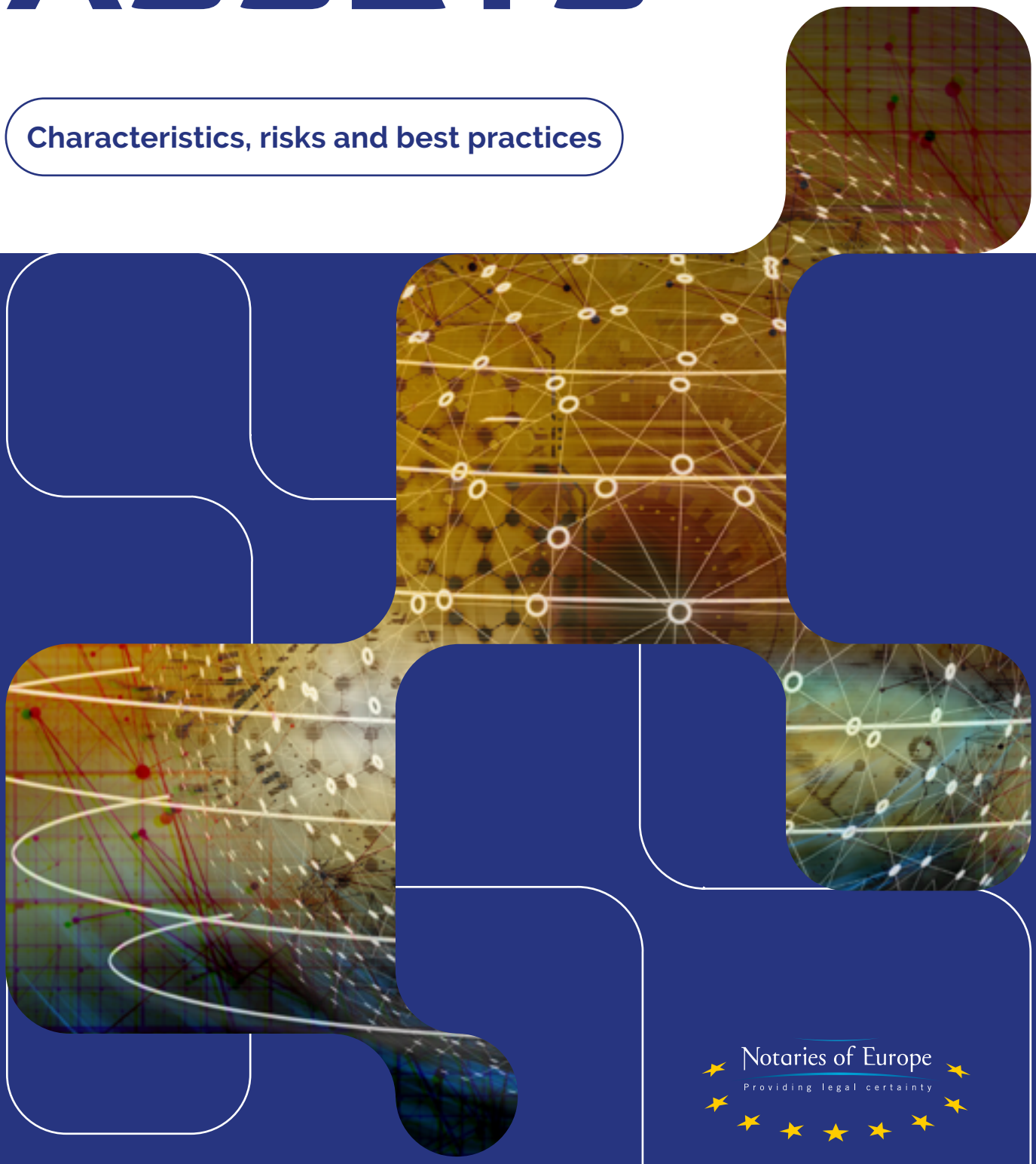
CRYPTO ASSETS

Characteristics, risks and best practices



Notaries of Europe

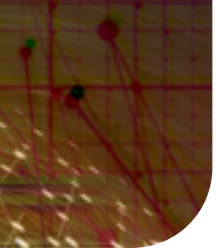
Providing legal certainty

Content

INTRO p.4

01 DEFINITIONS AND ELEMENTS OF THE CRYPTO SYSTEM p.6

02 CHARACTERIS-TICS OF CRYPTO ASSETS AND POTENTIAL RISKS OF ITS USE p.10



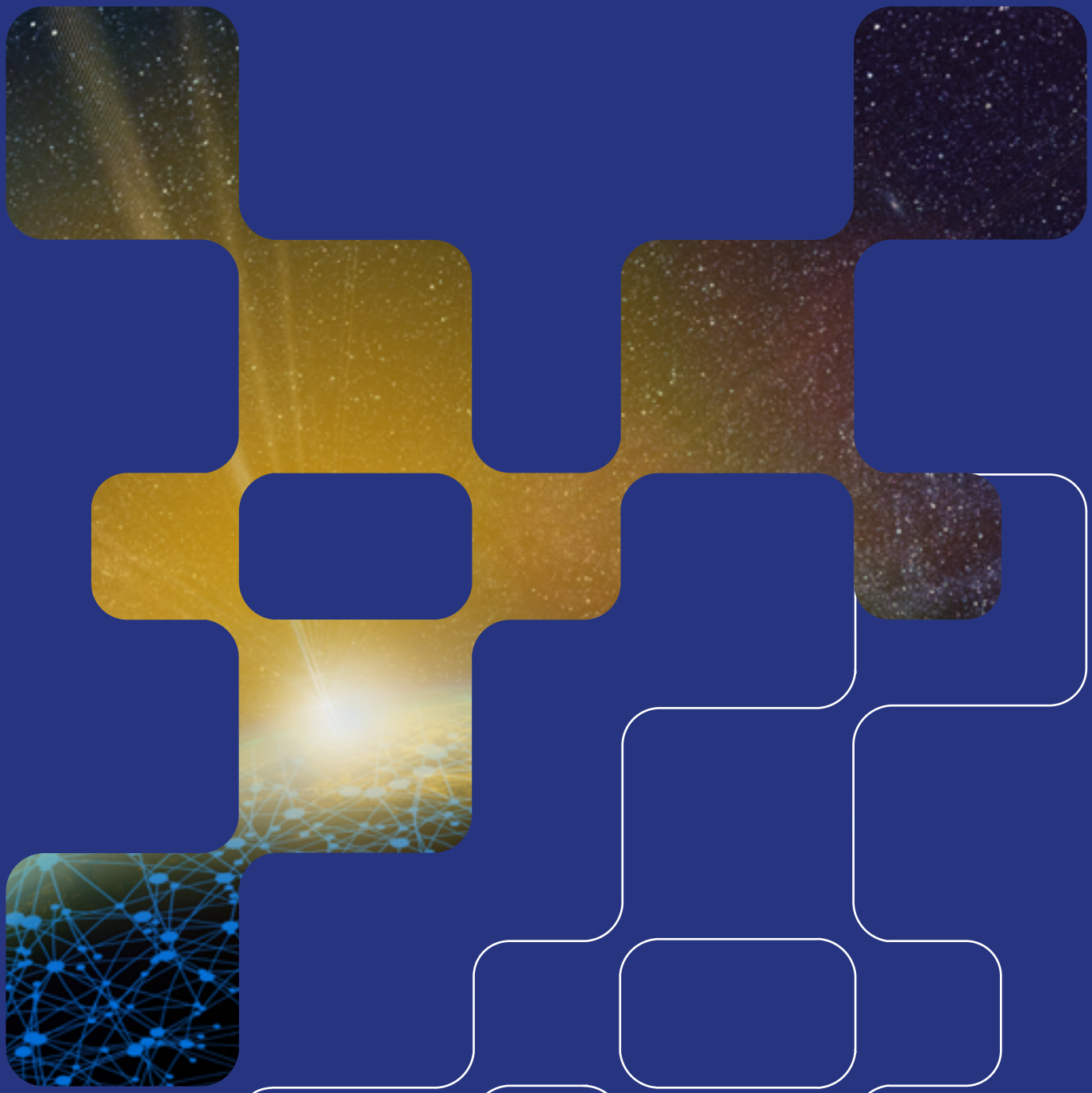
03 REGULATION OF CRYPTO ASSETS p.14

04 NOTARIAL TRANS-ACTIONS IN WHICH THESE RISKS MAY APPEAR p.18

05 BEST PRACTICES TO MITIGATE THE RISKS p.22

CONCLUSIONS p.26

INTRODUCTION



Bitcoin, the first crypto asset to be created, was born sixteen years ago, only one year after the financial crisis of 2008, by a person or group of people using the alias Satoshi Nakamoto. The nature of crypto assets offered a new alternative to financial systems entirely hedged and controlled by central authorities. Introducing Bitcoin - a new financial tool that is said to be entirely controlled and verified by the users themselves - would guarantee anonymity, could be transferred to anyone anywhere in the world and all of that without the help of an unworthy middleman[1]. Or, in the words of the founder Satoshi Nakamoto, "a Peer-to-Peer Electronic Cash System"[2].

Since then, thousands of other crypto assets have been developed and gone into use[3], all relatively different from one another in the way that they are designed and the degree of popularity amongst users[4]. They can be acquired both online and physically. They have been adopted by governments while at the same time banned by others. But there was a general understanding amongst regulators that if laws were to be established for their use, it had to be done on a global scale and in a coordinated manner.

The last decade has seen a continual growth in their adoption by businesses, individuals and even governments as a method of payment as well as potentially lucrative assets to invest in. This exponential growth of their use could be related to a variety of factors, based on their characteristics. The first could refer to the high levels of privacy and security that they offer due to the fact that all transactions dating back to their invention are recorded on a public ledger available to everyone while maintaining the identity of the beneficiaries anonymous.

The second could refer to their decentralized nature, signifying that they are not subject to government or regulatory control as are traditional currencies.

Thirdly, because they do not require the intermediation of banks and work digitally, they offer lower-cost transactions, leaving a more attractive proposition to people looking for more effective modes of transfer.

Nevertheless, there has also been a significant amount of skepticism due to their novel nature, the immense volatility of their value and the risks of their use for money laundering and terrorist financing.

The purpose of this paper is to gain an understanding of what crypto assets are and how they may or may not create new facilities to launder money and finance terrorist organizations.

Moreover, regulations that have so far been adopted by the FATF and the EU regarding crypto assets will be dissected in order to establish how they may help prevent the two aforementioned illegal activities from being facilitated.

In addition, we will attempt to identify some of the notarial transactions in which this above-average risk may arise and in which, therefore, it is advisable to apply some of the measures proposed in this document to mitigate risks.

This document has been drafted with the intention of being as useful as possible to notaries in different countries. Therefore, it does not take into account possible national regulations on the use of crypto assets in the field of notarial practice. Its content should be considered in accordance with compliance with applicable national legislation, taking into account possible prohibitions and/or limitations on its use in certain types of transactions carried out before a notary that may exist at national level.

