Kryptoměny

Roman Hlawiczka

30.11.2021

Kryptoměny

Kryptoměny jsou digitální měny používající kryptografii k zabezpečení transakcí a vytváření nových jednotek měny. Nejznámějšími měnami jsou Bitcoin, Litecoin, Dogecoin, ……..

Platby touto měnou jsou zcela anonymní, pohyb měny je transparentní. První kryptoměnou se stal Bitcoin.

Kryptoměny

- Kryptoměny jsou pohledem českého práva věcí v právním smyslu, která může obdobně jako některé komodity (např. drahé kovy či stavební kámen) plnit za určitých okolností roli prostředku směny. Nejedná se však o zákonné platidlo (legal tender), čímž se liší od bankovek a mincí. Kryptoměny jsou nehmotné věci dle § 496 občanského zákoníku. Jsou věcí nehmotnou, movitou, zastupitelnou, nezuživatelnou a dělitelnou. Můžou se chovat jako druh platidla (směna), výrobek (těžba) či investice (na kryptoburze). Kryptoměna je nosičem nějaké hodnoty. Ta je většinou určena cenou, za kterou se dá kryptoměna prodat – tedy trhem.

Bitcoin

je internetová platební síť, používající komunikaci peer-to-peer (P2P), nevyžaduje tedy spojení se serverem. Stejný název nese i digitální měna (BTC), používaná v této síti. Unikátnost měny je v její decentralizaci, nikdo nemůže měnu ovlivňovat, je nezávislá na vládě, jednotlivcích, dokonce ani zakladatelé měny nemohou její tok násilně změnit. Nikdo nemůže o osudu měny rozhodovat, její hodnota závisí pouze na nabídce a poptávce na trhu.

Bitcoin

Síť funguje od roku 2009. Roku 2008 ji popsal a vytvořil člověk nebo skupina lidí podepsaná jako Satoshi Nakamoto, přičemž ještě 2 měsíce před tím byla zaregistrována doména bitcoin.org.

K autorství se v květnu 2016 přihlásil Australan Craig Steven Wright, což bylo ale rychle zpochybněno. Sahil Gupta označil za pravděpodobného autora bitcoinu Elona Muska, který má hluboké znalosti ekonomie, šifrování a kódování, Elon Musk ale toto tvrzení odmítl.

Zabezpečení finančních operací

K zajištění bezpečnosti sítě je využita kryptografie, umožňující používat pouze peníze, které daný uživatel vlastní, a zabraňující opakovanému využití již utracených peněz.

Všechny transakce jsou ukládány do tzv. „block chain“, který je viditelný všem uživatelům.

Zabezpečení finančních operací

Bitcoin umožňuje pseudonymní držení a převod měny. Bitcoiny mohou být uloženy v osobním počítači ve formě souboru s peněženkou nebo uchovávány pomocí služby třetí strany. Je však možné mít peněženku i zcela offline (na papíře) a lze zcela offline adresu vygenerovat. Peer-to-peer topologie a chybějící centrální autorita zabraňuje komukoliv manipulovat se zásobou této měny. Konečné množství bitcoinů v oběhu je předem dané, a proto není možné vyvolat umělou inflaci vytvořením množství většího.

Celkové množství Bitcoinů

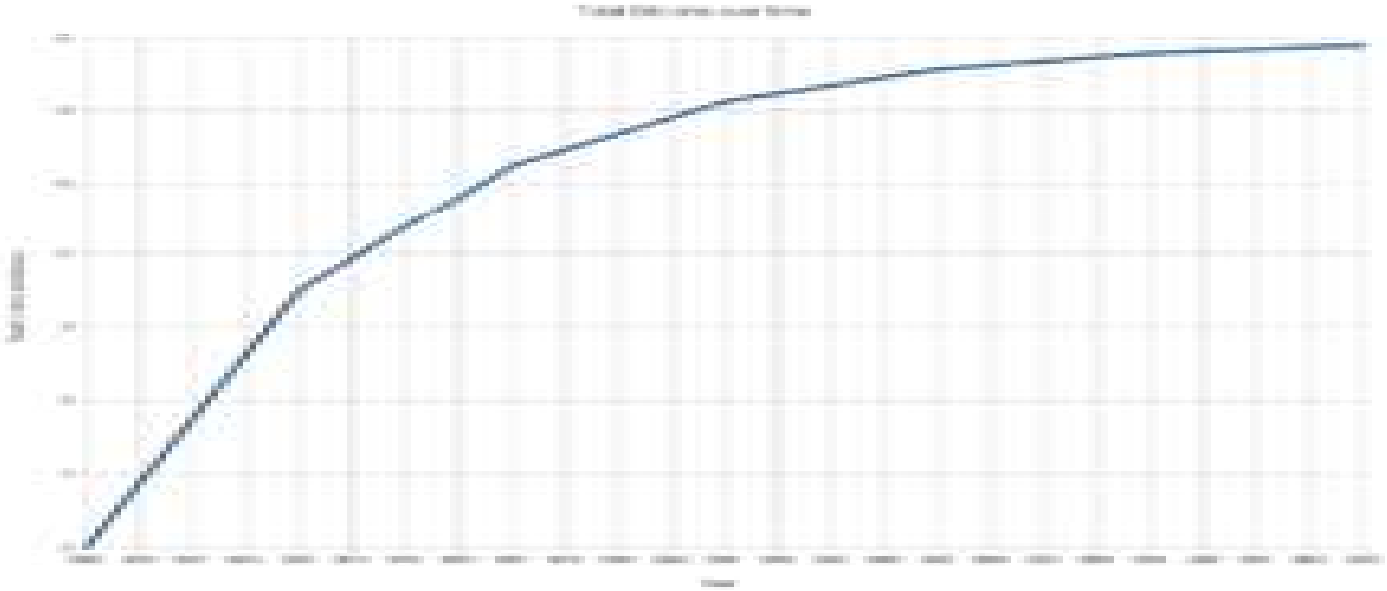
Konečné množství bitcoinů je předem známo a uvolňování bitcoinů do oběhu je definováno ve zdrojovém kódu protokolu.

Celkové množství Bitcoinů, včetně dosud nevytěžených, dosahuje počtu 21 000 000.

Tento počet je konečný, pevně stanovený. Poslední Bitcoin bude dle výpočtů vytěžen v roce 2140 (většina do roku 2030).

Celkové množství Bitcoinů

Pokud tedy bude stále stejný zájem o novou měnu, dojde k deflaci. S tím je v protokolu počítáno, protože lze platit i zlomky bitcoinů. V současnosti má síť dělitelnost na 8 desetinných míst, je možné ji však rozšířit.



Hodnota bitcoinu

Bitcoin je samostatná měna, zcela nezávislá na tradičních měnách jako koruna, euro apod.

Hodnota bitcoinu – podobně jako většiny ostatních měn – vychází z poptávky a nabídky na trhu, a je tedy dána ekonomickou rovnováhou.

Bitcoin není kryt zlatem ani jinými komoditami, ale podobně jako u jiných běžných měn je jeho hodnota závislá na důvěře, že s ním bude možno v budoucnu zaplatit stejně jako dnes. Někteří autoři též poukazují na to, že už skutečnost, že existuje měna, která je nezávislá na rozhodnutí centrálních autorit, je sama o sobě hodnotná.

