Analýza možností investic do dalších tříd aktiv: část I. digitální aktiva

Obsah

1. Bitcoin – úvod 3
2. Popis trhu s bitcoinem 5
3. Formy investice 7
4. Risk-return charakteristiky 8
5. Možnost implementace v ČNB 21
6. Bitcoin jako součást DR? 25
7. Externí studie 31
8. Komunikace 41
9. Stablecoiny a deposit tokeny 46
10. Závěr 50
Glosář pojmů 52

1. BITCOIN – ÚVOD

Bitcoin je prvním a dosud nejznámějším digitálním nástrojem určeným k provádění bezpečných transakcí a uchování hodnoty. Často je proto označován za digitální měnu. Hned v úvodu je však důležité zdůraznit, že tzv. *CBDC* – neboli digitální měny vydávané centrálními bankami – s bitcoinem ani technologiemi, na nichž je založen, nemusí mít (a často ani nemají) nic společného.

Vznik bitcoinu: 2008

Bezpečnost bitcoinu je založena na teorii kryptografie a na ní postavených algoritmech[1]. Základní koncept byl vytvořen v roce 2008 vývojářem (či možná skupinou vývojářů) vystupujícím pod pseudonymem Satoshi Nakamoto[2]. Systém samotný odstartoval svou existenci vytvořením tzv. genesis bloku v roce 2009. Deklarovaným cílem vzniku bitcoinu bylo umožnit provádění transakcí zcela bez účasti finančních institucí a dalších zprostředkovatelů. Bitcoin je do dnešních dnů považován za alternativu k tradičním měnám, která je odolná vůči regulaci, sankcím a dalším omezením ze strany státu a regulátorů, inflaci (bitcoinů bude konečný počet, což povede k trvalé deflaci) a umožňuje úplnou anonymitu.

Co je to blockchain?

Ekosystém bitcoinu je založen na decentralizované síti jednotlivých uzlů tvořících tzv. *blockchain*. Pojem blockchain se ovšem používá i ve významu datové struktury, řetězce bloků, které jednotlivé uzly této sítě udržují. V praxi tato nejednoznačnost nehraje roli, termín blockchain je používán v obou těchto významech. Tedy označuje jak počítačovou síť, na jejíchž jednotlivých uzlech (tzv. *nodech*) je řetězec bloků udržován, tak i tento samotný řetězec obsahující záznamy o veškerých provedených operacích.

Bitcoin a blockchain jsou považovány za tzv. *permissionless* systém, který je otevřený pro kohokoli, účast není nijak schvalována, připojit k síti, ať už jako uživatel či jako provozovatel uzlu, se může každý. Stejně tak nejsou nějakou centrální autoritou jakkoliv schvalovány jednotlivé transakce, ty jsou ověřovány automaticky na základě pravidel protokolu.

Protokol: jádro bitcoinu

Protokol tvoří vlastní fundament bitcoinu. Popsán je přímo ve zdrojovém kódu (tzv. Bitcoin Core, viz https://github.com/bitcoin/bitcoin) a definuje celou řadu pravidel[3]:

- formát transakcí (struktura jednotlivých polí, náležitosti elektronického podpisu, jak se ověřují),
- tvorbu bloků (definuje jejich strukturu, maximální velikost, časové razítko, pořadí),
- pravidla potvrzování (tzv. těžba, její obtížnost atd.),
- konsenzus (způsob, jak se uzly dohodnou na „správném“ stavu blockchainu),
- specifikaci síťové komunikace (např. šifrovací algoritmy),
- ekonomické aspekty (odměna za těžbu, halving, maximální počet bitcoinů).

Účelem této analýzy není detailně popisovat veškeré teoretické a technické detaily fungování bitcoinu. Pro usnadnění uvádíme v příloze kapitoly 1

1 Hashovací funkce SHA-256, digitální podpisy založené na eliptických křivkách atd.

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

3 Strukturovaný popis protokolu, historie, principy jsou uvedeny na Bitcoin Wiki – https://en.bitcoin.it/wiki/Main_Page

stručný glosář. Text se pak obecně snažíme udržet ve formě, která je pochopitelná bez podrobné znalosti teoretických základů těchto technologií. Volně dostupná je však celá řada materiálů, které na různé úrovni odbornosti a detailu problematiku vysvětlují[4].

Bitcoin – víra a determinanty jeho hodnoty a existence

V praxi je vnímání bitcoinu různé. Od kontroverze až po příležitost. Jak vnímat bitcoin v prostředí správy devizových rezerv? Pokud není zcela odmítnut z principiálních a dalších důvodů, lze bitcoin považovat za obchodovatelnou hodnotu (tj. existuje trh a existuje i cena), jež je determinována vírou, že i) bude i nadále existovat, ii) její cena poroste, iii) lze ji použít v dalších transakcích, tedy že někdo jiný bitcoiny akceptuje ve víře, že je bude moci zase použít.

Bitcoin není závazkem, nefiguruje v ničích pasivech, vzniká coby produkt „výrobního“ procesu, přičemž technologie a náklady na technologii lze považovat za jistou formu závazku producentů.

Není jednoduché tuto víru, o kterou se ovšem opírají i fiat peníze, vyhodnotit z hlediska existence (default risk), z hlediska stability ceny (market risk) a z hlediska operačních rizik (úschova, právní rámec atp.). K bitcoinu nelze nalézt komplexní ekvivalent; lze však nalézt ekvivalenty k jeho jednotlivým vlastnostem, jako jsou unikátnost, atraktivita, popularita, funkčnost, nezávislost.

Historie trhu s bitcoinem velmi krátká

Slabinou bitcoinu je jeho relativně krátká historie. Všechny důkazy a argumenty PRO se odvolávají na to, co se stalo během tohoto omezeného období, resp. co se během něj ještě nestihlo stát. Tato krátká historie naznačuje, že aktuální cena bitcoinu zřejmě není zdaleka konečná (jak směrem dolů, tak směrem nahoru). Což je umocněno faktem, že systém je uzavřený, bitcoiny se nespotřebovávají (byť část z nich se postupně ztrácí) a jednou dokonce přestanou přibývat.

Struktura textu

Text je strukturován do několika kapitol. V kapitole č. 2 krátce popisujeme historii a současnost trhu s bitcoinem. V kapitole č. 3 popisujeme formy možné investice. V kapitole č. 4 se zabýváme tím nejjednodušším, tedy statistickou analýzou výnosů a rizikových parametrů bitcoinu. Vše, co následuje, je svou povahou podstatně komplexnější a odpovědi na kladené otázky jsou často bohužel nejednoznačné. Kapitola č. 5 obsahuje analýzu toho, zda a jak by tuto investici bylo možné provést v prostředí ČNB. Kapitola č. 6 se zabývá možností zahrnout bitcoin do devizových rezerv a s tím spojené teoretické a praktické otázky. Případná investice do bitcoinu přináší celou řadu rizik, které u „konvenčních“ tříd aktiv neexistují, k jejich analýze proto byly zadány dvě externí studie – jejich výsledky shrnujeme v kapitole č. 7 a pokoušíme se zde odpovědět na nejsložitější otázky, které se v souvislosti s bitcoinem nejčastěji vyskytují. Jako přílohu ke kapitole uvádíme krátký glosář, ve kterém krátce vysvětlujeme hlavní používané pojmy.

---

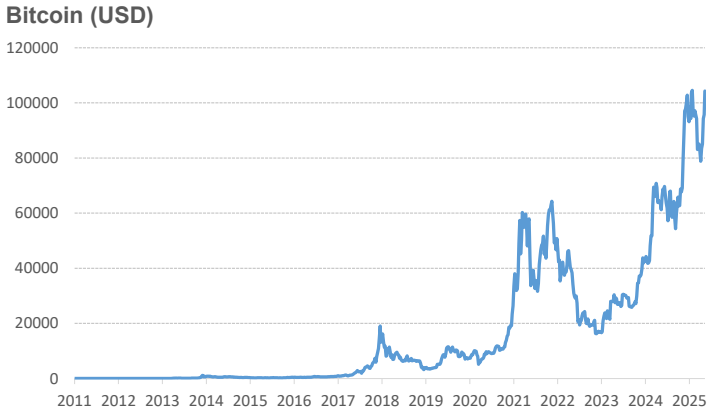
4 Oficiální web, https://bitcoin.org/cs/jak-to-funguje
Andreas M. Antonopoulos – Mastering Bitcoin, https://github.com/bitcoinbook/bitcoinbook/blob/develop/BOOK.md
bitcoin na Investopedia, https://www.investopedia.com/terms/b/bitcoin.asp

2. POPIS TRHU S BITCOINEM

Krátká historie trhu s bitcoinem

Bitcoin ještě po vytvoření prvotního bloku neměl komerční hodnotu, sloužil převážně pro experimentální účely. Za první komerční transakci se považuje nákup dvou pizz za 10 000 BTC provedený 22. května 2010[5]. Krátce nato vzniká první burza (bitcoinmarket.com), 1 bitcoin se obchoduje za 0,003 USD. V následujících letech se obchodování s bitcoinem rozvíjí, vznikají další burzy, mj. Mt. Gox, která se stává dominantním místem obchodu. Mt. Gox krachuje v roce 2014 a pro bitcoin nastává období stagnace. Trh znovu ožívá až v roce 2017, kdy bitcoin koncem roku poprvé dosáhne hranice 20 000 USD. Během let 2020 až 2021 se objevují první velcí hráči (např. Tesla a MicroStrategy) a vznikají první bitcoinové ETF. V roce 2021 přijímá El Salvador bitcoin jako zákonné platidlo[6]. Trh i nadále zažívá obrovskou volatilitu – po dosažení nových maxim pravidelně následují razantní poklesy. Zdá se však, že body obratu (jak dočasná minima, tak nové rekordní hodnoty) v průběhu času trvale rostou. Po krachu FTX v listopadu 2022 klesá bitcoin až pod 16 000 USD, dočasně jistě působí také narůstající snaha ze strany finančních regulátorů vymezit i na tomto trhu pravidla. Ani to však nezabránilo obnovení důvěry a dalšímu růstu popularity bitcoinu v letech 2024 a 2025, velmi pozitivní roli jistě sehrálo spuštění bitcoinových ETF v USA.

Graf 1-1



zdroj: Bloomberg, graf ČNB

Shrnutí současného postavení bitcoinu:

spíše než platební prostředek se z bitcoinu stala alternativa pro uchování hodnoty

Bitcoin se etabloval jako alternativní digitální aktivum, které někteří investoři vnímají podobně jako např. zlato – tedy jako uchovatele hodnoty v nejistých časech. Zůstává velmi volatilní, i přesto se v omezené míře stává součástí institucionálních portfolií. V některých jurisdikcích vznikly první regulované ETF fondy orientované na bitcoin. Jeho decentralizovaná povaha, omezená nabídka a nezávislost na centrálních bankách z něj dělají nástroj, který někteří investoři vyhledávají jako zajištění v době inflace a geopolitické nestability. Na druhou stranu se však dosud nestal široce používaným platebním prostředkem a v tomto ohledu jeho pozice spíše slábne. Nehledě

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

6 Na konci ledna 2025 Salvador upravil tzv. „Bitcoin Law“: zákon odstraňuje povinnost akceptovat bitcoin (např. obchodníci už nejsou nuceni ho přijímat). Bitcoin přestává být používán jako měna ve veřejných transakcích, tedy nelze jím platit daně nebo ukládat dluhy proti státu. Zůstává sice tzv. „legal tender“ v legislativním jazyce – ale je to formální, nikoliv povinné.

na existenci různých modifikací[7], které usnadňují placení pomocí bitcoinu, jej v této úloze nahrazují spíše tzv. *stablecoiny*. Vyloučit nelze také pokračující snahy o nejrůznější regulatorní omezení. Celkově je dnes bitcoin vnímán spíše jako strategické aktivum než jako běžný platební prostředek.

2.1 Tržní infrastruktura bitcoinu

Tržní infrastruktura bitcoinu se v řadě ohledů podobá klasickým finančním trhům, ale vykazuje také zásadní rozdíly vyplývající z její decentralizované povahy.

Decentralizovaná povaha

Bitcoin nemá vlastní centrální clearingovou ani emisní instituci, centrální banku či jinou autoritu, která by řídila platební styk nebo určovala množství oběživa. Veškeré transakce probíhají přímo v blockchainu, kde jsou potvrzovány účastníky bitcoinové sítě, tedy prostřednictvím tzv. *těžařů*, s využitím mechanismu *proof-of-work*. To představuje zásadní rozdíl oproti klasickým měnám, jejichž páteř tvoří centrální banka a síť bankovních platebních systémů.

Burzy a obchodní platformy

Namísto klasických devizových trhů funguje pro bitcoin síť krypto burz (Binance, Coinbase, Kraken aj.), OTC desků a decentralizovaných burz (DEX). Ty zajišťují likviditu a cenotvorbu. Na rozdíl od tradičního FX trhu, kde je likvidita soustředěná a regulovaná, je u bitcoinu roztříštěná mezi stovky platforem různé kvality.

Custody a clearing

V klasických měnách hraje klíčovou roli centrální banka jako clearingová instituce. U bitcoinu je custody a vypořádání přenesené na soukromé subjekty: burzy, specializované custodiany nebo samotné uživatele, kteří drží privátní klíče.

Likvidita

Bitcoin je zdaleka nejlikvidnější kryptoměna. Denní spotový objem obchodů dosahuje desítek miliard USD, což jej přibližuje menším národním měnám. Stále však výrazně zaostává za hlavními měnovými páry (USD/EUR, USD/JPY), kde objemy přesahují biliony USD denně. Likvidita bitcoinu umožňuje provádět obchody až ve stovkách milionů dolarů, ale při velkých objemech zůstává vliv na cenu vyšší než na FX trzích.

Tržní infrastruktura bitcoinu stojí na decentralizovaném blockchainu a síti soukromých burz a custodianů, zatímco klasické měny využívají centrálně řízenou infrastrukturu, často navázanou na centrální banky. Z hlediska likvidity je bitcoin sice nejrozvinutějším digitálním aktivem, hlavním světovým měnám se ale stále nemůže ani vzdáleně rovnat.

Za zmínku jistě stojí, že existuje celá řada projektů, ve kterých centrální banky, ale též soukromé instituce, využívají technologie tokenizace a blockchainu. Za všechny jmenujme alespoň projekt Agora od BIS/IIF, jehož cílem je zlepšit přeshraniční platební styk[8], a projekty Pontes/Appia ECB zaměřené na propojení distribuovaných účetních knih a systému Target2[9].

7 Např. Lightning Network na tzv. Level-2 sítě umožňuje rychlé a levné transakce.

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 Trh s deriváty na bitcoin

Trh s deriváty je již rozvinutý a nejčastěji organizovaný na burzách

Trh s deriváty na bitcoin je dnes velmi rozvinutý a nabízí nástroje srovnatelné s tradičními finančními trhy. Nejvýznamnější jsou futures kontrakty, které se obchodují jak na regulovaných trzích (např. CME v USA), tak na specializovaných burzách (Binance, OKX, Bybit). Umožňují jak zajištění proti cenovým výkyvům, tak vybudování expozice na změnu ceny bitcoinu a tvoří páteř institucionálního obchodování s bitcoiny. Ještě populárnější jsou tzv. perpetual futures (neboli *perps*) – kontrakty bez exspirace. Díky vysoké likviditě jsou dnes nejpoužívanějším bitcoinovým derivátem.

Existují ale i OTC deriváty

Vedle toho existují také forwardy uzavírané bilaterálně na OTC trhu. Ty se často používají k zajištění budoucích příjmů těžařů či fondů. Opce (zejména vanilla call a put) se obchodují na CME i specializovaných burzách (Deribit) a umožňují vytvářet komplexní strategie.

Repo trh v klasickém smyslu neexistuje, funguje ale alternativa

Pokud jde o nástroje podobné repo trhu, klasický standardizovaný „repo market“ na bitcoin neexistuje. Přesto funguje BTC lending a borrowing, kdy si instituce či investoři půjčují bitcoiny proti zástavě (typicky stablecoinů nebo fiat měny). Principálně je tento obchod velmi podobný repu, nicméně jde o bilaterální či burzovní půjčky, nikoli o jednotný mezibankovní trh.

Specifickou kategorií jsou i termínované transakce (deliverable forwards), které se používají zejména na OTC trhu. Umožňují dohodnout pevnou cenu a datum dodání BTC, často se používají jako nástroj zajištění.

Celkově je trh s deriváty na bitcoin pestrý – od likvidních futures a „perps“ na burzách, přes opce, až po specializované forwardy a repo-like lending obchody. Každý z nástrojů má jinou roli: spekulace, hedging, financování či arbitráž.

Samozřejmě však prozatím stále platí, že ve srovnání s deriváty na klasické měny je trh s deriváty na bitcoin výrazně menší a méně likvidní.

3. FORMY INVESTICE

Přímá investice

Pro většinu investorů je hlavní možností jak investovat do bitcoinu *přímá investice*. Transakce probíhají na burzách (Binance, Coinbase, Kraken atd.), v posledních letech se však rozvinul také OTC trh (Goldman Sachs, JP Morgan, Morgan Stanley, Standard Chartered, Nomura atd., tedy standardní protistrany ČNB), který představuje vhodnější platformu pro obchody prováděné ve větších objemech. Vznikají též brokeři specializovaní na digitální aktiva (Cumberland/DRW, Galaxy Digital, Jump Trading, B2C2); brokery ČNB při obchodování obvykle nevyužívá, nicméně toto je vlastní rozhodnutí centrální banky, které je možné v případě potřeby revidovat.

Self-custody vs. externí custody

V případě přímé investice se za nejdůležitější otázku považuje jak bitcoiny uchovávat. Nabízí se možnost držet bitcoiny pomocí vlastních prostředků (tzv. self-custody), nebo prostřednictvím dalších institucí (burzy, tradiční či specializovaní custodiani).

Pro self-custody v malých objemech drobní investoři typicky využívají softwarové peněženky, pro účely ČNB však toto řešení můžeme z bezpečnostních důvodů zcela vyloučit. Pro větší držené objemy se pak nabízejí specializovaná hardwarová zařízení (typicky tzv. HSM, hardware

security module, v detailu viz kapitolu 5.2), která umožňují bezpečnou správu privátních klíčů.

Přímou investici lze kombinovat i se službami externích custodianů. Ty dnes nabízí celá řada tradičních institucí, mimo jiné BNY, Fidelity Digital Assets, State Street Digital, ZKB atd., existují i specializované nové instituce zaměřené jen na digitální aktiva, zejména Coinbase Custody. Externí custody nabízí celou řadu výhod, jež jsou detailně popsány v kapitole 5.3).

Nepřímá investice: ETF (dražší), deriváty

Do bitcoinu lze dnes investovat i *nepřímo*. Za hlavní takovou možnost se považují burzovně obchodovatelné fondy (ETF), jež představují tradiční typ instrumentu, který ČNB již dnes využívá zejména při správě akciového portfolia, a je tedy na jeho použití okamžitě připravená. Za hlavní fondy se dnes považují Blackrock iShares Bitcoin Trust (IBIT) a Grayscale Bitcoin Trust (GBTC). Hlavní nevýhodou použití ETF jsou poplatky, GBTC účtuje 1,5 %, IBIT 0,25 %, což v případě větších spravovaných objemů znamená částky vyšší, než by představovaly případné náklady na externí custody služby.

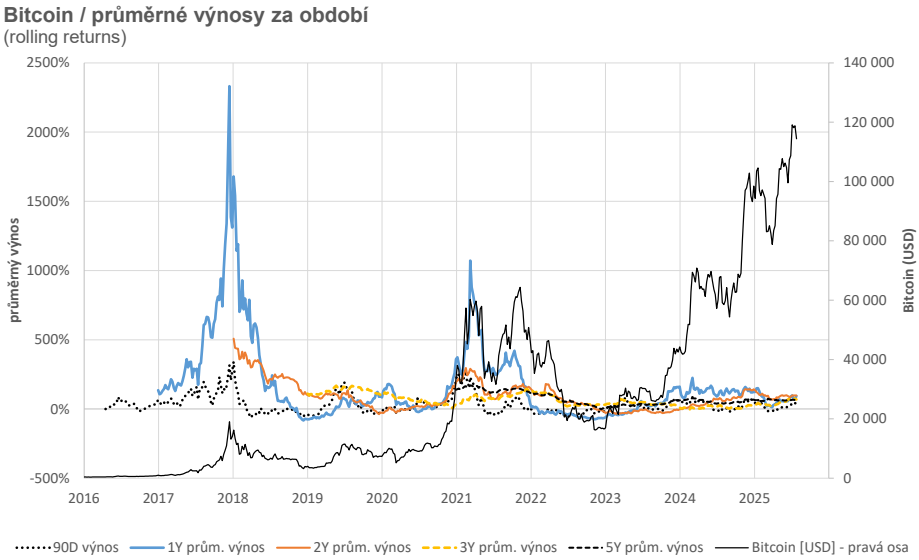
Existují ovšem i další nepřímé možnosti, zejména deriváty (opce, futures apod.) obchodované na specializovaných burzách, Binance, Bybit, Deribit atd., některé banky dnes již nabízejí i total return swapy na bitcoin. Někteří investoři pak z nejrůznějších (často regulatorních) důvodů volí expozici na firmy, které mají ve své bilanci značný podíl bitcoinu a jejichž akcie tak vývoj ceny bitcoinu následují (zejm. Strategy – dříve MicroStrategy[10]).

4. RISK-RETURN CHARAKTERISTIKY

Výnosy a volatilita spojená s bitcoinem se vymykají srovnání s konvenčními aktivy – vzhledem k růstu hodnoty z 0,3 centu (!) na počátku své existence až na současné hodnoty nad 100 000 USD a s tím spojeným růstem o „miliony procent“ je nutná při práci s příslušnými daty velká opatrnost. Více než u jakýchkoliv jiných aktiv zde platí upozornění, že minulá výkonnost není zárukou budoucích výsledků. I z tohoto důvodu uvádíme historické výnosy bitcoinu v následujícím textu jen pro ilustraci a zdůrazňujeme, že bychom podobné hodnoty neměli považovat za budoucí očekávané výnosy. Toto je však typické pro většinu nově vznikajících trhů a hospodářských odvětví – počáteční boom se již nikdy nebude opakovat. Trh čeká spíše ustálení, pokles volatility, ale také výkonnosti.

