Analysis of possible investment in other asset classes: Part I: Digital assets

Contents

1. BITCOIN – AN INTRODUCTION

Bitcoin is the first and most well-known digital asset for making secure transactions and storing value. It is therefore often referred to as a digital currency. However, it is important to emphasise from the outset that central bank digital currencies (CBDCs) may have little or nothing in common with bitcoin or the technologies on which it is based.

Creation of bitcoin: 2008

Bitcoin's security is founded on cryptographic theory and the algorithms derived from it.[1] The core concept was created in 2008 by a developer (or group of developers) using the pseudonym Satoshi Nakamoto.[2] The system itself was launched with the mining of the "genesis block" in 2009. The declared aim of creating bitcoin was to enable transactions to be made without the involvement of financial institutions or other intermediaries. To this day, bitcoin is regarded as an alternative to traditional currencies – one that is resistant to regulation, sanctions and other government or regulatory restrictions, and to inflation (the number of bitcoins will be finite, leading to constant deflation), and one that offers a high degree of pseudonymity.

What is blockchain?

The bitcoin ecosystem is built on a decentralised network of nodes forming what is known as the blockchain. However, the same term is also used to refer to the data structure – the chain of blocks – maintained by the nodes in this network. In practice, this ambiguity is not an issue – the term blockchain is used in both senses: as the computer network whose nodes maintain the blockchain, and as the chain itself, which contains records of all transactions executed.

Bitcoin and blockchain are considered a permissionless system, meaning they are open to anyone. Participation is not subject to approval; anyone can connect to the network, whether as a user or as a node operator. Likewise, individual transactions are not authorised by any central authority but are validated automatically according to the rules of the protocol.

The protocol: the core of bitcoin

The protocol forms the fundamental basis of bitcoin. It is described directly in the source code (known as Bitcoin Core, see https://github.com/bitcoin/bitcoin) and defines a wide range of rules:[3]

- the format of transactions (structure of individual fields, electronic signature requirements, verification methods),
- block creation (structure, maximum size, timestamp, ordering),
- confirmation rules (mining, its difficulty, etc.),
- consensus (how nodes agree on the "correct" state of the blockchain),
- network communication specifications (e.g. encryption algorithms),
- economic aspects (mining rewards, halving, maximum number of bitcoins).

The purpose of this analysis is not to describe all the theoretical and technical details of how bitcoin works. To aid understanding, a brief glossary is provided in Appendix 1. We generally try to keep the text in a form that can be understood by someone who does not have a detailed knowledge of the theoretical foundations of these technologies. A wide range of materials

1 The SHA-256 hash function, digital signatures based on elliptic curves, etc.

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

3 A structured description of the protocol, history and principles are given in the Bitcoin Wiki – https://en.bitcoin.it/wiki/Main_Page

that explain the topic at varying levels of expertise and detail are freely available.[4]

Bitcoin – belief and the determinants of its value and existence

Perceptions of bitcoin differ in practice, ranging from controversy to opportunity. How should we view bitcoin in the reserves management context? Unless it is entirely rejected on principle or for other reasons, bitcoin can be regarded as having a marketable value (i.e. there is a market and a price) determined by the belief that (i) it will continue to exist, (ii) its price will increase, and (iii) it can be used in other transactions, i.e. someone else will accept bitcoins in the belief that they will be able to use them again.

Bitcoin is no one's liability. It comes into existence as the output of a "production" process. The technology used and the associated costs can be viewed as a form of liability borne by the producers.

This belief – which also underpins fiat currencies – is not easy to assess in terms of existence (default risk), price stability (market risk) and operational risks (custody, legal framework, etc.). There is no comprehensive equivalent to bitcoin; however, equivalents can be found for some of its attributes, such as uniqueness, appeal, popularity, functionality and independence.

The history of the bitcoin market is very short

One limitation of bitcoin is its relatively short history. All the arguments *for* it refer back to what has – or has not – happened during this limited period. This short track record suggests that the current price of bitcoin is likely far from final (it may yet go up or down). This effect is reinforced by the fact that the system is closed: bitcoins are not consumed (although some are gradually lost), and one day, no more will be created.

Structure of the report

This report is structured into several sections. Section 2 gives a brief account of the past and present of the bitcoin market. In section 3, we describe types of potential investment. Section 4 deals with the simplest aspect of the issue, namely the statistical analysis of the benefits and risk parameters of bitcoin. Everything that follows is much more complex and, regrettably, the answers to the questions asked are often not clear-cut. Section 5 contains an analysis of whether and how such an investment could be made in the CNB's environment. Section 6 discusses the option of including bitcoin in the international reserves, along with related theoretical and practical issues. Any potential investment in bitcoin entails a whole range of risks that do not exist in the case of "conventional" asset classes. Two external studies were therefore commissioned to analyse these risks. In section 7, we summarise the results of these studies and attempt to answer the most difficult and most frequently asked questions connected with bitcoin. In the appendix, we present a short glossary explaining the key terms used.

4 Official website: https://bitcoin.org/en/how-it-works,
Andreas M. Antonopoulos – *Mastering bitcoin*,
https://github.com/bitcoinbook/bitcoinbook/blob/develop/BOOK.md,
bitcoin on Investopedia, https://www.investopedia.com/terms/b/bitcoin.asp

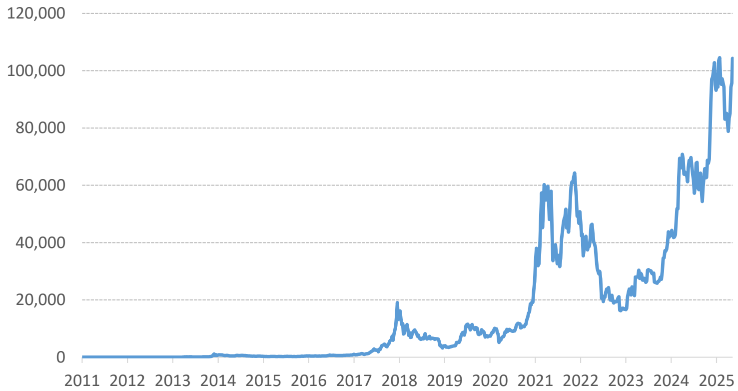
2. A DESCRIPTION OF THE BITCOIN MARKET

A brief history of the bitcoin market

After the genesis block was mined, bitcoin initially had no commercial value and was used primarily for experimental purposes. The first commercial transaction is considered to be the purchase of two pizzas for 10,000 BTC on 22 May 2010.[5] Soon afterwards, the first exchange (bitcoinmarket.com) was launched, with one bitcoin trading at $0.003. In the following years, bitcoin trading expanded and new exchanges sprang up. These included Mt. Gox, which became the dominant trading venue. Its collapse in 2014 ushered in a period of stagnation for bitcoin. The market revived in 2017, when bitcoin reached $20,000 for the first time at the year-end. In 2020–2021, the first major players (e.g. Tesla and MicroStrategy) entered the market and the first bitcoin ETFs were launched. In 2021, El Salvador adopted bitcoin as legal tender.[6] The market continued to experience huge volatility, with new highs regularly followed by sharp drops. However, the turning points (both the temporary lows and the new record highs) seemed to be rising steadily over time. Following the collapse of FTX in November 2022, bitcoin fell below $16,000. Increasing efforts by financial regulators to establish rules for the crypto market also kept the price down temporarily. None of this, however, prevented a restoration of confidence and a renewed rise in bitcoin's popularity in 2024 and 2025. The launch of bitcoin ETFs in the USA no doubt played a very positive role.

Chart 1-1

Bitcoin (USD)



Source: Bloomberg; chart: CNB

Summary of bitcoin's current position:

Bitcoin has become an alternative store of value rather than a means of payment

Bitcoin has established itself as an alternative digital asset, one which some investors view similarly to gold – as a store of value in times of uncertainty. Despite remaining highly volatile, it has begun to feature in institutional portfolios to a limited extent. The first regulated bitcoin ETFs have been created in some jurisdictions. Bitcoin's decentralised nature, limited supply and independence from central banks make it an instrument sought by some investors as a hedge against inflation and geopolitical instability. On the

5 Bitcoin Pizza Day – https://trakx.io/resources/insights/bitcoin-pizza-day/

6 El Salvador amended its "Bitcoin Law" at the end of January 2025. The amendment removes the obligation to accept bitcoin – for example, merchants are no longer required to accept it as payment. Bitcoin is no longer used as a currency in public transactions, meaning it cannot be used to pay taxes or settle government debts. While it remains "legal tender" in legislative terms, this status is now symbolic rather than mandatory.

other hand, it has not yet become a widely used means of payment, and its role in this regard appears to be weakening. Despite the existence of various modifications[7] that facilitate payments by bitcoin, this function is increasingly being fulfilled by stablecoins. Continued efforts to impose various regulatory restrictions cannot be ruled out. Overall, bitcoin is now seen more as a strategic asset than as a conventional means of payment.

2.1 Bitcoin market infrastructure

In many respects, bitcoin's market infrastructure resembles that of traditional financial markets. However, it also exhibits fundamental differences stemming from its decentralised nature.

Decentralised nature

Bitcoin does not have a central clearing or issuing institution, nor is there any central bank or other authority that manages payments or controls the quantity of bitcoin in circulation. All transactions take place directly on the blockchain, where they are verified by participants in the bitcoin network – miners – using the proof-of-work mechanism. This represents a fundamental distinction from conventional currencies, which rely on a central bank and a network of banking payment systems.

Exchanges and trading platforms

Instead of traditional foreign exchange markets, bitcoin operates through a network of crypto exchanges (e.g. Binance, Coinbase and Kraken), OTC desks and decentralised exchanges (DEXs). These platforms provide liquidity and facilitate price discovery. Unlike the traditional FX market, where liquidity is concentrated and regulated, bitcoin's liquidity is fragmented across hundreds of platforms of varying quality.

Custody and clearing

For traditional currencies, the central bank plays a central role as the clearing institution. In the case of bitcoin, custody and settlement are delegated to private entities: exchanges, specialised custodians or individual users who hold their own private keys.

Liquidity

Bitcoin is by far the most liquid cryptocurrency. Daily spot trading volumes run to tens of billions of US dollars, placing it on par with smaller national currencies. However, it still lags significantly behind the major currency pairs (USD/EUR and USD/JPY), where daily volumes exceed trillions of dollars. Bitcoin's liquidity allows for trades in the hundreds of millions of dollars, but large transactions still have a greater price impact than in FX markets.

Bitcoin's market infrastructure is built on a decentralised blockchain and a network of private exchanges and custodians, whereas traditional currencies rely on a centrally managed infrastructure, often linked to central banks. In terms of liquidity, bitcoin is the most developed digital asset, but it remains far from comparable to the world's leading currencies.

It is worth noting that there are numerous projects in which central banks – as well as private institutions – are using tokenisation and blockchain. Notable examples include the BIS/IIF Project Agorá, which aims to enhance cross-border payments,[8] and the ECB's Pontes and Appia projects, which focus on linking distributed ledgers and the Target2 system.[9]

7 For example, the second-layer Lightning Network enables fast and cheap transactions.

8 https://www.bis.org/about/bisih/topics/fmis/agora.htm

9 https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr250701~f4a98dd9dc.en.html

2.2 The bitcoin derivatives market

The derivatives market is already highly developed and is most often organised on exchanges

The bitcoin derivatives market is now highly developed, offering instruments comparable to those found in traditional financial markets. The most significant are futures contracts, which are traded both on regulated markets (such as the CME in the USA) and on specialised exchanges (Binance, OKX, Bybit). These contracts enable both hedging against price fluctuations and building of exposure to bitcoin price movements, and form the backbone of institutional bitcoin trading. Even more popular are "perpetual futures" (or perps) – contracts without an expiry date. Thanks to their high liquidity, they are currently the most widely used bitcoin derivative.

But OTC derivatives also exist

There are also forwards traded bilaterally on the OTC market. These are often used to hedge miners' or funds' future revenues. Options – in particular vanilla calls and puts – are traded on the CME and specialised exchanges such as Deribit, allowing complex strategies to be constructed.

There is no repo market in the classic sense, but an alternative is in operation

As for instruments akin to repurchase agreements, there is no classic standardised "repo market" for bitcoin. Nevertheless, bitcoin lending and borrowing exists, with institutions or investors borrowing bitcoins against collateral (typically stablecoins or fiat currency). In principle, such transactions are very similar to repos, although they involve bilateral or exchange-based loans rather than constituting a unified interbank market.

Deliverable forwards are another specific category of transactions. Used primarily in the OTC market, they allow participants to agree a fixed price and delivery date for bitcoin, and are often employed as a hedging tool.

Overall, the bitcoin derivatives market is diverse – ranging from liquid futures and perps on exchanges, through options, to specialised forwards and repo-like lending transactions. Each instrument serves a different purpose: speculation, hedging, financing or arbitrage.

That said, it remains true that the bitcoin derivatives market is significantly smaller and less liquid than traditional currency derivatives markets.

3. FORMS OF INVESTMENT

Direct investment

For most investors, the primary way to invest in bitcoin is *direct investment*. Transactions are conducted on exchanges such as Binance, Coinbase and Kraken. However, the OTC market has also expanded in recent years (to include standard CNB counterparties such as Goldman Sachs, JP Morgan, Morgan Stanley, Standard Chartered and Nomura). It offers a more suitable platform for larger-scale trades. Brokers specialising in digital assets have also emerged (Cumberland/DRW, Galaxy Digital, Jump Trading, B2C2); the CNB typically does not use brokers for trading, but this is its own decision and can be reviewed if necessary.

Self-custody versus external custody

In the case of direct investment, the key question is how to store bitcoins. Investors can choose to hold bitcoins themselves (self-custody) or through other institutions (exchanges or traditional or specialised custodians).

For self-custody, retail investors typically use software wallets for small holdings. In the case of the CNB, however, this solution can be ruled out for security reasons. For larger holdings, specialised hardware devices are available – typically hardware security modules (HSMs), which allow for secure management of private keys (see section 5.2 for details).

Direct investment can also be combined with external custody services. These are now offered by a wide range of traditional institutions, including BNY, Fidelity Digital Assets, State Street Digital and ZKB. There are also new institutions specialising solely in digital assets, most notably Coinbase Custody. External custody offers a number of advantages, as described in detail in section 5.3.

Indirect investment: ETFs (more expensive), derivatives

Indirect investment in bitcoin is also possible. The main option here is exchange-traded funds (ETFs). These are a traditional type of instrument that the CNB already uses in the management of its equity portfolio. It is therefore ready to implement this alternative immediately. The leading funds today are BlackRock's iShares Bitcoin Trust (IBIT) and Grayscale Bitcoin Trust (GBTC). The main drawback of using ETFs is the associated fees: GBTC charges 1.5% and IBIT 0.25%. For larger portfolios, these fees exceed the potential costs of external custody services.

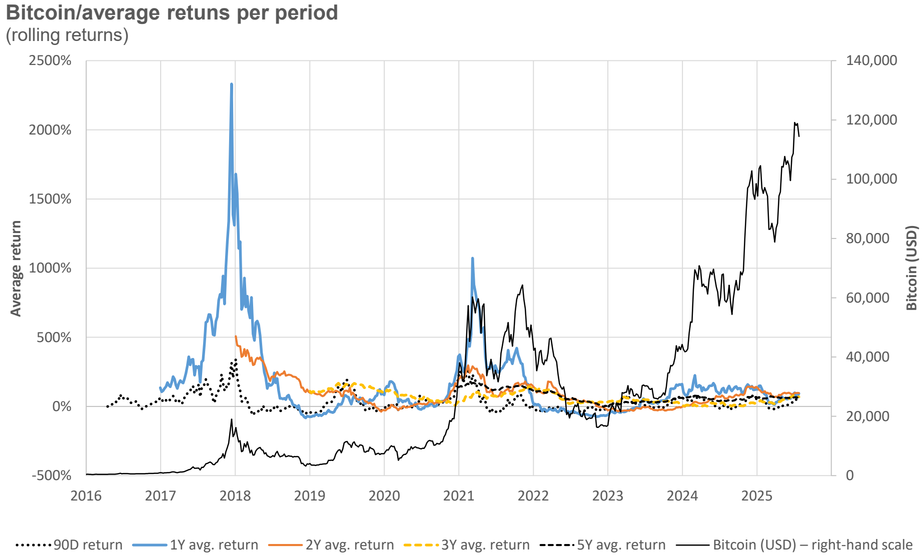
Other indirect options include derivatives (e.g. options and futures) traded on specialised exchanges like Binance, Bybit and Deribit. Some banks now also offer total return swaps on bitcoin. For various reasons – often regulatory – some investors choose exposures to companies that hold large amounts of bitcoin on their balance sheets and whose share prices therefore tend to track the price of bitcoin (most notably Strategy – formerly MicroStrategy).[10]

4. RISK-RETURN CHARACTERISTICS

The returns and volatility associated with bitcoin defy comparison with conventional assets. Given its rise in value from just 0.3 cents (!) at the outset to current levels above $100,000 – an increase of "millions of per cent" – great caution is required when working with the relevant data. More than with any other asset, the warning applies here that past performance is no guarantee of future results. For this reason, in the following text we present bitcoin's historical returns for illustrative purposes only, and we emphasise that they should not be treated as expected future returns. This pattern is typical of most emerging markets and industries – the initial boom is unlikely to be repeated. The market is more likely to stabilise, with both volatility and performance declining.

