PRÁCE S DATY NA INTERNETU

PhDr. Jan Lavrinčík, Ph.D.

Podpora kompetencí vedoucích pedagogických pracovníků při implementaci digitálních technologií do života školy/školského zařízení

STUDIJNÍ TEXTY K DISTANČNÍMU VZDĚLÁVÁNÍ

EVROPSKÁ UNIE
Evropské strukturální a investiční fondy
Operační program Výzkum, vývoj a vzdělávání

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Pedagogická fakulta

Univerzita Palackého v Olomouci

Tato publikace je výstupem projektu Kompetence leadera úspěšné školy, reg. č. CZ.02.3.68/0.0/0.0/16_032/0008145

Jméno řešitele: Ing. Alena Opletalová, Ph.D.

Název díla: Práce s daty na internetu
Autor: PhDr. Jan Lavrinčík, Ph.D. a řešitelský kolektiv projektu Centra celoživotního vzdělávání Pedagogické fakulty Univerzity Palackého v Olomouci.

URL autora: www.ccv.upol.cz
URL odkaz na původní dílo: www.klus.upol.cz

PRÁCE S DATY NA INTERNETU

OBSAH

CÍLE DISTANČNÍHO TEXTU

- Definovat pojem data.
- Popsat postupy práce s daty na internetu.
- Na příkladech uvést práci se zdrojovými daty na internetu.
- Definovat způsoby ochrany a zabezpečení při práci s daty na internetu.
- Na příkladech uvést práci s daty a zabezpečením při platbách na internetu.
- Definovat způsoby ochrany a zabezpečení při práci s platbami na internetu.

1 DATA NA INTERNETU

1.1 Definice pojmu data

Pokud se máme začít bavit o pojmu data, pokusíme se jej nejprve definovat. V obecném významu jsou data údaje, které se používají pro popis nějakého jevu nebo vlastnosti pozorovaného objektu. V běžné praxi se nejběžněji data získávají zápisem, měřením nebo pozorováním. (Pokorný, 2009)

Data můžeme dělit na:

- **Tvrdá data –** jsou jednoznačně vymezená, většinou číselného charakteru a mají minimální chybovost.
- **Měkká data –** jsou data zejména sociologických šetření, například obliba vlády (postoje lidí k nějaké osobě, věci nebo situaci).

V oblasti informačních a komunikačních technologií mají data samozřejmě mírně odlišný význam. V informatice jsou pod tímto termínem chápány údaje zaznamenané v digitální podobě a dále určené k dalšímu zpracování. Data mohou mít podobu souborů (dokumentů, prezentací, tabulek, textu, obrázku, zvuku, videa apod.).

S daty v počítači můžeme dále pracovat různými způsoby. Pojďme se podívat na základní způsoby práce s daty (Pokorný, 2009):

1. **Konverze dat** – jedná se o převod dat mezi různými formáty. Například obrazová data na počítači můžeme uložit do nekomprimovaného formátu BMP nebo využít formát JPG se ztrátovou kompresí anebo formát PNG pracující s bezztrátovou kompresí.
2. **Komprese dat –** je speciální přístup práce s daty, kdy je primárním cílem zmenšení jejich objemu formou ztrátové nebo bezztrátové komprese. Bezztrátová komprese má zpravidla nižší účinnost, ale umožňuje zpětnou rekonstrukci dat bez jakýchkoliv ztrát (používá se na data obecného charakteru). Naopak ztrátová komprese se primárně využívá pro multimediální soubory a využívá nedokonalosti vjemových orgánů (zraku a sluchu). Zpětná rekonstrukce je vždy spjata s výraznými ztrátami.
3. Šifrování dat **–** se používá v informačních a komunikačních technologiích jako ochrana proti zneužití neautorizovanou osobou nebo společností.

Reprezentace dat na počítači z pohledu číselných soustav:

- **Desítková soustava –** je číselná soustava, v níž se pro zápis hodnot využívá číslic 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0. Jedná se o nejpoužívanější číselnou soustavu v běžném životě i vědě a technice.
- **Dvojková soustava –** je číselná soustava, která pro zápis hodnot využívá pouze číslic 0 a 1. Dvojková soustava se používá ve všech moderních ICT zařízeních, protože 0 a 1 dobře odpovídá stavům elektrického obvodu vypnuto a zapnuto.
- Šestnáctková soustava **–** je číselná soustava (někdy také nazývána hexadecimální), v níž se pro zápis hodnot využívají znaky 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 0, A, B, C, D, E, F. Jedná se o číselnou soustavu hojně využívanou v informačních a komunikačních technologiích. Například zápis barev v HTML kódu internetových stránek je realizován zpravidla vždy v hexadecimálním formátu.

Příklady

Příklady zápisu některých barev na internetové stránce: bílá barva #FFFFFF, červená barva #FF0000, černá barva #000000.

