BRIEFING

European Parliament

Understanding crypto assets

An overview of blockchain technology's uses and challenges

SUMMARY

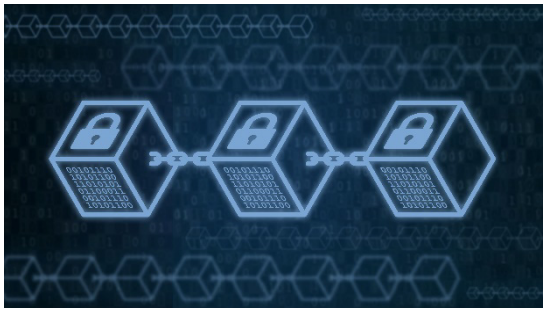
Blockchain and its applications, in particular cryptocurrencies, have grabbed the headlines, but many people still do not know how they work. This briefing provides an overview of the uses and challenges of this technology, based on published information.

Blockchain originated as part of the enabling digital ledger technology (DLT) developed at the end of the 20th century. DLT works as a digital database containing information (as a record book or ledger) that can be simultaneously used and shared through a network (as a shared digital ledger). The technology is considered to render the recorded elements unchangeable (immutable) and the process open (decentralised) by using a publicly accessible network. However, in practice, the outcomes can differ from the initial technological design.

Virtually anything of value (assets) can be tracked and traded on a blockchain. Blockchain works with tokens (values in the digital ledger), tokenisation (using the blockchain for existing assets) and smart contracts (computerised and pre-specified conditions that self-execute when they are met).

Currencies and assets can be exchanged and traded in both the 'real' and virtual world. The use of blockchain for currencies originated from an analysis of shortcomings in the traditional financial environment. Crypto assets range from tangible to non-tangible assets, and to understand them one must look into their substance and the conditions attached to them in their digital definition.

After more than a decade, a number of challenges have appeared, ranging from the protection of citizens to the preservation of the legal economy and the carbon impact of crypto assets. This briefing looks at both the implementation of blockchain technology over this period and at whether it has delivered the expected outcomes.



IN THIS BRIEFING

EPRS | European Parliamentary Research Service

Author: Cécile Remeur
Members' Research Service

PE 757.580 – December 2023

EN

Introduction

Cryptocurrencies have grabbed the headlines as they have boomed and dwindled. However, many people do not know what lies behind them and how they work. And their ups and downs are a reminder of how asset values can fluctuate and of the volatility of markets.

Cryptocurrencies, like any crypto asset, rely on digital ledger technology (DLT),[1] of which blockchain is probably the most widely known example. Blockchains, combined with electronic money, resulted in the launch of cryptocurrency, the most well-known example of which dates back to 2008.

Blockchain has many uses, and is not limited to money; virtually anything of value (assets) can be tracked and traded on a blockchain. Indeed, some blockchain advocates believe that the real potential of blockchain is only now being discovered, while others stress that 'crypto innovation' is no longer in its infancy. Recent research by academics and public and private stakeholders has aimed to provide an understanding of how the latest blockchain technology (such as Web3 – see also the box on page 4) functions and the challenges it brings.

The enabling technology: Blockchain

Blockchain is a way to reach agreement within a network of computers. In the late 1980s and 1990s, computer scientists came up with a consensus model that overcame this by means of a 'signed chain of information used as an electronic ledger for digitally signing documents in a way that could easily show none of the signed documents in the collection had been changed'. In other words, blockchains are essentially databases which, instead of relying on a centralised authority to update them, use a consensus mechanism to decide who gets to add the transactions to the database.

Overview of blockchain technology

Blockchain has been defined as follows: '... distributed digital ledgers of cryptographically signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it 'tamper evident' – see the box on page 4 for an explanation) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating 'tamper resistance'). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules.'[2]

A distributed ledger is a network where every participant can communicate with one another without going to a centralised point. It allows network participants to establish a shared and immutable record of ownership and to share a database of electronic records and build consensus regarding the validity of transactions through cryptographic algorithms. In other words, it is a synchronised database stored by all active participants in the network (peer-to-peer, or P2P).