10 However, the shares of Strategy (ticker: MSTR) show even greater volatility than bitcoin itself.

Chart 1-2



Source: Bloomberg data; calculation and chart: CNB

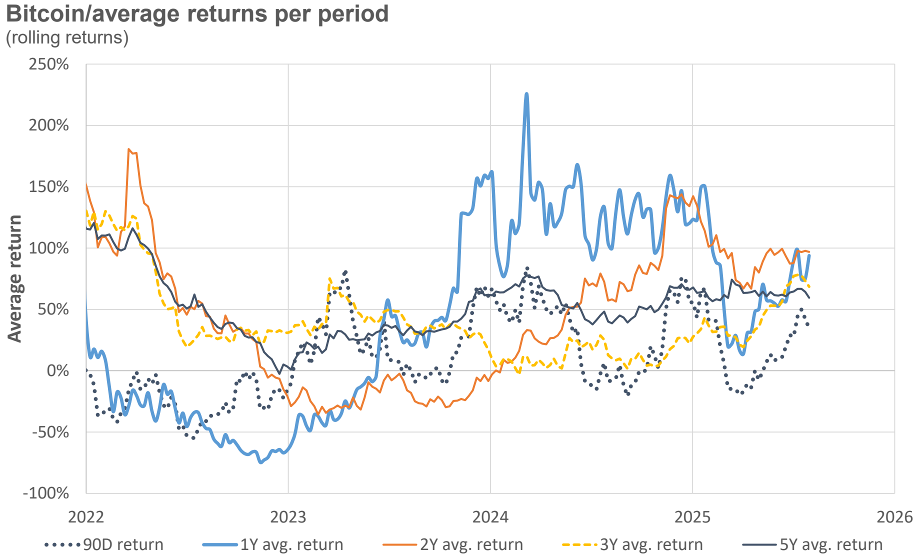
Growth in BTC of thousands of per cent – a one-off event connected with very low prices

As shown in the chart above, the annual changes in the price of bitcoin exceeded 2,000% in 2017–2018. This was because the price was rising from very low levels (at the end of 2016, bitcoin was trading below $1,000). We have therefore deliberately excluded this period from our analysis and instead focus on the post-2018 era.

Rolling returns: Three- and five-year periods since 2020 in positive figures only

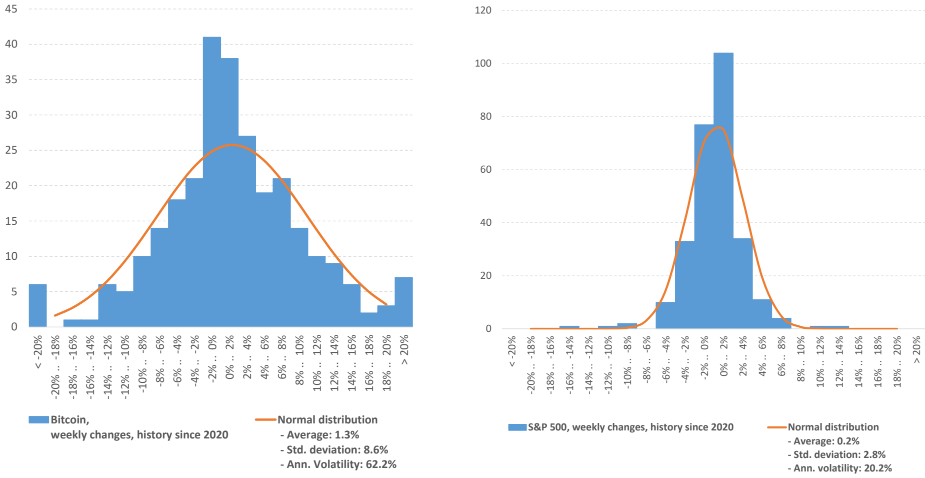
The chart below presents the same data, but only from 2022 on. Notably, while the returns associated with holding bitcoin for short time scales (90 days, one year) have been negative for quite long periods, all average returns linked with the three- and five-year periods have been positive. In this respect, bitcoin's price behaviour resembles that of equities, where the probability of negative returns also decreases significantly with longer periods.

Chart 1-3

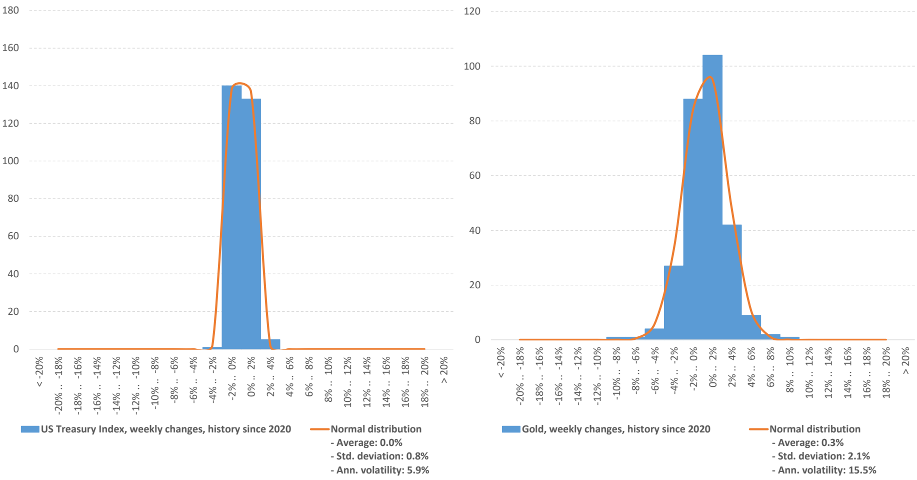


Source: Bloomberg data; calculation and chart: CNB

Charts 1-4 and 1-5 – histograms of weekly changes



Charts 1-6 and 1-7 – histograms of weekly changes



Source: Bloomberg, S&P and ICE data; calculation and chart: CNB

We also conducted a more theoretical study of the statistical properties of bitcoin prices. Perhaps the most interesting findings emerged from analysing the shape of the return distribution. We hypothesised that the daily changes in the price of bitcoin follow a stable ("fat tail") distribution, and compared this with the performance of the S&P 500 index, also assuming a stable distribution. In the vast majority of years between 2011 and 2025, our hypothesis regarding the shape of the distribution was not rejected for either bitcoin or equities. Furthermore, we found that bitcoin's statistical properties have been very similar to those of equities in recent years, although the scale of its gains and losses have of course been much larger.

4.1 Volatility

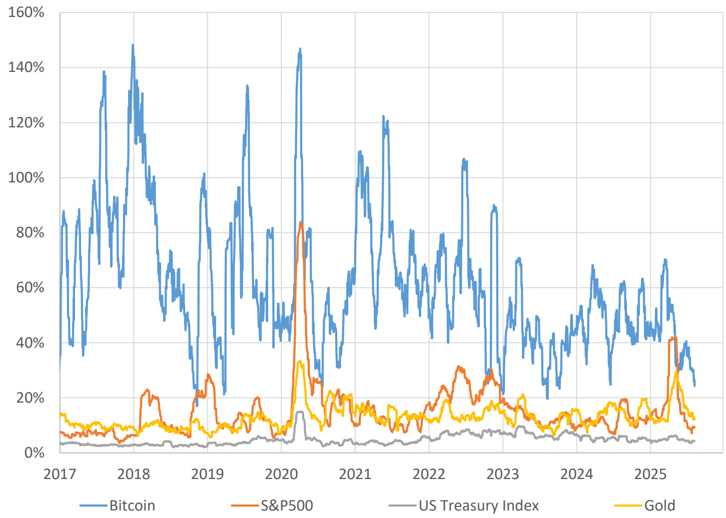
High but not extreme volatility

As repeatedly mentioned, bitcoin is an asset characterised by very high price volatility. The histograms above show the frequency of weekly price changes for bitcoin, the S&P 500 equity index, US government bonds (US Treasury Index G0Q0) and gold over the past five years (since January 2020). This period therefore covers both the onset of the Covid-19 pandemic and the beginning of the war in Ukraine. As the chart illustrates – and as expected – bitcoin was the most volatile of these asset classes during this period. In annual terms, bitcoin's volatility reached 62%, compared to approximately 20% for equities, 16% for gold and just 6% for bonds. In this respect, there are no major surprises. However, it is worth noting that bitcoin's volatility is not an order of magnitude or more higher than that of other assets, as one might assume from price charts alone. The histograms also clearly show that bitcoin's return distribution deviates significantly from a normal distribution. While the probability of extreme fluctuations – positive or negative – is very low for other assets, in the case of bitcoin, it actually increases with the size of the fluctuation. It can therefore be expected that "black swan" events will be more common than rare in the world of bitcoin.

An interesting detail emerges when we look at the short-term volatility, as shown in the 30-day view in Chart 1-8. The general rule still applies: bitcoin's volatility is a multiple of the volatility of equities and an order of magnitude higher than that of bonds. However, there are exceptions – for example, during the early stages of the Covid-19 pandemic and following the imposition of "reciprocal tariffs" by the US administration in April 2025, when the short-term volatility in equities and bitcoin was at similar levels. It is worth noting, though, that while periods of heightened volatility are rare for traditional assets, they have so far been the norm for bitcoin.

Chart 1-8

30D rolling volatility (annualised)

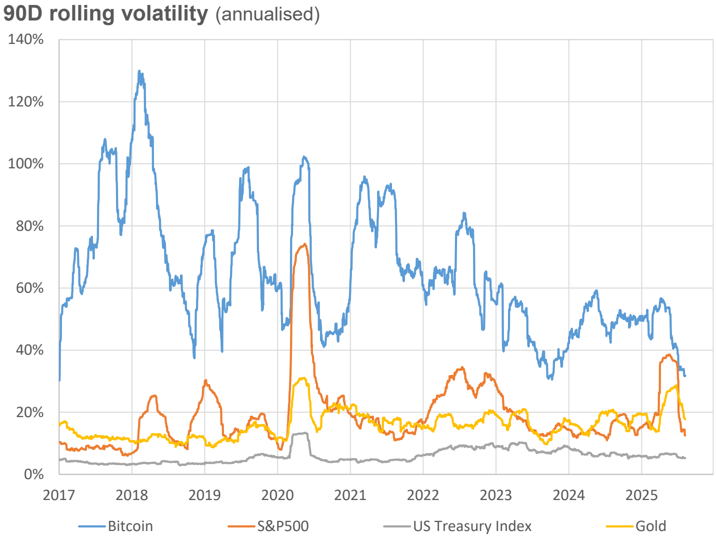


Source: Bloomberg data; CNB calculation

The short-term volatility of equities and bitcoin has been comparable during some episodes

The longer-term volatility provides an even clearer picture. The 90-day volatility view (Chart 1-9) confirms the earlier observations – while bitcoin's volatility is high, it is not orders of magnitude greater than that of other risky assets, contrary to what its astronomical prices might suggest.

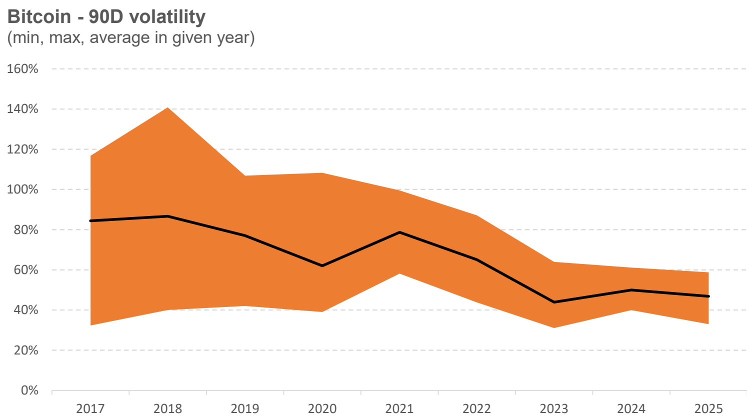
Chart 1-9



Source: Bloomberg data; CNB calculation

Looking at bitcoin's volatility over time, however, appears to support the theory that bitcoin is gradually losing some of its wildness as it gains wider acceptance. Of course, nearly 60% volatility is far from "normal" in traditional finance. Nonetheless, the trends seem to support the idea that bitcoin's extreme volatility – and the associated sharp rises and falls in its value – may now be a thing of the past. The trend shown in the following chart supports this theory.

Chart 1-10



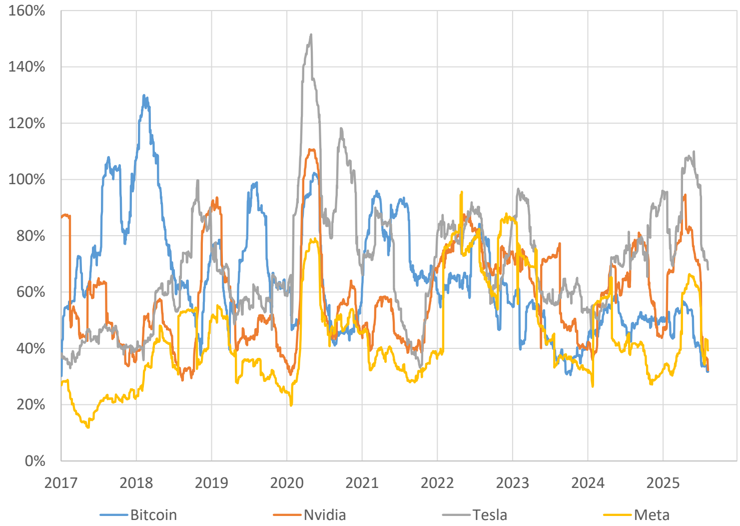
Source: Bloomberg data; calculation and chart: CNB

Bitcoin's volatility is comparable to that of tech companies

It is also interesting to compare bitcoin's volatility with that of certain technology stocks. As shown in the next chart, for most of the period under review, at least one of the (arbitrarily selected) tech stocks exhibited higher volatility than bitcoin – particularly in recent times. A likely explanation is that tech companies are subject to booms (currently AI). As previously mentioned, booms are always accompanied by increased volatility, which subsides once the innovation becomes a widely accepted standard.

Chart 1-11

90D rolling volatility (annualised)

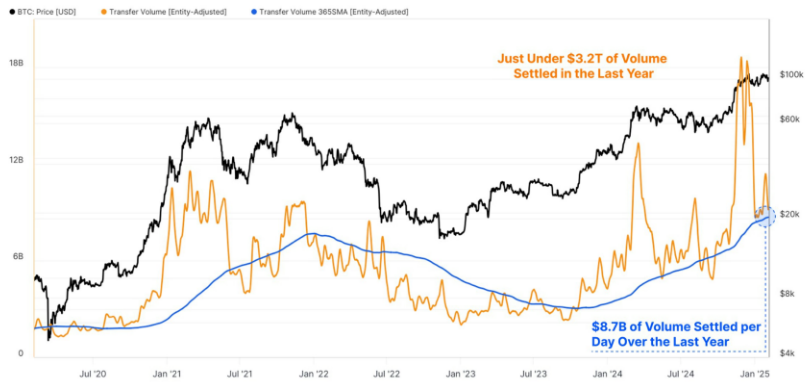


Source: Bloomberg data; calculation and chart: CNB

The high volatility in the bitcoin market reflects the relatively small size of the market (especially compared to the volumes of bonds and equities traded) and hence – due to its lower liquidity – a higher proportion of speculative transactions. It probably also reflects a persistently high share of retail investors, who are more sensitive to market developments (such investors track the market and thereby amplify market movements). It is estimated that on-chain bitcoin transactions averaged about $8.7 billion per day in 2024.[11] For comparison, daily trading volumes in Apple Inc. shares regularly exceed $3 billion.

Chart 1-12

Total Transfer Volume (Entity-Adjusted)



glassnode

Source: Bloomberg data; calculation and chart: CNB

Nevertheless, bitcoin trading volumes continue to grow steadily by many measures. This supports the theory that bitcoin's price volatility will continue to decline as trading volumes increase, due to rising liquidity.

11 Not all transactions recorded on the blockchain reflect true trading activity. For example, according to the analytics firm Glassnode, fewer than 25% of on-chain volumes represent genuine value transfers between two separate entities. https://bitcoinist.com/bitcoin-settled-3-2-economic-volume-2024

4.2 The Sharpe ratio

Bitcoin's Sharpe ratio is similar to that for equities and gold

The Sharpe ratio is frequently used to evaluate asset returns. It expresses the excess return over the risk-free rate per unit of volatility.[12] Despite its very high volatility, bitcoin's Sharpe ratio is comparable to that of other asset classes, particularly equities and gold. In other words, bitcoin's high volatility has been compensated for by higher returns to a degree similar to other risky assets. The following table summarises the Sharpe ratios for selected asset classes since the beginning of 2021.

The analysis presented in this section does not in itself constitute a reason for including or not including bitcoin or other assets in the reserves. Its purpose is simply to evaluate the excess returns bitcoin has historically offered in relation to its volatility, and to compare it on that basis with other assets.

Table 1-1

Return, volatility, Sharpe ratio

	average return [% p.a.]	average volatility [% p.a.]	Sharpe ratio
Bonds (UST 1-10Y)	0.22%	3.74%	-0.81
S&P500	14.19%	15.51%	0.71
NASDAQ	13.48%	19.32%	0.53
Russel2000	5.88%	20.36%	0.13
Gold	13.05%	13.44%	0.73
Bitcoin	50.26%	62.97%	0.75

data: Bloomberg, 01/21 - 07/25, calculation CNB

It is important to repeat the usual caveat here – as with other statistical measures, the results depend heavily on the input data, particularly the choice of observation period. This problem increases with the degree of volatility of the asset. Values calculated for periods shifted by just a few months can differ dramatically.

The Sharpe ratios are highly unstable, but to a similar degree as with other assets…

Chart 1-13 summarises the evolution of the Sharpe ratio over a rolling 12-month period. It shows the high instability of this indicator, ranging from strongly positive values above 4 to negative values approaching −2. Nevertheless, the chart broadly confirms the long-term averages shown in the table above. Bitcoin's Sharpe ratio generally tracks that of equities to a surprisingly high degree.