Rizika

Jako jedno z rizik budoucí hodnoty bitcoinu je uváděn klesající podíl bitcoinu na celkové tržní kapitalizaci alternativních měn.

Od roku 2013 do poloviny roku 2017 klesl podíl tržní kapitalizace bitcoinu oproti ostatním kryptoměnám ze zhruba 95 % na méně než 40 %.

Rizika

Hodnota bitcoinu není určena počtem či výkonem těžařů: při zvýšení hodnoty se zvedne výkon těžařů, ne naopak. Těžaři neurčují hodnotu bitcoinu, ta je dána pouze poměrem mezi nabídkou a poptávkou.

Též bývá chybně uváděno, že je kryta vzácností, nepadělatelností apod. Tyto vlivy nemají přímou vazbu na hodnotu, ale na důvěru, která má vliv na nabídku a poptávku. Na hodnotě se tedy podílejí, ale nepřímo.

Historie hodnoty bitcoinu

Kurz bitcoinu se občas vyznačuje vysokou volatilitou, tedy prudkým kolísáním ceny v krátkém časovém úseku.

Ze střednědobého a dlouhodobého hlediska však vykazuje neustálý nárůst.

Historie hodnoty bitcoinu

Bitcoin začínal jako čistě akademický projekt, kdy ho používali především odborníci a zájemci o technologii samotnou. Technologie však zaujala natolik, že hodnota bitcoinu po dlouhou dobu stoupala. To přivedlo i zájemce, kteří investují čistě ze spekulativních důvodů. Hodnota bitcoinu tak zažila za svoji krátkou existenci prudký růst, vrchol investiční bubliny i částečný pád.

Historie hodnoty bitcoinu

Obchodování s bitcoinem je možné rozdělit do tří období:

V období do června roku 2013 se bitcoinem zabývali téměř výhradně IT specialisté.

V roce 2013 si situace v kryptoměnách ve větším měřítku všimli profesionální investoři, do svých platforem zařadili bitcoin obchodníci s deriváty.

V průběhu roku 2017 se k obchodování s bitcoinem přidala i širší veřejnost.

Historie hodnoty bitcoinu

Vzrůst a pád hodnoty bitcoinu byl dán různými podněty. V období do roku 2013 souvisela cena bitcoinu více s dostupností technologií a vytěženým množstvím kryptoměny.

V období od roku 2013 do roku 2017 byla důležitá vzrůstající akceptace bitcoinu obchodníky, zprávy o regulaci, případně zákazech kryptoměn a podvodech nebo krachu bitcoinových burz. Projevily se také nepopulární kroky tradičních bank (např. zdaňování bankovních vkladů na Kypru).

Historie hodnoty bitcoinu

V roce 2017 má podstatný vliv důvěra v další růst a přísun nových kupujících, bitcoinové platformy také hlásí značný nárůst počtu nově otevřených obchodních účtů v řádu jednotek procent za den.

Historie hodnoty bitcoinu

- Z 24.5.2017 na 25.5.2017 stoupla cena o 500 dolarů .
- V průběhu 2 měsíců do konce listopadu 2017 vzrostla cena bitcoinu o 150 % až na 10 000 USD.
- do konce roku 2017 na téměř 20 000 USD.

Tento stav je přirovnáván k tulipánové horečce. Danou tezi ještě podporuje následný prudký propad kurzu bitcoinu o více než polovinu, k němuž došlo během ledna a února 2018.

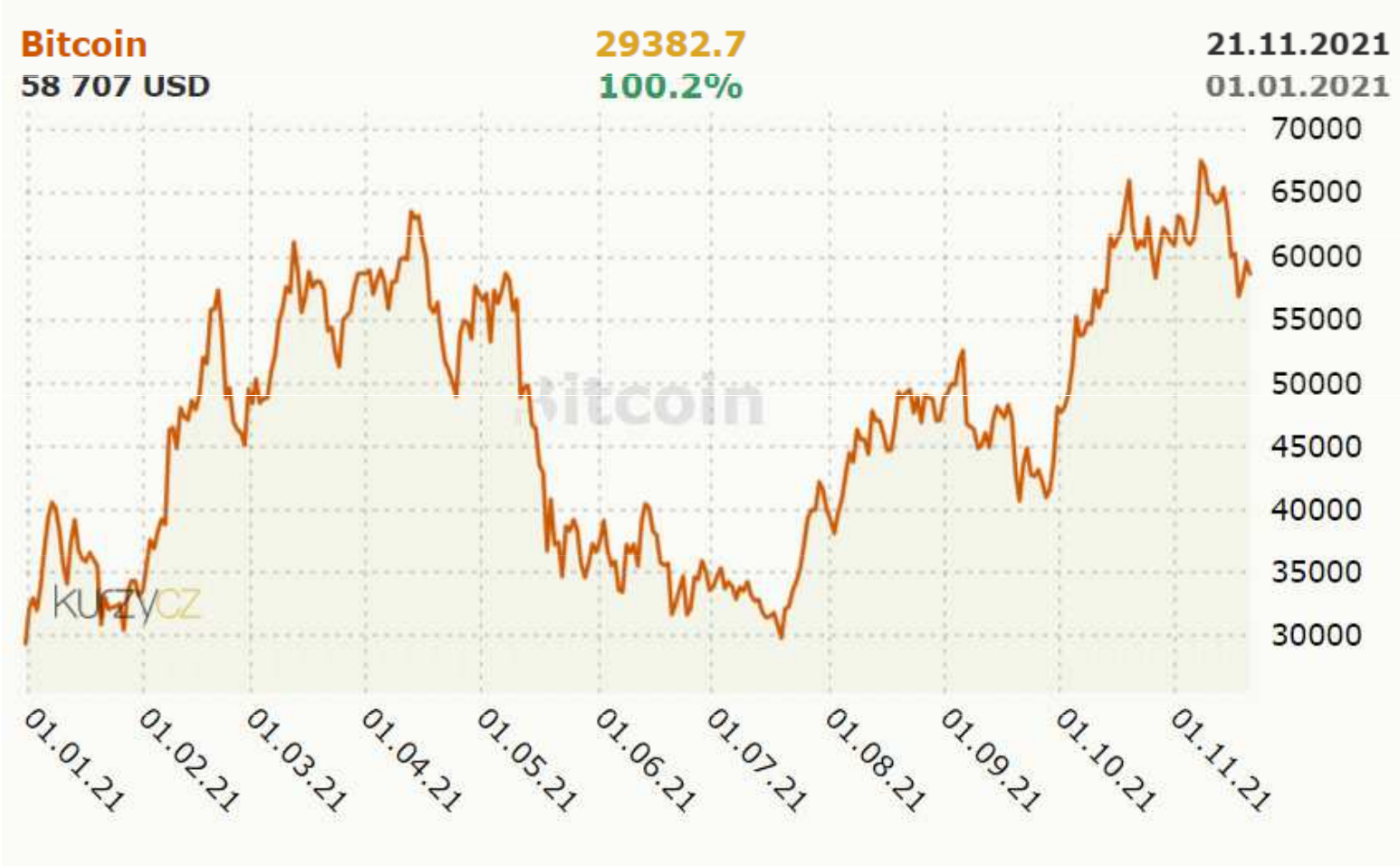
Vývoj ceny BTC

Maxima a minima hodnoty Bitcoin rok 2021

Měsíc	Maximum	Minimum	Měna
01/2021	40 580.5	29 324.6	USD
02/2021	57 408.8	33 523.8	USD
03/2021	61 231.6	48 411.5	USD
04/2021	63 537.9	49 001.6	USD
05/2021	58 774.1	34 586.8	USD
06/2021	40 463.5	31 626.9	USD