DLT[3] technology has four characteristics:

1. it includes a **ledger**: a collection of transactions providing a full transaction history, meaning that the transactions and values cannot be over-ridden (this is known as an 'append only' ledger);
2. it is cryptographically secure: data in the ledger has not been tampered with and is attestable (through **hashing**, i.e. converting data into a fixed-length string of letters and numbers);
3. the ledger is **shared** among multiple participants (transparency);
4. it can be **distributed**: more nodes (a node being an individual system within the blockchain) reduce the ability for a bad actor to impact the protocol governing the consensus mechanism.

Blockchain technology uses a pair of keys: one public, one private. The private key must be kept by users, who can store it manually or through software (referred to as a 'wallet', which can store more

elements). Special hardware or private escrow services can be used to ensure security of private keys.

Variations in the implementation of blockchain

A key question is determining which user publishes the next block in the chain. The system can work without prior knowledge between parties ('permissionless', whereby anyone can create an account anonymously), or with more access controls ('permissioned', where there may be some trust between participants).[4]

Permissionless blockchain networks are decentralised ledger platforms open to anyone who can read and write a ledger, which brings the risk of malicious users disrupting the system. This risk is often addressed through trust and an agreement between users that requires them to expand and maintain resources when attempting to publish blocks. Non-malicious behaviour is generally promoted by rewarding the publishers of blocks that conform with the protocol with a native cryptocurrency.

Permissioned blockchains are ones where users' publishing blocks are authorised by some authority (either centralised or decentralised). They involve more trust and more transparency, which can be a disincentive to committing fraud (since the user can be identified). It requires fewer resources, is quicker, and is less expensive in terms of computation.

The **consensus model** aims to determine which user publishes the next block, which must be valid and can be verified by each network user on the basis of the initial state of the system (the 'genesis block'). The way to achieve this varies, depending in particular on whether the blockchain is permissionless or not. For permissionless blockchain, there are usually many publishing nodes (which know each other only by their public address) competing at the same time, which implies computation. Generally, as the level of trust increases, the need for resource usage diminishes.

There are several consensus models, in particular proof of work (PoW) and proof of stake (PoS). In the PoW, a user publishes the next block by being the first to solve a computationally intensive puzzle, the solution to which is the proof. The PoS is based on the idea that the more a user has invested in the system the less likely they are to subvert it. This can operate through random selection of 'staked' users, multi-round voting, or delegate systems, with reputation being one of the incentives not to act maliciously. Another consensus model is related to real identity, namely proof of authority or proof of identity.

Some typical features

Blockchain technology in itself does not operate according to a unique model. The technology offers a range of variants, which have different and even opposite features. Some experts have placed decentralisation and immutability, in particular, in a category of 'accidental characteristics of blockchain', meaning those features that it 'may have but might lack'.

Blockchain ledgers are described as **immutable** (unchangeable). In some particular situations, however, the chain cannot be considered as fully immutable.

A blockchain network can be **open** to all when it is decentralised and no users enjoy control through centralised power, as in the case of permissionless blockchain. Permissioned blockchain, when an authority or founders do enjoy specific rights over the software and management, are not open to all users but to those selected by the authority; they present varying degrees of **centralisation**.

Actual functioning and **governance** (ownership or control) may be less clear-cut: permissioned blockchains are often set up and run by an owner or a consortium. Permissionless blockchains are governed by network users, publishing nodes and software developers, and the level of resources needed can lead to them operating in a rather concentrated format.

Other features derive from the fact that blockchain networks are essentially made up of transactions added to the database. Blockchain functions in a way that is **complex** (e.g. hashing), **automated** (resulting in possible rigidity due to self-executing codes) and highly **interconnected**. It also requires an intense level of computing and software creation, the capacity for which is not widely available among the population at large. These specific capacity requirements lead to the existence of concentrated pools of users that have the necessary IT resources (and computing power).

DLT terminology (non-exhaustive)

DAO: Decentralised autonomous organisations.

Forks: Changes to a blockchain network. These can be backward-compatible ('soft fork'), but when this is not the case they are referred to as 'hard fork', the consequences of which can be the splitting of the blockchain.

Governance tokens: These give their holders voting powers on the direction of a blockchain project.

Mining: The act of solving a puzzle within the PoW consensus model.

Nocoiner: A sceptic who does not own any cryptocurrency and doubts their value.

Tamper evident: A process that makes alterations to data easily detectable.

Tamper resistant: A process which makes alterations to data difficult, costly or both.