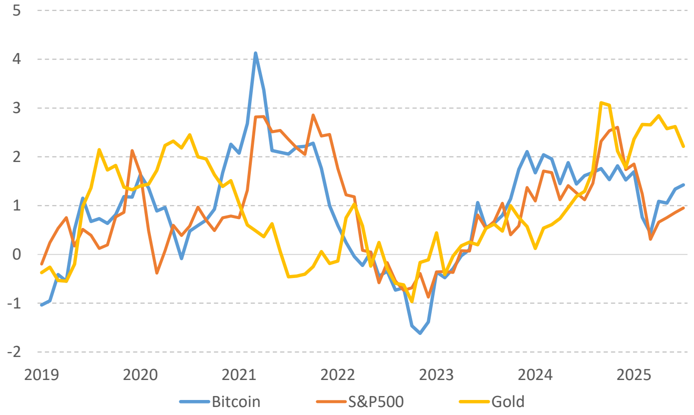
The chart also shows that the Sharpe ratios for equities and gold vary significantly as well. Therefore, bitcoin does not appear to differ from these assets in terms of this statistical measure.

—

12 The Sharpe ratio is defined as $s = \frac{r - r_f}{\sigma}$, where r is the return, r_f is the risk-free return and σ is the volatility.

Chart 1-13

Sharpe ratio / trailing 12m periods



Source: Bloomberg data; calculation and chart: CNB

4.3 Correlation with prices of other assets

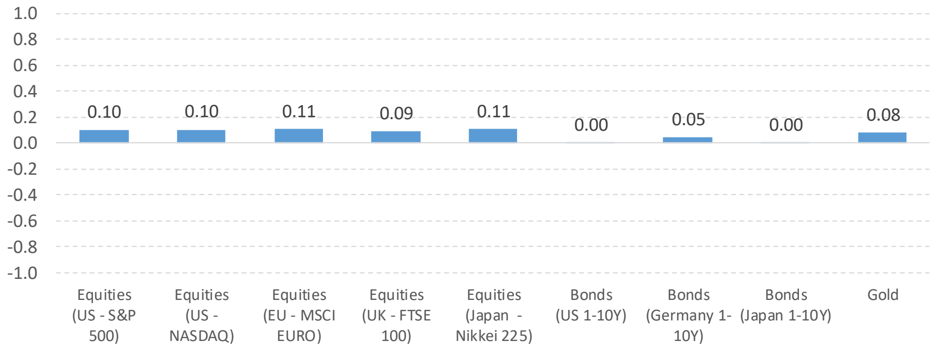
Bitcoin has a low correlation with equities and bonds

Over the longest possible time scale (i.e. since bitcoin's inception and the start of bitcoin trading in 2010/2011; see Chart 1-14), bitcoin shows near-zero coefficients of correlation with other assets.

Chart 1-14

Correlation coefficients: Bitcoin against other assets

(data 01/11 - 10/25, in local currency, frequency: weekly)



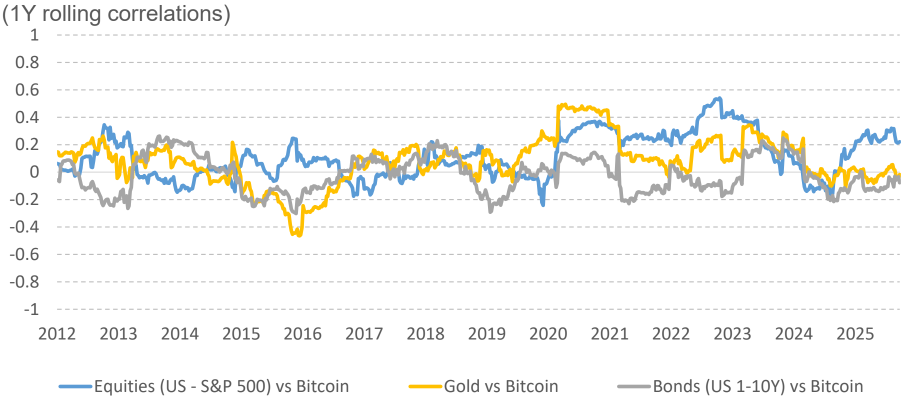
Source: Bloomberg data; CNB calculation

A closer look at shorter-term correlations (Chart 1-15, showing the history of the correlation coefficients calculated for the past year) confirms the general observation that the correlation values may fluctuate significantly, and that even for assets where a correlation is typically expected (for example, a negative correlation between bond and equity returns), it may not be perfectly stable over time.

Chart 1-15

Correlation coefficients

(1Y rolling correlations)



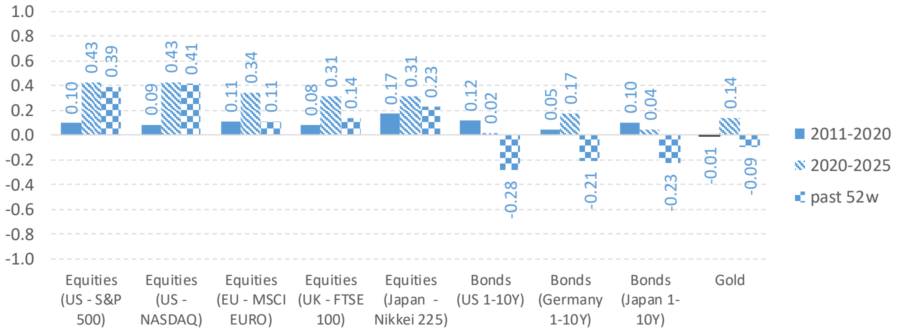
Source: Bloomberg data; CNB calculation

A change occurred after 2020: bitcoin generally tracks the prices of other risky assets

A similar pattern is observed for bitcoin – until 2020, the correlation coefficients between bitcoin and bonds/equities/gold were very close to zero (seldom above 0.2), but the situation in later years is very different. Between 2020 and 2023, bitcoin's correlation with equities never fell below 0.2, whereas during 2023 it reached levels around 0.6 and remained only slightly below that in 2025. However, the negative short-term correlation coefficients between bitcoin and bonds can probably be considered a positive signal; long periods of negative correlation appear to have continued even after 2020, with levels as low as −0.4 in some periods.

Chart 1-16

Bitcoin Correlation Across Asset Classes and Periods



Source: Bloomberg data; CNB calculation

Table 1-2 provides an overview of the annual correlation coefficients as of October 2025. The data show that the price of bitcoin over the past year has broadly followed the equity market trend (the correlation with the S&P 500 being 0.4), while its correlation with bonds – and to a lesser extent gold – has been mostly inverse.

Table 1-2

Correlation matrix

(date range 10/24 - 10/25, local currency , frequency: weekly)

	Equities (US - S&P 500)	Equities (US - NASDAQ)	Equities (EU - MSCI EURO)	Equities (UK - FTSE 100)	Equities (Canada - S&P TSX)	Equities (Japan - Nikkei 225)	Bonds (US 1-10Y)	Bonds (Germany 1-10Y)	Bonds (Canada 1-10Y)	Bonds (Japan 1-10Y)	Bitcoin	Gold
Equities (US - S&P 500)	100%	95%	29%	21%	66%	43%	-2%	-4%	8%	-29%	**39%**	-16%
Equities (US - NASDAQ)	95%	100%	19%	4%	53%	39%	-15%	-10%	-2%	-23%	**41%**	-24%
Equities (EU - MSCI EURO)	29%	19%	100%	88%	57%	68%	3%	-23%	27%	-47%	**11%**	25%
Equities (UK - FTSE 100)	21%	4%	88%	100%	65%	62%	13%	-9%	29%	-47%	**14%**	40%
Equities (Canada - S&P TSX)	66%	53%	57%	65%	100%	58%	21%	6%	37%	-38%	**27%**	32%
Equities (Japan - Nikkei 225)	43%	39%	68%	62%	58%	100%	-2%	-18%	22%	-34%	**23%**	16%
Bonds (US 1-10Y)	-2%	-15%	3%	13%	21%	-2%	100%	54%	72%	32%	**-28%**	35%
Bonds (Germany 1-10Y)	-4%	-10%	-23%	-9%	6%	-18%	54%	100%	37%	45%	**-21%**	25%
Bonds (Canada 1-10Y)	8%	-2%	27%	29%	37%	22%	72%	37%	100%	18%	**-18%**	31%
Bonds (Japan 1-10Y)	-29%	-23%	-47%	-47%	-38%	-34%	32%	45%	18%	100%	**-23%**	11%
Bitcoin	**39%**	**41%**	**11%**	**14%**	**27%**	**23%**	**-28%**	**-21%**	**-18%**	**-23%**	**100%**	**-10%**
Gold	-16%	-24%	25%	40%	32%	16%	35%	25%	31%	11%	**-10%**	100%

Source: Bloomberg data; CNB calculation

We therefore consider the following to be the key conclusions:

- from the perspective of its longer-term price history, including bitcoin in the reserve mix may offer diversification benefits due to its lower correlation coefficients,
- a change has occurred since 2020; bitcoin has shown some similarity to equity price movements, but the diversification effect remains pronounced in relation to bonds,
- surprisingly, bitcoin continues to show very low correlation with the gold price.

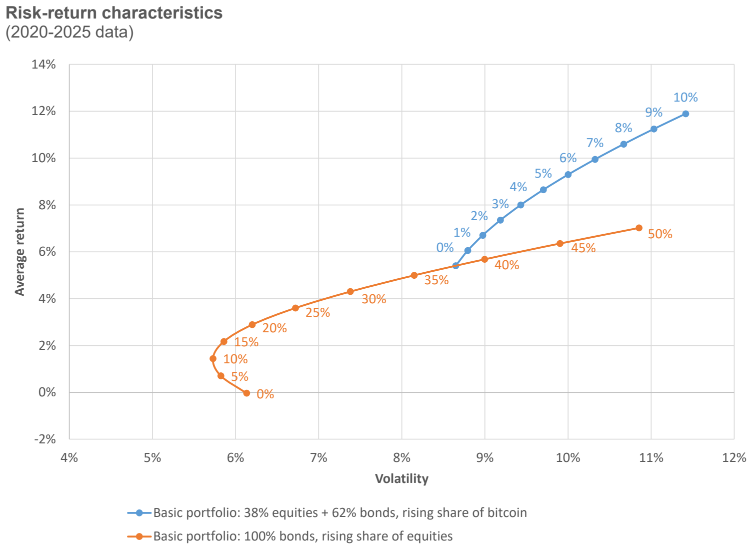
However, it remains important to bear in mind the partial unreliability of bitcoin-related statistical data, a point that has been mentioned repeatedly in the text above. In other words, past developments should not be assumed to predict future outcomes.

4.4 The effect of including bitcoin in the portfolio

Bitcoin's relatively high price volatility and its lower diversification potential observed above all after 2020 suggest that adding bitcoin to the portfolio will not have a major effect. The blue data series in the following chart is based on a stylised simple portfolio comprising 38% equities[13] (S&P 500) and 62% bonds (US Treasury Index), to which we gradually add bitcoin (with the shares of equities and bonds falling proportionately). We only analyse returns in US dollars and hence do not take into account the effects of other exchange rates.

13 Under the current conditions, a 38% share of equities in the investment tranche would correspond roughly to a 30% share of equities in the total international reserve portfolio.

Chart 1-17



Source: Bloomberg data; CNB calculation

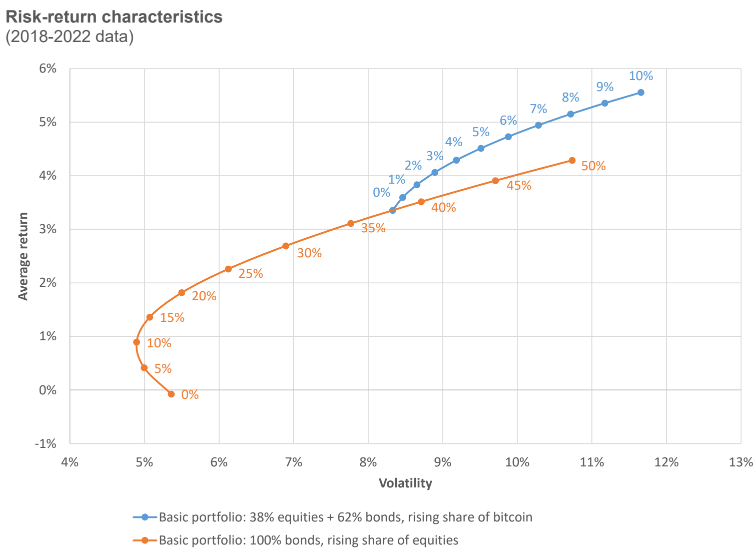
Efficient frontier

The chart confirms our expectations – there is no volume of bitcoin that, if added, would lower the overall volatility of the portfolio, regardless of periods of negative correlation between bitcoin and bonds. Despite certain statistical similarities between bitcoin and equities, it is impossible to find a portfolio structure for which the volatility decreases or at least stagnates amid rising returns, unlike in the case of equities. However, the blue bitcoin curve reveals another advantage – it is very steep. An additional unit of volatility is more than compensated for by the return (in other words, the Sharpe ratio increases). However, this merely reflects the returns recorded by bitcoin since 2020 – they were very high, averaging 65% p.a. (in the same period, equities gained only 12% p.a. and bonds hovered around zero) – as well as the gradual decline in bitcoin's volatility over time. We must emphasise, though, that it is not possible to say whether this trend is set to continue.

The following charts demonstrate how the choice of time series affects the conclusions of the above analysis. The first shows the data for 2018–2022, when bitcoin recorded only low growth (just 2.3% p.a. on average) and the second is for 2022 alone, when bitcoin fell sharply (by 64%).

Different data periods lead to different results
(danger of cherry-picking)

Chart 1-18

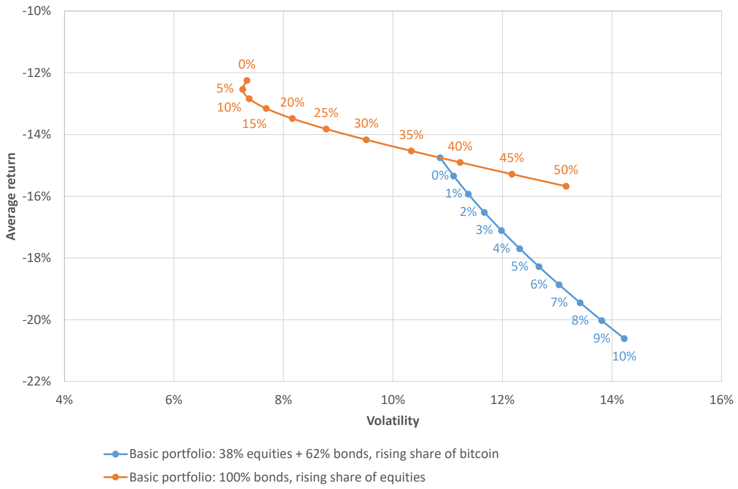


Source: Bloomberg data; CNB calculation

In 2018–2022, the blue bitcoin curve is significantly flatter – even if 10% of bitcoin is added to the portfolio, the return rises by only around 2 pp.

Chart 1-19

Risk-return characteristics
(01-12/2022 data)



Source: Bloomberg data; CNB calculation

2022 scenario:
a negative extreme that affected most assets

The 2022 scenario is extreme – including 10% of bitcoin leads to a decrease in the portfolio return to −21%. We should add, however, that almost all asset classes were in negative figures that year.

The risk of cherry-picking is high for bitcoin

For some parameters, such as expected return, it will be better to use our own estimates instead of historical data

These scenarios reveal one of the drawbacks of an approach like this – the danger of cherry-picking, i.e. choosing only those periods in which the results were "favourable" (whatever that may mean). This risk must be borne in mind in the case of bitcoin, given its fairly dramatic price history and its relatively short time series compared to other assets. This issue may be addressed, for example, by explicitly setting the assumptions entering the analysis ad hoc, i.e. by specifying, for example, that we expect bitcoin to rise by 30% p.a. (or by 20%, 40%, 80% etc.) and then considering whether the increase in portfolio volatility is compensated for by a sufficient increase in the expected return. It will clearly not be easy to make such an ad hoc expert estimate, especially for an asset whose price is purely the result of market movements and which lacks intrinsic value.

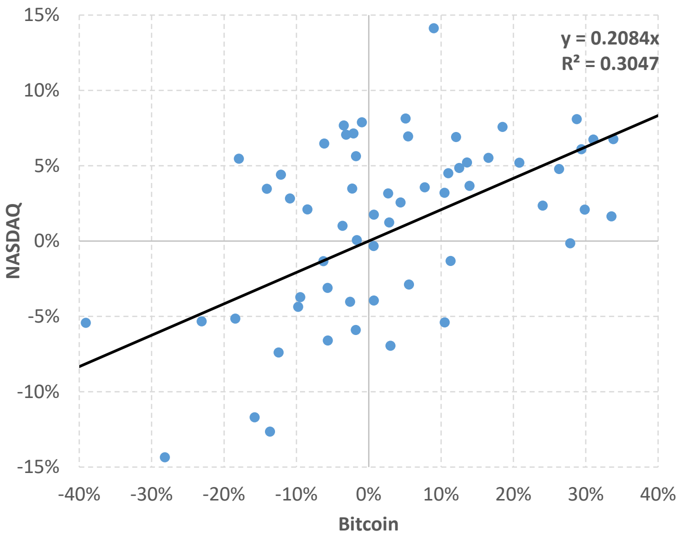
4.5 Case study – bitcoin for lower volatility?

As has been repeated several times here, the statistical properties of bitcoin deviate significantly from those of conventional assets, although they most closely resemble those of equities. What sets bitcoin apart from equities, however, is its high volatility, coupled with even higher – sometimes extreme – returns. Including it in the portfolio may yield unexpected benefits.

