A radiography of crypto-assets and their risks

Fredrik Andersson and Judith Arnal

In-Depth Analysis

A heterogenous concept with increasing public awareness but lower levels of understanding

There are many types of crypto-assets. Nevertheless, they all share 3 features in common: (1) they are a digital representation of rights, (2) they are based on Distributed Ledger Technology (DLT), with one version of this being blockchain technology and (3) they exist on a spectrum of decentralisation, and do not rely on the support of a central public authority.

Public awareness of crypto-assets has increased but there is still room for improvement in understanding. According to the British Financial Conduct Authority, in 2019, only 42% of adults had heard about crypto-assets. This is in contrast to 73% in 2020, 78% in 2021 and 91% in 2022. However, only 74% of those who had heard of crypto in 2022, were able to correctly identify its definition from a list of statements. According to this analysis, 10% of crypto-asset owners believe they receive the same protection as other traditional banking products. While 79% of crypto-asset users purchased crypto-assets using disposable income or cash, 6% bought crypto-assets using credit or borrowed money, and 19% used long term savings or previous gains from sold crypto-assets. Another survey by the OECD for Asia also arrives at similar conclusions. Significant contributions have also been made in academia, with Panos and Karkkainen (2019) showing that while financially literate consumers are more likely to be aware of crypto-assets, they are not more likely to own them. In fact, this is confirmed by Carbó, Cuadros and Rodríguez (2023), who show that people with higher financial literacy skills are less likely to own cryptocurrencies.

This in-depth analysis aims to clarify the main concepts, use cases and risks surrounding the world of crypto-assets. This policy paper lists and explains the main features, potential benefits, actors and elements of the value chain of crypto-assets, pointing out the risks they pose and provides concrete examples of cases where these risks have materialised. Following the analysis, the different regulatory approaches followed in the main jurisdictions are explained and a few policy recommendations are put forward.

The relevance of blockchain, the blockchain trilemma, layer 2 blockchain technology and bridges

The first relevant crypto initiative was born in 2008 when traditional financial architecture was being questioned. On 31 October 2008 an unknown person or group of people under the name Satoshi Nakamoto put forward a paper describing the original plan and protocol for Bitcoin. This paper addressed the 'double spending problem,' i.e. a fundamental flaw in a digital cash protocol that allows the same single digital token to be spent more than once, by using blockchain technology.

Blockchain is a distributed database or ledger (hence, the name Distributed Ledger Technology – DLT) that is shared among the nodes of a computer network. The main innovation of blockchain is that it is a coordination technology that ensures the security of a record of data without the need for third party intervention. Information is collected and coordinated in blocks, which have certain storage capacity. When this storage capacity is filled, the block is closed and is linked to the previously filled block. Successive blocks form a chain of data, giving rise to the name 'blockchain'. In the vast majority of crypto-assets, blockchain is used in a decentralised manner, so that no single person has control over it, allowing all users to master it collectively. Data entered in public, permissionless blockchains are immutable, permanently recorded and visible to anyone.

Having gone through the process of purchasing a crypto-asset, it has been, for quite some time, showcased that a crypto transfer is the most time efficient way to transfer value within and between jurisdictions. The transfer of crypto is almost instantaneous and does not require an intermediary. While this is becoming possible through traditional means of payments, they are still limited to certain countries or areas, and can be expensive.

Nevertheless, using blockchain technology has created what is known as the **blockchain trilemma**. This means that a single blockchain network cannot encompass security, scalability and decentralisation all at once, with scalability being the point usually left behind. Technical solutions to cater for scalability issues have been put in place. One such solution is layer 2 blockchain technology, which is basically a secondary protocol built on top of an existing blockchain system. Examples of this are 'Lightning Network', which is the layer 2 payment protocol of Bitcoin, or 'Polygon', which is the most widely adopted layer 2 solution for Ethereum.

Most blockchain networks exist in the form of isolated communities, in which interactions are certainly restricted. Thus, blockchain bridges, also known as cross-chain bridges, have been introduced, allowing for the interoperability of different blockchain networks.

Nevertheless, blockchain bridges are not exempt from risks and in fact, in the last few months, a number of attacks have been carried out against crypto bridges. Examples of such attacks are hacks against Ronin Bridge, BNB, Wormhole or Nomad, leading to losses above EUR 2 billion. According to a report by crypto data aggregator Token Terminal, cross-chain bridges are the target of 50% of exploits in Decentralised Finance.

Most relevant consensus mechanisms: proof of work and proof of stake. Environmental and security risks

In order for blockchain technology to ensure trust (or even go further, by making trust unnecessary) and for transactions to be validated, a consensus mechanism is generally needed. Consensus mechanisms rely on software rather than on human action. When someone wants to make a transaction with crypto-assets, their transaction is first sent to a memory pool or mempool, where it

awaits assignment to a new block. The transaction will be validated according to the consensus mechanism used.

Up until 2022, proof of work was the consensus mechanism used by the two major crypto-assets: Bitcoin and Ethereum. Proof of work entails costly computational work, with nodes competing in a mathematical contest, usually with the node with the highest computing capabilities succeeding. The successful node will win a reward (this is 'mining') and once the solution is confirmed by the other nodes in the network, consensus is reached and the transaction is validated. Apart from Bitcoin, at present, the other most relevant crypto-asset using a proof of work mechanism is Dogecoin.

Nevertheless, given accusations about environmental damage stemming from proof of work mechanisms, Ethereum completed its migration to a proof of stake mechanism in September 2022. This operation was known as the 'Merge' and has allegedly reduced direct energy consumption by 99%. Under a proof of stake mechanism, validators are selected according to their stakes, i.e. the amount of crypto-assets they own and block to ensure a correct validation of the operation. As in the case of proof of work, the successful validator will win a reward (this is 'minting'). Aside from Ethereum, the other most relevant crypto-asset running on a proof of stake mechanism is Cardano.

Though proof of work and proof of stake are the most commonly used consensus mechanisms, others exist, such as proof of authority or proof of history. Ripple's blockchain technology XRP Ledger (XRPL) relies on a proof of authority mechanism, which consists of granting validation powers to a small and designated number of actors. Even if explanations have been provided showing that it is not possible for any entity to exercise centralised control over the ledger under this consensus mechanism, some crypto-purists believe this goes back to a centralised system. Solana uses a combination of proof of stake and proof of history consensus mechanisms.

Another relevant issue is that the stablecoin (a crypto asset with its value tied to a fiat currency) Tether, the third largest crypto assets by market capitalisation, does not rely on any sort of consensus mechanism.

In spite of the significant move made by Ethereum, the still massive reliance of crypto-assets on energy intensive proof of work mechanisms creates a non-negligible environmental risk. Some crypto-assets have a significant carbon footprint and are estimated to consume as much energy each year as individual countries such as Austria, the Netherlands or Spain. In any case, alternatives are currently being sought, e.g. through cogeneration, to reduce energy consumption of proof of work mechanisms.

Moreover, consensus mechanisms can also be vulnerable to security issues, for example, through the '51% attacks', which could jeopardise the decentralisation principle on which the whole system is based. A 51% attack is an attack on a cryptocurrency blockchain by a group of miners who control more than 50% of the network's mining hash rate. Owning 51% of the nodes on the network gives the controlling parties the power to alter the blockchain. Among notable examples of 51% attacks are the 2018 attack on Bitcoin Gold, which resulted in almost USD 18 million worth of the currency being double spent or attacks against Vertcoin, resulting in doubling spending of more than USD 100 000 worth of the crypto.