Web3: This refers to a decentralised online ecosystem based on the blockchain where platforms and apps are not owned by a central gatekeeper, but rather by users, who will earn their ownership stake by helping to develop and maintain those services.

Range of tokens, from money to other assets

Before looking into the large range of uses, it is helpful to clarify the concept of tokens resulting from the use of blockchain.

Tokens, tokenisation and smart contracts

In general, a **token** is an object that represents another object (either physical or virtual), or an abstract concept. A digital token is a unit of value represented in the ledger. Some commentators see them as 'the linchpin of the new digital economy ... connecting the digital world with assets and services existing in the physical world'. In computing, there are a number of types of token.

Tokens can perform multiple functions. Smart contracts play a key role in linking the numerical value (the token) to assets or services, which can either be virtual or not. Tokens differ from electronic documents due to the use of cryptography and their integration in a database; in other words, they are a subcategory of electronic record. Tokens can represent commercial instruments, including instruments designed for the transferring and exercising of rights in commercial and financial transactions and documents of title. As such, they can be seen as a different technique through which to exercise and transfer rights.

Tokenisation means using blockchain technology for existing financial or tangible assets. It occurs when an existing asset is recorded on a blockchain platform and represented as a token in order to improve processes around trading and transfer of the asset. **Native** tokens are intangible, non-physical assets that derive their value from the blockchain platform (online or virtual assets). **Non-native** tokens are those that represent tangible, intangible and/or financial assets that exist elsewhere, representing rights of property over an asset (off-line assets or services). However, assets recorded through blockchain could be recorded with another technology.

Among existing token taxonomies, the functional taxonomy identifies tokens according to the function assigned by parties. **Payment tokens** are accepted by parties for the settlement of

obligations between them, **security tokens** perform the same function as traditional securities, such as bonds or shares, while **utility tokens** can be similar to vouchers. Utility and payment tokens are based only on the actual usages by market participants. In addition, all tokens are flexible and can perform multiple functions.

An alternative classification for tokens is based on **fungibility**. Fungible tokens provide the same rights and are replaceable with other assets of the same category (for instance, commodities), whereas non-fungible assets each possess unique characteristics preventing their replacement (for instance, a work of art or a trademark).

A **smart contract** is a computerised transaction protocol (self-executing applications) that can trigger an action if some pre-specified conditions are met, then execute the terms of a contract.[5] It is a collection of codes and data inserted in the ledger, and associated with tokens on the blockchain. The substance of a smart contract is not limited and it can be used for almost any activity or product. However, some experts have asked 'how smart smart contracts are', particularly because 'the claim that smart contracts are more efficient and carry no legal costs is negated by the rise of ex-ante costs in the form of thorough due diligence and the need to consider an exhaustive amount of scenarios for contracts to be complete. In conditions of low uncertainty, such contracts may be easier to design and execute. However, when uncertainty is high, the exact costs may be high and the range of unanticipated events large.'

A wide range of uses mimicking real-world assets

Tokens can be classified as digital assets, in the broader category of non-tangible assets. However, they can include different functions and characteristics (and have several), and can be defined as an item of property owned by a person or company. The first use which comes to mind is cryptocurrency.[6]

A wide variety of crypto assets

While all crypto assets use some form of blockchain, not all applications of blockchain involve crypto assets. Crypto assets can be defined as a type of private asset that depends primarily on blockchain to secure digital value or contractual rights; they can be transferred, stored or traded electronically. There is a wide variety of crypto assets, including payment/exchange tokens.[7] A virtual currency is a crypto asset, but not every crypto asset is a virtual currency.

'Non-fungible tokens' (NFTs) are another type of crypto asset. They use blockchain technology to certify the authenticity and ownership of a specific and unique digital objet. Anything that can be digitised can be turned into an NFT, including, for instance, a hyperlink to a digital or physical work of art.

In the European Union, Article 3 of the Markets in Crypto-Assets Regulation (MiCA), adopted in May 2023, includes the following definitions: 'crypto-asset', 'asset-referenced token', 'electronic money token' and 'utility token'.[8]

Cryptomoney

Cryptocurrencies are the most widely known tokens. Payment involves trust in the money itself and the payment system that executes the transaction, and both are changing with digital innovation. Money is fungible, durable, convenient to carry and divide, recognisable and reliable. It serves as a medium of exchange, a unit of account and a means to store value. Currency is one form of money.