Měsíc	Maximum	Minimum	Měna
07/2021	42 202.2	29 791.9	USD
08/2021	49 507.4	38 133.6	USD
09/2021	52 631.2	40 711.5	USD
10/2021	65 993.7	47 698.8	USD
11/2021	67 528.8	60 961.7	USD

Bitcoin - hodnota bitcoinu vývoj 2021 v USD



Zdroj: https://www.kurzy.cz/bitcoin/vyvoj-

Hlavní kryptoměny		13.11.2021 09:26:25
Bitcoin	63927.68 $ ↓	1410270 Kč ↓
Bitcoin Cash	663.1132 $ ↓	14628.54 Kč ↓
Dash	222.4073 $ ↓	4906.395 Kč ↓
EOS	4.891199 $ ↓	107.9018 Kč ↓
Ethereum	4638.465 $ ↑	102326.4 Kč ↑
Litecoin	250.5486 $ ↓	5527.203 Kč ↓
Monero	263.6625 $ ↓	5816.501 Kč ↓
NEO	47.66431 $ ↑	1051.493 Kč ↑
Stellar	0.37504 $ ↓	8.27354 Kč ↓
XRP (Ripple)	1.1941 $ ↑	26.34232 Kč ↑

Historie hodnoty bitcoinu

V průběhu obchodování s bitcoinem se objevily tzv. cenové bubliny, kdy cena bitcoinu prudce rostla na několikanásobek v období týdnů až měsíců, s následnou korekcí.

Jednotlivé cenové fáze u bitcoinu souvisejí s cykly takzvaného půlení (halvingu), tedy snižováním odměny vyplácené těžařům na polovinu. K tomu dochází přibližně jednou za čtyři roky.

Snahy o regulaci

V roce 2013 Německo bitcoin uznalo jako oficiální virtuální měnu, zisky z transakcí se daní standardní sazbou daně z příjmu fyzické osoby. Nedaněné zisky lze realizovat pouze držením bitcoinu déle než 1 kalendářní rok. Zdaněny jsou také transakce mezi bitcoinem a altcoiny, kdy se hodnota transakce převádí na aktuální kurz v euru. Zdaněna je i těžba bitcoinů, kdy těžař je oprávněn odečíst veškeré náklady na těžbu bitcoinu, jako jsou nákup zařízení či spotřeba elektrické energie.

A co říká na kryptoměny německá ekonomika?

Německé hospodářství je u tématu kryptoměn rozpolcené. Asi polovina podniků v nich vidí jen něco pro spekulanty (54 %) nebo příliš složitou problematiku (53 %). Dalších 46 % je dokonce přesvědčeno, že je to oblast pro kriminální podsvětí a k praní špinavých peněz či financování terorismu... Různé mezinárodní koncerny plánují přesto jejich integraci do svých platebních systémů, anebo do nich už ukládají část svých peněžních rezerv. Asi každá třetí společnost v Německu (37 %) počítá s tím, že kurzy kryptoměn budou v následujících letech značně padat. Podobný podíl (39 %) naopak míní, že se kryptoměny hodí jako dlouhodobá investice.

Snahy o regulaci, danění

Investoři mají povinnost danit dosažené zisky podle stávajících regulí.

V prosinci 2013 Čínská lidová banka zakázala finančním institucím používat bitcoin, zatímco jeho používání veřejností povolila.[77]

Snahy o regulaci, danění

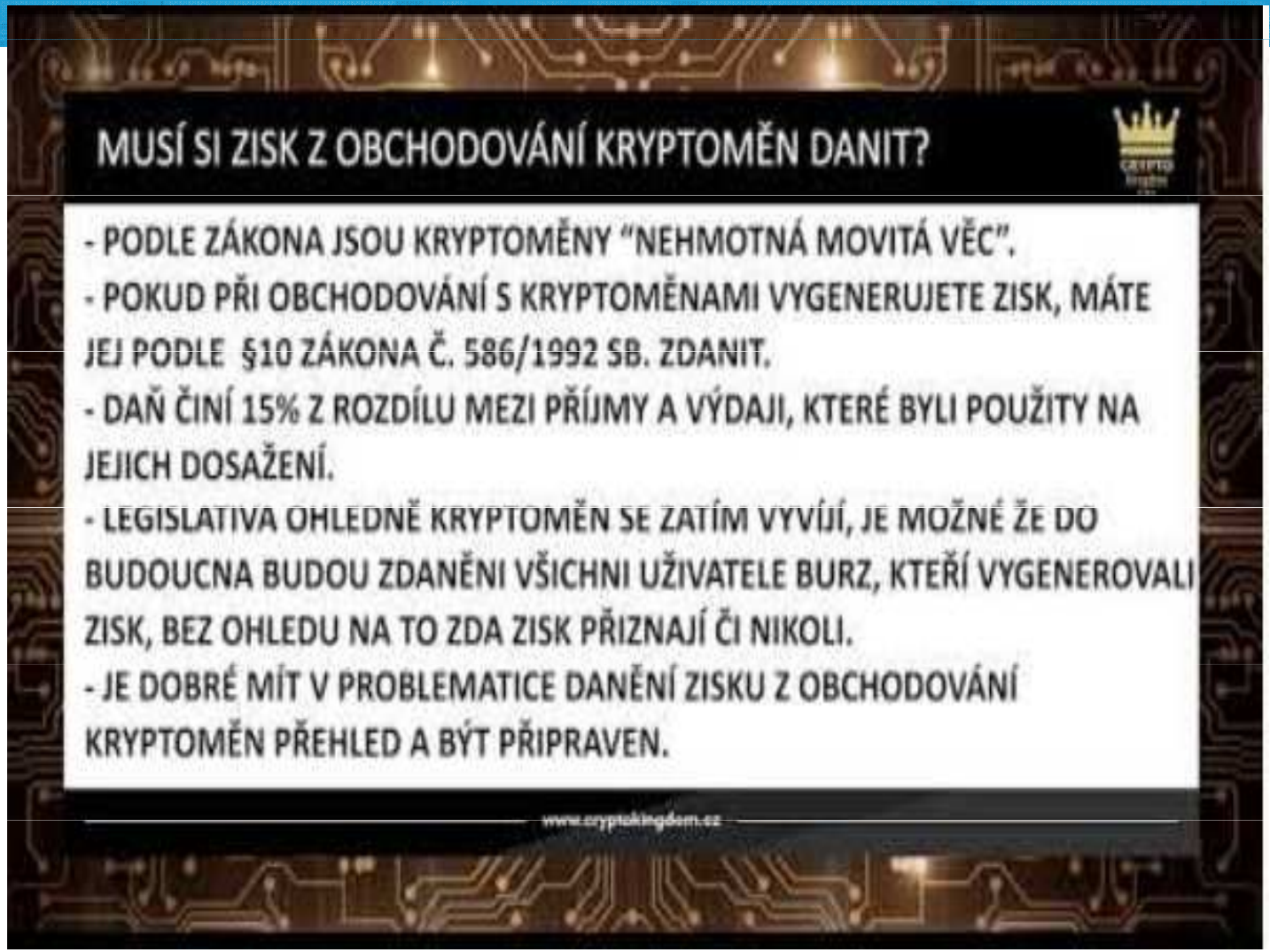
V září 2015 americká Komise pro komoditní obchody (Commodity Futures Trading Commission, CFTC) oficiálně označila bitcoin za komoditu.

