b), while the stalemate with Sidewalk Labs has yet to be resolved.

3.1.4 Montreál

Located in the province of Québec, Montreal is the second-largest city in Canada, with 1,704,694 residents in 2016 (CANADA, 2016) and was ranked as the fourteenth best city in the world to live in by The Global Liveability Report 2015 (THE ECONOMIST, 2015). Until 2014, when the city government launched the Montreal Smart and Digital City project, there was no defined public sector plan for developing a smart infrastructure in the city. Instead, it evolved from interactions between civil society, private initiatives, and universities, institutionalizing as a network of "creativity" and "learning" (LEYDESDORFF e DEAKIN, 2011). Beyond becoming a notable global cultural hub, factors like an aging population, obsolescent public infrastructure, and the presence of major information and communication technology providers led to bottom-up smart solutions focused on public health, electric distribution, and public transportation, but also on the environment and education. With the largest transportation-sharing network in North America in 2013 and a legal system for public engagement and consultation, Montreal was ranked as the tenth smartest city in North America by Fast Company (COHEN, n.d.). However, Ben Letaifa (2015) points out that the main problem with the city's smart system is its lack of coordination; as different initiatives arise independently and often competitively, frequent governmental changes hinder the convergence and communication between these initiatives for long-term planning and political commitment. This is further complicated by the gray areas created by overlapping competencies between municipal, provincial, and federal spheres. With the Montreal Smart and Digital City initiative in 2014, the Montreal municipality began seeking to develop an infrastructure that coordinated the initiatives and made the management of smart infrastructure transparent and open to public participation (MONTRÉAL, 2014).

4 DECENTRALIZED DIGITAL PLATFORMS

4.1 Blockchains

To understand the notion of crypto-asset platforms, it is necessary to trace their pioneering technology: blockchains. The backdrop for the development of this technology arises from discussions about creating a 100% digital currency, a discussion that dates back to the dawn of the internet (this discussion summarizes the description provided in Martins, 2016). The challenge to overcome was to create a currency that served as a store of value for the user, but that didn't face the problem of "double-spending," meaning the currency could not be cloned and used for numerous transactions.

Notable precedents in crypto-asset technology include Wei Dai's (1998) privacy system, based on pseudonymous wallets with encrypted keys, and Nick Szabo's (2006) proof-of-work concept, which established an incentive system for transaction validation. Bitcoin, conceived by Satoshi Nakamoto (2008), consolidates these technologies into a structure called blockchain. In the blockchain, miners accumulate transactions in blocks, which are linked in sequence and encrypted. The miner who decrypts a block's encryption broadcasts its information, receiving fees and coins as a reward. This process, termed "proof of

work," aims to ensure transaction integrity, preventing manipulations and duplicated transactions.

Blockchain's innovation was recognized not only as a tool for financial transactions but also as a publicly auditable record of various kinds of information while keeping users pseudonymous. This enabled the creation of a trustworthy "virtual notary" robust to manipulations, without the need for a central entity validating transactions. This also led to the development of smart properties linked to platforms and smart contracts, which are executed automatically according to pre-established code, both crucial for the contemporary conception of the Internet of Things (IoT).

Davidson, De Filippi, and Potts (2018) posit that, while blockchains have various applications, their main innovation is the ability to coordinate and solve problems previously confined to institutions. Thus, blockchains can serve as alternatives or complements to state action, enhancing their efficiency.

4.2 Data Processing Scalability and IoT Crypto-assets - A Case Study of IOTA

Blockchains were the first part of a technological revolution, but they present scalability problems. Compiling a large ledger of all possible transactions and articulating them sequentially to be read by all network participants is an extremely costly and slow, albeit secure, way to realize a decentralized platform. For some practical applications, including IoT, the number of transactions grows non-linearly with the number of users or connected devices, making blockchains unfeasible and incentivizing the development of new technologies aimed at a larger number of transactions.

However, if the network is not limited, there is a real possibility of a unified platform for IoT. This idea resonates in the technology of the first "alternative cryptocurrency" (altcoin) not derived from the blockchain. Using a mathematical formulation called "Directed Acyclic Graph" (DAG), the researchers of the IOTA cryptocurrency developed a technique where past transactions confirm current ones (POPOV, 2018). In this case, there is a Proof-of-Work for each transaction, which must confirm the two preceding ones. In this way, as the number of transactions increases, the potential for confirmation and network speed increases.