For the purposes of the following exercise, we selected the NASDAQ index of tech companies, which itself exhibits slightly higher volatility than the more commonly used S&P 500 index. We first examined its correlation with bitcoin. The scatter plot below confirms a strong relationship between the prices of the two assets. An R^2 of 0.3 may seem quite low, but it corresponds to a relatively high correlation coefficient of 55%. Other statistical indicators confirm a strong relationship.[14]

Chart 1-20

1M price changes: bitcoin vs NASDAQ

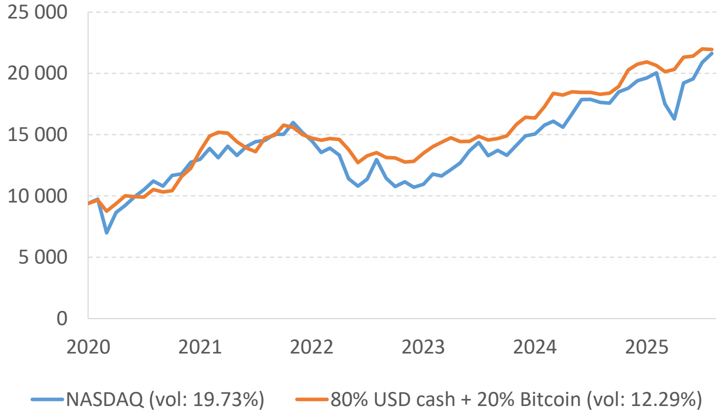


Source: Bloomberg data; CNB calculation

Let's now create a synthetic replication of the NASDAQ using a simple combination of cash dollars remunerated at risk-free money market rates and an investment in bitcoin. The shares of cash and bitcoin will be 80% and 20% respectively. The portfolio will be rebalanced to ideal weights at a monthly frequency. The following chart compares the NASDAQ with the synthetic alternative.

Chart 1-21

NASDAQ versus **80% cash + 20% BTC**



Source: Bloomberg data; CNB calculation

This calculation, in itself, is not particularly interesting – it merely confirms the obvious fact that correlated assets tend to play largely interchangeable roles in portfolios. More interesting is the comparison of the two curves in the preceding chart: the synthetic one is noticeably smoother than the original NASDAQ and appears to contain fewer major swings. Indeed, the

14 The p-value for the test of the hypothesis that the correlation coefficient is non-zero is 0.0001%.

average volatility of the NASDAQ over this period was almost 20%, while that of the synthetic substitute was only 12.3%. This is a rather surprising outcome, contrasting with our expectation that including a highly volatile asset must lead to an increase in volatility. However, this is an illusion that can be easily refuted either by means of a simple calculation,[15] or intuitively – when bitcoin generates a return, the gains are realised and converted into cash, creating a "buffer" that compensates for losses in the event of a decline in the price of bitcoin. The total return is thus smoothed.[16]

5. POTENTIAL IMPLEMENTATION AT THE CNB

5.1 Compliance with legislation

Bitcoin transactions can be made on the basis of legal authorisation Article 32 of the Act on the CNB

Bitcoin transactions can be made on the basis of Article 32 of the Act on the CNB, which stipulates that:

> The Czech National Bank shall be entitled to carry out transactions on the financial market for the performance of its tasks, in particular
>
> a) keeping accounts of banks, foreign bank branches and credit unions and accepting their deposits,
>
> b) trading in investment instruments and other securities, foreign exchange, precious metals, receivables and other assets in the form of purchases and sales, repo transactions, deposits, loans, borrowings or futures,
>
> c) conducting credit operations.

The CNB has concluded that bitcoin can generally be regarded as an asset within the meaning of subparagraph b). However, the additional condition in the opening sentence of the article, namely that the asset is traded on the financial market, is considered crucial. The term "financial market" is not defined explicitly in Czech law. However, in the CNB's opinion, the broadest definition applies, including all market subcategories, and there can be no doubt that digital assets are traded on the "financial market".

Another relevant provision of the Act on the CNB that must be mentioned is Article 35, governing the powers and activities of the CNB in the foreign exchange area. Subparagraph c) of this article stipulates that the CNB manages international reserves in gold and foreign exchange. The question is whether bitcoin can be regarded as foreign exchange. The term "foreign exchange" is not defined in Czech law. It used to be defined in the now repealed Foreign Exchange Act, under which foreign exchange was foreign currency funds, foreign securities and the rights and obligations derived from them that can be valued in terms of money (hereinafter "financial derivatives"). In the CNB's opinion, bitcoin is not a foreign currency (it does not meet the definition in the now repealed Foreign Exchange Act, nor does it conform to the general meaning of "foreign exchange" in the sense of the currency of a foreign country). Although current law does not define "foreign

---

15 $vol_{syn} = \sqrt{\omega_{BTC}^2 vol_{BTC}^2 + \omega_{USD}^2 vol_{USD}^2 + 2\omega_{BTC}\omega_{USD}\rho_{BTC-USD} vol_{BTC} vol_{USD}}$,
where $\omega_{USD} = 0.8$, $\omega_{BTC} = 0.2$, $vol_{USD} \approx 0$ and $vol_{BTC} \approx 60\%$;
the second and third terms are close to zero and can be ignored, $vol_{syn} = \sqrt{0.2^2 \cdot 0.6^2} = 12\%$

16 The "barbell principle" introduced by Nassim Taleb, who coined the term "black swan".

exchange", this does not mean that any asset can be included under that term.

To gain **practical experience** with bitcoin/blockchain, the CNB may also proceed in accordance with **Article 40 of the CNB Act**

Another, more limited possibility is offered by Article 40, paragraph 1 of which stipulates the following:

> The Czech National Bank shall be entitled to engage in investment and commercial activities insofar as is necessary to provide for its own operations.

In the CNB's opinion, this provision may be applied if the CNB wants to conduct a small-scale practical test of technologies (blockchain etc.) and procedures related to investment in bitcoin in order to obtain expertise and experience in this area. Under Article 40, bitcoin may therefore qualify as an activity carried on in order to fulfil statutory duties.

In the case of the CNB, potential bitcoin transactions can be regarded as **conforming to the Statute of the ESCB and of the ECB**

The ECB is not authorised to issue binding instructions relating to the execution of open market operations pursuant to Article 32(1) of the Act on the CNB. The area of open market operations and international reserves management, and the division of competences between the ECB and the NCB in this respect, is governed by the Statute of the ESCB and of the ECB. In this respect, the status of a non-euro area central bank differs fundamentally from that of a euro area one. The objectives in Article 2 of the Statute, i.e. primarily to maintain price stability, apply to the CNB. However, Article 3 of the Statute, which stipulates the tasks of the ESCB (among other things to define and implement monetary policy, and to hold and maintain official foreign reserves), does not apply to the CNB. The Statute of the ESCB also contains a rule similar to Article 40 of the Act on the CNB.

Direct purchases of bitcoin are therefore in accordance with both the Act on the CNB and the Statute of the ESCB and of the ECB.

Indirect investment: fully in accordance

The situation in the case of indirect investment, for example through ETFs, is absolutely clear – from the perspective of legal restrictions, there is no difference between the already traded ETF instruments linked to MBS market indices or stock indices and those whose prices are linked to bitcoin.

5.2 Possible technical solutions for self-custody

A range of solutions are available for secure self-custody of bitcoins:

- software wallets – generally considered sufficient for holding small amounts of bitcoin,
- simple USB tokens (e.g. Ledger, Coldcard, Trezor), which use various techniques to prevent the export of private keys,[17]
- hardware security modules (HSMs) – dedicated devices or computer cards used for similar purposes as USB tokens, i.e. for secure storage of private keys without the possibility of export.

A number of industry jargon terms are used that are not always applied correctly, often leading to confusion. Typically, a distinction is made between cold storage (devices or wallets completely disconnected from computer networks, or only connected occasionally) and hot wallets (wallets routinely

17 Some of these devices contain a secure element, a specialised chip that prevents private key export. Others rely on open-source cryptographic solutions (e.g. Trezor One/T). Both approaches have their critics: in the first, users rely on a "black-box" chip; in the other, there is a theoretically exploitable physical vulnerability (voltage glitching or ROM/flash memory dumping).

connected to the internet). Then there is “offline solutions”, a broader term also encompassing cold storage and sometimes used interchangeably in practice. At its core, however, the issue is not one of terminology but of solving three fundamental problems: (1) how to securely generate the private key, (2) how to store it, and (3) how to prevent its misuse.

MPC+HSM: currently considered best practice in the industry

A widely cited example of a highly secure setup today is the combination of multisignature (multisig) or MPC (multi-party computation) with an HSM device. This technically complex but highly effective solution is currently considered best practice. It typically involves several HSMs (certified to FIPS 140-2 Level 3) and MPC, usually complemented by an orchestrator to manage signing operations, along with audit and logging layers. The private key is not generated as a whole, but in parts using a distributed protocol (distributed key generation, DKG). Individual partial keys (known as shards) are created and these are then used in different HSMs. The MPC orchestrator then manages the signing process,[18] requiring a threshold number of partial signatures to be combined into a final signature – without the full key ever existing in a single instance. This solution is currently regarded as highly secure.

Air-gapped solution

If high-frequency trading is not required, the entire setup can be fully isolated from any network. Unsigned transactions (partially signed bitcoin transactions, PSBTs) are transferred via portable media (or other “air-gapped” methods) into a completely offline system, where they are signed. The signed transactions are then transferred back to the online environment and submitted to the blockchain network for processing.

Self-custody only with appropriate security; transactions are irreversible

A disadvantage of such a robust system design is the considerable financial cost associated with acquiring various specialised hardware devices. However, we must repeat the context in which the CNB would find itself when handling bitcoin, especially the risk of misuse of the CNB’s private keys in an environment of irreversible operations on the blockchain. In this regard, fraudulent transactions on the blockchain differ significantly from those on traditional financial markets – misuse is irreversible. Therefore, top-tier transaction security is an absolute priority.

Multisig as a simpler alternative?

As a simpler yet still secure alternative, a solution based purely on the multisignature (multisig) principle can be used. Unlike MPC, multisig is a native feature of the bitcoin protocol – meaning it is supported directly by the blockchain itself from the outset, not just by external applications. While it does not offer all the functionalities of MPC and HSMs, from the perspective of private key security, it is a proven method frequently used in institutional practice. Multisig also allows for the configuration of approval schemes (e.g. 2 of 3, 3 of 5), so that executing a transaction requires cooperation between multiple independent parties or devices. This significantly reduces the risk of key misuse through a single compromised point. From a financial standpoint, multisig is less costly than the robust MPC+HSM combination and may therefore offer a suitable compromise, especially in cases where the highest level of resilience is not required but security standards remain a priority.

—

18 The input transaction is passed to the orchestrator, which initiates the MPC protocol between the HSM units. Each unit calculates its “signature share”, which the orchestrator then combines into a single signature. The completed signature is attached to the transaction and sent to the bitcoin network.

5.3 External custody of bitcoin holdings

Directly traded bitcoin can also be transferred to external custodians. There are many such providers:

- **BNY Mellon**
(launched a custody platform for bitcoin and Ethereum in October 2022, mainly serving institutional clients in the USA; combines traditional securities custody with custody of digital assets);
- **Fidelity Digital Assets**
(a division of Fidelity Investments; has provided custody and trading services for BTC since 2018; strongly focused on institutional investors, hedge funds and family offices);
- **State Street Digital**
(partnership with Copper; provides technology for the custody of digital assets);
- **Nomura/Laser Digital**
(the Japanese investment bank has expanded into the digital asset space through its dedicated “Laser Digital” division; offers institutions custody of BTC and other digital assets);
- **Zürcher Kantonalbank** (ZKB)
(as of 2024, enables custody and trading of cryptocurrencies, including bitcoin);
- **DZ Bank**
(offers custody services for cryptocurrencies, including bitcoin, via a platform for institutional clients since 2023);
- **Coinbase Custody**
(a subsidiary of the Coinbase exchange specialising in the management of digital assets).

All of these companies offer custody services to institutional clients with the aim of enabling bitcoin to be held in compliance with regulatory and security requirements, similarly to traditional financial assets. Investors therefore do not need to concern themselves with the detailed security aspects of the technologies used or the potential for their misuse.

The use of external custody services offers a wide range of benefits. The services are regulated (subject to oversight by the SEC, FINMA, etc.) and the processes – including digital ones – are audited (ISAE 3000, 3402, SOC 1/2). They can be easily integrated into existing client systems. And some custodians are specifically insured against loss of digital assets (albeit to a limited extent).

Bitcoin held in external custody is bankruptcy remote

A key element of clients’ considerations regarding the security of assets held in external custody is the concept of bankruptcy remoteness, i.e. the fact that client assets do not become part of the custodian’s bankruptcy estate in the event of insolvency. International practice demonstrates that client protection is possible in this area, but only if the assets are contractually and technically ring-fenced (e.g. unique blockchain address, prohibition of disposal without consent, trust structure). A contract alone is insufficient unless accompanied by a real-world set-up that proves the digital assets are held "on the client's behalf" and not as part of the custodian's own assets.[19]

It is also important to distinguish whether balances are held in a custody account or with a broker, an exchange, etc. Only assets held in custody accounts are considered bankruptcy remote. This was demonstrated by the cases of Mt. Gox (where clients received compensation amounting to tens of per cent of the originally held volume[20]) and FTX, where funds held in customer accounts became part of the bankruptcy estate. Clients had to register for insolvency proceedings and were largely saved by the fact that their claims were denominated in US dollars and that the price of bitcoin rose sharply following the collapse of the exchanges. In any case, if a major exchange with an associated custody business were to fail today, clients' balances in custody accounts would not be affected by the bankruptcy of the exchange (unlike in the cases of Mt. Gox and FTX).

Option of combining external custody with an internal MPC solution

When using certain external custody service providers (such as BNY), who typically use external MPC orchestration platforms for key management (such as Fireblocks), the CNB would still need to manage a private key or keys. Transactions are initiated and subsequently approved directly on the custodian's platform – whether via a web interface or, for example, from the client's internal system via a public API. However, before execution on the blockchain, each transaction must be co-signed within the MPC framework using key shards held by both the custodian and the client.

Coinbase custody completely relieves clients of the need to manage key security

Other custodians (e.g. Coinbase Custody) have full control over the client's private key. They use MPC technology internally, but all the shards of the private key are entirely in their hands. The main advantage of this approach is its operational simplicity: clients are not required to build parallel infrastructure similar to that operated by the custodians themselves. Coinbase Custody, in particular, is a dominant player in services for ETFs (81% of ETF funds reportedly use this provider). Its services are also used by Strategy (formerly MicroStrategy) and others. This method of holding bitcoin is, however, sometimes criticised due to the absence of key control – something that can be viewed from one perspective as an advantage (a simple solution) and from another as a disadvantage (loss of control).

Co-custody model

Co-custody: a more complex but highly secure solution

One of the options described above involves the use of an external custodian combined with the CNB co-signing via MPC technology (e.g. Fireblocks) – a model sometimes referred to as co-custody. The requirement to co-sign transactions using MPC makes this a technically more demanding process, one that is comparable in a sense to the requirements of self-custody. This model is generally regarded as a highly secure solution.

19 See, for example, Clifford Chance & Komainu: *Custody of cryptoassets: Moving towards industry best practice* (2023), pp. 43–44: "It is possible that the client may agree that, although the arrangement is called 'custody', the cryptoassets will be transferred to the custodian…in which case it is hard to see how such cryptoassets could be regarded as held on trust." https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2023/06/custody-of-cryptoassets.pdf

20 Paradoxically, even this partial compensation may today be more valuable in dollar terms than the amount clients originally held at the time of the exchange's collapse.

6. BITCOIN AS PART OF THE RESERVES?

This section looks at a rather diverse mix of issues related to whether and how bitcoin can be included in the international reserves in practice, i.e. how to approach accounting and audit-related matters.

We ponder more philosophical questions at the end of the section. First, we focus on the parallels between bitcoin and gold. At the very end, we also look at factors that currently make bitcoin such an unusual asset.

We consider it important to note that there are a host of negative views on bitcoin in the public domain, be it the various illegitimate or outright criminal ways of using bitcoin, matters related to the dark web, or other issues. We therefore explicitly refrain from attempting to list them all in this analysis.

6.1 Can bitcoin become part of the official reserves?

Direct investments in bitcoin would not be reported as part of the official reserves

The CNB has held bilateral consultations with IMF and ECB representatives on the statistical reporting of potential central bank bitcoin holdings. The outcome of these meetings is that all the institutions concur that **directly held bitcoin is not a reserve asset**, therefore its value would not enter Section "A. Official reserve assets" of the reserves template.[21]

Directly held bitcoin should not be reflected simultaneously in any other part of the IMF template (not only Section I, but also Sections II–IV). Section "I.B Other foreign currency assets" refers exclusively to foreign currency assets not included under I.A. Unlike Section I.A, this category includes any foreign currency assets issued by Czech residents and illiquid cross-border foreign currency assets. The remaining sections of the template do not methodologically allow for the inclusion of directly held bitcoin either.

The CNB can still consider bitcoin to be part of its reserves

Inclusion in accordance with the aforementioned position taken by the IMF and ECB is important in view of the commitment to adhere to international statistical methodology and to ensure international comparability of reported statistics. However, this does not mean that, as regards the internal analysis of the impacts on the international reserves and the CNB's communications with the public, the CNB could not hold bitcoin as part of (its own definition of) the international reserves. However, it is still necessary to take into account that bitcoin held in this way will not become part of the official reserves under IMF methodology, so certain differences may arise between the volumes of reserves reported internally and officially. However, the CNB is already in this situation today.[22] Therefore, when we refer in this report to the possibility of including bitcoin or any other asset in the international reserves, we do not mean its treatment in terms of IMF or ECB methodology,

—

21 This is because directly held bitcoin does not meet the statistical criteria for reserve assets under the applicable macroeconomic statistics methodologies (SNA/ESA/BPM), with which the template is generally consistent (see paragraph 110 of the IMF Guidelines). With the exception of gold, which is historically included, Section A applies solely to financial instruments with a counterparty, which must be a non-resident. Bitcoin does not meet the above non-resident counterparty condition. According to the manuals currently in force and the interpretation thereof, digital assets with no counterparty (i.e. including bitcoin) are thus deemed non-financial assets. For completeness, we add that, besides the existence of a counterparty, the criteria for reserve assets are denomination in foreign currency and liquidity. The methodology for recording reserve assets is described in detail in the Balance of Payments and International Investment Position Manual (BPM6), specifically in paragraphs 6.64–6.116.

