Ekonomika Economics
Management Management
Inovace Innovation

EMI, Vol. 8, Issue 3, 2016
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

VYUŽITÍ BITCOINU JAKO NÁSTROJE PRO ALTERNATIVNÍ DECENTRALIZOVANOU INVESTICI

BITCOIN USE AS A TOOL FOR ALTERNATIVE LOCAL INVESTMENT

Jan Lavrinčík
Moravská vysoká škola Olomouc, Czech Republic
jan.lavrincik@mvso.cz

Abstrakt:
Článek se zabývá obchodními možnostmi s kryptoměnou Bitcoin. Vysvětluje, co to je kryptoměna Bitcoin, v čem spočívá pojem decentralizované měny a naznačuje možnosti, jak dohledat všechny transakce. Zaměřuje se především na strategie získání/nákupu Bitcoinů, jejich obchodováním na burzách s kryptoměnami, potenciálem těžby Bitcoinu, sběru na službách faucet. Přibližuje význam budování alternativních investic z pohledu anonymity a daňové politiky EU. Velký důraz je kladen na praktické ukázky práce s Bitcoiny v období mezi prosinec 2015 až květen 2016.

Klíčová slova:
Bitcoin, kryptoměna, faucet, těžba, cloud mining, burza.

Abstract:
The article deals with cryptocurrency Bitcoin and its business opportunities. Explains what it is cryptocurrency Bitcoin, what is the concept of decentralized currency and suggests ways to trace all transactions. It focuses primarily on strategies for acquisition / purchase Bitcoin, trading them on exchanges with cryptocurrency, potential mining bitcoin, collection services to the faucet. About the importance of building alternative investments in terms of anonymity and tax policy. Great emphasis is placed on practical demonstrations of working with Bitcoin in the period between December 2015 and May 2016.

Klíčová slova:
Bitcoin, kryptoměna, faucet, těžba, cloud mining, burza.

Key words:
Bitcoin, cryptocurrency, faucet, mining, mining cloud, stock market.

JEL: E42, G35, J33.

Úvod: Kryptoměna Bitcoin

V současné době se můžeme v odborné literatuře nebo při platebním styku setkat s pojmem kryptoměna. Za předchůdce kryptoměny jsou často považovány digitální a virtuální měna (Zákon č. 284/2009, Schlossberger, 2012, s. 142-143). Označení kryptoměna vyjadřuje, že měna je postavena na poznatcích z oboru kryptografie (nauka o metodách utajování smyslu informace převodem do podoby, která je čitelná jen s předem definovanou znalostí, pochází z řečtiny – kryptós = skrytý a gráphein = psát). V současné době je známo více než 100 kryptoměn (Bter.com: BitCoin and Crypto-currency Exchange Platform) z nichž nejznámější, nejpoužívanější a nejstarší je Bitcoin. Mezi další obchodovatelné

EMI, Vol. 8, Issue 3, 2016
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

kryptoměny patří Litecoin, Dogecoin, Dash, Quark, Ethereum a další. Rozdíl mezi klasickou měnou Fiat a kryptoměnou Bitcoin bychom mohli shrnout do přehledné tabulky číslo 1. Za nejvýznamnější inovaci můžeme považovat to, že každá peněženka je anonymní, můžeme ji darovat, nelze ji zdanit a dohledat jejího majitele.

Tabulka 1: Rozdíl mezi klasickou měnou Fiat a Bitcoin.

FIAT	BITCOIN
- Státní monopol, vláda, CB. - Lze tisknout, devalvovat, znárodnit. - Účty lze zabavit, obstavit, zjistit zůstatek. - Transakce jsou vratné. - Lze padělat.	- Matematické zákony a výpočetní síla (GPU – CUDA). - Přesný počet 21 miliónů, postupně těžený. - BTC adresa je skrytá. - Transakce jsou nevratné. - Nelze padělat, znárodnit, zdanit, dohledat majitele.

