PROČ BITCOIN?

- CZ24 News | 3. července 2021

Pochopení kryptoměn vyžaduje nějaké množství času, a tyto články by vám mohly pomoci. Snažím se **bitcoin vysvětlit tak, aby to pochopil každý.**

„To není pro mne. Koukání do grafů a obchodování akcií – na to já nejsem,“ prohlásil můj známý. *„To nejsou akcie. Dá se s tím platit a není to vázáno na nějakou firmu,“* zkusil jsem ho ještě jednou přesvědčit. Marně. *„Dobře, tak mi pověz, v čem se to liší. Když to jde dolu, nakupuješ, a když nahoru, prodáváš. Jenže to nejde předvídat. Nakonec stejně přijdeš o peníze.“* O dva měsíce později mi známý volá a dotazuje se, jak že přesně ten Bitcoin funguje, že by ho to zajímalo. Za posledních několik týdnů cena kryptoměny několikanásobně vzrostla.

Jenže vysvětlit bitcoin není jednoduchý úkol. Pokud chceme porozumět, jak kryptoměny fungují, a mít jasno v tom, proč jim tak zázračně roste cena, musíme strávit nějaký čas zjišťováním informací. Vyhneme se tak bezhlavé investici do technologie, které ani pořádně nerozumíme. Často se stává, že lidé investují své peníze, aniž by chápali, do čeho je v tu chvíli vkládají. Když později přijdou o své úspory, mohou jen litovat své zbrklosti. Tomu lze studiem předejít. Na světě jsou tací, kteří díky bitcoinu velmi zbohatli, ale i nešťastníci, kteří o své peníze přišli, a už je nikdy neuvidí.

Bitcoin je nová technologie, jejíž složky byly objeveny dříve, ale doposud nebyly poskládány dohromady. Je to systém založený na principech, které tvůrce chytře spojil a vytvořil tak něco nového. Vynálezce je anonymní a již nemá žádnou kontrolu nad fungováním bitcoinu. Síť počítačů je tedy kompletně nezávislá na svém tvůrci. Tato technologie znamená nezávislé internetové peníze. Když si schováte prostředky v bance, musíte instituci věřit, že vám je v budoucnu vydá. To je určité riziko. Díky bitcoinu se již na nikoho spoléhat nemusíte. Dle mého názoru mají kryptoměny velký potenciál, stejně jako internet v 90. letech. Nemohu vám zaručit, že bitcoin změní svět. Mohu však vysvětlit, proč si to myslím.

Nejvíce lidí ke kryptoměnám přitahuje rychle rostoucí cena. Velmi pravděpodobně jste se o bitcoinu doslechli právě v souvislosti s tím, kolik stojí. Také se vám možná doneslo, že bitcoinů je jen omezené množství; ve finále jich bude zhruba 21 milionů. Omezená nabídka uchvacuje lidskou pozornost.

Bitcoin představuje alternativu současnému bankovnímu systému. Platit jím je jednoduché – stačí si nainstalovat aplikaci do telefonu. Můžeme příteli poslat peníze za pivo, zaplatit nákup elektroniky nebo si objednat pizzu. Účty lze vytvářet okamžitě a bez schvalovacích procesů. Kryptoměny může zkrátka používat kdokoliv.

Ke každému bitcoinovému účtu existuje heslo. Ten, kdo ho zná, může s účtem libovolně nakládat. To znamená především odesílat z účtu peníze a sdělovat ostatním adresy v případě, že potřebuje bitcoiny přijmout. Pokud je heslo ztraceno, k účtu se už nikdo nedostane. Zodpovědnost je tedy v rukou toho, kdo účet vytvoří. Pokud jsou prostředky převedeny na jiný účet, již není možné transakci vrátit. Bitcoin vrací zodpovědnost zpět do rukou lidu. Schovávejme svá hesla bezpečně, a nikdo nám nebude moci vzít naše peníze.