1 https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency

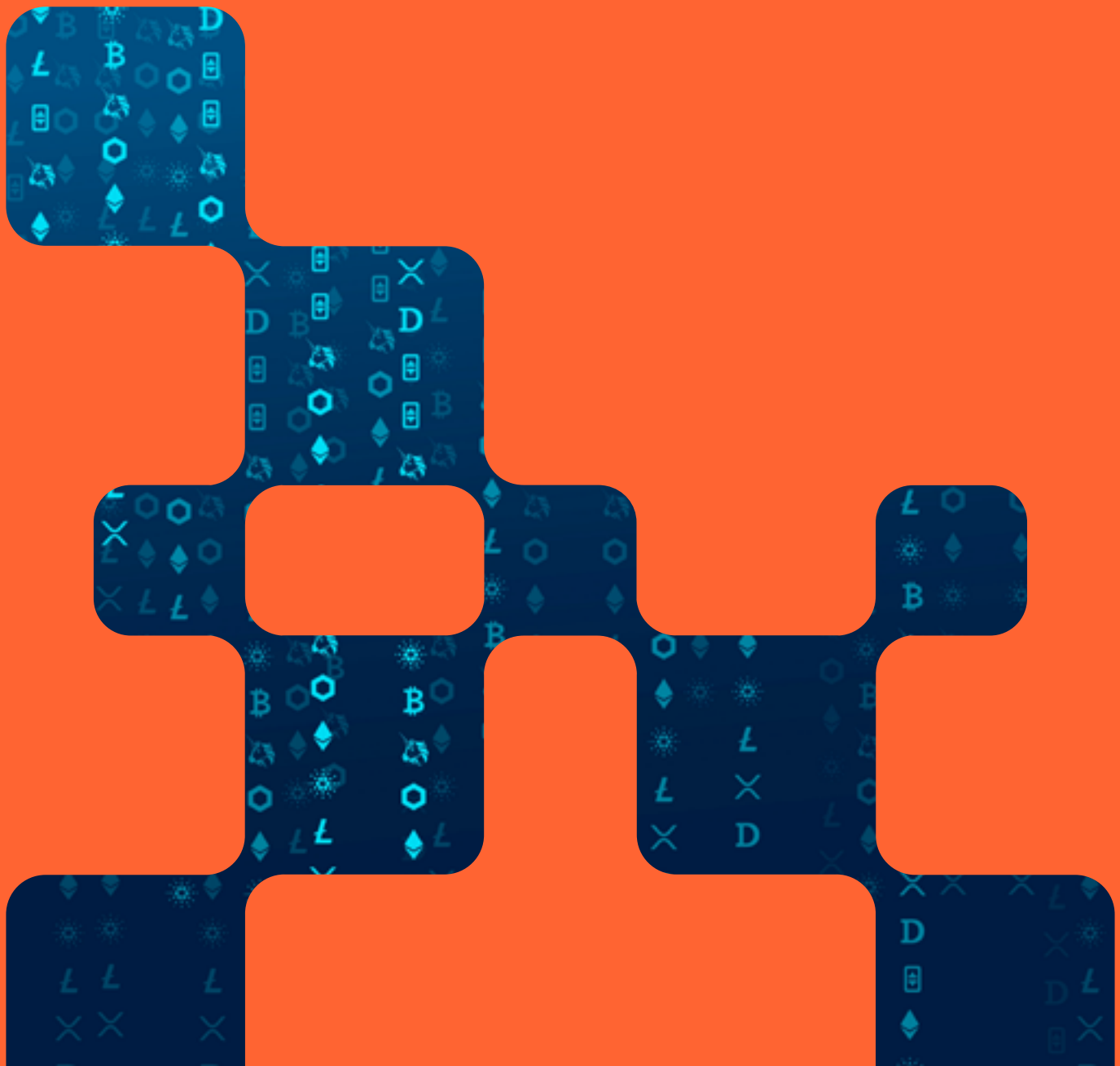
2 https://bitcoin.org/bitcoin.pdf

3 https://www.statista.com/statistics/863917/number-crypto-coins-tokens/

4 https://www.sciencedirect.com/science/article/abs/pii/S0167811622000647

1

DEFINITIONS AND ELEMENTS OF THE CRYPTO SYSTEM



According to Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023, on markets in crypto assets (MiCA Regulation) "crypto asset" means "*a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology*". This is also the definition that is being used in Regulation (EU) 2024/1624 (AMLR) of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, cf. Art. 2 no. 1 sub-no. (7) AMLR.

The most common types of crypto assets are:

- **Cryptocurrencies (or virtual currencies):** Digital assets designed as a means of payment. Example: Bitcoin (BTC), Ethereum (ETH). They have no physical backing and are not directly linked to real-world assets.
- **Stablecoins**: Crypto assets that seek to maintain a stable parity with a fiat currency (such as the dollar or the euro). Example: USDT, USDC, DAI. They are used to avoid the volatility typical of cryptocurrencies.
- **Security tokens (value tokens)**: They represent tokenized financial securities, such as shares in a company or rights to assets. They are usually subject to financial regulation.
- **Utility tokens**: These give access to a product or service within a platform. They are not intended for investment, but rather for functional purposes. Example: tokens for access to services on a blockchain network.
- **NFTs (non-fungible tokens)**: These represent unique digital assets, such as digital art, collectibles, or virtual tickets. They are not interchangeable with each other.

Unlike fiat money (such as the euro or the dollar), crypto assets are not necessarily issued or guaranteed by a central bank or public authority, although some are designed to maintain parity with traditional currencies (as is the case with certain stablecoins).

As mentioned in the definition, crypto assets rely on digital ledger technology (DLT)[5] of which blockchain is probably the most widely known example. Blockchains, combined with electronic money, resulted in the launch of crypto assets, Bitcoin being the first and most important of these crypto assets.

Blockchain has been defined as "*…distributed digital ledgers of cryptographically signed transactions that are grouped into blocks*[6]". Each block is cryptographically linked to the previous one after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify. New blocks are replicated across copies of the ledger within the network, and conflicts are resolved automatically using established rules.

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.

5 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.

6 National Institute of Standards and Technology Internal Report 8202. https://doi.org/10.6028/NIST.IR.8202

Considering the characteristics of blockchain and in order to better understand crypto assets, their risks and the potential best practices to mitigate them (further detailed in the following chapters) it is essential to know, in general terms, the most important participants in the crypto system.

In this sense, in June 2014, the Financial Action Task Force (FATF) published an initial document entitled "Virtual Currencies: Key Definitions and Potential AML/CFT Risks"[7] (adopting the definition of "virtual assets" in 2018), updated in 2018 by the "Updated guidance: a risk-based approach to virtual assets and virtual asset service providers"[8], which were also updated in October 2021. These documents define the most relevant related terms as follows (definitions included literally)[9]:

- An **exchanger** (also sometimes called a virtual currency exchange) is a person or entity engaged as a business in the exchange of virtual currency for real currency, funds, or other forms of virtual currency and also precious metals, and vice versa, for a fee (commission). Exchangers generally accept a wide range of payments, including cash, wires, credit cards, and other virtual currencies, and can be administrator-affiliated, non-affiliated, or a third-party provider. Exchangers can act as a bourse or as an exchange desk. Individuals typically use exchangers to deposit and withdraw money from virtual currency accounts.

- A **user** is a person/entity who obtains virtual currency and uses it to purchase real or virtual goods or services or send transfers in a personal capacity to another person (for personal use), or who holds the virtual currency as a (personal) investment. Users can obtain virtual currency in several ways. For example, they can (1) purchase virtual currency, using real money (from an exchanger or, for certain centralized virtual currencies, directly from the administrator/issuer); (2) engage in specific activities that earn virtual currency payments (e.g., respond to a promotion, complete an online survey, provide a real or virtual good or service); (3) with some decentralized virtual currencies (e.g., Bitcoin), self-generate units of the currency by «mining» them (see definition of miner, below), and receive them as gifts, rewards, or as part of a free initial distribution.

- A **miner** is an individual or entity that participates in a decentralized virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system. Miners may be users, if they self generate a convertible virtual currency solely for their own purposes, e.g., to hold for investment or to use to pay an existing obligation or to purchase goods and services. Miners may also participate in a virtual currency system as exchangers, creating the virtual currency as a business in order to sell it for fiat currency or other virtual currency.

- **Virtual currency wallet** is a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency. Wallets can be stored both online ("hot storage") or offline ("cold storage").

- A **wallet provider** is an entity that provides a virtual currency wallet (i.e., a means (software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency). A wallet **holds the user's private keys** [emphasis added by author], which allow the user to spend virtual currency allocated to the virtual currency address in the blockchain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to more easily conduct the virtual currency transactions. The wallet provider maintains the customer's virtual currency balance and generally also provides storage and transaction security. For example, beyond providing bitcoin addresses, the wallet may offer encryption; multiple key (multi-key) signature protection, backup/cold storage; and mixers.