Vznik Bitcoinu se datuje do roku 2008, kdy Satoshi Nakamoto publikoval dokument (Bitcoin P2P e cash paper) na webu metzdowd.com popisující protokol Bitcoin (from:'Satoshi Nakamoto.'). Z dalších zajímavých milníků stojí za zmínku datum 3. ledna 2009 - byl vytěžen první Bitcoin, 12. ledna 2009 – proběhla první bitcoinová transakce, 9. února 2011 – hodnota Bitcoinu poprvé překonala hranici 1 USD, 19. listopad 2013 Bitcoin dosahuje historicky nejvyšší hodnoty 1242 USD za 1 BTC (Bitcoin Firsts; Bitcoin history: The Complete History of Bitcoin).

Když jsme zmínili u Bitcoinu označení kryptoměna, znamená to, že se jedná o protokol, algoritmus a nehmatatelnou měnu (Senate Committee Listens to Bitcoin Experts, Expresses Open-Mindedness, On Bitcoin; Hearings Homeland Security & Governmental Affairs Committee). Při práci s Bitcoinem se používá zkratka BTC. Vzhledem k současnému kurzu pohybujímu se okolo hodnoty 460 EUR / 1BTC je Bitcoin dělen na menší jednotku Satoshi (dle jména zakladatele), kde 1 satoshi = 0,000 000 01 BTC. Cenu Bitcoinu na burze v největší míře ovlivňují nákupy a prodeje, přičemž nejvíce je jich zrealizováno v Číně. Vzhledem k historickému vývoji hodnoty této měny můžeme uvést, že se jedná o vysoce volatilní kryptoměnu. K dalším faktorům, které mohou ovlivnit její cenu, to jsou například mikroekonomické a makroekonomické ukazatele, ekonomické krize, spekulativní bubliny, prohlášení respektovaných členů komunity, technologické inovace, odměny za těžbu, vládní zásahy, regulace Bitcoinu v dané zemi Muchholz, Delaney, Warren, Parker 2012; Yermack 2013).

Graf 1: Historický vývoj ceny Bitcoinu.

EMI, Vol. 8, Issue 3, 2016
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

K uchovávání Bitcoinu, jelikož se jedná o nehmatatelnou měnu, se používají tzv. peněženky. Ty mohou být elektronické na serveru poskytovatele (on-line) nebo ve formě softwaru. On-line peněženky mají tu výhodu, že umožňují prostřednictví mobilní aplikace mít Bitcoiny okamžitě připravené k platbě, ale nehodí se na držení větších obnosů z důvodu bezpečnosti. Každá peněženka, abychom na ni mohli přijímat Bitcoiny má svoje jedinečné číslo v síti, může například vypadat následovně: 14ECFC5r6DYsfW3Gqo4GucLxDFcHeGdsdb (Jak začít s Bitcoiny na btctipcz).

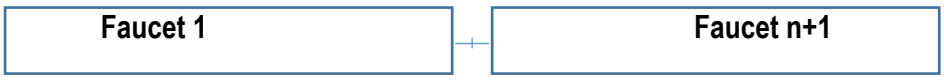
Když chceme vytvořit transakci mezi dvěma peněženkami, potřebujeme bitcoinovou adresu, což je veřejná 160bitová hash generovaná pomocí protokolu digitálního podpisu s využitím eliptických křivek ECDSA (Base58Check encoding; Bitcoin Base58 Encoder, Decoder, and Validator; bitcoin/base58.cpp at master). Ta se skládá z veřejného a privátního klíče. Každou transakci je nutné podepsat privátním klíčem. Veřejný klíč, pak může použít kdokoliv, kdo chce zjistit, zda má daný uživatel vlastnická práva k daným Bitcoinům ((Base58Check encoding; Bitcoin Base58 Encoder, Decoder, and Validator). S Bitcoiny lze specifickým způsobem pracovat, proto se v další kapitole zaměříme zejména na vybrané modely práce s kryptoměnou Bitcoin.