Types of crypto-assets: traditional crypto-assets and stablecoins

There are several taxonomies that attempt to categorise crypto-assets into different categories. Payment tokens, security tokens and utility tokens are a first attempt to classify crypto-assets based on

their purpose. Another option is to refer to Bitcoin as the main crypto-asset by market capitalisation, as will be explained later, and to refer to altcoins as all other crypto-assets.

However, for the purpose of this analysis, we will make a distinction between traditional crypto-assets and stablecoins. At the same time, stablecoins can be classified into a number of categories, as will be explained later.

An increasingly important but highly volatile market

As can be seen in *Figure 1* which shows the evolution of overall crypto-asset market capitalisation between July 2010 and September 2023, crypto-assets have gained in market capitalisation, though it looks like a very volatile market. Indeed, total market capitalisation was above USD 3 trillion on 10 November 2021, before rapidly plummeting well below USD 850 billion barely 13 months later. At the time of writing this analysis (March 2024), market capitalisation is again above USD 1 trillion.

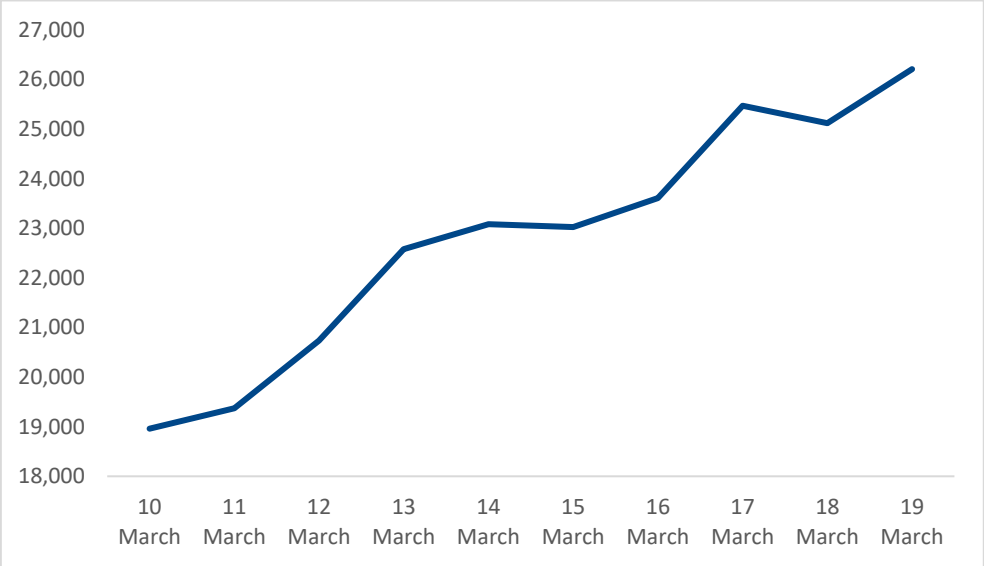
Figure 1: Overall cryptocurrency market capitalisation (in billion US dollars) – September 2010 to March 2024

Source: Statista

A nice, simple way of illustrating the volatility of crypto-assets is the anecdote of 'pizza day'. On 22 May 2010, somebody offered 10 000 bitcoins to anyone who could make him two pizzas. Someone indeed arranged for those two pizzas to be delivered and received 10 000 bitcoins in exchange. On 2 January 2024, 10 000 bitcoins were worth more than USD 453 million. In November 2021, however, they were worth more than USD 660 million and today, 26 March 2024, more than USD 702 million.

Another example of volatility that can be seen in *Figure 2* is the huge increase in the value of Bitcoin following the collapse of Silicon Valley Bank (SVB) in March 2023. Even if some in financial markets labelled this as a victory for crypto-assets and implied that this was due to their perception as safe havens, the truth is that these wild swings in prices do not contribute to stability.

Figure 2: Evolution of Bitcoin price following the collapse of SVB (2023)



Source: Statista

Main crypto-assets by market capitalisation: Bitcoin and Ethereum, 2 stablecoins and a meme coin

According to CoinMarketCap, by early January 2024 there were almost 9,000 crypto-assets, however, only 2 of them (Bitcoin and Ethereum) concentrate a market capitalisation share of more than 80%, as can be seen in *Table 1*. Nevertheless, the market share of Bitcoin has significantly decreased in the last few years; in 2016, it was above 90%.

Table 1: Crypto-asset per market share (26 March 2024)

Crypto-assets	Market Cap (billion USD)	% crypto market share
Bitcoin	1368	61,8
Ethereum	430	19,4
Tether	104	4,7
BNB	88	4,0
Solana	85	3,8
XRP	35	1,6
USDC	32	1,4
Dogecoin	26	1,2
Cardano	24	1,1
Avalanche	22	1,0

Source: CoinMarketCap (26 March 2024)

There are some important differences between Bitcoin and Ethereum: (1) whereas Bitcoin only offers a crypto-asset or token, Ethereum offers both tokens and the technology, a distributed machine, for executing smart contracts and the connection of decentralised applications (dApps); (2) as indicated above, Bitcoin relies on a proof of work consensus mechanism, whereas Ethereum has moved to a proof of stake mechanism; (3) the different type of consensus mechanism used implies that new Bitcoins are created through 'mining', whereas new Ethereum tokens are created by 'minting'; (4) whereas there is cap on the maximum amount of Bitcoin that can be created (21 million), there is none in Ethereum (there is only an annual cap, 18 million); and (5) blocks in Bitcoin's blockchain are validated every 10 minutes, in contrast to blocks in Ethereum, which are validated every 12 seconds.

Since there is a maximum cap of 21 million Bitcoins (in order to be anti-inflationary) and there are already more than 18 million Bitcoins in circulation, one could argue that this limit will soon be reached. However, this is not the case because of 'halving'. 'Halving' basically implies that the rewards obtained by miners decrease for every 210 000 blocks that are mined, which on average happens every 4 years. At this pace, it is estimated that 21 million Bitcoins will only be mined by the year 2140. 'Halving' practices logically decrease the incentives for mining activities, as rewards are deemed to be constantly lower.

