

Sep 09:31 boot
Sep 15:50 dev
Sep 09:32 etc
Sep 15:52 home
Sep 2015 lib -> usr/lib
Sep 2015 lib64 -> usr/lib64
Jul 10:01 lost+found
Aug 22:45 mnt
Sep 2015 opt
Sep 15:52 private -> /home
Sep 08:15 proc
Aug 15:37 root
Sep 15:50 run
Sep 2015 sbin -> usr/sbin
Sep 2015 srv



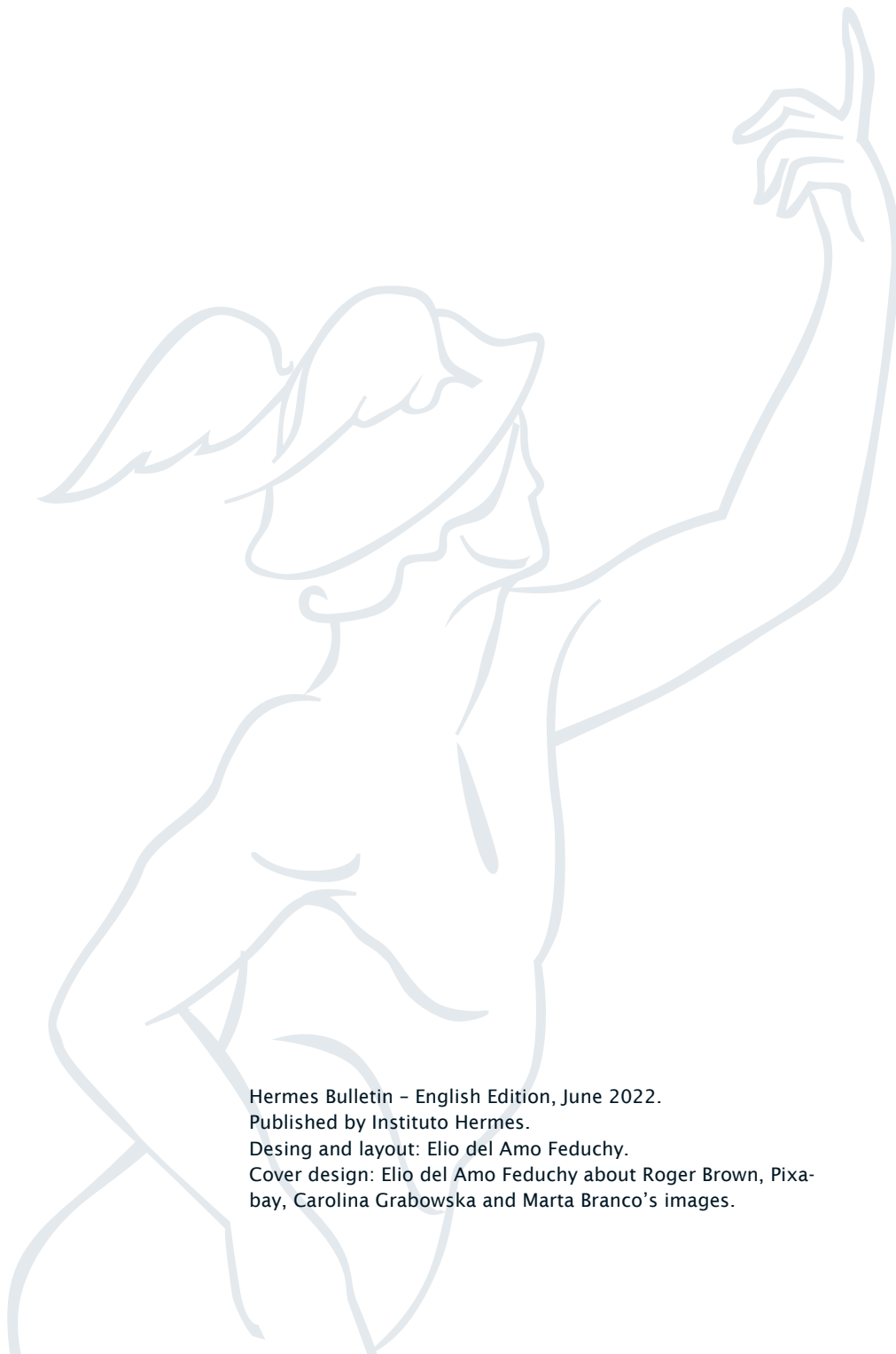
Instituto
Hermes

Derechos de ciudadanía digital



Hermes Bulletin

Year III • nº 9 • June 2022



Hermes Bulletin – English Edition, June 2022.

Published by Instituto Hermes.

Desing and layout: Elio del Amo Feduchy.

Cover design: Elio del Amo Feduchy about Roger Brown, Pixabay, Carolina Grabowska and Marta Branco's images.



Index

Hermes Bulletin – English Edition

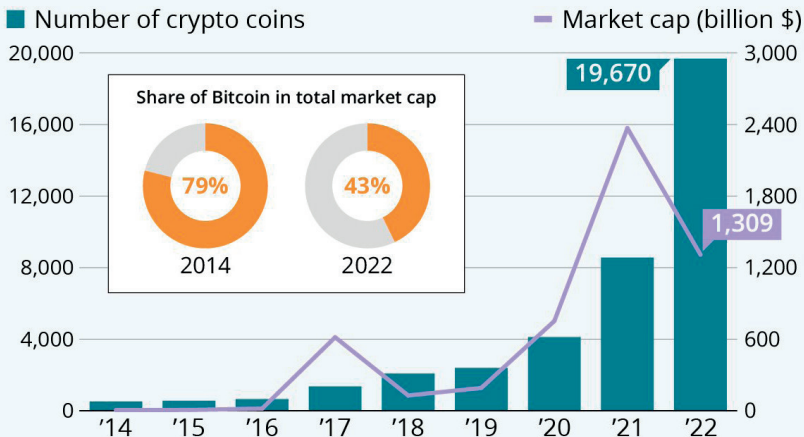
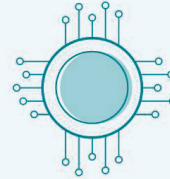
- Cryptocurrencies: Should we let them crash or prevent the disaster so as not to lose control? 2
- French Presidency of the EU: Launching the digital decade..... 5
- Emirates: A China in the Western World?..... 7
- Digital detoxification in Japan..... 8
- EU Digital Product Passport 9
- SMEs and cybersecurity 10

- Our Recommendations 11**
 - Report..... 11
 - Scientific articles and references..... 12
 - Book 13

Cryptocurrencies: Should we let them crash or prevent the disaster so as not to lose control?

The Evolution of the Crypto Economy

Total number of cryptocurrencies and overall market capitalization*



* At the end of the respective years from 2014 to 2021, May 31 for 2022.

Sources: Statista Digital Economy Compass 2022, CoinMarketCap



statista

In May 2022, a dress rehearsal for a cryptocurrencies “crash” took place. Luna lost 97% of its value in the course of just 24 hours. Bitcoin, the original cryptocurrency, peaked last November and has since declined in value by more than 50%. U.S. municipal cryptos, the latest hype, have fared no better: MiamiCoin is down more than 90% from its peak, and NewYorkCityCoin is down more than 80%. “Stablecoins,” which are “neither stable nor a coin,” as Nobel prize-winning economist Paul Krugman noted in his Times subscriber newsletter, have met the same fate. Proponents of cryptos, the latest expression of the techno-libertarian current that has been so important in digital culture since its origins, claim that cryptocurrency crashes have occurred before -with bitcoin- and that speculators who weathered the bump ended up making capital gains.

But it is hard to imagine how. The famous bitcoin recoveries were the result of the arrival of speculative funds that were attracted by rapid price surges and encouraged by an expansive monetary policy that generated immense pockets of cheap money in search of a destination.