10 Akcie Strategy (ticker: MSTR) však mají ještě vyšší volatilitu, než samotný Bitcoin.

Graf 1-2



Zdroj: data Bloomberg, kalkulace a graf ČNB

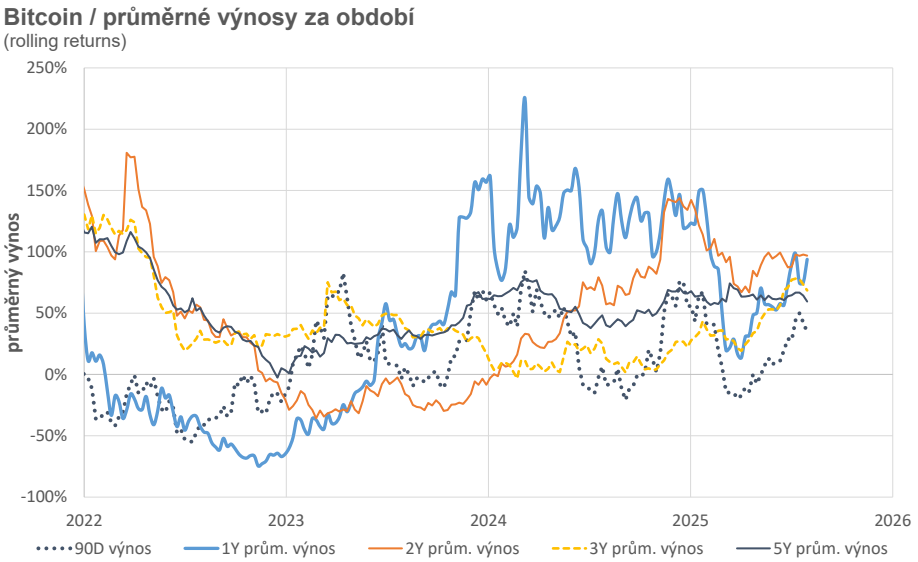
Růst BTC o tisíce procent – jednorázová událost spojena s velmi nízkými cenami

Jak je z grafu výše patrné, v období 2017 až 2018 dosahovaly roční změny ceny bitcoinu i více než 2000 %, důvodem je přitom růst cen z velmi nízkých hodnot (koncem roku 2016 činila cena bitcoinu méně než 1 000 USD). Toto období tedy z našich analýz záměrně vynecháváme a soustředíme se spíše na období až po této epizodě.

Rolling výnosy: 3leté a 5leté horizonty od roku 2020 jen v kladných hodnotách

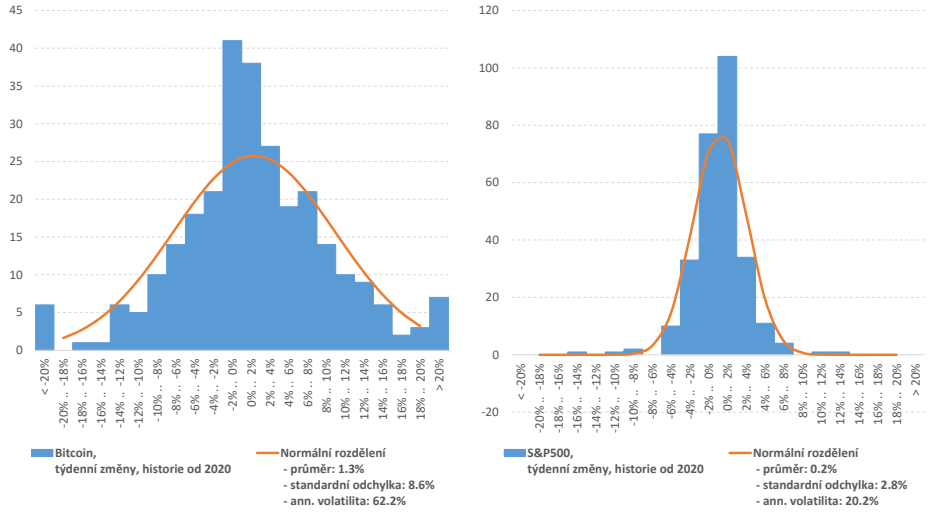
Na grafu níže jsou uvedena stejná data, ale pouze za období začínající rokem 2022. Pozoruhodné je, že ačkoliv výnosy spojené s držením bitcoinu v kratších horizontech (90 dní, 1 rok) zaznamenaly poměrně dlouhá období záporných hodnot, všechny průměrné výnosy spojené s 3letým a 5letým horizontem byly kladné. V tomto ohledu je cenový vývoj bitcoinu obdobný jako u akcií, kde se pravděpodobnost záporného výnosu také v delším horizontu významně snižuje.

Graf 1-3

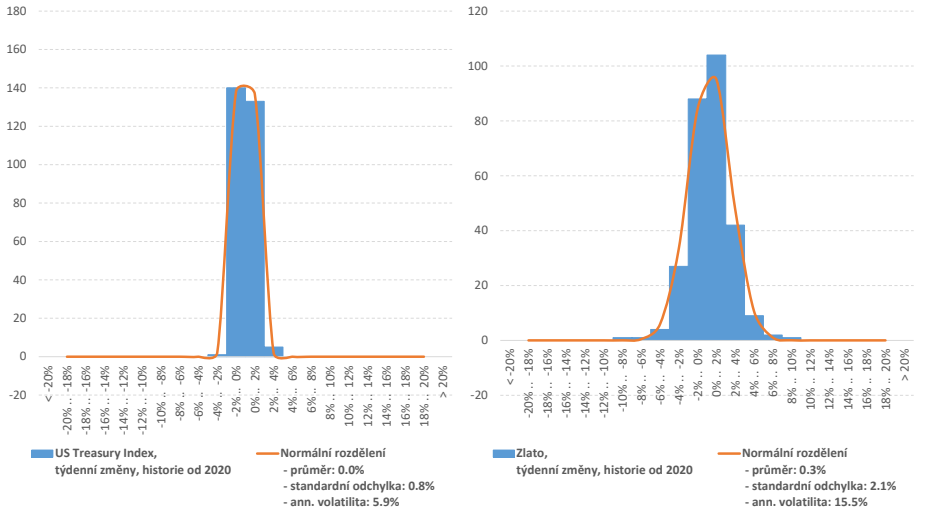


Zdroj: data Bloomberg, kalkulace a graf ČNB

Grafy 1-4, 1-5 – histogramy týdenních změn



Grafy 1-6, 1-7 – histogramy týdenních změn



Zdroj: data Bloomberg, S&P, ICE, kalkulace a graf ČNB

Zabývali jsme se též teoretičtějším studiem statistických vlastností cen bitcoinu. K asi nejzajímavějším poznatkům jsme dospěli z hlediska analýzy tvaru rozdělení výnosů. Za hypotézu jsme zvolili předpoklad, že denní změny cen bitcoinu budou distribuovány podle tzv. stabilního rozdělení (rozdělení typu „fat tail“) a srovnali jsme ho pro tyto účely s vývojem indexu S&P500, kde jsme opět předpokládali stabilní rozdělení. Ve výrazné většině let ze sledovaného období 2011 až 2025 nedošlo k odmítnutí hypotézy o tvaru rozdělení, jak u BTC, tak u akcií. Zároveň bylo zjištěno, že bitcoin je v posledních několika letech co do statistických vlastností velmi blízký akciím, ale škála výnosů a ztrát je samozřejmě řádově rozdílná.

4.1 Volatilita

Vysoká, nikoliv extrémní volatilita

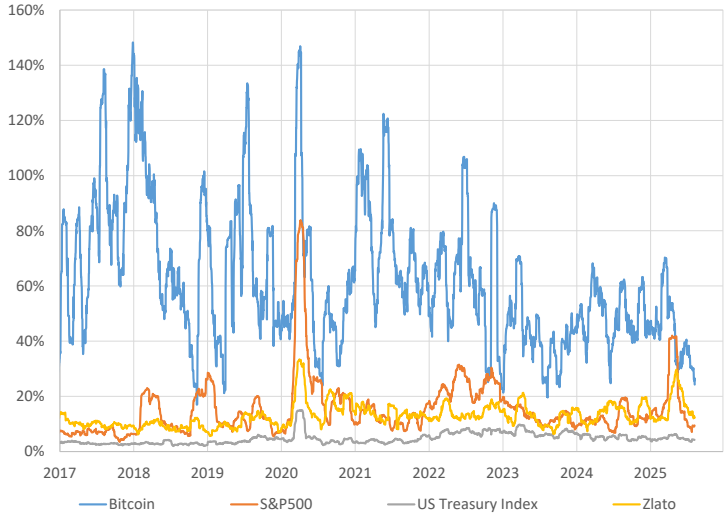
Jak již bylo opakovaně zmíněno, bitcoin je aktivem s velmi vysokou cenovou volatilitou. Výše uvedené histogramy ukazují četnost týdenních změn hodnoty bitcoinu, akciového indexu S&P 500, amerických vládních dluhopisů (US Treasury Index G0Q0) a zlata v období za posledních 5 let (od ledna 2020). Toto období tedy zahrnuje jak začátek pandemie covid-19, tak začátek války na Ukrajině. Jak je z grafu patrné, bitcoin je (nutno říct

podle očekávání) v tomto období a z těchto tříd aktiv nejvolatilnější; v ročním vyjádření dosahovala v tomto období volatilita bitcoinu 62 %, akcie zaznamenaly přibližně 20 %, zlato 16 % a bondy jen přibližně 6 %. V tomto ohledu se tedy nekoná žádné velké překvapení. Za zmínku však stojí, že se nejedná o volatilitu o řád či více vyšší, jak by bylo nejspíše možné z cenových grafů čekat. Z histogramů je také dobře patrné, že rozdělení výnosů bitcoinu se výrazně vymyká normálnímu rozdělení. Zatímco v případě ostatních aktiv je pravděpodobnost extrémních výkyvů, ať kladných či záporných, velmi nízká, v případě bitcoinu dokonce roste s velikostí výkyvu. Lze tedy očekávat, že události typu „černá labuť“ budou ve světě BTC spíše běžnou nežli vzácnou záležitostí.

Zajímavý detail přináší i pohled na krátkodobou volatilitu, v následujícím grafu 1-8 je uvedena v 30denním vyjádření. Obecně platí již zmíněné, tedy že volatilita bitcoinu se pohybuje v násobcích volatility akcií a je o řád vyšší, než u dluhopisů. Existují však také výjimky, jako bylo například období počátku pandemie covid-19 či při uvalení „recipročních cel“ ze strany americké administrativy v dubnu 2025, kdy krátkodobá volatilita dosáhla u akcií a bitcoinu obdobných úrovní. Zde je ale vhodné poznamenat, že zatímco v případě klasických aktiv jsou periody zvýšené volatility vzácné, v případě bitcoinu byly dosud spíše pravidlem.

Graf 1-8

30D rolling volatilita (annualizováno)



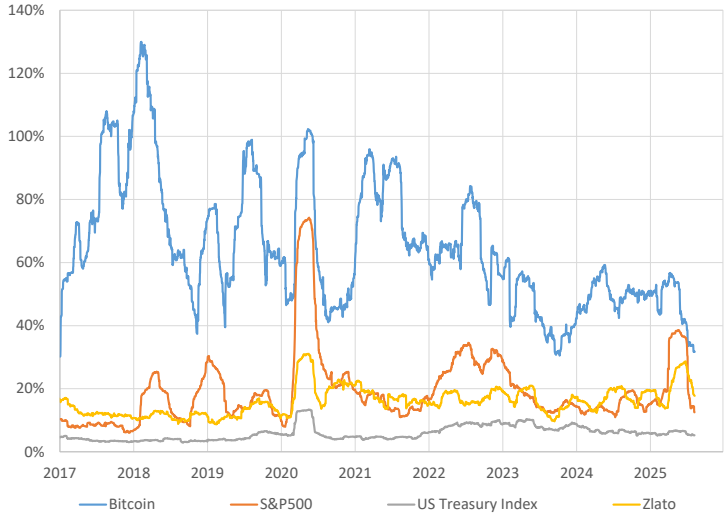
Zdroj: data Bloomberg, kalkulace ČNB

Krátkodobá volatilita akcií a bitcoinu během některých epizod srovnatelná

Ještě zřetelnější obrázek poskytují delší volatility. Pohled na 90denní volatility (graf 1-9) potvrzuje již uvedené – volatilita bitcoinu je sice vysoká, ve srovnání s dalšími rizikovými aktivy se však nejedná o řádově vyšší hodnoty, jak by se mohlo z astronomických cen bitcoinu zdát.

Graf 1-9

90D rolling volatilita (annualizováno)

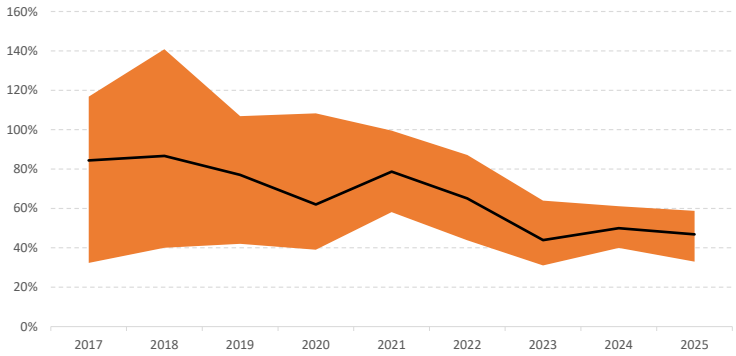


Zdroj: data Bloomberg, kalkulace ČNB

Pohled na volatilitu bitcoinu v čase však, zdá se, potvrzuje teorii, že bitcoin již s postoupnou akceptací ztrácí něco ze své divokosti. Samozřejmě, téměř 60% volatilita není nic, co by bylo v tradičních financích považováno za „normální“, přesto, trendy nejspíš podporují teorii, že již dnes je extrémně vysoká volatilita (a s ní spojené prudké nárůsty a poklesy hodnoty) již minulostí. Pohled na trend v následujícím grafu tuto teorii podporuje.

Graf 1-10

Bitcoin - 90D volatilita
(min, max, průměr v daném roce)



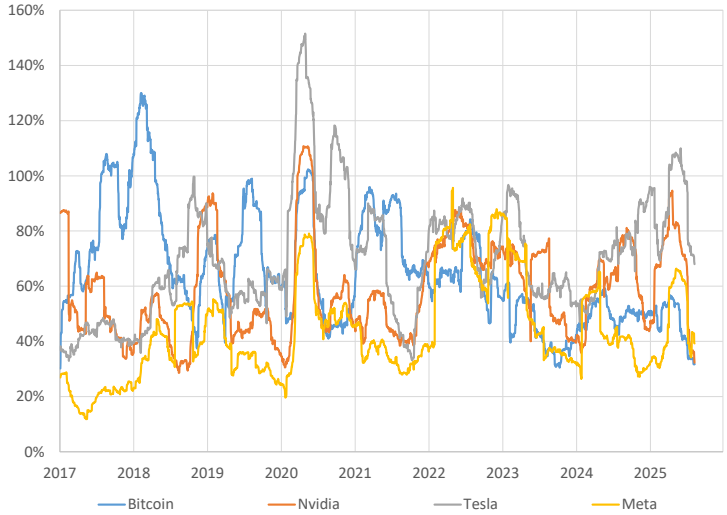
Zdroj: data Bloomberg, kalkulace a graf ČNB

Bitcoin srovnatelně volatilní s technologickými společnostmi

Zajímavé je taktéž srovnání volatility bitcoinu s volatilitou cen akcií některých technologických společností. Jak je patrné z následujícího grafu, po většinu období se vyskytla některá (z arbitrárně vybraných akcií), jež měla vyšší volatilitu než bitcoin, a platilo to zejména pro nedávné období. Pravděpodobným důvodem je skutečnost, že technologické firmy podléhají „boomům“ (aktuálně AI). Jak již bylo zmíněno, boom s sebou vždy nese zvýšenou volatilitu, která odezní, jakmile se novinka změní v široce akceptovaný standard.

Graf 1-11

90D rolling volatilita (annualizováno)

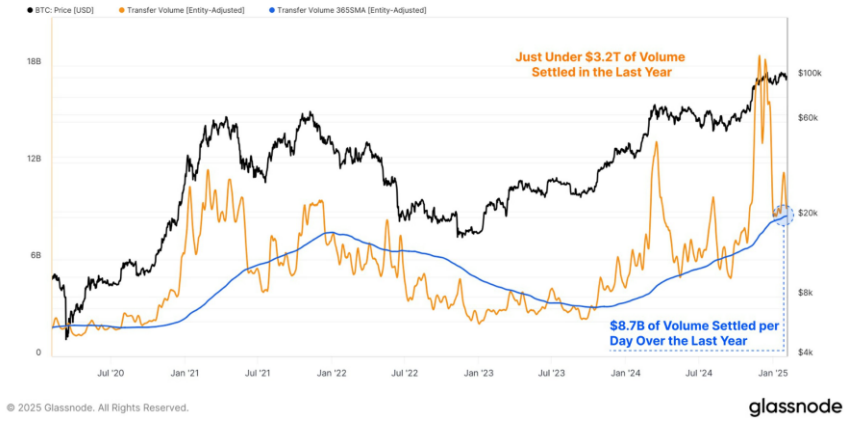


Zdroj: data Bloomberg, kalkulace a graf ČNB

Vysoká volatilita na trhu s bitcoinem je reflexí malého objemu trhu (zejména v porovnání s objemy zobchodovaných dluhopisů a akcií) a tedy v důsledku jeho nižší likvidity, vyšším podílem spekulativních transakcí a pravděpodobně též přetrvávajícím vysokým podílem maloobchodních investorů, kteří citlivěji reagují na tržní vývoj (následují trh a tím posilují tržní pohyby). Odhaduje se, že tzv. on-chain transakce s bitcoinem odpovídaly v roce 2024 denně průměrně cca 8,7 mld. USD[11]. Pro srovnání – objemy s akciemi Apple Inc. vykazují běžně denní objem obchodů vyšší než 13 mld. USD.

Graf 1-12

Total Transfer Volume (Entity-Adjusted)



zdroj: data Bloomberg, kalkulace a graf ČNB

Objemy obchodů s bitcoinem však podle mnoha ukazatelů neustále rostou. Toto podporuje teorii, že ruku v ruce s tím bude volatilita ceny bitcoinu dále klesat v důsledku růstu likvidity.

11 Ne všechny transakce odehrávající se na blockchainu reflektují skutečnou obchodní aktivitu. Např. podle analytické firmy Glassnode méně než 25 % on-chain objemů odpovídá skutečným převodům hodnoty mezi různými subjekty. https://bitcoinist.com/bitcoin-settled-3-2-economic-volume-2024

4.2 Sharpe ratio

Hodnota Sharpe ratio obdobná jako u akcií a zlata

Pro hodnocení výše výnosů aktiv se velmi často používá Sharpe ratio, které udává nadvýnos nad bezrizikovou sazbou na jednotku volatility[12]. Bitcoin i přes velmi vysokou volatilitu vykazuje Sharpe ratio podobné některým dalším třídám aktiv, zejména akciím a zlatu. Jinými slovy pro bitcoin platí, že jeho vysoká volatilita byla kompenzována vyššími výnosy v míře srovnatelné s dalšími rizikovými aktivy. Následující tabulka shrnuje hodnoty Sharpe ratio pro některé třídy aktiv od počátku roku 2021.

Analýza obsažená v této kapitole sama o sobě nepředstavuje důvod, proč by bitcoin či další aktiva, měla či neměla být zařazena do devizových rezerv. Smyslem je pouze zhodnotit nadvýnosy, které bitcoin historicky nabízel, ve vztahu k jeho volatilitě, a porovnat jej na tomto základě s dalšími aktivy.

Tabulka 1-1

Výnos, volatilita, Sharpe

	průměrný výnos [% ann.]	průměrná volatilita [% ann.]	Sharpe ratio
Bondy (UST 1-10let)	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
Zlato	13.05%	13.44%	0.73
Bitcoin	50.26%	62.97%	0.75

data: Bloomberg, 01/21 až 07/25, kalkulace ČNB

Na tomto místě je třeba opakovat upozornění – podobně jako u dalších statistických veličin, velmi záleží na vstupních datech, zejména potom na volbě sledovaného období. Tento problém se prohlubuje s mírou volatility sledovaného aktiva, výsledné hodnoty, vypočtené pro období jen o několik měsíců posunuté, mohou být diametrálně odlišné.

Hodnoty Sharpe ratio jsou velmi nestálé

ale v obdobné míře, jako u další aktiv…

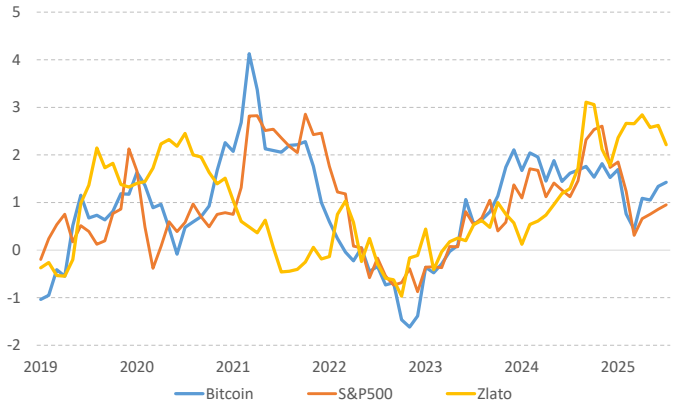
Následující graf 1-13 shrnuje vývoj Sharpe ratio na klouzavém 12M období. Je z něj patrná vysoká nestabilita tohoto ukazatele, jenž se pohybuje od velmi pozitivních hodnot přes 4 až po záporné hodnoty blížící se -2. Nehledě na to, graf ve velké míře potvrzuje dlouhodobé průměry udané v tabulce výše. Sharpe ratio bitcoinu obecně následuje vývoj Sharpe ratio akcií v až překvapivě vysoké míře.

Z grafu je dále patrné, že hodnoty Sharpe ratio se výrazně mění také pro akcie a zlato. Nelze tedy říci, že by se bitcoin z hlediska této statické veličiny odlišoval od těchto aktiv.

12 Sharpe ratio je definováno jako $s = \frac{r - r_f}{\sigma}$, kde r je výnos, r_f je bezrizikový výnos a σ je volatilita.

