2 Crypto-assets – Terminology, overview and milestones

2.1 Terminology, classification and definitions

Even the basic term 'crypto-asset' presents a number of challenges in terms of definition. Thus – at least prior to MiCAR – there was no general consensus on what constitutes a crypto-asset and what does not.[16] Most definitions began with the framework of the first – and still the most important – crypto-asset: Bitcoin.[17] It is generally accepted that crypto-assets, sometimes also referred to as virtual or crypto-currencies (see below), – as the name suggests – are linked to cryptography, or encryption.[18] This is linked to the concept of the system's decentralisation – traditional crypto-assets have a highly decentralised approach and are characterised by the absence of intermediaries. There is no central server where all data is stored, as is the case with traditional companies. Instead, the data is distributed across all members of the system (so-called *nodes*)[19]. In this context, the term *'distributed ledger'* is used.[20] Put simply, this means that all data is stored on every participating node and not centrally on a single server. It is precisely this technical feature that makes encryption indispensable, as otherwise anyone in the system would have access to all data points. Encryption, or more precisely the combination of a private and public key, ensures that only those who possess both keys can access their crypto-assets. Cryptography is thus an indispensable security element of crypto-assets and not, as is often claimed, the purpose of the system, for example to anonymise cash flows. Ownership of crypto-assets is verified by the public and private keys. Due to the absence of a central control authority, the so-called 'double-spending' problem must be resolved; this arises because there is no central control over transactions, meaning an owner could potentially execute two transactions simultaneously, one of which without actually possessing the funds (for further details, see Chapter 2.2). For this reason, *Nakamoto*[21] had already provided for verification by the network – so-called miners check the validity of the transactions.[22] Mining can – again, in simplified terms – be understood as a decentralised verification network for transactions.[23] Individual transactions are collected into blocks, the blocks are linked together, and the preceding blocks are verified in the process.[24] This is referred to as the 'blockchain', a kind

16 *Wyman*, Cryptocurrencies and public policy (2018), https://www.oliverwyman.com/our-expertise/insights/2018/feb/cryptocurrencies-and-public-policy.html.
17 See Chapter 2.2 and *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf.
18 A fairly accessible summary of the associated cryptographic methods can be found, for example, at *Bitcoin Blog*, Bitcoin cryptography for beginners, https://bitcoinblog.de/2013/12/22/kryptografie-des-bitcoins-fuer-anfaenger/.
19 See, for example, *Bitcoin Core*, Running a full node, https://bitcoin.org/en/full-node#minimum-requirements.
20 For this term, see *Coindesk*, What is a distributed ledger, https://www.coindesk.com/information/what-is-a-distributed-ledger.
21 *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system, op. cit., 3f.
22 In the case of Bitcoin, this is achieved by means of so-called Proof of Work; for further details on this and on all of the above, see Chapter 2.2.
23 *BTC Echo*, How does Bitcoin mining work, https://www.btc-echo.de/tutorial/wie-kann-ich-bitcoins-minen/.
24 See also *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system, op. cit.; this is an essential component for the security of the system, as each additional block drastically increases the likelihood and the effort required for a hacking attack (see, for example, the calculation in Nakamoto, op. cit., p. 7 et seq.).

of database that is stored in a decentralised manner and, due to this decentralisation, is immutable.[25] All these are essential elements of a crypto-asset. In general, the crypto world is characterised by a widespread lack of standards and recognised terminology. Some definitions have focused more on the intended uses and, in my view, have fallen short of capturing the possibilities that have emerged since the wave of ICOs.[26]

A first definition at European level was established relatively early on[27] and was widely regarded as successful (apart from the term 'currency', see below) in the 5th Anti-Money Laundering Directive:[28]

> *'virtual currencies' means a digital representation of value that is not issued or guaranteed by a central bank or public authority, is not necessarily linked to a legally established currency, and does not have the legal status of a currency or money, but is accepted by natural or legal persons as a means of exchange and can be transferred, stored and traded electronically;*

In the past, crypto-assets were frequently referred to as cryptocurrencies or virtual currencies. However, as they are not a 'currency', this term has previously been criticised and described as misleading.[29] Correctly speaking, they are not legal tender, which, as is well known, can only be issued by the OeNB/ECB.[30] However, the ECJ – in its only ruling to date on Bitcoin – speaks very clearly of a currency[31] and the first definition under European law also referred to 'virtual currencies' (see above).

Regardless of this the umbrella term 'crypto-assets' has become established.[32] This is explicitly reflected, for example, in the basic legal definition of crypto-assets,[33] although it should be noted that the German version of the text may not be entirely convincing:[34]

> *'crypto-asset' means a digital representation of a value or a right which can be electronically transferred and stored using distributed ledger technology or similar technology;*

In my view, this discussion and historical development of the term also reflects a functional perspective; whilst Bitcoin was indeed intended as a means of payment in 2008, the concept of it as an asset has now indisputably prevailed. Crypto-assets are used and viewed much more as an investment than as a means of payment.