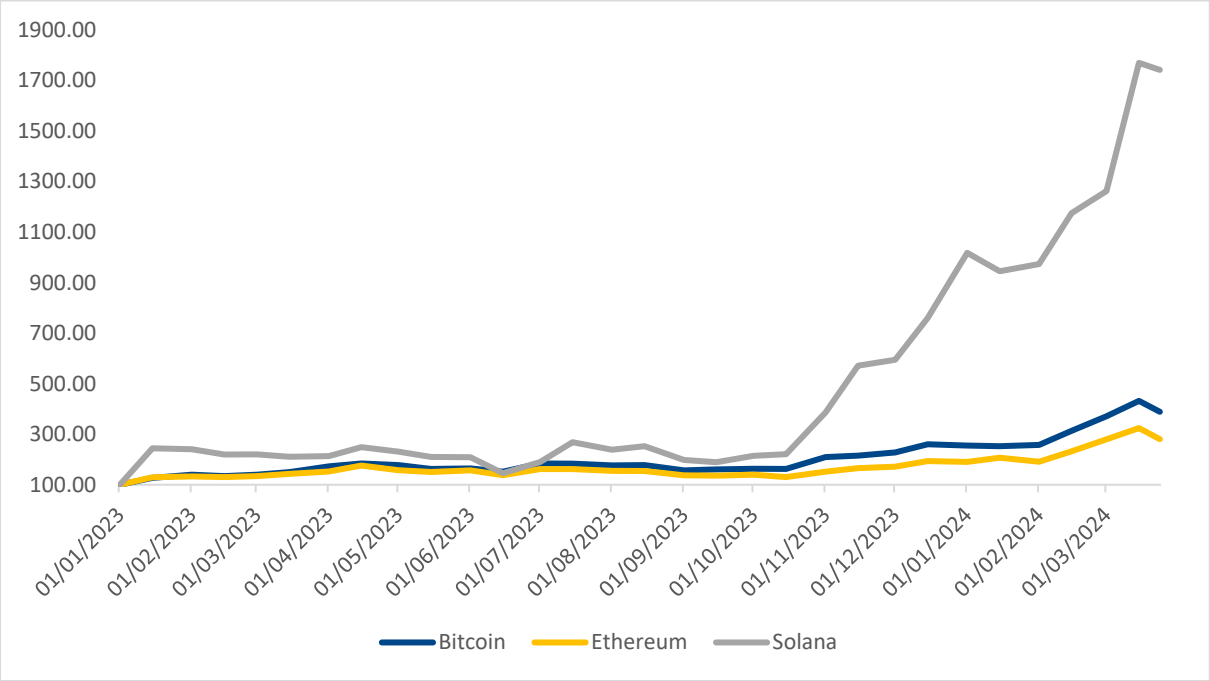
An interesting development for Bitcoin is its introduction as legal tender in El Salvador. In 2021, the parliament in El Salvador voted to accept Bitcoin as legal tender, which led the government to purchase Bitcoin intensively. However, only a few months after the government invested in Bitcoin, the value of Bitcoin dropped significantly, exposing the economy to the volatility of Bitcoin. The value has surpassed the purchasing price since the beginning of 2024, but the economic impacts generated by the adoption remain unclear. While public reserves should have increased, a lot of investment was required to establish the infrastructure to use Bitcoin. The government also had to use public campaigns to try to convince the population to adopt it. It has become clear with the fluctuations in Bitcoin's value since 2021 that the government has no control over the stability of its currency and their economy fully exposed to speculation.

Of the 10 crypto-assets with the the highest market capitalisation, there are 2 are so called 'stablecoins': Tether and USDC. More information on stablecoins will be provided under the next section.

Interestingly, Dogecoin (#10 by market share) was originally a meme coin. In 2013, It was created by two software engineers who created a crypto-asset as a joke to demonstrate how easy it was to create one. Nevertheless, the 'likes' in social media of well-known businessmen such as Elon Musk took the crypto-asset to a completely different realm, making it now the tenth most important crypto-asset in terms of market capitalisation.

The Solana crypto was developed to promote the use of Decentralised Finance (DeFi). Solana is simultaneously a crypto platform and a crypto-asset. It enables high speed transactions by bundling them, while still relying on a consensus mechanism. This allows for large-scale transactions, similar to those from traditional payment schemes. In 2023, the increase in the price of Solana reached 1,000%, – way above the price evolution of other major crypto-assets, as can be seen in *Figure 3*.

Figure 3: Evolution of the price of Bitcoin, Ethereum and Solana since 1 January 2023 (Base = 100)



Source: Statista – price evolution Bitcoin, Ethereum and Solana

Avalanche is another interesting crypto currency. The solemn focus of the currency is to ensure fast and low cost transactions. The use of Avalanche has increased significantly in the past few months and low transaction fees have managed to make it an interesting platform for DeFi crypto transactions.

Another interesting crypto is XRP and the XRP ledger. Developed in 2012 and used by Ripple, it was introduced to fill the gap of low cost and fast decentralised payments technology. It was developed to facilitate payments between businesses, allowing them to use the platform to achieve more efficient cross-border payments.

Stablecoins: a good option against volatility?

Stablecoins can guarantee their value through various systems, mainly through the backing of fiat currency, financial instruments, other cryptocurrencies, or algorithmically.

Kickstarting the development and discussions of stablecoins in 2019 was Libra (later called Diem). It was developed by Facebook (now Meta) to allow users to purchase tokens for digital exchanges from any currency. These tokens would be backed by currencies and securities. The coin raised many concerns among regulators, which led to a lack of trust in the currency. It was feared that the coin would be used for money laundering, and as a result it was eventually dismissed.

Five years later, the stablecoin market is valued at more than USD 130 billion and is largely dominated by two digital cash assets, Tether and USDC. While most of the assets are backed in US dollar equivalents, the stablecoin market is starting to see interest from traditional players like PayPal and Société Générale, as will be explained below.

A first example of a currency backed stablecoin is the Tether token. Launched in 2014, Tether is mainly purchasable as backed by US dollars, but it can also be held in Chinese yuan, euro, and Mexican peso

equivalents. Every Tether dollar is supposed to have a reserve equivalent ensuring it remains pegged 1-to-1 with the USD. The Tether is also available for purchase in gold equivalent. The reserves held are split between cash and cash equivalents (such as US Treasury bills and Reverse Repurchase agreements), corporate bonds, precious metals, secured loans and Bitcoin. The USD-pegged Tether has experienced marginal turbulence on multiple occasions.

In April 2017 the value of Tether dropped almost 10% below the value of the dollar. The decoupling from the dollar lasted for a few months, before re-stabilising back at the initial 1-to-1 level. A similar event occurred between October and December 2018, with a 2-3% value deviation from the 1-to-1 level. However, since May 2020, Tether has never deviated by more than a few thousand up or down from the dollar. Backed by reserve assets, Tether can be considered a more stable crypto alternative to Bitcoin or Ethereum. Nevertheless, the stability of the coin relies on the stability of the reserve currency. Further, it relies on transparency over the assets held, ensuring continuous trust in the stablecoin. However, its value remains very sensitive to any transparency rumours linked to the internal assets held to back the stablecoin and potential external reputational changes of crypto currencies in general.

The other major stablecoin, also mainly backed in US dollars is the USD Coin (USDC). The USDC is regulated and reserved in dollars, theoretically making it possible, to always exchange one USDC for a US dollar. The USDC is backed by the SEC-registered Circle Reserve Fund. Composed of short-dated US Treasuries, overnight US treasury repurchase agreements, the fund is complemented by cash holdings at Reserve Banks. While an EURC is also available, the volumes in circulation, and hence the reserve volumes, are limited. While there is a USD equivalent of 24.3 billion in circulation, the euro equivalent is limited to EUR 51.1 million (7 December 2023). The EURC is backed 1-to-1 with the euro through cash reserves held in American financial institutions. To assure transparency and maintain trust in the USDC, reserve holdings are disclosed weekly. On top of the weekly reporting, auditors from the big four review reserve holdings monthly, this, in order to ensure truthful behaviour. Introduced in 2018, the USDC has only seen minor fluctuations over the years, generally never exceeding a 4% increase or decrease in value. Since April 2020 it has never dropped below 0.968 or risen above a value of 1.01 compared to the US dollar. The only exception was in March 2023, when the Silicon Valley Bank went bankrupt.

