TO BE DIGITAL OR NOT TO BE

Florie Mazzorana, International University of Monaco, OMNES Education

ABSTRACT

Decentralized Digital Identities (DDIs) are poised to replace current national credentials. Based on blockchain technology, these new frameworks intend to take on a wide range of functions, among others: remote identification on the internet, self-control over personal data and marketing, standardization of travel passports, electronic voting, certification of school graduation, address for digital currencies and other activities and legal documents linked to our common social lives.

DDIs are a revolution that has many advantages. By simplifying and securely keeping identity records around the world, they reduce the risk of losing proof of citizenship, increase the economic potential of many services and jobs, and can greatly simplify access to social life. However, DDIs are likely to escape the control of national democracies. They also make individuals more vulnerable to powerful foreign states and private groups as these may require them to disclose a lot of personal data information in order to access services or territories.
Moreover, because they merge physical and digital existences, digital identities also multiply the means of controlling and tracing people, equating them with objects and products, which raises ethical questions.

Keywords: Digital Identity, Decentralized, Blockchain, ID2020, DDI, Global Citizenship, Digital Marketing.

INTRODUCTION

In today's world, the web and connectivity between people and devices have become more essential than ever. The Covid crisis has accelerated this trend, making digitalization the objective at all costs, in all sectors, both in the private and public spheres. At the same time, our movements in the real "physical" world have been restricted and - in many countries - conditioned on the presentation of QR codes. This is undoubtedly a first step toward digital identities and the fusion of our digital and physical existences. To be digital or not to be? may be the contemporary million-dollar question. No QR code, no valid digital identity, no movements nor social rights.

Many projects, led by Foundations, the United Nations or private groups, aim to replace our current legal systems with a global and decentralized digital one. In this new system the digital identities of all inhabitants of the planet are included in a blockchain, which makes possible their remote authentication (White et al., 2017; W3C, 2021).

As a result, digital identities may soon be required to access internet services, to receive money, to travel abroad, to receive health services, and even to go to school or vote. The advantages put forward by DDI technology providers and stakeholders are numerous: a DDI can give more security and control over the use of personal data, over confidentiality, over the transfer of future digital currencies. Also, it contributes to global inclusion, health and security.

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

Nevertheless, such systems are designed and promoted by private parties - even potentially altruistic ones - which influence international institutions such as the UN and the EU to advocate for a new generation of proof of identity going beyond national systems.

On the other hand, DDIs also present potential risks: they facilitate the tracking of individuals both on the internet and in their physical lives; they make them more vulnerable to lobbyists of governing institutions; they can quickly deploy restrictions on freedom. There is also a risk that individuals will be coerced into disclosing personal data to access essential services or, under regimes of terror like the Taliban or ISIS regimes, to prove their obedience.

In this article, we first introduce and develop the concept of decentralized digital identity and its underlying blockchain technology.
Then, we present the advantages and the threats posed by such an evolution of our legal identity systems.

Our analysis shows that, because they are defined and managed globally, Decentralized Digital Identity systems are very likely to escape the control of our national democracies. Also, because they aspire to encompass a full range of personal information to give access to common social services, they require full transparency from the institutions that manage them. Due to these concerns, the involvement of external foundations and private companies in the implementation of our new identity systems should be carefully considered.

From Traditional Proof of Legal Identity to Decentralized Digital Identities

The physical documents that validate the identity of individuals vary from country to country. They can be linked to key life events such as a birth, a wedding or divorce certificate. They can also be linked to a national identification number such as an identity card or passport. (United Nations ESCAP, 2021).

The Importance of Legal Identity

Legal identity is a fundamental element of human rights because it recognizes the existence of people, their right to reside in a specific geographic area, and enables them to claim justice in national courts. It also standardizes the recognition of individuals, which helps the State better organize social life.

For this reason, the United Nations has made as a priority objective of the 2030 agenda "*to provide legal identity for all, including birth registration*" (Agenda 2030, UN, objective 16.9). *Identity documents are the "gateway to unlocking other rights*" (Dahan 7 Gelb, 2015). Without proof of identity, people are at high risk of social exclusion. However, achieving goal 16.9 of Agenda 2030 involves developing digital solutions to support birth registration and secure proof of existence in order to preserve access to fundamental social rights.

Toward Decentralized Digital Identity

In its simplest definition, identity is proof of existence and citizenship. In its extended and contemporary version, it also encompass a digital footprint that can include physical characteristics, social status (advanced degrees), health status (such as vaccinations) and social rights. An ideological shift in social policies has recently taken place, emphasizing the need to provide individuals with documentation - and more recently digital tools - to make them easily identifiable by international actors, states, and increasingly, financial institutions (World Bank

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

Legal Review, 2016) while preserving their rights. In the most advanced projects of digital identity, key objectives are to enable remote authentication through the web, to prevent problems of identity theft, to preserve copyright, data compensation and limit unwanted disclosures of personal information. Another objective is to guarantee refugees and people from underdeveloped countries the assurance of retaining proof of existence and citizenship throughout their lives.