25 For the key aspects, see *Futurezone*, 'What exactly is this blockchain?', https://futurezone.at/digital-life/was-ist-eigentlich-diese-blockchain/270.616.934.

26 See, for example, the definition by *the Bank for International Settlements*, Digital Currencies (2015), https://www.bis.org/ cpmi/publ/d137.htm. For instance, it states there – alongside 'virtual' and 'peer-to-peer' – that there must be no liable party, which, in my view, already appears questionable in the case of Ethereum.

27 Applicable from 10 January 2020 until the entry into force of MiCAR.

28 Article 1(2)(d)(18) of the 5th EU Anti-Money Laundering Directive (Directive 2018/843).

29 See, for example, *Dobrowolski*, 'Overview of the different regulatory frameworks for Initial Coin Offerings', Der Gesellschafter, 3/2018, 147; also critical: *OENB*, 'Are virtual currencies such as Bitcoin an alternative to traditional currencies such as the euro?', https://www.oenb.at/FAQ/sonstiges.html.

30 See Section 61 NBG.

31 ECJ, 22 October 2015, C-264/14 (Hedqvist).

32 See also *FMA*, What is an ICO?,loc. cit.

33 See Article 3(1)(5) MiCAR.

34 The English version explicitly refers to a 'crypto-asset'. In my view, the German translation as 'Wert falls somewhat short.

Furthermore, the term 'asset' also encompasses means of payment[35] and can therefore be used as an umbrella term.[36]

The two most significant crypto-assets to date (*Bitcoin* and *Ethereum*) will be discussed in more detail in the following chapters, as these also represent major milestones in the "crypto-asset world" and will also significantly shape future developments in this area. For example, the development of Bitcoin was what initially triggered the entire development of crypto-assets. The same applies to Ethereum in relation to Initial Coin Offerings. Without the programmability[37] of a blockchain, these would simply not have been possible.

The term 'Initial Coin Offering' *(ICO)* will play an important role in this book. The term was chosen in reference to the term for an initial public offering (IPO).[38] With the help of 'smart contracts' – a program code that executes agreed obligations fully automatically when certain factors ('triggers') are met[39] – existing crypto-assets are collected as funding and new tokens are issued.[40] The new tokens are generally linked to a specific company or project – the potential uses of such tokens are, in principle, unlimited. Regulatory authorities rightly point out that tokens vary in design and therefore cannot be categorised generally; rather, a case-by-case assessment is required.[41] Technically, ICOs are frequently conducted on the Ethereum blockchain (e.g. ERC-20 tokens).[42] As mentioned in the introduction, these tokens newly created via ICOs are often grouped under the term 'altcoins'.[43]

This also shows that there is no universally applicable distinction between the terms 'coin' and 'token'. For example, in an Initial *Coin* Offering, a *token* is usually issued, which is then in turn (at least partially) referred to as *an altcoin*. To be more precise, although a clear distinction does exist, it is not applied precisely in common parlance. Rather, the terms are often used as synonyms.[44] Whilst a coin has its own blockchain, tokens are based on an existing blockchain.[45] In the remainder of this book, this distinction will generally be observed; however, where common terms – such as ICO – are used, these are adopted.

35 Asset is generally translated as 'asset' and thus encompasses all forms of capital investment, including money and foreign exchange, for example *Gründerszene*, Lexicon on the term 'Asset', https://www.gruenderszene.de/lexikon/begriffe/asset?interstitial_click.

36 This is also explicitly stated by *the FMA*, 'What is an ICO?', op. cit.

37 See *Buterin*, op. cit., 1.

38 See, e.g., *a creative construction*: ICO instead of IPO, https://www.creativeconstruction.de/blog/ico-statt-ipo-wie-das-blockchain-basierte-finanzierungsmodell-die-startup-welt-auf-den-kopf-stellt/.

39 For a detailed discussion of smart contracts, see, for example, *Szabo*, 'Formalizing and securing relationships on public networks', https://ojphi.org/ojs/index.php/fm/article/view/548/469; *Christidis et al*, Blockchains and Smart Contracts for the Internet of Things, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408.

40 See also *FMA*, What is an ICO? op. cit.

41 See, e.g., *FMA*, What is an ICO? op. cit.

42 For more on this term, see BTC Echo, What is an ERC-20 token?, https://www.btc-echo.de/tutorial/was-ist-ein-erc-20-token/. For a detailed explanation, see *Github*, OpenSource on the ERC-20 standard, https://github.com/ethereum/EIPs/blob/ma-ster/EIPS/eip-20.md.

43 For example, *Investopedia*, Definition – Altcoin, https://www.investopedia.com/terms/a/altcoin.asp. However, the term is also used in different ways; see, for example, *Blockchainwelt*, What are Altcoins?, https://blockchainwelt.de/ altcoin-definition-und-uebersicht/.

44 Explicitly so in *FMA*, What is an ICO? op. cit.

45 See, e.g., see *Cointrend*, What are tokens and how do they differ from coins?, https://cointrend.de/kryptowiki/token/.