To také znamená, že se provozovatelé bitcoinových burz musejí registrovat a provozovat své obchody pod dohledem. Austrálie již dříve prohlásila, že bitcoin je nehmotným aktivem, čímž ho učinila zdanitelným.

Snahy o regulaci, danění

Obavy z přísnějšího postupu států vůči kryptoměnám přispěly začátkem roku 2018 k propadu hodnoty bitcoinu a dalších digitálních měn až o polovinu.

V červenci roku 2018 vstoupila v platnost směrnice ALM (Anti Money Laundering) Evropského parlamentu. Podle ní jsou členské státy EU povinny do 20. ledna 2020 zřídit specializované registry, do kterých se zaregistrují všechny firmy, které nabízí směnu nebo ukládání kryptoměn.


MUSÍ SI ZISK Z OBCHODOVÁNÍ KRYPTOMĚN DANIT?
- PODLE ZÁKONA JSOU KRYPTOMĚNY "NEHMOTNÁ MOVITÁ VĚC".
- POKUD PŘI OBCHODOVÁNÍ S KRYPTOMĚNAMI VYGENERUJETE ZISK, MÁTE JEJ PODLE §10 ZÁKONA Č. 586/1992 SB. ZDANIT.
- DAŇ ČINÍ 15% Z ROZDÍLU MEZI PŘÍJMY A VÝDAJI, KTERÉ BYLI POUŽITY NA JEJICH DOSAŽENÍ.
- LEGISLATIVA OHLEDNĚ KRYPTOMĚN SE ZATÍM VYVÍJÍ, JE MOŽNÉ ŽE DO BUDOUCNA BUDOU ZDANĚNI VŠICHNI UŽIVATELE BURZ, KTEŘÍ VYGENEROVALI ZISK, BEZ OHLEDU NA TO ZDA ZISK PŘIZNAJÍ ČI NIKOLI.
- JE DOBRÉ MÍT V PROBLEMATICE DANĚNÍ ZISKU Z OBCHODOVÁNÍ KRYPTOMĚN PŘEHLED A BÝT PŘIPRAVEN.
www.cryptokingdom.cz

Kryptoměny jsou nehmotný majetek

Z pohledu státních orgánů České republiky jsou kryptoměny považovány za nehmotný movitý majetek. ČNB je totiž jako peněžní prostředky neuznává. Nákup a prodej kryptoměn tak nepovažuje za platební službu. Kryptoměny nejsou podle ČNB virtuálními penězi, cizí měnou a nelze je ani považovat za obdobu cenného papíru.

Z výkladu zákona od daních z příjmů nám vyplývá, že u nás kryptoměny nemají žádné vyjímky jako je tomu například u akcií, cenných papírů, zlata či nemovitostí. Důležité je také zmínit skutečnost, že platby ve virtuálních měnách podléhají povinnosti EET.

Obchodování kryptoměny právnicko u osobou

Než vůbec nakoupit svůj první bitcoin na firmu, tak vaše účetní by měla vytvořit interní směrnici pro oceňování kryptoměn. Zpravidla se dělá přecenění jako průměrný kurz ze třech burz, což v případě altcoinů může být složitější. Na konci účetního období se nakoupené kryptoměny přecenění a zisk nebo ztráta se promítají do výsledku hospodaření právnické osoby. Není potřeba tedy směna na fiat. Pro účetní by samozřejmě bylo nejjednodušší altcoiny prodat na konci roku do bitcoinu a ocenit tak jen samotný bitcoin. Účetní by pak neměla zapomenout i zvolit účetní metodu, pokud vaše firma nakupuje/prodává kryptoměny častěji.

Obchodování kryptoměn fyzickou osobou

Vzhledem k tomu, že dle české legislativy je bitcoin nehmotným movitým majetkem, nelze zařadit příjmy z prodeje kryptoměn do kapitálových příjmů. Veškeré obchody, které na burzách probíhají, spadají tím pádem pod §10 Zákona o daních z příjmů – Ostatní příjmy. Takový příjem podléhá 15% dani. V praxi vezmete nákup kryptoměny a poplatky, které jste zaplatili a máte celkový náklad. Jakmile provedet směnu na fiat, tak od vašeho příjmu odečtete náklady. Zbývající zisk pak zdaníte 15 %. Měli byste si dát pozor na to, že existují situace, kdy váš zisk může být ekvivalentem peněz. V praxi to znamená, že prodám bitcoin za jinou kryptoměnu, nebo si za bitcoin koupím jinou službu. V těchto případech už v daném roce vzniká zisk, který byste měli zdanit.

Potřebujeme pro manipulaci s bitcoinem živnost?

Je důležité zmínit rozdíl mezi obchodováním s kryptoměnami a jeho jejich těžením. Rozdíl totiž není ve výši daně z příjmu, ale v nutnosti zřízení živnostenského oprávnění. Zatímco k obchodování s bitcoinem či jinými kryptoměnami živnostenské oprávnění nepotřebujete, na jejich těžení již ano. Podle zákona se totiž tato činnost řadí již mezi podnikání. Mimo zřízení živnostenského oprávnění vám tak také vyplývá povinnost přihlásit se k sociálnímu a zdravotnímu pojištění. Příjem z tohoto podnikání se zdaňuje dle §7 Zákona o dani z příjmu.

Co přinese budoucnost?

Do budoucna samozřejmě není vyloučeno, že se zákony změní a může se tak stát, že budete potřebovat živnostenské oprávnění jak na těžbu, tak i obchodování kryptoměn. Momentálně se totiž možné obchodovat s kryptoměnami bez živnostenského oprávnění pouze na základě toho, že není tato činnost uvedena v živnostenském zákoně. Dá se říci, že podle živnostenského zákona se obchodování s kryptoměnami považuje za nákup a prodej akcií, čili správu vlastního majetku.

Kontroverze

- zabudovaná deflace měny: kvůli omezenému množství peněz bude docházet k trvalé deflaci, avšak mnoho ekonomů zastává přínos spíše inflace.

- krytí měny: hodnota měny je pouze spekulativní, samotná měna není ničím kryta. Častým protinázorem je poukázání na fakt, že současné fiat měny taktéž nejsou ničím kryté.