7 FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, June 2014.

8 FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2021.

9 FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, June 2014 (p. 7) and FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2021 (p. 24)

- **Virtual asset service provider** is any natural or legal person who is not covered elsewhere under the Recommendations [meaning the FATF- Recommendations] and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:

  > Exchange between virtual assets and fiat currencies,
  > Exchange between one or more forms of virtual assets,
  > Transfer of virtual assets,
  > Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets,
  > Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

Once familiar with the most relevant terms, it is necessary to understand the basic functioning of the blockchain and how transactions happen. A simple breakdown of how it works goes as follows:

- The first thing that must happen for a transaction to take place is that the two people involved in the transaction must have a **digital wallet**. It is essentially a digital version of a bank account or a "cold wallet" where crypto assets can be stored. These may be stored on the internet, on a desktop computer or on a mobile device.

- The next step consists of **acquiring crypto assets**. This is done by either using a fiat currency or another crypto asset on a crypto assets exchange platform (through an exchanger) or peer-to-peer. The exchangers are usually available on the web as a service to trade the different currencies and vary in size (number of users) and variety (number of available currencies).

- Once an individual has a wallet and crypto assets, they can be transferred to another user. To do so, it will only be necessary to know the **recipient's digital wallet address**. There are no borders in this transaction and it is completed within a few minutes.

- The details of the transaction are recorded (amount sent and wallet addresses) and is verified by other users on the blockchain's network. Each transaction is recorded as a "block" of data on the blockchain.[10]

- The verification process is done to make sure that the transaction is legitimate. This process is called "mining", which requires other users' devices computing power to solve mathematical problems. This process is also called a consensus mechanism that prevents duplications of transactions or fraudulent actions as well as preventing a single actor or group from exercising too much influence on the process. When this has been completed, the transaction is added to the blockchain.

- Once the transaction has been confirmed and has been placed on the blockchain, the **transaction is complete**, the crypto assets has been transferred, and the receiving party can now use the crypto assets.

- In crypto asset transactions (such as sending or receiving Bitcoin or Ethereum), each transaction confirmed on the blockchain is associated with **a hash**. This hash a) uniquely identifies the transaction, b) allows it to be publicly verified in block explorers, c) guarantees that the transaction information has not been altered, d) can be used as evidence (for example, to prove that a transfer was made on a specific date and in a specific amount).

This process, although seemingly complex, creates an infrastructure for financial transactions that offers a greater level of security and significant transparency regarding which transactions are occurring, while not revealing the identity of senders and recipients.

10 cf. https://www.ibm.com/think/topics/blockchain.

2

CHARACTERISTICS OF CRYPTO ASSETS AND POTENTIAL RISKS OF ITS USE

Characteristics

As already defined, crypto assets are digital representations of value or rights that are recorded and transmitted using distributed ledger technologies, such as blockchain, and can be used as a means of payment/exchange, investment (e.g. granting ownership rights), access to certain services within a digital ecosystem or for a combination of these features.

The following are the key characteristics that allow a crypto asset to be identified and understood:

- **Convertible (or open)**. They have an equivalent value in fiat currency and can be exchanged back-and-forth for fiat currency.[11]
- **Decentralized**. They are distributed, open-source, math-based virtual currencies that have no central administrating authority, and no central monitoring or oversight.[12]
- **Security**. The cryptographic algorithms that are used to guarantee the legitimacy and the secrecy of the identity of users make them less exposed to hacks, fraud and other kinds of cyber-attacks. The digital wallets also are secured using private keys that are the equivalent of passwords only accessible by its owner on their hardware.
- **Transparency**. Transactions are usually publicly recorded on the blockchain and traceable.
- **Pseudo-anonymous**. Crypto assets allow transactions to be carried out without revealing personal identity. The pseudo-anonymity factor translates into increased privacy for users as well as complementing the security of their use. The degree of anonymity will vary depending on the crypto asset and its technical design. This will make their use more difficult to decrypt or trace, increasing the privacy of the financial activities being conducted.
- **Volatility**. The value of crypto assets has been subject to high volatility since their introduction. Conditioned by markets and people's trust in them, as well as changes in their regulation, they have for the time being proven to be a risk-filled investment.
- **Irreversibility of the transactions**. Once a transaction has been completed, there is no way to take it back. Hence if a mistake is made or a disagreement ensues from a contract, close to nothing can be done to rectify the situation. This also applies to the setup of an account in that if a password is forgotten, there is no way of retrieving it.

11 cf. FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, June 2014, p. 4.

12 cf. FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, June 2014, p. 5.

Potential risks of its use

As recognized by Regulation (EU) 2024/1624 of the European Parliament and of the Council of 31 May 2024 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, "*technology keeps evolving, offering opportunities to the private sector to develop new products and systems to exchange funds or value. While this is a positive phenomenon, it can generate new money laundering and terrorist financing risks, as criminals continuously manage to find ways to exploit vulnerabilities in order to hide and move illicit funds around the world*"[13].

In June 2014, the Financial Action Task Force (FATF) published an initial document entitled "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" in response to the emergence of virtual currencies and their associated payment mechanisms, which highlighted the potential risks of this type of asset in relation to money laundering and terrorist financing.

That document[14], in addition to including definitions of most of the related terms, explained how by using various «anonymization schemes» (darknets and mixers) the origin of a transaction could be hidden, and anonymization could be facilitated.

First, crypto assets systems can be traded on the Internet, are generally characterized by non-face-to-face customer relationships and may permit anonymous funding (cash funding or third-party funding through virtual exchangers that do not properly identify the funding source). They may also permit anonymous transfers, if the sender and recipient are not adequately identified.

Decentralized systems are particularly vulnerable to anonymity risks. For example, by design, Bitcoin addresses, which function as accounts, have no names or other customer identification attached and there is no central oversight body. Law enforcement cannot target one central location or entity (administrator) for investigative or asset seizure purposes (although authorities can target individual exchangers for client information that the exchanger, as obliged entity, must collect). It thus offers a level of potential anonymity, especially if crypto assets were not obtained through a regulated exchanger.

Crypto assets' global reach likewise increases its potential AML/CFT risks. Crypto assets systems can be accessed via the Internet (including via mobile phones) and can be used to make cross-border payments and funds transfers.

In addition, they commonly rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments. These components of a crypto assets system may be located in jurisdictions that do not have adequate AML/CFT controls. Centralized crypto assets systems could be complicit in money laundering and could deliberately seek out jurisdictions with weak AML/CFT regimes. Decentralized convertible crypto assets allowing anonymous person-to-person transactions may seem to exist in a digital universe entirely outside the reach of any particular country.

Generally speaking (not only in the notarial field) this type of crypto assets could be used in a generic laundering operation in various ways, but basically, we point out three:

13 Regulation (EU 2024/1624 recital 7.

14 FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, June 2014, p. 9-10.

- As a way of moving illicit funds without leaving a trace and away from the predicate offence (in the so-called cover-up phase of laundering). Crypto assets are bought and given to another person anywhere in the world, the funds have changed ownership and country, but no bank transfer or physical movement of funds has been necessary.