2.2 Bitcoin – the starting point for crypto-assets

Bitcoin was first described in a white paper in 2008 by Satoshi Nakamoto[46] – a pseudonym.[47] On 3 January 2009, the Bitcoin network went online for the first time; Nakamoto generated (via 'mining') the first block[48].[49] Even before Bitcoin, multiple attempts had been made to create digital money.[50] Initially, the media covered Bitcoin from just two perspectives: on the one hand as a financial bubble phenomenon and on the other as a means of payment for illegal activities (e.g. on the 'Darknet'). It was only later that the underlying technology ('blockchain', see Chapter 2.1) and the innovation associated with crypto-assets were examined in greater detail.[51] The history of Bitcoin is characterised by extreme price fluctuations, both upwards ("bull run"/"to the moon") and downwards.[52] The high volatility of crypto-assets in general, and of Bitcoin in particular, is not usually observed in financial markets. In this context, however, it should also be noted that the value of Bitcoin has currently 'stabilised' and remains high. In addition to technical aspects of the blockchain, the limited money supply of Bitcoin (21 million units) has recently been highlighted with increasing frequency.[53] Bitcoin is therefore regarded as a mechanism for preserving value.[54] Comparisons are frequently drawn with (digital) gold;[55] in some quarters, there is even discussion as to whether it should be held as part of central bank reserves.[56]

In my view, the most exciting aspect of Bitcoin is the interlinking of several specialist fields to create a new and innovative means of payment. From today's ex-post perspective, Nakamoto's visionary idea – which was probably only fully appreciated by both the scientific community and the financial sector at a later date – appears groundbreaking in 2008. Through the interdisciplinary combination of cryptography, economic incentives and computer science, the basic parameters for a peer-to-peer-based, global payment

46 To this day, it is not known who or which group lies behind this name. The identity is a much-discussed topic within the community – there are numerous theories: for an overview, see *Wikipedia*, Satoshi Nakamoto https://en.wikipedia.org/wiki/Satoshi_Nakamoto.

47 *Nakamoto*, Bitcoin: A peer-to-peer electronic cash system, https://bitcoin.org/bitcoin.pdf.

48 See the publicly accessible blockchain, Block 0: https://blockexplorer.com/block/000000000019d6689c08 5ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.

49 For further details, see *Wallace*, The rise and fall of Bitcoin, https://www.wired.com/2011/11/mf-bitcoin/.

50 For an overview, see *Tschorsch/Scheuermann*, Bitcoin and beyond: A technical Survey on Decentralised Digital Currencies, https://eprint.iacr.org/2015/464.pdf.

51 See, for example, *Sinegal* (2018). Blockchain: The disruptive power of decentralisation, http://www.morningstar.at/at/ news/168301/blockchain-die-disruptive-macht-der-dezentralisierung.aspx/.

52 See the chart on *Coinmarketcap*, Bitcoin Chart https://coinmarketcap.com/currencies/bitcoin/.

53 See, for example*, BTC Echo,* "No guarantee of 21 million Bitcoin"? BlackRock faces criticism, 20 December 2024, https://www.btc-echo.de/schlagzeilen/keine-garantie-fuer-21-millionen-bitcoin-blackrock-erntet-kritik-198083/

54 For example, *Fidelity*, "Bitcoin as an aspirational store of value", February 2024, https://www.fidelitydigitalassets.com/sites/g/ files/djuvja3256/files/acquiadam/1125481.2.0%20-%20FDA%20Bitcoin%20as%20an%20Aspirational%20 Store%20of%20Value%20Revisited%20V2.pdf.

55 See, for example, *Deutsche Bank*, "I could potentially see Bitcoin to become the 21st century gold", https://www.db.com/ what-next/digital-disruption/dossier-payments/i-could-potentially-see-bitcoin-to-become-the-21st-century-gold.

56 For example, in the Czech Republic – *Euronews*, https://www.euronews.com/next/2025/02/17/should-european-banks -con-sider-holding-cryptocurrencies-like-bitcoin-as-a-reserve-asset, 17 February 2025 or the US – *DerStandard,* How Trump plans to strengthen the dollar with a state-backed Bitcoin reserve, 20 February 2025, https://www.derstandard.at/ story/3000000257620/so-will-trump-mit-einer-staatlichen-bitcoin-reserve-den-dollar-staerken.

network was created.[57] Although the concept of decentralisation can be traced back to the French Revolution (18th century), in my view it has only really taken hold in large sections of society in recent years, with the aftermath of the financial crisis certainly having reinforced these developments.[58] This, combined with a growing distrust of the state and political and economic institutions, has shaped the development of crypto-assets. On the other hand, innovation in the financial market has also been rather moderate in recent decades – whilst news can now be sent around the world in fractions of a second, payment transactions have not accelerated to the same extent. Even today, 'instant'[59] or 'peer-to-peer'[60] transactions in the financial market are regarded as an innovative step, even though Bitcoin made this possible over 15 years ago.