Kontroverze

- zneužitelnost pro trestnou činnost: měna je kvůli náročné vystopovatelnosti a nemožnosti kontroly vhodná k trestné činnosti. Ke stejnému účelu však lze zneužít i běžnou hotovost, neboť ta je také relativně anonymní. Ale také velké množství komodit.
- český směnárenský server Bitcash.cz byl hacknut, majitelům zmizely bitcoiny za několik milionů korun. Nicméně je třeba si uvědomit, že bezpečnost jakékoliv směnárny nemá nic společného s bezpečnostní samotného Bitcoinu.

Základní způsob fungování

Veškerá komunikace v síti probíhá pomocí počítačového programu (nebo jiného klienta, např. na mobilu), který komunikuje s dalšími uzly (účastníky). Účastníci jsou dvojího druhu: koncoví uživatelé a těžaři. Každý účastník může být koncový uživatel, těžař, anebo obojí.

Koncoví uživatelé

jsou lidé, kteří si posílají peníze. Každý uživatel má jednu nebo více peněženek, které slouží jako adresy pro platby. Současně si také udržují distribuovanou databázi všech proběhlých transakcí v síti – tzv. blockchain. Tak každý uzel ví, která mince/část v síti patří které peněžence. Každé peněžence náleží soukromý a veřejný klíč.

Koncoví uživatelé

Pokud chce uživatel poslat peníze, vezme patřičný obnos svých mincí + případný poplatek (viz dále) a vytvoří transakci, kterou podepíše soukromým klíčem. Tuto informaci rozešle všem uzlům (uživatelům), ke kterým je připojen, ti to rozešlou dalším apod. do celé sítě. K příjemci tak informace o platbě probublá téměř ihned (v řádu sekund), transakce však ještě není tzv. potvrzena.

Co je to těžba kryptoměn

Bitcoin, Litecoin, Dogecoin i další kryptoměny vznikají tzv. těžbou (mining). Jde o výpočet matematické úlohy, za jejíž úspěšné řešení obdrží těžař (miner) kryptoměny určité množství mincí dané kryptoměny. Při těžbě kryptoměn zároveň dochází ke kontrole a potvrzování platebních transakcí (převodu kryptoměny z účtu na účet), které v síti dané kryptoměny probíhají.

Těžař (resp. jeho těžební software) si vybere určitý počet dosud nepotvrzených platebních transakcí do tzv. bloku. Základním kritériem pro zahrnutí nebo nezahrnutí transakce do bloku je poplatek, který uživatelé při zadání transakce nabídli. Transakce s poplatkem vyberou mineři k potvrzení dříve.

Vyřešení matematické úlohy obvykle spočívá v nalezení určité hodnoty v závislosti na hešovacích funkcích, na seskupených platebních transakcích a na aktuálním tzv. limitu. Vzhledem k použití hešovací funkce je možnost nalezení správného řešení náhodná, je tedy závislá na výkonu hardware hledajících řešení, nikoliv na matematických schopnostech těžaře. Limit je aktualizován tak, aby se v celé síti podařilo najít řešení právě řešených bloků průměrně jednou za určitý časový interval (např. 1x za 20 minut), takže šance na nalezení řešení je nepřímo úměrná momentální výkonnosti sítě.

Pozn. Velmi zjednodušeně se dá říci, že hešovací funkce je funkce, která z libovolných vstupních dat vytvoří malé číslo (tzv. zahešuje původní data na tzv. heš). K vlastnostem funkce patří, že z výsledného heše je obtížné nalézt původní vstupní data. A těžaři kryptoměn mají za úkol nalézt právě taková vstupní data, která když se zahešují, bude výsledný heš nižší než aktuální limit. Těžební program tedy upraví vstupní data, zahešuje a porovná s limitem. Pokud je výsledek hešování větší než limit, cyklus opakují. Použít hešovací funkci je jednoduchá a rychlá operace, ale protože není možno odhadnout, jak je nutno vstupní data pro správný výsledek upravit, může být cyklus opakován jednou nebo bilionkrát, než těžař kryptoměn dojde ke vstupním datům, která požadovanou podmínku splňují. Čím má těžařův stroj větší výkon, tím více zahešování a úprav dokáže za časovou jednotku provést a tím má větší šanci na rychlé nalezení řešení.

Způsob těžby

V začátcích se těžilo přes počítačové procesory, později přes grafické karty, ale dnes se u velké části kryptoměn využívají výkonné ASIC čipy (speciální extrémně rychlý hardware, který je pro řešení kryptografických úloh přímo vytvořen a který je zároveň optimalizován pro spotřebu energie). Návratnost individuální těžby resp. sdružování individuálních těžařů do poolů se odvíjí od jednotlivé kryptoměny. Například pro Bitcoin již tento způsob nelze doporučit, protože konkurence je obrovská, u méně populárních měn ještě prostor pro takovou těžbu pravděpodobně je. Nicméně obecně je v současnosti těžba kryptoměn náročná a nákladná investice s nejistou návratností.

Role těžby v blockchainu Bitcoinu

Když se řekne slovo blockchain, spousta lidí se zasekne a zjistí, že vlastně vůbec neví, o co se jedná. Přitom to není zas tak složité. Chce to jen investovat nějaký čas do studia.

Blockchain je v doslovném překladu **řetěz** z **bloků**. Bloky v tomto případě nejsou nic jiného, než účetní knihy. V Bitcoinu má jedna taková kniha průměrnou životnost 10 minut a má omezené místo. Její obsah tvoří v naprosté většině pohyby mezi adresami (transakce), avšak jsou zde i dvě věci navíc. **Nonce a hash předchozího bloku.** Jedná se o dva velmi důležité pojmy, které se v tomto článku objeví ještě mockrát, proto je důležité, abyste následující definici pochopili.

- Prozatím si vystačíme s vysvětlením, že **nonce** je určité číslo, které se přidává na konec každého bloku.
  Příkladem nonce může být číslo: *147 483 646*.
- **Hash** už je lehce složitější. Pokud vezmeme nějaký soubor dat, pomocí speciální funkce jej můžeme přeložit na jedno číslo. Asi jako když si vezmeme nějaký text a přeložíme ho do morseovky. Rozdíl je, že hash v případě Bitcoinu nelze převést zpět do dat, ze kterých byl vytvořen, zatímco morseovka ano. A navíc pokud v tomto souboru dat změníme byť jen jediný údaj, celý hash bude mít úplně jinou podobu.
  Příkladem hashe může být:
  000000000000000000007643ed71fcf50b3a2d27ca978f653771b854b8e947e08.

Z toho plyne následující: **každý blok má svůj specifický hash**.

Teď už ale k tématu. Těžaři bitcoinů mají ve své podstatě naprosto primitivní práci. Jejich úkolem je najít konkrétní nonce (číselný kód), který přidají k transakcím v aktuálně otevřeném bloku, a z toho celého vytvořit hash, který má předem určené parametry – počet nul na začátku.