Cryptocurrencies were developed with the promise that the decentralised and secure system would be quicker, cheaper and more efficient and democratic (financial inclusion). The proponents of cryptocurrencies presented them as the answer to the shortcomings shown by traditional intermediaries in the 2008 crisis.

A cryptocurrency is a privately issued means of payment and value storage system that functions as 'electronic cash protected through cryptographic mechanisms instead of a central repository or authority'. Cryptocurrencies do not require central intermediaries for clearing and settlement; users believe the system works because they can see it and track it. Transactions can be token-based (assets need to be proven genuine) or account-based (need for user identification).

A central feature of cryptocurrencies is that, like cash, their use or ownership does not intrinsically reveal the personal or business identity of those involved in a transaction. Holders exercise control through a private 'key' (or address not inherently linked to identifiable beneficial owners), held in a 'wallet', but transactions reveal (at most) only a public address from which it is encrypted, and from which it cannot be inferred; hence, they are '**quasi-anonymous**'. A second important feature of cryptocurrencies is that, unlike cash, they are **transparent** in the sense that details of all transactions on a particular coin are publicly available (though not linked to the owner). A third feature of cryptocurrencies that amplifies the difficulties posed by anonymity is their **extra-territoriality**: transactions reveal no information on the jurisdictional location of those transacting.

Decentralised finance (DeFi)

DeFi is an umbrella term commonly used to describe a variety of services in crypto asset markets that aim to provide service transactions analogous to those provided by the traditional financial (TradFi) system The role of financial institutions and market infrastructures is replaced to varying degrees by self-executing code ('smart contracts'). DeFi uses various smart contracts to allow any network participant that meets smart contract criteria to directly fill the roles of automated market makers and liquidity providers, among others, to facilitate transactions in cryptocurrencies. DeFi based on technology requires trust in a combination of internet service providers, core software developers, miners, wallets, exchanges, and stablecoin issuers.

Source: The financial stability risks of decentralised finance, BIS, August 2023.

The word 'currency' within cryptocurrency can be seen to be misleading, because the extreme price volatility of most cryptocurrencies means that they do not discharge the store of value and unit of account functions of currencies. In addition, they bear a transaction cost (in terms of the computing power needed to validate transactions) and require time to be used (due to the need to record them in the ledger). This helps to explain why cryptocurrencies have not become a means of payment to purchase goods and services.

Exchanges and trades

Crypto-trading platforms are digital marketplaces allowing buyers and sellers to transact crypto assets for other crypto assets or for *fiat* currencies. The most popular crypto-trading platforms are those for trading cryptocurrencies.

Users send and receive cryptocurrency and crypto assets on-chain using public and private keys, which are unique strings of alphanumeric characters. Users may store and access them in wallets (software or hardware) that can either be connected to the internet (hot wallets) or not (cold wallets).[9] Unhosted wallets are a type of self-custody wallet that lets users keep their crypto asset balances out of any exchange, or from any third party.

There are broadly three ways in which they may be traded. One is directly peer-to-peer (P2P), without the involvement of any third party. The second is through decentralised exchanges, whose purpose is to facilitate such P2P trades, with customers retaining custody of their private keys. The third is through centralised exchanges, which generally hold their customers' private keys and make transactions on their behalf, charging a commission or fee for doing so.

When the private keys are hosted by a third-party wallet provider, centralisation is reintroduced and the risks of losing a wallet are reduced. When wallets keep the private keys for the users, they are referred to as a 'custodial wallet'. Custodial wallets are provided by centralised intermediaries and utilised in off-chain transactions (not requiring specific expertise). Transactions can occur **off-chain** between parties on the same platform and entail physical debiting and crediting of digital balances.

A crypto exchange is any system (online platforms) where users can buy, sell and trade various crypto assets. Interacting with cryptocurrency through exchanges is centralised, and individuals must often use official identification and provide addresses in order to transact. While being more user-friendly than on-chain transactions, they resemble traditional financial institutions: they facilitate the buying and selling of unbacked crypto assets and also provide much wider services than traditional securities exchanges. Crypto assets can also be traded on payment apps, that have broadened their scope to cryptocurrencies.

