Práce s virtuální měnou v běžné praxi
Working with virtual currency in general practice

Vlastimil Čejp

Abstrakt: Článek popisuje praktické aspekty držení virtuálních měn a problematiku běžného platebního styku s využitím bitcoinů. Článek zvažuje potenciální nové bankovní služby v oblasti virtuálních měn.

Klíčová slova: bitcoin, peněženka, virtuální měna, banka

Abstract: The article describes the practical aspects of holding virtual currencies and issue regular payment using Bitcoin. Article considers potential new banking services in the field of virtual currencies.

Keywords: Bitcoin, wallet, virtual currency, bank

JEL Classification: G23,O33

Úvod

Virtuální měny a zvláště bitcoin jako její nejznámější představitel, ať si to přejeme nebo ne, se stávají významným fenoménem v ekonomice i informatice. Roste množství bitcoinů v oběhu, roste počet uživatelů i podnikatelů akceptujících bitcoiny jako platidlo. Vznikla celá řada následovatelů bitcoinů jako jsou litecoin, namecoin, altcoin a další. Všechny státy světa řeší, jak se k tomuto fenoménu postavit, hlavně jak ho legislativně zakotvit. Jednak státy mají zájem na vybírání daní a v neposlední řadě hrozí nebezpečí zneužití bitcoinů k k financování obchodu se zbraněmi, drogami, k podpoře terorismu, korupci a dalším podobným činnostem.

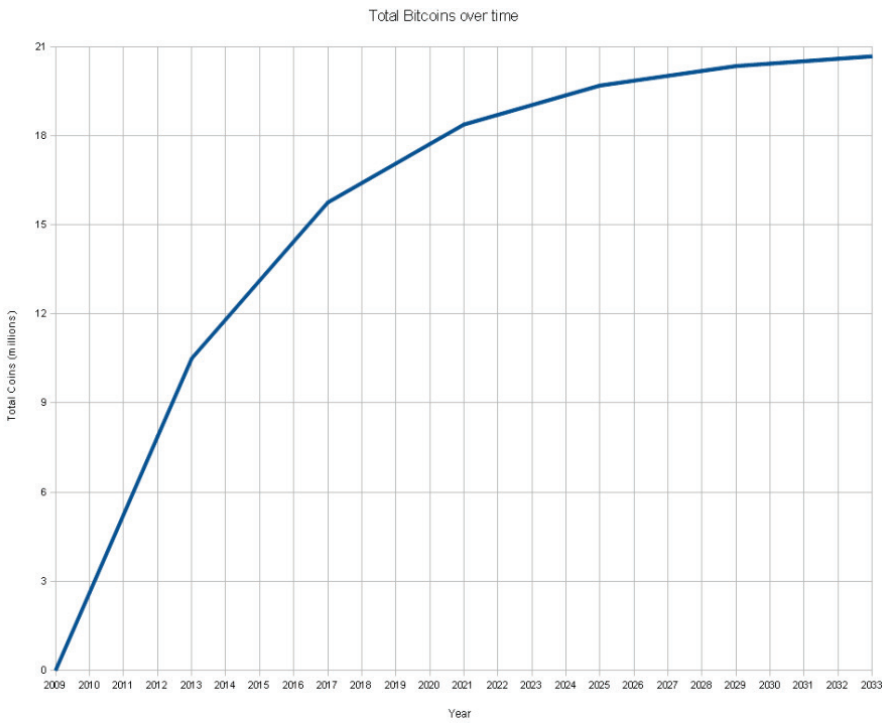
Bitcoiny fungují jako P2P platební síť. Ačkoli v minulosti bylo již několik snah o vytvoření elektronické měny jako například populární fazole viz. [1], unikátnost bitcoinů spočívá v tom, že jsou decentralizované. Celý algoritmus je navržen tak, že ho nemůže nikdo včetně autorů ovlivnit. Nelze měnit počet bitcoinů v oběhu, nelze vytvářet nekontrolovaně nové bitcoiny a podobně.

Doslova každý uživatel sdílí s ostatními databázi všech transakcí a zůstatků na všech „účtech" tzv. adresách bitcoinové sítě. Pokud někdo chce uskutečnit platbu, vezme příslušnou částku, udá, na jakou adresu ji posílá, informaci podepíše svým soukromým klíčem a pošle ji ostatním uživatelům. Informace o platbě je tak okamžitě rozeslána všem ostatním.