The key characteristics of Bitcoin are described below, which apply in part to other crypto-assets as well. Decentralisation was already mentioned in the introduction above, but will be explained in more detail. Bitcoins are not issued by any central authority; no single person acts as an issuer – rather, a digital open-source[61] program generates Bitcoin as a reward for solving a computational problem and distributes it. This provides the incentive for carrying out verification activities within the Bitcoin network ('mining'); the rewards are halved every 210,000 blocks (roughly every four years). Initially, 50 Bitcoins were distributed for a successfully verified block; currently (2025), the 'mining reward' stands at 3.125 Bitcoins and will be reduced to 1.625 Bitcoins in 2028. This also explains why there is often talk of deflation (= the price of the asset rises) in the Bitcoin network. The maximum number of Bitcoins is 21 million; any change can only be achieved democratically through a majority of computing power ('fork'), as no one owns or controls the Bitcoin network. "Mining" thus serves two functions in the Bitcoin network: on the one hand, the creation of new units of value and thus an increase in the money supply, and on the other hand, the verification of transactions, as there is no central authority that can control, manage or influence the transactions. This distinguishes the Bitcoin network significantly from the rest of the financial market; a bank transfer is always centrally controlled and managed by a bank. The payment/transfer therefore takes place directly between users (a true "peer-to-peer" network). All transactions are recorded in a public ledger ('blockchain') – as already explained in Chapter 2.1, this blockchain is not stored centrally on a server, but on every computer participating in the system.[62] Bitcoins are held by the users themselves – through the safekeeping of the private key – in the form of so-called electronic wallets.

57 See also *Berentsen/Schär*, Bitcoin, Blockchain and Cryptoassets (2017).

58 For a historical overview of decentralisation and various perspectives, see: *Wikipedia*, Decentralisation, https://en.wikipedia.org/wiki/Decentralization.

59 See, for example, the ECB's TIPS project, which was launched in November 2018: ECB, What is TARGET Instant Payment Settlement (TIPS)?, https://www.ecb.europa.eu/paym/target/tips/html/index.en.html.

60 This does not actually take place on a peer-to-peer basis, but always via central bank interfaces; however, the front-end allows users to make payments easily, for example via a telephone number. From a purely technical perspective, however, it involves an IBAN linked to a telephone number and a standard bank transaction. See, for example, *Zoin*, What is Zoin?, https://www.zoin.at/was-ist-zoin/.

61 Thus, a system that is visible to everyone and can be modified according to common rules.

62 The data volume currently (April 2019) amounts to approximately 220 gigabytes: *Statista*, Size of Bitcoin Blockchain https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/.

This also gives rise to the pseudonymity[63] of the Bitcoin network – wallet addresses cannot be linked to any specific individual. Any transaction involving such wallets requires authorisation via the private key, which – unlike the existing financial system – makes it impossible for third parties to access them. An example will illustrate this: A court determines that 10 Bitcoins have been stolen. The thief is found, and the money is still in 'his' wallet – the only way to recover the money is for him to hand over the private key; no central authority can freeze the account or carry out a chargeback. In the 'traditional' financial market, the bank would freeze the account on a court order and later carry out a chargeback. This sometimes results in police authorities knowing where the 'money' is but being unable to access it.[64] This peculiarity becomes even clearer in the event of the loss of the private key – the bitcoins in this wallet are completely lost and can no longer be 'restored'/recovered/used.[65] This also means that a transaction that has been initiated and executed cannot be reversed by anyone (except the recipient in the sense of a return transfer). The actual use of crypto-assets, and Bitcoin in particular, for illegal payments,[66] which is made possible by pseudonymity, must be critically highlighted. Furthermore, technical aspects of blockchain technology present challenges.[67] Scalability is particularly worth mentioning.[68] However, work has been underway for some time to address this challenge.[69] The extreme energy consumption is also frequently criticised. Here, other crypto-assets are attempting to explore new avenues;[70] see, for example, the next chapter on the transition of Ethereum.

63 There is often a misconception regarding the anonymity of the Bitcoin network. However, since all transactions can be traced once the wallet has been uniquely identified and linked to a person, what exists is pseudonymity.

64 See, for example, *Quartz* on the so-called WannaCry (ransomware): 'The hackers behind the WannaCry ransomware attack have finally cashed out', https://qz.com/1045270/wannacry-update-the-hackers-behind-ransomware-attack-fi-nally-cashed-out-about-140000-in-bitcoin/.

65 Estimates suggest over a third of all Bitcoins are lost, *Ethereumworldnews*, 36% of BTC in Circulation is Lost, https://ethereumworldnews.com/36-of-btc-in-circulation-is-lost-making-bitcoin-technically-more-scarce/. The private key can be lost in many situations – for example, an old hard drive containing the private key was thrown away: *Welt*, 32-year-old accidentally throws 94 million in the bin, https://www.welt.de/wirtschaft/article171372723/32-Jaehriger-wirft-versehentlich-94-Millionen-Euro-auf-den-Muell.html or the private key not being handed over following a death: *DerStandard*, Crypto millionaire dies – family searches for private keys, https://derstandard.at/2000080919325/Krypto-Millionaer-verstorben-Familie-sucht-nach-Private-Keys-fuer-Vermoegen.