Digital money terminology (non-exhaustive)

Central bank digital currencies (CBDCs) are a direct liability of the central bank and, as such, do not carry any credit risk.

A **digital wallet** is a software application that stores payment or account details to facilitate traditional payments that use a bank.

E-money (electronic money, or digital currency) is a digital form of cash stored and exchanged electronically (by a prepaid card or electronic device). It refers to money (backed by *fiat* money) that exists in commercial banks or e-money issuers' computer systems (as a liability on their balance sheets).

Mixer (or tumbler) is a process by which users of a cryptocurrency send theirs to a company that 'mixes' or 'tumbles' the funds with other depositors' and then sends back an equivalent amount of mixed cryptocurrency.

Stablecoins are a subset of cryptocurrency that is designed to be less volatile than other crypto assets. They claim to maintain a stable value relative to a specified asset, or a pool or basket of assets.

Virtual currency means a digital representation of value that is not issued or guaranteed by a central bank or a public authority, but is accepted by natural or legal persons as a means of exchange, and which can be transferred, stored and traded electronically.

Source: Cryptocurrencies and monetary policy (see also the box on page 4).

Virtual meets reality

When a new technology is developed, positive expectations may arise. The implementation of blockchain after a decade shows that it is necessary to look into the substance of each crypto asset to grasp its actual scope and challenges.

Looking into the substance

The use of a new technology does open up potential opportunities, but the mere use of the technology does not amount to the realisation of all the expected potential outcomes.

Some software engineers have stressed that: 'The real world has fundamental constraints that make the technology unworkable, [and] whenever it has to interact with the outside world the benefits of decentralisation disappear and the solutions end up simply recreating slower and worse versions of processes and structures that already exist ... . There are fundamental limitations to the scalability of blockchain-based technologies.' Similarly, the assumption that participants would cooperate in maintaining the system might not remain a plausible assumption when the scope broadens, which might in turn require adaptations that differ from the initial characteristics. In addition, recording an asset on a distributed ledger does not change its characteristics or the set of attached risks that warrant scrutiny by regulators.

Some features in practice

After more than a decade of blockchain, have crypto assets delivered the outcomes expected of them? Some experts identify financial inclusion, disintermediation and decentralisation as examples of positive, expected outcomes that might not have been met.

Crypto assets were expected to function in a decentralised way without intermediaries, in contrast to traditional intermediaries (particularly in the financial system). Yet, in practice the technology can lead to centralisation and create intermediaries, or at least a situation where 'a subset of participants can garner excessive, centralised control over the entire system', because important points of centralisation are inherent in many blockchains. This results in critical service providers who are key to the ongoing operation of networks; this is the case in the PoS, where there is an incentive to concentrate.[10] In the PoW, the necessary resources to participate have the same consequence.

Researchers at the Bank for International Settlements (BIS) have concluded that there is a decentralisation illusion, where the tendency to centralise cannot be solved by further technology. Increasing off-chain transactions suggest that some centralised entities are taking the role of financial market infrastructures. In principle, for crypto assets, traditional financial market infrastructure tasks, such as clearing and settlement, are carried out by the underlying technology in a decentralised manner. For example, such transactions will require that some crypto asset service providers offer clearing services and settlement services. However, in practice most users access their crypto assets through centralised entities that provide easy-to-use interfaces.

As for disintermediation, the crypto-universe is filled with intermediaries, including hosted wallets (where investors store their crypto assets), exchanges (where investors exchange sovereign currencies and crypto assets) or miners (who charge fees to validate crypto transactions – and can profit from their power to decide which transactions to approve and in what order). Many of these entities hold information on their users and can accept or block transactions from certain addresses or can share transaction data with other organisations. These entities act as intermediaries.

Some also see crypto as bringing complexity, rigidity and opacity. The complexity is both technological and financial, which makes it difficult to understand for a layperson. Complexity can make products and the related risks harder to understand, anticipate and address, which can lead to a seemingly minor problem cascading through the system due to unexpected interactions between components, with the risk of becoming a destabilising element.

In addition, automated functioning with smart contracts brings rigidity, as they implement codes when conditions are met. This may prevent them from having room for manoeuvre to take into account unexpected or unanticipated situations and leaving them some time to react. In addition, automated implementation of a number of similar provisions can create a cumulative effect of implementation of the same code (potentially creating contagion or runs).[11] In addition, the difficulty in identifying actors might also complicate identifying to where risks have been moved, and to whom emergency support needs to be provided.