22 According to IMF methodology, official reserves may include, for example, repurchase agreements, meaning that reserves can be "artificially" increased relative to the net value of the assets held.

but rather the inclusion of the asset in the overall mix of assets and liabilities held by the CNB.

Bitcoin ETFs as part of the reserves

The situation is completely different for indirect investments via ETFs – such investments would be reported in the usual way as part of the international reserves, similarly to ETFs with other underlying assets.

6.2 Direct investment in bitcoin in the CNB's accounts

There are various ways in which bitcoin could appear in the CNB's accounts. However, provided it is held over the long term and the number of transactions is not too high (in the sense that that CNB will not become a high-frequency trader), it can be assumed that the following rules will apply.

Bitcoin in the CNB's balance sheet: an intangible asset

Directly held bitcoin will be reported as a specific intangible asset in the balance sheet item "Tangible and intangible assets". In the case of a significant volume (CZK billions), the creation of a separate sub-item in the ten-day balance sheet would be considered.

Bitcoin will be valued at its acquisition price or its current fair value, whichever is the lower, i.e. it will be recorded in the account at acquisition price, and an allowance will be created if the fair value decreases. Profits and losses will be recorded only when realised. For significant volumes, the current fair value of the holdings will also have to be disclosed in the financial statements.

Bitcoin purchases could only appear in the CNB's costs if very small-volume purchases were made with the aim of testing internal infrastructure under development. Purchases in larger volumes will not appear in the costs at all. From an accounting point of view, this is similar to selling one type of asset from the reserves and buying another.

6.3 How would the CNB prove ownership of bitcoin held in self-custody to an external auditor?

How to prove the volume of BTC held to the auditor (or to the public)?

A variety of options are available…

This issue is still not entirely clear, and if the CNB opted for self-custody, it would have to be explicitly discussed and the specific method agreed upon with the external auditor. (This problem only applies to the direct method of holding bitcoin; it does not exist when external custody is used, because confirmation is provided directly by the custodian.) In preliminary consultations, the CNB's current auditors confirmed they do not consider this an insurmountable problem.

There are a number of ways to do this:

- off-chain cryptographic proof of private key ownership (proof-of-ownership)
  (using BIP 322, the CNB would sign a pre-agreed text using its private key and the auditor would then verify that the relevant address holds the declared amount of bitcoin),
- microtransaction (proof-of-control)
  (the CNB would send a small transaction from its address; this method is less preferred, as it involves the movement of funds and associated costs),
- The CNB would publicly declare its address
  (this would allow anyone to view all transactions and balances at this address; disclosure of the address is considered by many to be a potential risk).

6.4 Bitcoin – digital gold?

Given its properties, bitcoin is often regarded as a new, digital form of gold.

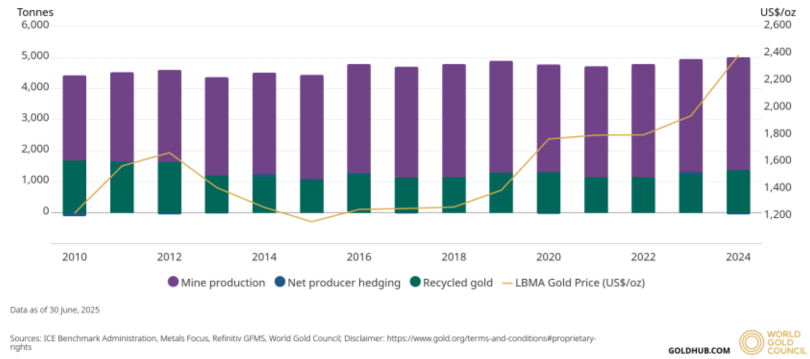
Limited supply, scarcity

The main argument is that only 21 million BTC can be issued, so supply is finite. As of July 2025, 19.9 million BTC had been mined, leaving only around 1.1 million to go. By the end of the current period (2024–2028), during which the reward per block mined is 3.125 BTC, around 0.4 million BTC will still be mined. In the following period (2028–2032), the reward will be halved, and a total of roughly 0.3 million BTC will be mined over those four years. Mining will get slower and slower and is expected to cease in 2140.

This is where the parallel with gold becomes particularly evident. According to data from the World Gold Council (WGC), 3,644 tonnes of gold were mined in 2024. Given the total amount of gold mined to date – around 212,000 tonnes – this represents an annual increase of around 1.7%. However, it is estimated that roughly 65% to 70% of gold is used for non-financial purposes (jewellery production, industry, healthcare, etc.). Gold mining is becoming increasingly difficult, but rising prices are naturally leading to the extraction of deposits previously considered unprofitable. Total gold production has been rising slightly in recent years, and according to WGC data, 2024 saw the highest annual volume of gold mined in history.

The total volume of bitcoin mined is currently growing at an annual rate of around 0.8%. After 2028, it will grow at 0.4% per year. Overall, it can thus be said that for financial purposes the growth in the volume of the two assets does not differ significantly, amounting to less than one per cent a year.

Chart 1-22: Volume of gold mining and recycling



Source: World Gold Council

The limited supply and continuously slowing rate of bitcoin mining is the reason bitcoin is an important “non-inflationary” alternative to other assets, similarly to gold and other commodities. It can thus be used as a hedge in a world where the volumes of fiat currencies issued are subject to the decisions of central banks.

Independence, no one’s liability

Bitcoin is not dependent on any central authority: it is no one’s liability and is designed as a permissionless system, i.e. no third party can prevent its transfer. Bitcoin can thus be transferred easily and quickly and at minimal cost. This sets it apart from gold, where transport between locations is a logistically complex and costly operation.

Like gold, bitcoin is not a liability of any individual or institution; no one will "repay" it – it is neither a debt nor a claim. Similarly, neither bitcoin nor gold is dependent on a central authority or government.

In these respects, the two assets are very similar, with bitcoin's digital form offering certain advantages.

Resistance to seizure and freezing

Bitcoin resembles physical assets (including gold, of course) held directly by investors (in safes, for example) in other respects too. The bitcoin protocol does not permit intervention by any authority that could press for the asset to be seized or frozen. This is again a characteristic that closely resembles gold. Bitcoin can, of course, be fraudulently misappropriated (e.g. through misuse of a private key), but the same applies to physical assets (e.g. theft from a vault, forced occupation).

Limited correlation with traditional assets

One of the reasons investors often include gold in their portfolios is its limited correlation with the prices of other financial assets. In this respect, bitcoin is largely similar – it exhibits virtually no correlation with bonds, while differing from gold in that it is affected to some extent by developments in markets for risky assets (such as equities) – see section 44.

Does bitcoin have intrinsic value?

The question of whether bitcoin has intrinsic value is a frequently discussed topic. The answer, however, is not straightforward. It depends on how one defines "intrinsic value" and from what perspective one looks at bitcoin.

If intrinsic value is understood as the present value of the future cash flows generated by an asset, then bitcoin does not have intrinsic value – it does not generate interest or yield, and its value is not backed by any asset. The same applies to gold. However, one could argue that gold can be used in industry, healthcare and jewellery production and must therefore have some intrinsic value (although if the financial aspect of holding gold were to disappear, this value would decline significantly).

There is, however, an alternative perspective. According to proponents of digital assets, intrinsic value should be assessed not only in terms of utility, but also with regard to scarcity, network effects, independence and other key factors. They also consider the ability to conduct transactions quickly and independently of authorities, and the fact that bitcoin is scarce (a 21 million BTC limit), to be essential aspects of its value. Its energy and technical intensity is also sometimes assessed from this point of view. According to some, bitcoin has a floor value, which – in simple terms – comprises the cost of acquiring the hardware required for mining and the energy needed to mine a single block, compared to the reward received (the transaction fees plus the block subsidy – the fixed reward granted to miners for each block mined). This floor value is currently estimated at around $80,000 per BTC.

Finally, there is yet another perspective, one that centres on whether currencies themselves have intrinsic value. Holding, for example, a $100 or €500 note probably does not have intrinsic value in and of itself, yet many market participants still choose to do so. In this respect, however, it should be noted that every currency is backed by the economy of the issuing country, which undoubtedly does have value.

World Bank study

The question of whether bitcoin has a role to play in international reserves management was also addressed in a 2024 study by the World Bank.[23] The study broadly confirms the above arguments, but it concludes that it is unlikely that central banks will replace gold with bitcoin in the foreseeable future. The authors cite as key arguments the historical role of gold (the gold standard and the Bretton Woods system) and the fact that gold is extremely secure and central banks already have the necessary infrastructure to hold and trade it. According to the World Bank, central banks do not currently hold gold because of its risk-return characteristics, but rather because gold and reserve currencies are considered largely equivalent – even after the collapse of the gold standard. For completeness, it should be noted that many of the arguments used in the study are now outdated, and its conclusions should be viewed critically, or with a degree of caution.

6.5 Bitcoin: belief, investment mania or a sea change in the approach to storing value

Rise in popularity

Since its inception in 2009, bitcoin has gradually evolved from a fringe experiment among technology enthusiasts into one of the most widely discussed assets today. Initially, interest was driven mainly by a community of cryptographers, libertarians and technological innovators, who saw in it above all a means of financial autonomy and resistance to traditional institutions. Over time, however, they were joined by the broader public – investors seeking profit, media drawn by dramatic price movements, and eventually financial institutions concerned about being left behind.

Bitcoin as a phenomenon of belief

One of the key drivers of bitcoin's price growth is actually "belief" – the conviction among investors that its value will continue to rise in the future. This effect is reinforced by each media mention of new price highs and by every story of a small investor becoming a millionaire. The psychological mechanism of FOMO (fear of missing out) further contributes to new entrants joining the market, which pushes the price up.

Between technology and trend

It may be tempting to label bitcoin as a speculative bubble, but this is overly one-sided. Bitcoin is based on a specific technological innovation – the blockchain – and offers real functions such as decentralised storage of value and a means of making relatively fast global payments. Its proponents therefore argue that, despite the price volatility, the underlying technology makes sense. Critics, on the other hand, claim that its actual use is limited and that its growth is driven largely by speculation.

The generational factor and the "next big thing"

The generational dimension is interesting. Bitcoin and other digital assets have become popular among the younger generation, who are quicker to embrace new technologies, less trusting of traditional institutions and more open to experimenting with new forms of investment. However, if bitcoin really is more of a cultural than an economic phenomenon, it may be replaced in the future by "the next big thing". History shows that generational trends change – what was once a symbol of progress for one generation may become merely a curiosity for the next.

—

23 *Can crypto-assets play a role in foreign reserve portfolios? Not today, and likely not in the near future*
https://documents1.worldbank.org/curated/en/099553102232444409/pdf/IDU1c16366af173fa148931a28b189e8eca412f3.pdf

Conclusion: belief or value?

The question then is: Is the rise in the price of bitcoin based on fundamentals, or is it just a result of collective belief? The truth probably lies somewhere in between. On one hand, we have a technology with real potential; on the other, the price in many respects behaves in ways typical of investment manias. Regardless of whether the future brings continued growth, stagnation, or bitcoin's replacement by another phenomenon, it is clear that bitcoin has already secured its place in history as an example of how belief in technological innovation can evolve into a global economic and cultural phenomenon.

7. EXTERNAL STUDIES

Studies by the University of Economics in Prague and Charles University

The following section summarises the main conclusions and recommendations contained in studies commissioned from and prepared by external experts. The first was prepared by a team of experts from the University of Economics in Prague and the second by a team from Charles University.

In the summary, we deliberately refrain from distinguishing which information is drawn from which specific study. Where a longer passage of text is cited, it is italicised.

In terms of the main conclusions and recommendations for the CNB, both studies are consistent with our own conclusions. For the potential integration of bitcoin at the CNB, they recommend that:

- its introduction should be gradual, with an emphasis on operational risks (governance, security);
- in the case of self-custody, robust technical solutions should be preferred (multisignature, MPC); alternatively, regulated services may be used (custody, ETFs);
- continuous follow-up monitoring of technological change and regulatory developments will be essential;
- both studies consider communication with the public to be key; in the case of direct investment under self-custody, transparency of holdings and auditability generally are regarded as important.

Both studies view bitcoin as a technologically stable and economically promising asset, which, however, given its nature, presents certain specific risks.

Both documents focus precisely on these risks, whether associated with bitcoin and blockchain technology itself, or with its economic and institutional aspects. The studies broadly address governance issues, scalability and other bitcoin-related areas. Their conclusions are summarised in the following subsections. Although certain aspects may be assessed critically, the message of both studies is the same: bitcoin is entering a phase of stability and is already ready to become part of institutional portfolios.

7.1 Digital risks

Technological development and governance of bitcoin

Bitcoin is:
- decentralised and distributed
- based on consensus and proof-of-work
- limited volume of BTC
- resilient to restrictions, manipulation and outages

The bitcoin protocol is a decentralised system for storing and transferring digital value. It uses distributed ledger technology (blockchain). At the core of the protocol is a proof-of-work consensus algorithm through which network participants (miners) take part in validating transactions and creating new blocks. Each full node in the network maintains a complete copy of the blockchain and independently verifies incoming transactions and blocks. This makes the system resistant to manipulation, censorship and failures of individual parts of the infrastructure. Key features of bitcoin are its openness, transparency and predetermined issuance schedule, which caps the number of bitcoins at 21 million.

Created in 2009, its architecture is now stable

The technological foundation of bitcoin was laid in 2009. Since then, it has undergone extensive development, but its core architecture remains stable and conservative. This stability is not accidental – it is a deliberate design feature intended to ensure its trustworthiness, security and predictability.

Base layer = Layer 1 (innovations can occur at higher layers without the need to modify the protocol)

Bitcoin's development takes place in three main layers. The first layer consists of the base protocol (Layer 1), where changes are very infrequent and typically take the form of soft forks, i.e. backward-compatible modifications. Well-known examples include SegWit (2017) and Taproot (2021). The second layer comprises supplementary solutions (Layer 2), such as the Lightning Network and the Liquid Network. This layer introduces new functionalities, mainly in the areas of micropayments, scalability and efficiency enhancement without interfering with the base layer. The third component is the supporting infrastructure – hardware wallets, libraries and security solutions such as multi-sig and MPC.

Bitcoin is an open-source project

Bitcoin is an open-source project. Its development is open and decentralised, yet it exhibits a high degree of coordination. The key mechanism is the Bitcoin Improvement Proposal process, used to submit and discuss proposed changes to the protocol. This is a technical standard, not a legally binding framework. Changes are only implemented if they gain sufficient consensus among developers, miners and node operators.

Bitcoin governance? The protocol

Bitcoin's governance is characterised by the absence of a central authority. No institution can change or enforce the rules of the network. The rules are embedded in the protocol – that is, encoded in the software and enforced through the technical behaviour of the network. This model of "governance without government" ensures strong resistance to censorship and abuse of power, but it also has certain disadvantages – such as slower responses to security threats and ineffective decision-making in the event of disputes.

However, even the protocol can be changed, provided there is a consensus

Changes to the protocol, such as Taproot and SegWit, have shown that even technically advanced and community-supported proposals take years to implement. With bitcoin, however, this slow pace of development is seen as a positive – a safeguard against hasty interventions that could undermine trust in the network.

Deviation from the protocol: isolation…

Network dynamics take the place of a legally binding rulebook: each participant decides which software to use, and any deviation from the consensus results in isolation. The risks of decentralised governance include the possibility of a hard fork, i.e. a permanent split of the blockchain. This has occurred in the past, for example with the creation of Bitcoin Cash. Such events do not pose a technical threat but can lead to short-term uncertainty and a loss of trust.

Bitcoin also benefits from the reputational incentives of its contributors – developers, node operators and miners have "skin in the game". They invest time, resources and reputation in a system whose stability affects the value of their own assets. This creates a natural incentive to maintain and develop the system responsibly.

Absence of a central authority: advantage or disadvantage?

From the perspective of institutional trust, the absence of a central authority is both an advantage and a risk. The advantage lies in strong resilience to political and regulatory interference. The risk is the absence of enforceable accountability in the event of failure. However, experience to date shows that bitcoin's community-based model functions consistently over the long term and is capable of handling key technical and organisational challenges.

Bitcoin's technological development and governance form a unique combination of technical stability and openness to innovation through community consensus. This model is not without risks but offers a high level of trustworthiness, which is vital for its potential institutional adoption, including its potential incorporation into the central bank's reserve strategy.

Risk of a hard fork

A hard fork is often cited as one of the main risks associated with bitcoin. However, both studies agree that this risk does not lead to data loss or direct devaluation.

Hard fork – a change to the protocol without backward compatibility (a new version of the software must be installed)

There have been several unsuccessful hard forks, but they did not threaten bitcoin

Hard forks – permanent splits of the blockchain into two or more incompatible branches due to the introduction of a backward-incompatible change to the protocol – can take various forms. They may be planned ones carried out with broad community consensus, typically aimed at introducing radical innovations. Such forks are rare in the bitcoin environment, where soft forks are preferred. However, there is also a risk of controversial hard forks, where no consensus is reached and an alternative software client with different rules is created. If this new client gains support from some of the nodes, another network will be created. The most well-known examples are Bitcoin Cash (2017) and the subsequent fork of that fork, Bitcoin SV (2018).