This technology was applied to IoT primarily because the application matches the technology remarkably well: the volume and consistency of ubiquitous application data would drive the platform to its maximum power. Once well implemented and connected to real applications, the network would be efficient in providing the unified platform that Smart Cities need. It is necessary, therefore, to study what could potentially prevent this reality and how, if it is suitable, to use it in public policies and regulatory frameworks. Currently, the most significant application case of this technology is IOTA itself, which warrants careful dissection.

4.2.1 Challenges and implementation of IOTA

The current development of IOTA raises three issues that make it difficult, however, to believe that it will be the platform of choice to support ubiquitous computing in Smart Cities. This is regardless of the discussion about privacy, as the technical feasibility of the current formulation of IOTA seems to face risks that discourage its adoption as the tool of choice for Smart Cities at the moment.

In addition to flaws identified in the fundamental functions of the cryptographies under which the network operates, there are doubts about the DAG itself. In a considerably technical article, Babaioff, Dobzinski, Oren, and Zohar (2012) discuss criteria for preventing a type of attack based on creating a massive number of puppet users to influence the system as a whole (Sybil attacks) in a cryptographic network. Bitcoin did not meet some of these criteria in its early stages, and it is unclear how IOTA's technology would also not be affected - there is a lack of tests to attest to the network's robustness. It is not uncommon for these problems to be found - years after the creation of Bitcoin, Eyal and Sirer (2018) found an attack that could be perpetuated by any number of interested parties. At the same time, these authors proposed a solution to the problem found in Bitcoin. IOTA's problem is more critical: the very structure imposed by the math that underpins the DAG seems to be susceptible to these attacks, possibly being not reliable enough currently if the countermeasures discussed by Popov (2018) are not implemented correctly.

Finally, it is not desirable to pour public resources, either through application development or study and connection to a platform, into a venture that presents risks of suffering severe damage or being proven unreliable overnight. The guidance of public administration should be towards efficiency and transparency in its expenditures. In this case, the role of the precautionary principle is clear, also from a budgetary perspective. This adds to the efforts needed to reduce exposure to risks to the population that may result from a critical network failure.

4.3 Other IoT decentralized network and its challenges

Although the crypto-asset market seems promising, among the top 100, only IOTA is directly related to IoT. VeChain, on the other hand, uses blockchain for supply chain activities, with potential applications in smart cities, but not directly in domestic IoT. VeChain, despite having fewer detectable problems compared to IOTA, faces relevant criticism.

Two criticisms stand out: its similarity to Ethereum and its new consensus algorithm, the Proof-of-Authority. The first criticism involves the risks associated with users interacting with the structures programmed on the Blockchain, which can lead to failures and governance challenges. The second risk of similarity to Ethereum is the scalability limitation of the blockchain, especially when the number of connected objects grows. Proposed solutions to these problems are still in early stages and without robust testing.

On the other hand, VeChain's Proof-of-Authority, based on the identity verification of participants, resembles the Ripple system, which requires a KYC (Know Your Customer) process. This approach is not fully decentralized. Although participants can integrate into the network without the KYC, they would have

validation power in only 20% of the blocks. This suggests a tilt towards centralization, giving excessive power to the blockchain coordinator. Such a scenario would likely not sustain a competitive market in terms of supply, raising concerns about its suitability for IoT applications.

5 OTHER DESIRED PROPERTIES FOR A PUBLIC IOT NETWORK

In emergency situations, therefore, one can use crypto-assets and modular blockchains to address infrastructure problems in developing countries. However, the dynamics driven by Internet of Things issues are somewhat more complex. The uses previously described pertain to databases and relatively simple financial transfers; when dealing with a technological platform, there is a constant evolution of applications and consumer demands, leading to new update needs.

Considering this less stable dynamic and the precautionary principle, it is necessary to map the risk sources in public structures concerning network security against attacks, the network's ability to genuinely integrate with city applications, and citizens' privacy. This subsection breaks down these three points and outlines safety conditions to justify public policies.

It should be noted that these policies boil down to the State developing applications on a platform; for example, a transit company saving data from cars and pedestrians passing by a speedometer through the platform. Other policies that encourage network formation or maintenance are not discussed as the purpose of these initial criteria. However, due to the dynamic nature of the asset, issues related to risks in network updating will be considered.