The most well-known DDI system under development uses blockchain technology. It is promoted by the United Nations and developed by the public-private partnership ID2020, and it includes a wide range of functions. The ID2020 alliance was created in 2014 by Microsoft, Accenture, the Rockefeller Foundation, IDEO and the Gavi Vaccine Alliance. It now brings together many other foundations and private companies such as Mastercard, Kiva, Mercy Corps, Grameen, IBM-Hyperledger and more recently Facebook. In May 2016, the ID2020 alliance initiated a summit at the United Nations headquarters to discuss how to provide a digital identity to everyone and how blockchain technology could help achieve this goal. Over the following years, the foundation worked on solutions enabling digital identities, including, most recently, the digital health pass for the Covid vaccine.

To better understand what's at stake in this technological evolution, let's first introduce block chain technology and present the ID2020 Decentralized Digital Identity Framework.

Blockchain Is an Efficient Technology to Provide Secure and Easy Access to Anyone's DDI

Current forms of recognition rely on central authorities that issue and validate personal credentials and national identity documents. As a result, according to the United Nations, more than a billion people in the world, mainly in developing countries, do not even have proof of their existence and cannot participate in society.

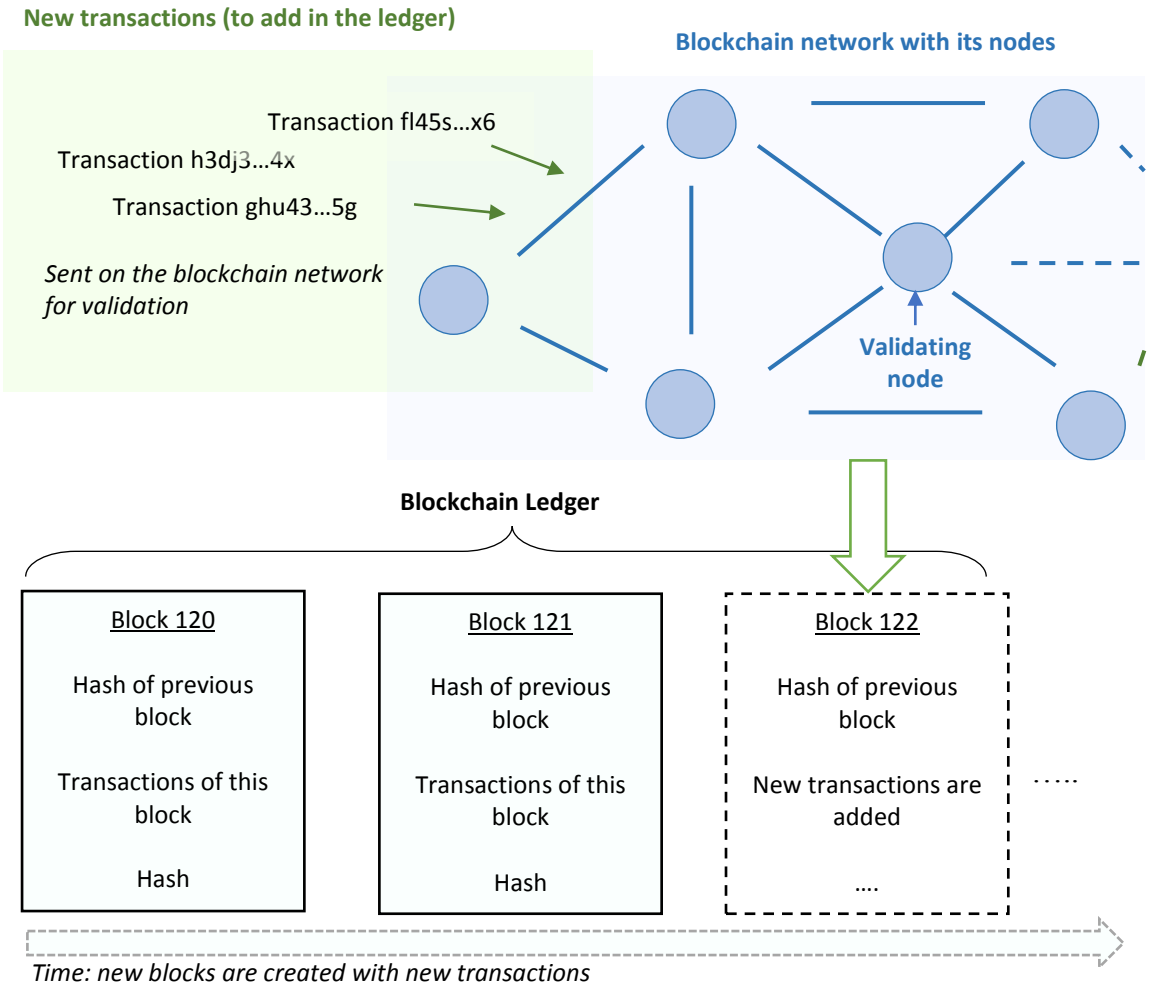
A secure and decentralized identity system is proposed to solve this problem: more precisely, a global database shared by several organizations and states in which people are registered at birth or using vaccine injections as an "*entry point*" for those already born: indeed, immunization also "*poses a huge opportunity to scale digital identity*" (ID2020, 2018). From such a perspective, the integrity of the registry's content is fundamental, and this is where the blockchain comes in.