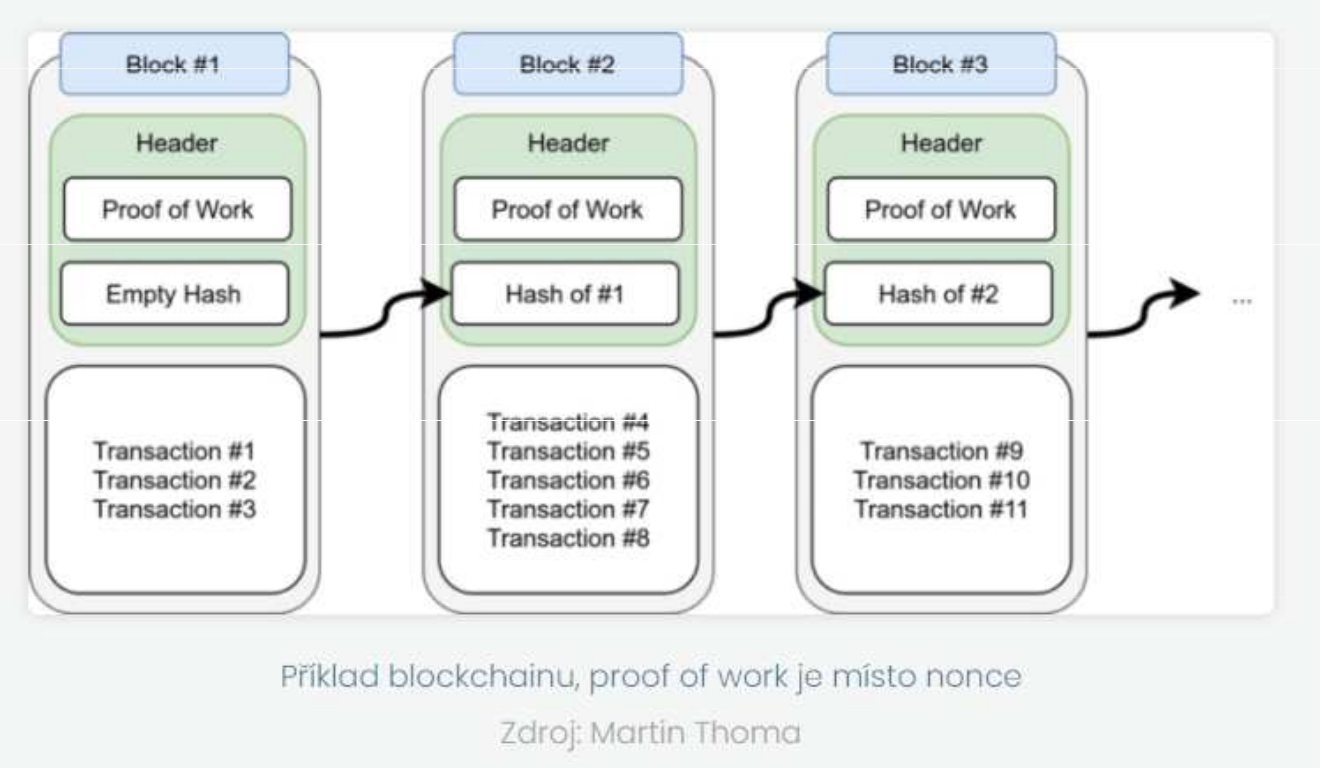
A protože se hash nedá zpětně „přečíst" a rozluštit, nikdo vlastně neví, jaká kombinace dat je potřebná k tomu, aby daný hash, který všichni těžaři hledají, vznikl. **Těžař tak musí vzít náhodný nonce, vypočítat hash a doufat, že je to správný hash**. Když se mu to nepovede, vše dělá znovu a znovu. Je to hra o štěstí.

Posuneme se zase o kousek dál.

Povedlo se nám najít (uhádnout) správný nonce a získali jsme tak správný hash celého bloku. Super, vytěžili jsme tento blok! Závod o tento blok skončil a my jsme jeho vítězem. **Jako odměnu získáme několik nově vytvořených bitcoinů**, které předtím nikdo nevlastnil. My jsme je vytěžili.

Začal ale nový závod – o blok následující. Námi vytěžený blok přidáme do následujícího bloku na začátek a znovu hledáme nonce.

> Fakticky jsme tak vzali všechny transakce z minulosti a napojili jsme je na novou účetní knihu. Proces se opakuje. Musíme vzít hash minulého bloku, transakce za posledních 10 minut a najít nonce. Ty dohromady převedeme na správný hash.

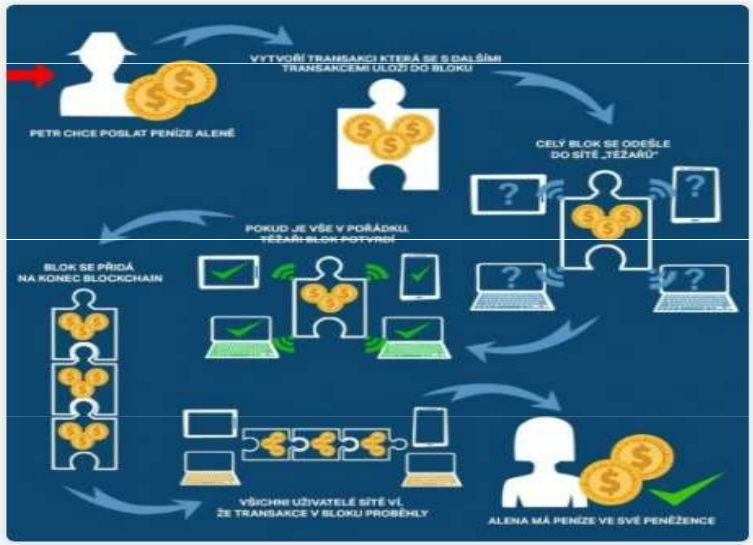


Příklad blockchainu, proof of work je místo nonce

Zdroj: Martin Thoma

Díky tomu má v sobě každý nový blok vlastně celou předešlou historii transakcí, která je určitým způsobem potvrzená a neměnná.

Postupně se nám tak tvoří řetěz účetních knih/bloků. Proto jméno blockchain. Nejedná se o nic jiného, než o sérii na sebe navazujících dat, jejichž platnost někdo ověřil.



Průběh transakcí u Bitcoinu

Náročnost těžby

Když Bitcoin vznikl, bylo možné ho těžit i na běžných počítačích. První těžaři jednoduše zkoušeli různé hodnoty nonce a s nimi se snažili uzavírat bloky. Někdy se to někomu povedlo, takový těžař poté získal za uzavření bloku odměnu, a jelo se dál.

> S postupným růstem sítě však rostla i cena bitcoinu a díky silám trhu začínalo těžit stále více lidí. Bitcoiny získané těžbou totiž mohli jejich těžaři prodat, za utržené peníze zaplatit elektřinu, kterou svůj těžební počítač poháněli, a něco jim zbylo navíc. Toho si všimli další lidé, kteří se těchto pomyslných závodů v těžbě účastnili, a snažili se o totéž.

Více těžařů logicky znamenalo, že patřičnou nonce našli v průměru rychleji. Uzavírání bloků a tvorba nových bitcoinů se tak zrychlovala.

Jenže tvůrce Bitcoinu, Satoshi Nakamoto, s tímto počítal. Zdrojový kód Bitcoinu má v sobě proto zabudovaný autoregulační mechanismus: pokud se sníží průměrný čas na vytěžení bloku, **mírně se zvedne obtížnost těžby**. Toho je dosaženo tak, že výsledný hash má o něco specifičtější parametry, které musí splňovat. Právě proto trvá déle, než ho těžaři najdou. Ale protože je těžařů více, v průměru se tak stane zase každých 10 minut.