Modely práce s kryptoměnou Bitcoin

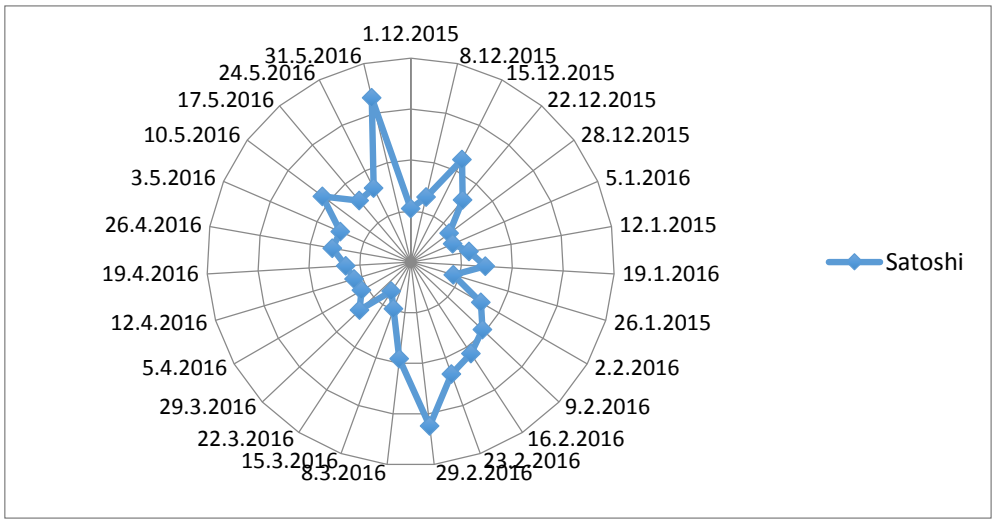
Modelový příklad č. 1 (získání bez vlastního vkladu - faucets)

Jednou z možností, jak získat zcela zdarma Bitcoiny, resp. menší jednotky Satoshi, je sběrem přes takzvané „faucety“. Celý obchodní model je založen na zobrazování reklamy na stránce, například využívající službu Google Adsence. Za kliknutí na reklamu dostane provozovatel webu zaplaceno, a o malou část této provize se ve formě Satoshi dělí s návštěvníkem. Stránky musejí být chráněny proti robotickému přístupu Captcha kódem a časovým limitem (zpravidla mezi 10 až 60 minut).

Obrázek 1: Model využití služeb faucet.



Graf 2: Ukázky profitability faucetu Daniela Bainbridge (Bitcoin Free, Bitcoin Aliens, Abudance, Blockchain Game) v období mezi 1.12.2015 – 31.5.2016.

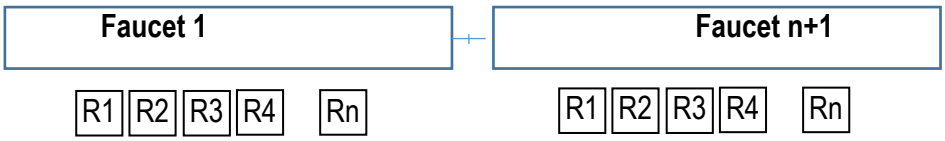


Výše uvedený model můžeme aktivním přístupem a úspěšnou registrací z referenčního odkazu rozšířit svoji základnu a získat z nasbíraných dat dle služby provizi mezi (10 – 50 %). Takto vytvořená

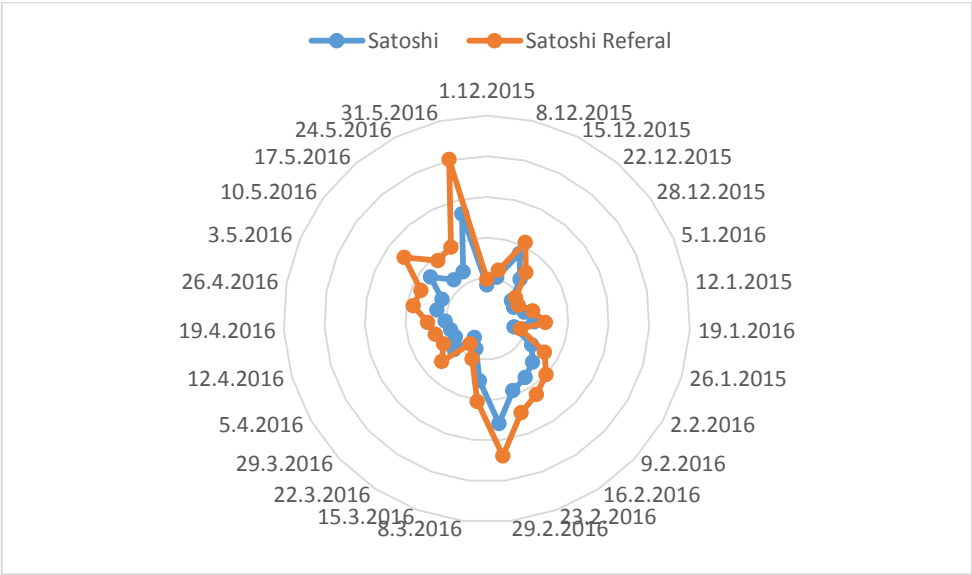
EMI, Vol. 8, Issue 3, 2016
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