Blockchain technology is mainly known to the public thanks to the popularization of Bitcoin. The digital currency also known as cryptocurrency consists of a peer-to-peer shared database, which regularly includes new transactions validated by millions of participants. More precisely, it relies on the sharing and synchronization, by the latter, of a ledger that contains all the history of bitcoin transactions. This ledger is updated every 10 minutes by adding a new block which contains new bitcoin transactions. Because it is built in the form of successive blocks, it has been called "*blockchain*". The immutability of a blockchain ledger is both ensured by the high number of network participants that validate the transactions and by a cryptographic fingerprint – called hash (Haber & Scott, 1997) – which is added at the top and bottom end of any new block. This "*hash*" makes it easy and quick to verify that no past transaction has been changed in the shared ledger.

Since the creation of Bitcoin, other types of blockchains have emerged, paving the way for a wider field of applications. For example, the Ethereum blockchain enables the execution of programs (called "*smart contracts*") in a decentralized manner and records their states and outcomes in its successive blocks (Bartoletti et al., 2017). Some blockchains are public (anyone

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

can review their content or contribute to validate the available information) and others are private or semi-private which means that only authorized companies or people can access information and/or validate it Figure 1.



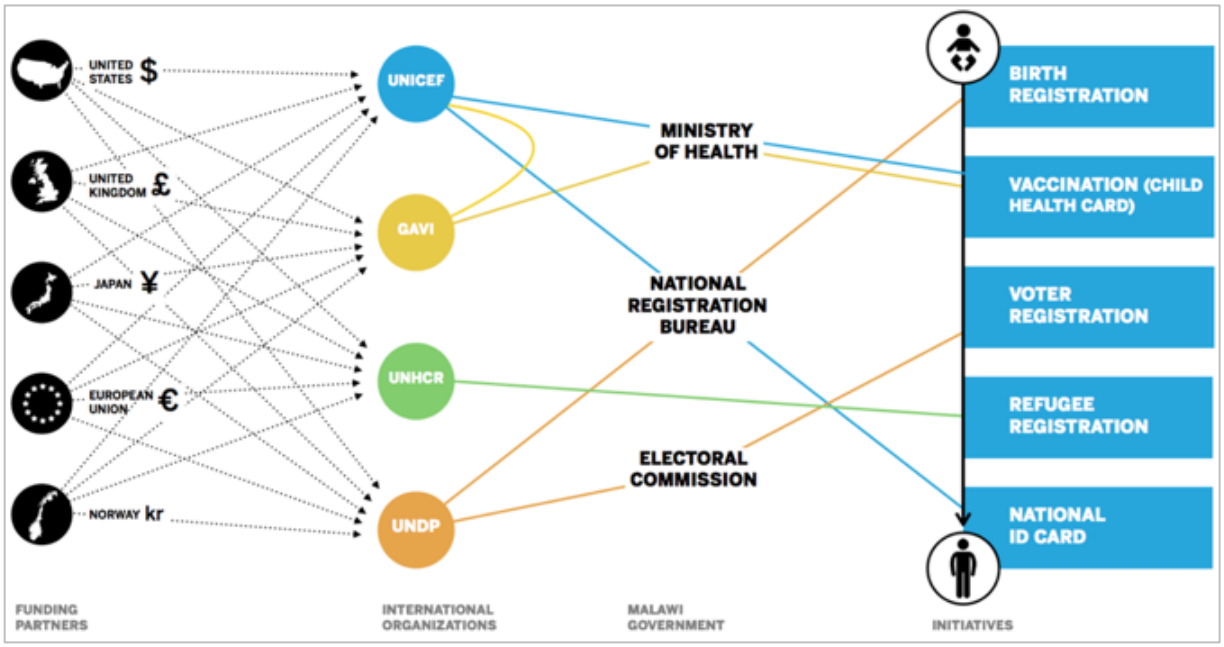
Source: authors

FIGURE 1
ILLUSTRATION OF A BLOCKCHAIN NETWORK WITH ITS VALIDATING NODES

The tamper-proof and immutable nature of blockchains have sparked enthusiasm in several industries. In particular, because it enables immediate control of information and makes modifications almost impossible, it has been seen as an ideal solution for organizing the traceability of food products or components throughout supply chains (Lacity & Van Hoek, 2021).

Likewise, some companies and international organizations Nakamoto (2009) have seen it as a powerful and providential tool for organizing and controlling identities on the planet and on the web. Indeed, in the field of identity, the blockchain is intended to be semi-private and distributed globally, managed mainly by countries and international organizations. However, in the ID2020 solution, some private companies and foundations may also be allowed to contribute to its management Figure 2.