66 For example*, DerStandard,* Bitcoin is booming as a means of payment on the dark web, https://derstandard.at/2000096604599/Bit-coin-boomt-als-Zahlungsmittel-im-Darknet?ref=rec.

67 For a detailed look at various challenges: *Bank for International Settlements* (2018), 'Looking beyond the hype', https://www.bis.org/publ/arpdf/ar2018_5_de.pdf.

68 See, for example, *BTC Echo*, Bitcoin vs Mastercard/Visa transaction volume, https://www.btc-echo.de/bitcoin-vs-ma-stercard-visa-transaktionsvolumen/.

69 Whether through changes to the blockchain, such as with other crypto-assets (see, for example, Blockchain Hero, 17,000 transactions per second, https://blockchain-hero.com/17-000-transaktionen-pro-sekunde/) or through additional innovations/technical measures, such as more transactions per block or off-chain transactions (see, for example, the Lightning Network or the general discussion on this topic, e.g. *Blocklab*, Discussion on Scaling, https://site.blocklab.de/2017/Skalierung/).

70 Examples include Proof of Stake/Trust procedures instead of Proof of Work (ensuring system integrity through high computational effort) (see, for example, *King/Nadal*, PPCoin: Peer-to-peer Crypto-Currency with Proof-of-stake (2012), https://pdfs.semanticscholar.org/0db3/8d32069f3341d34c35085dc009a85ba13c13.pdf).

From a regulatory perspective, it was recognised in most European countries[71] and – following extensive discussion – also in the USA[72] that, prior to MiCAR, no financial market regulations applied to Bitcoin. However, as the FMA correctly clarifies, this does not generally mean that no regulations apply to business activities relating to Bitcoin.[73] Prior to MiCAR, Bitcoin was classified in Germany as "unit of account" and thus as a financial instrument.[74] However, a German criminal court also rejected this classification;[75] BaFin and the German Federal Ministry of Finance (BMF) nevertheless maintained the classification as a unit of account/financial instrument.[76] Put simply, this meant that any trading, brokerage activity, intermediation, etc. was already subject to a licensing requirement prior to MiCAR.[77] In the course of the implementation of MiCAR in Germany, this peculiarity was resolved.[78] Bitcoin has also been classified differently under tax law: until a landmark ruling by the ECJ, some EU countries assumed that Bitcoin transactions were subject to VAT, which the ECJ rejected on the grounds of their comparability with currencies.[79]

Since the first edition, the broader context and technological infrastructure surrounding Bitcoin have evolved considerably. In addition to its well-known features – such as the decentralised creation of new coins and blockchain-based transaction processing – the focus is now on the implementation of second-layer solutions, in particular the Lightning Network. This network enables significantly faster and more cost-effective transactions, thereby helping to further realise the original vision of a global peer-to-peer payment network. At the same time, increased institutional interest has led to greater integration of Bitcoin into traditional financial systems. This development is reflected in regulatory adjustments, such as the inclusion of Bitcoin within the scope of MiCAR, and the – aforementioned – reassessment of its role as 'digital gold'. The increasing use of renewable energy in the mining sector – together with the significantly lower electricity consumption in the Lightning Network – underscores the growing debate on sustainability and the technical and environmental challenges. Overall, these developments reflect a maturing of the Bitcoin ecosystem, which has evolved from an experimental payment instrument into an integral part of modern financial markets.

71 See, for example, *EBA*, EBA warns consumers on virtual currencies (2013): https://eba.europa.eu/-/eba-warns-consum-ers-on-virtual-currencies or, for many, *FMA*, Focus on Bitcoin: https://www.fma.gv.at/fma-themenfokusse/fma-fokus-bitcoin-co/.

72 For a detailed discussion, see, for example, *Brito/Castillo*, Bitcoin – A primer for Policymakers (2013), https://www.mercatus.org/sys-tem/files/Brito_BitcoinPrimer.pdf.

73 For example, where activities subject to authorisation are carried out in connection with bitcoins, such as the collection of funds to purchase bitcoins with the obligation to return the resulting profit or loss (deposit for management); for other cases, see *FMA*, Focus on Bitcoin https://www.fma.gv.at/querschnittsthe-men/fintechnavigator/bitcoin-co/.

74 See *BaFin*, Bitcoins: Supervisory Assessment and Risks for Users (2013), https://www.bafin.de/SharedDocs/ Veroeffentlichungen/DE/Fachartikel/2014/fa_bj_1401_bitcoins.html.

75 Berlin Court of Appeal, 25 September 2018, (4) 161 SS 28/18 (35/18).

76 See the parliamentary questions, summarised at: *Private Banking Magazine*, BMF classifies trading in crypto-assets as subject to authorisation, https://www.private-banking-magazin.de/nach-urteil-gegen-verwaltungs-praxis-der-bafin-bmf-stuft-handel-mit-krypto-assets-als/.