aktivní struktura může znásobit zisky a sběr se tak může stát profitabilním a stabilním nástrojem pro budování pasivního příjmu.

Obrázek 2: Model služeb faucet s využitím referenčních linků.



Graf 3: Ukázky profitability faucetu Daniela Bainbridge s referenčními linky (Bitcoin Free, Bitcoin Aliens, Abudance, Blockchain Game) v období mezi 1.12.2015 – 31.5.2016.



Dílčí závěr: Sběr Satoshi z faucetů není profitabilní a výdělky se při kombinaci více služeb dají počítat od 2 – 10 euro/týdně. V případě kombinace z referenčních odkazů jde znásobit profit. Službu lze považovat za profitabilní v případě struktury minimálně 50 – 100 aktivních členů. Model je vhodný k získání úvodních satoshi na vyzkoušení systému plateb a eliminaci rizik.

Modelový příklad č. 2 (bez vlastního vkladu – těžba kryptoměny)

Bitcoin se těží pomocí výpočetní síly grafických karet. Za vytěžení každého Bitcoinu je poskytována odměna, která je závislá na výkonu těžebního zařízení, náročnosti sítě. V současné době se těžba jednotlivcům nevyplatí, a proto jsou sdružováni to tzv. „těžebních poolů“. Jedním z nejznámějších českých poolů je https://slushpool.com/home/.

Zdrojový kód 1: Ukázka nastavení těžební aplikace Mac Miner.

```
{
"pools" : [
        {
                "url" : "stratum+tcp://stratum.bitcoin.cz:3333",
                "user" : "USER NAME.NUMBER OF WORKER",
                "pass" : "ANYTHING"
        }
]
```

EMI, Vol. 8, Issue 3, 2016
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

}

Modelový příklad pro grafickou kartu Radeon HD7870, která dokáže počítat rychlostí přibližně 400 Mhash/s (milionů hashů za vteřinu). S výpočetním výkonem této grafické karty se dnes dá vytěžit okolo 0.000006 BTC denně. Zisk odpovídá hodnotě několika haléřů.

Dílčí závěr: Těžba bitcoinů není profitabilní, protože na ni máme vysoké pořizovací náklady na hardware a spotřebu elektrické energie. K dosažení profitability je zapotřebí nákup levného hardware a vlastní výrobu elektrické energie z obnovitelných zdrojů (solární, vodní elektrárny). Navíc musíme počítat s postupně se zvyšující náročností těžby a tím i klesající odměnou.

Modelový příklad č. 3 (vlastní vklad do 1 BTC)

Cloudová těžba je založená na pronájmu určitého počtu výpočetních jednotek, které těží odpovídající množství kryptoměny. Reálná návratnost investice se pohybuje v horizontu 4 – 6 měsíců a teprve poté může být těžba profitabilní. Při cloudové těžbě by měla platit stejná pravidla, jako při běžné těžbě, tzn. zvyšující se obtížnost výpočtu a klesající odměna za vytěžený blok. Proto dle dlouhodobých analýz je výhodné mezi 25 – 35 % reinvestovat do nákupu výpočetní síly a tím udržovat stejnou úroveň výkonu těžby.

Jako krátkodobé obchody můžeme považovat obchody, které mají zpravidla délku v horizontu desítek vteřin až jednoho měsíce. Využívají se k nim specializované burzy, z nichž nejznámější je www.bter.com. Obchodování má podobný charakter jako Forex (Foreign Exchange) s tím rozdílem, že kapitál je obchodován většinou mezi kryptoměnami, kterých je z pohledu obchodování k dispozici více než 100 (například: Dogecoin, Litecoin, Ethereum atp.).