The example of art-related NFTs and intellectual property rights

NFTs and intellectual property rights show the importance of looking into the substance beyond the technology, to ascertain the scope and rights attached to the NFT. For instance, NFTs can record the creation and ownership of an artwork (be it tangible or digital). However, the actual scope is defined in the related smart contract. Some buyers might think that they are acquiring the underlying work of art, and all of its accompanying rights, but in reality they are simply buying the metadata associated with the work, not the work itself.

Transfer of property and licensing of copyright are two separate elements. There is a general presumption that the copyright stays with the creator of the work, who can transfer or sell the rights to the copyright to the purchaser of an NFT by contract. The form of the contract does not alter its scope. The owner only owns the representation in the NFT, unless the smart contract transfers the

copyright (which generally is not transferred in its entirety). This implies, for instance, that the NFT owner cannot oppose a representation of the digital or tangible piece of art enshrined in its NFTs, nor reproduce it for sale, in the absence of a transfer of corresponding copyrights, nor bar representations of the piece of art.

NFTs are also hit by reality in another manner. An NFT that links to a digital representation of an item protected by property rights in order to sell it may infringe intellectual property rights, namely trademarks, or the owner's design or model rights, which bar the sale of imitations. This is particularly the case when it is accompanied by active commercialisation amounting to 'cybersquatting'.

Challenges

The main challenges of crypto assets relate to the protection of citizens, the preservation of the (legal) economy and the carbon impact of crypto assets. For cryptocurrencies, this applies to those that are not digital representations of sovereign currencies (CBDCs).

Challenges regarding citizens' protection

It has been claimed that crypto has the potential to improve **financial inclusion**. However, the technology is not living up to this promise of inclusion, as adoption rates remain low, due in part to scalability issues (i.e. the ability to work efficiently as a payment tool at large volumes). On a global scale, decentralised finance has the potential to reach populations currently excluded from the financial system. According to research for the BIS, the inherent limitations of blockchains restrict the possibilities for improving financial inclusion. In practice, complexity, risk and cost remain major obstacles to address before the crypto ecosystem could be the solution to financial exclusion. In the end, crypto is not providing unbanked or underbanked populations with an alternative route to financial inclusion.

In addition, the **privacy** provided by crypto might come at the expense of security for its users, apart from the risk of obfuscating the legal obligations that rest on users and facilitators (in particular, legal requirements concerning tax and anti-money-laundering). In the EU, ensuring that blockchain complies with the General Data Protection Regulation may be challenging, but it requires a case-by-case analysis of the actual features of each blockchain. This, in turn, raises another issue regarding the territorial scope of the data protection rules relating to crypto.

It is important to **protect consumers and investors** from malpractice, misuse of power and even the exploitative activities of participants and intermediaries, as consumers and some investors (particularly small investors) may not possess sufficient knowledge to combat or be wary of some of these practices. They may buy unsuitable products, face large losses, or be exposed to fraudulent activity. As the European Supervisory Authorities stressed in 2022, crypto assets are not suited to most retail consumers as an investment or as a means of payment or exchange, due to extreme price movements, product complexity, the risk of fraud and malicious activities, hacks, operational risks and security issues, and the risk of misleading advertisements, including through social media and influencers.[12]

For instance, a recent BIS study on Crypto shocks and retail losses has established that a majority of crypto app users in nearly all economies made losses on their holdings over a period longer than six years. Crypto failures may differ in scope according to the nature and functioning of the crypto assets. In some cases, the investors exercise an individual proprietary right, in others ownership may be shared between platform users, while in others they do not have such rights.[13]

There is currently a global push for clearer policies on crypto assets. However, some experts stress that either enforcement of existing rules (on banking, securities, consumer and investor protection rules) on the basis of 'same substance same rules' or the implementation of new rules specific to crypto assets will still not make them safe.

Challenges regarding the legal economy

Crypto assets still comprise a small share of total global financial assets, but it is a larger share than sub-prime mortgages had before the global financial crisis started. As such, they are considered to require specific attention with regard to **financial stability**. This is all the more so as some experts stress that actors involved with crypto assets have little incentive to protect financial stability because it is a public good (people cannot be excluded from or asked to pay for it). Linkages between crypto assets and the traditional financial system could be an important channel of shock transmission and require specific attention to understand any systemic risks that may emerge from a growing crypto asset universe.