Pochopení kryptoměn vyžaduje nějaké množství času, a tyto články by vám mohly pomoci. Snažím se bitcoin vysvětlit tak, aby to pochopil každý. Občas se proto dopouštím zjednodušení. Určitě se vyplatí hledat informace i jinde.

Dříve jsem napsal, že Bitcoin je alternativou dnešního bankovnictví. Věřím, že je dokonce lepší než peníze současné. Bohužel, mezi lidmi není moc známo, v jakém finančním systému to vlastně žijeme. V tomto článku stručně popíši historii peněz.

Peníze vznikly jako prostředek směny. Bylo jednodušší vztahovat ceny výrobků k jedné věci, než zjišťovat, za co přesně by se (výrobky) daly vyměnit. Drahé kovy (především zlato a stříbro) byly ideální. Lidem se líbil jejich vzhled a těchto kovů nebylo mnoho; byly vzácné. Pokud se někdo chtěl ke zlatu dostat, musel ho vytěžit, nebo za něco směnit. Drahé kovy používané k platbám představovaly určité vynaložené úsilí potřebné k jejich získání a lidé si jich cenili.

Postupem času vznikly banky. Kdekomu bylo nepříjemné zlato schovávat, tak vděčně platil bankéřům, kteří drahý kov zabezpečili. Bankéři vydávali lidem poukázky na zlato, které si u nich schovali – bankovky. Vlastník bankovky si mohl do banky zajít pro zlato, které mu náleželo.

V roce 2008 byl zveřejněn vynález pojmenovaný bitcoin. Tvůrce (dost možná tvůrci) se podepsal jako Satoshi Nakamoto, dodnes je v anonymitě.

V roce 2008 byl zveřejněn vynález pojmenovaný Bitcoin. Tvůrce (dost možná tvůrci) se

podepsal jako Satoshi Nakamoto, dodnes je v anonymitě. V úvodním dokumentu je popsána myšlenka peněžního systému, kde není třeba nikomu věřit. Mohli byste si být jisti, že peníze, které držíte, nebude nikdo znehodnocovat uvolňováním nových. Tento systém začal fungovat v roce 2009. Od roku 2010 se Satoshi neozval a nemá žádnou kontrolu nad fungováním svého výtvoru.

Bitcoin je systém, který dokáže uchovávat informace (především finančního charakteru), aniž by byl centralizovaný (díky *blockchainu*). Kdokoliv může svým počítačem přispět k udržování tohoto systému v chodu. Jednotlivým počítačům se říká uzly, protože představují pomyslné body sítě, které jsou propojeny vlákny. Každý uzel udržuje na svém pevném disku tabulku (databázi), ve které je zaznamenáno, kolik bitcoinů je na jakém účtu. To znamená, že záznamy jsou veřejně dostupné, kdokoliv je může zkontrolovat. Z čísla účtu však není jasné, komu bitcoiny patří.

Uzly také přijímají nové transakce (převody bitcoinů) a sdělují je ostatním. Přibližně každých 10 minut jeden z počítačů nalezne číslo, které splňuje určité matematické požadavky. Výsledek rozešle ostatním a počítače uloží kopii tabulky tak, jak právě vypadala ve chvíli, kdy byl zjištěn. Této události říkáme *uzamčení bloku*.

Po uzamčení bloku se celý proces opakuje. Počítače se opět snaží nalézt číslo a (průměrně) za 10 minut se to některému z nich povede. Tím uzamkne další blok. Bloky se takto zamykají jeden za druhým, navazují na sebe a tvoří souvislý řetěz. Tomuto řetězu bloků se říká *blockchain* (z anglického „block“ a „chain“). V blockchainu jsou zapsány veškeré transakce od spuštění Bitcoinu.