Graf 1-13

Sharpe Ratio / trailing 12m období



Zdroj: data Bloomberg, kalkulace a graf ČNB

4.3 Korelace s vývojem cen dalších aktiv

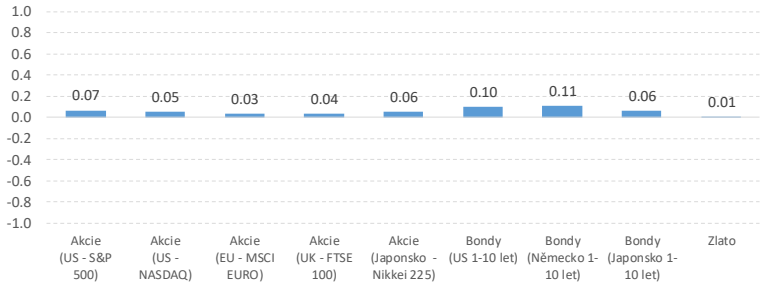
Nízká korelace bitcoinu s akciemi a dluhopisy

V nejdelší možné perspektivě (tj. od momentu vzniku, resp. počátku obchodování s bitcoinem v letech 2010/2011, viz graf 1-14) vykazuje bitcoin hodnoty korelačních koeficientů s dalšími aktivy velmi blízko nule.

Graf 1-14

Korelační koeficienty: Bitcoin proti dalším aktivům

(data 01/11 - 10/25, v lokálních měnách, frekvence měsíční)



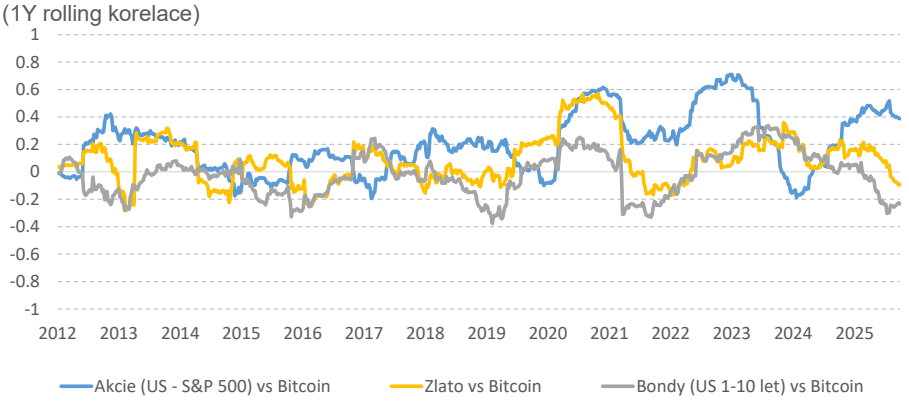
zdroj: data Bloomberg, kalkulace ČNB

Bližší pohled na krátkodobější korelace (graf 1-15, zobrazuje historický vývoj korelačních koeficientů kalkulovaných za období posledního roku) potvrzuje obecněji platný fakt, že hodnoty korelací mohou procházet výraznými výkyvy, a že i pro aktiva, u kterých se obvykle předpokládá nějaký vztah (např. záporné korelace mezi výnosy dluhopisů a akcií), nemusí tento vztah být v čase dokonale stabilní.

Graf 1-15

Korelační koeficienty

(1Y rolling korelace)



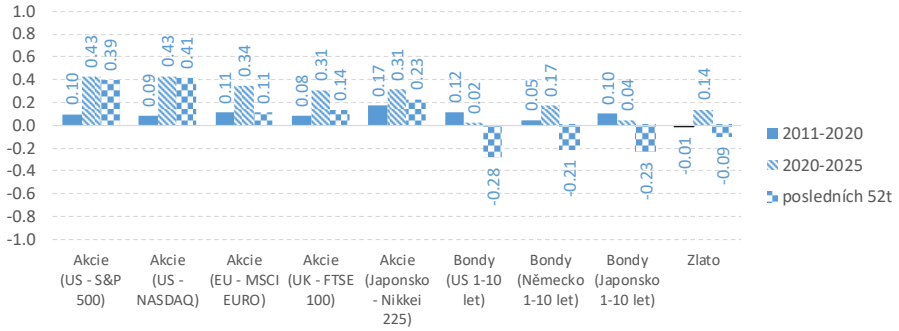
zdroj: data Bloomberg, kalkulace ČNB

Po roce 2020 došlo ke změně režimu: bitcoin obecně následuje cenový vývoj dalších rizikových aktiv

Podobný vývoj lze sledovat i u bitcoinu – zatímco až do roku 2020 byly hodnoty korelačních koeficientů mezi bitcoinem a dluhopisy/akciemi/zlatem velmi blízké nule (nad hodnotou 0,2 se pohybuje jen zřídka), výrazně jiná situace je v pozdějším období. Během let 2020 až 2023 se korelace bitcoinu proti akciím naopak pod hodnotou 0,2 vůbec nevyskytovala, během roku 2023 pak dosáhla úrovní na 0,6 a jen o něco níž se pohybuje v roce 2025. Za pozitivní signál je však nejspíš nutné považovat záporné hodnoty krátkodobých korelačních koeficientů mezi bitcoinem a dluhopisy – zdá se, že i v období po roce 2020 pokračují dlouhé epizody jejich záporných hodnot, přičemž v některých obdobích se pohybují až na úrovni −0,4.

Graf 1-16

Korelační koeficienty bitcoinu proti dalším aktivům v různých obdobích



zdroj: data Bloomberg, kalkulace ČNB

Tabulka 1–2 uvádí přehled ročních korelačních koeficientů k říjnu 2025. Z dat vyplývá, že cenový vývoj bitcoinu v uplynulém roce vykazoval spíše shodný trend s akciovými trhy (korelace s S&P 0,4), zatímco ve vztahu k dluhopisům, a v menší míře i ke zlatu, byl vývoj převážně opačný.

Tabulka 1-2

Korelační matice

(data 10/24 - 10/25, v lokální měně, frekvence týdenní)

	Akcie (US - S&P 500)	Akcie (US - NASDAQ)	Akcie (EU - MSCI EURO)	Akcie (UK - FTSE 100)	Akcie (Kanada - S&P TSX)	Akcie (Japonsko - Nikkei 225)	Bondy (US 1-10 let)	Bondy (Německo 1-10 let)	Bondy (Kanada 1-10 let)	Bondy (Japonsko 1-10 let)	Bitcoin	Zlato
Akcie (US - S&P 500)	100%	95%	29%	21%	66%	43%	-2%	-4%	8%	-29%	39%	-16%
Akcie (US - NASDAQ)	95%	100%	19%	4%	53%	39%	-15%	-10%	-2%	-23%	41%	-24%
Akcie (EU - MSCI EURO)	29%	19%	100%	88%	57%	68%	3%	-23%	27%	-49%	11%	25%
Akcie (UK - FTSE 100)	21%	4%	88%	100%	65%	62%	13%	-9%	29%	-47%	14%	40%
Akcie (Kanada - S&P TSX)	66%	53%	57%	65%	100%	58%	21%	6%	37%	-38%	27%	32%
Akcie (Japonsko - Nikkei 225)	43%	39%	68%	62%	58%	100%	-2%	-18%	22%	-34%	23%	16%
Bondy (US 1-10 let)	-2%	-15%	3%	13%	21%	-2%	100%	54%	72%	32%	-28%	35%
Bondy (Německo 1-10 let)	-4%	-10%	-23%	-9%	6%	-18%	54%	100%	37%	45%	-21%	25%
Bondy (Kanada 1-10 let)	8%	-2%	27%	29%	37%	22%	72%	37%	100%	18%	-18%	31%
Bondy (Japonsko 1-10 let)	-29%	-23%	-49%	-47%	-38%	-34%	32%	45%	18%	100%	-23%	11%
Bitcoin	39%	41%	11%	14%	27%	23%	-28%	-21%	-18%	-23%	100%	-10%
Zlato	-16%	-24%	25%	40%	32%	16%	35%	25%	31%	11%	-10%	100%

zdroj: data Bloomberg, kalkulace ČNB

Za hlavní závěry proto považujeme:

- z hlediska delšího historického vývoje ceny bitcoinu, může jeho zařazení do rezervního mixu z důvodu nižších hodnot korelačních koeficientů přinést diverzifikační benefity,
- v období po roce 2020 došlo k posunu, bitcoin vykazuje určitou podobnost s cenovým vývojem akcií, diverzifikační efekt se však stále výrazně projevuje proti dluhopisům,
- poměrně překvapivě zůstává bitcoin velmi málo korelován s vývojem cen zlata.

Na zřeteli je však třeba i nadále mít určitou nespolehlivost statistických údajů spojených s bitcoinem, na který jsme však v předchozím textu upozorňovali již několikrát. Jinými slovy – dosavadní vývoj nemusí být v žádném případě následován shodným vývojem v budoucnu.

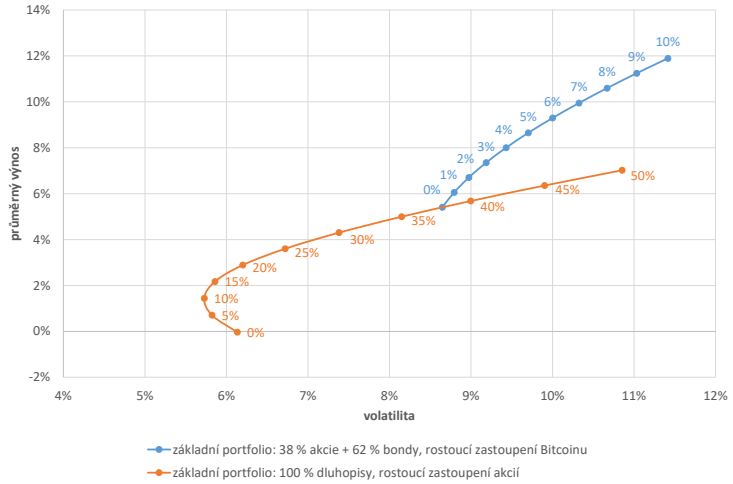
4.4 Vliv začlenění bitcoinu do portfolia

Relativně vysoká volatilita ceny bitcoinu a jeho především v období po roce 2020 pozorovaný nižší diverzifikační potenciál naznačují, že přidání bitcoinu do portfolia nepřinese výraznější efekt. Modrá datová řada na následujícím grafu vychází ze stylizovaného jednoduchého portfolia skládajícího se z 38 % akcií[13] (index S&P 500) a 62 % bondů (US Treasury Index), do nějž postupně přidáváme bitcoin (přičemž v příslušném poměru klesá zastoupení akcií i bondů). Analyzujeme pouze výnosy v americkém dolaru, v potaz tedy nebereme vliv dalších kurzů.

13 38% zastoupení akcií v investiční tranši by za stávajících podmínek odpovídalo zhruba 30% podílu akcií na celém portfoliu devizivých rezerv.

Graf 1-17

Risk / return charakteristiky
(data 2020-2025)



Zdroj: data Bloomberg, kalkulace ČNB

Efficient frontier

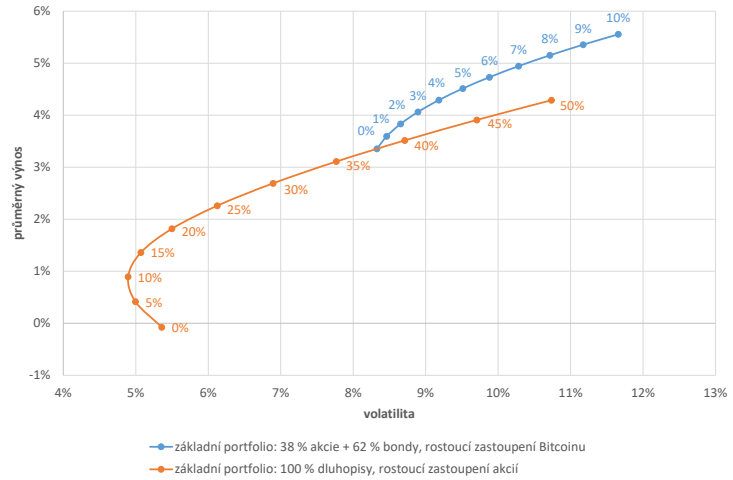
Graf potvrzuje naše očekávání, tj. neexistuje žádný objem bitcoinu, jehož přidáním by poklesla celková míra volatility výsledného portfolia, nehledě na periody záporné korelace bitcoinu s dluhopisy. I přes určité statické podobnosti BTC s akciemi, není možné nalézt takovou strukturu portfolia, kdy by při rostoucím výnosu volatilita klesala nebo alespoň stagnovala, jak je tomu právě v případě akcií. Modrá bitcoinová křivka však vykazuje jinou výhodu – je velmi strmá, přidáním jednotky volatility je více než kompenzováno výnosem (jinými slovy, roste tzv. Sharpe ratio). To je ovšem pouze reflexí toho, jaké výnosy bitcoin od roku 2020 zaznamenal – byly velmi vysoké, v průměru 65 % p.a. (akcie ve stejném období získaly pouze cca 12 % p.a., bondy se pohybovaly okolo nuly) – ale také postupného poklesu volatility bitcoinu v čase. Je však třeba zdůraznit, že nelze říci, zda tento trend bude pokračovat.

Následující grafy demonstrují vliv volby časové řady na závěry výše provedené analýzy. Nejprve na datech za roky 2018 až 2022, kdy bitcoin zaznamenal jen malý nárůst (průměrně jen 2,3 % p.a.), dále potom jen za rok 2022, kdy bitcoin výrazně propadl (o 64 %).

Různá datová období vedou k různým výsledkům
(nebezpečí cherry-pickingu)

Graf 1-18

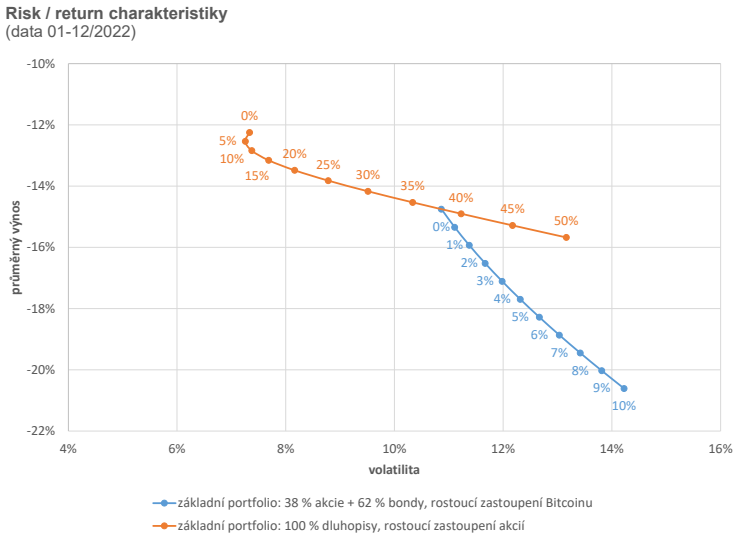
Risk / return charakteristiky
(data 2018-2022)



Zdroj: data Bloomberg, kalkulace ČNB

U situace z let 2018 až 2022 je patrné, že modrá křivka bitcoinu je výrazně plošší – i přidáním až 10 % bitcoinu do portfolia vzroste výnos jen o cca 2 p.b.

Graf 1-19



Zdroj: data Bloomberg, kalkulace ČNB

Scénář roku 2022: negativní extrém, který postihl většinu aktiv

Scénář roku 2022 je pak naprostým extrémem, zahrnutím 10 % bitcoinu klesá výnos portfolia až k -21 %. Zde je však nutné podotknout, že v tomto roce prodělávaly prakticky všechny třídy aktiv.

Riziko cherry-pickingu u bitcoinu vysoké

Pro některé parametry, jako je třeba očekávaný výnos, bude vhodnější nepoužít historická data, ale vlastní odhady

Uvedené scénáře odhalují jednu ze slabin podobného přístupu – nebezpečí tzv. cherry-picking, konkrétně vybrání jen takového období, kdy jsou výsledky „příznivé“ (ať už to znamená cokoliv). V případě bitcoinu je potřeba mít toto riziko na paměti s ohledem na poměrně dramatickou historii vývoje jeho cen a ve srovnání s ostatními aktivy relativně krátké časové řady. Řešením může být např. možnost explicitně stanovit předpoklady, se kterými do analýzy vstupujeme ad-hoc, tedy např. stanovit, že očekáváme, že bitcoin poroste 30 % p.a. (nebo 20, 40, 80 % apod.), a následně pak zvážit, zda je navýšení volatility portfolia kompenzováno dostatečným nárůstem očekávaného výnosu. Je nabíledni, že takovýto ad-hoc expertní odhad nebude snadný, obzvláště pak u aktiva, jehož cena je výsledkem čistě tržních pohybů, a které nemá vnitřní hodnotu.

4.5 Case study – s bitcoinem za nižší volatilitou?

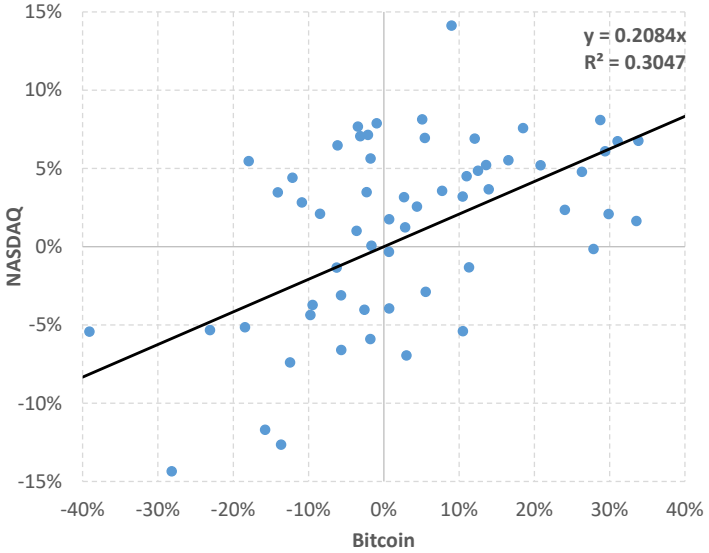
Jak už bylo několikrát zopakováno – statistické vlastnosti bitcoinu se ve velké míře vymykají konvenčním aktivům, i když nejvíce se blíží akciím. Od nich jej nicméně odlišuje zejména vysoká volatilita, ovšem spojená s ještě vyššími, až extrémními, výnosy. Jeho začlenění do portfolia pak může přinést některé neočekávané přínosy.

Pro účely následujícího cvičení jsme vybrali akciový index technologických firem NASDAQ, který sám o sobě vykazuje o něco vyšší volatilitu ve srovnání s častěji používaným indexem S&P500. Nejprve jsme zkoumali korelaci s bitcoinem. Bodový graf níže potvrzuje, že mezi cenami obou aktiv existuje silná vazba. R^2 na úrovni 0,3 by se mohl zdát poměrně nízký,

odpovídá však relativně vysokému korelačnímu koeficientu na úrovni 55 %, a silný statistický vztah potvrzují i další statistiky[14].

Graf 1-20

1M změny cen Bitcoin vs NASDAQ

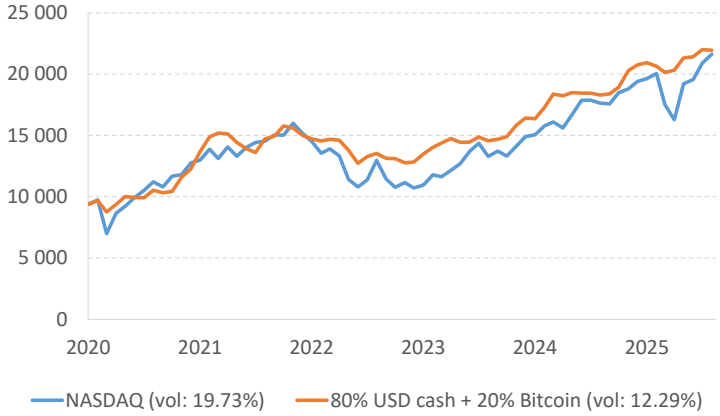


Zdroj: data Bloomberg, kalkulace ČNB

Pokusme se nyní o syntetickou replikaci indexu NASDAQ pomocí jednoduché kombinace USD hotovosti úročené krátkými bezrizikovými sazbami peněžního trhu a investice do bitcoinu. Hotovost bude zastoupena z 80 %, bitcoin z 20 %, přičemž toto portfolio bude rebalancováno na ideální váhy s měsíční frekvencí. Srovnání vývoje indexu NASDAQ se syntetickou alternativou uvádí následující graf.

Graf 1-21

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



Zdroj: data Bloomberg, kalkulace ČNB

Tato kalkulace sama o sobě až do tohoto momentu není příliš zajímavá, potvrzuje pouze zřejmý fakt, že korelovaná aktiva mají v portfoliích do značné míry zastupitelnou roli. Zajímavější je pohled na obě křivky v předcházejícím grafu – syntetická je oproti originálnímu NASDAQu zřetelně hladší a zdá se, že obsahuje méně výrazných výkyvů. A skutečně –

14 Test hypotézy o nenulovosti korelačního koeficientu, p-hodnota 0,0001 %.

průměrná volatilita indexu NASDAQ za toto období dosahuje necelých 20 %, zatímco syntetická náhrada pouze 12,3 %. To je mírně překvapující výsledek, který je v rozporu s naším očekáváním, že zahrnutím aktiva s velmi vysokou volatilitou, musí dojít k růstu volatility. Ve skutečnosti však jde o iluzi, kterou lze snadno vyvrátit jednoduchou kalkulací[15], popř. také intuitivně – v momentě, kdy BTC generuje zisk, jsou výnosy realizovány a přeměny na hotovost, čímž vzniká „zásobník“, který kompenzuje ztráty v případě poklesu ceny bitcoinu. Ve výsledku tak dojde k vyhlazení celkového výnosu[16].

5. MOŽNOST IMPLEMENTACE V ČNB

5.1 Compliance s legislativou

Obchody s bitcoinem lze provádět na základě zákonného zmocnění v § 32 ZoČNB

Operace s bitcoinem lze provádět na základě § 32 zákona o ČNB, který stanoví, že:

> Česká národní banka je oprávněna k plnění svých úkolů provádět obchody na finančním trhu, zejména:
>
> a) vést účty bank, poboček zahraničních bank, spořitelních a úvěrních družstev a přijímat jejich vklady,
>
> b) obchodovat s investičními nástroji a dalšími cennými papíry, devizovými hodnotami, drahými kovy, pohledávkami a dalšími aktivy formou nákupů a prodejů, repo obchodů, vkladů, výpůjček, zápůjček nebo termínovaných obchodů,
>
> c) provádět úvěrové operace.