Dnes už je situace naprosto odlišná. K tomu, abyste mohli bitcoiny těžit, budete potřebovat speciální hardware, který se nazývá **ASIC miner**.

ASIC miner L3

Je to kus železa s jedinou funkcí (hádání nonce), kterou však dělá perfektně, rychle a v poměru nejlevněji. Těžit bitcoin není ale žádný med ani s nově koupeným ASICem. Díky technologickému vývoji jsou zařízení do pár měsíců zastaralá.

Vzhledem k ohromné konkurenci a obtížnosti už je v podstatě nemožné, abychom bitcoin těžili výhodně např. na grafických kartách, které se k tomu dříve také používaly. Mining pomocí ASICů sežere ohromné množství elektřiny a pokud ji nemáme za hubičku, je nesmysl se o těžbu snažit. Jednoduše za elektřinu zaplatíte mnohem více, než za kolik vytěžené bitcoiny prodáte.

Jeden zajímavý fakt: Univerzita Cambridge došla v roce 2021 k závěru, že celá Bitcoinová síť spotřebuje více elektřiny než celá Argentina. Odkaz na článek je přiložený zde.

Odkaz na článek je přiložený zde.

Hlavní otázka – vyplatí se těžba bitcoinu?

V naprosté většině případů je odpověď jasná: ne. Naším nepřítelem je zde elektřina. Její cena je největším nákladem, který musíte neustále udržovat. Už jen po jejím započtení budete pravděpodobně v mínusu. A to stále mluvíme o tom, že chcete těžit s ASICem. O grafických kartách se nemá vůbec cenu bavit (u Bitcoinu), protože jsou pomalejší a na spotřebu hladovější. Pokud si to i tak chcete vyzkoušet, na internetu existují jednoduché kalkulačky. Pro bitcoin například tato.

Není ale nutné hned couvat. Pokud vás celý nápad nadchl, jsou tu i jiné možnosti než jen Bitcoin. Velká část kryptoměn se na grafických kartách stále těžit dá, u některých je to dokonce jediná cesta (nemožnost využít ASIC). Pro spočítání výnosů v altcoinech nejlépe funguje stránka whattomine.io.

Zajímavou možností může být i ohřev díky ASICům. Když jsou zapnuté, vytváří vysoké množství odpadního tepla, kterým se dá například vytápět místnost. Vytěžené kryptoměny vám následně pokryjí část nákladů. Nevýhodou je však velká hlučnost.

Těžaři

Těžaři potvrzují transakce v síti. Těžař seskupí transakce čekající na potvrzení, přidá k nim odkaz na předchozí potvrzený blok transakcí a údaj zvaný kryptografická nonce. Snaží se najít takovou nonci, aby se hash SHA-2 nového bloku vešel pod sítí stanovený limit. Limit je nastaven tak, aby se to v celé síti dařilo průměrně jednou za 10 minut, takže nalezení vhodné nonce je obtížné a to tím více, čím výkonnější celá síť je.

Těžaři

Těžař, kterému se nalezení nonce a tím i vytvoření a potvrzení nového bloku transakcí podaří, si ponechá veškeré poplatky ze zahrnutých transakcí a odměnu za potvrzení bloku. Odměna za potvrzení bloku je momentálně jediný a předem stanovený způsob emise nových bitcoinů. Odměna se však každých 210 000 bloků (tj. každé 4 roky) snižuje na polovinu a růst množství peněz zpomaluje.

Těžaři

Těžař si může vybrat, které transakce do nového bloku zahrne a které ne (podle výše poplatku).

Protože je síť anonymní, těžaři nevědí nic o odesílatelích ani příjemcích a jediným smysluplným kritériem pro zahrnutí nebo nezahrnutí transakce do bloku je právě zvolený poplatek. O tom, který těžař první nalezne vhodnou nonci (a rozhoduje o zařazení transakcí) rozhoduje náhoda.

Těžaři

Transakční poplatky a odměna za potvrzení bloku jsou ekonomickou motivací činnosti těžařů. Snižováním odměny dojde ke stále většímu vyžadování transakčních poplatků.

Možnost padělání

Těžaři řeší umělý problém nalezení kryptografické nonce proto, aby potvrzení nového bloku bylo velice složité, a tedy i velice obtížně padělatelné, přitom ale snadno ověřitelné. Pokud by chtěl útočník změnit platební historii, musel by mít k dispozici výpočetní výkon větší, než je výpočetní výkon celého zbytku sítě. Tomuto teoretickému útoku se také říká 51% útok. Bitcoin počítá s tím, že takové množství výkonu žádná jedna entita nemá.

Možnost padělání

I kdyby se to ale někomu povedlo, mohl by měnit pouze své vlastní transakce a zamezit potvrzování ostatních transakcí (tedy nemohl by například převádět cizí peníze k sobě ani stávající databázi nějak ničit).

51% útok je nepravděpodobný, např. v květnu 2013 byla síť těžařů více než 60× výkonnější než nejrychlejší superpočítač světa.

Možnost padělání

Získat nadpoloviční většinu výpočetního výkonu v celé síti by navíc bylo pro útočníky velmi nákladné. I kdyby byli ochotni investovat a opravdu síť tímto způsobem napadnout, klesla by důvěra v samotný bitcoin a s ním i jeho cena. Díky naprosté transparentnosti by totiž všichni uživatelé sítě snadno zjistili, že nejdelší větev na blockchainu, která je považována za platnou, je prodlužována pouze jedním uzlem.

Možnost padělání

Pokud by 51% útok někdy proběhl, jednalo by se spíše o podkopání důvěry v samotnou Bitcoinovou síť, než snaha o reálné odcizení prostředků.

Princip těžby

- Úkolem těžaře je vyřešit matematický problém. Zjednodušeně řečeno, snaží se najít ve zvoleném blockchainu číslo hashe nižší, než je číslo aktuálně zvolené sítí.
- Je-li matematický problém úspěšně vyřešen, síť potvrdí nalezení bloku. K nalezení jednoho bloku dochází průměrně každých 10 minut.
- Pravděpodobnost nalezení bloku je vzhledem k počtu těžařů po celém světě velmi nízká. Ke zvýšení šance na úspěch se někteří těžaři začali seskupovat do tzv. mining pool.

Princip těžby

Jedná se o uskupení, které svým společným výpočetním výkonem zvyšuje šanci k nalezení bloku. Odměna se pak rozdělí mezi všechny těžaře, podle poskytnutého výkonu.

Každý nový blok odkazuje na předchozí blok, a tím potvrzuje i všechny předešlé transakce. Tudíž každá transakce je potvrzena tolikrát, kolik bloků bylo vytvořeno od prvního zahrnutí (včetně toho prvního bloku). Čím více potvrzení, tím obtížnější je padělatelnost celého procesu, a tím tedy více může příjemce věřit, že mu peníze skutečně přišly.