Crypto prices went up again once investment funds reached a ceiling. This time cryptos were pulling in the savings of a less educated, middle- and low-income public. This public invested their savings after being enticed by celebrity commercials and SuperBowl advertising.

The May crash, however, has alienated both audiences and with good reason. This is because capturing an investor profile that is poorer than the average for a high-risk investment generally means losing that investor when prices fall and his/her savings disappear. After all, these investors are less prepared than the average individual investor to manage losses.

If we take speculative demand out of the equation, we find that there is no “real” demand for cryptocurrency. That is, there is no underlying economic uses for which someone would want to purchase any type of currency to, for example, import furniture, fruit or oil. After all, it is not as though cryptocurrency is used to cover production and labor costs. The only national economy that bet on converting a cryptocurrency, bitcoin, into a generalized medium of exchange was El Salvador. It is not a great power and neither was a revolution in the currency market expected. But the result, in any case, was a disastrous failure for the Salvadoran economy and public accounts. It is not likely that other governments will want to follow in its wake.

With that being the case, the only real economic activity which regularly involves cryptos are cybercrime and money laundering.

In early June, the US Federal Trade Commission reported that “about one of every four dollars reported lost to fraud” were lost due to cryptocurrencies. But, as Europol recently reported, even in these sectors, the volatility intrinsic to a pure speculative asset is such that cybercriminals tend to, not only limit their use to ransomware and international transfers, but to purchase state-guaranteed international currencies as soon as they can.

Beyond the sophistication of black money, there is nothing. Nothing? Nothing.

It sounds extreme and implausible to suggest that an asset class that has become so large, whose promoters have acquired so much political influence, could lack any real value: that it is a house built not on sand, but on nothing at all.

But I remember the housing bubble and the subprime crisis. And if you ask me, we seem to have gone from the Big Short to the Big Scam.

Paul Krugman

So, we confront the real question of whether we should let cryptocurrencies go through new cycles of expansion among ever poorer and less educated audiences before crashing again and again, or whether we should intervene in order to stop this from happening.

The technical inefficiency and unnecessary nature of blockchain, its disproportionate consumption of electricity, its brutal impact on the environment, and its more harmful social effects (cryptosects, addiction, etc.), would suggest the latter.

In April 2022, the Indian government imposed a 30% levy on profits derived from investment in cryptocurrencies and NFT's (Non Fungible Tokens). This action led to a 70% plunge in trading volume on the country's major cryptocurrency exchanges, along with the loss of an estimated 50% of the value of several cryptocurrency trading companies.

Despite the strength of the blow, and despite the support of notable Indian politicians who insist that "banning cryptocurrencies is the best thing that could be done for the country," the numbers are still coming in for some cryptocurrencies. There are still "cryptominers" who, with an electricity system on the ropes, emit CO2 on account of Indian imports of Russian oil.

The question in countries like Spain however, is posed differently. Indian fiscal policy directed against cryptocurrencies could be an example to follow for Spain, especially since, in contrast with India, it does not suffer from relevant clandestine mining.

Some could object, however, that it is "too late". On June 13 Binance, the largest online cryptocurrency exchange, joined Celsius and "paused" Bitcoin convertibility. As a result, the price of Bitcoin plummeted to its lowest point since December 2020. It was an 18% drop that wiped out years of investment in one fell swoop. The news started off a bad day

in the stock market. Subsequently, throughout the rest of the day, the headlines switched their attention to global downtrends and their underlying causes.

Neither the danger nor the existence of cryptos, however, will cease with another steep price drop. Cryptos of course lose, during these drops, thousands of investors whose personal wealth has been damaged and who are ashamed of not having seen the fall coming. But thousands more will come. There is too much invested in exchange platforms and too many advertising budgets already approved for the crypto world for it to cease to prey on new victims. More and more of these new victims are less educated and increasingly desperate. Many of them repeat ad nauseam in cryptoforums that they need a “lucky break” in order to “re-gain their freedom”.