ČNB dospěla k závěru, že bitcoin lze považovat obecně za aktivum ve smyslu písmene b). Nicméně za klíčové se považuje posouzení splnění další podmínky uvedené v úvodní větě ustanovení, a sice že toto aktivum je obchodováno na finančním trhu. Pojem „finanční trh“ sice není v českém právním řádu výslovně definován, podle názoru ČNBse však jedná o nejširší definici trhu, která v sobě zahrnuje všechny podkategorie trhů a o tom, že se digitální aktiva obchodují na „finančním trhu“ nemůže být pochyb.

Dalším relevantním ustanovením zákona o ČNB, které je třeba uvést, je § 35, který upravuje pravomoci a činnosti ČNB v devizovém hospodářství a v písm. d) stanoví, že ČNB nakládá s devizovými rezervami ve zlatě a devizových hodnotách. Otázkou je, zda lze bitcoin považovat za devizovou hodnotu. Pojem devizová hodnota není v českém právním řádu definován. Jeho definici obsahoval dnes již zrušený devizový zákon, podle kterého jsou devizovými hodnotami peněžní prostředky v cizí měně, zahraniční cenné papíry a dále penězi ocenitelná práva a závazky od nich odvozené (dále jen „finanční deriváty“). Podle názoru ČNB bitcoin není cizí měnou (neodpovídá ani definici v – byť již zrušeném – devizovém zákoně, ani obecnému významu slova „deviza“ jako měna cizího státu). Ačkoliv současný právní

---

15 $vol_{syn} = \sqrt{\omega_{BTC}^2 vol_{BTC}^2 + \omega_{USD}^2 vol_{USD}^2 + 2\omega_{BTC}\omega_{USD}\rho_{BTC-USD} vol_{BTC} vol_{USD}}$,
kde $\omega_{USD} = 0{,}8$, $\omega_{BTC} = 0{,}2$, $vol_{USD} \approx 0$ a $vol_{BTC} \approx 60\ \%$,
přičemž druhý a třetí člen se blíží nule a je možné je zanedbat, $vol_{syn} = \sqrt{0{,}2^2 \cdot 0{,}6^2} = 12\ \%$

16 Tzv. „princip činky“, který zavedl N. Taleb, autor pojmu „černá labuť“.

řád pojem „devizová hodnota“ nedefinuje, neznamená to, že pod tento pojem lze podřadit jakékoliv aktivum.

Pro získání **praktických zkušeností** s bitcoinem/blockchainem lze postupovat i podle **§ 40 ZoČNB**

Další, byť omezenou možnost poskytuje § 40, který v prvním odstavci stanoví, že:

> Česká národní banka je oprávněna provádět investiční a obchodní činnost v rozsahu nezbytném pro zajištění svých činností.

Podle názoru ČNB je toto ustanovení možné použít v případě, že by ČNB chtěla v malém objemu prakticky otestovat technologie (blockchain apod.) a postupy spojené s investováním do bitcoinu, a získat tak znalosti a zkušenosti se spojenými technologiemi (blockchain apod.). Bitcoin lze tedy ve smyslu §40 kvalifikovat jako aktivitu sloužící k plnění zákonných úkolů.

Případné operace s bitcoinem lze **v případě ČNB** považovat za **konformní** se **Statutem ESCB a ECB**

ECB není oprávněna vydat závaznou instrukci týkající se provádění obchodů na volném trhu podle § 32 odst. 1 zákona o ČNB. Problematika obchodů na volném trhu, správy devizových rezerv, resp. dělení kompetencí mezi ECB a NCB v této oblasti, je upravena ve Statutu ESCB a ECB. Postavení centrální banky mimo eurozónu je v tomto ohledu zásadně odlišné od centrální banky v eurozóně. Pro ČNB sice platí cíle uvedené v čl. 2 Statutu, tj. primárně udržovat cenovou stabilitu, na druhou stranu čl. 3 Statutu, který stanoví úkoly ESCB, mj. úkol vymezovat a provádět měnovou politiku a úkol držet a spravovat devizové rezervy, se na ČNB nevztahuje. Statut ESCB obsahuje také pravidlo obdobné § 40 zákona o ČNB.

Přímé nákupy bitcoinu jsou tedy v souladu se zákonem o ČNB i Statutem ESCB a ECB.

Nepřímé investice: zcela v souladu

Naprosto jednoznačná je pak situace v případě nepřímých investic, např. prostřednictvím ETF fondů – zde z hlediska zákonných omezení neexistuje rozdíl, mezi již dnes obchodovanými instrumenty ETF navázanými na indexy MBS trhu či akciové indexy a těmi, jejichž ceny jsou navázány na bitcoin.

5.2 Možnosti technického řešení self-custody

Pro zajištění bezpečného držení bitcoinů v self-custody existuje celá řada řešení:

- softwarové „peněženky“ - obecně vnímáno jako postačující řešení v případě malých objemů držených bitcoinů,
- jednoduchá zařízení typu USB token (Ledger, Coldcard, Trezor), která mají různými technikami zabránit exportu privátního klíče[17],
- hardwarové security moduly (HSM), tedy dedikovaná zařízení či počítačové karty používané k obdobným účelům jako USB tokeny, tedy k bezpečnému uchování privátního klíče bez možnosti jeho exportu apod.

V oborovém žargonu se používá řada pojmů, které nejsou vždy uplatňovány zcela korektně, a proto často vznikají nejasnosti. Typicky se rozlišuje mezi tzv. *cold storage* (zařízení nebo peněženky zcela odpojené od počítačových

17 Některá z těchto zařízení obsahují tzv. secure element, specializovaný čip, který neumožňuje export privátního klíče, jiná spoléhají na open source kryptografická řešení (kupř. Trezor One/T); existuje kritika obou přístupů, v jednom uživatelé spoléhají na „black-box“ čip, v druhém existuje teoreticky využitelná fyzická zranitelnost (voltage glitching nebo dump ROM/flash paměti).

sítí, případně připojované jen výjimečně) a *hot wallets* (peněženky běžně připojené k internetu). Kromě toho se hovoří o *offline řešeních*, což je obecnější pojem, který zahrnuje i cold storage, a v praxi bývá někdy používán zaměnitelně. V jádru však nejde o názvosloví, ale o řešení tří základních problémů: (1) jak bezpečně privátní klíč vytvořit, (2) jak jej uchovat a (3) jak zabránit jeho zneužití.

MPC + HSM: dnes v oboru považováno za „best practice“

Za příklad velmi bezpečného zařízení se dnes udává kombinace multisignature (tzv. multisig) či MPC (Multi-Party Comptutation) a hardwarového zařízení HSM. Jedná se o technicky náročné, ale velmi účinné řešení, které je dnes považováno za „best practice“. Jeho jádrem je obvykle několik HSM modulů (certifikovaných na FIPS 140-2 Level 3) a MPC, které je obvykle doplněné o orchestrátor řídící podpisové operace, a dále o auditní a logovací vrstvy. Generování privátního klíče neprobíhá v celku, ale po částech pomocí distribuovaného protokolu (tzv. DKG, Distributed Key Generation), vytvořeny jsou jednotlivé parciální klíče (tzv. shards), a tyto jednotlivé části jsou použity v různých HSM modulech. MPC orchestrace pak řídí podpisové operace[18], vyžaduje se určitý počet parciálních podpisů (threshold), které se zkombinují do jednoho výsledného podpisu, aniž by kdy vznikl celý klíč v jedné instanci. Toto řešení je v současnosti považováno za velmi bezpečné.

„Air-gapped“ řešení

Pokud není vyžadována vysoká frekvence obchodních příkazů, lze uvažovat o úplné izolaci tohoto řešení od počítačové sítě, nepodepsané transakce (partially signed bitcoin transaction, PSBT) jsou pak na přenosných médiích (či jiným tzv. „air-gapped“ způsobem) dopraveny do systému zcela odpojeného od sítě, kde jsou PSBT podepsány, a výsledné podepsané transakce přeneseny do on-line světa a sítě blockchain ke zpracování.

Self-custody jen s patřičným zabezpečením, transakce jsou nevratné

Nevýhodou takto navrženého robustního systému je značná finanční náročnost na pořízení celé řady specializovaných hardwarových zařízení. V tomto bodě je však důležité zopakovat kontext, ve kterém by se ČNB při nakládání s bitcoinem pohybovala – jedná se zejména o riziko zneužití privátních klíčů ČNB v prostředí nevratného charakteru operací prováděných na blockchainu. V tomto se podvodné transakce na blockchainu výrazně liší od ostatních transakcí prováděných na finančních trzích - jejich zneužití je nevratné. Prvotřídní zabezpečení transakcí je tedy naprostou prioritou.

Multisig jako jednodušší alternativa?

Jako jednodušší a přitom bezpečnou alternativu je možné využít také řešení postavené čistě na principu multisignature (multisig). Na rozdíl od MPC je multisig přímo nativní součástí bitcoinového protokolu – tedy mechanismus, který je od počátku podporován samotným blockchainem, nikoli pouze externími aplikacemi. To sice nenabízí všechny funkcionality MPC a HSM, ale z pohledu bezpečnosti privátních klíčů jde o osvědčenou metodu, která je často využívána v institucionální praxi. I multisig umožňuje nastavit schvalovací schémata (např. 2-z-3, 3-z-5), takže k provedení transakce je nutná spolupráce více nezávislých subjektů či zařízení. Tím je výrazně sníženo riziko zneužití klíče jediným kompromitovaným bodem. Z pohledu finančních nákladů je multisig řešení méně náročné než robustní kombinace MPC+HSM, a může proto představovat vhodný kompromis zejména v případech, kdy není vyžadována nejvyšší možná úroveň odolnosti, ale bezpečnostní standardy zůstávají prioritou.

---

18 Vstupní transakce se předá orchestrátoru, ten zahájí MPC protokol mezi HSM jednotkami. Každá jednotka vypočítá „podpisovou část“, ty pak orchestrátor spojí do jednoho podpisu a hotový podpis je připojen k transakci a odeslán do bitcoinové sítě.

5.3 Externí custody držených bitcoinů

Přímo obchodované bitcoiny lze převádět k držbě i na externí custodiany. Těch existuje celá řada:

- **BNY Mellon**
  (v říjnu 2022 spustil custody platformu pro bitcoin a ethereum, slouží především institucionálním klientům v USA, spojuje tradiční úschovu cenných papírů s úschovou digitálních aktiv),
- **Fidelity Digital Assets**
  (Divize Fidelity Investments, poskytuje custody a obchodování pro BTC již od roku 2018, silně orientovaná na institucionální investory, hedge fondy a tzv. family offices),
- **State Street Digital**
  (partnerství s firmou Copper, technologie pro úschovu digitálních aktiv),
- **Nomura / Laser Digital**
  (japonská investiční banka expandovala do oblasti digitálních aktiv prostřednictvím vlastní divize „Laser Digital“, nabízí úschovu BTC a dalších digitálních aktiv pro instituce),
- **Zürcher Kantonalbank** (ZKB)
  (od 2024 umožňuje úschovu a obchod s kryptoměnami včetně bitcoinu),
- **DZ Bank**
  (od 2023 nabízí custody pro kryptoměny včetně bitcoinu v rámci platformy pro institucionální klientelu),
- **Coinbase Custody**
  (dceřiná instituce burzy Coinbase, zaměřující se na správu digitálních aktiv).

Všechny tyto společnosti nabízejí custody služby institucionálním klientům s cílem umožnit držení BTC v souladu s regulačními a bezpečnostními požadavky obdobně, jako je tomu u tradičních finančních aktiv. Investoři se tak nemusí zabývat detailně bezpečností použitých technologií a možnostmi jejího zneužití.

Využití externích custody služeb zahrnuje celou řadu výhod, jedná se o regulované služby (pod dohledem SEC, FINMA apod.), procesy – včetně digitálních – jsou auditovány (ISAE 3000, 3402, SOC 1/2), lze snadno integrovat do stávajících systémů klientů, někteří custodiani jsou specificky proti ztrátě digitálních aktiv pojištěni (byť v omezeném rozsahu).

Bitcoiny držené v externí custody jsou bankruptcy remote

Pro klienty je důležitým elementem úvah o bezpečnosti aktiv držených prostřednictvím externího custody tzv. bankruptcy remoteness. Tedy fakt, že klientská aktiva se v případě úpadku custodiana nestávají součástí konkurzní podstaty. Zahraniční praxe ukazuje, že ochrana klienta je i v této oblasti možná – ale jen tehdy, pokud je majetek smluvně i technicky oddělen (např. unikátní blockchain adresa, zákaz nakládání bez souhlasu, trustová struktura). Pouhá smlouva nestačí, pokud ji neprovází reálné nastavení, které potvrzuje, že digitální aktiva jsou držená „pro klienta“ a nikoli jako součást majetku custodiana[19].

—

19 Viz např. Clifford Chance & Komainu: Custody of Cryptoassets: Moving Towards Industry Best Practice (2023), s. 43–44: “It is possible that the client may agree that, although the

Důležité je také rozlišovat, zda jsou zůstatky drženy na custody účtu, či u brokera, burzy atd. Za tzv. *bankruptcy remote* se považují výhradně aktiva na custody účtech. O tom se přesvědčili klienti Mt. Gox (náhrada v řádu desítek procent původně držených objemů[20]) či burzy FTX, kdy se prostředky držené na zákaznických účtech staly součástí konkurzní podstaty. Klienti se přihlašovali do insolvenčního řízení a z velké části je zachránilo to, že tyto pohledávky byly vyčíslovány v USD a že cena bitcoinů od momentu kolapsu burz výrazně vzrostla. Buď jak buď – kdyby dnes teoreticky zkolabovala nějaká z velkých burz s navázaným custody byznysem, zůstatků klientů na custody účtech by se krach burzy, na rozdíl od situace v Mt. Gox či FTX, neměl nijak dotknout.

Možnost kombinace externí custody a interního MPC řešení

Při použití některých poskytovatelů externích custody služeb (např. BNY atd.), kteří typicky využívají externí tzv. MPC orchestrační platformu pro správu klíčů (Fireblocks aj.) by pro ČNB zcela neodpadla nutnost spravovat privátní klíč či privátní klíče. Transakce jsou sice iniciovány a následně také schváleny přímo na platformě custodiana (ať už přes webové rozhraní, či např. z interního systému klienta přes veřejné API), před provedením vlastní transakce na blockchainu je však nutné spolupodepsat transakci v MPC, kdy jsou použity fragmenty (shards) klíče uložené u custodiana, ale také u klienta.

Coinbase custody zcela zbavuje klienty nutnosti řešit zabezpečení klíčů

Jiní custodiani (např. Coinbase Custody) mají nad privátním klíče klienta úplnou kontrolu, MPC technologii využívají interně, avšak všechny fragmenty privátního klíče jsou plně v jeho rukou. Takový přístup má hlavní výhodu v operační jednoduchosti, klienti nejsou nuceni k budování paralelních struktur infrastruktury podobné té, jež provozují samotní custodiani. Konkrétně Coinbase Custody je dominantním hráčem na poli služeb pro ETF fondy (uvádí se, že až 81 % ETF fondů používá právě tuto společnost), jeho služby využívá i společnost Strategy (dříve MicroStrategy) atd. Tento způsob držení bitcoinů je však někdy kritizován, právě pro absenci kontroly klíčů – to je tak možné spatřovat z určité perspektivy jako výhodu (jednoduché řešení), z jiného jako nevýhodu (ztráta kontroly).

Model co-custody

Co-custody složitější, ale velmi bezpečné řešení

V předchozím textu byla popsána možnost využití externího custodiana v kombinaci se spolupodpisem ČNB prostřednictvím technologie MPC (např. Fireblocks) – model někdy označovaný jako *co-custody*. Nutnost spolupodepisovat transakce pomocí MPC z tohoto řešení činí technologicky složitější proces, který je v určitém smyslu obdobný požadavkům na self-custody. Obecně jej lze považovat za velmi bezpečné řešení.

6. BITCOIN JAKO SOUČÁST DR?

V této kapitole se zabýváme mírně různorodou směsí problémů spojených s otázkou, zda a jak lze bitcoin v praxi začlenit do devizových rezerv, tedy např. jak uchopit účetní, či s auditem spojené otázky.

---

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 Paradoxně i tato částečná náhrada může být dnes v dolarovém vyjádření hodnotnější, než kolik klienti původně drželi v době kolapsu burzy.

V závěru kapitoly jsme se pak pokusili zamyslet i nad filozofičtějšími otázkami. Nejprve jsme se zaměřili na paralely mezi bitcoinem a zlatem, v úplném závěru jsme se pak podívali i na faktory, které z bitcoinu dělají v současnosti tak výjimečné aktivum.

Považujeme za podstatné uvést i to, že možných negativních pohledů na bitcoin se ve veřejném prostoru objevuje celá řada. Ať už se jedná o nejrůznější nelegitimní či rovnou kriminální způsoby použití bitcoinu, záležitosti spojené s darknety apod. Explicitně se proto ani nepokoušíme všechny je v této analýze uvést.

6.1 Může se bitcoin stát součástí oficiálních devizových rezerv?

Přímé investice do bitcoinu by nebyly vykazovány jako součást oficiálních devizových rezerv

ČNB otázku statistického zachycení možné držby bitcoinu centrální bankou bilaterálně konzultovala se zástupci MMF i ECB. Výsledkem schůzek je shodné stanovisko všech institucí, že **přímo držené bitcoiny nejsou rezervním aktivem** a jejich hodnota by tak nevstupovala do části „A. Official reserve assets“ výkazu devizových rezerv[21].

Přímo držené bitcoiny by se současně neměly odrazit ani v jiných částech výkazu MMF (nejen v části I. ale ani v částech II.-IV.). Část „I.B Other foreign currency assets“ se týká pouze cizoměnových aktiv nezařazených v části I.B, oproti části I.A. jsou zde zařazena i případná cizoměnová aktiva emitovaná rezidentem ČR nebo přeshraniční nelikvidní cizoměnová aktiva. Ani další části výkazu zařazení bezprostředně drženého bitcoinu metodicky neumožňují.

ČNB může bitcoin i přesto za součást svých rezerv považovat

Zařazení v souladu s výše uvedeným stanoviskem MMF i ECB je důležité s ohledem na závazek respektovat mezinárodní statistickou metodiku a za účelem mezinárodní srovnatelnosti vykazovaných statistik. Toto však neznamená, že z hlediska interní analýzy dopadů na DR či vlastní komunikace ČNB směrem k veřejnosti by ČNB nemohla bitcoin držet. Stále je ale nutné brát v potaz, že takto držené bitcoiny se nestanou součástí oficiálních devizových rezerv podle metodiky MMF, a může proto dojít k určitým rozdílům mezi interně a oficiálně vykazovaným objemem rezerv. V tomto stavu je však ČNB již dnes[22]. Pokud tedy v textu hovoříme ve zkratce o možnosti zařazení bitcoinu či jiného aktiva do devizových rezerv, není tím míněno jeho zacházení z hlediska metodiky MMF či ECB, ale spíše o zařazení daného aktiva do celkového mixu aktiv a pasiv držených ČNB.

ETF na bitcoin součástí rezerv

Zcela odlišná je situace v případě nepřímých investic prostřednictvím ETF – takové investice by byly vykazovány normálním způsobem jako součást devizových rezerv, obdobně jako ETF s dalšími podkladovými aktivy.

---

21 Důvodem je skutečnost, že bezprostředně držený bitcoin nesplňuje statistická kritéria pro rezervní aktivum ve smyslu platných metodik makroekonomických statistik (SNA/ESA/BPM), s kterými je template v obecném metodickém souladu (viz par. 110 Guideline IMF). S výjimkou historicky zařazovaného zlata jsou v části „A.“ zachycena výlučně finanční instrumenty s protistranou, kterou musí být nerezident. Uvedenou podmínku existence nerezidentské protistrany Bitcoin nesplňuje, dle aktuálně platných manuálů a jejich interpretace jsou tak digitální aktiva bez protistrany (tedy i bitcoin) považována za nefinanční aktivum. Pro úplnost dodáváme, že vedle existence protistrany jsou dalšími kritérii pro rezervní aktiva cizoměnovost a likvidnost. Detailně je metodika zachycení rezervních aktiv popsána v manuálu platební bilance a investiční pozice (BPM6), konkrétně par. 6.64-6.116.

22 Podle metodiky MMF se do výše oficiálních rezerv zahrnují např. i repo operace, tj. může dojít k „umělému“ navýšení rezerv oproti čisté hodnotě držených aktiv.

6.2 Přímé investice do bitcoinu v účetnictví ČNB

Existuje celá řada variant, jak by se mohl bitcoin v účetnictví ČNB projevit. Nicméně za předpokladu jeho dlouhodobé držby a ne příliš vysokého počtu transakcí (ve smyslu – ČNB se nestane high-frequency traderem) lze předpokládat následující pravidla.

Bitcoin v rozvaze ČNB: nehmotný majetek

Přímo držené bitcoiny budou vykazovány jako specifický nehmotný majetek v položce bilance „Hmotný a nehmotný majetek“. V případě významného objemu (mld. Kč) by bylo zváženo vytvoření samostatné dílčí položky v dekádní rozvaze.

Bitcoin bude oceňován nižší z ceny pořízení a aktuální reálné hodnoty, tj. bude na účtu v ceně pořízení a při poklesu reálné hodnoty bude vytvořena opravná položka. Zisky a ztráty budou účtovány pouze jako realizované. Při významném objemu bude nutné v účetní závěrce publikovat také aktuální reálnou hodnotu držby.

V nákladech ČNB by se nákupy bitcoinu mohly projevit pouze v případě, že dojde k objemově velmi nízkým nákupům s cílem otestovat budovanou interní infrastrukturu. Ve významnějších objemech nákupů se potom v nákladech vůbec neobjeví, z účetního hlediska půjde o podobné operace, jako když prodá jeden typ aktiva z devizových rezerv a nakoupí jiný.

6.3 Jak by ČNB prokazovala vlastnictví bitcoinů držených v self-custody externímu auditorovi?

Jak prokázat auditorovi (či veřejnosti) objem držených BTC?

Existuje celá řada možností…

V této otázce ještě stále není zcela jasno, a v případě, že by se ČNB rozhodla pro self-custody (tento problém se týká výhradně přímého způsobu držení bitcoinů, při využití externí custody neexistuje, protože potvrzení dodá přímo custodian), musela by být tato otázka explicitně diskutována a konkrétní způsob dohodnut s externím auditorem. Současní auditoři ČNB však při předběžných konzultacích potvrzovali, že to nepovažují za nepřekonatelný problém.