77 See *BaFin*, op. cit.

78 See the German implementing legislation in detail: KMAG and FinmaDiG.

79 ECJ 22 October 2015, C-264/14 (Hedqvist).

All in all, there is – with the exception of Germany – a consensus that, due to its structure, Bitcoin did not fall under financial market regulations prior to the entry into force of MiCAR. However, the 5th Anti-Money Laundering Directive had already extended the due diligence obligations for combating money laundering to virtual currencies and thus to Bitcoin. According to the prevailing view, however, Bitcoin has been subject to the provisions of MiCAR since 30 December 2024 – despite its 'special decentralised status'.[80] In my view, it is undisputed that MiCAR applies to the provision of crypto-services relating to Bitcoin.[81] However, in the absence of identifiable issuers[82], it is argued that Bitcoin does not fall under Parts II–IV of MiCAR and that, consequently, there may be no obligation to publish a white paper.[83]

2.3 Ethereum – a significant expansion of the scope

On the one hand, Ethereum is technically based largely on Bitcoin, whilst on the other hand, significant additional features and developments have been incorporated. The most important differences are briefly outlined below. The Ethereum white paper was published in 2014,[84] and the network went live in 2015.[85] The very title of the white paper[86] makes it clear that Ethereum primarily serves a different purpose to Bitcoin. Whilst, as outlined above, Nakamoto primarily had a payment function in mind, *Buterin* deliberately designed Ethereum as the basis for a programmable network on the blockchain.[87] Unlike Bitcoin, it is therefore possible to programme and use applications on the Ethereum blockchain. This further development enabled the creation of ICOs.[88] In other words: without Ethereum, there would be significantly fewer tokens and this work would lack a foundation.

Ethereum is generally described as the largest and most established decentralised software platform.[89] In 2014, Ethereum issued the token underlying the platform (Ether, ETH) as part of a pre-sale,[90] the demand was enormous and more than 25,000 bitcoins were raised,[91] which, at the price at the time, corresponded to approximately 12.5 million US dollars.[92] This process is often classified as the first ICO. Ether plays a key dual role within the Ethereum network: on the one hand, this crypto-asset can – as usual – be traded, transferred, etc. (similar to Bitcoin); on the other hand, Ether functions as a means of settlement in programmes on the Ethereum platform. An example will illustrate this: if a programmer creates a 'casino-like' programme developed on the blockchain[93] with the following

80 *Völkel* in *Kalss/Krönke/Völkel* (eds), Crypto-Assets (2025) Art. 3 MiCAR para. 26 et seq., hereinafter *Kalss/Krönke/Völkel*.
81 See, e.g., *Lehmann/Völkel* in *Kalss/Krönke/Völkel* Art. 3 MiCAR para. 88.
82 See, for example, *FMA*, Bitcoin & Co (expressly stating "in the absence of an issuer"), https://www.fma.gv.at/kontaktstelle-fintech-sandbox/fintechnavigator/bitcoin-co/.
83 In this sense, see *Lehmann/Völkel* in *Kalss/Krönke/Völkel,* Art. 3 MiCAR, para. 88.
84 *Buterin*, A next generation smart contract & decentralised application platform, http://blockchainlab.com/pdf/Ethere-um_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.
85 30 June 2015, see the first block on *Etherscan*, Genesis Block, https://etherscan.io/block/0.
86 "Smart contract and decentralised application platform"; both components are examined in more detail in this chapter; see also Chapter 2.4.
87 *Buterin*, op. cit.
88 See Chapter 2.4.
89 For example, *Investopedia*, Bitcoin vs Ethereum, https://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethe-reum-driven-different-purposes.asp.
90 For details, see *Buterin*, Launching the Ether Sale, https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/.
91 *Buterin*, Ether Sale: A Statistical Overview, https://blog.ethereum.org/2014/08/08/ether-sale-a-statistical-overview/.
92 *Coinmarketcap*, Bitcoin Chart, https://coinmarketcap.com/currencies/bitcoin/#charts.
93 Based on *Sillaber*, lecture on cryptocurrencies at the FMA (2018).

payout matrix: if the bet is correct, the stake is doubled; if incorrect, it is reduced to zero, and this programme would be processed using Ether; one would therefore bet Ether in this decentralised casino.[94] Even large-scale projects, such as those by Microsoft, were previously primarily processed on the Ethereum blockchain.[95] Ethereum also exhibits significantly better scalability than Bitcoin,[96] although the complexity of its programmability has in the past[97] led to security vulnerabilities in the Ethereum blockchain. The so-called 'DAO hack' (Decentralised Autonomous Organisations[98]), in which Ether worth approximately 70 million US dollars at the time was stolen,[99] led to two significant consequences: on the one hand – although the error was to be found in the implemented programme and not in the Ethereum blockchain itself[100] – an update (a so-called 'fork') of the Ethereum blockchain was decided upon and implemented[101]; and secondly, the US SEC classified the DAO as a security under financial market law.[102] Ether itself was also subject to a comprehensive review to determine whether it falls under US securities law.[103] The conclusion was – in my view, at any rate, correctly – that it did not.[104] It should be noted at this point that the American understanding of securities is not identical to the European concept of securities. The European concept of securities is generally regarded as narrower, particularly as the American concept is shaped by case law and is therefore more adaptable.