That is why it is never too late to establish a national policy that takes up the banner of investor protection for this type of asset. A tax such as the Indian one of 30% on profits, added to the usual charge on income, could be sufficiently dissuasive to reduce social risk and minimize “infection”.

French Presidency of the EU: Launching the digital decade

France held the rotating presidency of the European Council from January to June 2022. President Macron had stated that laying the foundations for a digital governance that would establish the **EU as a global digital power** was included among his objectives.

During this period, the European Parliament and the Council reached a political agreement on the proposed **Digital Services Act** (DSA), which complements the political agreement of March 22 on the Digital Markets Act.

The DSA aims to create a safe and responsible online environment. It contains measures to counteract illegal online content, to empower users and civil society, and to assess and mitigate risks arising from the excessive concentration of power of large digital platforms.

Despite the opposition of large platforms such as **Meta**, which had even gone so far as to threaten to leave Europe, the **DSA** has already proven to be an international reference. It has been hailed by **President Obama** as “**the model to be followed**” by the US.

The French Presidency has also left its mark on **digital relations with the United States**. In June, the Union joined the United States and several international partners in presenting a “**Declaration on the Future of the Internet**”. This first step towards a digital Western bloc advocates an open, free, global, interoperable, reliable and secure Internet. The signatories affirmed their commitment to protect and respect digital rights as well as human rights in the online world.

The growing federalization of digital development policy, however, was a less positive outcome of the French presidency. In May, COREPER (Committee of Permanent Representatives) gave the French presidency a mandate to conduct inter-institutional negotiations with the European Parliament to monitor each country’s individual progress towards completing the objectives of the “**Digital Decade**”.

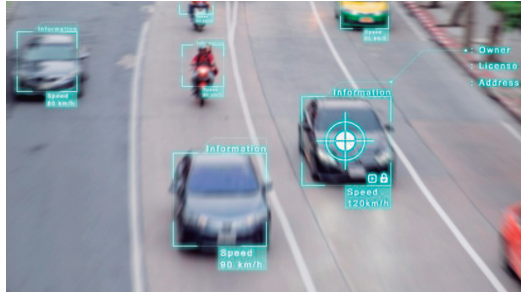
This mandate establishes a system that limits the influence of the European Commission in monitoring and steering the progress of Member States’ digital governance. Whereas before it was able to directly influence the process and require countries to follow a particular path, its role has now been reduced to providing guidance and issue recommendations.

From now on, **countries will have more freedom to undertake the necessary reforms in the digital area**. It is feared that the final effect will be the decrease of homogeneity and the regression of some Balkan and Eastern countries.



Emirates: A China in the Western World?

The United Arab Emirates has undertaken heavy investment in recent years. The UAE aspires to have AI developments account for 20% of the national GDP by 2030.



The first uses of AI adopted by the state were mainly geared towards the provision of financial services, but by 2018 it had shifted its focus to **security and population monitoring**. That year, the Dubai Police Force began using "*Oyoon*". Oyoon is a program that deploys cameras in the public space in order to monitor in real time the movements of people and identify them through facial recognition and voice recording.

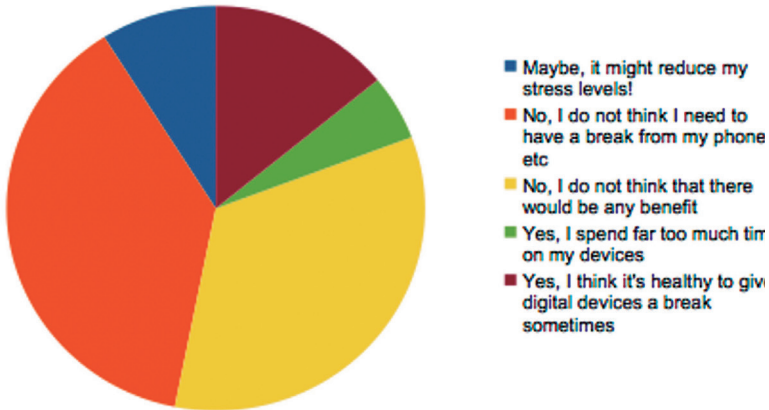


Oyoon was heavily criticized for invading people's privacy without any safeguards or judicial control. But the Covid-19 pandemic directed its use toward public health. The software monitored thermal sensors and identified which people were infected and which were not.