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.



Source: ID2020 Presentation. Posted by Accenture. Date: 2017

FIGURE 2
CONTRIBUTORS TO THE GLOBAL LEDGER OF DIGITAL IDENTITIES SEEN FROM ID2020

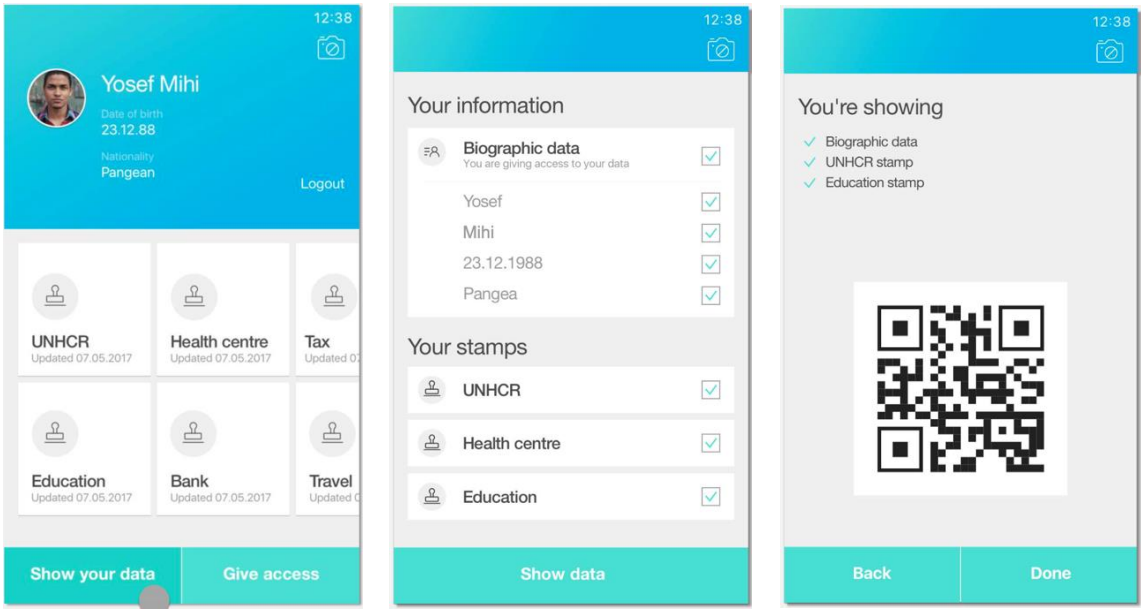
Enhanced Decentralized Digital Identities

The ID2020 and UN initiative goes much further than the sole management of proof identity.

First of all, it enables access to and the sharing of personal information, without the worry of using or losing paper documentation. The DDI blockchain system includes or connects to a biometric system that manages fingerprints, iris scans and other data of similar nature[1].

In addition, to better support individuals in their travels and daily life, it also integrates information related to their social life, transforming digital proof of identity into a complete digital personal wallet. For example, in the Yosef digital credentials shown in Figure 3, education level, refugee status, and bank account information are also linked to his digital wallet. In such a solution, DDIs are more than just proof, they become the key for accessing professional life, social services, for paying taxes or receiving money.

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.



Source: ID2020 Presentation. Posted by Accenture. Date: 2018.

FIGURE 3
CONTENT OF INDIVIDUAL DIGITAL IDENTITY SEEN FROM ID2021

Such wallets also intend to condition access to social life and services in function of personal status: for example, refugee status, or vaccine status required to go to school (ID2020, 2019).

Thus, the concept of identity management has evolved in recent years, moving from a national identity concept to a connected global identity system aimed at managing the entire social life of people. This shift is a revolution that calls for questioning both the advantages and the threats it can represent Figure 3.

In the following parts of this article, we review the advantages and threats of DDI systems and highlight its major contemporary challenges.

Advantages: Trust, self-appropriation of identity and worldwide standardization

As advanced by the United Nations and many promoters of DDI projects, decentralized digital identification has many advantages: it guarantees trust in transactions and communications on the Internet; it reassigns ownership of the data to their actual owners; it can improve social inclusion and individual protection; it represents a significant potential economic value.

Trust

The first well-known advantage of DDIs is to limit security breaches in data protection and fraudulent identification. Digital identities are necessary to ensure that people can trust online

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

service providers and vice versa. Indeed, by way of illustration: companies must ensure that outsiders cannot access their sensitive information, in particular when working remotely; banks need to ensure that the right people are accessing and using their digital financial assets and services; governments try to avoid fraud and facilitate access to social services in their country.
An increasing part of our life is digital and passes through the Internet. However, people use many passwords and IDs across multiple platforms, leading to an increase in fake identities and associated fraudulent activity. From this point of view, a digital identity would bring a lot of trust to the Internet.