The May 2023 European Systemic Risk Board study on Crypto-assets and decentralised finance: Systemic implications and policy options concluded, among other things, that: 'Given the exponential growth dynamics of crypto-assets seen in the past, the future development of these markets is uncertain. There are various instances in which crypto-assets could pose a systemic risk, for example if (i) their interconnectedness with the traditional financial system increases over time, (ii) their connections to the traditional financial system are not identified before they cause problems, and (iii) similar technologies are adopted in traditional finance.'

There is acknowledgement that crypto needs comprehensive policies to protect economies and investors, which is on the agenda of the G20, to answer the question whether crypto could be re-creating the 2008 financial crisis. In September 2023, the International Monetary Fund (IMF) and the Financial Stability Board (FSB) issued a roadmap to ensure effective, flexible and coordinated implementation of the comprehensive policy response for crypto assets.

Little is known about who really owns crypto assets, or about their capital gains and how they are distributed. All these elements raise **tax** questions related to the definition of where taxable events are in this economic activity and to tax design and implementation. This means that studies on taxation of cryptocurrency are gross estimates. Accommodating cryptocurrencies within tax systems not designed to handle them is challenging. As stated in the 2023 IMF report on Taxing Cryptocurrencies: 'Incorporating that possibility ... is more than just a matter of expanding legal definitions ... . The element of anonymity inherent in crypto assets raises issues of enforcement that have long been associated with the use of cash. Those in turn raise issues for ... coherence in the taxation of capital income (viewing crypto assets as a form of property) and – less noted, but perhaps ultimately more significant – in the taxation of final sales under the VAT and similar taxes.'

On the interaction between crypto assets and **anti-money-laundering** provisions, the BIS set the stage as follows in its 2021 insight paper on Supervising cryptoassets for anti-money laundering: 'Although certain cryptoassets have the potential to make payments and transfers more efficient, some of their features may heighten money laundering/terrorist financing (ML/TF) risks. In particular, the speed of transactions, global reach, potential for anonymous activity and the potential for transactions to take place without financial intermediaries make cryptoassets vulnerable to misuse. In fact, the scale of illicit use of cryptoassets is already significant.' However, the nature of blockchain, which records every transaction, carries the potential to combat the phenomenon, provided that customer identification is possible.[14] There are specific anti-money-laundering provisions on virtual assets (VAs) and VA service providers (VASPs).[15]

Crypto assets may also be used to circumvent **sanctions**, as evidenced by some increases in trading volumes in crypto assets using specific currencies.

Challenges regarding carbon footprint

The consensus mechanism for PoW crypto assets has a significant carbon footprint, because it requires vast amounts of computational power to solve the complex mathematical puzzle of mining the crypto asset, validating transactions and securing the expanding network. There are some recent estimates of the carbon footprint of crypto assets, which vary and differ from one year to the

next, but which show that crypto assets consume a similar amount of energy each year as some mid-sized countries.

There are initiatives to address this challenge, via renewable energies for instance, which are not generally implemented (but only on a voluntary basis) and might have other impacts (for example, using energies that are not available for other consumption). Another way to reduce computational power, and hence energy consumption, is through recourse to the PoS consensus mechanism. This still has implications for the functioning of the crypto assets and some of its key features (such as decentralisation). As they are now, researchers consider that some crypto assets do not price in the negative externalities of their energy consumption and private and social costs, which renders them an unsustainable investment that might not meet the green transition requirements.

MAIN REFERENCES

Allen H., DeFi: Shadow Banking 2.0?, *William & Mary Law Review*, Vol. 64, pp. 919-968, 2023.

Aramonte S., Huang W. and Schrimpf A., DeFi risks and the decentralisation illusion, BIS, 2023.

Baer K., de Mooij R., Hebous S. and Keen M., Taxing Cryptocurrencies, IMF Working Paper No. 2023/144, July 2023.

Buckley R., Didenko A. and Trzecinski M., Blockchain and its Applications: A Conceptual Legal Primer, *Journal of International Economic Law*, Vol. 26, Issue 2, June 2023.

