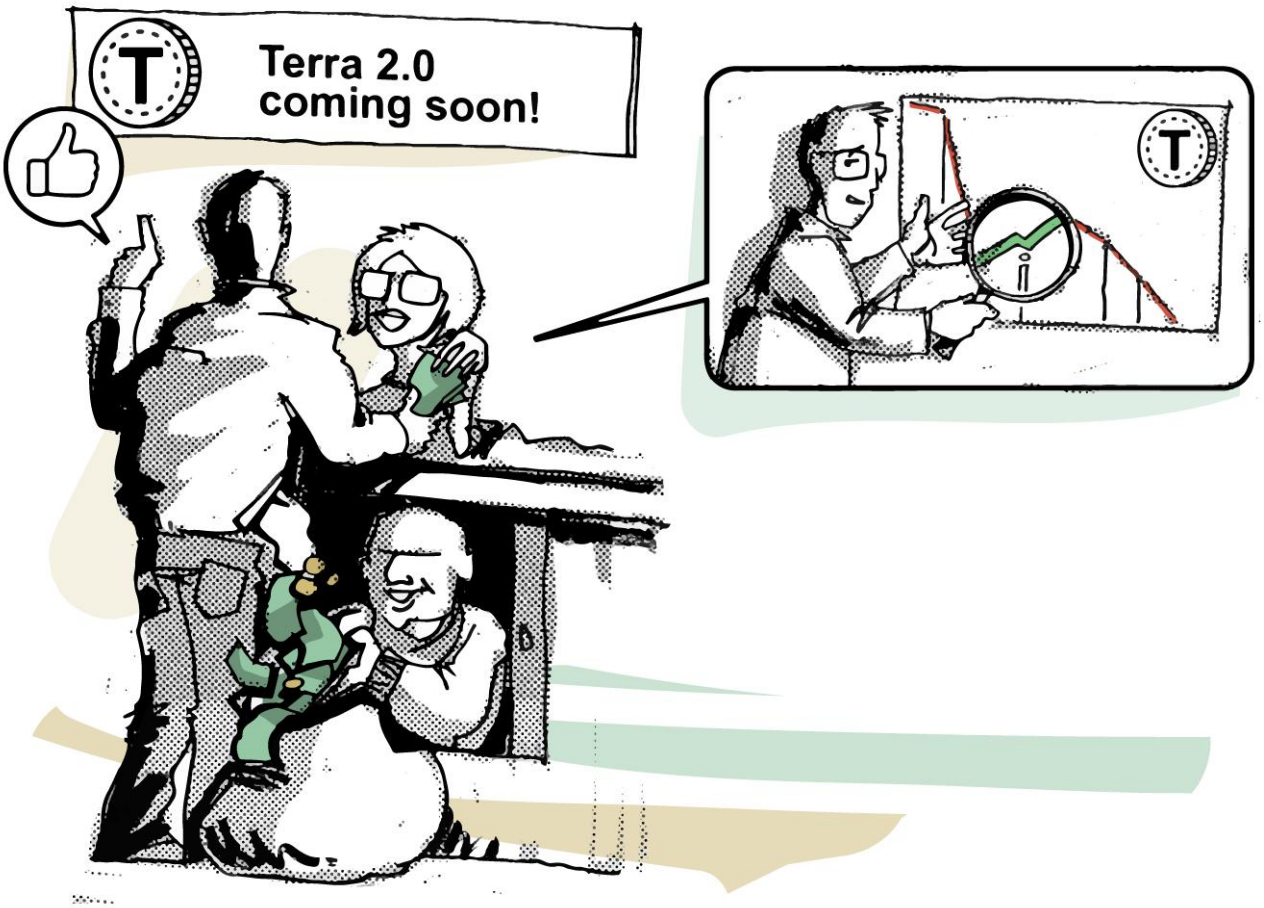
digwatch GENEVA INTERNET PLATFORM

NEWSLETTER

Issue 70, **June 2022**



Crypto market in danger?

Pages 2–3

TRENDING

Online content policy, the crypto market crash, and digital issues on the agendas of G7 digital ministers, TTC, and the Quad..

Pages 2-3

NIS2

A political agreement on the EU's NIS2 has been reached. We look at its background, its main components, and the next steps in its legislative journey.

Pages 6-7

DIGITAL AT DAVOS

Digital topics underpinned the packed agenda of the World Economic Forum's (WEF) flagship annual meeting held in Davos. Here's what was discussed.