Existuje celá řada možností, jak tento krok provést:

- off-chain kryptografický důkaz vlastnictví privátního klíče (proof-of-ownership)
  (ČNB pomocí BIP 322 podepíše svým privátním klíčem předem domluvený text, auditor následně ověří, že příslušná adresa drží deklarované množství bitcoinů),
- mikrotransakce (proof-of-control)
  (ČNB odešle malou transakci ze své adresy; tato metoda je méně preferovaná, protože způsobuje pohyb prostředků a související náklady),
- ČNB veřejně deklaruje svou adresu
  (to umožňuje komukoliv sledovat veškeré transakce a zůstatky na této adrese; zveřejnění adresy je však mnohými považováno za možné riziko).

6.4 Bitcoin – digitální zlato?

Bitcoin je vzhledem ke svým vlastnostem často považován za novou, digitální formu zlata.

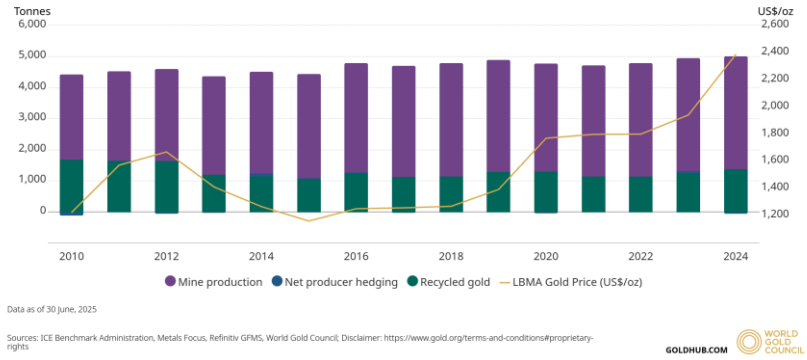
Omezená nabídka, vzácnost

Za hlavní argument je nejčastěji považován fakt, že emitováno může být celkově pouze 21 milionů bitcoinů a že tento objem je konečný. K červenci 2025 bylo přitom vytěženo již 19,9 mil. bitcoinů, k dosažení finální hranice tedy zbývá již jen přibližně 1,1 mil. BTC. Do konce současného období 2024 až 2028, kdy odměna za vytěžený blok představuje 3,125 BTC, bude přitom vytěženo ještě zhruba 0,4 mil. BTC, v následujícím období (2028 až 2032) poklesne odměna na polovinu (tzv. *halving*) a celkově bude za tyto 4 roky vytěženo zhruba 0,3 mil. BTC. Těžba bude dále pomalejší a pomalejší, a očekává se, že ustane v roce 2140.

Paralela se zlatem se v tomto bodu vysloveně nabízí. Zlata bylo podle údajů World Gold Council (WGC) v roce 2024 vytěženo 3 644 tun, což při celkovém objemu vytěženého zlata okolo 212 000 tun činí přibližně 1,7% roční nárůst. Nicméně odhaduje se, že přibližně 65 až 70 % zlata je použito k nefinančním účelům (výroba šperků, průmysl, zdravotnictví atd.). Těžba zlata je sice stále obtížnější, s rostoucí cenou jsou však přirozeně těžena také ložiska, která byla v minulosti považovaná za nerentabilní. Celková těžba zlata v posledních letech mírně roste, v roce 2024 bylo podle údajů WGC dosaženo nejvyššího objemu za rok vytěženého zlata v historii.

Celkový objem vytěžených bitcoinů nyní roste v ročním vyjádření přibližně 0,8% tempem, po roce 2028 pak bude jeho objem růst o 0,4 % za rok. Celkově lze tedy konstatovat, že pro finanční účely se růst objemu obou aktiv výrazněji neliší a dosahuje řádově necelého procenta za rok.

Graf 1-22: Objem těžby a recyklace zlata



Zdroj: World Gold Council

Omezená nabídka a stále zpomalující těžba bitcoinu je důvodem, proč BTC představuje důležitou „neinflační“ alternativu k dalším aktivům podobně jako zlato či další komodity. Sloužit proto může jako hedge (pojistka) ve světě, kde „fiat“ měny podléhají co do emitovaných objemů rozhodování centrálních bank.

Nezávislost, no-one’s liability

Bitcoin není závislý na žádné centrální autoritě, není ničím závazkem a je navržen jako tzv. permissionless, tedy převodu nemůže žádná další strana zabránit. Bitcoin lze tedy snadno a rychle převést za použití minimálních nákladů, čímž se však výrazně liší od zlata, kde transport mezi lokacemi představuje logisticky složitou a nákladnou operaci.

Stejně jako zlato, bitcoin nepředstavuje závazek za jakoukoliv osobou či institucí, nikdo jej nebude „splácet“, není to dluh či pohledávka. A podobně pak nejsou bitcoin ani zlato závislé na centrální autoritě či vládě.

V těchto rysech jsou si tedy obě aktiva velmi podobná, přičemž digitální podoba bitcoinu přináší některé výhody.

Odolnost proti zabavení, zmrazení

Bitcoin připomíná fyzická aktiva (mezi něž samozřejmě patří i zlato) držené investory přímo (v sejfu apod.) i v dalších aspektech. Protokol bitcoinu neumožňuje zásah jakékoliv autority, po jejímž nátlaku by mohlo dojít k zabavení či zmrazení tohoto aktiva. Opět, to je charakteristika, kterou se velmi podobá zlatu. Bitcoin samozřejmě lze podvodně zcizit (zneužití privátního klíče atd.), to je však možné i u fyzických aktiv (vykradení trezoru, okupace…).

Omezená korelace s tradičními aktivy

Jedním z důvodů, proč investoři často zařazují zlato do svého portfolia, je jeho omezená korelace s cenovým vývojem dalších finančních aktiv. V tomto je bitcoin do značné míry podobný – s dluhopisy nekoreluje téměř vůbec, od zlata se liší naopak tím, že v určité míře podléhá vývoji na trhu s rizikovými aktivy (např. akciemi) – viz kapitola 4.

Má bitcoin vnitřní hodnotu?

Otázka, zda má bitcoin vnitřní hodnotu (intrinsic value), patří mezi často diskutovaná témata. Odpověď však není jednoznačná – záleží na tom, jak definujeme „vnitřní hodnotu“ a z jakého pohledu se na bitcoin díváme.

Pokud za vnitřní hodnotu považujeme současnou hodnotu budoucích peněžních toků, které aktivum generuje, bitcoin vnitřní hodnotu nemá – negeneruje úrok či výnos, jeho hodnota není opřena o žádný statek. Podobně je tomu také v případě zlata. Zde lze však argumentovat, že jej můžeme využít v průmyslu, zdravotnictví, či k výrobě šperků, a že tudíž určitou vnitřní hodnotu musí mít (byť pokud by zmizel finanční aspekt držby, tato hodnota by značně poklesla).

Existuje však také alternativní pohled. Podle zastánců digitálních aktiv je třeba vnitřní hodnotu posuzovat nejen z hlediska užitečnosti, ale rovněž s ohledem na princip vzácnosti, síťový efekt, nezávislost a další klíčové faktory. Jako podstatné rysy vnímají též hodnotu schopnosti provádět transakce rychle a nezávisle na autoritách, a skutečnost, že je vzácný (viz omezení na 21 mil. BTC). Občas je pak z tohoto hlediska hodnocena též jeho energetická a technická náročnost. Podle některých existuje minimální hodnota (floor value) bitcoinu, která zjednodušeně zahrnuje náklady na pořízení hardwaru nutného pro těžbu a energii potřebnou k vytěžení jednoho bloku ve srovnání se získanou odměnou (sumě transakčních poplatků a tzv. *block subsidy* – tedy pevně stanovené odměny udělované těžařům za každý vytěžený blok) – tato minimální hodnota je dnes odhadována na přibližně 80 tis. USD/BTC.

A konečně existuje ještě jeden úhel pohledu – spočívá v odpovědi na otázku, zda mají vnitřní hodnotu samotné měny. Držení např. stodolarových či pětiseteurových bankovek samo o sobě taktéž hodnotu nejspíš nemá, a přesto tak řada tržních účastníků činí. V tomto ohledu je ale nutné poznamenat, že za každou měnou stojí ekonomika daného státu, která jistě svoji hodnotu má.

Studie World Bank

Otázkou, zda může bitcoin hrát roli při správě devizových rezerv, se zabývala také studie Světové banky z roku 2024[23]. Text obecně potvrzuje výše zmiňované argumenty, přesto dochází k závěru, že je nepravděpodobné, že by centrální banky v dohledné době zlato nahradily bitcoinem. Za hlavní argumenty autoři považují historickou úlohu zlata (zlatý standard a brettonwoodský systém), jehož držba je extrémně bezpečná, a pro něž již centrální banky mají vybudovanou infrastrukturu. Podle World Bank nyní centrální banky zlato nedrží kvůli jeho risk-return charakteristikám, ale spíše jako důsledek náhledu, že zlato a rezervní měny jsou i po kolapsu zlatého standardu do značné míry ekvivalenty. Pro úplnost je nutné dodat, že mnoho v textu použitých argumentů je dnes již neplatných a jeho závěry je třeba vnímat kriticky, resp. s určitou rezervou.

6.5 Bitcoin: víra, investiční mánie, nebo fundamentální změna přístupu k uchování hodnoty

Vzestup popularity

Bitcoin se od svého vzniku v roce 2009 postupně vyvinul z okrajového experimentu technologických nadšenců v jedno z nejdiskutovanějších aktiv dnešní doby. Zpočátku byl zájem tažen zejména komunitou kryptografů, libertariánů a technologických inovátorů, kteří v něm spatřovali především možnost finanční autonomie a odpor proti tradičním institucím. Postupně se však připojila širší veřejnost – investoři hledající zisk, média přitahovaná dramatickými cenovými pohyby a nakonec také finanční instituce, které se obávaly, že zůstanou pozadu.

Bitcoin jako fenomén víry

Jedním z klíčových motorů růstu ceny bitcoinu je skutečně „víra“ – přesvědčení investorů, že jeho hodnota bude v budoucnu stále růst. Tento efekt se posiluje s každou mediální zmínkou o nových cenových maximech a s každým příběhem o tom, jak se z drobného investora stal milionář. Psychologický mechanismus FOMO (fear of missing out – strach z toho něco propásnout) dále přispívá k tomu, že do trhu vstupují noví zájemci, což žene cenu vzhůru.

Mezi technologií a módní vlnou

Označit bitcoin za spekulativní bublinu je sice lákavé, avšak příliš jednostranné. Bitcoin totiž stojí na určité technologické inovaci – blockchainu – a nabízí reálné funkce, jako je decentralizované ukládání hodnoty či možnost relativně rychlých globálních plateb. Zastánci proto argumentují, že i když je cena volatilní, pod povrchem existuje technologie, která dává smysl. Kritici naopak tvrdí, že skutečné využití je omezené a že dominantním faktorem růstu je právě spekulace.

Generační faktor a „next-big-thing“

Zajímavým aspektem je generační rovina. Bitcoin a další digitální aktiva si oblíbila mladší generace, která přijímá nové technologie s menšími obavami, méně důvěřuje tradičním institucím a je otevřenější experimentům s novými formami investic. Pokud je ale bitcoin skutečně spíše kulturním než ekonomickým fenoménem, může být v budoucnu nahrazen „další velkou věcí“. Historie ukazuje, že generační trendy se proměňují – co bylo symbolem pokroku pro jednu generaci, může být pro příští jen kuriozitou.

—

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

Závěr: víra, nebo hodnota?

Otázka tedy zní: stojí růst ceny bitcoinu na fundamentu, nebo jde jen o kolektivní víru? Pravda možná leží někde mezi. Na jedné straně zde je technologie s reálným potenciálem, na druhé straně se cena v mnoha ohledech chová podle zákonitostí investičních mánií. Ať už budoucnost přinese pokračující růst, stagnaci, nebo nahrazení bitcoinů jiným fenoménem, je zřejmé, že bitcoin se již zapsal do historie jako příklad toho, jak může víra v technologickou inovaci přerůst v celosvětový ekonomický i kulturní příběh.

7. EXTERNÍ STUDIE

Studie VŠE a UK

Následující text shrnuje hlavní závěry a doporučení obsažená ve studiích objednaných a vypracovaných externími experty. První studii zpracoval tým expertů VŠE v Praze a druhou tým expertů Univerzity Karlovy.

Ve shrnutí záměrně nerozlišujeme, z které konkrétní studie jsou které informace čerpány. Pokud je citován souvislejší fragment textu, je zvýrazněn kurzívou.

Z hlediska hlavních závěrů a doporučení pro ČNB jsou obě studie ve shodě s našimi vlastními závěry. Pro případnou integraci bitcoinu v ČNB uvádějí:

- zavádění by mělo být postupné, s důrazem na operační rizika (governance, bezpečnost),
- v případě self-custody by měla být preferována robustní technická řešení (multisig, MPC), alternativně využívat regulované služby (custody, ETF),
- nezbytné bude následné kontinuální sledování technologických a regulatorních změn,
- za důležitý element považují obě studie komunikaci s veřejností, v případě přímé investice v self-custody transparentnost držení a obecně auditovatelnost.

Obě studie považují bitcoin za technologicky stabilní a ekonomicky perspektivní aktivum, které však vzhledem ke své povaze vykazuje některá ryze specifická rizika.

Těžištěm zájmu obou dokumentů byla právě tato rizika, ať už jsou spojena se samotnou technologií bitcoinu a blockchainu či jeho ekonomickými a institucionálními aspekty. Práce se široce zabývají otázkami governance, škálovatelností a dalšími oblastmi navázanými na bitcoin. Závěry obou studií shrnujeme v dalších podkapitolách, a byť mohou být některé dílčí aspekty hodnoceny kriticky, vyznění obou studií je shodné: bitcoin se dostává do fáze stability a již nyní je připraven stát se součástí institucionálních portfolií.

7.1 Digitální rizika

Technologický rozvoj a governance bitcoinu

Bitcoin je:
- decentralizovaný a distribuovaný
- založený na kosenzu a Proof-of-Work
- omezený objem BTC
- odolný vůči omezením, manipulaci a výpadkům

Bitcoin protokol je decentralizovaný systém pro uchovávání a přenos digitální hodnoty, který využívá technologii distribuované účetní knihy (blockchain). Základem protokolu je konsenzuální algoritmus Proof-of-Work, díky němuž se účastníci sítě (tzv. těžaři) podílejí na validaci transakcí a vytváření nových bloků. Každý plnohodnotný uzel v síti uchovává úplnou kopii blockchainu a nezávisle ověřuje příchozí transakce i bloky. Díky tomu je systém odolný vůči manipulaci, cenzuře i výpadkům jednotlivých částí infrastruktury. Klíčovým rysem bitcoinu je jeho otevřenost, transparentnost a předem daný emisní plán, který omezuje maximální počet bitcoinů na 21 milionů kusů.

Vznikl v 2009, dnes je architektura stabilní

Technologický základ bitcoinu byl položen v roce 2009. Od té doby prošel rozsáhlým vývojem, avšak základní architektura zůstává stabilní a konzervativní. Tato stabilita není náhodná – jde o záměrný prvek designu, jehož cílem je zajištění důvěryhodnosti, bezpečnosti a předvídatelnosti systému.

Základní vrstva = Layer 1
(k inovacím může docházet na vyšších vrstvách bez nutnosti měnit protokol)

Rozvoj bitcoinu probíhá ve třech hlavních vrstvách. První vrstvu tvoří základní protokol (Layer 1), kde jsou změny velmi řídké a typicky mají podobu tzv. *soft-forků* – tedy zpětně kompatibilních úprav. Známými příklady jsou SegWit (2017) a Taproot (2021). Druhou vrstvu představují nadstavbová řešení (Layer 2), jako je Lightning Network či Liquid Network. Tato vrstva přináší nové funkcionality, především v oblasti mikroplateb, škálovatelnosti a zvyšování efektivity bez zásahu do základní vrstvy. Třetí složkou je podpůrná infrastruktura – hardware peněženky, knihovny, bezpečnostní řešení jako multi-sig či MPC.

Bitcoin je „open-source“ projekt

Bitcoin je open-source projekt. Jeho vývoj je otevřený a decentralizovaný, a přesto vykazuje vysoký stupeň koordinace. Klíčovým mechanismem je návrhový proces BIP (Bitcoin Improvement Proposal), který slouží k předkládání a diskusi návrhů na změny protokolu. Nejde o právně závazný rámec, ale o technický standard. Případné změny jsou implementovány pouze tehdy, pokud získají dostatečný konsenzus mezi vývojáři, těžaři a provozovateli uzlů.

Governance bitcoinu? Protokol

Governance bitcoinu je specifická svou absencí centrální autority. Neexistuje žádná instituce, která by mohla měnit pravidla sítě nebo vynucovat jejich dodržování. Pravidla jsou obsažena v tzv. protokolu, tedy jsou zakódována v softwaru a vynucována technickým chováním sítě. Tento model „governance bez vlády“ zajišťuje vysokou odolnost vůči cenzuře nebo zneužití moci, ale zároveň přináší určité nevýhody – např. pomalejší reakci na bezpečnostní hrozby nebo neefektivní rozhodovací proces v případě sporů.

I protokol je však možné změnit, pokud existuje konsenzus

Změny v protokolu, například zmíněné Taproot nebo SegWit, ukázaly, že i technicky vyspělé a komunitně podporované návrhy potřebují roky k implementaci. Tento pomalý rytmus vývoje je však v bitcoinu vnímán pozitivně – jako ochrana proti unáhleným zásahům, které by mohly ohrozit důvěru v síť.

Odchýlení od protokolu: izolace…

Absence právně závazného rule-booku je nahrazena síťovou dynamikou: každý účastník sítě se rozhoduje, který software použije, a odchýlení od většinového konsenzu znamená izolaci. Rizika decentralizované governance zahrnují možnost hard-forku, tedy trvalého rozdělení blockchainu, což se historicky stalo např. při vzniku Bitcoin Cash. Přestože

taková událost nepředstavuje technickou hrozbu, může vést ke krátkodobé nejistotě a narušení důvěry.

Bitcoin rovněž těží z reputačních motivací svých přispěvatelů – vývojáři, provozovatelé uzlů a těžaři mají tzv. skin in the game. Investují čas, zdroje a reputaci do systému, jehož stabilita ovlivňuje hodnotu jejich vlastních aktiv. Tím vzniká přirozená motivace k údržbě a zodpovědnému rozvoji.

Chybějící centrální autorita: výhoda, či nevýhoda?

Z hlediska institucionální důvěry představuje absence centralizované autority výhodu i riziko. Výhodou je vysoká odolnost vůči politickému nebo regulatornímu zásahu. Rizikem je neexistence vymahatelné odpovědnosti v případě selhání. Dosavadní zkušenost však ukazuje, že komunitní model bitcoinu dlouhodobě funguje stabilně a je schopen zvládat zásadní technické a organizační výzvy.

Technologický vývoj a governance bitcoinu tvoří unikátní kombinaci technické stability s otevřeností k inovacím prostřednictvím komunitního konsenzu. Tento model není bez rizik, ale zároveň nabízí vysokou úroveň důvěryhodnosti, která je nezbytná pro jeho možné institucionální přijetí – včetně potenciálního začlenění do rezervní strategie centrální banky.

Riziko hard forku

Hard fork je často zmiňován jako jedno z hlavních rizik, jež bývá s bitcoinem spojováno. Obě studie se nicméně shodují, že toto riziko nevede ke ztrátě dat či přímé devalvaci.

Hard fork – změna protokolu bez zpětné kompatibility (nasadit se musí nová verze softwaru)

Několik neúspěšných hard forků již nastalo, bitcoin to neohrozilo

Hard forky – tedy trvalé rozdělení blockchainu na dvě či více nekompatibilní větve v důsledku zavedení zpětně nekompatibilní změny protokolu – mohou mít různou podobu. Buď se jedná o *plánované hard forky* prováděné se širokou shodou komunity, typicky s cílem zavést radikální inovace. V prostředí bitcoinu se téměř nevyskytují, preferovány jsou *soft-forky*. Existuje však i riziko *kontroverzních hard forků*, kdy shody dosaženo není, vytvořen je alternativní softwarový klient s odlišnými pravidly a pokud tento nový klient získá podporu části uzlů, dojde k vytvoření další sítě. Nejznámějším příkladem takovéhoto forku je Bitcoin Cash (2017) či následný fork tohoto forku Bitcoin SV (2018).

Hard fork – držitelé získají přístup k prostředkům na obou větvích!

Držitelé privátních klíčů však mají i v případě hard forku přístup ke stejným prostředkům na obou větvích řetězce. Hlavním problémem tak není samotné rozdělení, ale tržní ocenění jednotlivých větví a související rizika, například potenciál tzv. *replay attacks* (opakované využití transakce na obou větvích) nebo dočasná nekompatibilita služeb.

Pravděpodobnost hard forku je obecně hodnocena jako velmi nízká. Těžaře, uživatele, vývojáře a ekonomicky významné hráče (burzy, pooly) spojuje zájem, aby se i nadále jednalo o úspěšnou platformu. Neshody mezi nimi mohou vést k erozi důvěry a následné fragmentaci řetězce. Rizikovým faktorem však mohou být vnější tlaky, ať už se jedná o regulatorní zásahy, které by mohly komunitu rozdělit podle geografických či právních hranic. V tomto ohledu se však zdá, že bitcoin vstupuje do příznivějšího období.

„Empirická zkušenost ukazuje, že rozkol v komunitě může vést k vytvoření nové větve, která si ale bez podpory infrastruktury nezíská tržní relevanci. Příkladem je vznik Bitcoin Cash (BCH) v roce 2017, ke kterému došlo v důsledku nesouhlasu s implementací SegWit a neochoty zvýšit velikost bloku. Obě větve dnes existují, ale bitcoin (BTC) si udržel více než 95 % kumulované tržní kapitalizace. Je nutné zmínit i částečně úspěšný a v mnoha ohledech specifický hard fork Litecoin, který má aktuálně kapitalizaci nižší

než BCH. Další hard forky jako Bitcoin Gold (BTG) mají minimální tržní kapitalizaci (aktuálně okolo 13 mil. USD oproti více než 2 bil. USD pro BTC), případně již nejsou udržovány (Bitcoin XT, Bitcoin Classic a Bitcoin Unlimited). To ukazuje, že trh preferuje stabilitu, technickou konzervativnost a síťový efekt originálního řetězce.“

Riziko hard forku hodnoceno jako nízké

Riziko dalšího hard forku bitcoinu tedy existuje, nicméně obě studie ho hodnotí jako nízké a i v případě jeho realizace nejsou důsledky dramatické. Hard forky tak nepředstavují riziko ztráty hodnoty, jako spíše zvýšení míry nejistoty v ekosystému bitcoinu. Možnost forku je obecnou vlastností otevřených systémů bez centrální autority. Bitcoin v tomto prostředí svou dominanci nejen neztratil, ale postupně posiluje. Jedna ze studií zmiňuje, že tento vývoj dobře popisuje teorie her a její koncept Schellingova bodu[24].