Circle, issuer of USDC, had deposited more than USD 3 billion in reserves at SVB. When SVB went bankrupt, the reserves went idle and the USDC no longer held reserves equal to the USDC amount in circulation. Creating uncertainty in the capacity of Circle to fill the gap, many rushed to sell USDC creating a rapid drop in value. The drop was, however, short lived as just days after SVB's bankruptcy, the Federal Reserve published a statement that it would cover all deposits held in the bank, meaning the reserve issue was no longer an issue for the USDC and the value returned to initial levels. In any case, this episode points to potential risks to the value of a stablecoin on the backing side as well as the issuing side (i.e. it is not just enough to have 1:1 backing, with the type of asset and the issuing entity or the entity where that asset is held playing a crucial role for the stability of the crypto-asset too).

Stablecoins have been shown to be sensitive to external factors. As the USDC showed, it was an external factor that caused the drop in value even when maintaining the committed 1-to-1 ratio with the USD. While Circle was trying to take measures to bring back the value of USDC to the intended level, it was ultimately the measures taken by the US Federal Reserve that restored confidence in the stablecoin.

Even if the volatility episodes of Tether and USDC has been occasional and short lived, there are other cases that ended with the disappearance of a stablecoin. A case in point is UST, an algorithmic stablecoin which aimed to maintain a value stable at USD 1 through interaction with another crypto,

Luna. However, in May 2022, UST's value decoupled from the dollar, triggering a massive sell-off, with its value plummeting to USD 0.20, and afterwards disappearing.

PayPal's stablecoin

The announcement on 7 August that PayPal would launch a stablecoin pegged to the US dollar (PayPal USD) caused quite a stir, as it was felt that this time around such a project could be a real success, as the idea was being promoted by a big player in payment systems used to dealing with regulators. Analysts even believed that what Facebook-Meta was not able to achieve with Libra-Diem would now be achieved.

PayPal has shown a strong interest in crypto-assets in the past few years. As early as October 2020, it announced that it would allow US users to buy, sell and hold certain crypto-assets. It expanded the service to customers in the UK in 2021 and Luxembourg in 2022. In 2023, PayPal announced the launch of PYUSD, a dollar-denominated stablecoin, available to its US-based customers.

PayPal USD is not an algorithmic stablecoin, seeking instead to guarantee its parity with the dollar by being fully backed by US dollar deposits, US government bonds and cash-like assets. This point is important: in a context of above-zero and rising interest rates, the returns from investments in the backing assets would go to PayPal and not to the stablecoin holders. That is, if instead of holding the stablecoin, the investor were to replicate the PayPal USD backing portfolio, they would earn the returns on those investments.

Initially, this crypto-asset will only be available to PayPal users in the US, allowing them various functionalities, such as transferring PYUSD between PayPal and compatible external wallets, making person-to-person payments using PYUSD, financing purchases with PYUSD and converting any of the cryptocurrencies supported by PayPal. PayPal executives have acknowledged that there is still a long way to go before the crypto-asset can be widely used for retail payments.

PYUSD would operate on the Ethereum blockchain network and would be issued by Paxos. This other point is also relevant: the issuer of PYUSD would be a New York-based crypto-asset trust corporation. Neither PayPal nor Paxos are supervised by a federal banking agency in the US, and in case of problems, they would not have access to FDIC funds. In other words, a deposit of up to USD 250 000 in an FDIC member institution in the US would be guaranteed by the FDIC. The same amount in PayPal USD would have no such guarantee and, in line with what is described above, no remuneration.

Société Générale's stablecoin

On 5 December 2023, Société Générale, France's third largest bank, announced the issue of its stablecoin Euro CoinVertible. As the name suggests, the first version of this coin would be pegged to the euro (EURCV). Confirmed in the Whitepaper, it will pegged to the euro and backed by cash and purchasable under the name EURCV. Under MiCA, which will become fully applicable as of the end of 2024, EURCV would be an Electronic Money Token, and a 'digital asset' ('*actif numérique*') under French Law, although the Autorité de contrôle prudential et de résolution (ACPR) has not yet classified it. The legal issuer of EURCV would be Société Générale Forge (SG-FORGE), a licenced investment firm under MiFID 2 and a registered digital asset service provider in France. Like other crypto-assets, EURCV would be based on blockchain technology, accessible through the Ethereum public blockchain. According to the White Paper issued by SG-FORCE, EURCV has been structured to meet the main requirements of the MiCA Regulation. However, the stablecoin is currently being restructured to comply with the upcoming MiCA Regulation, although it might still be subject to evolutions to fully comply with MiCA and also to the EU DLT Pilot Regime for Security Token Regulation.

As stated in the White Paper, the three key elements of EURCV project are: (1) a clear legal structure, (2) resilient collateral and financial mechanisms and (3) a robust technical framework. The legal structure relies on the full segregation of collateral assets from the fiduciary's own assets and activities and a direct recourse of the EURCV holders on the collateral.

As for the resilience of the collateral, EURCV will currently be backed exclusively by cash deposits. Collateral assets composition and valuation will be published on SG-FORCE's webpage every day. Regarding the technical framework, EURCV relies on the CAST Framework, an open-source initiative, built and implemented by major financial institutions, designed to foster adoption of digital assets, by providing legal, operational and technical frameworks.

SG-FORGE may accept a range of assets in exchange for EURCV. Since EURCV is a digital asset and not a debt instrument, the holder will only have a claim against the fiduciary and no redemption rights against SG-Forge.

Just over a week after Société Générale, DWS, announced that they will launch a euro denominated stablecoin during 2024. Through AllUnity, a joint venture between DWS, Galaxy Digital and Flow Traders, a stablecoin will be made publicly available. According to DWS CEO, Stefan Hoops, the venture will 'bridge the gap between traditional and digital finance ecosystems'. While the project seems to be entering its final stages, there are still some legal requirements that need to be met. These requirements include obtaining an Electronic Money Institute licence and the requirement under MiCA to publish a white paper.

Why would a traditional financial player want to issue a stablecoin?

First, it is a way of showing leadership in innovation and digital trends, as traditional financial players have not issued crypto-assets massively until now. By issuing a stablecoin, the players are hoping to get access to a new client base, tapping the crypto community and breaking the silos.

Second, according to the issuers, the stablecoin intends to offer added value in wholesale processes, such as corporate treasury, cash management, liquidity funding and refinancing solutions.

Third, by demonstrating such a proactive and pioneering attitude, the issuing entity is attempting to position itself as an influential player in policy decisions. For instance, in the White Paper, SG-Forge calls for the setting of common operating standards, similar to the CAST initiative, on which EURCV is based, and advocates for a set of principles and goals for asset tokenisation.

Fourth, issuing a stablecoin allows credit institutions to enter the crypto market and have their assets traded on crypto exchanges.

Fifth, depending on how the stablecoin works, the issuing entity could make money out of it: capital gains stemming from deposits and securities could be kept by the issuer, with the stablecoin holder exclusively receiving the initial value.