Page 10

GENEVA

Many policy discussions take place in Geneva every month. Catch up on the latest news from International Geneva.

Page 11

Top digital policy trends

1. Online content policy

On 14 May, Payton Gendron allegedly killed 10 people and wounded 3 more in a mass shooting in a Buffalo grocery store.

Two days before, a manifesto he allegedly wrote was posted in GoogleDocs, outlining a planned shooting and claiming that he had been radicalised on 4chan – an image-based bulletin board with anonymous contributors.

Gendron created a private chat room on the communications app Discord, which served as his personal diary chat log. He streamed the attack on the streaming platform Twitch, which claimed it took down the video within two minutes of the attack starting. However, a recording of the video was swiftly posted on Streamable, another streaming website.

Links to the recording were shared across Facebook and Twitter, who struggled to contain it. Some users who flagged the video on Facebook were notified that it did not violate Facebook's rules. A clip allegedly displaying a first-person view of the gunman firing at people was viewable on Twitter more than four hours after it was posted. TikTok users reportedly uploaded videos sharing accounts and search terms to take viewers to the full video on Twitter.

The Buffalo shooting bolstered calls for accountability of online platforms. Twitch, Discord, and 4chan face a probe by the New York Attorney General about their role in the promotion of violence. New Jersey is launching a similar probe into Twitch and Discord.

The world was still reeling from the news of the Buffalo shooting when Salvador Ramos allegedly killed 21 people and wounded 19 more in a mass shooting in a Uvalde, Texas elementary school on 24 May. Reports suggest that Ramos posted pictures of the two guns he used in the attack on 20 May on Instagram. Meta, the parent company of Instagram and Facebook, does not limit photos or hashtags around firearms, making detection harder. As the caption for the Instagram post read 'Kids be scared,' and did not otherwise call for violence, it flew under the radar. Minutes before the attack, Ramos sent private messages on Facebook announcing he would shoot an elementary school, uncovered in the subsequent investigation.

These events fuelled an ongoing discussion on social media's responsibility for online content and freedom of speech in the USA. The US Supreme Court was about to decide on the implementation of the Texas social media law that prohibits social media platforms with at least 50 million active users from blocking, removing, or 'demonetizing' content based on users' views. This law would make it illegal for large social media platforms to remove content posted by the shooters. The tech companies filed an emergency appeal right after the Buffalo shooting, emphasising the arguments to block this law. On 31 May 2022, the US Supreme Court sided with the technology industry and blocked the controversial Texas law. A debate on hate speech and content takedown concluded in the EU as well, as part of the negotiations of the Digital Services Act. The very large online platforms are bound to remove content targeting victims of cyber violence 'immediately' and other content deemed illegal must be removed 'swiftly'. We wrote about the DSA in more detail in our Newsletter last month.

The tragic events of May raise important policy questions: Will the Christchurch Call to eliminate terrorist and violent extremist content online be strengthened or will a new initiative pop up? Will we see stronger policies that make it more difficult to upload violent videos to online platforms? Or will we see calls for weaker encryption on private conversations?

The Christchurch shooting led to the creation of the Christchurch Call when several governments and online platforms vowed to enhance efforts to eliminate terrorist and violent extremist content online. The head of the Christchurch Call claims that its tools made it harder for the Buffalo shooting video to go viral.

2. Crypto market in danger

Popular stablecoin Terra survived a total blowup in May: Cryptocurrency coin Luna (related to the Terra ecosystem), which traded for $110, fell to $0.05 the next day, wiping almost $50 billion in

value. This major breakdown rang alarms with investors and regulators worldwide. Many suspected this might be the end of the cryptocurrency craze, given that all tech companies experienced difficulties and a decline in share prices. But cryptomarkets are still standing at almost the same level. Terra coin is going through the rebuttal, while several crypto exchanges announced they will start trading Terra 2.0 as soon as it is available.

What are stablecoins? Why was Terra so popular among investors? How can we protect investors and customers? *Read more on pages 8-9.*

3. Digital in high politics

This month, digital policy was on the agenda of the G7 digital ministers, the US-EU Trade and Technology Council (TTC), and the Quad Leaders' Summit.