Dále musí následovat tzv. potvrzení této transakce. Další skupina uživatelů tzv. těžaři seskupí několik transakcí a snaží se nalézt šifru (kryptografickou nonci) potvrzující tyto transakce. Za potvrzení transakcí je těžaři uvolněna odměna v bitcoinech. Což je jediný způsob, jak vznikají nové bitcoiny. Bez těžařů by nevznikaly nové bitcoiny, ani by nešly realizovat transakce. Navíc ten, kdo zadává transakci, může nabídnout těžařům poplatek a tím zkrátit čas, kdy si právě jeho transakci vyberou těžaři k potvrzení. Každé potvrzení je náročnější než to předchozí a potvrzuje i všechny předešlé transakce. Každá transakce je tak opakovaně potvrzována, čím je vícekrát potvrzena tím je obtížnější ji padělat. Prakticky je to nemožné už při prvním potvrzení a s každým dalším potvrzení se úvahy o padělání stávají více teoretické. Ten, kdo by chtěl změnit transakce v síti, by musel disponovat obrovským výpočetním výkonem, který by cca 100násobně převyšoval výkon současných největších světových superpočítačů. Distribuovaný výpočet v síti je tak současně i ochranou před zneužitím jednotlivcem či skupinou. Podrobněji o způsobu výpočtu viz [3].

Nové bitcoiny se tak objevují postupně. Celkově existuje 21 mil bitcoinů resp. (resp. 20 999 999,9769). Pokud bude nárůst výpočetního výkonu postupovat jako dosud, dá se odhadnout, že všechny bitcoiny budou vypočteny někdy v roce 2140 (většina však do r. 2030). Zatím je bitcoiny možno dělit na 8 desetinných míst, ale existuje možnost rozšíření. Tj. bude-li i za 100let stále o tuto měnu zájem, nebude problém pracovat s velmi malými zlomky bitcoinu.

Odhadovaný počet bitcoinů do r. 2033



Zdroj: https://en.bitcoin.it/wiki/File:Total_bitcoins_over_time_graph.png

1. Jak funguje bitcoin v praxi

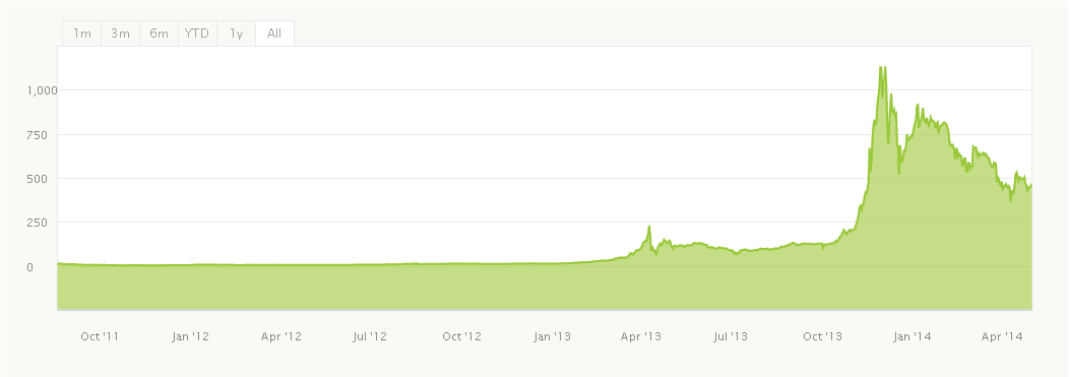
Tento článek popisuje práci s bitcoiny jako práci s měnou – řekněme virtuální měnou. Virtuální protože de facto neexistuje ve fyzické podobě, ale pouze v datové reprezentaci v počítači, kde používáme stejné označení. Srovnání s měnou se nabízí, ale pravdou je, že názor legislativců na povahu bitcoinu není jednotný. Někdy se hovoří o komoditě, cenině a připodobňuje se tak k dalším existujícím entitám. Popravdě státy a centrální banky s mocí nad vlastní měnou někdy předvádějí takové věci, že není divu, že běžný občan ztrácí důvěru v klasické měny viz [2]. Vznik virtuálním měn je možná reakcí na takové chování. Účelem tohoto článku není přispět k odpovědi na tuto otázku, ale zamyslet se nad reálnou použitelností bitcoinů a virtuálních měn obecně.