Emancipate from Tech Monopolistic Positions and Digital Slavery

The second benefit of DDIs, mainly related to their decentralized and blockchain nature, is that they reassign ownership of data to their actual owners. Internet today is dominated by the "Big Five" (Apple, Facebook, Amazon, Google and Microsoft), who have the possibility to make fortunes through the use of their users' personal data. Indeed, we provide them with personal information for free, in return for which we receive access to their applications and services. We can log out and leave their platforms at any time but, while doing so, we leave everything behind: information about us, our contact details, our notes, our ratings, our posts and our digital representation on these networks. In practice, we have no ownership rights on the data we generate (Snower, 2018). We also ignore how this information is used and we are subject to aggressive and targeted advertisements, remaining powerless in front of these global digital monopolies. At the Global Solutions Initiative Summit in 2018 in Berlin, German Chancellor Angela Merkel called for a new system of data ownership rights and suggested that digital data be priced by its true owners (Snower et al., 2018). For such a revolution to be possible, identifiers must be associated with Internet connections, and (financial) wallets with personal information. Additionally, digital identities must work in all countries and jurisdictions, requiring a decentralized global solution that can be used for every transaction.

As a result, decentralized digital identities appear to be necessary if we are to make this new kind of data economy possible.

Social Inclusion

Inclusion is a core aspiration of the 2030 Agenda, in which giving everyone and everywhere a digital identity is one way to achieve it. According to the World Bank and the United Nations, social inclusion is "the process of improving the conditions for participation in society for people who are disadvantaged (for example by their age, sex, disability, race, ethnicity, origin, religion or economic status) through improved opportunities, access to resources, voice and respect for the law" (DESA, 2016). In this sense, it is not only an objective but also a process, which requires both:

1. fight against social exclusion, by removing obstacles to people's participation in society, including certain discriminatory policies and attitudes and behaviors
2. and to take active inclusion measures to facilitate this participation.

"*Fair and robust systems of legal identity and birth registration are recognized in the new 2030 Agenda for Sustainable Development as an important foundation for promoting inclusive societies*" (DESA, 2016). In fact, proof of identity is essential in most countries to access school,

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

health services, etc. People unable to prove their identity cannot claim their rights and access legal services.

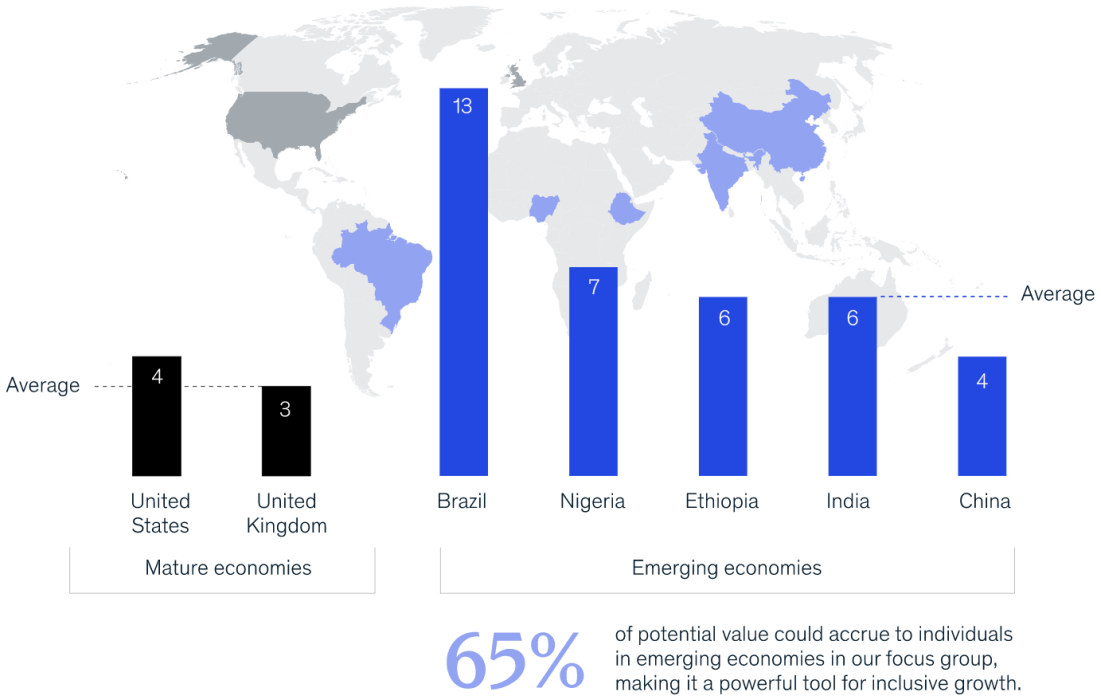
Thus, a digital identity solution managed by a global group of nations and institutions seems to offer more guarantee to always keep track of existence and citizenship.
It can also facilitate the continuity of access to services and social life for all citizens. For example, in Estonia, around 30% of people vote online, of which 20% say they would not vote in a polling center (White et al., 2017). In addition, a digital ID coupled with an accurate and up-to-date death registration system can help maintain a reliable and authentic voter register, which is essential to ensure the overall integrity of the electoral process. To further illustrate how DDI can improve social life and protect individual rights, in India, the right of residents to claim subsidized food at ration shops is guaranteed because their identity and claim are authenticated through a remote digital ID system, rather than at the discretion of local authorities.
However, such access in a nation depends above all on the policies enforced, and this inclusion only becomes a reality if said nations treat their individuals fairly, without discrimination or segregation.