G7 digital ministers. At their Dusseldorf meeting on 10 and 11 May 2022, digital ministers of G7 countries reiterated their commitment to 'mak[ing] concentrated efforts to maintain a free, global, open, interoperable, reliable and secure internet that supports innovation and strengthens respect for democratic values and universal human rights'. They adopted an action plan to promote data free flow with trust (DFFT), and a set of principles for domestic legal frameworks to promote the use of electronic transferable records. A Joint Declaration on cyber resilience of digital infrastructure in response to the Russian war against Ukraine was issued, highlighting the G7's commitment to increasing the cyber resilience of digital infrastructures and to continuing to support Ukraine in defending its networks against cyber incidents.

US-EU TTC. Key outcomes of the second ministerial meeting of the US-EU TTC on 16 May include:

- The launch of a Strategic Standardisation Information mechanism dedicated to facilitating the exchange of information on the development of international standards.
- The establishment of an AI sub-group tasked with developing a roadmap on evaluation and measurement tools for trustworthy AI, and a project on privacy-enhancing technologies.
- The creation of a policy dialogue on issues related to content moderation, and a commitment to developing a common analytical framework for identifying 'foreign information manipulation and interference' that should enable effective countermeasures.
- The creation of a sub-working group tasked with developing a common understanding on semiconductor shortages and facilitating coordination in this area.
- The launch of a taskforce on public financing for secure and resilient connectivity and information and communication technology and services (ICTS) supply chains in third countries, to promote the use of 'trusted/non-high-risk suppliers' and facilitate collaboration on the US-EU public financing of ICTS projects in third countries based on common principles.

Quad Leaders' Summit. On 24 May, the prime ministers of Australia, India, and Japan and the president of the USA met in Tokyo for the second Quad Leaders' Summit and agreed to:

- Deepen collaboration and pursue complementary actions in digital connectivity.
- Cooperate on improving the defence of their critical infrastructure.
- Coordinate cybersecurity-related capacity-building programmes in the Indo-Pacific region, in the framework of the Quad Cybersecurity Partnership.
- Advance interoperability and security in 5G and beyond 5G by signing a new Memorandum of Cooperation on 5G Supplier Diversification and Open RAN.
- Advance cooperation on semiconductors and other critical technologies and enhance resilience against various risks. A Common Statement of Principles on Critical Technology Supply Chains was issued, listing security, transparency, autonomy, and integrity as 'voluntary principles to assist governments and organisations in making decisions about their suppliers and the security of their products'.
- Strengthen cooperation in international standardisation organisations.
- Deepen discussions and cooperation on issues related to biotechnology and quantum technologies.

Digital policy developments that made headlines

The digital policy landscape changes daily, so here are all the main developments from May. We've decoded them into bite-sized authoritative updates. There's more detail in each update on the Digital Watch observatory.

Increasing relevance

Global digital governance architecture

The UN Secretariat launched a public consultation on what should be included in the Global Digital Compact.

Low relevance

Sustainable development

The EU and Japan launched a digital partnership to foster economic growth and achieve a sustainable society. The UN Economic and Social Commission for Asia and the Pacific released papers exploring the intersection of connectivity and the digital economy and the status of cross-border connectivity in South-East Asia.

Increasing relevance

Security

The Second Additional Protocol to the Budapest Convention on Cybercrime was opened for signature.

Costa Rica declared a state of national emergency amid Conti ransomware attacks. Later on, researchers reported that Conti is shutting down operations and reorganising.

The USA, the EU, Canada, and the UK attributed the Viasat cyberattack to Russia. The hacktivist collective Anonymous has declared cyberwar against Killnet, a group of pro-Russian hackers. Killnet itself declared cyberwar on 10 countries. REvil ransomware operations seem to have returned.

The European Commission launched a strategy for a Better Internet for Kids and a legislative proposal against child sexual abuse material.

Increasing relevance

E-commerce and the internet economy

The European Commission argued that Apple has abused its dominant position in mobile wallets on iOS. The UK is investigating whether Google's practices in the ad tech market are anticompetitive.

Japan passed a landmark law on stablecoin regulation. The Central African Republic announced plans to launch a cryptocurrency investment platform. Uzbekistan exempted crypto operations from income tax.

Low relevance

Infrastructure

Canada announced a plan to ban Huawei and ZTE from 4G and 5G networks.

WIPO suspended domain name dispute resolution services for .ua.

Low relevance

Digital rights

The European Commission presented proposals for a European Health Data Space.

Meta has rewritten and redesigned its Privacy Policy came with a new privacy tool allowing users to set a default audience for their posts. The US District of Columbia is suing Mark Zuckerberg over privacy breaches in the Cambridge Analytica scandal.