Ano, virtuální měny přinášejí svobodu, měnu bez vlivu politiků a států, práci s penězi bez bank, převody hodnot napříč světem bez nesmyslných bankovních poplatků a vůbec potřeby bank. Realita však není až tak jednoduchá.

Předně při práci s bitcoinem je třeba počítat se zatím velmi volatilním kurzem. Obecně je bitcon deflační měnou, tj. jeho hodnota by měla růst. Reálná směnitelnost bitcoinu

na dolar, euro či korunu je však dána nabídkou a poptávkou. Ochota lidí měnit reálné peníze za virtuální měnu a naopak závisí na mnoha faktorech – různá prohlášení politiků o tom, jak budou a nebudou regulovat tuto měnu nebo zprávy o defraudaci prostředků klientů na burzách směňujících bitcoiny na peníze a naopak výrazně ovlivňují aktuální výši kurzu. Nehledě na to, že i relativně malý počet transakcí a uživatelů znamená, že každý větší obchod může snadno významně změnit kurz. Nemluvě o tom, že existují skupiny uživatelů domlouvajících se na sociálních sítích a záměrně se snažících takové operace provádět za účelem vlastního obohacení. Při neexistence regulace tento postup však není nelegální.

Vývoj kurzu bitcoinu k USD dle burzy bitstamp



Zdroj: www.bitstamp.net

Aktuální hodnota v době tvorby tohoto článku se pohybovala v řádu cca 450USD za 1 bitcoin (BTC) tj. cca 8900Kč za 1BTC. Změny kurzu v řádu i desítek procent během dne však nejsou výjimkou. Budeme-li optimisticky předpokládat, že si bitcoin najde svoji relativně stabilní hodnotu, je tu další problém – informatická a matematická složitost práce s bitcoiny.

2. IT a práce s bitcoinem

Pro zkušené informatiky, pro které P2P sítě nejsou ničím zvláštním, i pro informatiky, kteří jsou zvyklí nakládat s šifrovacími klíči, pro které není zálohování a hodnota dat prázdným pojmem, je jistě způsob práce s touto virtuální měnou akceptovatelný. Pro běžného uživatele je zde ale celá řada nástrah:

Drobnou technickou komplikací pro běžného uživatele je už to, že musí mít ve svém zařízení a klientovi komplet celu databázi všech transakcí za celou historii bitcoinu. Záleží na typu klienta, ale v dnešní době je to cca 12GB dat. Pokud se tato databáze stahuje klientovi na mobil, nemusí to být úplně zanedbatelný objem dat.

Pokud navíc v této souvislosti uvážíme, že využívání bitcoinů je teprve v počátcích, dá se očekávat, že velikost databáze poroste. Už dnes je například instalace klientského SW na chytrý mobilní telefon představuje právě kvůli stažení databáze poměrně časově náročnou operaci. I když rychlosti připojení k internetu i datové kapacity stále rostou, nelze tento problém eliminovat. Jistým řešením je využití cloudové peněženky – tj. de facto služby cizího serveru, kde máme peněženku uloženou včetně právě sdílené transakční databáze. Nicméně musíme pak tomu serveru důvěřovat, protože mu sdělujeme privátní klíče pro ovládání peněženky. Tuto službu nabízí například server BLOCKCHAIN - https://blockchain.info/.

Ztráta šifrovacího klíče (peněženky) – dalším problémem je vlastnost, která měla být výhodou. Ano uživatel je nezávislý na autoritách, bankách apod. Je to ale vykoupeno zodpovědností uživatele. Na zařízení, kde máte instalován klient – svoji peněženku jsou i Vaše šifrovací klíče, které umožňují manipulaci s jednotlivými adresami tj. se samotnými bitcoiny. V případě ztráty či smazání nebo zničení počítače přijdete nenávratně i o bitcoiny. Nezanedbatelné množství bitcoinů je dnes nenávratně ztraceno právě z peněženek uživatelů, kteří přišli o data. Zapomenutý pin či heslo do internetového bankovnictví Vám Vaše banka vyřeší (možná zdarma, možná za poplatek) ale o peníze nepřijdete. Když ale máte na starosti notebook, kde jsou klíče k bitcoinům, jejichž hodnota třeba násobně převyšuje cenu hardware, je zodpovědnost jen na Vás.