Blockchain je uložen na spoustě místech, proto neexistuje žádné centrum. Stejně tak počítače, které udržují celý systém v chodu, jsou všude možně. Bitcoin tedy nelze „vypnout“. Dokud totiž bude alespoň jeden počítač Bitcoin udžovat, bude jej možné využívat. Jenže počítačů, které jsou připojeny, je dnes obrovské množství. A nejen to, jsou po celém světě, na každém kontinentu. Uvědomme si, že díky architektuře Bitcoinu neexistují v síti výpadky. Pokud se kterýkoliv uzel odpojí, nestane se vůbec nic, ostatní udržují síť v chodu i nadále.

Proč by někdo připojoval svůj počítač?

Ptáte se ale, proč by měl někdo zájem připojit svůj počítač do Bitcoinové sítě? Vždyť neustálé počítání spotřebuje velké množství elektřiny. Ano, to je pravda. Udržování sítě v chodu stojí vskutku nezanedbatelné peníze. Proč by to tedy někdo dělal?

Důvodem je skutečnost, že prvému počítači, který přijde s vhodným číslem, a uzamkne tak blok, je přidělena odměna v podobě bitcoinů. Část těchto mincí je zbrusu nová, k tomu těžaři obdrží ještě poplatky zaplacené s transakcemi. Je to podobné, jako když někdo vytěží zlato (proto se tento proces označuje těžba). Na rozdíl od zlata ale víme, kolik bitcoinů bude vytěženo, a kdy to (přibližně) bude.

Z připojení počítače do sítě se rázem stává zajímavá podnikatelská příležitost. Když pokryjete potřebné náklady (elektřinu), dostanete odměnu (bitcoiny). Lidé, kteří spatří možný výdělek, nakoupí výkonné počítače přispívající k chodu celé sítě.

V momentě, kdy některý počítač dojde k výsledku, jej rozešle ostatním. Těžař, který ho

vypočítal jako první, obdrží odměnu a matematická hádanka se opakuje. Počítače se snaží znovu najít číslo. Jak již víme, takto funguje blockchain. Tomuto konceptu se říká Proof of work. Znamená, že k fungování Bitcoinu je třeba vzácného zdroje – elektřiny.

V delším časovém horizontu lze počítat s pravděpodobností. Pokud vlastním jeden z deseti stejně výkonných počítačů, které jsou v síti zapojené, znamená to, že statisticky každý desátý blok dokáže vytěžit můj počítač. Mohu si tedy spočítat, že odměnu získám průměrně jednou za 100 minut.

Problém nastal ve chvíli, kdy se připojilo mnoho počítačů. Dnes už je v Bitcoinové síti nashromážděn značný výpočetní výkon. O velikost odměny se bát nemusíme; je dostačující. Háček je v pravděpodobnosti, že odměnu získá právě můj počítač – šance je vskutku malá. Proto se těžaři začali spojovat dohromady. Vytvořili jakési skupiny. Když jeden z počítačů ve skupině došel k výsledku, svou odměnu pak rozdělil mezi spojence podle toho, jak velkým výpočetním výkonem přispěli. Takové skupině se říká pool. Odměna je pak sice menší, zato přichází častěji.

Zhruba každé čtyři roky dojde k půlení. Nových bitcoinů začne přibývat méně. Dosavadní částka se sníží na polovinu. Při spuštění sítě v roce 2009 byla výše odměny stanovena na 50 btc. Od té doby se každé čtyři roky zmenšuje, v roce 2021 vzniká každých 10 minut jen 6,25 nových btc. Bitcoiny jsou tedy dělitelné. Nejmenší část, jedna stomiliontina, se nazývá satoshi (1 bitcoin = 100 000 000 satoshi). Nových bitcoinů bude přibývat, ale méně a méně. V roce 2021 je vytěženo 90% mincí, které kdy budou existovat.