Internet disruptions were recorded in Pakistan amid public protests.

Increased relevance

Content policy

The US Supreme Court blocked a controversial Texas law that prohibits social media platforms with at least 50 million active users from blocking, removing, or demonetising content based on user views.

Austria launched an action plan to address deepfakes.

ICYM: Elon Musk is still committed to the acquisition of Twitter but demanded that Twitter show that spam accounts number less than 5% of all Twitter accounts for the deal to move forward. Twitter's board stated it plans to 'close the transaction and enforce the merger agreement' between Musk and Twitter. The matter is now at the SEC, which must approve Musk's offer to buy Twitter (which is publicly traded).

Low relevance

Jurisdiction and legal issues

Big tech companies face lawsuits in Russia for pulling services out of the country.

The Spanish data protection agency fined Google €10 million over GDPR breaches.

Google announced it reached content licensing agreements with over 300 publishers in Europe, in line with the EU's copyright directive.

Increased relevance

New technologies

Ireland appointed its first Artificial Intelligence Ambassador. Singapore launched an AI testing framework. Civil society groups called on the European Parliament to ban biometric surveillance. The US government warned against disability discrimination caused by AI tools used to make employment decisions.

Clearview AI agreed to stop selling its facial recognition software to private firms in the USA. In the UK, the company was ordered to delete data belonging to UK residents.

The US President issued a national security memorandum and an executive order aimed at ensuring US leadership in quantum information science and mitigating risks associated with quantum computers. Researchers at Delft University of Technology announced progress steps towards a future quantum internet.

The NIS2 directive

On 13 May, the European Parliament and the Council reached a political agreement on a *Directive on measures for a high common level of cybersecurity across the Union*, commonly referred to as NIS2. We tackle the document's background, its main components, and the next steps in its legislative journey.

Background

The EU Commission adopted a proposal for a revised Directive on Security of Network and Information Systems in December 2020 'to further improve the resilience and incident response capacities of public and private entities, competent authorities and the Union as a whole in the field of cybersecurity and critical infrastructure protection'. The revised directive, known as NIS2, builds on the Directive on security of network and information systems (NIS1), adopted in 2016, the first EU legislation on cybersecurity, providing legal measures to enhance the overall level of cybersecurity in the EU.

Aims and purpose

According to the EU Commission proposal, NIS2 is aimed at revamping and updating the existing legal framework while considering the rapid digitalisation of the EU internal market and the growing cybersecurity threat landscape that the COVID-19 pandemic has further intensified.

Furthermore, NIS2 addresses a couple of shortcomings that prevented the NIS directive from unleashing its full potential. The EU Commission's evaluation of NIS1 revealed the following shortcomings:

1. the low level of cyber resilience of businesses operating in the EU;
2. inconsistent resilience across member states and sectors; and
3. the low level of joint situational awareness and lack of joint crisis response.

Sectors concerned

One of the key changes in NIS2 is that it does not differentiate between operators of essential services and digital services providers. NIS2 significantly broadens the industry sectors and breaks them down into two categories as listed in Annex I and Annex II of the directive. Both must comply with cybersecurity risk management requirements and reporting obligations:

- **Essential sectors** include health, energy, transport, banking, digital infrastructure, and public administration and space sectors.
- **Important sectors** include entities manufacturing medical devices, postal services, waste management, food production and processing, and digital providers.

When it comes to supervision and enforcement, however, the procedure for essential and important sectors differs. Member states are obliged to ensure that measures imposed on entities in essential sectors are effective and proportionate, and they have the power to conduct on-site inspections or targeted regular audits based on risk assessments, among others. On the contrary, important entities are subject for investigation only if evidence of non-compliance emerges.

As with the NIS1, micro and small entities are excluded from the scope of the NIS2.

NIS 2 sectors. Image source: jtsec.es

Novelties of NIS2

The following is a non-exhaustive list of NIS2 requirements broken down into four categories:

Coordinated cybersecurity regulatory frameworks. Like NIS1, NIS2 obliges EU member states to adopt national cybersecurity strategies that should define strategic objectives, a governance framework, and measures to ensure preparedness, among others. NIS2 obliges EU member states to set up computer security incident response teams (CSIRTs), which should also act as coordinators for vulnerability disclosure. NIS2 tasks the European Union Agency for Cybersecurity (ENISA) to develop a European vulnerability registry, which should encompass information about vulnerabilities, affected ICT products and services, and the severity of the vulnerabilities, among others.