Hard fork – holders gain access to funds on both branches!

Even in the event of a hard fork, however, private key holders have access to the same funds on both branches of the chain. The main issue is therefore not the split itself, but the market valuation of the separate branches and the associated risks, such as the potential for replay attacks (the repeated use of a transaction on both branches) and temporary incompatibility of services.

Hard forks are generally seen as highly unlikely. Miners, users, developers and economically significant actors (exchanges, pools) share an interest in maintaining a successful platform. Disagreements among them can lead to an erosion of trust and subsequent fragmentation of the chain. However, external pressures – such as regulatory interventions, which could divide the community along geographical or legal lines – may also pose a risk. In this respect, however, bitcoin appears to be entering a more favourable era.

> *"Empirical experience shows that a split in the community can lead to the creation of a new branch, which, however, will fail to gain market relevance without infrastructure support. An example is the emergence of Bitcoin Cash (BCH) in 2017, which resulted from a disagreement over the implementation of SegWit and an unwillingness to increase the block size. Both branches still exist today, but bitcoin (BTC) has retained more than 95% of the combined market capitalisation. We should also mention the partially successful and in many respects specific hard fork Litecoin, which currently*

has a lower market capitalisation than BCH. Other hard forks, such as Bitcoin Gold (BTG), have minimal market capitalisation (currently around $13 million, as against more than $2 trillion for BTC), or are no longer maintained (Bitcoin XT, Bitcoin Classic and Bitcoin Unlimited). This demonstrates that the market favours stability, technical conservatism and the network effect of the original chain."

Risk of hard fork assessed as low

So, there is still a risk of another bitcoin hard fork, but both studies assess it as low, and even if it were to materialise, the consequences would not be dramatic. Hard forks thus do not pose a risk of loss of value, but rather increase uncertainty in the bitcoin ecosystem. The possibility of a fork is a general feature of open systems with no central authority. In this environment, Bitcoin has not just maintained its dominance, but gradually strengthened it. One of the studies notes that this outcome is well described by game theory, specifically the Schelling point concept.[24]

Risk of a 51% attack

51% attack = control over the blockchain enabling manipulation of blocks

A 51% attack is a critical vulnerability common to all blockchain-based technologies. In principle, it involves the risk of a single entity (or coordinated group) taking control of the majority of the network's computing power ("hashrate") and producing the longest chain of blocks. This would allow it manipulate the blockchain, for example by double spending, preventing certain transactions from being confirmed and excluding other miners. Only the majority attacker would be able to mine new blocks.

Given the scale of resources invested in mining and its high degree of fragmentation, it is not currently considered a risk in the case of bitcoin

The risk of such an attack on bitcoin is currently considered to be very low. The cost of acquiring the hardware needed to achieve 51% hashrate is estimated at hundreds of billions of dollars. However, a potential attacker would face significant economic risk – a successful attack of this kind would probably result in a loss of trust in bitcoin and a slump in its market price. This could result in the funds acquired being lower than the attacker's total costs (the drop in the bitcoin price and the devaluation of costly mining hardware). In practice, then, the incentive to carry out a 51% attack is greatly limited by a combination of high costs, technological constraints and adverse economic consequences.

Bitcoin's dominance is a threat to other digital currencies

While bitcoin itself is too costly a target for a successful attack of this kind, the hardware currently used to mine it can often be easily repurposed to mine smaller "coins". These alternative chains are exposed to a disproportionately higher risk of attack. This has led to several incidents in the past.[25] This security asymmetry is one of the factors that further reinforces bitcoin's dominant position.

Despite the very low level of risk, it is generally recommended to require multiple transaction confirmations. It is said that six confirmations (the creation of six additional blocks in the blockchain) is practically irreversible.

To sum up, while a 51% attack is theoretically possible, the studies consider this threat to be extremely unlikely in practice for economic, technical, coordination and reputational reasons.

—

24 This refers to the solution that gamers prefer when communication is not possible – the one that appears intuitive and natural. In this case, the Schelling point is the original version of bitcoin. In other words, tried and tested solutions are generally preferred.

25 Examples include Bitcoin Gold in 2018, where $18 million was stolen; Bitcoin SV, which suffered a series of 51% attacks in 2021 during which hackers deleted and altered recent blocks; and Ethereum Classic in 2020, when several million dollars were reportedly stolen.

Risk of quantum computers[26]

The development of quantum computers is a theoretical threat

In practice, however, misuse for such purposes is not is not expected in the near future

The development of quantum computers is considered to be a risk to bitcoin. The risk of their use for a 51% attack is largely theoretical. A quantum processor would require around one million physical quantum bits (qubits).[27] The most advanced quantum processors currently contain hundreds to low thousands of qubits, but the technology is still highly error-prone.[28]

The situation as regards private key compromise is a little different. The currently used 256-bit ECDSA asymmetric cryptography could theoretically be compromised using 1,500–2,000 logical qubits.[29] Once a public key has been disclosed, it would be possible to compute and misuse the private key. However, the current technology is several orders of magnitude away from the level required for such an attack. Creating stable logical qubits is no longer a major challenge. However, the issue of executing computational operations with this type of qubit is still not fully resolved. It is estimated that a cryptographically relevant quantum computer will become available in 2030 at the earliest and more likely in the mid-2030s.

A defence exists and is under development: **post-quantum cryptography**

The community is aware of this threat, and discussions on quantum-resistant signature schemes (post-quantum cryptography) have been ongoing for some time. Various other areas that rely on current cryptographic algorithms are also potentially at risk, including banking applications and digital signatures in general. Bitcoin is therefore not the only technology exposed to this threat. It is part of a broader set of technologies that rely on digital trust, which would need to respond in time and change the way they operate. There are currently several initiatives addressing the transition to post-quantum cryptography. Examples include Project Leap overseen by the Bank for International Settlements (BIS), which focuses on interbank communication, and the recommendations of the UK's National Cyber Security Centre.[30] There are also various post-quantum encryption algorithms currently undergoing standardisation at NIST: the hash-based XMSS scheme, lattice-based systems and the multivariate Rainbow.

Even without post-quantum cryptography, there are defence options: **demonstrating legitimate acquisition**

Even in the highly unlikely event that a secure method of post-quantum cryptography cannot be found, this would not necessarily lead to the demise of bitcoin. In such case, bitcoin holders would demonstrate a legitimate transaction as the basis for holding the asset, rather than just possession of the private key. Authorised holders would therefore not lose their bitcoins; it is unlikely that they could simply be stolen from wallets in such a situation without any possibility of defence.

Risk of dependence on the internet

Bitcoin is not entirely dependent on the internet

The two opinions agree that the internet (specifically the currently used TCP/IP communication protocol) is merely a medium for the functioning of bitcoin. However, the existence and functioning of bitcoin – its cryptographic

—

26 This section was prepared in collaboration with Martin Veselý, who contributed by correcting certain inaccuracies found in the two studies.

27 C. Gidney: *How to factor 2048 bit RSA integers with less than a million noisy qubits*; C. Gidney and M. Ekera: *How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits*.

28 Google's Willow chip: 105 physical qubits; IBM's Condor: 1,121 physical qubits, but without error correction, making it unusable for attacks in practice; Atom Computing (in collaboration with Microsoft): 50 logical qubits in 2026/more than 1,000 physical qubits. D-Wave: 5,000 qubits, but the processor is designed exclusively for optimisation tasks.

29 A logical qubit is a group of physical qubits combined for error correction purposes. Depending on the error correction code used, one logical qubit requires 10–1,000 physical qubits.

30 *Timelines for migration to post-quantum cryptography*.

principles and the method of recording entries in the distributed ledger, the blockchain – are not dependent on the internet.

A temporary interruption of communication in the network is not a problem

Reorganisation occurs once node connectivity is restored

Let's now describe the impact an internet outage would have. Blocks that already exist would continue to do so in individual nodes, as each node continuously retains its own copy. Without the ability to communicate with other nodes, the bitcoin network would probably fragment into local, isolated islands, which, in the extreme case, would consist only of individual miners. Within these islands, mining of new blocks would continue. Once connectivity is restored (whether through the resumption of internet service or its replacement by alternative communication channels), nodes would exchange information about the state of their chains, and in an effort to reach consensus, the longest chain would become the new global chain. Shorter chains would be reorganised and their transactions would be returned (to the mempool) for processing. It is evident that the island with the highest computational power would have the advantage. This process in which shorter chains are "discarded" and the longest chain becomes the new consensus is called blockchain reorganisation.

The risk of significant blockchain reorganisation increases with the duration of the outage. Efforts are already being made to prevent divergence across nodes by means of non-internet channels that replace the internet with alternative methods of information transmission. For example, Blockstream Satellite[31] continuously broadcasts the state of the blockchain via satellites, independently of internet status. There are also terrestrial alternative networks[32] pursuing the same goal.

A prolonged interruption of communication would be a problem

A prolonged internet outage would, of course, pose a problem for bitcoin. It would cease to function as a means of conducting transactions, lose liquidity and very likely experience a dramatic decline in value. It is important to emphasise, though, that in such a scenario, the entire world would be in deep crisis – conventional payment systems, cloud services, logistics and supply chains would probably cease to function. The loss of bitcoin's value would thus be only a secondary manifestation of a broader systemic crisis.

7.2 Regulatory and other similar risks

Risk of government rejection/geographical risks

The possibility of regulatory intervention by individual governments is not merely a theoretical threat.

The most significant restriction occurred in China in 2021

Mining simply moved elsewhere…

The biggest event of this kind is considered to be China's intervention in 2021, when bitcoin mining was banned across the country. The stated objective was to reduce energy consumption, but efforts to control capital flows also played a role behind the scenes. There was an immediate drop in global hashrate – by as much as 50% according to available data. Mining quickly relocated to other jurisdictions, mainly the USA, Kazakhstan, Russia and South-East Asian countries. This is not merely a figurative description of the situation – bitcoin mining hardware really was physically relocated to other countries to a large extent. In this context, it is notable how quickly the original performance of the network was restored.

31 https://blockstream.com/satellite/

32 goTenna, Locha Mesh, Kryptoradio

Chart 1-23

Bitcoin network hashrate [TH/s]

Source: data – blockchain.com, CNB chart

Fewer miners means higher individual profits

In this context, we should mention the economic incentives associated with such interventions. The ban on mining in China led to a dramatic drop in the overall performance of the network. This meant that for the remaining miners outside China, the probability of finding a block doubled. This caused a sharp increase in expected mining revenues and created strong economic pressure for the rapid relocation of mining infrastructure – which is precisely what happened. By 2022, the network's performance had returned to its original levels, and it subsequently continued to grow rapidly.

There are of course other regulatory risks as well. These may relate to the taxation of mining, licensing requirements, geoblocking of access and – in connection with consumer protection – frequent calls for the introduction of standard KYC/AML procedures. Tax issues are also under discussion. The potential restriction of access to critical internet infrastructure and the adoption of legislation that would prohibit mining without state approval are considered the most serious risks from bitcoin's perspective. Such approaches are currently being considered mainly by authoritarian regimes, where there is strong pressure to control capital flows.

Rather than seeking to restrict bitcoin through regulation the approach now being adopted is to **regulate it and place it on an "equal footing" with other assets**

From a global perspective, however, a "tolerate and tax" strategy is increasingly prevalent. Individual countries are realising that excessive regulation or bans would merely lead to the relocation of mining to other countries, resulting in the loss of potential tax revenues. Taxes, reporting requirements, capital requirements and other measures are gradually being introduced without losing control of the market. This now appears to be the best strategy for all stakeholders.

Tougher restrictions/regulation possible if bitcoin continues to grow rapidly

Another potential risk is intervention by governments if bitcoin were to gain macroeconomic relevance. Were it to move beyond the role of a speculative asset and reach a scale where it could threaten monetary sovereignty, capital market stability or fiscal policy, it could be viewed as a systemic risk. In such case, authorities might introduce substantial restrictions.

Bitcoin <> DLT!

However, the approach taken by countries is currently moving in the opposite direction. In the USA, the arrival of the Trump administration created a significantly more favourable environment, and even in Europe –

despite vocal opposition from the ECB[33] – there is a general trend towards increasing acceptance. More broadly, we are seeing a boom in technologies based on distributed ledger systems (DLT).

Overall, given the decentralised nature of bitcoin's infrastructure, regulatory restrictions are highly unlikely to have a significant impact – except in the potential case of a (globally) coordinated political decision to restrict bitcoin.

Environmental and reputational pressures

Proof-of-work: the cause of high energy consumption

Bitcoin was designed with a consensus mechanism for confirming transactions based on proof-of-work (PoW). In practice, this involves the seemingly pointless search for a cryptographic hash with special properties – a highly complex and computationally intensive process. This gives rise to a serious problem: extreme energy consumption. It is estimated that bitcoin miners currently consume 140–180 TWh a year (for comparison, the Czech Republic generated 77 TWh in 2023). This corresponds to an average power output of around 20 GW, equivalent to 20 Temelín reactor units.

Energy consumption may be seen as an issue in itself. It may lead to regulatory efforts to restrict PoW-based technologies and replace them with alternatives, such as proof-of-stake (PoS) as used by Ethereum. It is thus closely linked to the risks mentioned in the previous section.

However, a significant shift is already underway. Bitcoin is often mined in locations with very cheap electricity (such as areas with year-round sunlight using solar power plants) or with unutilised energy surpluses (miners as "buyers of last resort" using machines typically running only during periods of energy overproduction, e.g. from renewable sources) and may thus be helping to stabilise local power grids. In addition, it is reported that bitcoin currently has a cleaner energy mix than the global energy sector on average. According to some estimates, more than half of the network's consumption already comes from renewable or low-emission sources.

Bitcoin's proof-of-work is considered an important security mechanism

Proof-of-work is regarded by the community as an important security feature of the entire bitcoin ecosystem. In theory, migration to proof-of-stake is possible,[34] and one can imagine a scenario in which bitcoin would be forced to take such a step through a globally coordinated effort by the world's major economic powers. However, consensus in the network is currently maintained by miners, i.e. proof-of-work holders who have already invested substantial amounts in mining infrastructure, so a transition to proof-of-stake is not in their interest.

7.3 Economic risks

Risk of bitcoin being replaced by another crypto-asset

Bitcoin's first-mover advantage contributed to its current dominance

Bitcoin benefits greatly from its first-mover advantage. Due to its rapid development, its large number of users and the sums invested in its mining infrastructure, it now seems that bitcoin could only be replaced by alternative digital assets if they offered fundamental innovations or utility (such as the above-mentioned quantum resistance, which, however, even bitcoin may

---

33 Christine Lagarde: "Bitcoin will not enter the reserves of any of the central banks of the General Council." https://www.bloomberg.com/news/articles/2025-01-30/lagarde-is-confident-eu-central-banks-will-shun-bitcoin-reserves

34 Ethereum successfully transitioned to PoS in 2022, reducing its energy intensity by 99%.

one day provide). However, the motives for current bitcoin miners and holders to migrate to another currency are very low.

Bitcoin's strength lies in game theory, and specifically in the Schelling point concept: rational participants spontaneously converge on the chain with the greatest accumulated work, liquidity and infrastructure, as it offers the lowest risk of reorganisation and the highest profit from mining and trading. Previous hard forks (BCH, BSV and ETHW) have shown that even slightly weaker chains quickly lose relevance, and the original bitcoin has always maintained the dominant position.

Bitcoin's current strong position and the lack of incentives for holders and miners to migrate to another (better) technology therefore now reinforce its dominance compared to other digital assets. The risk of migration and the related potential devaluation of bitcoin is thus considered very low.

Risk of limiting mining incentives

Halving will be gradually replaced by transaction fees

As is widely known, bitcoin was designed in such a way that no more than 21 million coins can ever be mined. New bitcoins are created solely through mining, i.e. by confirming transactions. For each newly mined block, the miner receives a fixed reward known as the block subsidy, currently BTC 3.125 (this reward is halved every four years[35]), plus the sum of all the transaction fees defined by the transfers contained in the block (these fees are set by the senders themselves at their own discretion; if they want to make their transactions more likely to be signed in the next block, they tend to voluntarily raise them slightly). There are thus concerns that reducing the block subsidy may make it economically inefficient to mine new blocks.

But there is still a theoretical risk that transaction fees and high mining costs could cause miners to quit the network

The studies consider this risk to be limited. It is assumed that the fees received for signed transactions will play an increasingly important role, a trend that can already be observed to a small extent today. In the past, when the block subsidy was a multiple of its current level, transaction fees played virtually no role. Today, they commonly make up several per cent of a miner's total reward, reaching 5% or more during peaks. In some periods (in 2017, for example), they even made up the bulk of the reward. This trend is expected to strengthen in the future.

Nevertheless, there is a theoretical risk of a "fee death spiral". If fee revenues became insufficient to cover miners' operating costs and the block subsidy ceased to exist, some miners would leave the network, which would reduce its security. Although this scenario has not yet been empirically observed, it cannot be ruled out, especially if demand for on-chain transactions drops significantly or if most activity shifts to secondary layers.

Risk of failure of (Micro)Strategy

Despite its unorthodox policy, (Micro)Strategy does not represent a major threat

One of the opinions explicitly addresses the possibility that the bitcoin market could be damaged if Michael Saylor's company Strategy (formerly MicroStrategy; ticker MSTR) gets into difficulty. Strategy is well known for its decision a while ago to invest heavily in bitcoin. To fund these purchases, it has used a wide range of financial instruments (ranging from conventional ones such as issues of its own shares, to unconventionally structured preferred bonds). It is estimated that Strategy currently holds about 2.9% of

—

35 There are theories that halving is an important factor in the rise in bitcoin's price. According to these theories, halving reduces the supply of new coins, which, given constant demand, puts upward pressure on the price of bitcoin.

the bitcoins in existence. Frequently mention is also made of the relatively high premium at which MSTR shares are now traded (150%–180% of the value of its bitcoin holdings depending on the market situation).