5.1 Network security

As seen in the case study of the city of San Francisco, network security is a fundamental aspect for guaranteeing public services in a Smart Cities environment. In the analysis of the IOTA crypto-asset technology, it was observed that there are several possible attacks on a decentralized cryptographic network. Digital security research is ongoing, with malicious attacks and defenses discovered frequently, but there is the test of time and testing protocols for cryptographic functions and architecture. A platform used in governmental applications must pass through these criteria and not be purely inspired by commercial motivations. Civil society organizations, universities, and other agencies should verify the security of, for example, hash functions adopted on the platform, as well as robustness against various types of attacks.

However, there are unexpected phenomena that may demand swift decisions by the network maintainers. De Filippi and Loveluck (2016) argue that there are two governances in a decentralized network: governance by the network and governance of the network. The former refers to the incentives participants have to act correctly; this goes through the quality of implementation, tools used, incentives to mine or not attack the network, and the like. The latter deals with how software developers coordinate network updates. Being a still recent technology, there are open questions in development that lead to conflicts between developers. In the case of Bitcoin, the largest crypto-asset, there were issues about how to scale the technology. This led to a schism in the network,

generating the division between Bitcoin and Bitcoin Cash. In the case of Ethereum, there was a critical failure in an application that froze millions of dollars. The developers' solution was to reverse the operations, which caused a contentious and rapid separation between those opposed to the repair — who founded Ethereum Classic — and those in favor who maintained Ethereum.

The same can happen on a platform where a smart city's operations exist. In this case, the development team responsible for the platform's governance must be accountable to the governments implementing the smart city's infrastructure. Therefore, there should be concern not only with technological aspects for the risk of attacks but also an institutional structure on how to deal with necessary changes in case of a failure. It is also worth noting that the use of IoT platforms does not replace the previous structure of conventional cities. In the event of, for example, a critical failure and traffic light outage, the conventional system should be adopted. It is concluded that, therefore, the implementation of a smart city policy based on these platforms is an addition to an urban apparatus, not a substitute in progress.

5.2 Platform connectivity

The effectiveness of a platform is not just based on its security but also its applicability in various contexts. This extends beyond smart cities, where a decentralized platform can foster a greater entrepreneurial inclination in the impacted areas. To attract non-governmental applications, it is vital to develop user-friendly interfaces for both users and developers. Thus, IoT networks should prioritize aspects such as design and user experience.

Concurrently, innovation incentive policies should create a conducive environment for the platform's evolution. With the right support, integration with the platform becomes simpler, as long as it is secure. However, in developing countries, the appropriate structures for this are sparse. Although the network's decentralized nature might favor development, governments and local organizations should focus on its practical application. In summary, the mere presence of the platform isn't enough to drive technological innovation. To be effective, especially in developing nations, the platform must be shaped to facilitate the implementation of successful public policies.

5.3 Privacy and citizen data

Decentralized networks per se allow for greater privacy due to the aspect of pseudonymity: when connecting to Bitcoin's blockchain, for instance, there's no need to declare one's identity. This isn't the case for all crypto-assets, as discussed in the case of VeChain, but generally, this behavior is prevalent. However, when using a network linked to an object, the data can be associated with the object's location. Also, once this data is beyond the control of the original user, it might be shared.

Two solutions for this arise from a blend of the network's "regulatory" design and technological advancements. The first is the so-called "opt-in policy". At every stage of data transmission, the individual would know to whom it's being sent, and they would need to approve this transmission. This policy has been discussed by

the development team behind the crypto-asset IOTA (MARIS, 2018) and other crypto-assets like the privacy coin Monero. This can be seen as a form of self-regulation that should be demanded in platforms used by governments.

The second solution involves clustering methods. These methods aim to group individual data into clusters without losing the information relevant to the entities that would utilize it. This field is currently undergoing cutting-edge research (AGGARWAL et al., 2010), making it highly feasible for implementation. Although this isn't always possible in the case of IoT, for smart cities and urban data control, this is an option. Therefore, governments and organizations that use this data should be regulated to employ these methods.

6 DISCUSSION

In general, it's possible to argue that crypto-asset platforms offer distinct advantages. Compared to challenges faced by radically decentralized smart city models, like that of Montreal, there's an opportunity here to reduce coordination costs for agents and infrastructure platform implementation. This would arise since their software foundations are essentially "ready-to-use" (eliminating the costs of building from scratch), and businesses would benefit from significant synergy by utilizing the same platform and having the flexibility to innovate (with the source code accessible to all). All of this structures the system in an intentionally open way, without necessarily needing to shape the business or community action model.