Cooperation. NIS2 envisages the formal establishment of a European cyber crises liaison organisation network (EU - CyCLONe) to 'support the coordinated management of large-scale cybersecurity incidents and crises at operational level and to ensure the regular exchange of information among Member States and EU institutions'. To assess the effectiveness of the EU member states' cybersecurity policies and the implementation of the cybersecurity risk management requirements and reporting obligations, the EU Commission will establish the so-called peer reviews.

Cybersecurity information-sharing arrangements. NIS2 emphasises information sharing and requires EU member states to ensure that organisations exchange relevant cybersecurity information among themselves, such as information relating to cyber threats, vulnerabilities, indicators of compromise, tactics, techniques and procedures, cybersecurity alerts, and configuration tools. Furthermore, member states are also encouraged to submit voluntary notifications of significant incidents or cyber threats.

Cybersecurity risk management and reporting obligations. NIS2 requires that EU member states will ensure that 'essential and important entities take appropriate and proportionate technical and organisational measures to

manage the risks posed to the security of network and information systems which those entities use in the provision of their services'. These include risk analysis and information system security policies, incident handling, business continuity and crisis management, supply chain security, policy and procedures (testing and auditing) to assess the effectiveness of cybersecurity risk management measures, and the use of cryptography and encryption. Moreover, EU member states are obliged to take all necessary coercive measures to bring the service, which is not in compliance with these requirements into compliance.

Unlike NIS1, NIS2 demands that member states ensure essential and important entities report any incident with the potential to cause operational disruption or financial losses. Entities should notify competent authorities or CSIRTs about the event within 24 hours. Furthermore, entities are requested to comply with European cybersecurity certification schemes.

Penalties

According to NIS2, EU member states are tasked with laying down rules on penalties applicable to the infringements of national provisions.Organisations that do not comply could be penalised a maximum of €10 million or 2% of worldwide annual turnover, whichever is greater.

Next steps

The provisional agreement is now subject to approval by the co-legislators, the European Council and the European Parliament. France, holding the Council's presidency, is expected to submit the agreement to the Council's Permanent Representatives Committee for approval soon. EU member states will have 18 months to transpose NIS2 into their national legislations.

Are stablecoins a danger to the crypto economy?

Popular stablecoin Terra survived a total blowup in May. What are stablecoins? Why was Terra so popular among investors? How can we protect investors and customers?

Stablecoin and the implications for the crypto industry

We often think of cryptocurrencies as investment vessels with a constant price increase. However, one type of cryptocurrency has a different role in the cryptocurrency ecosystem. It tends to have a stable $1-per-coin price. In other words, it is pegged to the US currency and called stablecoin. Stablecoins are necessary for the functioning of decentralised finance (DeFi) technologies and the proper working of online exchanges. In DeFi, stablecoins are used as collateral and online exchanges use them for mutual settlements. The most prominent stablecoin, Tether, is often considered to be a reason for the quick and explosive growth of online exchanges.

The Terra story

There are two quite different types of stablecoin. One type is backed by US dollars (or in some cases a basket of currencies), meaning that every stablecoin issued has its analogue counterpart stored in a vault. This offers investors security to convert their wealth into digital tokens and limits the fear of instant market crashes, which occur often in crypto trading. Knowing that people will not hold stablecoins for long, the second type of stablecoin – the so-called algorithmic stablecoins – offer a pretty hefty reward for staking. Staking is similar to holding a fixed-term savings account in a bank; the crypto version offers up to 20% profit for not moving your coins for a certain amount of time. They use algorithms to buy/sell in order to balance the value of the coin to $1. The star of the promised stablecoin rise was a currency built by the South Korean programmer Kwon Do-hyung, better known as Do Kwon. He created the Terra ecosystem with the native TerraUSD and Luna tokens that were issued on the network. One significant change from other algorithmic stablecoins was that Terra was to hold its peg to the US dollar by using the bitcoin price as a main balancing factor. Do Kwon appeared on media outlets around the world. The idea was propagated as a 'currency for a new monetary system based on bitcoin, rather than fiat currencies'. This remarkable promise of a 20% yield for the 12-month period was a trap for small investors or late comers who pushed their portfolios into these locked pools from which the stablecoin pulled its liquidity. It was estimated that the Terra ecosystem was worth more than $18 billion.