Despite its unorthodox policy, MicroStrategy does not represent a major threat

However, the opinion focuses on the fact that Strategy's overall debt remains relatively low (with leverage at only around 20%) and that for the company to run into difficulties, bitcoin would need to fall to very low levels and remain there for an extended period (it would have to stay at around $18,000 for several years). The opinion therefore states that Strategy does not represent an immediate threat to bitcoin.

Very high volatility of the price of bitcoin

When assessing volatility, the analyses arrive at similar conclusions to the CNB that the volatility of the price of bitcoin is very high compared to other, more "conventional" assets. Nevertheless, significant changes are visible in this area too.

Volatility is very high, occasionally approaching that of gold and stock indices

First, bitcoin remains an asset with relatively low market capitalisation despite growth in its total capitalisation to more than $2 trillion (the size of the US government bond market, for example, is close to $30 trillion). As a result, trading may lead to larger price swings. Moreover, the market is heavily influenced by the activity of retail investors, who are highly sensitive to any media news. This increases the risk of procyclical herd behaviour.

Bitcoin's price volatility is still far high than that of gold (which itself is considered a highly volatile asset). However, it is gradually approaching the volatility levels of some higher-risk stocks (e.g. tech companies). In some periods (in April 2025, for instance), bitcoin's volatility temporarily fell below that of stock indices (S&P 500 and NASDAQ) and even gold. It is assumed that the declining volatility goes hand in hand with the growing number of institutional investors and their buy-and-hold strategy. The behaviour of large bitcoin holders (whales), whose exchange holdings have been getting smaller and smaller since 2020, is having a similar effect on volatility. It is therefore possible that, as bitcoin's market capitalisation has gradually increased and the role of institutional investors has grown, the bitcoin market has entered a new phase characterised by lower volatility.

Volatility – a threat or an opportunity?

However, one of the external opinions highlights an important aspect of volatility – its high levels are not only a threat, but also a potential source of exceptional returns. It mentions economic studies that consistently find a positive relationship between volatility and market premia, after adjustment for macroeconomic factors. In other words, assets with highly volatile prices offer exceptional returns (but potentially also exceptional losses).

7.4 Operational risk

Risk of loss/abuse of the private key

The risk associated with the loss or abuse of the private key to directly held bitcoins (self-custody) is incomparable to any other risk the CNB currently faces.[36] The studies agree that if the CNB decides to invest in

[36] This is due mainly to transaction irreversibility. Once a bitcoin transaction is confirmed in the blockchain, it cannot be cancelled, reversed, disputed or revoked. By contrast, transactions in conventional financial instruments are reversible to some degree.

bitcoin, it will have to assess this risk thoroughly and set up robust processes to eliminate it.

Bitcoin adoption would have to be cautious and well-planned

Operational risks incomparable to "conventional assets"

Both studies recommend integrating bitcoin gradually and cautiously. They propose external key management in the initial phases (either by investing in ETFs or by using a custodian that completely isolates the investor from the management of private keys, as is the case of the most widely used Coinbase Custody, for example) and only limited internal testing of direct bitcoin holdings with self-custody. According to the external reviews, the security options are the same as those described in section 5.2 – mainly MPC and multi-sig. The studies consider MPC to be the most modern and – for financial institutions – the most suitable technology.

As regards bitcoin management practices, the first standards are beginning to emerge. These include the Cryptocurrency Security Standard (CCSS), an open standard defining key management security requirements. At the international level, the ISO/TC 307 technical committee is also addressing standardisation,[37] although self-custody standards have yet to be finalised.

Institutions often avoid self-custody…

Both studies note that, due to the scale of these risks, many institutional investors have so far elected to completely avoid the issue of self-custody – either by purchasing ETFs or by using Coinbase Custody without the private key management option.[38]

But: "not your keys, not your coins"!

In this context, certain risks associated with the loss of control over private keys are also mentioned, such as regulatory oversight, intermediated access or dependence on an external entity, and geopolitical and security risks. In general, this results in a disconnection from direct ownership of on-chain assets ("not your keys, not your coins"). It was for these reasons that El Salvador switched from BitGo to its own cold wallet solution.

8. COMMUNICATION

8.1 List of statements made by other CBs on the topic

A whole range of central bank representatives have commented on bitcoin in the past. For reference, we present some of their statements here.

ECB:

- Lagarde (01/2025): "*Reserves have to be liquid, secure, and safe,… bitcoin does not meet these criteria due to its volatility and potential risks linked to money laundering and illicit activities.*" https://www.euronews.com/business/2025/01/30/lagarde-hints-at-further-ecb-rate-cuts-rules-out-bitcoin-reserves
- So virtual, yes, but currency, no. Why not? (2018, updated 2021) Q&As on why the ECB considers Bitcoin not to be a real currency, but only a speculative asset - https://www.ecb.europa.eu/ecb-and-you/explainers/tell-me/html/what-is-bitcoin.en.html

37 https://www.iso.org/committee/6266604.html

38 This is also the primary bitcoin holding method used by BlackRock's iBit ETF. As one of the world's largest asset managers, BlackRock can hardly be considered technologically backward, so this confirms how complex the issue is. The same approach is also used by Fidelity and the US government, for example.

- Bindseil, Schaaf (2022): “*Bitcoin is rarely used for legal transactions*” https://www.ecb.europa.eu/press/blog/date/2022/html/ecb.blog221130~5301eecd19.en.html
- Bindseil, Schaaf (01/2024): “*ETF approval for bitcoin – the naked emperor’s new clothes*” https://www.ecb.europa.eu/press/blog/date/2024/html/ecb.blog20240222~0929f86e23.en.html

Fed:

- Powell (12/2024): “*We’re not allowed to own bitcoin*” https://finance.yahoo.com/news/fed-cant-hold-bitcoin-not-211628096.html
- Powell (12/2024): “*People use Bitcoin as a speculative asset. It’s like gold – it’s just virtual and digital*“ https://finance.yahoo.com/news/fed-chair-powell-bitcoin-gold-190021426.html
- Powell (06/2025): “*Bitcoin and other crypto assets have matured and become more mainstream, and…the central bank is reassessing policy statements…*” https://www.cnbc.com/video/2025/06/25/fed-chair-powell-the-crypto-industry-is-maturing-becoming-more-mainstream.html

BoE:

- Bailey (05/2022): “*Bitcoin has no intrinsic value and is not a practical means of payment.*” https://bitcoinmagazine.com/markets/bank-of-england-governor-says-bitcoin-isnt-practical
- Cunliffe (11/2021): “*But they [cryptoassets] are growing very fast and they are integrating more into what you might call the traditional financial system so the point at which they might pose a risk is getting closer…*” https://moneytothemasses.com/news/bank-of-england-warns-of-bitcoin-risks-everything-you-need-to-know

BoC:

- Chapman, Wilkins (2019): “*From a central banking perspective, the monetary landscape 10 to 15 years from now could look radically different than it does today.”* https://www.bankofcanada.ca/2019/02/staff-discussion-paper-2019-1/

RBA:

- Bullock (11/2024): “*Don’t call it an alternative currency,…It’s not a currency, it’s not money; it’s being used as some sort of asset class. I don’t really see a role for it in the Australian economy or payments system.*” https://decrypt.co/292051/australia-risks-falling-behind-as-rba-governor-rejects-cryptos-financial-role

In this context, it is important to note that many central bank officials have often commented on the potential introduction of CBDCs, the regulation of stablecoins and similar topics. However, these areas are not the focus of this text and, for that reason, such quotes are omitted from the list above.

For completeness, we note that there were reports in September 2025 (https://www.markets.com/news/el-salvador-diversifies-reserves-gold-purchase-imf-bitcoin-948-en-eu/) that El Salvador had stopped buying bitcoin earlier in the year in response to pressure from the IMF.

8.2 Controversies surrounding bitcoin

There are a number of issues that the public feels strongly about when it comes to bitcoin. If the CNB does decide to invest in bitcoin, some of these topics may be raised in the Czech public debate.

Energy intensity of mining

The most frequently mentioned controversy is the high electricity consumption resulting from the proof-of-work principle on which bitcoin is based. As mentioned in section 7.2, the annual consumption of the bitcoin network is currently estimated at 140–180 TWh. For illustration, this corresponds to roughly double the total annual electricity generation in the Czech Republic. It is therefore a serious problem.

Today, however, it seems that this problem is no longer as critical as it was, for the following reasons:

- mining is being relocated to areas with abundant or even surplus cheap electricity (such as regions with year-round sunlight using solar power plants),
- access to cheap energy is an important economic factor in deciding on new mining projects – renewable energy is now the dominant source for new projects,
- miners are already helping to stabilise the power grid by taking advantage of very low (or even negative) spot electricity prices and limiting mining during peaks,
- it is reported that bitcoin mining now has a “cleaner” energy mix than the global economy on average.

If, despite this, efforts were made to ban or restrict bitcoin for this reason (for example by regulators, or in the event of globally coordinated action by governments), there would still theoretically be the option to replace the proof-of-work concept with another mechanism. Ethereum made such a transition in 2022. Although no such change is currently being planned for bitcoin, this is a possible fall-back option.

Illicit activity

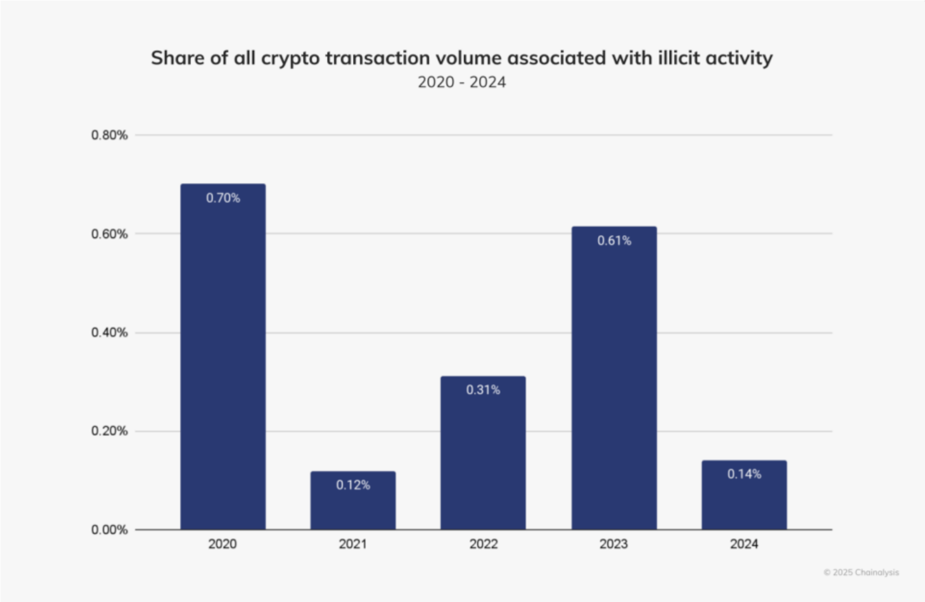
Bitcoin is often referred to as an instrument of the underworld. Its use in financing illicit activity on the dark web and for money laundering and extortion, among other things, is frequently highlighted. The anonymity of bitcoin transactions is regarded as the main reason for such conduct.

In this context, the case involving bitcoins donated to the Czech Ministry of Justice by Tomáš Jiřikovský, convicted operator of the illegal Sheep Marketplace (and later probably also Nucleus Market), provided a valuable insight. The public was surprised to discover that, thanks to the public ledger, bitcoin transactions are perfectly transparent and traceable even after many years of inactivity. As a result, the bitcoins donated to the ministry turned out to be practically impossible to sell.

This traceability is the likely reason why, according to independent analyses, bitcoin is not used for illicit activity to any great extent. According to chainalysis.com,[39] only 0.14% of crypto-asset transactions were associated with illicit activity in 2024.

39 https://www.chainalysis.com/blog/2025-crypto-crime-report-introduction/

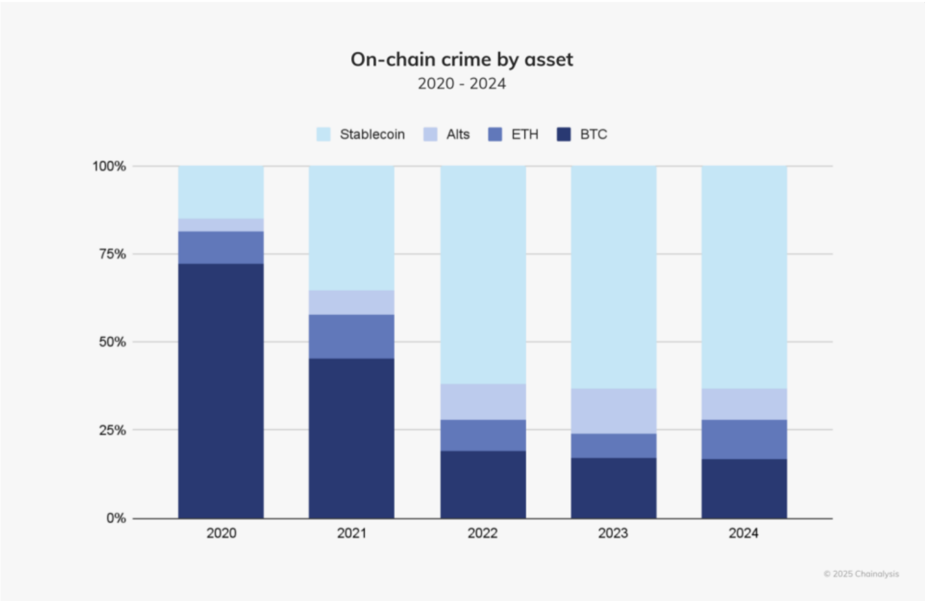
Chart 1-24



Source: chainalysis.com

This surprisingly low share of transactions associated with the underworld is broken down by type of digital asset in the following chart. The data confirm the hypothesis mentioned above that bitcoin is not a suitable instrument for this type of activity. Bitcoin's share in illegal transactions has dropped since 2020, when it stood at 63%, to 17% by 2024, while the share of stablecoins in this segment has been increasing (64%).

Chart 1-25



Source: chainalysis.com

According to UN data, conventional currencies such as the dollar and euro remain the dominant means of payment used by the underworld. We are not trying to suggest that there are bigger problems elsewhere, but rather that the existence of certain adverse phenomena does not automatically mean that all activities involving an instrument used in such phenomena must be restricted at all costs. Attempts to restrict the use of bitcoin for this reason should therefore be viewed similarly to efforts to limit cash transactions, for example.

Clean vs. tainted bitcoins

In practice, bitcoins are distinguished by their cleanliness, or their degree of "contamination", depending on their origin and transaction history. Newly mined bitcoins (referred to as virgin coins) are considered clean. Bitcoins that have passed through exchanges or wallets are examined to determine whether they have been used in illicit activity or transactions on darknet marketplaces, whether they come from extortion (such as via ransomware) or whether they have been used to finance terrorism.

Specialised companies such as Chainalysis and Elliptic evaluate addresses and transactions and assign them a risk score. The degree of contamination is usually referred to as taint and contaminated bitcoins as tainted. The degree of taint reflects how closely the coin is linked to addresses or transactions associated with illicit activity. A high taint score means that the coin either originates directly from illicit activity or has been somehow associated with it.

At the everyday user level, taint does not usually play a role – buyers can obtain virtually clean coins by purchasing on a regulated exchange. Exchanges in both the USA and the EU must strictly comply with AML and KYC regulations, so they carefully examine the origin of incoming bitcoins and refuse to trade tainted ones.

The same applies to OTC trades – the seller is responsible for the origin of the coins and therefore takes great care not to accept bitcoins linked to criminal activity, mixers[40] or the darknet. OTC desks thus largely mirror exchange standards and often require strictly clean bitcoins (this is why they sometimes trade virgin bitcoins with a small premium).

There is no globally recognised technical standard. However, best practices are beginning to emerge. They vary slightly across markets but they share some common features: KYC procedures for clients, AML screening of incoming bitcoins, use of blockchain analytics tools and avoidance of sanctioned addresses, for example.

The relationship between bitcoin and fiat currencies

Central banks may also consider bitcoin controversial because it threatens their monopoly on currency issuance and other functions.

This is clearly a legitimate concern – the mass use of digital assets like bitcoin could undermine the ability of central banks to conduct monetary policy. Another aspect is that bitcoin's high volatility could also jeopardise financial stability if it became more widely used.

In both respects, however, bitcoin is currently very far from able to cause these risks to materialise. Due to its current limitations (especially regarding the number of possible on-chain transactions), it is unlikely to be used on a large scale for everyday transactions and thus replace traditional currencies. This is reinforced by the frequently mentioned high volatility of its price. Bitcoin is therefore likely to remain primarily an asset for storing value, while

40 Also known as tumblers – specialised services that mix potentially identifiable or tainted bitcoins with other coins to obscure their origin or remove their taint.

transactions are likely to be made using CBDCs or stablecoins pegged to conventional currencies.

9. STABLECOINS AND DEPOSIT TOKENS

As the analysis of bitcoin's investment potential naturally raises the broader question of the nature and use of digital assets, it is appropriate to include a brief overview of other types of crypto-assets designed to act not as a speculative investment instrument, but as a stable store of value and a means of settling transactions efficiently.

This section therefore summarises the basic principles and regulatory aspects of stablecoins and deposit tokens, which are stable digital forms of money pegged to existing currency units or bank deposits.

9.1 Characteristics and operating principles

Digital assets with a stable value pegged to a currency or asset

Stablecoins are a type of digital asset that aims to maintain a stable value relative to a chosen reference asset, pool of assets or basket of assets. The underlying asset might be a fiat currency, a commodity or another crypto-asset. Stability is ensured through various mechanisms, typically reserve backing, collateralisation or algorithmic control of supply and demand. Although their name suggests stability, stablecoins may temporarily deviate from their target value in practice depending on the design of, and confidence in, the model.