- As a way of keeping illicit funds out of the control of authorities. Crypto assets may be bought and kept in the wallet without being traded.

- As a way of giving a legal appearance to the money invested in crypto assets, simulating a possible profit from trading them (in the integration or return phase of laundering). Crypto assets would be bought as anonymously as possible and sold through a financial institution, simulating a capital gain from the difference between the purchase price (in theory much lower) and the sale price (very high). In this possibility, how the crypto assets were purchased and the existence of some kind of documentary justification (either true or simulated) of the date of purchase and the price paid could be useful to try to justify the existence of a capital gain.

3

REGULATION OF CRYPTO ASSETS

The FATF is the intergovernmental body which sets the international standards to prevent money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction.

As mentioned before, in June 2014, the Financial Action Task Force (FATF) published the initial document entitled "Virtual Currencies: Key Definitions and Potential AML/CFT Risks".

In this document, the FATF defined "virtual currency" as "***a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or a (3) store of value but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction***"[15].

In addition to defining most of the related terms, the document explained how various "anonymity programs" (dark networks and mixers) could be used to hide the origin of a transaction and facilitate anonymity.

In June 2015, the FATF issued the "Guidance for a Risk-Based Approach to Virtual Currencies" as part of a staged approach to addressing the ML/TF risks associated with virtual currency payment products and services.

As the virtual asset market continued to evolve and develop, the FATF recognized the need for further clarification on the application of the FATF Standards to virtual assets and their service providers. In October 2018, the FATF adopted two new Glossary definitions – "virtual asset" and "virtual asset service provider" (VASP) – and updated Recommendation 15, requiring that **VASPs be regulated for anti-money laundering and countering the financing of terrorism (AML/CFT) purposes**, that they be licensed or registered, and subject to effective systems for monitoring or supervision.[16]

Virtual assets, defined as "*a digital representation of value that can be digitally traded, or transferred and can be used for payments or investments. Virtual assets do not include digital representations of fiat currencies, securities, and other financial assets that are already covered elsewhere in the FATF Recommendations*"[17] is the term the FATF uses to refer to crypto assets and other digital assets.

In June 2019, the FATF adopted an Interpretive Note to Recommendation 15 (INR.15) to further clarify how the FATF requirements apply in relation to virtual assets and VASPs. These changes were accompanied by a new "Guidance for a Risk-Based Approach for Virtual Assets and VASPs".

Taking into account the worldwide trend regarding regulation of crypto assets, and especially the fact that many European Union (EU) Member States decided to introduce bespoke regimes for crypto assets, it is no wonder that the European Union decided to take some legislative steps.

Directive (EU) 2018/843 was the first legal instrument to address the risks of money laundering and terrorist financing posed by crypto assets in the Union.[18] Unlike the FATF, it extended the scope of the AML/CFT framework only to **two types of crypto asset service providers** (CASP): providers engaged in exchange services between virtual currencies and fiat currencies, and custodian wallet providers.

Due to rapid technological developments and the advancement in FATF standards, it was necessary to review that approach. The first step to completing and updating the Union legal framework was achieved with Regulation (EU) 2023/1114 of the European Parliament and of the Council on markets in crypto assets (MiCA Regulation), which set requirements for crypto asset service providers wishing to apply for an authorization to provide their services in the internal market.

15 FATF, Virtual Currencies: Key Definitions and Potential AML/CFT Risks, June 2014, p. 4.

16 FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2021, p. 8.

17 FATF, Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, 2021, p. 109.

18 cf. Regulation (EU) 2024/1624

It institutes uniform EU market rules for crypto assets and also introduced a definition of **crypto assets**[19] and **crypto asset service providers**[20] (in accordance with definitions provided by the FATF) encompassing a broader range of activities. In addition, Regulation (EU) 2023/1113 extended traceability requirements to transfers of crypto assets carried out by crypto asset service providers covered by Regulation (EU) 2023/1114 and amended Directive (EU) 2015/849 to require Member States to make those crypto-asset service providers obliged entities.

The second step was achieved on 31 May 2024, with Regulation (EU) 2024/1624 of the European Parliament and of the Council on the **prevention of the use of the financial system for the purposes of money laundering or terrorist financing** (AMLR). This Regulation extended the scope of application to all crypto asset service providers[21], imposing a series of specific obligations on them. Some of the main obligations that CASPs must comply with under this regulation are detailed below:

- **Customer due diligence measures**. CASPs must apply customer due diligence measures, among others, in the following cases:
  - When establishing a business relationship.
  - When carrying out an occasional transaction with a minimum value of EUR 1,000, regardless of whether the transaction is carried out as a single transaction or through related transactions.[22]
  - When there are suspicions of money laundering or terrorist financing.
- These measures include identifying and verifying the identity of the customer and the beneficial owner, as well as obtaining information on the purpose and intended nature of the business relationship.
- **Risk assessment and management**. Crypto asset service providers must implement policies, procedures, and internal controls to mitigate and manage the risks of money laundering, terrorist financing, and evasion of financial sanctions. This includes conducting and updating risk assessments throughout the company, especially when launching new products, services, or practices.
- **Suspicious transactions reporting**. CASPs are required to report suspicious transactions. As entities subject to anti-money laundering and counter-terrorist financing (AML/CFT) obligations, they must inform the Financial Intelligence Unit (FIU) of their member state when they detect activities that may be related to these crimes.
- **Appointment of compliance officers**. CASPs must designate a member of the management body responsible for the implementation of the internal policies, procedures, and controls of the obligated entity. In addition, they must appoint a compliance manager responsible for the day-to-day implementation of the procedures and the submission of transaction reports.
- **Prohibition of anonymous accounts and measures against anonymity**. The regulation prohibits the provision and custody of anonymous crypto asset accounts or accounts that enable anonymization or increased obfuscation of transactions by crypto asset service providers[23]. This includes specific measures to mitigate risks in relation to transactions with self-hosted addresses[24].
- **Enhanced measures for cross-border correspondent relationships**. CASPs must apply enhanced due diligence measures specific to cross-border correspondent relationships, especially when dealing with individual customer entities from third countries identified as high-risk[25].

19 cf. Art. 3 no. 1 sub-no. (5) Regulation (EU) 2023/1114.

20 cf. Art. 3 no. 1 sub-no. (15) Regulation (EU) 2023/1114.

21 cf. Art. 3(2) in connection with Art. 2 no. 1 para. 1 lit. (i) AMLR.

22 cf. Art. 19 (3) AMLR.

23 Art. 79 AMLR.

24 Art. 40 AMLR.

25 Art. 37 AMLR.

4

NOTARIAL TRANSACTIONS IN WHICH THESE RISKS MAY APPEAR

Notaries, as entities subject to anti-money laundering and counter-terrorist financing (AML/CFT) requirements, play an essential role in monitoring the legality of legal transactions.