Zhruba v roce 2140 nové bitcoiny přestanou vznikat definitivně. V té době bude vytěženo asi 21 milionů btc. Těžaři pak budou motivováni už jen poplatky, které jsou součástí každé transakce. Výši poplatku určuje ten, kdo bitcoiny odesílá. Velikost bloku je omezená. Pakliže nastavíte vyšší poplatek, těžaři budou více motivováni zanést transakci do blockchainu a ocitne se tam rychleji. Naopak, pokud nespěcháte, poplatek nastavíte nižší, jelikož nevadí, že převod bude zaznamenán až v řádu hodin.

Za zabezpečení svých bitcoinů je zodpovědný jejich majitel. Pokud je klíč ztracen, nikdo se k bitcoinům nedostane, jsou tedy doslova ztracené. To je daň, kterou platíme za nedotknutelnost našich peněz.

Úplným základem pro uchování bitcoinů je seed. Na základě seedu lze generovat prakticky neomezené množství účtů (privátních klíčů). Na blockchainu se lze dopátrat těchto účtů, najdeme tam veškeré transakce a zůstatky. Bez znalosti seedu však nelze zjistit, které účty k němu patří. Jeví se tak kompletně nezávislé. **Kdokoliv zná seed, může s bitcoiny** pod něj spadající **manipulovat**. Ke každému účtu patří nespočet adres, které slouží pro příjem bitcoinů. Často se adresy přenáší pomocí QR kódů.

Počet klíčů je nepředstavitelně velký. Pohybujeme se v číslech jako je 2^256 (to je přibližně 10^77 – odhady počtu atomů ve známém vesmíru se pohybují okolo 10^80). Uhádnout klíč je prakticky *nemožné* (kombinací je prostě příliš mnoho). Když chcete vytvořit heslo, stačí jen vygenerovat náhodné číslo. Bitcoinový účet si tedy může vytvořit i vy. Pro jeho založení není třeba žádné identifikace, nebo ověřování totožnosti. Může to udělat kdokoliv s chytrým telefonem nebo s

pomocí počítače. Bránit někomu vlastnit bitcoiny je obzvlášť složité. Dokonce vám ani nikdo nemůže pozastavit účet, či zabavit prostředky. I kdyby nějakým způsobem zjistil, který účet je váš, stále bez seedu nezmůže vůbec nic. Proto je důležité své přístupové údaje chránit.

Pro usnadnění práce se seed obvykle zaznamenává ve formě anglických slov. Těch je obvykle 24 nebo 12 a záleží na jejich pořadí. Bitcoiny lze tedy uchovávat jen tak, že jsou někde zaznamenána tato slova. Když ale chceme s prostředky manipulovat, potřebujeme k tomu nějaký program. Běžné jsou softwarové peněženky, které lze nainstalovat do počítače i telefonu. Tyto aplikace slouží ke správě účtů – pomocí rozhraní můžeme generovat adresy pro příjem i odesílat bitcoiny jinam. Nevýhodou takové peněženky je riziko viru. Zaprvé musíme věřit, že námi používaná peněženka není chybná a nesdílí naše klíče (proto doporučuji volit známější open-source peněženky). Zadruhé vaše zařízení může obsahovat škodlivý software, který by se dostal k uloženým klíčům.

Řešením je hardwarová peněženka. Velikostí se podobá flash disku a disponuje malou obrazovkou. Zařízení je schopno vygenerovat seed, privátní klíče a adresy, po připojení k počítači lze účty spravovat. Všechna hesla při tom však neopustí peněženku – počítač se k nim nedostane. Jelikož jsou hardwarové peněženky navrženy pouze pro správu a uchování kryptoměn, riziko viru je podstatně nižší.

Za zabezpečení svých bitcoinů je zodpovědný jejich majitel. Pokud je klíč ztracen, nikdo se k bitcoinům nedostane, jsou tedy doslova ztracené. To je daň, kterou platíme za nedotknutelnost našich peněz. Nakonec snad jen pamatujme, že když někdo bitcoiny ztratí, bude jich méně k dostání, tedy budou vzácnější.