Finally, it is a way for banks to fight deposit flight if stablecoins were to be considered safer and become popular. Entering the market would allow them to keep customers from moving their assets to the stablecoins of new competitors. Traditional players have an advantage compared to new market entrants, as they are licenced, facilitating the issuing of a stablecoin.

And why would financial consumers want to own those stablecoins?

The answer depends very much on whether we are talking about a retail or a wholesale customer. In the case of a retail customer, the interests are not as clear-cut. In fact, if the stablecoin holder replicated

the collateral investment portfolio, instead of investing in the stablecoin, they would retain the proceeds of those investments. However, in the case of a stablecoin, unless otherwise designed, they will simply recover the value they initially invested.

Moreover, irrespective of the transparency and high quality of the collateral and even if the issuing entity is linked to a traditional bank, retail customers need to understand that they are not covered by any Deposit Guarantee Scheme. Nevertheless, in the case of wholesale customers, properly designed stablecoins can bring added value along the lines of some use cases. For retailers interested in holding crypto, purchasing stablecoins puts the holder on-ramp, which would allow them to purchase other crypto-assets directly, without the need for any further exchanges. Later when the crypto is reconverted to a stablecoin, the holder can choose to hold it, to reinvest it in another crypto-asset, or convert it back to fiat currency.

Public keys, private keys and wallets

Purchasing crypto is always accompanied by holding an access key. This security key can either be a private key or a private and public key. Both types of access keys use cryptography to ensure high protection and safe access to any crypto holdings.

Cryptography is based on three properties. The first property regards confidentiality. It ensures that access to the encrypted information and its content is limited to key holders. The second property regards integrity. The integrity part of cryptography, protects the available data in order to ensure its reliability. In crypto this takes the form of the blockchain, where mutations made to the data are visible to everyone that is part of the chain. The third property regards authenticity. This ensures that the public or private key holder is the single entity capable of encrypting and decrypting the stored information.

A cryptographic key scrambles data in order to make it random, ensuring that only the key holder is able to reorganise and unlock the data. The data remain ‘scrambled’ making any access impossible until a key is used to restructure the data, allowing for access.

Taking a closer look at the two types of cryptography used in securing crypto, we first look at the private key, also known as symmetric cryptography. Symmetric cryptography uses a single key to encrypt and decrypt access. The key is able to dismantle the data that is encrypted between the holder and the crypto manager and is held privately with only the key holder capable of accessing the encrypted crypto.

The second type of encryption key is the public key cryptography, also known as asymmetric cryptography. Asymmetric cryptography is the most common type of encryption used in blockchain technology. The technology is based on the use of two keys where, on top of the private key, a public key is added before using the private key to unlock the protected data. As the name stipulates, the public key is available to anyone to use. However, the data that have been encrypted with the public key require a private key to be decrypted. The public key intervenes first. It will algorithmically encrypt the text that is received in order to create a cipher text. It is then that the cipher text is decrypted with the private key, coming out again as plain text.

Private keys can be both physical or digital. The platform used to purchase crypto, together with the holder preference, will define whether they use a physical or digital wallet to hold their encryption key.

The most common type of physical key is a USB private key. This option is appealing for crypto holders who wish to store the key in a physical location and avoid online connectivity.

Digital keys, on the other hand, are usually stored in a mobile app or through the use of software, in 'wallets'. A digital wallet is available in two different structures, a hosted wallet and a non-custodial wallet. In most situations, when crypto currency is purchased via an application, it remains within the application. After an individual purchases crypto, the platform continues *hosting* it. The purchase is then accessible through the wallet set up on the platform. Hosted wallets offer customer solutions for lost or forgotten passwords and keep the crypto stored on the holder's account. While they facilitate holding crypto, online hosted wallets are much more sensitive to external threats such as hacking and scams.

A non-custodial wallet, also called a self-custody wallet, does not use a third party to hold the crypto. Instead, the customer has purchased a software that enables local storage of the purchased crypto. Two types of software wallets are available to customers, hot wallets and cold wallets.

A hot wallet is always connected to the internet and allows for the purchase and sale of crypto at all times, while cold wallets are held offline. While they can connect to the internet, they require additional actions to enable crypto transactions.

The cold wallet has the advantage of less exposure to external threats, such as to hacking and cyber-attacks. The customer is fully responsible for safeguarding their holdings and ensuring that their private key is kept safe. Should a customer lose the key or forget the password, it is almost impossible to retrieve the crypto held within the software. If someone finds the key, they would have full access to the content of the wallet. Chainalysis found that 20% of Bitcoins held in 2020 had not moved in 5 years or more, meaning that they were considered lost. This equates to 3.7 million Bitcoin, which is worth USD 258 billion at today's Bitcoin value.

Over the years, crypto holders have been victims of multiple and increasingly reoccurring hacks and cyber-attacks. The years 2021 and 2022 saw significant increases in the number of attacks on crypto trading platforms and on volumes stolen during the hacking. The most hacking intensive year in terms of number of attacks to date (awaiting the final numbers for 2023) with more than 200 attacks, was 2021. The number of attacks decreased in 2022, but the value of stolen assets increased, with the value of cryptos stolen totalling more than USD 3.8 billion.

The largest hack of cryptocurrency so far occurred in March 2022. The victims of the attack were the Ronin Network exchange, where the blockchain bridge was targeted, as mentioned above. Stablecoins were the focus of the hack with Ethereum and USDC coins valued at USD 615 million stolen. The hacking was made possible through the theft of private keys.

In 2021, another major hack took place, with crypto tokens worth USD 613 million stolen. The victim of the breach was the swapping platform Poly Network, a centralised crypto trading platform. While the breach was extensive, the hacker returned all the money. A large crypto attack also took place in 2018 on the Coincheck exchange. Hackers managed to retrieve crypto-assets worth more than USD 500 million and more than 260 000 Coincheck customers were victims of the attack. Since then, Coincheck has reimbursed all victims.

The world's largest crypto platform, Binance, was also victim of a hacking in 2019. During the attack one wallet was targeted and the victim lost Bitcoins worth USD 40 million. The hackers were able to carry out the attack by obtaining public and private keys data, allowing them to unlock and transfer the Bitcoins. Following the attack, the full value of the stolen Bitcoin was reimbursed by Binance.

The incidents mentioned above represent just a very small share of all hacks and breaches that have taken place in the last few years. There have been increasingly large thefts, with victims reimbursed for

some breaches. DeFi trading platforms have opened up to fulfil the increased demand for trade in crypto. A selling point for decentralised trading platforms has been the increased transparency they bring to crypto trading. While bringing opportunities for interested parties by facilitated access and increased transparency in crypto trading, it has also led to an increasing number of hacking opportunities as more information is shared by the platforms, allowing qualified hackers to exploit security loopholes.

Exchanges or crypto-assets trading platforms

Exchanging crypto is most commonly done via two different types of crypto exchange, centralised crypto currency exchanges (CEX), and decentralised crypto exchanges (DEX). The first type, the CEX, functions just like a traditional stock exchange, as an intermediary between the buyer and seller. The second type of exchange, the DEX, allows for peer-to-peer crypto transfers. Both types of exchanges have advantages and disadvantages.