Despite literature on the "privacy paradox" regarding the atomized adoption of IoT services and social networks, centralized infrastructure implementation can incite social tensions over data privacy issues, as seen in the Toronto case study. Regardless of the implementation model, crypto-asset platforms have developed networks that aim to be widely compatible with technologies focused on preserving user privacy; in this regard, societal concerns raised by movements like #BlockSidewalk would be diminished.

The advent of Smart Cities isn't immune to discussions about its risks. Distributing data processing would prevent bottlenecks seen in the operation of basic urban services, like in Las Vegas. However, as perceived from the study of IOTA and VeChain, the two qualities of privacy and decentralization still pose a technology trade-off challenge to be overcome.

Furthermore, Kitchin and Dodge (2019), for example, list five primary vulnerabilities that integrated systems can face concerning cyberattacks: weak software security and data encryption; integrated use of outdated insecure systems with inadequate maintenance; many platform interdependencies and attack entry points; cascade effects where interconnected entities pass adverse effects to one another; human error and malice from (former) employees. Given these vulnerabilities, hacker attacks on smart city networks can significantly disrupt public service. Amid the problems of cyberattack risks, as exemplified by San Francisco, decentralized digital platforms emerge as a potential solution. This would occur since data processing "servers" would organize distributedly, without focal points targeted for hackers to breach and manipulate data. However, this system's success will depend on the crypto-asset platform's network design and encryption quality, something initiatives like IOTA have yet to effectively address.

In this context, despite the current shortcomings of platforms dedicated to IoT, the potential benefit of a decentralized network is evident, should a successful technology emerge. Once developed, the platform would bring advantages to the entire ecosystem supporting a smart city – in other terms, a positive technological externality. From an economic and pragmatic standpoint, an institutional environment conducive to its development should be fostered. As the evolution of these technologies arises from knowledge production, the presence of incentives for study groups in cryptography, parallel computing, and other techniques in national labs and universities is a strategy that governments keen on modernizing their urban infrastructure should consider, irrespective of creating their applications on the networks. In this sense, it's indicated that the technology of crypto-asset systems would best be promoted in policy arrangements focused on diffusion and with a transformative change approach, due to the technology emphasizing the network's bottom-up aspect and relying on transformations in the city's socio-technical systems, transcending production and affecting cities' social and environmental interaction mode.

7 CONCLUSION

The discussions around smart cities introduce new perspectives on urban policies. The integration of sensor systems and data quantifiers into the internet (Internet of Things) allows for more efficient decision-making for day-to-day life in cities, both from an individual perspective and democratic decisions about public goods, such as in the targeting of the provision of urgent services in the case of public administration.

However, a conceptualization of IoT in democracies has been developed, revealing the necessary conditions for a network to be suitable for this function; the implementation of a transformation plan for metropolises into smart cities encounters a series of considerations. Guided by the precautionary principle, desired properties for the technology used as an IoT platform were listed: scalability in data processing, network security against hacker attacks (which would pose systemic risks to all linked urban services), the reduction of difficulty in producing new services in cities due to the need to connect to the network, and the minimization of the undue publicization of data produced by the citizens themselves, or the increase in control over them by the state.

Amid this problem, the development of scalable crypto-assets seeks to provide solutions for the development of IoT networks that can contribute to the formation of smart cities. As a general rule, the technology derived from Bitcoin tends to bring multiple layers of encryption, which would provide robustness against cyberattacks (as seen in San Francisco); it distributes data processing to gain scale and seek to avoid bottlenecks (as seen in Las Vegas); the implementation of a crypto-asset platform with a simple interface would bring high connectivity and reduce the costs of creating a new service linked to the network (reducing the coordination costs seen in Montreal). Even with the inconsistencies of user preferences for atomized services with data protection raised by the literature on the 'Privacy Paradox,' crypto-assets focused on IoT usually bring technologies that preserve user privacy in the face of the public manager and service provider. In this way, potential social tensions, such as those seen in Toronto due to a centralized

implementation of intelligent infrastructure without privacy treatment, would be reduced.