Unlock Economic Value

Using a digital ID on the web and remotely can increase the use of financial services, improve access to employment, increase agricultural productivity and help save time. It can also help reduce costs, fraud, increase sales of goods and services, improve labor productivity, and efficient tax collection.

Indeed, to illustrate this potential positive shift, many people in society are excluded from digital financial services due to a lack of formal ID (GSM, 2021). Opening a financial account that requires one's identity to be verified in person puts those living outside urban centers at even greater risk of financial exclusion if mobile network operators or banks do not have a physical presence in the area. Similarly, a robust, government-recognized ID can help smallholder farmers in under-developed countries, formally register land and livestock, and access mobile, financial, and other services that would allow them to work, sell, and spend income formally (Worldbank, 2018). Digital ID systems are also efficient national system to fight against social fraud: indeed, combined with accurate and up-to-date death registration systems, it become easier for states to quickly identify social protection fraud.
According to the Digital ID Report from Mc Kinsey, by 2030, digital ID could create an economic value equivalent to 6 % of GDP in emerging economies and 3 % in developed ones, assuming high levels of adoption Figure 4.

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.



Note: Average is calculated over the range of 23 mature and emerging economies in our analysis. Value estimates assume the digital ID program enables multiple high-value use cases, attains high levels of adoption and usage, and has the attributes required of good ID, including that it is established with individual consent, protects user privacy, and ensures control over personal data.

Source: Mc Kinsey, "*Digital Identification, a key to inclusive growth*". Date: 2017.

FIGURE 4
INCREASE IN ECONOMIC VALUE BY 2030, % OF GDP

Threats Object-Like Humans, Over-Control, and Corporate Increased Influence Over States

Decentralized Digital IDs represent a technological shift that can be used to create value or cause damage They confer unprecedented privileges to the public and to a few designated private actors in the access and control of personal data.

In the solutions under development, national states are losing control over the digital identifiers of their populations. As simple nodes, they count barely more in the maintenance of the database than the private actors or the international organizations involved. Thus, the DDI system in motion escapes the democratic control of the individuals it controls.

History provides sad examples of abuse of traditional identification programs, including the tracking or persecution of ethnic and religious groups. Digital identification, if poorly designed, could be used in even more targeted ways against the interests of individuals or groups by governments. It can also be used to influence people or limit their freedom according to the objectives of private companies.

Many potential reasons could motivate a diversion, among others: financial gain from the disclosure and use of personal data, political manipulation, social control and apartheid by monitoring and restricting access to payments, travel, social media, and essential social services like schools, hospitals or libraries.

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

Is the QR-Readable Human A new Kind of Product whose behavior has To Match Business Plans Projections?

The global market for Identity and Access Management tools and solutions is expected to reach $29.79 billion by 2027, while the global identity verification market is expected to reach $17.8 billion by 2026 (Renieris, 2021). One major issue raised by this technical emergence of technology in the management of our identities and movements, including in the case of pandemic tech, is that democracies barely control it. They even outsource to private companies and industry consortia their national strategy and the decisions they make. But potential abuse or failure in systems like DDIs have important consequences for people. We must consider that the economic model of private companies, despite being initially well-intentioned and involved in such a human-sensitive topic, remains the maximization of profits. As a result, there is a high risk of diversion and of placing human consequences on the backburner.

From this point of view, it becomes a concern to note that the promoters of current DDI projects are private actors whose target markets are, among others: the business of cloud-data, IA, digital, identity and security solutions (Microsoft), credit card transactions and wallet payments (Mastercard), or the distribution of drugs and vaccines (Gavi foundation and associated members). Accenture also, one of the initial founders of the ID2020 alliance have recently acquired Novetta (Accenture, 2021), an analytics company serving U.S. Federal organizations and positioned on machine learning, cyber engineering and information exploitation to assist defense, intelligence and law enforcement organizations as well as companies of any sector. At the same time, they advise and have a "long-standing partnership with the UN Global Compact and advancement of the UN Sustainable Development Goals". Similarly, Microsoft commercializes its Azure AD which includes cloud-based identity and access management solutions.

Thus, the designers and political advisers of DDI systems are also those who take stakes in their related markets. Even though their skills may be required, they can also greatly influence institutions and advocate for the need for their solutions for no good reason. It becomes thus legitimate to wonder whether, in current digital identification solutions, humans are not likely to become profit-units of the business models of large influential companies and treated as so. This means that the tool allowing humans to move around or connect to services could also be used to influence them - or even coerce them - in a way that is consistent with the business plans of powerful companies.