Emirates is the first country in the Western bloc to massively deploy cameras, sensors and microphones in order to monitor the population on a permanent basis.

Digital detoxification in Japan

Some 50% of respondents in Japan admitted that they were aware of their dependence on cell phones.



The figures, which demonstrate an increased psychological dependency on digital devices, are a reflection of the post-pandemic “new normal” in Japan. Included among the “norms”, is sending and receiving work-related emails late at night. In the Japanese cultural and work context, recipients believe they absolutely must respond to work emails so that they do not appear to be disengaged from the company they work for. These habits compel them to be under a **constant state of tension** and apprehension since they are prepared to react to any possible stimulus.

Social isolation has also contributed to **young people’s increased use of addictive social networks**. The problem is therefore not limited to the working-age generations, but is growing alarmingly among students as young as 14.

Social awareness of this problem has led to the emergence this year of a whole sector of centers dedicated to digital detox.

These centers offer courses on the disadvantages of the excessive use of mobile devices and screen-time. These are not programs that are intended to demonize smartphones or to turn people into de-digitalized

hermits. The main objective of these programs is to get patients to re-evaluate **their relationship with devices** in order to develop a **healthy use** of them and improve their **quality of life**. After all, devices are a means to an end, not an end in themselves. It is people who should be in control of these devices, not the other way around.

As expected, participants **discovered that *digital detoxing* was far more difficult than they imagined**. Feelings of anxiety and distress are reported by many of them, which stem from a worry they share of not knowing if someone is going to try to contact them.

EU Digital Product Passport

Frans Timmermans presented the **Sustainable Product Regulation Proposal** and explained that the war in Ukraine, as well as the experience of the pandemic, have exposed the need for European countries to redu-



ce their *over-dependence on primary natural resources, fossil fuels, and outside suppliers*.

The war on Ukraine forced the member states of the EU to rethink the way in which the European New Deal was being implemented since it now had to reassess its relationship with other countries.

For example, whereas the **Ecodesign Directive** of 2009 was focused on regulating energy-related products, the **Sustainable Product Regulation Proposal** will regulate almost all categories of physical goods placed on the EU market. The products that will now be regulated include tablets, smartphones, and photovoltaic solar systems. The framework establishes a wide set of requirements on the durability, recyclability, and resource efficiency of products. This initiative not only expands upon the Ecodesign Directive, but it also is intended to further promote the “circular economy”.

Introduced in the regulation is a **Digital Product Passport**, a digital tool that is intended to transfer crucial information between different stakeholders across value chains. The EU also sees the potential for the passport to provide other data-sharing opportunities.

Although this “Passport” is limited to physical products for the time being, its expansion to the service sector has not been ruled out.

Digital services are dependent on data centers, which are highly intensive in energy consumption. Will we know soon if the energy that our favorite Internet sites and apps consume is renewable or not?

SMEs and cybersecurity

In 2021, 53% of SMEs in Spain suffered a cyberattack. What’s more, these figures are expected to continue to rise this year.

FinCEN (Financial Crimes Enforcement Network), says that, between January and June 2021 alone, it has monitored a traffic of over €4.5 billion in bitcoins allegedly associated with payments derived from cybercams. In Spain alone, cyber-attacks cost €75,000 on average for each SME attacked.

The data is shocking because SMEs make up 99% of the Spanish business fabric. They represent 62% of GDP, provide more than 60% of priva-

Herramienta de autodiagnóstico
¿Conoces el nivel de seguridad en el que se encuentra tu organización?