A key feature of the Ethereum blockchain is so-called 'smart contracts'. Put simply, a program code is used on the Ethereum blockchain to digitally represent a contract. Using an 'if-then' pattern, the system checks whether all the conditions for execution are met and, if so, the contract is executed automatically – neither party can prevent this. Should the necessary conditions not be met, the Ether used is returned.[105]

94 As outlined in Chapter 2.4, various proprietary tokens were issued as part of ICOs, which may have similar functions and thus, in some cases, had a more specific use case. In this instance, for example, a specific 'casino token' would be issued and utilised.

95 See *Microsoft Azure*, Blockchain as a Service, https://azure.microsoft.com/en-us/blog/ethereum-blockchain-as-a-service-now-on-azure/.

96 12 seconds per block (ETH) instead of 10 minutes (BTC), which corresponds to a significantly higher transaction rate.

97 See *Medium,* The Story of the DAO – its history and consequences, https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee. See *Ethereum Blog*, Security Alert – Ethereum, https://blog.ethereum.org/2019/01/15/security-alert-ethereum-constantinople-postponement/.

98 The key characteristics are already apparent from the name: it is a decentralised programme, which is generally structured on a grassroots democratic basis (with voting rights, for example, determined by the number of tokens held) and where anonymous participation is possible. Ultimately, this means that – in the absence of a central issuing authority and any means of exerting influence – there is no single entity. This poses major challenges for legal scholarship, such as against whom a lawsuit should be brought, who is liable or responsible for the actions, etc. For details on the DAO and its classification under company law, see: *Thöni*, 'Die DAO (Decentralized Autonomous Organization) – eine Gesellschaft sui generis?', GES 2018, 371ff.

99 For further details, see *Medium*, op. cit., p.https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee

100 Put simply, a payment could be triggered multiple times within a contract.

101 See, for example, *Coincodex*, The DAO hack – what happened and what followed https://coincodex.com/article/50/the-dao-hack-what-happened-and-what-followed/.

102 *SEC*, Press Release on DAO, https://www.sec.gov/news/press-release/2017-131.

103 *Ethereumworldnews*, SEC clarifies comments on ETH were not binding, https://ethereumworldnews.com/sec-chair-man-clarifies-the-comments-on-ethereum-eth-were-non-binding-and-not-the-law/.

104 *BTC Echo*, SEC halts investigation into Ethereum, 19 June 2024, https://www. btc-echo.de/schlagzeilen/sec-stoppt-ermittlungen-gegen-ethereum-186762/.

105 For an overview: *Futurezone*, What exactly are smart contracts?, https://futurezone.at/digital-life/blockchain-was-sind-eigentlich-smart-contracts/293.031.908.

However, this essentially requires that both the monetary system – which could in principle be covered by crypto-assets – and the goods or services to be purchased are linked to the blockchain. Two brief examples will illustrate this: a company offers digital services, such as a digital subscription. This digital subscription can, for example, be used with the 'subscription token'. The subscription token is offered via a smart contract; anyone who a) transfers sufficient Ether to the specified address (this automatically triggers the smart contract) and b) meets the requirements will have the subscription token credited to their wallet automatically. If insufficient funds have been transferred or other requirements are not met, the user receives their Ether back (minus transaction fees). If, in the future, property is also listed on a blockchain-like/compatible database,[106] fully automated settlement of a property transaction would also be possible. The entry in the land register could be made within a few minutes. The potential applications for this technology are essentially unlimited. Examples include securities settlement, purchase contracts of all kinds, tendering procedures, automated regulatory reporting for business transactions, political elections and much more. Although this technology will only play a role in everyday life in the future – particularly as there are currently simply too few assets represented on the blockchain – its relevance should notbe underestimated. The fast and, above all, automated settlement resolves the issues of step-by-step transactions and advance performance.[107] Smart contracts gained significant relevance when the number of ICOs rose massively and they established themselves as a new form of financing. All of this will be discussed in the next chapter.

Since the first edition, the Ethereum ecosystem has also evolved significantly. Of particular note is the transition from the original 'proof-of-work' consensus mechanism to the significantly more energy-efficient 'proof-of-stake' procedure as part of the so-called Ethereum Merge, which was successfully completed in September 2022.[108] This not only drastically reduced the network's energy consumption but also laid the foundation for further scaling measures. Similar to Bitcoin, additional 'simplifications' ('Layer 2') have emerged.[109]

Furthermore, Ethereum has established itself as the preferred infrastructure for a wide range of decentralised applications (dApps)[110] – whether in the field of DeFi (Decentralised Finance),[111] NFTs (Non-Fungible Tokens)[112] or the tokenisation of real-world assets ("Real World Assets")[113].