Princip těžby

Obtížnost nalezení bloku (limit hashe) je každých 14 dní upravována podle aktuální výpočetní síly všech těžařů tak, aby byl nový blok uvolněn průměrně každých 10 minut. Měna je tedy do sítě uvolňována přibližně stejnou rychlostí, nehledě na počet těžařů či celkový výkon v síti.

Náklady na těžbu

Součástí nákladů na fungování bitcoinu je spotřeba elektrické energie na těžení nových bitcoinů.

Na začátku listopadu 2017 podle odhadů bitcoin spotřeboval 25,76 TWh elektřiny za rok. Kdyby byl bitcoin zemí, podle v té době aktuálního žebříčku spotřeby energie by umístil na 68. místě, těsně za Ománem. Energie spotřebovaná na těžbu bitcoinu by tak pokryla asi 36 % elektrické energie spotřebované v roce 2016 v Česku.

Náklady na těžbu

Začátkem roku 2018 vyžadovalo ověření jedné transakce bitcoinem stejné množství energie jako 465 tisíc plateb kartou VISA.[35]

Zastánci bitcoinu ale argumentují, že energetická náročnost má smysl sama o sobě, neboť brání snahám manipulovat s údaji v blockchainu. Ve srovnání s energetickou náročností současného finančního sektoru, kam by se počítaly i náklady na provoz centrál bank či tisk a rozvoz bankovek, údajně stále nejde o tak vysoká čísla.

Náklady na těžbu

Kvůli vysoké spotřebě pro jejich těžení jsou podle amerického ekonoma Nouriela Roubiniho nejen bitcoin i další digitální měny přírodní pohromou.

Je nutno ovšem dodat, že podle analýzy z roku 2019 pochází 74% výpočetního výkonu vynaloženého na těžbu Bitcoinu z obnovitelných zdrojů.

Náklady na těžbu

Okolo 60-70% vytěžených Bitcoinů pochází z Číny, která sice získává více než dvě třetiny energie z uhelných elektráren, nicméně těžení Bitcoinu se v Číně odehrává především v oblastech bohatých na větrnou a vodní energii. 80% těžby se koncentruje v provincii Sichuan bohatou na hydroelektrárny. Těžení v těchto oblastech absorbuje nadprodukci hydroenergie, která by jinak přišla na zmar. Těžbě Bitcoinu v ostatních zemích také dominují obnovitelné zdroje. Island (100%), Québec (99.8%), Britská Kolumbie (98.4%), Norsko (98%).

Peněženky

K aktivní účasti ve světě Bitcoinů potřebuje mít každý uživatel minimálně jednu peněženku, často však více. Slouží jako místo k uchování, odesílání nebo přijímání měny. Za vlastníka je považován ten, kdo zná soukromý klíč k peněžence. Ztráta klíče znamená ztrátu veškeré obsažené měny. Každá peněženka má adresu v podobě 34místného kódu složeného z písmen a číslic. Slouží jako identifikátor pro příchozí transakce. Jedna peněženka může mít více adres.

Jak je na tom trh s kryptoměnami? Tenhle graf stojí za to sledovat

- *Když je na maximu cena bitcoinu, běžní příznivci kryptoměn mají jasno, že je trh na vzestupu. Když se ale připojí další čtyři "těžké" váhy kryptosvěta, jimiž jsou ether, XRP, Binance Coin a Cardano, a jejich index posune historický rekord, je zřejmé i skeptikům, že trhu opravdu dominují býci. Není totiž řeč o žádných drobných shitcoinech , ale o mega caps kryptoměnového trhu.*

Graf samozřejmě neříká nic jiného, než že ceny rostou, například postupné schvalování prvních ETF zaměřených na bitcoin ale slibuje, že se na stále více etablovaný trh začnou proudit peníze některých kategorií institucionálních investorů. Takže jsou-li kryptoměny spekulativní bublina, případně pyramidová hra, minimálně by nemělo hned tak dojít k jejich kolapsu.

Otázka: Klienti slyšeli o velkých výnosech Bitcoinu a jiných kryptoměn a o možnosti investovat do derivátů, jejichž podkladovým aktivem jsou právě kryptoměny. Na tuto investici jim však nezbývá dostatek volných finančních prostředků. Jak se může investiční poradce zachovat?

Odpovědi (Jedná správná odpověď)

A	Investiční poradce může klientům zprostředkovat investici do futures na kryptoměny i bez volných prostředků, protože klienti mají rezervu na spořícím účtu, kterou v případě poklesu takového derivátu mohou použít.
B	Investiční poradce nemůže klientům zprostředkovat investici do derivátu na kryptoměny, protože klientům na tuto investici nezbývá dostatek prostředků a jedná se o velice specifickou a spekulativní investici, která pro klienty není vhodným produktem.
C	Investiční poradce nemůže investici do derivátu na kryptoměny klientům zprostředkovat, protože deriváty na kryptoměny neexistují, protože podkladovým aktivem derivátu musejí být investiční nástroje.
D	Investiční poradce může klientům zprostředkovat investici do futures na kryptoměny i bez volných prostředků, protože tento derivát ze své podstaty umožňuje uhradit cenu za podkladové aktivum až v budoucnu.

Otázka: Klienti slyšeli o velkých výnosech Bitcoinu a jiných kryptoměn a o možnosti investovat do derivátů, jejichž podkladovým aktivem jsou právě kryptoměny. Na tuto investici jim však nezbývá dostatek volných finančních prostředků. Jak se může investiční poradce zachovat?

Odpovědi (Jedná správná odpověď)

A	Investiční poradce může klientům zprostředkovat investici do futures na kryptoměny i bez volných prostředků, protože klienti mají rezervu na spořícím účtu, kterou v případě poklesu takového derivátu mohou použít.
B	Investiční poradce nemůže klientům zprostředkovat investici do derivátu na kryptoměny, protože klientům na tuto investici nezbývá dostatek prostředků a jedná se o velice specifickou a spekulativní investici, která pro klienty není vhodným produktem.
C	Investiční poradce nemůže investici do derivátu na kryptoměny klientům zprostředkovat, protože deriváty na kryptoměny neexistují, protože podkladovým aktivem derivátu musejí být investiční nástroje.
D	Investiční poradce může klientům zprostředkovat investici do futures na kryptoměny i bez volných prostředků, protože tento derivát ze své podstaty umožňuje uhradit cenu za podkladové aktivum až v budoucnu.

Poradce je jednoznačně povinen upozornit klienty na to, že se jedná o vysoce rizikovou spekulaci, která nemá s investicí nic společného, že je v rozporu s jejich investičním profilem a navíc, že takovouto službu pro ně není oprávněn vykonat.

Zákon č. 256/2004 Sb., o podnikání na kap. trhu, § 15h a Nařízení EK 2017/565 čl. 54 odst. 2, 5, 10

- CRYPTOCOIN: CryptoCoin. [online]. [cit. 2016-01-ŧϵ]. Přístup z internetu: www.cryptocoin.cc
- 65 IFREEDOM: Co jsou kryptoŵěŶy. [online]. [cit. 2016-01-ŧϵ]. Přístup z internetu: www.ifreedom.cz/cojsou-kryptomeny/
- 66 Zdroj: cs.wikipedia.org/wiki/Bitcoin

- DĚKUJI ZA POZORNOST