Riziko 51% útoku

51% útok = ovládnutí blockchainu, které umožní manipulaci s bloky

51% útok je kritickou zranitelností společnou pro všechny technologie založené na blockchainu. V principu se jedná o riziko, že jeden subjekt (či ve shodě jednající skupina subjektů) ovládne většinu výpočetního výkonu sítě (v hantýrce označovaný jako hashrate) a s tímto výkonem dokáže vytvářet nejdelší řetězec bloků. Tímto způsobem potom může s blockchainem manipulovat (např. provádět double spending, zabraňovat potvrzování některých transakcí a hrozí též vytěsňování ostatních těžařů – těžit nové bloky bude pouze majoritní útočník).

Vzhledem k objemu prostředků investovaných do těžby a její vysoké fragmentaci se dnes za riziko u bitcoinu nepovažuje

V současnosti je riziko takového útoku považováno u bitcoinu za velmi nízké. Odhaduje se, že náklady na získání hardwaru potřebného k dosažení 51 % hashrate činí v současnosti stovky miliard USD. Potenciální útočník by však čelil zásadnímu ekonomickému riziku – úspěšný útok tohoto typu by pravděpodobně vedl ke ztrátě důvěry v bitcoin a k prudkému poklesu jeho tržní ceny. Výsledkem by mohlo být, že hodnota získaných prostředků by byla nižší než celkové náklady útočníka (propad ceny bitcoinu, znehodnocení nákladně pořízeného těžebního hardwaru). Motivace k realizaci 51% útoku je tedy v praxi výrazně omezena kombinací vysokých nákladů, technologických limitů a negativních ekonomických důsledků.

Dominance bitcoinu je hrozbou pro další digitální měny

Zatímco bitcoin samotný je tedy k úspěšnému provedení tohoto typu útoku příliš nákladný cíl, existující hardware nasazený dnes k jeho těžbě může být často snadno přesměrován na těžbu menších „coinů“. Tyto alternativní řetězce pak čelí disproporčně vyššímu riziku útoků, což ostatně v minulosti vedlo k řadě incidentů[25]. Právě tato bezpečnostní asymetrie je jedním z faktorů, které dále upevňují dominantní postavení bitcoinu.

I přes velmi nízkou míru rizika se však obvykle doporučuje vyžadovat několikeré potvrzení transakce. Uvádí se, že za prakticky nezvratné se považuje šestinásobné potvrzení (tj. vytvoření šesti dalších bloků v blockchainu).

Souhrnně – 51% útok je teoreticky možný, v praxi však v důsledku ekonomických, technických, koordinačních a reputačních důvodů považují studie takovou hrozbu za krajně nepravděpodobnou.

—

24 Jedná se o řešení, které účastníci hry preferují při nemožnosti vzájemné komunikace, a které se zdá intuitivní a přirozené. V tomto případě je zmíněným bodem původní verze bitcoinu, jinými slovy je preferováno to, co je vyzkoušené a funkční.

25 Bitcoin Gold v roce 2018 – ukradeno bylo 18 mil. USD, bitcoin SV v roce 2021 utrpěl celou řadu 51% útoků a hackerům se podařilo smazat či pozměnit nejnovější bloky, Ethereum Classic v roce 2020, ukradeno bylo údajně několik milionů dolarů

Riziko kvantových počítačů[26]

Rozvoj kvantových počítačů představuje teoretickou hrozbu

V praxi se však zneužití pro tyto účely v blízké budoucnosti nečeká

Za riziko je pro bitcoin považován rozvoj kvantových počítačů. Riziko jejich nasazení k provedení 51% útoku je spíše teoretické, počet požadovaných fyzických kvantových bitů (tzv. *qubitů*) v kvantovém procesoru by se musel pohybovat okolo milionu[27]. V současnosti mají nejrozvinutější kvantové procesory stovky až nižší tisíce qubitů, ale technologie je stále velmi chybová[28].

Mírně odlišná je situace v otázce prolomení privátního klíče. Při použití přibližně 1 500 až 2 000 logických qubitů[29] je prolomení dnes používané 256bitové ECDSA asymetrické kryptografie teoreticky možné. Pro jednou zveřejněný public klíč by pak bylo možné vypočíst privátní klíč a následně jej pak zneužít. Při dnešním stavu technologií jsme však několik řádů od stavu, který by takový útok vyžadoval. Vytvoření stabilních logických qubitů dnes již není výrazný problém. Stále ale není plně vyřešena otázka provádění výpočetních operací s tímto typem qubitů. Odhaduje se, že tzv. kryptograficky relevantní kvantový počítač bude dostupný nejdříve v roce 2030, ale spíše až okolo poloviny třetí dekády.

Obrana existuje a rozvíjí se: **postkvantová kryptografie**

Komunita si je této hrozby vědoma a již nějakou dobu se diskutuje nad kvantově odolnými podpisovými schématy (tzv. postkvantová kryptografie). Stejně tak je potenciálně ohrožena celá řada dalších oblastí závisejících na dnešních kryptografických algoritmech, včetně bankovních aplikací, obecně digitálních podpisů atd. Bitcoin tedy není jedinou technologií, která je tímto rizikem ohrožena. Je součástí širší množiny technologií závisejících na digitální důvěře, která by musela včas reagovat a změnit způsob svého fungování. Aktuálně existuje řada iniciativ zabývajících se přechodem na postkvantovou kryptografii. Příkladem je projekt LEAP zaštítěný Bankou pro mezinárodní platby (BIS) týkající se mezibankovní komunikace či doporučení bezpečnostní agentury Velké Británie[30]. Rovněž existuje řada postkvantových šifrovacích algoritmů, které v současnosti prochází standardizačním procesem NIST: hash-based schéma XMSS, lattice-based systémy či multivariantní Rainbow.

I bez postkvantové kryptografie existují možnosti obrany: **prokazování nabývacího titulu**

Ani ve velmi nepravděpodobném případě, že nebudeme schopni nalézt bezpečný způsob postkvantové kryptografie, to nemusí nutně vést ke konci bitcoinu. Držitelé bitcoinů by v takovém případě prokazovali nabývací titul (legitimní transakce) k aktivům, nikoli tedy jen vlastnictví soukromého klíče. Oprávnění držitelé bitcoinů by tak o ně nepřišli, není pravděpodobné, že by je v takové situaci šlo prostě odcizit z peněženek bez jakékoliv možnosti obrany.

---

26 Tato kapitola vznikla ve spolupráci s Martinem Veselým, který tímto doplnil některé nepřesnosti obsažené v obou studiích.

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

28 Google Willow chip: 105 fyzických qubitů, IBM Condor: dosahuje 1121 fyzických qubitů, ale bez error-correctionu, tedy v praxi k útoku nepoužitelné, Atom Computing (ve spojení s Microsoftem): 50 logických qubitů v roce 2026 / přes 1000 fyzických qubitů. D-Wave: 5 000 qubitů, ale procesor je určen pouze pro optimalizační úlohy.

29 Logický qubit je skupina fyzických qubitů seskupených za účelem korekce chyb. Podle použitého opravného kódu je na jeden logický qubit potřeba 10 až 1 000 fyzických qubitů.

30 Timelines for migration to post-quantum cryptography

Riziko závislosti na internetu

Bitcoin není na internetu zcela závislý

Obě stanoviska se shodují, že internet (resp. dnes používaný komunikační protokol TCP/IP) je pro fungování bitcoinu pouhým médiem. Existence a fungování bitcoinu, tedy jeho kryptografické principy a způsob ukládání záznamů do distribuované účetní knihy, blockchainu, však na internetu závislé nejsou.

Dočasné přerušení komunikace v síti není problém

Po obnovení spojení mezi nody dojde k reorganizaci

Popišme, jaké dopady by výpadek internetu měl. Již existující bloky dále v jednotlivých uzlech přetrvávají, každý uzel si totiž neustále uchovává svou kopii. Bez možnosti komunikovat s ostatními uzly by se bitcoinová síť pravděpodobně rozpadla na lokální izolované ostrovy, jež by v extrémní situaci byly tvořeny jen jednotlivými těžaři. V rámci těchto ostrovů by dále probíhala těžba nových bloků. Po navázání konektivity (ať už z důvodu znovuobnovení provozu internetu či jeho nahrazením alternativními komunikačními prostředky) si uzly vymění informace o stavu svých řetězců, a ve snaze dosáhnout konsenzu se novým globálním řetězcem stane ten nejdelší. Kratší řetězce jsou reorganizovány a jejich transakce se vrací zpět (do mempoolu) ke zpracování. Je zřejmé, že výhodu by měl ostrov s nejvyšším výpočetním výkonem. Tento proces, kdy dojde k „zahození“ kratších řetězců a novým konsenzem se stává nejdelší řetězec, se nazývá *reorganizace* blockchainu.

Riziko výrazné reorganizace blockchainu roste s délkou výpadku. Divergenci mezi vývojem v jednotlivých uzlech se již dnes snaží zabránit mimointernetové kanály, které nahrazují internet alternativními způsoby přenosu informací. Například Blockstream Satellite[31] vysílá kontinuálně stav blockchainu prostřednictvím družic bez závislosti na stavu internetu, existují i pozemní alternativní sítě[32] usilující o totéž.

Problémem by bylo trvalejší přerušení komunikace

Trvalejší výpadek internetu by však samozřejmě pro bitcoin problém představoval. Bitcoin by přestal fungovat jako prostředek pro provádění transakcí, přišel by o likviditu a velmi pravděpodobně by to vedlo k dramatickému poklesu jeho hodnoty. Je však nutné zdůraznit, že v takovémto scénáři by byl v hluboké krizi celý svět – nefungovaly by pravděpodobně klasické platební systémy, cloudové služby, došlo by k rozpadu logistiky, dodavatelských řetězců atd. Ztráta hodnoty bitcoinu by tak byla jen sekundárním projevem široké systémové krize.

7.2 Regulatorní a další podobná rizika

Riziko státního odmítnutí / geografická rizika

Možnost regulačních zásahů jednotlivých států není pouze teoretickou hrozbou.

K největšímu omezení došlo v 2021 v Číně

Těžba se jen přesunula jinam…

Za největší událost tohoto typu se považuje zásah Číny v roce 2021, kdy byla v zemi plošně zakázána těžba bitcoinu. Deklarovaným cílem bylo omezení energetické náročnosti, v pozadí však hrály roli i snahy o kontrolu kapitálových toků. Okamžitě došlo k poklesu globálního hashrate – podle dostupných dat až o 50 %. Těžba se však rychle přesunula do jiných jurisdikcí, zejména USA, Kazachstánu, Ruska a zemí jihovýchodní Asie. A nejedná se jen o nadnesený popis situace, ve velké míře opravdu došlo k fyzickému přesunu hardwaru používanému k těžbě bitcoinu do jiných

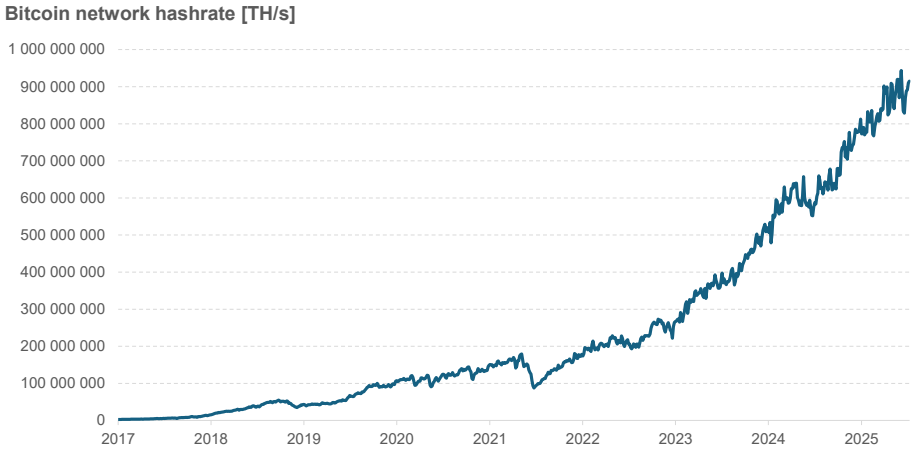
—

31 https://blockstream.com/satellite/

32 goTenna, Locha Mesh, Kryptoradio

zemí. V této souvislosti je pozoruhodné, jak rychle bylo dosaženo původní výkonnosti sítě.

Graf 1-23



Zdroj: data – blockchain.com, graf ČNB

Méně těžařů znamená jejich vyšší zisky

V této souvislosti je vhodné zmínit ekonomické incentivy, které jsou s podobnými zásahy spojeny. Zákaz těžby v Číně vedl k dramatickému poklesu celkového výkonu sítě, což znamenalo, že pro zbývající těžaře mimo Čínu dvojnásobně vzrostla pravděpodobnost nalezení bloku. To způsobilo výrazný nárůst očekávaných výnosů těžby a vytvořilo silný ekonomický tlak na rychlou relokaci těžební infrastruktury, což se přesně stalo. Již během roku 2022 byl výkon sítě zpět na původních úrovních a následně pokračoval v prudkém růstu.

Existují však samozřejmě také další regulatorní rizika, týkat se mohou zdanění těžby, požadavků na licencování těžby, geoblokace přístupu, v souvislosti s ochranou spotřebitele se často mluví i o nutnosti zavést standardní KYC/AML postupy, diskutují se rovněž daňové otázky. Z hlediska bitcoinu se za nejzávažnější riziko považuje možnost omezení přístupu ke kritické internetové infrastruktuře či přijetí legislativy, která by bez souhlasu státu těžbu neumožňovala. Takovéto přístupy jsou v současnosti zvažovány převážně v autoritářských režimech, kde existuje silný tlak na kontrolu kapitálových toků.

Spíše než snaha omezit Bitcoin regulací se dnes prosazuje přístup **zregulovat a „zrovnoprávnit“ na úroveň ostatních aktiv**

Z globálního hlediska se však stále ve větší míře převládá strategie „toleruj a zdaňuj“. Jednotlivé státy si uvědomují, že přemrštěná regulace či zákazy by vedly pouze k přesunu těžby do ostatních zemí, a došlo by tak ke ztrátě potenciálních daňových příjmů. Postupně jsou tak zaváděny daně, reporting, kapitálové požadavky atd. bez ztráty kontroly nad trhem. Tato strategie se tak nyní zdá jako nejvýhodnější pro všechny zapojené subjekty.

Výraznější restrikce/regulace možné, pokud Bitcoin dál prudce poroste

Možným rizikem je také zásah států v případě, že by bitcoin dosáhl makroekonomické relevance. Pokud by přesáhl rozměr spekulativního aktiva a dosáhl velikosti, kdy by mohl ohrožovat měnovou suverenitu, stabilitu kapitálových trhů či ohrožoval fiskální politiku, může být vnímán jako systémové riziko. Autority by pak mohly přistoupit k výrazným restrikcím.

Bitcoin <> DLT!

Přístup zemí se však v současnosti vyvíjí spíše opačným směrem. V USA v důsledku nástupu Trumpovy administrativy zavládlo výrazně příznivější

prostředí, a i v Evropě – i přes hlasitý odpor ECB[33] – celkově dochází ke stále většímu přijetí. Obecně pak nastává rozmach technologií založených na distribuovaném registru/účetní knize (distributed ledger technology, DLT).

Celkově tedy lze říct, že vzhledem k decentralizované povaze infrastruktury bitcoinu je velmi nepravděpodobné, že by regulatorní omezení měla výraznější dopad, s výjimkou situace, kde by došlo ke (globálně) koordinovanému politickému rozhodnutí bitcoin omezit.

Environmentální a reputační tlaky

Proof-of-Work příčinou vysoké energetické náročnosti

Bitcoin byl navržen s konsenzuálním mechanismem pro potvrzování transakcí založeným na tzv. Proof-of-Work (PoW). V praxi se jedná o na první pohled nesmyslné hledání kryptografického otisku (tzv. hash) s určitými vlastnostmi, což je velmi složitý a výpočetně náročný proces. Toto hledání s sebou nese vážný problém, extrémní energetickou spotřebu. Odhaduje se, že v současnosti těžaři bitcoinu spotřebovávají 140 až 180 TWh za rok (pro srovnání – ČR vyprodukovala v 2023 77 TWh), což odpovídá průměrnému příkonu okolo 20 GW, tedy 20 temelínských bloků.

Spotřeba energie může být vnímána jako sama o sobě problematická. Jednak může vést k regulatorní snaze omezit technologie založené na PoW a nahradit je alternativami (např. Proof-of-Stake/PoS používaný Ethereum) a úzce tak souvisí s riziky zmiňovanými v předchozí kapitole.

Již dnes však dochází k výraznému posunu, bitcoin je často těžen v místech s velmi levnou elektřinou (např. na místech s celoročním slunečním svitem při využití solárních elektráren) či s nevyužitelnými přebytky energie (těžaři jako „kupci poslední instance“, jejich stroje tak typicky běží jen v momentech energetické nadprodukce, např. z OZE) a mohou tak přispívat ke stabilizaci rozvodných sítí v místě svého působení. Navíc se uvádí, že bitcoin má dnes čistší energetický mix než vykazuje v průměru světová energetika. Podle některých odhadů pochází již dnes více než polovina spotřeby sítě z obnovitelných či nízkoemisních zdrojů.

Proof-of-Work bitcoinu je považován za důležitý bezpečnostní mechanismus

Proof-of-Work je vnímán komunitou jako důležitý bezpečnostní aspekt fungování celého ekosystému bitcoinu. Teoreticky je přechod na Proof-of-Stake možný[34] a lze si představit scénář, kdy by k takovému kroku byl bitcoin přinucen globální koordinovanou snahou ze strany hlavních světových ekonomických mocností. Nicméně konsenzus v síti dnes udržují těžaři, tedy držitelé Proof-of-Work, kteří již investovali značné finanční prostředky do těžební infrastruktury, a přechod na Proof-of-Stake proto není v jejich zájmu.

---

33 Christine Lagarde: „Žádný členský stát EU nepřijme Bitcoin do rezerv.“ https://www.bloomberg.com/news/articles/2025-01-30/lagarde-is-confident-eu-central-banks-will-shun-bitcoin-reserves

34 Ethereum úspěšně přešlo na PoS v roce 2022, energetická náročnost poklesla o 99 %.

7.3 Ekonomická rizika

Riziko nahrazení bitcoinu jiným kryptoaktivem

Prvenství bitcoinu napomohlo jeho současné dominanci

Bitcoin ve velké míře těží ze svého prvenství. Díky rychlému rozvoji, počtu uživatelů a objemu investic do těžební infrastruktury se dnes zdá, že alternativní digitální aktiva by mohla bitcoin nahradit pouze v případě, že nabídnou zásadní inovace či užitek (např. již zmiňovanou kvantovou odolnost, kterou však nakonec může poskytnout i bitcoin). Mezi stávajícími těžaři či držiteli bitcoinu jsou však motivy k přechodu na jinou měnu velmi nízké.

Síla bitcoinu stojí na teorii her, a konkrétně na Schellingově bodu: racionální účastníci spontánně konvergují k řetězci s největší kumulovanou prací, likviditou a infrastrukturou, protože právě tam je nejnižší riziko reorganizace a nejvyšší profit z těžby i obchodování. Minulé hard-forky (BCH, BSV, ETHW) ukázaly, že i mírně slabší řetězec rychle ztrácí na významu a dominantní pozici si vždy udržel původní bitcoin.

Současné silné postavení bitcoinu a neexistující pobídky držitelů a těžařů pro přechod k jiné (lepší) technologii proto dnes spíše posilují dominantní postavení bitcoinu ve srovnání s ostatními digitálními aktivy. Riziko přechodu a s ním spojená možnost znehodnocení bitcoinu je proto považováno za velmi nízké.

Riziko omezení podpory těžby

Halving bude postupně nahrazován transakčními poplatky

Jak je všeobecně známo, bitcoin byl navržen tak, aby nebylo možné vytěžit více než 21 milionů kusů. Nové bitcoiny vznikají výhradně těžbou, tedy potvrzováním transakcí. Za nově vytěžený blok obdrží těžař pevně stanovenou odměnu, tzv. block subsidy, která v současnosti činí 3,125 BTC (v pravidelném čtyřletém cyklu dojde ke snížení odměny na polovinu – tzv. halving[35]) a dále součet všech transakčních poplatků definovaných jednotlivými převody obsažených v bloku (tyto poplatky si odesílatelé stanovují sami na základě vlastního uvážení, pokud tedy chtějí zvýšit pravděpodobnost zapsání transakce již v příštím bloku, typicky je dobrovolně mírně zvýší). Obava tak plyne z faktu, že snižováním block subsidy se může stát, že těžba nových bloků bude ekonomicky neefektivní.

Teoretické riziko, že transakční poplatky a vysoké náklady na těžbu povedou k opouštění sítě, však přesto existuje

Studie toto riziko považují za omezené. Předpokládá se, že stále důležitější roli budou hrát poplatky ze zapsaných transakcí, což je ostatně trend pozorovaný v malé míře už dnes. V dobách, kdy block subsidy činila násobky současné úrovně, nehrály transakční poplatky prakticky žádnou roli. Dnes běžně představují několik procent z celkové odměny těžařů, ve špičkách dosahují 5 a více procent a v několika obdobích (např. v roce 2017) dosáhly dokonce většinu odměny. V budoucnu se předpokládá zesílení tohoto trendu.

Přesto existuje teoretické riziko tzv. „fee death spiral“. Pokud by výnosy z poplatků nebyly dostatečné k pokrytí provozních nákladů těžařů a zároveň by block subsidy již neexistovala, část těžařů by síť opustila, čímž by došlo ke snížení bezpečnosti. Ačkoliv tento scénář zatím nebyl empiricky pozorován, nelze jej vyloučit, zejména pokud by poptávka po on-chain

35 Existují teorie, podle kterých je halving důležitým faktorem, v jehož důsledku roste cena bitcoinu. Podle těchto teorií tímto způsobem klesá nabídka nových coinů, což při jinak shodné poptávce vyvolává tlak na cenu bitcoinu.

transakcích zásadně poklesla nebo se většina provozu přesunula do sekundárních vrstev.