However, it should be noted that the contribution of crypto-assets to smart cities is still in its infancy. As an example of IOTA, recently launched assets still raise doubts about their security against attacks, unlike platforms already consolidated for ten years, such as Bitcoin itself; moreover, the robustness of data privacy among users is not yet fully understood, or if there are leaks.

Nevertheless, it is possible to assess that the perspectives that crypto-asset technology brings to solving the problems faced in the implementation of smart cities converge towards models of diffusion policies and transformative change, which implies a research field that can be developed involving initiatives from various sectors of society in terms of production and social interaction, which would require an institutional and educational environment conducive to this type of innovation.

Desenho de políticas de inovação em criptoativos escaláveis nos serviços públicos urbanos

RESUMO

Este artigo analisa a adequação dos criptoativos em soluções de IoT para cidades inteligentes, sob as perspectivas de modelos de inovação de cima para baixo e de baixo para cima, discutindo os riscos e condições para uma implementação segura, conforme o Princípio da Precaução. A tecnologia emergente da Internet das Coisas (IoT) promete solucionar problemas urbanos através da coleta e processamento de dados para decisões eficazes, sendo essencial para as cidades inteligentes. Desafios como segurança de dados, interoperabilidade e riscos de hacking persistem. Os criptoativos, pela sua descentralização e segurança, surgem como possíveis solucionadores desses desafios. Após discutir a taxonomia das políticas de inovação urbana e riscos associados, o estudo investiga casos de crises em cidades inteligentes globais, explorando como iniciativas baseadas em criptoativos buscam enfrentar esses riscos. Descobre-se que a natureza distribuída dos criptoativos aborda problemas típicos de cidades inteligentes, mas riscos operacionais, como os vistos na IOTA e VEChain, demandam cautela quanto à segurança do sistema, indicando uma maior compatibilidade com o modelo de inovação de baixo para cima. Os resultados propõem maneiras de integrar essa nova tecnologia aos serviços urbanos, visando aumentar o bem-estar e a robustez para prevenir falhas na implementação desses serviços.

PALAVRAS-CHAVE: Cidades Inteligentes; Criptoativos; Risco de cauda grossa; Princípio da Precaução.

REFERENCES

AGGARWAL, Gagan et al. Achieving anonymity via clustering. ACM Transactions on Algorithms, v. 6, n. 3, p. 1–19, jun. 2010.

AKHTAR, Norman; HASLEY, Kevin. Smart cities face challenges and opportunities | Computer Weekly. Disponível em: <https://www.computerweekly.com/opinion/Smart-cities-face-challenges-and-opportunities>. Acesso em: 6 out. 2023.

ALBINO, Vito; BERARDI, Umberto; DANGELICO, Rosa Maria. Smart Cities: Definitions, Dimensions, Performance, and Initiatives. Journal of Urban Technology, v. 22, n. 1, p. 3–21, 2 jan. 2015.

ATZORI, Luigi; IERA, Antonio; MORABITO, Giacomo. Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. Ad Hoc Networks, v. 56, p. 122–140, 2017.

AUCI, Sabrina; MUNDULA, Luigi. Smart cities and a stochastic frontier analysis: a comparison among European Cities. Available at SSRN 2150839, 2012. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2150839>. Acesso em: 6 out. 2023.

BABAIOFF, Moshe et al. On bitcoin and red balloons. In: EC '12: ACM CONFERENCE ON ELECTRONIC COMMERCE, 4 jun. 2012, Valencia Spain. Anais... Valencia Spain: ACM, 4 jun. 2012. p. 56–73. Disponível em: <https://dl.acm.org/doi/10.1145/2229012.2229022>. Acesso em: 6 out. 2023.

BARTH, Susanne; DE JONG, Menno DT. The privacy paradox–Investigating discrepancies between expressed privacy concerns and actual online behavior–A systematic literature review. Telematics and informatics, v. 34, n. 7, p. 1038–1058, 2017.

BARUH, Lemi; SECINTI, Ekin; CEMALCILAR, Zeynep. Online privacy concerns and privacy management: A meta-analytical review. Journal of Communication, v. 67, n. 1, p. 26–53, 2017.

CALABRESE, Francesco. Wikicity: Real-time location-sensitive tools for the city. Handbook of research on urban informatics: The practice and promise of the real-time city. [S.l.]: IGI global, 2009. p. 390–413. Disponível em: <https://www.igi-global.com/chapter/handbook-research-urban-informatics/21816>. Acesso em: 6 out. 2023.