Příklad cldmine.com: investice 0,5 BTC, výběr 0,03 BTC za období 10 dnů představuje návratnost investice za 5,56 měsíce (0,5 BTC / 0,03 = 16,67; 16,67 x 10 = 166,7 dnů; 167 / 30 = 5,56 měsíce).

Tabulka 2: Ukázka příkladů krátkodobých obchodů.

Datum nákup	Počet BTC	Cena	Datum prodej	Počet	Cena	Zisk [USD]
25.3.2013	1 BTC	73,6 USD	10.4.2013	1 BTC	230 USD	+ 156,4 USD
26.5.2016	1 BTC	452 USD	1.6.2016	1 BTC	542 USD	+ 90 USD

Dílčí závěr: V případě, že disponujeme větším objemem finančních prostředků, tak se jedná o profitabilní strategii, nabízející potenciálně zajímavý zisk v desítkách procent/měsíc. Na cenu v uvedených případech měl největší vliv obrovský nárůst poptávky na trhu a to zejména v Číně.

Modelový příklad č. 4 (vlastní vklad 1 BTC a dlouhodobé držení pozice)

Dlouhodobé nákupy představují z pohledu běžných trhů doporučený časový horizont v rozpětí 2 – 7 let, dle brokera. Vývoj kryptoměny je v krátkém časovém intervalu rychlejší, proto tento horizont můžeme i zkrátit na 6 – 36 měsíců. Na dlouhodobých nákupech lze spekulovat zejména na předem daném počtu Bitcoinů, kterých bude v oběhu 21 000 000 a zvyšující se náročnosti těžby a snižující se odměně za vytěžený blok. Uvedené faktory a poptávka na trhu můžu vést k překonání zatím nejvyšší tržní ceny z 19. listopadu 2013.

Tabulka 3: Ukázka příkladů dlouhodobých jednorázových obchodů.

Datum nákup	Počet BTC	Cena	Datum prodej	Počet	Cena	Zisk [USD]
1.5.2009	1 BTC	0,65 USD	19.11.2013	1 BTC	1242 USD	+ 1241,35 USD

EMI, Vol. 8, Issue 3, 2016
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

27.1.2015	1 BTC	197 USD	1.6.2016	1 BTC	542 USD	+ 345 USD

Dílčí závěr: V případě, že disponujeme větším objemem finančních prostředků, tak se jedná o profitabilní strategii, nabízející potenciálně zajímavý zisk v desítkách procent/měsíc. Držení větších finančních prostředků Bitcoinů je ovšem rizikové z pohledu bezpečnosti, kde se jako zajímavý bezpečnostní prvek jeví využití hardwarové ochrany Bitcoin Trezorem (BTCtip: Bitcoin Trezor).

Diskuze a závěr

Kryptoměny a zejména Bitcoin jsou poměrně mladou záležitostí a možnosti jejich využití jsou v počátcích. Česká komunita patří díky těžebním poolům a zejména Bitcoin Trezoru ke světové špičce v oblasti práce s Bitcoiny. U nás už můžeme najít více než 200 akceptačních míst pro platbu, nákup či prodej Bitcoinů. Z hlediska analyzovaných modelů můžeme stanovit následující závěr. Sběr bitcoinů ze služeb faucet je neefektivní a stává se efektivním až v případě vytvoření velké sítě z referenčních linků zahrnující více než 100 uživatelů. Fyzická těžba prostřednictví výkonu grafické karty má výnosy menší než řády jednotek. Diskutovanými a do budoucna zajímavými cestami se jeví cloudová těžba založená na pronájmu výpočetní síly, obchodování s kryptoměnami na specializovaných burzách typu www.bter.com. Obchodní potenciál se díky vysoké volatilitě pohybuje v řádu desítek procent měsíčně. Pokud Bitcoiny vlastníte, když srovnáme cenu z konce května 2015 (235 EUR / 1 BTC) a května 2016 (462 EUR / 1 BTC), tak se jeví jako výhodná strategie dlouhodobé držení. Pokud se chystáte nakupovat a obáváte se rizika ztráty z pohledu volatility, můžete zkusit strategii pravidelného nákupu.