Everything looked stable enough (pun intended) for the new crypto era, except one small detail: the idea that bitcoin price would steadily rise and never go down -- let's say 25% in two days. Looking at the history, this was a naive assumption, because exactly that happened. The steep price fall triggered a run on the bank as investors put TerraUSD into a death spiral losing 99.8% of its value.

Reserves depleted quickly, handled by techies rather than financial wizards who understood stock exchanges and market movements. Other funds were locked in and unable to be accessed. This marked the demise of the most promising rising star of the cryptoworld. In a short outburst, TerraUSD wiped out more than $50 billion of investments, causing a serious concern that the whole cryptocurrency market would collapse. Do Kwon is facing an investigation by the Seoul Southern District Prosecutor's Office, which will investigate Terraform Labs, the organisation behind the Terra stablecoin project. It has assigned the case to its Financial and Securities Crime Joint Investigation Team.

In a statement from the law firm hired by the five investors bringing charges against Terraform Labs, they said: 'The design and issuance of Luna and Terra to attract investors, but the failure to properly inform them about the flaws, and the unlimited expansion of Luna's issuance amounted to defrauding investors.'. And this is indeed an important idea

that we need to tackle if we are going to see a meaningful introduction of cryptocurrency economies to regular finance.

The idea of algorithmic stablecoins has been seriously shaken, but this is certainly not the end of cryptocurrencies. The collapse of Terra's ecosystem tells yet another story about greed and the willingness to gamble with investors' money (Bitconnect, OneCoin, the list is long).

Other stablecoins

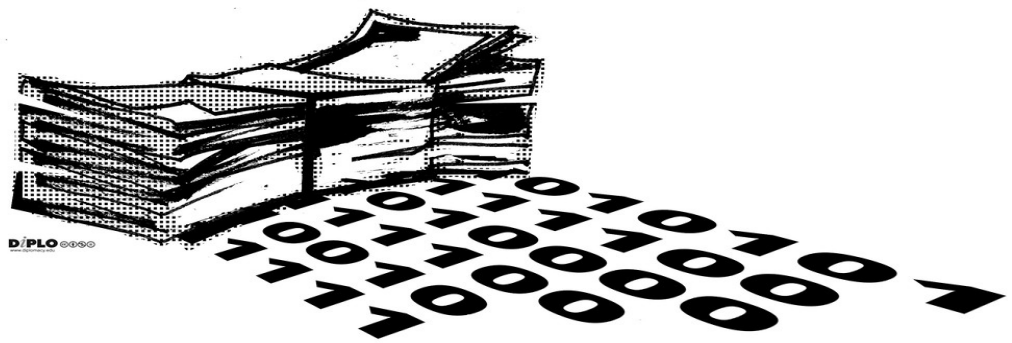
The explosion of stablecoins started in 2020–221. From a $6 billion evaluation on 31 December 2019, the amount of funds rose to $181 billion in May 2022 (according to the metrics from cryptoblock). The biggest stablecoin on the market is the US-based Tether. Tether Holding Limited, the company behind the Tether cryptocurrency, has so far issued more than 70 billion tokens (equivalent to $70 billion) and it offers a daily overview of its reserves. According to the company, all $70 billion is redeemable in fiat currencies and stored in safe vaults. The Tether cryptocurrency is often cited as a main reason for the rise of global cryptocurrency exchanges, as they use Tether as a tool for mutual settlement. Nevertheless, Tether was always under the suspicious eyes of investors and the crypto industry. Those concerns were addressed back in 2021, when the US Commodity Futures Trading Commission (CFTC), conducted an investigation and issued a statement that Tether was not telling the whole truth. Tether Holdings Limited was hit with a $41 million fine. The CFTC stated that a fine was issued 'for making untrue or misleading statements and omissions of material fact in connection with the U.S. dollar tether token (USDT) stablecoin'. This decision created additional uneasiness for the whole industry and pushed regulators to speed up work on the framework in which stablecoins can be audited quickly and efficiently.

Stablecoin regulation

This is not the first time stablecoins have come under the regulatory spotlight. Back in 2019, Facebook announced that it would create a stablecoin under the name of Libra. They announced it would be pegged to a basket of international currencies. This raised a significant response from US and worldwide regulators, prompting the G7's Financial Stability Board (FSB)to develop a strategy for further stablecoin regulation. The FSB is working on the global regulation of stablecoins as they are seen as the main adversary to the Central Bank Digital Currencies (CBDCs) whose creation is already in motion.