Převezměme zodpovědnost do vlastních rukou.

Protože Bitcoin není řízen centrálně, zavést změny v jeho fungování není tak jednoduché. Zároveň ale není třeba žádného schvalovacího procesu; kdokoliv může vystavit svůj zlepšovací návrh na internet. Pokud těžaři shledají inovaci prospěšnou, nic jim nebrání v užívání nové verze. Když se ukáže, že je změna užitečná, ostatní nemají důvod se jí stranit, byli by na tom jen hůře. Jsou-li změny v programu natolik razantní, že nemohou fungovat s dosavadní verzí, blockchain se rozdělí na dvě větve – část historie transakcí mají poté obě větve stejnou. Nově vzniklá síť funguje nezávisle. Obyčejně se stane, že většina těžařů se ustálí na jedné větvi, a Bitcoin pokračuje dál. Z méně využívané větve se stává odnož Bitcoinu, jako je Bitcoin Cash nebo Bitcoin Gold.

Ptáte se, proč si úpravou programu těžaři nezajistí více bitcoinů? Takový krok se neslučuje s jejich zájmy; skutečná hodnota celého systému spočívá v tom, že nové mince přibývat nebudou, a těžaři to dobře vědí. Nicméně, vždyť se o to může pokusit kdokoliv, jen by jeho větev blockchainu nejspíše nikdo nevyužíval. Existuje tedy způsob, kterým můžeme inovovat, aniž bychom potřebovali autoritu, která vydává aktualizace. Možná, že díky tomu je riziko technických chyb i nižší.

Ani cena bitcoinu není určována centrálně. Odvíjí od toho, za kolik jsou lidé ochotni jej prodat. Většinou se obchody uskutečňují na internetových burzách, ale bitcoin si mohou směnit i lidé jen mezi sebou. Dvě strany se dohodnou na nějaké ceně a obchod proběhne, nebo se neshodnou, a k výměně nedojde. Jelikož ale spoustu nákupů probíhá právě přes internet, lze jednoduše zjistit, na jaké ceně se dohodli ostatní. Nedává potom smysl (až na výjimky), aby někdo kupoval bitcoin dráž,

než ho nabízí lidé na burze. Mohl by ho totiž koupit právě tam a ušetřit. Stejně tak je nevýhodné prodávat bitcoin levněji, protože ho lze prodat lépe. V jednu chvíli může být více lidí, kteří chtějí nakoupit, než těch toužících prodat. Aby si někdo zajistil, že na něj dojde, nabídne, že zaplatí více. To udělají i další. Pro některé už cena v tu chvíli bude příliš vysoká a tak svou nabídku nezvýší. Cena v tu chvíli vzroste, jelikož se lidé právě dohodli na vyšší ceně. V opačném případě cena klesá.

Satoshi inspiroval ostatní, kteří spatřili různá využití jeho vynálezu. Jejich představy byly ale příliš komplexní, tak se místo snažení změnit Bitcoin rozhodli přijít s něčím novým. Začaly vznikat i jiné blockchainy, a nebyly to odnože Bitcoinu. Celá oblast decentralizovaných internetových peněz se začala nazývat kryptoměny. Všem kryptoměnám vyjma Bitcoinu se říká altcoiny (alternativní mince). Altcoiny se liší především svým fungováním. Jejich autor je většinou známý a to může znamenat slabé místo. Je totiž součástí kryptoměny a celá technologie na něm do značné míry závisí.

Kryptoměny jsou stále poměrně volatilní (tzn. jejich cena je proměnlivá). Čím více lidí bude využívat Bitcoin, tím bude síť hodnotnější. Je to naše šance na lepší peníze, které nelze zfalšovat, a nikdo je neznehodnocuje inflací.

Převezměme zodpovědnost do vlastních rukou.

Autor: ANTONIO VILLICI

Zdroj: pravyprostor