CANADA. Census Profile, 2016 Census. . [S.l.]: Statistics Canada. , 2016

CANADIAN CIVIL LIBERTIES ASSOCIATION. OPEN LETTER FROM CCLA: CALLING FOR A RESET ON WATERFRONT TORONTO. . [S.l: s.n.]. , 2019

CARAGLIU, Andrea; DEL BO, Chiara; NIJKAMP, Peter. Smart Cities in Europe. Journal of Urban Technology, v. 18, n. 2, p. 65–82, abr. 2011.

CHADWICK, Andrew. Web 2.0: New challenges for the study of e-democracy in an era of informational exuberance. Isjlp, v. 5, p. 9, 2008.

CHEN, Thomas M. Smart grids, smart cities need better networks [Editor's Note]. Ieee Network, v. 24, n. 2, p. 2–3, 2010.

COHEN, Boyd. The 10 Smartest Cities In North America. Disponível em: <https://www.fastcompany.com/3021592/the-10-smartest-cities-in-north-america>. Acesso em: 6 out. 2023.

DAI, Wei. b-money. URL http://www. weidai. com/bmoney. txt, 1998.

DAVIDSON, Sinclair; DE FILIPPI, Primavera; POTTS, Jason. Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, v. 14, n. 4, p. 639–658, 2018.

DE FILIPPI, Primavera; LOVELUCK, Benjamin. The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. Internet policy review, v. 5, n. 4, 2016. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2852691>. Acesso em: 6 out. 2023.

EDQUIST, Charles. The Systems of Innovation Approach and Innovation Policy: An account of the state of the art. 2001, [S.l: s.n.], 2001. p. 12–15. Disponível em: <https://www.researchgate.net/profile/Charles-Edquist-2/publication/228823918_The_Systems_of_Innovation_Approach_and_Innovation_Policy_An_Account_of_the_State_of_the_Art/links/548177b90cf20f081e727cb6/The-Systems-of-Innovation-Approach-and-Innovation-Policy-An-Account-of-the-State-of-the-Art.pdf>. Acesso em: 6 out. 2023.

ERGAS, Henry. Does technology policy matter. Technology and global industry: Companies and nations in the world economy, v. 191, p. 245, 1987.

EYAL, Ittay; SIRER, Emin Gün. Majority is not enough: bitcoin mining is vulnerable. Communications of the ACM, v. 61, n. 7, p. 95–102, 25 jun. 2018.

GLAESER, Edward L. Learning in cities. Journal of urban Economics, v. 46, n. 2, p. 254–277, 1999.

GOERTZ, Gary. Social science concepts: A user's guide. [S.l.]: Princeton University Press, 2006. Disponível em: <https://books.google.com/books?hl=pt-BR&lr=&id=vwNxlyT-M94C&oi=fnd&pg=PR9&dq=Goertz,+G.+(2006).+Social+science+concepts:+A+user%27s+guide.+Princeton+University+Press.&ots=cSt03TlYe4&sig=YyQ2f2kZuKvFV7dVz95pTF88FBY>. Acesso em: 6 out. 2023.

GREENFIELD, A. Against the Smart City. New York, Do Projects. 2013.

HALL, Peter Geoffrey. Cities in civilization. [S.l.]: Citeseer, 1998. v. 21. Disponível em: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=4e6777445df5d497e15b10dac9dfc04a3a4deb22>. Acesso em: 6 out. 2023.

HSU, Chin-Lung; LIN, Judy Chuan-Chuan. An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. Computers in human behavior, v. 62, p. 516–527, 2016.

JOHNSON, Björn. Cities, systems of innovation and economic development. Innovation, v. 10, n. 2–3, p. 146–155, out. 2008.

KITCHIN, Rob; DODGE, Martin. The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. Journal of Urban Technology, v. 26, n. 2, p. 47–65, 3 abr. 2019.

KOMNINOS, N. et al. Smart City Planning from an Evolutionary Perspective. Journal of Urban Technology, v. 26, n. 2, p. 3–20, 3 abr. 2019.

KUK, George; JANSSEN, Marij. The business Models and Information Architectures of Smart Cities. Journal of Urban Technology, v. 18, p. 2–39, 2011.

LAMBOOY, Jan. The evolution of spatial patterns over long time-horizons: the relation with technology and economic development. The handbook of evolutionary economic geography, p. 471–486, 2010.