Work on consumer protection laws and overall education around cryptocurrencies should be the first steps towards a crypto-enabled future. What we need is a clear regulatory framework that will protect investors and enable steady growth. In light of the joint effort to reach an optimal regulatory framework, the government of Japan introduced the world's first law tackling the issue of stablecoins. In this new proposal, Japan will ask stablecoin issuers for 'a mandatory link with the yen and [to enshrine] the right to redeem them at face value'. This is a first step towards global regulation, but it needs to be followed by the informative decisions by regulators and market actors.

Looking to the future, the mix of technology and finance will be the hardest to get right, as this area is sensitive to any kind of mistake or oversight. All of these will be quickly and mercilessly exploited by financial people who have been in this game much longer than the tech community. How to create an effective but safe environment is the main question in this area.



Digital at Davos

The World Economic Forum's (WEF) flagship annual meeting was held in Davos 22–26 May. Leaders gathered in a new situation 'characterised by an emerging multipolar world as a result of the pandemic and war'. The war in Ukraine took centre stage with digital topics underpinning the meeting's packed agenda. Here's what was discussed.

The crash of the crypto market ensured that cryptocurrencies were high on the Davos agenda. Critics came out in full force to discuss the future of cryptocurrencies and central bank digital currencies. Also discussed were the quantum economy, trade-offs emerging in the digital economy for businesses, the need to ensure innovative and open digital trade through digital services, the future of retail, and the future of work.

Frontier technologies, AI, metaverse, digital health, cybersecurity, augmented reality, digital inclusion, digital and climate, data governance, and tackling harmful content online were also discussed.

Consideration was given to the future of the internet, namely how to use the multistakeholder approach to prevent a future splinternet, build trust in the digital era and advance digital cooperation.

Post-Davos reports note that attendance was halved and that the absence of Russia and China made the discussions less global and therefore less meaningful.

Critics also note that the mood in Davos was 'terrible', that high-level guests were missing, and that the forum left its attendees wondering whether globalisation was dead.

Critics say that Davos concluded without definitive solutions for the war in Ukraine, food and energy crises, and economic uncertainty.

In the digital realm, Davos tried to envision some solutions. A number of initiatives were launched:

- The Digital Foreign Direct Investment Initiative, launched by WEF and the Digital Cooperation Organization (DCO), will 'offer unique insights on how to create a digital ecosystem that brings prosperity to people to help government to better serve their citizens and also encourage businesses to grow', explained DCO Secretary-General Deemah Al Yahya.
- The Digital Inclusion Navigator helps policymakers find the best practices and resources to further digital inclusion. The platform's focus is on expanding access to and use of digital technologies and on the role of digital services in healthcare, financial services, and education.
- The Lighthouse Countries Network, driven by the UN Development Programme (UNDP) and a network of Lighthouse Countries including Bahrain, Bangladesh, and Rwanda, is being launched to accelerate digital inclusion in the health, education, and finance sectors on a national level.
- The Cyber Resilience Pledge, championed by WEF and companies in the oil and gas industry, outlines a commitment towards strengthening cyber resilience across the industry through adopting actionable frameworks and guidelines, collaborating on common industry and supply chain challenges, and sharing lessons learned.
- WEF announced the launch of a Global Dialogue on Digital Cooperation. It remains to be seen what this means and how it will be aligned with ongoing digital cooperation initiatives at the UN level (we're thinking, for instance, about the development of the Global Digital Compact called for by the UN Secretary-General in his *Our Common Agenda* report)

Policy updates from International Geneva

Many policy discussions take place in Geneva every month. In this space, we update you with all that's been happening in the past few weeks. For other event reports, visit the Past Events section on the GIP Digital Watch observatory.

Humanitarian Networks and Partnership Week (HNPW) | 2–22 May 2022

The hybrid HNPW brought together humanitarian networks and partnerships to address key humanitarian issues. One of the largest humanitarian events of its kind, it gathered participants from the UN, NGOs, member states, the private sector, military, academia, and beyond to discuss common challenges in humanitarian affairs.

Unpacking EU regulations on digital markets and services | 10 May 2022

In light of the recent political agreement reached between the EU Parliament and EU member states on the Digital Services Act (DSA) package, panellists discussed the economic, ethical, and political challenges of the development of large digital platforms and intermediate services. They also analysed the legislative work carried out by European institutions and enumerated the challenges linked to the implementation of the DSA and the Digital Markets Act (DMA). The webinar was organised by The Permanent Representation of France to the UN in Geneva, the Geneva Internet Platform (GIP), and the Delegation of the European Union to the UN in Geneva.