With the growing use of crypto assets in the global economy, notaries are increasingly exposed to new risks arising from the misuse of such digital instruments. The gradual incorporation of crypto assets into legal transactions poses new challenges for notaries, particularly in the area of anti-money laundering and counter-terrorist financing (AML/CFT).

Although crypto assets are legitimate technological tools, their opacity and ease of transfer can be exploited for illicit purposes. In this context, it is essential to identify some of the notarial transactions, provided that these are allowed under the national notarial professional law, in which such assets may be involved and to assess the associated risks.

In addition, some of these transactions may be prohibited by law in certain countries, as in Germany, where Section 16a of the German Anti-Money Laundering Act generally prohibits the payment with cash, crypto assets, gold, platinum or precious stones in real estate transactions (transactions aimed at the purchase or exchange of domestic real estate).

Sale of real estate

Crypto assets can be used as a means of payment, directly or indirectly, in real estate transactions. The difficulty of verifying the origin of the funds used, similar to the use of cash, represents a significant risk, as these transactions can be used to "launder" proceeds from criminal activities through tangible assets that enjoy a presumption of legality reinforced by notarial intervention.

It is very important to bear in mind that crypto assets are not considered as money, but as assets with (variable) economic value. Therefore, transactions involving crypto assets are not strictly speaking "sales", but exchanges.

Incorporation of companies and capital contributions

In the process of incorporating a company or increasing its share capital, crypto assets may be contributed as assets capable of economic valuation. This contribution could be made in three ways:

i. Delivering the keys to the wallet as a valuable element.
ii. Delivering crypto assets from the members' wallet to a partnership wallet.
iii. By stating that the crypto assets are the property of the company, but without contributing anything else (similar to when a movable asset is contributed but not registered in any registry).

The lack of uniform standards for their valuation, together with the possible opacity of the origin of such assets, may facilitate the entry of illicit funds into corporate structures that later operate with the appearance of legality.

As in the previous case, the contribution of crypto assets constitutes a non-monetary contribution, as would be the case with the contribution of a vehicle, real estate or other rights.

Loans and debt acknowledgments

Loan agreements in which the capital provided or repaid is denominated in crypto assets can also be used as a means of concealing irregular transfers of funds between individuals or entities. As in other transactions, the risk is increased when the parties involved operate from jurisdictions with low financial transparency. Crypto assets can also be provided as collateral for the repayment of the loan.

Donations and gratuitous transfers

The donation of crypto assets is another potential risk, especially if it is made between persons with distant or non-existent family ties. These transactions may conceal payments or obligations arising from illicit activities and often lack clear economic justification.

Acts of declaration and formalization

The declaration of ownership of crypto assets (for example, in wills, marriage settlements, deed of statements or declarations of assets) may entail risks if used to simulate wealth or to introduce assets of unknown origin into public documents intended to be permanent and public.

Acts of custody

i. **Custody of private keys or access credentials**
The notary may be required to hold private keys, seed phrases, or physical devices (such as hardware wallets) that allow access to crypto assets. This modality is similar to the traditional custody of documents or physical assets, although with an added technological responsibility.

ii. **Conditional custody (escrow or deposit in guarantee)**
The notary may be required to act as a third-party custodian of keys or devices that allow access to crypto assets, linking their delivery to the fulfilment of certain conditions (e.g., payment of a price, performance of an obligation, etc.).

iii. **Custody in the context of testamentary or succession transactions**
The notary may hold information necessary to access crypto assets in order to deliver them to the rightful heir after the death of the owner. This function may include keys, access instructions, or multi-factor authentication elements.

iv. **Custody as a means of proof or documentation**
In some cases, the notary may be asked to record or hold documents or media related to the possession or transactions of crypto assets (such as screenshots of wallets, transactions on block explorers, etc.).

The various types of custody of crypto assets that may be requested from a notary— such as custody of private keys, escrow, management in inheritance contexts, or probative documentation—carry significant risks of money laundering and terrorist financing, as they can be used to conceal the illicit origin of funds, simulate transactions, legitimize assets of dubious origin, or introduce undeclared assets into the formal economic circuit. Notarial intervention, by providing a presumption of legality, can be inadvertently exploited as a concealment mechanism if adequate due diligence measures and verification of the origin and purpose of the assets are not applied.

5

BEST PRACTICES TO MITIGATE THE RISKS

The emergence of crypto assets in notarial transactions, although legitimate in many cases, requires increased attention from notaries. As seen before, these transactions can be used as mechanisms to legitimize capital of criminal origin or finance illegal activities under the cover of public documents.

Therefore, asking about and analysing the origin of the funds, the economic justification for the transaction, and identifying the customer and beneficial owner are essential.

However, considering the specific characteristics of crypto assets, in addition to the customer due diligence obligations, a series of specific preventive measures adapted to this new reality may be applied.

Some of the most relevant measures we recommend are outlined below:

Understanding the type of crypto asset

Identify whether the asset in question is a privacy token (such as Monero, Zcash, or Dash in private mode), a utility token, an NFT, or a stablecoin, and the acquisition method (through regulated exchangers, peer-to-peer, etc) as levels of anonymity and stability vary significantly. Apply greater scrutiny to assets designed or acquired to hide transactions.

Enhanced verification of the ownership and the origin of funds

As we have seen, in transactions involving crypto assets as a means of payment or contribution (e.g., in sales, capital contributions, or donations) it is almost impossible to really know who owns the crypto assets and who receives them. At most we will have a public key of a wallet that delivers the crypto asset and another that receives them.

In addition, we cannot be sure that the payer/contributor/donator is the only one in possession of these keys and therefore, in that moment, crypto assets may be changing ownership without the notary's knowledge. In cases of capital contributions, this is not very different from when certain movable assets (e.g. a laptop computer or a printer) that cannot be registered in any registry are handed over.

Although the notary will not be able to certify reliably that the crypto assets have changed ownership, he or she will be able to take certain actions that will help to learn more about the transaction. The notary may request documentation or certain actions from the customers intended to prove the ownership of the assets and the lawful origin of the assets. This may include:

- **Statements from regulated exchangers** (if the assets were acquired thorough an exchanger and/or are in wallets controlled and managed by wallet providers) certifying the ownership of the wallet where they are allocated, as often requested to a financial institution to certify the ownership of a bank account.

- In case of transactions with self-hosted addresses (unhosted wallets), request that the customer prove ownership of the self-hosted wallet through **technical evidence** (digital signatures, screenshots with metadata, signed wallets, etc.) and, if possible, the traceability of the funds deposited into it.

- Previous tax returns showing the crypto assets, if mandatory to be declared according to the regulation of the country.

- Contractual documentation supporting their legitimate acquisition.

- If the crypto assets are hosted by exchangers/ wallet providers, the notary can request the customer to access the wallet, in his presence, through its mobile phone. Even it is not a certain proof of ownership of the wallet or the assets, it can demonstrate access and control over the wallet.