LETAIFA, Soumaya Ben. How to strategize smart cities: Revealing the SMART model. Journal of business research, v. 68, n. 7, p. 1414–1419, 2015.

LEYDESDORFF, Loet; DEAKIN, Mark. The Triple-Helix Model of Smart Cities: A Neo-Evolutionary Perspective. Journal of Urban Technology, v. 18, n. 2, p. 53–63, 1 abr. 2011.

MARIS, Koen. Privacy is not a currency. IOTA. [S.l: s.n.]. Disponível em: <https://blog.iota.org/privacy-is-not-a-currency-63018fc45920 2018.>. , 2018

MARTINS, Armando N.G.L; CIVITARESE, Jamil. The Precautionary Principle and Experimental Public Policy in the Developing World: An Application to Decentralized Ledgers Technologies. In: CONGRESSO INTERNACIONAL DE TEORIA DAS INSTITUIÇÕES: 30 ANOS DA CONSTITUIÇÃO, 2018, Rio de Janeiro, RJ. Anais... Rio de Janeiro, RJ: [s.n.], 2018.

MARTINS, Armando Nogueira da Gama Lamela. Quem tem medo do Bitcoin? O funcionamento das moedas criptografadas e algumas perspectivas de inovações institucionais. Revista Jurídica Luso Brasileira, Lisboa, ano, v. 2, p. 137–171, 2016.

MAYOR'S OFFICE OF INNOVATION SAN FRANCISCO. About the Mayor's Office of Innovation San Francisco. Disponível em: <https://sf.gov/departments/mayors-office-innovation/about>. Acesso em: 6 out. 2023.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES. Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil. . [S.l: s.n.]. , 2016

MONTRÉAL. Montréal Smart and Digital City. . [S.l: s.n.]. , 2014

MORETTI, Enrico. Human capital externalities in cities. Handbook of regional and urban economics. [S.l.]: Elsevier, 2004. v. 4. p. 2243–2291. Disponível em: <https://www.sciencedirect.com/science/article/pii/S1574008004800087>. Acesso em: 6 out. 2023.

NAKAMOTO, Satoshi. Bitcoin: A peer-to-peer electronic cash system. 2008. Disponível em: <https://assets.pubpub.org/d8wct41f/31611263538139.pdf>. Acesso em: 6 out. 2023.

NARULA, Neha. Cryptographic Vulnerabilities in IOTA. Medium. [S.l: s.n.]. , 2017

NELSON, Richard R.; WINTER, Sidney G. In search of useful theory of innovation. Research policy, v. 6, n. 1, p. 36–76, 1977.

NIEPOW, Daniel. Rail Insider-San Francisco's Muni hack: A case study in prepping for ransomware attacks. Information For Rail Career Professionals From Progressive Railroading Magazine. Disponível em: <https://www.progressiverailroading.com/security/article/San-Franciscos-Muni-hack-A-case-study-in-prepping-for-ransomware-attacks--50602>. Acesso em: 6 out. 2023.

PARTRIDGE, Helen L. Developing a human perspective to the digital divide in the'smart city'. 2004, [S.l: s.n.], 2004. Disponível em: <https://eprints.qut.edu.au/1299>. Acesso em: 6 out. 2023.

POPOV, Serguei. The tangle. White paper, v. 1, n. 3, p. 30, 2018.

POREMBA, Sue. San Francisco Muni Ransomware Attack Should Be a Warning to Critical Infrastructure. Disponível em: <https://www.itbusinessedge.com/security/san-francisco-muni-ransomware-attack-should-be-a-warning-to-critical-infrastructure/>. Acesso em: 6 out. 2023.

REICHERT, Corinne. Las Vegas announces smart city plans with Cisco | ZDNET. Disponível em: <https://www.zdnet.com/article/las-vegas-announces-smart-city-plans-with-cisco/>. Acesso em: 6 out. 2023.

ROSENBERG, Nathan. Inside the Black Box: Technology and Economics. [S.l.]: Cambridge University Press, 1982.

SCHOT, Johan; STEINMUELLER, W. Edward. Three frames for innovation policy: R&D, systems of innovation and transformative change. Research policy, v. 47, n. 9, p. 1554–1567, 2018.