Riziko selhání společnosti (Micro)Strategy

Jedno ze stanovisek se explicitně věnuje možnosti, že by trh s bitcoinem mohly poškodit případné ekonomické problémy společnosti Strategy (dříve MicroStrategy, ticker MSTR) Michaela Saylora. Ta je známá tím, že před časem vsadila na investice do bitcoinu, přičemž tyto nákupy financuje celou řadou finančních produktů (od těch zcela konvenčních, jako jsou úpisy vlastních akcií společnosti, až po poměrně neortodoxně strukturované preferred dluhopisy). Odhaduje se, že Strategy dnes sama drží zhruba 2,9 % objemu existujících bitcoinů. Často je zmiňována i poměrně vysoká prémie, se kterou se dnes akcie MSTR obchodují (v závislosti na vývoji trhu 150 až 180 % hodnoty držených bitcoinů).

(Micro)Strategy i přes neortodoxní politiku firmy nepředstavuje výraznější hrozbu

Stanovisko se však soustředí na fakt, že celkový dluh Strategy je stále poměrně nízký (pákový efekt jen přibližně 20 %) a že k tomu, aby se společnost vůbec mohla dostat do problémů, musel by bitcoin poklesnout na velmi nízké hodnoty a zůstat na nich po delší dobu (zmiňováno je, že několik let by se bitcoin musel pohybovat okolo 18 000 USD). Stanovisko tak konstatuje, že společnost Strategy pro bitcoin nepředstavuje bezprostřední hrozbu.

Velmi vysoká volatilita ceny bitcoinu

Analýzy docházejí při hodnocení volatility ke shodným závěrům, jako ČNB samotná – volatilita ceny bitcoinu je ve srovnání s ostatními, „konvenčními“, aktivy velmi vysoká. Nicméně, i zde lze pozorovat znatelný vývoj.

Volatilita velmi vysoká, epizodně se blíží zlatu a akciovým indexům

Předně, bitcoin i přes nárůst celkové kapitalizace nad 2 biliony USD zůstává aktivem s relativně nízkou tržní kapitalizací (kupř. velikost trhu s americkými vládními dluhopisy se blíží k 30 bilionům), obchodní aktivita tedy může vést k větším cenovým výkyvům. Trh je navíc ve velké míře ovlivňován obchodní aktivitou retailových investorů, kteří jsou velmi citliví na jakékoliv mediální zprávy – roste tak riziko stádního procyklického chování.

Volatilita – hrozba, nebo příležitost?

Volatilita BTC stále dosahuje násobků volatility ceny zlata (které je samo o sobě považováno za velmi volatilní aktivum), avšak postupně se přibližuje k volatilitě cen některých rizikovějších akciových titulů (kupř. technologických společností). V některých obdobích (04/2025) pak volatilita bitcoinu krátkodobě poklesla pod volatilitu akciových indexů (S&P500, NASDAQ, ale i zlata). Předpokládá se, že klesající volatilita jde ruku v ruce s přibývajícími institucionálními investory a jejich buy&hold strategií. Ve stejném směru pak působí i aktivity velkých držitelů bitcoinů (tzv. whales), kteří od roku 2020 drží na burzách stále menší objem svých holdingů. Jako určitou možnost pak lze považovat i to, že s postupným růstem tržní kapitalizace bitcoinu a stále větší rolí institucionálních investorů, trh s bitcoinem již přešel do nové fáze charakterizované nižší volatilitou.

Jedno externí stanovisko však uvádí důležitý aspekt spojený s volatilitou – její vysoké hodnoty nejsou jen hrozbou, ale také potenciál pro mimořádné výnosy. Zmiňovány jsou ekonomické studie, které po očištění o makroekonomické faktory dlouhodobě potvrzují pozitivní vztah mezi volatilitou a tržními prémiemi. Jinými slovy – že aktiva, jejichž ceny jsou velmi volatilní, nabízejí mimořádné výnosy (ale také možnost mimořádné ztráty).

7.4 Operační rizika

Riziko ztráty/zneužití privátního klíče

Riziko spojené se ztrátou či zneužitím privátního klíče k přímo drženým bitcoinům (self-custody) není srovnatelné s žádným jiným operačním rizikem, se kterým se ČNB dnes setkává[36]. Studie se shodují, že pokud se ČNB pro investici do BTC rozhodne, bude nutné důkladně toto riziko vyhodnotit a nastavit robustní procesy, které by jej eliminovaly.

Případné přijetí bitcoinu musí být opatrné a dobře naplánované

Obě studie doporučují postupnou a opatrnou integraci bitcoinu. Správu klíčů v prvních fázích navrhují spíše zajistit externě (buď prostřednictvím investice do ETF, či použitím custodiana, který investora od správy privátních klíčů zcela izoluje, což je případ např. nejrozšířenější Coinbase Custody) a interně pak jen v omezeném rozsahu testovat přímé držení bitcoinu při použití self-custody. Možnosti zabezpečení se pak podle externích posudků shodují s těmi popsanými v kapitole 5.2: tj. zejména MPC a multi-sig. Za nejmodernější a pro finanční instituce nejvhodnější pak považují použít právě MPC.

Operační rizika nesrovnatelná s „konvenčními aktivy“

Z hlediska postupů při správě BTC se začínají objevovat první standardy. Existuje např. rámec Cryptocurrency Security Standard (CCSS), což je otevřený standard definující bezpečnostní požadavky pro správu klíčů. Na mezinárodní úrovni se standardizací zabývá i technická komise ISO/TC 307[37], standardy pro self-custody však prozatím nejsou finalizovány.

Instituce se self-custody často vyhýbají…

Obě studie zmiňují, že řada institucionálních investorů se kvůli rozsahu těchto rizik rozhodla prozatím problematice self-custody zcela vyhnout, a to buď prostřednictvím nákupu ETF, či využitím Coinbase Custody bez možnosti nakládat s privátními klíči[38].

Ale: „not your keys, not your coins“!

V této souvislosti jsou však zmiňována i určitá rizika, která s sebou ztráta kontroly nad klíči přináší – regulatorní dohled, zprostředkovanost či závislost na externím subjektu, geopolitická a bezpečnostní rizika. Obecně pak z tohoto vyplývá odpojení od přímého vlastnictví „on-chain“ aktiv („not your keys, not your coins“). Právě z těchto důvodů přešel z BitGo na vlastní cold wallet řešení El Salvador.

8. KOMUNIKACE

8.1 Seznam vystoupení jiných cb k tématu

K bitcoinu se v minulosti vyjádřila celá řada představitelů centrálních bank. Pro přehled uvádíme některé z jejich výroků.

ECB:

- Lagarde (01/2025): "*Reserves have to be liquid, secure, and safe, … Bitcoin does not meet these criteria due to its volatility and potential*

---

36 Zejména v důsledku irevezibility transakcí.Jakmile je bitcoinová transakce potvrzena v blockchainu, nelze ji zrušit, revertovat, reklamovat či stornovat. U konvenčních finančních nástrojů určitá míra reverzibility existuje.

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

38 Ostatně toto je i primární způsob držení bitcoinu i fondem ETF iBit společnosti BlackRock – jednoho z největších světových správců aktiv přitom jistě nelze považovat za technologicky zaostalou společnost, spíše to potvrzuje, za jak komplikovanou záležitost se jedná. Stejný přístup pak používá i společnost Fidelity, nebo třeba vláda USA.

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, aktualizováno 2021)
  Q&A proč ECB nepovažuje bitcoin za opravdovou měnu, ale pouze za spekulativní aktivum – https://www.ecb.europa.eu/ecb-and-you/explainers/tell-me/html/what-is-bitcoin.en.html
- 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 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

V této souvislosti je důležité uvést, že celá řada představitelů centrálních bank se mnohokrát vyjádřila k možnosti zavedení CBDC, regulaci

stablecoinů, apod. Nejde však o oblast, kterou se tento text zabývá, ve výše uvedeném seznamu proto tyto citace vynecháváme.

Pro úplnost uvádíme, že se v září 2025 vyskytly zprávy (https://www.markets.com/news/el-salvador-diversifies-reserves-gold-purchase-imf-bitcoin-948-en-eu/) o tom, že Salvador již dříve během roku nákupy bitcoinu ukončil v reakci na tlak MMF.

8.2 Kontroverze kolem bitcoinu

Existuje celá řada témat, která veřejnost v souvislosti s bitcoinem vnímá kriticky. Pokud se ČNB rozhodne do bitcoinu investovat, některá z nich se mohou vyskytnout i v české veřejné debatě.

Energetická náročnost těžby

Nejčastěji zmiňovanou kontroverzí je vysoká spotřeba elektrické energie vyplývající z principu proof-of-work, na němž je bitcoin založen. Jak bylo uvedeno v kapitole 7.2, v současnosti se roční spotřeba sítě bitcoin odhaduje na 140 až 180 TWh. Pro ilustraci, to odpovídá zhruba dvojnásobku celkové roční produkce elektřiny v Česku. Jedná se tedy o závažný problém.

Ten, jak se zdá, však již dnes není až tak kritickým z následujících důvodů:

- těžba se přesunuje do míst s dostatkem či dokonce přebytky levné elektrické energie (např. do oblastí s celoročním slunečním svitem při současném využití solárních elektráren),
- při rozhodování o nových těžařských projektech je zdroj levné energie důležitým ekonomickým faktorem – využití obnovitelných zdrojů je dnes dominantním zdrojem u nových projektů,
- těžaři již dnes pomáhají při stabilizaci elektrické sítě, tj. využívají velmi nízkých (či dokonce záporných) spotových cen elektřiny a těžbu naopak omezují ve špičkách,
- uvádí se, že těžba bitcoinu má dnes již „čistší“ energetický mix, než v průměru vykazuje globální ekonomika.

Pokud by i přesto existovala (např. ze strany regulátorů, či v případě globálně koordinované snahy států) snaha bitcoin z tohoto důvodu zakázat či omezit, teoreticky stále zbývá možnost nahradit proof-of-work koncept jiným mechanismem. Podobný krok učinilo Ethereum již v roce 2022, a byť se v současnosti nic podobného neplánuje, představuje to jeden z možných záložních plánů.

Nelegální aktivity

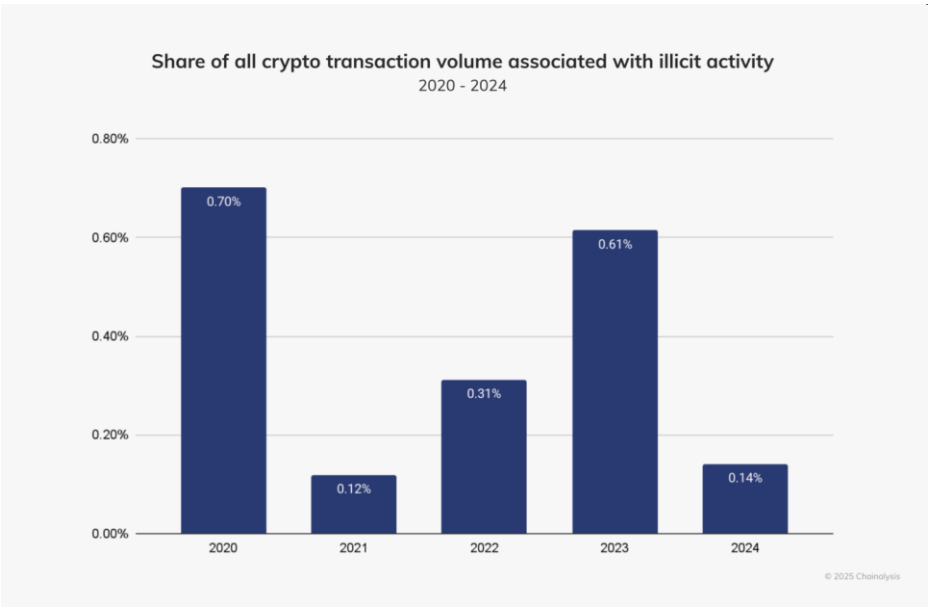
O bitcoinu je často referováno jako o nástroji podsvětí. Bývá zdůrazňováno jeho použití k financování nelegálních aktivit na tzv. dark-webu, při praní špinavých peněz, vydírání atp., přičemž za hlavní motiv k tomuto jednání je považována anonymita bitcoinových transakcí.

V tomto kontextu byla velmi poučná kauza darovaných bitcoinů odsouzeného provozovatele nelegálních tržišť Sheep Marketplace (a pravděpodobně též následně Nucleus Market) Tomáše Jiřikovského. Pro širokou veřejnost bylo překvapením zjištění, že bitcoinové transakce jsou díky veřejné účetní knize dokonale transparentní a vysledovatelné i po mnoha letech neaktivity. Ministerstvu darované bitcoiny se v důsledku ukázaly být jako prakticky neprodejné.

Tato určitá vysledovatelnost transakcí je pravděpodobným vysvětlením, proč podle nezávislých analýz bitcoin není ve výraznější míře k nelegálním

aktivitám využíván. Podle chainalysis.com[39] bylo v roce 2024 pouze 0,14 % transakcí s kryptoaktivy spojováno s nelegálními aktivitami.

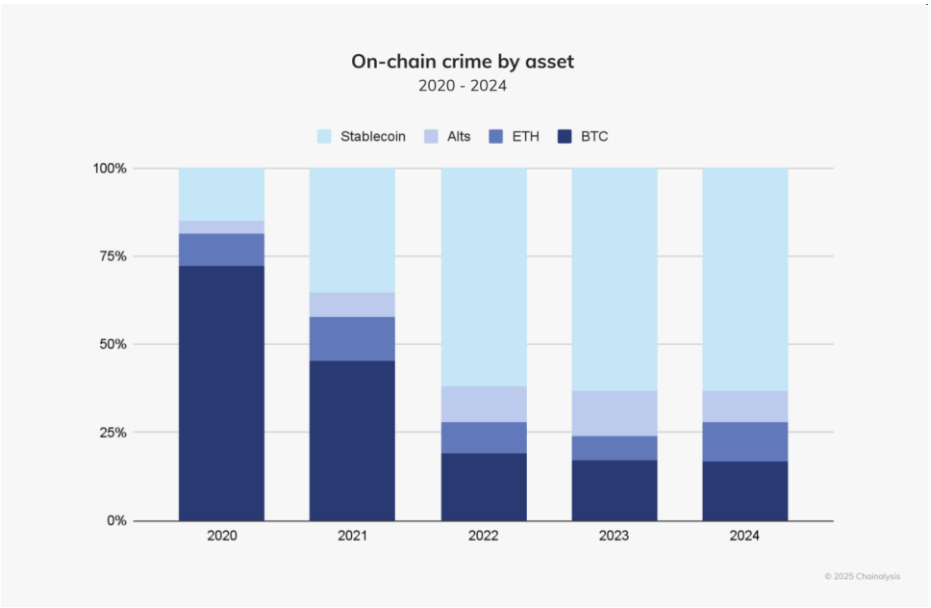
Graf 1-24



Zdroj: chainalysis.com

Tento překvapivě nízký podíl s podsvětím spojených transakcí rozděluje analýza v následujícím grafu na jednotlivé typy digitálních aktiv. Údaje potvrzují hypotézu zmiňovanou v textu výše, že bitcoin není pro tento typ aktivit vhodným prostředkem. Od roku 2020, kdy podíl bitcoinu na nelegálních transakcích činil 63 %, poklesl do roku 2024 na 17 %, přičemž stále větší podíl v tomto segmentu získávají stablecoiny (64 %).

Graf 1-25



Zdroj: chainalysis.com

Podle údajů OSN zároveň zůstávají dominantním prostředkem používaným podsvětím i nadále konvenční měny typu dolaru či eura. Nesnažíme se tím

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

ukázat, že jinde existují větší problémy – spíše chceme upozornit na to, že existence některých nepříznivých jevů nemusí automaticky znamenat, že je nutné za každou cenu omezovat veškeré aktivity s nástrojem, který je při nich využit. Pokusy omezovat z tohoto důvodu používání bitcoinu by tedy měly být vnímány obdobně jako např. snahy omezit transakce s hotovostí.

Čisté vs. špinavé bitcoiny

V praxi se podle původu a historie transakcí rozlišuje určitá čistota, resp. míra „znečištění“ bitcoinů. Za čisté (tzv. *virgin coins*) se považují nově vytěžené bitcoiny. Ty, které již prošly burzami nebo peněženkami, jsou zkoumány, zda nebyly použity pro nelegální činnosti, obchody na darknet tržištích, nepocházejí z vydírání (např. prostřednictvím *ransomware*) či nebyly použity k financování terorismu.

Existují specializované firmy (např. Chainalysis, Elliptic), které vyhodnocují adresy a transakce a přiřazují jim skóre rizikovosti. Míra znečištění bitconů je pak obvykle označována jako tzv. *taint*, a znečištěné bitcoiny jako *tainted bitcoins*. Míra znečištění je dána měrou, do jaké je daná mince propojena s adresami či transakcemi spojenými s nelegální činností. Pokud má mince vysoký taint, znamená to, že přímo pochází z nelegálních aktivit nebo s nimi byla alespoň nějak propojena.

Na běžné uživatelské úrovni toto většinou nehraje roli – nákupem na regulované burze lze získat prakticky čisté bitcoiny. Burzy (ať už v USA, nebo EU) musí striktně dodržovat AML a KYC předpisy, na původ přijímaných bitcoinů tedy velmi dají a k obchodování tainted bitcoiny nepřijmou.

Obdobná je situace také v případě OTC obchodů – zde je za původ zodpovědná prodávající strana, a v důsledku i ta velmi dbá na to, aby nepřijala bitcoiny spojené s kriminalitou, „mixéry“[40] či darknetem. OTC desky obchodníků tedy ve velké míře kopírují standardy burz, často vyžadují striktně čisté bitcoiny (proto také virgin bitcoiny někdy obchodují s malou prémií).

Globálně uznávaný technický standard neexistuje. Ale best practices se ustalují a byť se na různých trzích mírně liší, některé rysy sdílí – KYC zákazníků, AML screening přijímaných bitcoinů, používání blockchain analytických nástrojů, vyhýbání se sankcionovaným adresám atd.

Vztah mezi bitcoinem a „fiat“ měnami

Centrální banky mohou bitcoin považovat za kontroverzní také z důvodu ohrožení jejich emisního monopolu a dalších funkcí.

Toto je zřejmě legitimní obava – masové využívání digitálních aktiv typu bitcoin by zřejmě mohlo ohrozit schopnost centrálních bank provádět měnovou politiku. Dalším aspektem je pak možnost, že vysoká volatilita bitcoinu v případě většího rozšíření ohrozí i finanční stabilitu.

V obou těchto pohledech je však bitcoin nyní velmi daleko od reálné možnosti tato rizika realizovat. Jednak je kvůli současným limitům bitcoinu (zejména co se týká počtu možných on-chain transakcí) nepravděpodobné, že by se začal ve velké míře využívat k provádění běžných transakcí, a že by tak mohl nahradit tradiční měny. Tento důvod dále posiluje již mnohokrát

—

40 Nebo též tumblery – specializované služby, které potenciálně identifikovatelné či tainted bitcoiny mísí s ostatními tak, aby došlo k zakrytí jejich původu či odstranění jejich taintu.

zmiňovaná vysoká cenová volatilita. Bitcoin tak pravděpodobně dále zůstane zejména aktivem pro úschovu hodnoty a pro provádění transakcí se spíše budou využívat samotnými centrálními bankami emitované CBDC či stablecoiny navázané na konvenční měny.

9. STABLECOINY A DEPOSIT TOKENY

Vzhledem k tomu, že analýza investičního potenciálu bitcoinu přirozeně otevírá širší otázku povahy a využití digitálních aktiv, je vhodné doplnit stručný přehled o jiných typech kryptoaktiv, jejichž cílem není spekulativní zhodnocení, ale stabilní uchování hodnoty a efektivní vypořádání transakcí.

Tato kapitola proto přináší shrnutí základních principů a regulatorních aspektů stablecoinů a deposit tokenů, které představují stabilní digitální formy peněz navázané na existující měnové jednotky nebo bankovní vklady.

9.1 Charakteristika a princip fungování

Digitální aktiva se stabilní hodnotou navázanou na měnu či aktivum

Stablecoiny představují typ digitálních aktiv, jejichž cílem je udržovat stabilní hodnotu ve vztahu ke zvolenému referenčnímu aktivu, skupině aktiv nebo koši aktiv. Tímto podkladovým aktivem může být fiat měna, komodita či jiné kryptoaktivum. Stabilita je zajišťována prostřednictvím různých mechanismů, typicky držením rezervních aktiv, zajišťovacích kolaterálů nebo algoritmickým řízením nabídky a poptávky. Přestože název naznačuje stabilitu, v praxi může dojít k dočasným odchylkám od cílové hodnoty v závislosti na konstrukci a důvěře v daný model.

Na rozdíl od kryptoměn s volně tržní hodnotou, jako je bitcoin, nejsou stablecoiny určeny primárně jako spekulativní investiční instrument. Slouží spíše jako digitální reprezentace existujících forem peněz či aktiv a plní funkci prostředku směny, uchovatele hodnoty a účetní jednotky s minimalizovanou volatilitou v prostředí distribuovaných účetních knih.

Mechanismus stability a hlavní modely stablecoinů

Základní stabilizační mechanismus spočívá v tom, že každý emitovaný token je v určitém poměru kryt reálnými aktivy, nebo jeho cenu udržuje algoritmický systém v rámci předem daného modelu. Emitent takových tokenů zpravidla umožňuje tzv. „mint a burn“ proces – tedy vytváření nových tokenů při přijímání vkladů v referenční měně a jejich spalování (převod zpět na fiat) při žádosti o zpětnou konverzi. Rozdíl mezi tržní a cílovou cenou je vyrovnáván pomocí arbitrážních pobídek, které motivují uživatele token nakoupit nebo prodat v okamžiku odchylky od parity.