Chen Y., Gurrola-Pérez P. and Lin K., A review of crypto-trading infrastructure, World Federation of Exchanges, August 2023.

Hallak I., Non-EU countries' regulations on crypto-assets and their potential implications for the EU, EPRS, European Parliament, September 2023.

Murray M., Transfers and licensing of copyrights to NFT purchasers, *Stanford Journal of Blockchain Law & Policy*, January 2023.

Garrido J., Digital Tokens: A Legal Perspective, IMF Working Paper No. 2023/151, July 2023.

Garcia Ocampo D., Branzoli N. and Cusmano L., Crypto, tokens and DeFi: navigating the regulatory landscape, BIS, May 2023.

Yaga D., Mell P., Roby N. and Scarfone K., Blockchain Technology Overview, National Institute of Standards and Technology, NISTIR 8202, October 2018.

Zlati G., Blockchain and criminal law; the fundamentals, *ERA Forum*, Vol. 24, pp. 295-315, July 2023.

ENDNOTES

1 In fact, 'distributed ledger technology' is often used as a synonym for blockchain. For the sake of simplicity, the term blockchain will be used, bearing in mind that DLT has a broader scope than blockchain technology.
2 For a detailed presentation, see Yaga D. et al, Blockchain Technology Overview.
3 In a blockchain, the sequence of blocks of data is created chronologically and linked together via a hash value. In other distributed ledger technologies, the database stored across all the nodes can have a different structure and sequence.
4 See also the classification based on a mechanism's degree of decentralisation, which goes from public blockchains, through consortium blockchains, to fully private ones (in Garrido J., Digital Tokens: A Legal Perspective, p. 10, Box 1).
5 Smart contracts were defined in 1994 as 'a computerised transaction protocol that executes the terms of a contract', Szabo N., 'Smart Contracts'.
6 For a presentation of the scope and terminology, see Garcia Ocampo D., Crypto, tokens and DeFi: navigating the regulatory landscape, BIS, May 2023.
7 Note that the IMF describes unbacked crypto assets as follows: 'These crypto assets are transferable, primarily designed to be used as a medium of exchange, and although they are often decentralised, there are examples of unbacked crypto assets that are centrally issued and controlled. Most unbacked crypto assets are currently used for speculation and not for payment purposes', Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, September 2022, p. 11.
8 Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets.
9 Regulating the Crypto Ecosystem: The Case of Unbacked Crypto Assets, p. 21: 'Most users and crypto asset exchanges alike use cold wallets for storing most of their crypto assets and keep only what is needed for transactions in the short term in a hot wallet. Hot wallets allow for the quicker transfer of crypto assets in peer-to-peer transactions. There is little real difference between cold and hot wallet technologies. A hot wallet becomes cold upon disconnecting it from the network.'
10 Aramonte S., Huang W. and Schrimpf A., DeFi risks and the decentralisation illusion, BIS, 2023, p. 8: 'Blockchains based on proof-of-stake, which are expected to improve scalability, allow validators to stake more of their coins so that they have a higher chance of 'winning' the next block and receiving compensation. Since the associated operational costs are mostly fixed, this setup naturally leads to concentration.'
11 Runs happen when people lose confidence that a particular asset will continue to retain its value and function as expected.
12 This applies to the situation as it is before the implementation of the MICA regulation. See also work on Principles on Blockchain Technology, Smart Contracts and Consumer Protection, by the European Law Institute.
13 For a presentation, see Kokorin I., The anatomy of crypto failures and investor protection under MiCAR, 2023.
14 See Europol spotlight, December 2021, Cryptocurrencies: tracing the evolution of criminal finances, p. 10: 'Pseudo-anonymity and decentralisation provide a favourable environment for criminals. It is important to highlight that cryptocurrencies are not anonymous. Every single transaction is logged in the blockchain, which is a ledger of all transactions distributed to all users in the network. Most blockchains are publicly available, making transactions traceable. However, a number of services and techniques can enhance anonymity and hinder law enforcement investigations.'
15 For more details, see the 6 July 2023 Council of Europe Moneyval report on money laundering and terrorist financing risks in the world of virtual assets.

DISCLAIMER AND COPYRIGHT

eprs@ep.europa.eu (contact)

www.eprs.ep.parl.union.eu (intranet)

www.europarl.europa.eu/thinktank (internet)

http://epthinktank.eu (blog)