EMI, Vol. 8, Issue 3, 2016
ISSN: 1804-1299 (Print), 1805-353X (Online)
www.emijournal.cz

Literatura

[1] "Zákon č. 284/2009 Sb., o platebním styku." [Online]. Available: https://portal.gov.cz/app/zakony/download?idBiblio=69225&nr=284~2F2009~20Sb.&ft=pdf. [10-Aug-2015].
[2] SCHLOSSBERGER, Otakar. Platební služby. Praha: Management Press, 2012. ISBN 978-80-7261-238-3.
[3] Bter.com: BitCoin and Crypto-currency Exchange Platform. [on-line]. 2013. [2016-05-05]. URL < http://www.bter.com/>.
[4] Bitcoin P2P e cash paper." [on-line]. 2015. [2016-05-05]. URL <http://article.gmane.org/gmane.comp.encryption.general/12588/>.
[5] "from:'Satoshi Nakamoto.'" [on-line]. 2015. [2016-05-05]. URL <http://www.mail-archive.com/search?l=cryptography@metzdowd.com&q=from:%22Satoshi+Nakamoto%22>.
[6] Bitcoin Firsts - Bitcoin Wiki. [on-line]. 2015. [2016-05-05]. URL <https://en.bitcoin.it/wiki/Bitcoin_Firsts>.
[7] "Bitcoin History: The Complete History of Bitcoin [Timeline]." [Online]. Available: http://historyofbitcoin.org/. [Accessed: 11-Aug-2015].
[8] Senate Committee Listens to Bitcoin Experts, Expresses Open-Mindedness, On Bitcoin [on-line]. 2013. [2016-05-05]. URL <http://onbitcoin.com/2013/11/18/senate-committee-listens-bitcoin-experts-expresses-open-mindedness/>.
[9] Hearings Homeland Security & Governmental Affairs Committee. [on-line]. 2015. [2016-05-05]. URL <http://www.hsgac.senate.gov/hearings/beyond-silk-road-potential-risks-threats-and-promises-of-virtual-currencies>.
[10] Martis Buchholz, Jess Delaney, Joseph Warren, and Jeff Parker, "Information, Price Volatility, and Demand for Bitcoin," jaro-2012. [on-line]. 2012. [2016-05-05]. URL <http://academic.reed.edu/economics/parker/s12/312/finalproj/Bitcoin.pdf>.
[11] D. Yermack, "Is Bitcoin a Real Currency? An economic appraisal," National Bureau of Economic Research, Working Paper 19747, Dec. 2013.
[12] Jak začít s Bitcoiny na btctipcz [Timeline]. [on-line]. 2015. [2016-05-05]. URL <http://btctip.cz/jak-zacit-s-bitcoiny-2/>.
[13] Base58Check encoding - Bitcoin Wiki. [on-line]. 2015. [2016-05-05]. URL <https://en.bitcoin.it/wiki/Base58Check_encoding/>.
[14] Bitcoin Base58 Encoder, Decoder, and Validator. [on-line]. 2015. [2016-05-05]. URL <http://lenschulwitz.com/base58/>.
[15] bitcoin/base58.cpp at master · bitcoin/bitcoin. [on-line]. 2015. [2016-05-05]. URL <https://github.com/bitcoin/bitcoin/blob/master/src/base58.cpp>.
[16] Technical background of version 1 Bitcoin addresses - Bitcoin Wiki. [on-line]. 2015. [2016-05-05]. URL < https://en.bitcoin.it/wiki/Technical_background_of_version_1_Bitcoin_addresses/>.
[17] Bitcoin: A Peer-to-Peer Electronic Cash System. [on-line]. 2015. [2016-05-05]. URL <https://bitcoin.org/en/bitcoin-paper/>.
[18] BTCtip: Bitcoin Trezor - Jak mít Bitcoiny v bezpečí. [on-line]. 2014. [2016-05-05]. URL <http://btctip.cz/bitcoin-trezor-recenze/>.