Verification of transfer completion

Another measure that can be applied is to verify that a transfer for the amount of crypto assets indicated by the parties in a transaction has been made from the address indicated by the originator to the address indicated by the recipient.

This can be done by using **blockchain explorers**. Blockchain explorers are free online tools that allow you to view and analyse information on a blockchain.

There are currently dozens of explorers for various blockchains. Among these, we can name Blockchain.info, BlockExplorer, BlockTrail, BlockCypher, and many more that work for Bitcoin.

EtherScan and EtherChain work for Ethereum, and there are many others for each existing blockchain. Regardless of which blockchain is explored, almost all of them display similar data, although they may differ in appearance.

Once chosen the blockchain explorer that supports the specific blockchain of interest (Bitcoin, Ethereum, etc.), **the transaction ID (TXID) or transaction hash, a wallet address,** should be entered in the explorer's search bar.

The explorer will display the information associated with the transaction, address, being searched for. This may include details such as:

- The value of the transaction.
- The addresses involved.
- The number of confirmations.
- The date and time of the transaction.
- The status of the transaction (confirmed, pending, etc.).

This way, in notarial transactions involving the movement of crypto assets (e.g. sales, capital contributions, or donations) it will be possible for the notary to certify that the transaction has been made from the address indicated by the originator (whose control or ownership was verified as suggested in paragraph a) to the address indicated by the recipient (whose control or ownership has also been verified as suggested in paragraph a) for the amount of crypto assets involved in the transaction.

Control and documentation in cases of notarial custody

Where custody of private keys, access devices, or documentation related to crypto assets is requested, the notary may:

- Clearly document the assignment, its conditions, and its purpose.
- Identify the depositor (and request documentation proving the ownership of the crypto assets as suggested in subparagraph a) and, where applicable, the beneficiary.
- Verify the real existence of the crypto assets: If the crypto assets are hosted by wallet providers, this can be done by requesting the customer to access the wallet, in his or her presence, through its mobile phone, to demonstrate ownership and the amount of crypto assets hosted in the wallet or by requesting documentation about the wallet or device balance.
- Assess the nature and economic volume of the underlying assets.
- Record any instructions related to the delivery, use, or return of such items.

Rejection of transactions involving mixed or anonymized assets

With the objective of preventing the use of techniques designed to hide the trail of crypto assets, it is highly recommended to consider not accepting transactions if the crypto assets originate from mixing services ("mixers"), tumbler services, or privacy protocols such as Tornado Cash, unless the customer provides documentary evidence of a legitimate reason and clear traceability.

Inclusion of warnings and limitations in the notarial documents

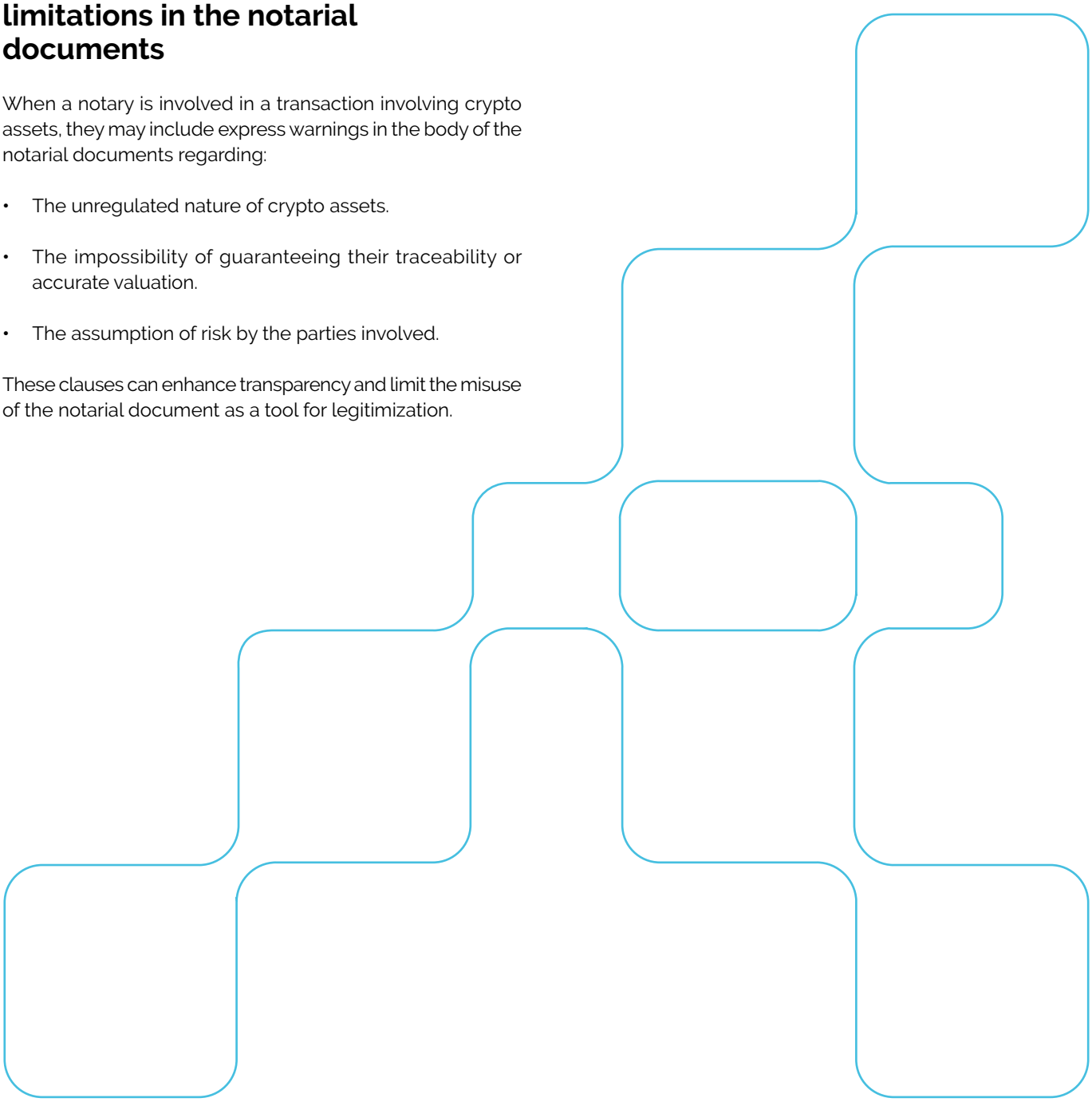
When a notary is involved in a transaction involving crypto assets, they may include express warnings in the body of the notarial documents regarding:

- The unregulated nature of crypto assets.
- The impossibility of guaranteeing their traceability or accurate valuation.
- The assumption of risk by the parties involved.