Podle způsobu zajištění a regulační architektury rozlišujeme tři hlavní modely stablecoinů:

- **Fiat-kolateralizované stablecoiny** jsou nejrozšířenějším modelem. Jejich hodnota je zajištěna rezervami v hotovosti nebo v krátkodobých státních pokladničních poukázkách, které emitent drží v poměru 1:1 vůči vydaným tokenům. Emitent zpravidla umožňuje držitelům zpětnou konverzi tokenů do referenční měny a pravidelně zveřejňuje informace o složení a objemu rezerv.
- **Krypto-kolateralizované stablecoiny** jsou zajištěny jinými kryptoaktivy, nejčastěji etherem (ETH), nativní měnou blockchainu Ethereum. Aby se kompenzovala volatilita podkladových aktiv, bývá zajištění poskytováno s přesahem nad nominální hodnotu vydaných tokenů (tzv. over-collateralization). Tyto modely fungují plně

decentralizovaně, bez centrálního emitenta, prostřednictvím chytrých kontraktů.

- **Algoritmické stablecoiny** představují model, u něhož je stabilita udržována automatickým řízením nabídky tokenů – prostřednictvím jejich nákupů, prodejů či změn oběhového množství na základě předem definovaných pravidel v kódu. Tyto systémy se snaží dosáhnout parity s referenční měnou bez přímého krytí reálnými aktivy. Po kolapsu projektu TerraUSD v roce 2022 však tento přístup ztratil prakticky veškerou důvěru a v institucionální praxi se již neuplatňuje.

Technologicky jsou stablecoiny realizovány jako tokeny na veřejných nebo povolených (blockchainových) sítích. Nejběžnější standardy zahrnují ERC-20 (Ethereum), TRC-20 (Tron) nebo standardy na řetězcích Solana či Base. Tímto způsobem je zajištěna kompatibilita s širokou škálou peněženek a obchodních platforem, což umožňuje rychlou a transparentní distribuci bez zprostředkovatelů.

9.2 Využití stablecoinů v praxi

Rychlé a nepřetržité vypořádání bez hranic

Z uživatelského i institucionálního pohledu jsou hlavní přednosti stablecoinů spojeny s efektivitou, rychlostí a nepřetržitou dostupností. V prostředí, kde bankovní vypořádání probíhá v omezených časových oknech a přeshraniční platby mohou trvat několik dnů, představují stablecoiny alternativu umožňující okamžitý přenos hodnoty v řádu sekund, a to celosvětově a bez ohledu na provozní dobu platebních systémů.

V praxi se stablecoiny používají zejména k vypořádání transakcí na kryptoměnových burzách, kde slouží jako zúčtovací jednotka a základní kotva pro obchodní páry – například BTC/USDT (bitcoin vůči stablecoinu Tether) nebo ETH/USDC (ether vůči stablecoinu USD Coin). Uživatelům poskytují možnost rychle přecházet mezi kryptoaktivy a digitální formou „hotovosti“, aniž by museli provádět klasický fiat převod. Pro mnohé investory ze zemí mimo USA navíc představují přístup k dolarové likviditě v prostředí, kde tradiční bankovní infrastruktura chybí nebo je příliš nákladná.

Stablecoiny jako páteř digitální ekonomiky

Rostoucí část poptávky pochází také z oblasti **decentralizovaných financí (DeFi)** – tedy ekosystému finančních služeb fungujících na technologii distribuované účetní knihy (DLT), zejména na blockchainu, bez tradičních zprostředkovatelů, jako jsou banky či clearingová centra. V těchto systémech stablecoiny plní roli zajišťovacího kolaterálu, zdroje likvidity a nástroje pro vypořádání transakcí v půjčovacích a derivátových protokolech.

Další významnou oblastí je **mezinárodní platební styk**, kde jsou stablecoiny využívány pro přeshraniční převody mezi podniky a finančními institucemi s nižšími náklady a bez zpoždění. Tímto způsobem se z nich stává jakýsi digitální ekvivalent norem SWIFT, ovšem bez jeho strukturálních omezení.

9.3 Regulatorní rámec

Rychlý rozvoj stablecoinů vedl k tomu, že v posledních letech vznikly první ucelené regulatorní rámce v hlavních finančních jurisdikcích. Zatímco ještě v roce 2021 panovala nejistota, zda mají být stablecoiny klasifikovány jako

kryptoaktiva, elektronické peníze či zvláštní druh dluhového instrumentu, dnes se situace zásadně vyjasňuje.

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

Ve **Spojených státech amerických** probíhá diskuse na federální úrovni již od roku 2022 a v roce 2025 dosáhla prvního uceleného návrhu tzv. **U.S. Stablecoin Bill (GENIUS Act)**[41]. Tento zákon vymezuje pojem „payment stablecoin" a ukládá emitentům povinnost držet rezervy v poměru 1:1 v hotovosti nebo vysoce likvidních státních pokladničních poukázkách. Zákon zakazuje částečné kolaterální modely, požaduje registraci emitentů a podřizuje je dohledu federálních orgánů (typicky OCC nebo Federal Reserve). Emitenti musí zveřejňovat měsíční přehledy rezerv a zajistit nezávislé audity. Cílem je zabránit systémovým rizikům a zajistit, aby stablecoiny plnily roli bezpečného platebního prostředku a neohrožovaly stabilitu bankovního sektoru.

V **Evropské unii** je problematika stablecoinů zahrnuta v nařízení **MiCA (Markets in Crypto-Assets Regulation)**[42], které nabylo částečné účinnosti v červnu 2024 a je plně účinné od prosince 2024. MiCA rozlišuje mezi dvěma kategoriemi – asset-referenced tokens (ART) a e-money tokens (EMT) – a stanovuje pro emitenty přísné požadavky na kapitál, řízení likvidity, transparentnost rezerv a ochranu spotřebitelů. Emitent musí získat povolení od národního orgánu dohledu, mít sídlo v EU a zveřejňovat informace o rezervách minimálně měsíčně. MiCA rovněž zakazuje vyplácení úroků z držby stablecoinů a stanoví limity pro objem transakcí v jednotlivých měnách, aby nedocházelo k obcházení měnové politiky.

K dalším jurisdikcím, které zavedly vlastní rámce, patří **Švýcarsko** a **Singapur**. Švýcarský regulátor FINMA posuzuje stablecoiny individuálně v závislosti na jejich struktuře – v praxi je většina modelů klasifikována jako forma elektronických peněz s důrazem na ochranu vkladů. Monetary Authority of Singapore (MAS) v roce 2023 spustila specifický režim pro stablecoiny s požadavky na plné krytí, transparentnost rezerv a licencování emitentů. Tento model se stal často citovaným vzorovým přístupem pro regulaci v Asii.

9.4 Zajištění stability a bezpečnost

Stabilita stojí na rezervách a transparentnosti

Bezpečnost stablecoinů je přímo závislá na kvalitě, transparentnosti a struktuře rezerv, které jejich emitenti drží k zajištění stability hodnoty. Fiat-kolateralizované modely mají rezervy uložené u bank a depozitářů, obvykle ve formě hotovosti a vysoce likvidních nízkorizikových aktiv, jako jsou krátkodobé státní cenné papíry. Emitenti tím minimalizují úvěrové a tržní riziko a zajišťují schopnost okamžitého vypořádání při odkupu tokenů.

Například **USD Coin (USDC)**, emitovaný společností Circle a spravovaný v součinnosti s burzou Coinbase, je plně kryt rezervami drženími u amerických bank a v pokladničních poukázkách. Společnost zveřejňuje měsíční atestace rezerv, které provádí nezávislá auditorská firma Deloitte[43]. Podobně **Tether (USDT)** publikuje kvartální zprávy o složení rezerv, včetně expozic v US Treasuries, bankovních vkladů a reverzních repo operací[44].

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

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

43 Circle: USDC Transparency Reports, viz www.circle.com

44 Tether: Reserves and Assurance Reports, viz www.tether.to

Ačkoli je transparentnost Tetheru dlouhodobě předmětem kritiky, v posledních letech emitent výrazně zlepšil úroveň zveřejňovaných informací a auditních standardů.

Rizika: emitent, likvidita, regulace, technologie

Z pohledu **řízení rizik** se u stablecoinů nejčastěji diskutují čtyři oblasti:

- **riziko emitenta**, které se týká možnosti insolvence nebo podvodného nakládání s rezervami,
- **likviditní riziko** spojené s náhlým masovým odkupem tokenů,
- **regulatorní nejistota** vyplývající ze změn ve výkladu právní povahy stablecoinů,
- **technologická a operační rizika** – například ztráta privátních klíčů nebo chyby v chytrých kontraktech.

Na druhé straně stablecoiny nabízejí výhodu plné trasovatelnosti a okamžité ověřitelnosti pohybu tokenů na blockchainu, což zvyšuje jejich auditovatelnost oproti tradičním off-chain systémům.

9.5 Příklady a formy implementace

Trh ovládají USDT a USDC

Tržní dominanci drží dva projekty – **Tether (USDT)** a **USD Coin (USDC)** – které dohromady představují více než 90 % celkové kapitalizace stablecoinového trhu.

USDT je nejstarším a nejlikvidnějším stablecoinem světa. Jeho silnou stránkou je rozsáhlé přijetí napříč burzami a DLT ekosystémy; slabší je naopak transparentnost rezerv a právní struktura emitenta sídlícího mimo jurisdikci USA. Přesto si Tether udržuje klíčové postavení díky likviditě a dostupnosti na více než desítce blockchainů.

USDC, spravovaný firmou Circle, představuje modelový příklad plně regulovaného stablecoinu se silným dohledem a auditní transparentností. Rezervy jsou drženy výhradně v hotovosti a vysoce likvidních vládních cenných papírech s minimálním úvěrovým rizikem, a emitent má jasně definovaný právní vztah k držitelům tokenů.

Deposit tokeny: tokenizované bankovní vklady

Vedle těchto veřejných stablecoinů se objevují také **deposit tokeny**, které představují digitalizovanou – tzv. tokenizovanou – formu bankovních vkladů. Každý takový token odpovídá konkrétnímu vkladu klienta u banky a je plně krytý závazkem banky vůči jeho držiteli. Na rozdíl od stablecoinů vydávaných nebankovními subjekty jsou deposit tokeny součástí regulovaného bankovního systému a podléhají stejným pravidlům jako klasické depozitní produkty.

JPM Coin: první praktická implementace

Nejznámější implementací tohoto konceptu je **JPM Coin / JPM Deposit Token (JPMD)**[45] vyvinutý bankou J.P. Morgan. Tento systém umožňuje okamžité vypořádání plateb mezi institucionálními klienty banky prostřednictvím interní digitální sítě, která je přístupná pouze schváleným účastníkům, a tedy funguje jako uzavřený systém určený pro regulované finanční instituce.

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

Tokenizovaná depozita: digitální vklady na DLT infrastruktuře

Na tento princip navazuje koncept **tokenizovaných depozit**[46] („tokenized deposits“), který rozvíjí řada velkých bank a technologických partnerů v rámci iniciativ typu **Kinexys Digital Payments Network**. Tokenizovaný depozit představuje digitální reprezentaci bankovního vkladu vydanou bankou na infrastruktuře DLT, kde každý token odpovídá reálnému závazku banky vůči držiteli a je plně krytý na její rozvaze. Tím je zajištěna právní jistota i ochrana vkladů v souladu s platnou bankovní regulací.

Z technického pohledu jsou tyto tokeny vydávány v tzv. permissioned ledger – uzavřeném prostředí přístupném pouze autorizovaným institucím – což umožňuje naprostou trasovatelnost, compliance a okamžité vypořádání transakcí bez rizika protistrany. Síť Kinexys a podobné projekty navrhují architekturu, která umožňuje vzájemnou interoperabilitu mezi bankami, a tím i možnost realizovat mezibankovní převody v reálném čase s výrazně nižšími náklady než v tradičních clearingových systémech.

Využití: reálné platby, vypořádání aktiv, propojení s CBDC

Tokenizovaná depozita nacházejí praktické uplatnění zejména v oblasti vypořádání mezibankovních transakcí, firemních plateb v reálném čase a on-chain settlementu tokenizovaných aktiv. Díky jejich plnému krytí na rozvaze banky se nepovažují za novou formu peněz, ale za technologické rozšíření stávajících depozitních účtů do digitálního prostředí DLT.

Na rozdíl od stablecoinů, které vydávají nebankovní subjekty a jsou volně obchodovány na veřejných trzích, zůstávají tokenizovaná depozita součástí regulovaného bankovního systému. Představují tak praktický nástroj pro efektivnější vypořádání, propojení bankovní likvidity s digitální ekonomikou a potenciální most k budoucím formám digitálních peněz včetně projektů CBDC, tedy digitální měny vydávané přímo centrální bankou.

10. ZÁVĚR

Bitcoin lze dnes považovat za vyspělý a životaschopný projekt, a to navzdory řadě známých problémů, které jej doprovázely v minulosti a doprovázejí dodnes. Za více než patnáct let existence se ukázal jako odolná technologie, jejíž základní principy – decentralizace, otevřený přístup a pevně daná „měnová“ politika – nebyly narušeny ani technickými problémy, ani snahami o regulaci či omezení ze strany států či nadnárodních autorit.

Bitcoin se postupně prosazuje jako uznávané aktivum v širším finančním ekosystému. Jeho role se však mění – od experimentální digitální měny a spekulativního aktiva směrem k etablovanému uchovateli hodnoty a technologickému standardu, o který se opírá řada nových služeb a finančních produktů. Přestože nelze očekávat opakování zcela mimořádných výnosů z prvních let jeho existence, významná část trhu předpokládá jeho postupný přesun do hlavního finančního proudu a širší institucionální přijetí.

46 V českém prostředí se většinou používá překlad „tokenizované depozitum“ jako doslovný ekvivalent anglického deposit token. Z terminologického hlediska však považujeme za vhodnější označení „depozitní token“, které lépe vystihuje charakter tohoto instrumentu jako tokenizované reprezentace bankovního vkladu.

Nabízí se možnost spojit testování s přípravou na externí „co-custody“

Z pohledu centrální banky považujeme za vhodné přistoupit již nyní k testování a detailnímu vyhodnocování technologie. Teoreticky je sice mnoho známo, teprve praxe však často odhalí detaily a obtíže každodenní operativy. Testování by mělo ČNB umožnit lépe porozumět možnostem technologií spojených s bitcoinem a blockchainem, ale také jejich omezením a rizikům. Z hlediska širšího zahrnutí bitcoinu do rezerv bychom za nejvhodnější možnost považovali směřování k modelu co-custody. To by umožnilo infrastrukturu vybudovanou během testovací fáze později použít ke spolu-podepisování transakcí. Jinými slovy, testovací fáze by sloužila též jako příprava na pozdější rutinní provoz. Zároveň by ovšem byly zachovány výhody použití externích custodianů (zejména dodatečná bezpečnost).

Digitální aktiva se stabilní hodnotou navázanou na měnu či vklad

Vedle bitcoinu, který představuje nejznámější formu digitálního aktiva, stojí za pozornost také tzv. stablecoiny a depozit tokeny. Tyto nástroje se snaží eliminovat volatilitu kryptoměn tím, že jsou vázány na hodnotu tradiční měny nebo bankovního vkladu. Zatímco stablecoiny, jako USDC či Tether, jsou vydávány nebankovními subjekty a nesou riziko emitenta, depozit tokeny představují regulovanou digitální formu bankovních vkladů a mohou fungovat jako most mezi tradičním finančním sektorem a tokenizovanými infrastrukturami. Jejich rozvoj je proto relevantní i z pohledu centrální banky.

GLOSÁŘ POJMŮ

Adresy (bitcoinové adresy): Alfanumerický řetězec (např. bc1q... nebo 1A1z...), který slouží jako veřejný identifikátor pro příjem bitcoinů. Je odvozen z veřejného klíče.

BIP (Bitcoin Improvement Proposal): Návrh na vylepšení bitcoinu. Každý BIP definuje změny protokolu, standardy nebo technické specifikace (např. BIP-32 – hierarchické peněženky, BIP-39 – mnemotechnická slova, BIP-322 – podepisování zpráv).

Bitcoinová síť: Decentralizovaná síť peer-to-peer uzlů, které společně ověřují, validují a šíří bitcoinové transakce.

Blockchain: Veřejná, distribuovaná databáze všech bitcoinových transakcí, uspořádaných v blocích navazujících v chronologickém řetězci.

Block (blok): Jednotka, ve které jsou zapsány nové transakce do blockchainu. Nový blok vzniká přibližně každých 10 minut.

Block subsidy (odměna za těžbu): Odměna, kterou získá těžař za nalezení bloku, v současnosti činí 3,125 BTC / blok. Tato odměna je jediným zdrojem emise nových bitcoinů, zhruba každé čtyři roky se při halvingu snižuje na polovinu.

CBDC: Digitální peníze emitované centrální bankou. Ne nutně musí technologicky záviset na technologii blockchainu apod.

Custody / Self-Custody: Způsob uchování kryptoměny. Custody znamená, že klíče drží třetí strana, self-custody znamená, že uživatel drží privátní klíče sám.

Digitální podpis: Kryptografická technika používaná k ověření pravosti a integrity zprávy, softwaru nebo digitálního dokumentu.

Full-node: Počítač připojený k bitcoinové síti, který uchovává kompletní historii blockchainu a samostatně ověřuje všechny transakce a bloky podle konsenzuálních pravidel sítě.

Halving: Událost, která nastává každých 210 000 bloků (cca každé 4 roky) a při které dojde ke snížení odměny za vytěžený blok.

Hardware peněženka: Fyzické zařízení (např. Trezor, Ledger) pro bezpečné uchování privátních klíčů offline.

Hard-fork: nekompatibilní změna protokolu. Starší, neaktualizované uzly bloky v novém formátu odmítnou, takže síť se tímto rozdělí na dvě nezávislé větve, pokud neupgradují všichni. Příklad: Bitcoin Cash.

Hash: Výstup z kryptografické funkce (např. SHA-256), který jednoznačně reprezentuje vstupní data pomocí výrazně menšího objemu dat. Funkce je však jednosměrná, tj. z hashe nelze zrekonstruovat vstupní data.

HSM (Hardware Security Module): Specializované zařízení pro bezpečné generování a uchování klíčů – používá se v institucionálních prostředích.

Lightning Network: Nadstavbová vrstva nad bitcoinem určená pro rychlé a levné mikroplatby. Umožňuje téměř okamžité transakce mimo hlavní blockchain.

Mempool: Dočasný prostor, kde čekají nepotvrzené transakce předtím, než jsou zařazeny do bloku.

MPC (Multi-Party Computation): Metoda správy klíčů, kdy je klíč rozdělen mezi více stran, které spolu interagují bez nutnosti mít klíč kompletně na jednom místě – zvyšuje bezpečnost i flexibilitu.

Multisig: Bezpečnostní metoda vyžadující k transakci více než jeden podpis (např. 2 ze 3 klíčů).

Node (uzel): Počítač, na kterém běží bitcoinový software a který se účastní provozu sítě – zejména ověřuje transakce a bloky. Uzel může být buď full node, jenž uchovává kompletní kopii blockchainu a plně ověřuje všechny transakce,

nebo light node, který pracuje jen s hlavičkami bloků a spoléhá na data od full nodů.

Off-chain: Aktivity nebo transakce, které probíhají mimo hlavní blockchain (tj. nepropisují se do těžených bloků).

On-chain: Transakce nebo data, která jsou zaznamenána přímo v blockchainu.

Privátní klíč: Tajná informace, která umožňuje operovat s bitcoiny. Musí být bezpečně chráněna. Privátní klíč slouží jako jedinečný identifikátor vlastníka peněženky (či obecně uložiště) s bitcoiny.

Permissionless: veřejný a otevřený blockchain, který může každý účastník číst, účastnit se na transakcích a kde přístup není závislý na schválení jakoukoliv entitou. Za takový blockchain je považována verze používaná bitcoinem, Ethereum atd.

Proof-of-Work: Konsensuální algoritmus, kterým těžaři validují bloky výpočetně náročným řešením matematického problému, s nímž je spojena vysoká spotřeba elektrické energie.

Public Key: Veřejná komponenta asymetrické kryptografie, slouží k vytvoření adresy a ověření podpisu.

Satoshi: Nejmenší, dále nedělitelná, jednotka bitcoinu, odpovídá jedné stamiliontině bitcoinu (10^{-8}). Často se zkracuje na sat, např. 5000 sats.

Seed / Recovery phrase: Mnemotechnická fráze (např. 12 nebo 24 slov), která slouží k obnovení celé peněženky. Musí být uchována v dokonalém bezpečí, její ztráta znamená riziko odcizení celého zůstatku peněženky.

Soft-fork: zpětně kompatibilní změna protokolu. Starší, neaktualizované uzly stále přijímají nové bloky jako validní, ale mohou odmítat některé transakce. Příklad: SegWit.

Stablecoin: Typ kryptoměny, jejíž hodnota je pevně navázána na jiné stabilní aktivum – nejčastěji na nějakou měnu (např. americký dolar – USDT apod.).

Taproot: Upgrade bitcoinu zvyšující soukromí, efektivitu a škálovatelnost díky zjednodušené logice skriptů.

Tokenizovaná depozita (Tokenized Deposits / Deposit Tokens): Digitální reprezentace bankovních vkladů vydaná bankou na DLT infrastruktuře. Každý token odpovídá reálnému depozitu na rozvaze banky, je plně kryt jejím závazkem a podléhá bankovní regulaci. Umožňuje rychlé a bezpečné vypořádání plateb v regulovaném prostředí.

Tokenizovaná aktiva (Tokenized Assets): Digitální tokeny, které reprezentují vlastnická či majetková práva k reálným aktivům (např. cenným papírům, fondům, komoditám či nemovitostem). Umožňují jejich obchodování, vypořádání a správu na DLT s vyšší efektivitou a transparentností.

Transakce (bitcoinová): Záznam v blockchainu, který přenáší vlastnictví bitcoinů z jedné adresy na jinou.

UTXO: Nepoužité výstupy předchozích transakcí. Tvoří základní jednotky bitcoinového zůstatku.

Wallet: Software nebo zařízení, které umožňuje správu bitcoinových adres, klíčů a transakcí. Peněženka může být typu:
- Hot wallet: Připojena k internetu (např. mobilní aplikace, webové peněženky), vhodná pro časté používání, ale méně bezpečná.
- Cold wallet: Není připojena k internetu (např. hardware peněženky, papírové peněženky), vhodná pro dlouhodobé uchování.
Každá peněženka generuje/spravuje jednu nebo více bitcoinových adres, které slouží jako cíle pro příjem bitcoinů.

Whitepaper: Původní dokument z roku 2008 od Satoshi Nakamota popisující princip bitcoinu.