The Ultimate Tool for the Success of Totalitarianism and Terror

According to Anah Arendt, totalitarian regimes go further than autocratic regimes in the sense that they not only seek to gain absolute political power and ban opposition, they also want to dominate all aspects of everyone's life (Arendt, 2007).

Research has already warned of the risks associated with population data systems in human rights violations (Seltzer & Anderson, 2001). A recent illustration is the case of Afghanistan (Vallance, 2021) with the Taliban inheriting the digital and biometric identity database created by development aid missions. The World Bank has long pushed for the adoption of digital identity systems in Afghanistan, providing technical advice and direct funding to the government.

The Bank argued that digital identity tools would lead to more inclusion, especially for women. As a result, name, date, place of birth, but also unique identification number has linked

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

each person to a biometric profile kept by the Afghan Ministry of the Interior (Jacobsen, 2021). Many other personal details such as the family tree or even the belonging to a particular tribe have been included. Even the names of those who worked for U.S. and coalition forces could be found.

Now, these tools can help the Taliban retaliate against people who collaborated and monitor women's participation in daily life. This is a clear example of why the mandatory collection of extensive and biometric data can be dangerous.

Risk of Exclusion

Inclusion is a core aspiration of the 2030 Agenda and "giving everyone everywhere a digital identity is one way to achieve it". Nonetheless, even pursuing this goal, the UN recognizes that conceptual and analytical work on what constitutes inclusion, as well as efforts to improve data availability, is still needed. In his book "Permanently foreign", Hayes de Kalaf (2018) shows how modern digital identity systems initially designed to include Dominicans for social life also resulted in exclusion.

More specifically, the author shows that, at the lower level, state-led practices have been developed to refuse to reissue to Haitian descendants the documents required to be included in these systems. As a result, they could no longer access health services, welfare and education.
Other examples showing that the systematic use of digital identifiers can limit inclusion also exist in the FinTech industry. For example, in Africa, innovative payment projects like M-Pesa have made a significant contribution to financial and social inclusion. These types of fintech solutions help fight poverty, precisely because they don't require formal identification, but rather a simple phone number or email address. The same phenomenon of inclusion has been fostered in some countries by cryptocurrencies, allowing cross-border financial flows even for the poorest and most deprived people, absent from national registers and banking systems. Introducing digital identity control in such innovations would again exclude these populations.

The Control of Opinions and Apartheid

One concern this raises is that legal identity, especially when combined with other characteristics such as immunization status, voting, school, gender, ethnicity ... can also be used as a bureaucratic tool to determine the political community to which we belong and the set of rights we can access (de Kalaf, 2018, p.9). Indeed, "social policy which encourages the improved targeting and identification of populations can also increases the visibility of 'undesirable' individuals to authorities."

Thus, the provision of proof of identity, for any social activity and for any movement in the real world and the digital world, opens the door to new types of human societies:
First of all, censored content can now be associated with the individuals at its origin. In such a world, it is no longer possible to read or post content without revealing one's identity. Also, an unwanted publication could be immediately followed by the denial of access to social networks or web services.

Second, if we make these digital identifiers mandatory to access common infrastructure and places of social life, censorship and restrictions on freedom could extend to the physical world. By way of illustration, in France and Italy, the current green passes to fight against covid use the DDI systems under development. They have the option of blocking access to libraries, cinemas, gymnasiums and public places to people without a valid QR code. It is easy to imagine

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

that, in the same way, these digital identifiers could be reconfigured according to other criteria to prevent some people from accessing these places of everyday life Figure 4.

In such societies, humans would no longer be truly free anywhere, having to make sure every moment in their minds that they behave as intended. All gestures and behaviors could be traced and identified, as well as opinions. Our world would also become a world of real identities but completely false behaviors.

Conclusion

Enthusiasm for Decentralized Digital Identities, in particular for the economic benefit they represent, should not mask the many ethical questions they raise. Conditioning access to social life and right to move around the use of digital identity wallets requires total integrity on the part of the public authorities and private groups that drive these new ecosystems.

To illustrate this matter, an observational study (Wouters, 2020) found that between 1999 and 2018, the pharmaceutical and health products industry spent $4.7 billion lobbying the U.S. federal government, contributions to presidential candidates, and legislative and party committees. The same is true in the European Union and in other countries, and in other industrial sectors. Social life, politics and politicians have almost always been influenced by private groups. As a result, offering the option to condition people's lives and social rights in such an intrusive way appears excessive and could quickly lead to dramatic abuse.

In this perspective, the measures promoted by the UN and related international institutions could fall into the caricature described by Scott (2008), measures disconnected from the diversity of realities. This observation raises questions because, according to the Scott's thesis, the more a human project is global and tends to standardization, the greater the disaster to come.