Unlike cryptocurrencies with freely floating market value, such as bitcoin, stablecoins are not primarily intended as a speculative investment instrument. They serve as a digital representation of existing forms of money or assets and fulfil the functions of a medium of exchange, a store of value and a unit of account with minimised volatility in a distributed ledger environment.

Stability mechanism and main stablecoin models

The basic stabilisation mechanism operates on the principle that each token issued is backed by real assets in a certain ratio, or its price is maintained by an algorithmic system within a predefined model. Issuers of such tokens usually enable a "mint-and-burn" process, i.e. tokens are minted upon receipt of deposits in the reference currency and burned (converted back to fiat) upon receipt of a redemption request. The difference between the market and target price is adjusted through arbitrage incentives that motivate users to buy or sell a token when its price deviates from parity.

According to the type of collateral and the regulatory architecture, we distinguish three main stablecoin models:

- **Fiat-collateralised stablecoins** are the most prevalent model. Their value is backed by reserves held in cash or short-term Treasury bills, which the issuer holds in a 1:1 ratio to the tokens issued. The issuer usually allows holders to convert tokens back into the reference currency and regularly publishes information on the composition and volume of reserves.
- **Crypto-collateralised stablecoins** are backed by other crypto-assets, most commonly ether (ETH), the native currency of the Ethereum blockchain. To account for the volatility of the underlying assets, collateral is usually provided in excess of the nominal value of

the tokens issued (over-collateralisation). These models operate as fully decentralised, without a central issuer, through smart contracts.

- **Algorithmic stablecoins** involve a model where stability is maintained by automatically managing the supply of tokens – through buying or selling tokens or adjusting the quantity in circulation based on predefined rules in the code. These systems aim to achieve parity with the reference currency with no direct backing by real assets. However, after the collapse of TerraUSD in 2022, this approach has lost virtually all credibility and is no longer used in institutional practice.

Technologically, stablecoins are implemented as tokens on public or permissioned (blockchain) networks. The most common standards include ERC-20 (Ethereum), TRC-20 (Tron) and the on-chain standards Solana and Base. These standards ensure compatibility with a wide range of wallets and trading platforms, enabling fast and transparent distribution with no intermediaries.

9.2 Use of stablecoins in practice

Fast and continuous settlement without borders

From both the user and institutional perspectives, the main advantages of stablecoins are efficiency, speed and continuous availability. In an environment where bank settlements occur within limited time windows and cross-border payments may take several days, stablecoins offer an alternative that enables instant transfer of value within seconds – globally and regardless of payment system operating hours.

In practice, stablecoins are primarily used to settle transactions on cryptocurrency exchanges, where they serve as a unit of account and an anchor for trading pairs – for example BTC/USDT (bitcoin against Tether) and ETH/USDC (ether against USD Coin). They allow users to switch quickly between crypto-assets and a digital form of "cash" without having to perform a traditional fiat conversion. For many investors outside the USA, they also provide access to dollar liquidity in environments where traditional banking infrastructure is lacking or is too costly.

Stablecoins as the backbone of the digital economy

A growing share of demand also comes from **decentralised finance (DeFi)** – an ecosystem of financial services operating on distributed ledger technology (DLT), mainly blockchain, without traditional intermediaries such as banks or clearing houses. In these systems, stablecoins act as collateral, a source of liquidity and a transaction settlement instrument in lending and derivatives protocols.

Another significant area is **international payments**, where stablecoins are used for cross-border transfers between businesses and financial institutions at lower cost and with no delays. In this way, stablecoins have become a digital equivalent of the SWIFT standards, but without the structural limitations.

9.3 Regulatory framework

The rapid development of stablecoins has led to the emergence of the first comprehensive regulatory frameworks in major financial jurisdictions in recent years. While in 2021 there was still uncertainty about whether stablecoins should be classified as crypto-assets, electronic money or a special type of debt instrument, the situation is now much clearer.

Regulation: GENIUS Act (USA); MiCA (EU)

In **the United States**, discussions about regulating stablecoin have been going on at the federal level since 2022, resulting in the first comprehensive proposal – the **US Stablecoin Bill (GENIUS Act)**[41] – in 2025. This law defines the term "payment stablecoin" and requires issuers to maintain reserves on a one-to-one basis using cash or highly liquid Treasury bills. The law prohibits fractional collateral models, requires issuers to register and subjects them to oversight by federal authorities (typically the OCC or the Federal Reserve). Issuers must publish monthly reserve reports and ensure independent audits. The goal is to prevent systemic risks and ensure that stablecoins serve as a safe means of payment without threatening the stability of the banking sector.

In **the European Union**, stablecoins are addressed in **MiCA (the Markets in Crypto-Assets Regulation)**,[42] which became partially effective in June 2024 and fully effective in December 2024. MiCA distinguishes between two categories – asset-referenced tokens (ART) and e-money tokens (EMT) – and lays down strict requirements for issuers regarding capital, liquidity management, reserve transparency and consumer protection. Issuers must obtain authorisation from a national supervisory authority, have their registered address in the EU and publish information on their reserves at least monthly. MiCA also prohibits the payment of interest on stablecoin holdings and sets limits on transaction volumes in individual currencies to prevent circumvention of monetary policy.

Other jurisdictions that have introduced their own frameworks include **Switzerland** and **Singapore**. The Swiss regulator FINMA assesses stablecoins individually based on their structure – in practice, most models are classified as a form of electronic money with an emphasis on deposit protection. The Monetary Authority of Singapore (MAS) launched a specific regimen for stablecoins in 2023, requiring full backing, reserve transparency and issuer licensing. This model has often been cited as a model approach to regulation in Asia.

9.4 Ensuring stability and security

Stability relies on reserves and transparency

The security of stablecoins is directly dependent on the quality, transparency and structure of the reserves held by their issuers to maintain stability of value. Reserves in fiat-collateralised models are kept with banks and custodians, usually in the form of cash and highly liquid, low-risk assets such as short-term government securities. This minimises issuers' credit and market risk and ensures they are able to settle token redemptions instantly.

For example, **USD Coin (USDC)**, issued by Circle and managed in cooperation with Coinbase, is fully backed by reserves held at US banks and in Treasury bills. The company publishes monthly reserve attestations conducted by the independent auditor Deloitte.[43] Similarly, **Tether (USDT)** publishes quarterly reports on the composition of its reserves, including exposures to US Treasuries, bank deposits and reverse repurchase agreements.[44] Although Tether's transparency has long been criticised, the

41 US Congress: GENIUS (Guiding and Establishing National Innovation for U.S. Stablecoins) Act – Payment Stablecoin Bill (2025); see https://congress.gov

42 European Commission: Markets in Crypto-Assets Regulation (MiCA); see https://finance.ec.europa.eu

43 Circle: USDC Transparency Reports; see www.circle.com

44 Tether: Reserves and Assurance Reports; see www.tether.to

issuer has significantly improved the quality of the information disclosed and audit standards in recent years.

Risks: issuer, liquidity, regulation, technology

From a **risk management** perspective, four areas are most frequently discussed for stablecoins:

- **issuer risk** concerning potential insolvency or fraudulent handling of reserves,
- **liquidity risk** linked to sudden mass redemptions of tokens,
- **regulatory uncertainty** arising from changes in the interpretation of the legal nature of stablecoins,
- **technological and operational risk** such as loss of private keys or errors in smart contracts.

On the other hand, stablecoins offer the advantage of full traceability and instant verifiability of token movements on the blockchain. This makes them more auditable than traditional off-chain systems.

9.5 Examples and forms of implementation

The market is dominated by USDT and USDC

Two projects – **Tether (USDT)** and **USD Coin (USDC)** – dominate the stablecoin market, together accounting for more than 90% of the total market capitalisation.

USDT is the oldest and most liquid stablecoin in the world. Its strength lies in broad acceptance across exchanges and DLT ecosystems; its weaknesses include limited reserve transparency and the legal structure of the issuer based outside US jurisdiction. Nevertheless, Tether maintains a key position thanks to its liquidity and availability on more than a dozen blockchains.

USDC, managed by Circle, is a model example of a fully regulated stablecoin with strong oversight and audit transparency. Reserves are held exclusively in cash and highly liquid government securities with minimal credit risk, and the issuer has a clearly defined legal relationship with token holders.

Deposit tokens: tokenised bank deposits

In addition, **deposit tokens**, representing a digital – tokenised – form of bank deposits, have started to emerge alongside public stablecoins. Each such token corresponds to a specific client deposit at a bank and is fully backed by the bank's obligation to the token holder. Unlike stablecoins issued by non-bank entities, deposit tokens are part of the regulated banking system and subject to the same rules as traditional deposit products.

JPM Coin: the first practical implementation

The best-known implementation of this concept is **JPM Coin/JPM Deposit Token (JPMD)**[45] developed by J.P. Morgan. This system enables instant settlement of payments between the bank's institutional clients via an internal digital network, which is accessible only to approved participants and thus functions as a closed system for regulated financial institutions.

Tokenised deposits: digital deposits on DLT infrastructure

Building on this principle is the concept of **tokenised deposits**, developed by many large banks and technology partners within initiatives such as the **Kinexys Digital Payments Network**. A tokenised deposit is a digital representation of a bank deposit issued by a bank on DLT infrastructure, where each token corresponds to a real obligation of the bank to the holder

45 J.P. Morgan: Deposit Tokens – FAQ and Concept Overview; see www.jpmorgan.com/kinexys

and is fully backed on its balance sheet. This ensures legal certainty and deposit protection in accordance with applicable banking regulations.

From a technical perspective, these tokens are issued on a permissioned ledger – a closed environment accessible only to authorised institutions – allowing full traceability, compliance and instant transaction settlement without counterparty risk. The Kinexys network and similar projects are designing architectures enabling interoperability between banks, thus allowing real-time interbank transfers to be made at significantly lower cost than in traditional clearing systems.

Use: real payments, asset settlement, integration with CBDC

Tokenised deposits find practical application primarily in interbank transaction settlement, real-time corporate payments and on-chain settlement of tokenised assets. Because they are fully backed on banks' balance sheets, they are not considered a new form of money but a technological extension of existing deposit accounts into the digital DLT environment.

Unlike stablecoins, which are issued by non-bank entities and freely traded on public markets, tokenised deposits remain part of the regulated banking system. They thus represent a practical tool for settling transactions more efficiently and linking bank liquidity with the digital economy, as well as a potential bridge to future forms of digital money, including CBDC, i.e. digital currency issued directly by central banks.

10. CONCLUSION

Bitcoin can now be considered a mature and viable project, despite various well-known problems that have accompanied it in the past and persist to this day. Over more than fifteen years of existence, it has proven to be a resilient technology whose core principles – decentralisation, open access and a strictly defined "monetary" policy – have not been undermined by technical problems or by attempts at regulation or restriction by governments and supranational authorities.

Bitcoin is gradually establishing itself as a recognised asset in the broader financial ecosystem. Its role, however, is evolving – from an experimental digital currency and a speculative asset towards an established store of value and a technological standard underpinning a range of new services and financial products. Although the exceptional returns seen in its early years cannot be expected to repeat, a significant part of the market expects bitcoin to move gradually into the financial mainstream and gain broader institutional acceptance.

There is the option to combine testing with preparation for external "co-custody"

From the central bank's perspective, we consider it appropriate now to start testing the technology and assessing it in detail. Although much is known in theory, only practice will reveal the details and difficulties of day-to-day operation. Testing should help the CNB to better understand the potential, limitations and risks of technologies related to bitcoin and blockchain. As regards the broader inclusion of bitcoin in reserves, we regard the co-custody model as the most suitable option. This model would enable us to use the infrastructure built during the testing phase later on for co-signing transactions. In other words, the testing phase would also serve as preparation for later routine operation. At the same time, however, the advantages of the use of external custodians (additional security in particular) would be maintained.

Digital assets with a stable value pegged to a currency or deposit

Alongside bitcoin, which is the best-known digital asset, attention should also be paid to stablecoins and deposit tokens. These instruments try to eliminate the volatility of cryptocurrencies by being pegged to the value of a traditional currency or a bank deposit. While stablecoins, such as USDC and Tether, are issued by non-bank entities and bear issuer risk, deposit tokens represent a regulated digital form of bank deposits and may function as a bridge between the traditional financial sector and tokenised infrastructures. Their development is therefore also relevant from the central bank's perspective.

GLOSSARY

Address (bitcoin address): An alphanumeric string (e.g. bc1q... or 1A1z...) that serves as a public identifier for receiving bitcoins. It is derived from a public key.

BIP (Bitcoin Improvement Proposal): A proposal for improving bitcoin. Each BIP defines protocol changes, standards or technical specifications (e.g. BIP-32 – hierarchical wallets, BIP-39 – mnemonic words, BIP-322 – message signing).

Bitcoin network: A decentralised network of peer-to-peer nodes that collectively verify, validate and propagate bitcoin transactions.

Block: A unit in which new transactions are recorded in the blockchain. A new block is created approximately every 10 minutes.

Block subsidy (mining reward): The reward a miner receives for finding a block, currently BTC 3.125 per block. This reward is the sole source of issuance of new bitcoins and is halved approximately every four years.

Blockchain: A public, distributed database of all bitcoin transactions, organised into blocks linked in a chronological chain.

CBDC: Digital money issued by a central bank. Does not necessarily rely on blockchain or other technology.

Custody/self-custody: A method of storing cryptocurrency. Custody means that keys are held by a third party; self-custody means that the user alone holds private keys.

Digital signature: A cryptographic technique used to verify the authenticity and integrity of a message, software or a digital document.

Full node: A computer connected to the bitcoin network that stores the complete blockchain history and independently verifies all transactions and blocks according to the network's consensus rules.

Halving: An event that occurs every 210,000 blocks (approximately every 4 years) during which the reward for mining a block is reduced.

Hard fork: An incompatible protocol change. Older, non-updated nodes reject blocks in the new format, causing the network to split into two independent branches unless all nodes upgrade. Example: Bitcoin Cash.

Hardware wallet: A physical device (e.g. Trezor, Ledger) for securely storing private keys offline.

Hash: The output of a cryptographic function (e.g. SHA-256) that uniquely represents input data using a significantly smaller amount of data. The function is one-way, i.e. the input data cannot be reconstructed from the hash.

HSM (hardware security module): A specialised device for securely generating and storing keys – used in institutional environments.

Lightning Network: A layer built on top of bitcoin designed for fast and low-cost micropayments. It enables near-instant transactions off the main blockchain.

Mempool: A temporary space where unconfirmed transactions wait before being included in a block.

MPC (multi-party computation): A key management method where a key is split among multiple parties that interact without the need to hold the full key in one place. This enhances security and flexibility.

Multisig: A security method requiring more than one signature to authorise a transaction (e.g. two out of three keys).

Node: A computer running bitcoin software and participating in network operation, primarily by verifying transactions and blocks. A node can be either a full node, which stores a complete copy of the blockchain and fully verifies all transactions, or a light node, which works only with block headers and relies on data from full nodes.

Off-chain: Activities or transactions off the main blockchain (i.e. not recorded in mined blocks).

On-chain: Transactions or data recorded directly on the blockchain.

Permissionless: A public and open blockchain that every participant can read and where all participants can take part in transactions and access does not depend on approval by any entity. The blockchain versions used by bitcoin and Ethereum are examples of such a blockchain.

Private key: A secret piece of information that enables its holder to operate with bitcoins. It must be securely protected. The private key serves as a unique identifier of the owner of a wallet (or generally storage) with bitcoins.

Proof-of-work: A consensus algorithm used by miners to validate blocks by solving a computationally intensive mathematical problem that consumes large amounts of electricity.

Public key: The public component of asymmetric cryptography, used to create an address and verify a signature.

Satoshi: The smallest indivisible unit of bitcoin, equal to one hundred millionth of a bitcoin (10^{-8}). Often abbreviated to “sat”, e.g. 5,000 sats.

Seed/recovery phrase: A mnemonic phrase (e.g. 12 or 24 words) used to restore an entire wallet. Must be kept perfectly secure. Losing it means risking theft of the entire wallet balance.

Soft-fork: A backward-compatible protocol change. Older, non-updated nodes still accept new blocks as valid but may reject some transactions. Example: SegWit.

Stablecoin: A type of cryptocurrency whose value is pegged to another stable asset, most often a currency (such as the US dollar – USDT).

Taproot: A bitcoin upgrade that improves privacy, efficiency and scalability through simplified script logic.

Tokenised assets: Digital tokens representing ownership or property rights to real assets (e.g. securities, funds, commodities or real estate). They allow these assets to be traded, settled and managed on DLT with greater efficiency and transparency.

Tokenised deposits/deposit tokens: Digital representations of bank deposits issued by a bank on DLT infrastructure. Each token corresponds to a real deposit on the bank’s balance sheet, is fully backed by an obligation of the bank, and is subject to banking regulation. Enables fast and secure payment settlement in a regulated environment.

Transaction (bitcoin): A record on the blockchain that transfers ownership of bitcoins from one address to another.

UTXO: Unspent transaction output. UTXOs form the basic units of a bitcoin balance.

Wallet: Software or a device that enables management of bitcoin addresses, keys and transactions. Wallet types include:
– Hot wallet: connected to the internet (e.g. mobile apps, web wallets), suitable for frequent use, but less secure.
– Cold wallet: not connected to the internet (e.g. hardware wallets, paper wallets), suitable for long-term storage.
Each wallet generates/manages one or more bitcoin addresses used as destinations for receiving bitcoins.

Whitepaper: The original 2008 document by Satoshi Nakamoto describing the principle of bitcoin.