75th World Health Assembly | 22–28 May 2022

Representatives of the World Health Organization's member states met in Geneva to discuss *Health for peace and peace for health*. In light of the COVID-19 pandemic, participants exchanged ideas on how to strengthen the preparedness of WHO and its member states to respond to health emergencies.

110th Session of the International Labour Conference | 27 May–11 June 2022

Member states of the International Labour Organization (ILO) are meeting to discuss occupational safety and health working conditions in the ILO's framework of fundamental principles and rights at work. Delegates are also undertaking the first discussion on apprenticeships with a view to setting a new international labour standard. They will also comment on the report *Decent work and the social and solidarity economy*. In this regard, a final outcome document is expected to be adopted and will be submitted to the plenary of the Conference for adoption on 11 June.

What to watch for: Global digital policy events in June

6-10 June, RightsCon2022 (online)

The 11th RightsCon will be hosted online, as its organiser Access Now believes this will substantially increase accessibility and improve the representation of all parties involved. The programme includes 18 categories such as AI; content policy; digital security for communities; global cyber norms; privacy and surveillance; and internet access, education, and inclusion.

6-15 June, ITU World Telecommunication Development Conference (WTDC-21), (Kigali, Rwanda)

The International Telecommunication Union (ITU) World Telecommunication Development Conference (WTDC-21) will take place between two Plenipotentiary Conferences. Conceived by the ITU's Telecommunication Development Bureau (BDT), its main purpose is to consider topics, projects, and programmes relevant to telecommunication development, and set the strategies and objectives for the development of telecommunication/ICT. The event theme is 'Connecting the unconnected to achieve sustainable development'. With 10 years left to deliver the sustainable development goals (SDGs), this event aims to accelerate action for its achievement through innovative approaches and new models of collaboration for connectivity and digital solutions.

13-16 June, ICANN74, (Hague, Netherlands)

ICANN74 will be held as a Policy Forum scheduled for 13–16 June 2022. Composed of nearly 100 sessions, the programme will revolve around topics such as new generic top-level domains (gTLDs) subsequent procedures, universal acceptance, ICANN's multistakeholder model, and overall policy updates from the various ICANN supporting organisations and advisory committees.

20-22 June, EuroDIG, (Trieste, Italy)

The 15th European Dialogue on Internet Governance (EuroDIG) will cover topics in four focus areas: Digital sovereignty – Is Europe going in the right direction to keep the internet safe and open?, Reality check – Do we implement effective regulations and set the right standards to solve the problems of the future?, Coming next – Outlook on new technologies and can existing governance bodies cope with them?, and the internet in troubled times. Through these areas, the conference will address the question asked at EuroDIG's first preparatory event: How to put Katowice IGF messages into practice?' EuroDIG 2022 will also include Youth Dialogue on Internet Governance (YOUthDIG). The GIP will once again partner with EuroDIG to deliver messages and reports from the event, which will be available on the Digital Watch observatory.

26-28 June, G7 Summit, (Bavarian Alps, Germany)

The G7 Summit will be hosted under Germany's presidency under the theme 'Progress towards an equitable world'. The German presidency focuses on five areas of action: sustainable planet, economic stability and transformation, healthy lives, investment in a better future, and becoming stronger together. This will include promoting a strong commitment to inclusive digitalisation.

About this issue: Issue 70 of the Digital Watch newsletter, published on 7 June 2022 by the Geneva Internet Platform and DiploFoundation
Contributors: Andrijana Gavrilović (Editor), Kristina Hojstricova, Pavlina Ittelson, Arvin Kamberi, Marco Lotti, Anđelija Mijatović, and Sorina Teleanu
Design: Diplo's CreativeLab | Get in touch: digitalwatch@diplomacy.edu
On the cover: *Crypto market in danger?* Credit: Vladimir Veljasević DiploFoundation (2022)
https://creativecommons.org/licenses/by-nc-nd/4.0/

The Geneva Internet Platform is an initiative of:

GENEVA INTERNET PLATFORM digwatch
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
REPUBLIQUE ET CANTON DE GENEVE
POST TENEBRAS LUX
DiPLO www.diplomacy.edu