Without denying the possible advances that a DDI can bring, we draw attention to the risks also posed by strategies aimed at providing everyone, everywhere, with legal and digital proof of identity. In particular, because the solutions proposed today aim to associate this identifier with access to the services of everyday life.

Too little empirical research has been conducted on the impact these measures can have on citizens and their basic social rights. Digital identity can be both an inclusive and an exclusive tool for accessing social rights. Before the economic and political world anticipates this revolution too quickly, it becomes urgent to conduct a thorough investigation of all the human implications that these tools imply, and not to limit it to only questions of security and improvement of the performance of our human societies.

ENDNOTES

[1]https://www.accenture.com/bg-en/insight-blockchain-id2020

REFERENCES

Accenture, (2021) "2021 Letter to Shareholders". https://www.accenture.com/be-en/about/company/2021-letter-shareholders-full-text

Arendt, H. (2007) The origins of totalitarianism. Duke University Press, 2007.

Bartoletti, Massimo, & Livio., P. (2017) "An empirical analysis of smart contracts: platforms, applications, and design patterns." International conference on financial cryptography and data security. *Springer*, Cham.

Dahan, M. & Gelb, A. (2015) The Identity Target in the Post-2015 Development Agenda: Enabling Access to Services for All. Washington, DC.

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.

DESA, UN. (2016) "Leaving no-one behind: The imperative of inclusive development." 2016 report on the World Social Situation. New York, NY: UN. Retrieved from https://www. un. org/esa/socdev/rwss/2016/full-report. pdf (2016).

Hayes., De., Kalaf, E.L. (2018) Making Foreign: Legal Identity, Social Policy and the Contours of Belonging in the Contemporary Dominican Republic. [Staff Thesis].

ID2020 (2018). Article: "Immunization: an entry point for digital identity" https://medium.com/id2020/immunization-an-entry-point-for-digital-identity-ea37d9c3b77e , 18 March 2018.

ID2020 (2019). "ID2020 at a glance". ID2020, website report. Published on the 18 December 2019. https://id2020.org/uploads/files/ID2020-Alliance-Overview.pdf

GSM Association. (2021) "Digital Identity: Accelerating financial inclusion during a crisis". March 2021. https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2021/03/Digital-Identity-Accelerating-Financial-Inclusion-During-a-Crisis.pdf

Haber, S., & Scott, S. (1997) "Secure names for bit-strings." Proceedings of the 4th ACM Conference on Computer and Communications Security.

Jacobsen, A. (2021) First Platoon: A Story of Modern War in the Age of Identity Dominance. *Penguin*, 1.

Lacity, M., & Remko, V.H. (2021) "What We've Learned So Far About Blockchain for Business." *MIT Sloan Management Review 62*.3: 48-54.

Nakamoto, S. (2009) "Bitcoin: A peer-to-peer electronic cash system Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin. org. Disponible en https://bitcoin. org/en/bitcoin-paper (2009)

Scott, James C. (2008) Seeing like a state. yale university Press, 2008.

Seltzer, W. & Anderson, M. (2001) 'The Dark Side of Numbers: The Role of Population Data Systems in Human Rights Abuses', *Social Research, 68*(2), 481–513.

Snower, D.J. "The Digital Freedom Pass: Emancipation from Digital Slavery." VoxEU. org 22 (2018).

Snower, D.J., et al. (2018). *Global Solutions Journal*. G20/t20 Argentina 2018 Special. Volume I Issue 2 September 2018. https://www.ifw-kiel.de/fileadmin/Dateiverwaltung/IfW_Unit/Global_Challenges_Center/Text/GlobalSolutionsJournal_2_2018_E-Reader.pdf

United Nations. ESCAP/77/13. Seventy-seventh session. Review of the implementation of the 2030 Agenda for Sustainable Development in Asia and the Pacific and issues pertinent to the subsidiary structure of the Commission. 9 February 2021.

Vallance, C. (2021) "Afghanistan: Will fingerprint data point Taliban to targets?". CNBC. 20 august 2021

White, O., et al. (2017) Digital identification. A key to inclusive growth. McKinsey Global Institute.

World Bank Legal Review (2016) Financing and Implementing the Post-2015 Development Agenda: The Role of Law and Justice Systems. 7. Edited by F. Fariello, L. Boisson de Chazournes, and K. E. Davis. Washington, DC: International Bank for Reconstruction and Development / The World Bank.

World Bank. (2018) The Role of Digital Identification in Agriculture: Emerging Applications. World Bank, 2018.

Wouters, O.J. (2020) "Lobbying expenditures and campaign contributions by the pharmaceutical and health product industry in the United States, 1999-2018." *JAMA internal medicine 180*.5: 688-697.

W3C (2021). Decentralized Identifiers (DIDs) v1.0. W3C Proposed recommendations.

Citation Information: Mazzorana, F. (2022). To be digital or not to be. *Academy of Marketing Studies Journal, 26*(S1), 1-13.