A CEX is on average more user-friendly and reliable, as it facilitates crypto trade within a defined structure while limiting the users' responsibility. They can however be more costly because of transaction fees and are more exposed to scams and fraudulent activity.

While DEXs are less exposed to external threats, they are more complex to use and trading from crypto to fiat currency is more challenging.

The growing popularity of purchasing crypto-assets has generated an increasing number of crypto trading platforms. CoinMarketCap, the world's largest crypto trading tracker, follows the trading activities of 224 different crypto exchanges.

The largest CEX is Binance, with almost 170 million users and a trade of crypto worth USD 65 billion daily. The platform allows the purchase and sale of more than 350 different crypto coins with trading available in more than 100 countries. The second largest but significantly smaller CEX is Coinbase. Also available in over 100 countries, the platform had a total trade volume of USD 154 billion in the last quarter, spread across more than 100 million users.

DEXs are significantly less popular than CEXs. According to CoinMarketCap, the largest decentralised DEXs are dYdX and Uniswap v3, with, at the time of writing this (March 2024), trades over the last 24h of around USD 1 billion. While popular and representing large volumes traded, it is significantly less than the average daily trade on Binance.

Founded in May 2019, FTX Trading Ltd (FTX) was one of the world's largest CEXs. Available for trade in Europe, Japan, the US and Hong Kong, it offered trade of crypto currencies and of stablecoins and later turned out to be an outright fraud.

The successful rise of FTX was almost as rapid as its fall. Over a period of only a few years it managed to establish itself as one of the world's leading crypto trading platforms. This success story ended abruptly in November 2022. Following the resignation of the CEO and co-founder Bankman-Fried, it was made public that the company was under investigation for fraudulent activity. Just a few weeks after the resignation of Bankman-Fried, the company filed for bankruptcy and Bankman-Fried was found guilty of fraud, conspiracy and money laundering.

FTX had developed a token, the FTT. It could be purchased and used on the FTX platform in order to get discounted fees or different types of rewards. While appearances show similarities with shares in a firm, FTT holders did not receive benefits generated by the FTX platform. The token played a crucial

role in the collapse of FTX when it was revealed that the FTT token had been used to inflate the balance sheet of FTX and Alameda Research, FTX's hedge fund. When it became known that parts of the funds had been used for taking out risky loans, the main competitor Binance, decided to sell all its FTT holdings, generating an exchange run.

The collapse of the FTX exchange has become a prime example for crypto sceptics. Crypto-assets are based on the idea of a decentralised financial system that does not fall under the same regulations as other financial institutions. The lack of transparency in this system runs the risk of generating criminal activity that is only unveiled when the consequences of its collapse are significant. In this case there was an USD 8 billion gap that had to be filled, money that those due will never fully be compensated for.

The beneficiaries of the FTX exchange are DEXs. By deteriorating the reputation of centralised crypto exchanges, DEXs gain the opportunity to showcase the advantages of a decentralised system that no longer relies on the appropriate behaviour of a centralised exchange.

The fall of FTX had significant impacts on crypto markets. Crypto exchanges with holdings in FTX were forced to temporarily freeze withdrawals, and a general decrease in trust was experienced towards the end of 2022.

The case of FTX highlights the need to put transparency requirements of crypto exchanges on a par with traditional exchanges. Increased transparency can help prevent other crypto exchanges from committing fraud as well as combat money laundering. This is why, over the last few years, multiple initiatives and regulations have been developed, with a particular focus on identifying those involved in crypto transfers.

Crypto-assets and financial interconnectedness

Crypto-assets are still marginal in financial terms, representing around 1% of the entire global financial system. Nevertheless, interconnections between traditional financial players and crypto-assets are increasing.

The case of the collapse of Terra-Luna is a clear example of this. In fact, with the collapse of UST and Luna, the private equity fund specialised in crypto investments, Three Arrows Capital, had to declare bankruptcy in May 2022, given its high exposure to the misnamed stablecoin. Far from being confined to this area, the financial earthquake also hit the financial firm Voyager Digital, which in July 2022 had to declare bankruptcy when it was unable to recover the loan of more than USD 600 million it had made to Three Arrows Capital. Celsius was also another victim of the UST and Luna reverberations, declaring bankruptcy in July 2022.

Silvergate Bank was a traditional financial institution offering services such as savings and loans to its customers. In 2016 it decided to start offering cryptocurrencies to its customers and lending to crypto companies. By expanding its activities, Silvergate Bank tried to bridge traditional finance with a crypto offering. The expansion progressively led the bank to focus most of its activities on lending to crypto institutions. Severely struck by the heavy crypto drop in 2022 and the collapse of FTX, the bank was forced to liquidate in 2023.

Signature Bank, similar to Silvergate Bank, was forced into liquidation in 2023. The bank was involved in traditional banking activity as well as in lending to crypto currency companies. When the Silicon Valley Bank collapsed in March 2023, Signature Bank experienced large deposit withdrawals, a bank run, from

their accounts. To prevent the bank from failing and causing a contagion of banking failures, regulators shut down its operations.

The need for public sector intervention: regulation

An interesting debate has arisen regarding the appropriateness of regulating crypto-assets. Some think introducing a regulation other than upfront prohibition would be a way of legitimising crypto-assets. In light of all the risks they entail, with many of them already materialising as explained before, it would simply be better to let crypto-assets self-combust and disappear.

In an ECB blogpost published on 22 February 2024, the Director General for Market Infrastructure and an adviser at the same Directorate-General 'reiterate that the fair value of Bitcoin is still zero'. More specifically, they highlight the following points: (1) Bitcoin transactions are still inconvenient, slow, and costly, only being used for payment in the darknet. Even the granting of legal tender status by the government in El Salvador has not managed to establish Bitcoin as successful means of payment; (2) Bitcoin is still not suitable as an investment, and does not generate any cash flow or dividends; and (3) the mining of Bitcoin using the proof of work mechanism continues to pollute the environment on the same scale as entire countries. Referring to the recent decision by the SEC to authorise a number of Bitcoin ETFs, ECB's officials argue that 'the use of ETFs as financing vehicles does not change the fair value of the underlying assets. An ETF with only one asset turns its actual financial logic on its head (although there are others in the United States). ETFs normally aim to diversify risk by holding many individual securities in a market'. They also refer to price manipulation, financing of criminal activities and lack of social benefits. Finally, the blogpost argues for a more stringent regulatory approach and criticises the EU and US's regulatory solution for including compromises that could be understood as a partial approval of Bitcoin investments and failing to deal with environmental costs.

Nevertheless, the approach followed by the EU, the UK and other international regulators is not to remove crypto-assets from the market, but rather to create a framework within which risks are limited as much as possible. Former ECB Board Member Fabio Panetta said he believes that crypto-assets will not disappear, as they intrinsically represent a way of gambling that has always been attractive to humanity. He argues that the societal cost of not regulating cryptos would simply be too high and lead to not protecting uninformed investors and not preventing the use of cryptos for tax evasion, money laundering, terrorist financing and the circumvention of sanctions.