El desconocimiento del riesgo no te exime de sus consecuencias

Objetivo
Ofrecer una herramienta con la que poder evaluar el grado de seguridad de una empresa y actuar en consecuencia.

Conoce el valor de tus activos de información

Conciencia acerca de la importancia de conocer los riesgos.

Facilita el desarrollo de Planes de Seguridad

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD
www.incibe.es

te employment, and 98% of them are already, to a greater or lesser extent, digitized.

Insurers state that, in Spain, only 18% of companies have specific insurance policies for cyber-attacks. The European average is 24%. Now insurers are focused on creating quantification systems with Artificial Intelligence. These quantification systems use hypothetical models in order to calculate possible damages from attacks.

But sources consulted in the Guardia Civil warned that there is a significant difference between being insured and gaining security. There are currently some 29,000 Spanish companies whose servers are compromised at root level (super user). What is created is a situation of permanent risk on a scale that could be significantly reduced if SMEs took basic security measures. The cybersecurity battle can only be won company by company, server by server.

Our recommendations

Report

“Foundation models,” the latest development on deep learning that will revolutionize AI development.

Foundation models are the latest development on deep learning (DL). Deep learning is a technique that rose to fame ten years ago and now dominates the field of AI. DLs, which are loosely based on the network structure of neurons in the human brain, are “trained” using millions or billions of examples of text, images or sound clips. In recent years, the high cost in both time and money to train DLs raised fears that this technique was reaching its limits. Concern was growing that an “AI winter” was coming. But foundation models show that DL creation can unlock increasingly impressive capabilities. No one knows where the limit is.

<https://www.economist.com/interactive/briefing/2022/06/11/huge-foundation-models-are-turbo-charging-ai-progress>

<https://www.economist.com/leaders/2022/06/09/artificial-intelligences-new-frontier>

Scientific articles and references

Science: “Memristive technologies for data storage, computation, encryption, and radio-frequency communication.”

Memristors, the future of AI, are hardware that work like a brain. Memristors already emulate the sensation of skin touch. This is a science magazine article explaining how they work, what they are based on, etc.

<https://www.science.org/doi/10.1126/scirobotics.abl7344>

ECFR: The Power Atlas

The major powers have realized that access to new technologies can be fundamental to their sovereignty. However, while the US and China are fully embracing geopolitical diplomacy, the EU is just beginning to learn to speak the language of technological power.

<https://ecfr.eu/special/power-atlas/technology/>

El Confidencial: Criticism of the effect of platforms on culture and cultural industries.

“...The conversion of networks into the new center of influence of public debate is far from having been socially beneficial”

https://www.elconfidencial.com/cultura/2022-06-05/dinero-poder-cultura-influencia-politica-economia_3436322/

Le Monde: Online pornography: why it is so difficult to verify the age of Internet users.

France discusses digital identity solutions to put an end to the impossibility of verifying the age of Internet users and thus of controlling the

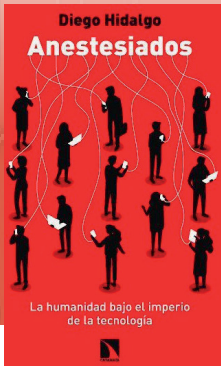
cultural and social impact of pornography on minors.

https://www.lemonde.fr/pixels/article/2022/05/24/pornographie-en-ligne-pourquoi-la-verification-de-l-age-des-internautes-est-si-difficile_6127424_4408996.html

PhysicsWorld: Quantum computing revisited: Optimists and realists

<https://physicsworld.com/a/the-quantum-hype-cycle-revisited/>

Book



«Anestesiados: La humanidad bajo el imperio de la tecnología», Diego Hidalgo, Libros de la Catarata

...We are still far from understanding the real impact of digital technology on our freedom.



Instituto Hermes
C/. Orense 81, 7ª planta - 28020 Madrid
fundacion@institutohermes.org
<https://institutohermes.org>