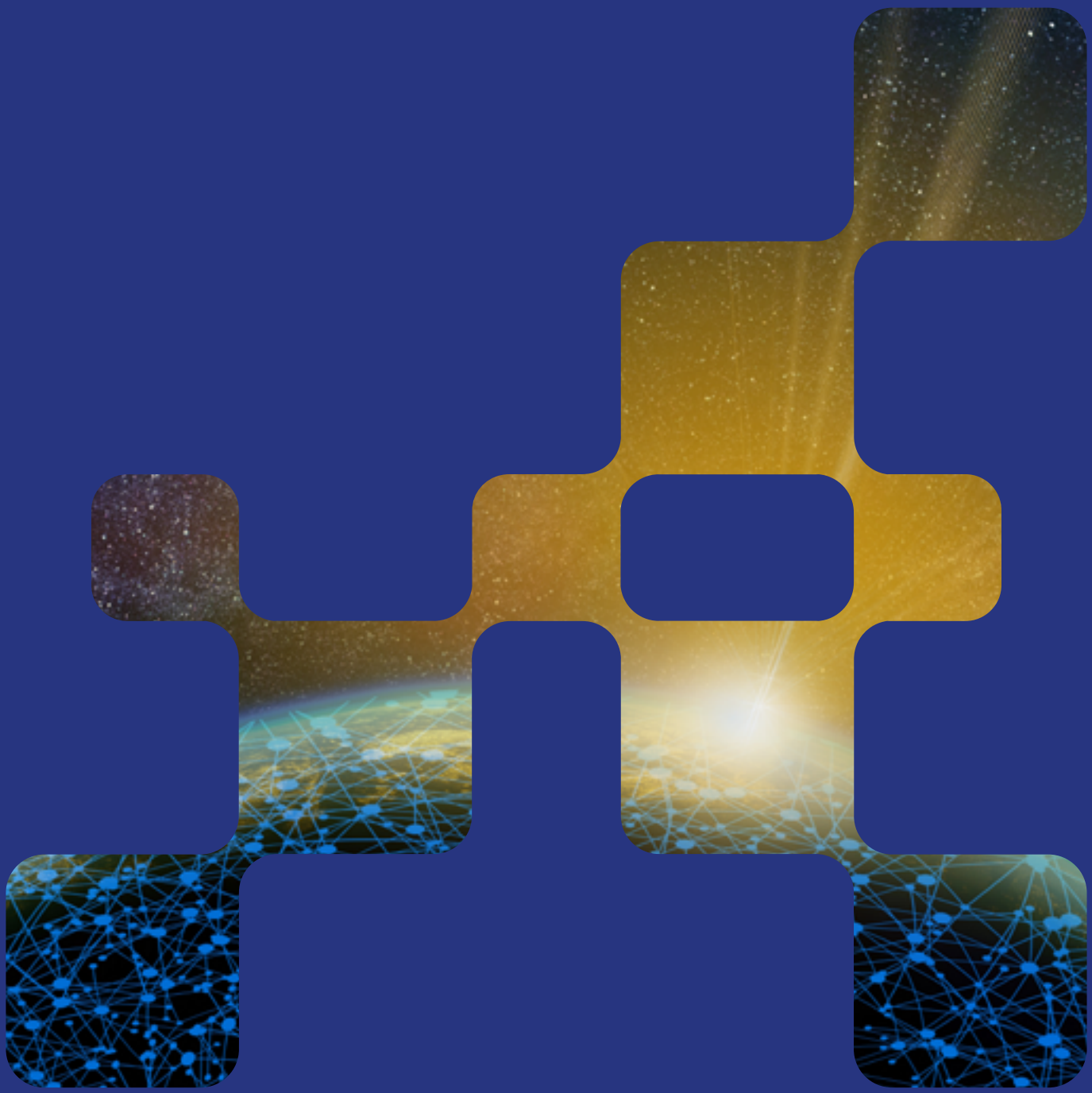
These clauses can enhance transparency and limit the misuse of the notarial document as a tool for legitimization.

Reporting of suspicious transactions

Where there are reasonable grounds to believe that crypto assets may be related to money laundering or terrorist financing, the notary must immediately report the transaction to the competent authority, in accordance with current regulations, without informing the parties.



CONCLUSIONS



As mentioned in the introduction, the last decade has seen a continual growth in their adoption by businesses, individuals and even governments as a method of payment as well as potentially lucrative assets to invest in.

However, the use of crypto assets poses significant risks in terms of money laundering and terrorist financing due to their digital, decentralized, and, in many cases, pseudonymous nature. These characteristics make transactions difficult to trace, allow for the rapid cross-border movement of funds, and facilitate anonymity, making them attractive tools for criminal and terrorist networks. It is difficult to know the legal origin of the funds used to acquire crypto assets.

It seems clear that, by using crypto assets, anonymity and the use of "front men" could be brought to any transaction, as it is almost impossible to verify who the real owner of the crypto assets is, because we only know the person who holds the keys.

In addition, it is difficult to know the legal origin of the funds used to acquire crypto assets and it is easy to hand them over without leaving any trace (simply handing over the keys to another person would suffice).

While crypto asset service providers (CASP) are key players in the management and custody of these assets, they are not the only ones who must address the associated risks. Other obliged entities - such as notaries - may be directly or indirectly exposed to transactions involving crypto assets. It is therefore essential to implement adequate measures to prevent money laundering and terrorist financing.

The lack of control and cooperation between different types of obliged entities can open regulatory gaps that favor opacity and abuse of the financial system. Consequently, it is essential that all obliged entities, regardless of their sector of activity, be trained to identify signs of risk associated with crypto assets, apply proportionate due diligence measures, and actively collaborate with the competent authorities.

Given their role in ensuring the legality of contracts, notaries must be particularly vigilant in transactions involving the direct or indirect use of crypto assets. The adoption of enhanced due diligence procedures and best practices to mitigate the risks, together with ongoing training and close cooperation with financial intelligence units, is essential to prevent their role from being inadvertently used as a channel for illicit activities.

In addition, the additional measures notaries may apply to mitigate the risks proposed in this document not only respond to general regulatory obligations but are also specifically tailored to the risks inherent to crypto assets, whose digital, decentralized, and sometimes anonymous nature makes them particularly sensitive instruments for ML/TF. The combination of forensic technology, legal context analysis, and professional judgment will enable notaries and other obliged entities to act responsibly and effectively.

Only through a coordinated, comprehensive, and proactive approach by all obliged sectors can an effective response to the threats posed by the illicit use of crypto assets be ensured. This protects not only the integrity of the financial system, but also economic stability and public safety as a whole.

Council of the Notariats of the European Union

Avenue de Cortenbergh, 120
B-1000 Bruxelles

+ 32 (0)2 513 95 29
info@cnue.be

www.cnue.be

Notaries of Europe
Providing legal certainty