The regulatory approach in the EU

The European Union is pioneering the introduction of crypto-assets' regulation under the name Market in Crypto-assets Regulation (MiCA), which even if it has already entered into force, it will only be applicable as of 30 December 2024. The objective of MiCA is to regulate and supervise the issuance, public offering and admission to trading of crypto-assets, as well as crypto-assets' service provision. Crypto-assets are defined as '*a digital representation of value or rights which may be transferred and stored electronically, using distributed ledger technology or similar technology.*' MiCA does not cover the issuance of traditional assets using DLT nor the issuance or provision of services of completely decentralised crypto-assets (e.g. Bitcoin). Central Bank Digital Currencies are not covered by MiCA either and Non-Fungible Tokens (NFTs) and Decentralised Finance (DeFi) are also left outside the scope.

The Regulation identifies three different types of crypto-assets, namely, Electronic Money Tokens (EMTs), Asset Referenced Tokens (ARTs) and crypto-assets which are neither EMTs nor ARTs and are not covered by MiFID. While EMTs purport to maintain a stable value by referring to the value of a fiat

currency that is legal tender, ARTs refer to the value of several fiat currencies that are legal tender, one or several commodities or one or several crypto-assets, or a combination of such assets. Therefore, the difference between EMTs and ARTs lies in the type of underlying asset, with ARTs using non-cash assets or a basket of currencies and EMTs a single currency, bringing them closer to the concept of electronic money.

EMTs can be offered by electronic money institutions or by credit institutions, which must produce a White Paper, to be notified to the competent authority. Electronic money institutions issuing EMTs will have to comply with electronic money regulations[1] regarding prudential requirements, capital, own resources, activities, relationships with third countries and exceptions. With regards to operational and liquidity risks, the competent authority can request compliance with obligations applicable to ARTs, such as reserve assets and own resources. Proceeds will have to be invested in safe and low risk assets denominated in the EMT's reference currency, with at least 30% of funds being in deposits in credit institutions. The holder of the EMT has a reimbursement right of the funds at any moment and for the nominal value. The issuer of the EMT cannot pay interest and needs to prepare a recovery plan and an operational plan to ensure reimbursement.

ARTs can only be offered by authorised institutions, by a competent authority or by credit institutions. Credit institutions do not need to apply for a specific authorisation to issue ARTs, but like the authorised institutions, need to prepare a White Paper, to be approved by the competent authority. The ECB can issue a binding opinion against the issuance, both ex ante and ex post. The main obligations issuers face are:(1) transparency (publication of the White Paper, market information and reserve assets), (2) policy to describe the ART's stabilisation mechanism, (3) the issuer cannot pay interest, (4) the issuer needs to prepare a recovery plan and an operational plan to ensure reimbursement, (5) if the issuer is not a credit institution, there is the obligation to count on own resources at all times and to seek authorisation for the acquisition of significant shareholding participation in the issuer. ART's reserve assets (i.e. the assets used as collateral) need to be operationally segregated from the rest of the assets and liabilities of the issuer, allow for the permanent reimbursement to holders, be valued at market prices and have an aggregated value of at least the ARTs in circulation.

ARTs and EMTs can be classified as 'significant' by the European Banking Authority (EBA), if they meet certain criteria. Guidance thresholds for the EBA to define and assess the criteria are included in MiCA. If an ART or EMT is classified as 'significant', they will be subject to additional requirements and the EBA will be responsible for carrying out relevant supervisory tasks such as establishing, managing and chairing supervisory colleges for all significant ARTs and significant EMTs. As for the direct supervision of issuers, the EBA will be solely responsible for significant ARTs, whereas significant EMTs will lead to a dual supervision by the EBA and the respective National Competent Authority.

As for crypto-assets which are neither EMTs nor ARTs and are not covered by MiFID, supervision will focus on offerors or persons seeking admission to trading of these crypto-assets. The offerors and the persons seeking admission to trading need to produce a White Paper, notify it to the competent authority and make it public. The offerors also need to ensure that the funds or crypto-assets collected during the offer to the public are kept in custody by a third party and that the retail buyer benefits from a right of withdrawal for 14 days.

Regarding crypto-assets service providers (CASPs), MiCA refers to the following: (1) the custody and administration of crypto-assets on behalf of clients; (2) the operation of a trading platform for crypto-

[1] The EMD is currently being reviewed and amendments are made in order to regulate EMDs and their activities under the two legislative proposals, the Payment Services Regulation and the Payment Services Directive 3.

assets; (3) the exchange of crypto-assets for funds; (4) the exchange of crypto-assets for other crypto-assets; (5) the execution of orders for crypto-assets on behalf of clients; (6) placing of crypto-assets; (7) the reception and transmission of orders for crypto-assets on behalf of clients; (8) providing advice on crypto-assets; (9) providing portfolio management on crypto-assets; (10) providing transfer services for crypto-assets on behalf of clients.

CASPs will need to obtain authorisation from the competent authority, specifying the services they will provide. They will also need to have a registered office in the Member State where part of their services is provided and will be allowed to provide services in the EU, through the right of establishment and freedom to provide services. CASPs are allowed to carry out activities beyond crypto-asset service provision. Credit institutions are allowed to provide the full range of services; investment firms can provide all services except transfer ones; alternative investment funds are entitled to provide reception and transmission of order services, as well as advisory and portfolio management services; electronic money institutions can provide transfer and custody services; central depository services can provide custody services; and trading platforms are allowed to operate crypto-assets' trading platforms.

Under the MiCA regulation, players located in third-party countries can benefit from the reverse solicitation exemption. This exemption, in order to not become the evident loophole of the legislation, will not be applicable for EU-based firms. If the reverse solicitation is not properly controlled, it could lead to misuse with large amounts of market actors avoiding the need to comply with the new legislation. To avoid such practices, the European Securities Market Authority has been charged under MiCA to develop guidelines on supervisory practices that allow for the detection and prevention of misuse of the reverse solicitation exemption.

The regulatory approach in the UK

The legal framework for crypto-assets in the United Kingdom has substantially changed following the adoption in 2023 of the Financial Services and Markets Act 2023 (FSMA). Under the FSMA, the definition of 'investment' encompasses crypto-assets, which are broadly defined as *'any cryptographically secured digital representation of value or contractual rights that can be transferred, stored, or traded electronically. This broad definition is a strategic move to encompass a wide array of digital assets within the regulatory perimeter'*.

The FSMA also introduces the 'Designated Activities Regime', to ensure that crypto-asset activities are properly regulated, and encompasses issuance, payment, exchange, investment, lending, safeguarding, and validation/governance activities related to crypto-assets.

Acknowledging the specific risks stablecoins can create in terms of financial stability and investor protection, the FSMA introduces specific provisions for payment stablecoins, which are addressed through the concept of Digital Settlement Assets. DSAs are defined as 'digital representations of value or rights used for settlement of payment obligations, which can be electronically transferred, stored, or traded'.

The FSMA also foresees specific provisions for the failure of systemic stablecoin firms, aiming at ensuring the continuity of services and the return of client funds and assets in case of failure.

Finally, the FSMA empowers the UK Treasury to establish financial markets infrastructure sandboxes, the first of which is the digital securities sandbox. The latter aims to understand how existing legislation must be adapted to accommodate digital assets and their related services.

The regulatory approach in the US

The legal framework for crypto-assets in the United States is currently fragmented, with several regulatory bodies and agencies involved, and ongoing legislative efforts to further clarify the role of federal stakeholders.