106 See also *BTC Echo*, Sweden now officially uses blockchain for land registry entries, https://www.btc-echo.de/schweden-nutzt-jetzt-offiziell-die-blockchain-fuer-grundbucheintragungen/.

107 For further details on legal issues relating to this topic: *Smets/Kapeller*, Smart Contracts: Contract Formation and Liability, ÖJZ 2018/39.

108 *Ethereum.org*, The Merge, https://ethereum.org/en/roadmap/merge/; *BTC Echo Academy*, https://www.btc-echo.de/ academy/library/ethereum-merge/.

109 Such as Optimistic Rollups or Sidechains; *OSL*, What are Ethereum Layer-2 […], https://osl.com/academy/article/what-are-ethereum-layer-2-blockchains-and-how-do-they-work.

110 For a detailed explanation of the term, see *Fireblocks*, Glossary – dApps, https://www.fireblocks.com/glossary/decentralized-applications/.

111 For more details, see *Lewis*, Understanding Decentralised Finance (2023).

112 For the definition and also the distinction from MiCAR: *FMA*, Non-Fungible Tokens, https://www.fma.gv.at/querschnittsthemen/markets-in-crypto-assets-regulation-micar/non-fungible-tokens-nfts/.

113 See, e.g., *Coinbase*: What are real-world assets?, https://www.coinbase.com/de/learn/crypto-glossary/what-are-real-world-assets-rwa.

These developments show that Ethereum has outgrown its original vision as a pure smart contract platform and has evolved into a dynamic ecosystem. The comprehensive possibilities offered by Ethereum have significantly shaped the discussion on digital infrastructure, governance models and the role of decentralised systems in the modern financial world, and even the discussion on the settlement of traditional financial market transactions via 'classic blockchain'[114].

In summary, it can be stated that the Bitcoin blockchain, as a pure database, digitally represents crypto-assets, whilst the Ethereum network represents a broader-based development, as programmes and applications on the blockchain can be created by any user, thereby placing much greater emphasis on the ecosystem concept and programmability.

2.4 Initial Coin Offerings (ICOs)

Smart contracts in their general form were already described in Chapter 2.3; here, however, the specific features of smart contracts in ICOs will be outlined. As already mentioned, the term 'Initial Coin Offering' *(ICO)* plays a central role in this book. With the help of 'smart contracts' – a program code that executes agreed obligations fully automatically when certain factors ('triggers') are met –[115] existing crypto-assets are collected as funding and new tokens are issued.[116] The new tokens are generally linked to a specific company or project. Regulatory authorities rightly point out that tokens vary in design and therefore no general classifications can be made; rather, a case-by-case assessment is required.[117] Technically, ICOs are frequently conducted on the Ethereum blockchain (e.g. ERC-20 tokens).[118] These tokens newly created via ICOs are often grouped under the term 'altcoins'.[119]

As already mentioned, a large majority of ICOs were based on the Ethereum platform; earlier analyses estimated that this accounted for more than three-quarters of projects.[120] Recently, however, a wide variety of other blockchains have also been utilised.[121] ICOs are primarily used for the purpose of financing business models/ideas.[122] The term ICO is modelled on Initial Public Offerings (IPOs) – partly due to their similar structure and primary financing purpose. As with IPOs, an upper limit is usually set beyond which no further funds are accepted ("hard Cap"); in some cases, minimum funding thresholds or

114 This refers to an 'open-source' and 'permissionless' blockchain, for example using Proof of Stake, rather than a specially developed blockchain.

115 For a detailed discussion of smart contracts, see, for example, *Szabo*, Formalising and securing relationships on public networks, https://ojphi.org/ojs/index.php/fm/article/view/548/469; *Christidis et al*, Blockchains and Smart Contracts for the Internet of Things, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7467408.

116 See also *FMA*, What is an ICO? op. cit.

117 See, e.g., *FMA*, What is an ICO? op. cit.

118 For more on this term, see *BTC Echo*, What is an ERC-20 token?, https://www.btc-echo.de/tutorial/was-ist-ein-erc-20-token/. For a detailed account, see *Github*, OpenSource on the ERC-20 standard, https://github.com/ethereum/EIPs/blob/ma-ster/EIPS/eip-20.md.

119 For example, *Investopedia*, Definition – Altcoin, https://www.investopedia.com/terms/a/altcoin.asp. However, the term is also used in different ways; see, for example, https://blockchainwelt.de/altcoin-definition-und-uebersicht/.

120 *Ernst & Young*, Research on ICO, 19; https://www.ey.com/Publication/vwLUAssets/ey-research-initial-coin-offerings-icos/$File/ey-research-initial-coin-offerings-icos.pdf.

121 Such as Solana or Polkadot; for an overview, see for example *BlockchainX,* https://medium.com/@blockchainx.tech/ top-5-best-blockchain-networks-to-build-an-ico-platform-on-d5c56d7d615f#:~:text=1.,contracts%20powered%20 by%20predefined%20conditions.

122 See, for example, *Investopedia*, Initial Coin Offering – Definition, https://www.investopedia.com/terms/i/initial-coin-offe-ring-ico.asp.