Práce s variabilními symboly – v bitcoinové síti neexistuje něco jako variabilní symbol. Bitcoiny jsou posílány vždy z jedné adresy na druhou bez jakékoli další identifikace. Nic ale nebrání tomu pro každou transakci vygenerovat novou adresu či celou peněženku. V platebním styku je třeba používat trochu jiné procesy než je to obvyklé v klasickém bankovním světě – účty, variabilní a specifické symboly atd.

Když přidáme relativně komplikované formální zápisy adres:
(např.: 1F3Hd4wtvUVTTMxeyjYzpR5TP9oheYHEuv – příklad bitcoinové adresy).

Navíc každá transakce má vlastní ID, které má ještě více znaků:
(např.: e185938b1897d43e7b5fe1c41aadbec7adcf21f348eb4c2665d66b54cd401550 – příklad ID transakce),

je pro běžného uživatele práce s těmito entitami ne příliš přívětivá. Pokud například chcete, aby Vám někdo zaplatil v bitcoinech danou částku, musí Váš klient vygenerovat příkaz, jehož bezchybné opsání je velmi náročné i když obsahuje bezpečnostní redundantní mechanizmy pro eliminaci překlepů. Obvykle se v praxi udává formou 2D čárového kódu, který si platící vyfotí např. mobilem:

Příklad požadavku na platbu 1BTC na danou adresu. (Generováno oficiálním open-source bitcoin klientem)

Paradoxně tak přednosti, se kterými dnes virtuální měny získávají tolik pozornosti a úspěchu, mohou být nepřekonatelným problémem pro běžné uživatele mimo IT komunitu, kde původně virtuální měny vzniky. Běžný uživatel může mít problémy toto vše zvládat včetně zodpovědnosti za vlastní data. Nemluvě o komplikované konverzi mezi virtuálními a reálnými měnami, která je zatím možná jen na specializovaných burzách. Otvírá se tak prostor pro nový typ bankovních (informatických) služeb. Je otázkou, zda se podaří politikům resp. legislativcům zaujmout rychle vhodný postoj k tomuto fenoménu. Aby se tyto služby na zatím prakticky vůbec neregulovaném trhu nestaly pouze příležitostí pro podvodníky. Různé státy se k problematice virtuálních měn staví různě, převážně ale spíše váhají. I český bankovní dohled se staví k této problematice trochu s odstupem, viz stanovisko České národní banky z 10. 2. 2014 viz: http://www.cnb.cz/miranda2/export/sites/www.cnb.cz/cs/faq/obchodovani_s_bitcoiny.pdf

Další vývoj ukáže, zda budeme každý sám sobě bankou nebo si korporace najdou opět svůj business i zákazníky nebo zda bitcoiny a další virtuální měny čeká stejný osud jako fazole z úvodu tohoto článku.

Reference

[1] Fazole.cz. FAZOLE S.R.O. [online]. [cit. 2014-05-03]. Dostupné z: http://www.fazole.cz/

[2] SELGIN, George. Centrální banky pošlapaly veškeré zásady: Přišel čas digitálních měn?. In: [online]. [cit. 2014-05-03]. Dostupné z: http://www.investicniweb.cz/2013/9/14/george-selgin-centralni-banky-poslapaly-veskere-zasady-prisel-cas-digitalnich-men/

[3] HRACH, Jan. Decentralizovaná kryptoměna Bitcoin. In: [online]. 27. 7. 2011 [cit. 2014-05-03]. Dostupné z: http://www.abclinuxu.cz/clanky/decentralizovana-kryptomena-bitcoin

[4] Bitcoin - Wiki. [online]. [cit. 2014-05-04]. Dostupné z: http://cs.wikipedia.org/wiki/Bitcoin

Ing. Vlastimil Čejp, Vysoká škola manažerské informatiky, ekonomiky a práva, a.s., Vltavská 585/14, 150 00 Praha 5, vlastimil.cejp@vsmiep.cz