The Securities and Exchange Commission (SEC) has regulatory authority over securities. The determination of whether a financial instrument is a security is based on the 'Howey Test', which is applied to each individual case, including when the SEC determines if a digital asset is a security. It should be noted that on 10 January 2024, the SEC approved the listing and trading of a number of spot Bitcoin exchange-traded product (ETP) shares. Nevertheless, this decision came together with a set of measures to increase investor protection, namely: (i) sponsors of Bitcoin ETPs will be required to provide full, fair, and truthful disclosure about the products; (ii) these products will be listed and traded on registered national securities exchanges, which are required to have rules designed to prevent fraud and manipulation; (iii) 10 spot Bitcoin ETPs have been approved simultaneously, helping create a level playing field for issuers and promoting competition. Moreover, Gary Gensler, Chair of the SEC, underlined the speculative nature of Bitcoin in a statement.

The Commodity Futures Trading Commission (CFTC) oversees commodities. Since Bitcoin and Ethereum are considered commodities under US law, they are overseen by the CFTC, including possible attempts of market manipulation. However, the classification of other crypto-assets as commodities remains less clear.

The Financial Crimes Enforcement Network (FinCEN) and State Regulators have jurisdiction over certain crypto-asset activities. While the definition of virtual currency varies among states, it is generally seen as a form of monetary value. New York and Louisiana, in particular, have specific licence types for virtual currency transactions. A current example of a regulatory proposal made by the FinCEN in the US regards Convertible Virtual Currencies (CVCs). CVCs combined with mixing practices have been receiving additional attention from regulators over the last years as they are believed to be closely linked to money laundering activities. CVCs are digital assets acting like a substitute for a 'real' currency as it is very easy to purchase and sell CVCs in exchange for fiat currency. The main use cases of a CVC is for purchasing goods, paying for services or for digital trading. The rationale behind the use of mixing software when transferring CVC assets is for it to act as cash equivalent, not making every asset movement traceable. However, as mixing obfuscates the source, destination and amount involved in a transaction, regulators see a potential close link between its use and money laundering, hence the reaction of US regulators.

There are currently several legislative proposals and bills aimed at clarifying the regulatory framework for digital assets in the US For instance, the Lummis-Gillibrand Responsible Financial Innovation Act seeks to define the roles of federal stakeholders, impose requirements for stablecoins, and dictate tax treatment among other things. Another proposal aims to grant regulatory jurisdiction entirely to the CFTC.

Some policy recommendations

Out of the three regulatory regimes presented above, the most comprehensive one is that of the EU via MiCA. But even if that is the case, MiCA will provide legal certainty for businesses, counterparties and consumers, but will only mitigate against potential risks posed by cryptos, not responding to all risks posed. Investor protection provided by MiCA will not be at the same level as for financial assets:

there is no investor guarantee fund, the supervision of price manipulations is much more lenient as there is no transaction reporting to the supervisor, and the custody requirements are also much less burdensome. In other words, when MiCA is in force, crypto-assets and their services will become regulated products but with less protection mechanisms in place than financial assets. Second, the MiCA regulation will not prevent a CASP established in a third country that does not comply with MiCA requirements from providing services to an EU citizen who so requests.

Moreover, the regulatory approach followed in other major jurisdictions does not match that of the EU (another example that the 'Brussels effect' is progressively losing force). The EU aims for a harmonised and comprehensive approach, while the US currently has a more complex and multi-agency framework, and the UK is developing a detailed and phased regulatory system post-Brexit. Each of these approaches reflects the region's priorities, challenges, and regulatory philosophies on the evolving world of crypto-assets. However, divergent regulatory regimes have the potential to create loopholes for financial stability and investor protection.

Based on the above, it becomes evident that a global regulatory approach is needed. A good example of a global regulatory approach is the one achieved by the Basel Committee on Banking Supervision. In December 2022, the committee endorsed a global prudential standard for banks' exposures to crypto-assets. This standard is to be implemented by 1 January 2025. Banks will need to classify crypto-assets into two different groups, which will entail different regulatory treatment. Basically, a difference will be made between (1) traditional tokenised assets and crypto-assets counting on an effective stabilisation mechanism and whose issuer is subject to capital and liquidity regulation and supervision, and (2) all other crypto-assets not falling under the first group. Those crypto-assets under group (2) that comply with a series of market criteria will be allowed to compensate net creditor and debtor positions when determining capital requirements. Nevertheless, all other crypto-assets will be subject to the highest risk weight of 1.250%, which entails the highest capital requirements.

Furthermore, any regulatory approach should ensure that investor protection is at the same level as that of financial assets. It is also important to cover new and increasingly relevant elements such as NFTs and DeFi. Failing to do so could put investor protection at risk, especially for retail investors who are less specialised and may have the wrong impression that they are benefiting from the same level of protection.

Conclusions

The crypto-assets market is characterised by its diversity and increasing public awareness. Blockchain technology, while revolutionary, faces significant challenges in scalability and security. The market is marked by the presence of various types of crypto-assets, including traditional cryptocurrencies and stablecoins, each with unique characteristics and implications. Key consensus mechanisms, such as proof of work and proof of stake, are critical for understanding the environmental and security aspects of these digital assets.

The volatility inherent in the crypto market, along with the prominent roles of major crypto-assets like Bitcoin and Ethereum, illustrate the dynamic nature of this field. The emergence and growing importance of stablecoins, with some major traditional players becoming issuers, add another layer of complexity. The risks associated with crypto investments, particularly in the context of hacks and security breaches, underscore the need for cautious engagement in this market.

While risks remain, crypto-assets can also bring added value, for instance for wholesale purposes or for retail customers in jurisdictions affected by high inflationary pressures and unstable currency systems.

In this regard, adequate and harmonised regulatory frameworks are needed to get the best out of digital technology, while preventing risks both to investors' protection and financial stability.

Regulatory responses in major jurisdictions like the EU and UK seem to be taking a similar route, while in the US regulation is diverging from the other two. Therefore, a global, coordinated regulatory approach is essential for managing the risks and maximising the benefits of crypto-assets.

European Credit Research Institute

The European Credit Research Institute (ECRI) is an independent, non-profit research institute that develops its expertise from an interdisciplinary team and networks of academic cooperation partners. It was founded in 1999 by a consortium of European banking and financial institutions. ECRI's operations and staff are managed by the Centre for European Policy Studies. ECRI provides in-depth analysis and insight into the structure, evolution, and regulation of retail financial services markets in Europe. Through its research activities, publications and conferences, ECRI keeps its members up to date on a variety of topics in the area of retail financial services at the European level, such as consumer credit and housing loans, credit reporting, consumer protection and electronic payments. ECRI also provides a venue for its members to participate in the EU level policy discussion.

For further information, visit the website: www.ecri.eu.

Centre for European Policy Studies

CEPS is one of Europe's leading think tanks and forums for debate on EU affairs, with an exceptionally strong in-house research capacity and an extensive network of partner institutes throughout the world. As an organisation, CEPS is committed to carrying out state-of-the-art policy research that addresses the challenges facing Europe and maintaining high standards of academic excellence and unqualified independence and impartiality. It provides a forum for discussion among all stakeholders in the European policy process and works to build collaborative networks of researchers, policymakers and business representatives across Europe.

For further information, visit the website: www.ceps.eu.