SCHUMPETER, Joseph. Capitalism, Socialism and Democracy. New York, NY: Harper & Brothers Publishers, 1942.

SELADA, Catarina. Smart Cities and the Quadruple Helix Innovation Systems Conceptual Framework: The Case of Portugal. In: DE OLIVEIRA MONTEIRO, SARA PAULINA; CARAYANNIS, ELIAS G. (Org.). . The Quadruple Innovation Helix Nexus. New York: Palgrave Macmillan US, 2017. p. 211–244. Disponível em: <http://link.springer.com/10.1057/978-1-137-55577-9_8>. Acesso em: 6 out. 2023.

SHEPARD, Mark. Sentient city: Ubiquitous computing, architecture, and the future of urban space. [S.l.]: The MIT press, 2011. Disponível em: <https://dl.acm.org/doi/abs/10.5555/1972523>. Acesso em: 6 out. 2023.

SHY, Oz. The economics of network industries. [S.l.]: Cambridge university press, 2001. Disponível em: <https://books.google.com/books?hl=pt-BR&lr=&id=xgt0BTJ54MgC&oi=fnd&pg=PR11&dq=Shy,+Oz.+(2001)+The+economics+of+network+industries.+Cambridge:+Cambridge+University+Press.&ots=bW3cPhijYp&sig=72i0HwHfsH0_Zwx15x8_momAQik>. Acesso em: 6 out. 2023.

SIDEWALK LABS. MIDP Volume 0 The Overview. . [S.l: s.n.]. , [S.d.]

SMARTCITIESWORLD. Civil liberties association sues Canadian government over Sidewalk Labs' Toronto smart city. Disponível em: <https://www.smartcitiesworld.net/news/news/civil-liberties-association-sues-canadian-government-over-sidewalk-labs-toronto-smart-city-4092>. Acesso em: 6 out. 2023a.

SMARTCITIESWORLD. Waterfront Toronto panel member resigns over public trust. Disponível em: <https://www.smartcitiesworld.net/news/news/waterfront-toronto-panel-member-resigns-over-public-trust-3423>. Acesso em: 6 out. 2023b.

STEELE, Katie. The precautionary principle: a new approach to public decision-making? Law, Probability and Risk, v. 5, n. 1, p. 19–31, 2006.

SUNSTEIN, Cass R. Beyond the Precautionary Principle. University of Pennsylvania Law Review, v. 151, n. 3, p. 1003–1058, 2003.

SZABO, Nick. Bit gold, unenumerated. blogspot. com (Mar. 29, 2006) Internet Archive. Retrived from http://unenumerated. blogspot. com/2005/12/bit-gold. html, 2008.

TALEB, Nassim Nicholas et al. The precautionary principle: fragility and black swans from policy actions. NYU Extreme Risk Initiative Working Paper, p. 1–24, 2014.

THE ECONOMIST. The Global Liveability Report 2015. . [S.l: s.n.], 2015.

THE WORLD BANK. The World Bank Data: Urban population (% of total). . [S.l: s.n.]. Disponível em: <https://data.worldbank.org/indicator/SP.URB.TOTL.IN.ZS>. , 2016

TONAR, Remington; TALTON, Ellis. Why Sidewalk Labs' Toronto Plan Is Flawed. Disponível em: <https://www.forbes.com/sites/ellistalton/2019/09/26/why-sidewalk-labs-toronto-plan-is-flawed/>. Acesso em: 6 out. 2023.

US CENSUS BUREAU. QuickFacts: San Francisco County, California. . [S.l.]: US Census Bureau., 2018.

WATERFRONT TORONTO'S DIGITAL STRATEGY ADVISORY PANEL. DSAP Preliminary Commentary and Questions on Sidewalk Labs' Draft Master Innovation and Development Plan. . [S.l: s.n.]. , 2019

Recebido: 03 nov. 2024.
Aprovado: 27 nov. 2024.
DOI: 10.3895/rbpd.v14n2.18245
Como citar: MARTINS, A.N. G. L. Innovation policy design to scalable crypto-assets in urban public services. **R. Bras. Planej. Desenv.** Curitiba, v. 14, n. 02, p. 293-318, mai./ago. 2025. Disponível em: <https://periodicos.utfpr.edu.br/rbpd>. Acesso em: XXX.
Correspondência:
Armando N. G. L. Martins
Av. Pasteur, 250 - Botafogo, Rio de Janeiro - RJ