SHRNUTÍ

- V obecném významu jsou data údaje, které se používají pro popis nějakého jevu nebo vlastnosti pozorovaného objektu. V běžné praxi se nejběžněji data získávají zápisem, měřením nebo pozorováním.
- V informatice jsou pod tímto termínem chápány údaje zaznamenané v digitální podobě a dále určené k dalšímu zpracování. Data mohou mít podobu souborů (dokumentů, prezentací, tabulek, textu, obrázku, zvuku, videa apod.).
- S daty v počítači můžeme dále pracovat různými způsoby: konverze dat, komprese dat a šifrování dat.
- Data jsou z pohledu číselných soustav v počítači reprezentována: desítkovou soustavou, dvojkovou soustavou a šestnáctkovou soustavou.

Kontrolní otázky a úkoly

1. *Definujte pojem data v obecném smyslu.*
2. *Srovnejte definice termínu data v obecném smyslu a z pohledu informačních a komunikačních technologií.*
3. *Jak můžeme pracovat s daty na počítači?*

2 BEZPEČNOST PŘI PRÁCI S DATY NA INTERNETU

2.1 Rizikové objekty na internetu

Za rizikové objekty na internetu můžeme považovat primárně počítačové viry, červy, trojské koně a další. Některé napadají soubory v počítači, jiné emailovou poštu, další dokáží prohlížet kontakty a jedny z těch nejmodernějších dokáží odposlouchávat, jaké znaky jsou vkládány prostřednictvím klávesnice do počítače. Napadení počítače můžeme v prvotní fázi pozorovat na jeho celkovém zpomalení, zpomalení internetu, poškozením operačního systému nebo nějaké aplikace, ztrátou dat v počítači. (Kernighan, 2019)

Prevence a předcházení problematickým jevům na internetu:

- Navštěvovat pouze bezpečné internetové stránky.
- Používat antivirový program s aktualizovanou virovou databází.
- Mít zapnutý standardní firewall operačního systému.
- Používat antispamové aplikace.
- Používat aplikace na čištění a údržbu složek s dočasnými soubory z internetu.
- Pravidelně aktualizovat operační systém a webový prohlížeč.
- Neotevírat emaily s přílohami z podezřelých adres a zejména jejich přílohy.
- Neposílat nikomu přihlašovací údaje ke kreditní kartě nebo bankovnímu účtu.
- Data z cizích flashdisků, externích paměťových médií vždy nejprve prověřit antivirovým programem.
- Pravidelně si zálohovat nejdůležitější data v počítači (cloud, externí harddisk bez trvalého připojení k internetu).

2.2 Práce se zabezpečením na internetu

Při práci na internetu musíme být velice obezřetní, jakým způsobem pracujeme s daty na internetu, zejména kde a jaká data (hesla) vkládáme a jakým způsobem dbáme o zabezpečení těchto dat. (Kernighan, 2019)

Heslo
Jedná se o základní bezpečnostní prostředek pro zabezpečení dat v oblasti ICT a zejména na internetu. Zadáním validního hesla se ověřuje identita člověka/společnosti. Kvalita a síla zabezpečení je přímo úměrná náročnosti a délce zvoleného hesla.

Sady znaků:
- Velká písmena A, B, C…
- Malá písmena a, b, c…
- Čísla 0, 1, 2…
- Písmena s diakritikou á, ú, ě…
- Speciální znaky <, /, (, !...

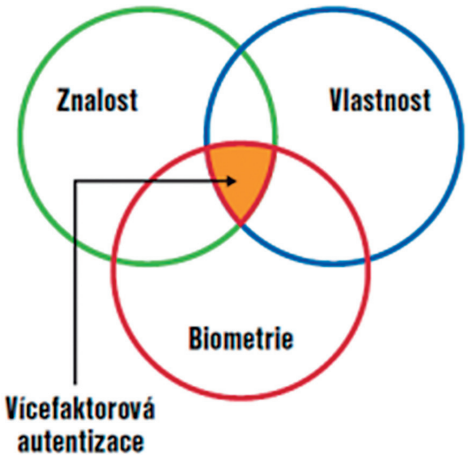
Čím více sad znaků použijeme, tím samozřejmě klesá šance na prolomení správného hesla. Dalším důležitým faktorem je i samotná délka hesla. Obecně se v dnešní době předpokládá, že silné heslo by mělo mít 8 a více znaků. Některé internetové služby už ani nedovolují heslo s méně než 8 znaky.

Ověření PINem

Jedná se specifické identifikační číslo k autentizaci člověka. Tento typ zabezpečení bývá zpravidla čtyřčíselný a primárně se využívá na kreditních, debetních kartách nebo SIM kartách. Síla ochrany není příliš velká, proto se většinou používá v kombinaci s maximálně 2 špatnými pokusy.

Vícefaktorové zabezpečení

Vícefaktorová autentizace je termín, který se objevuje v souvislosti se zabezpečeným řízením přístupu (k internetu nebo k cloudovým službám). Jedná se o poměrně širokou oblast, která proniká fyzickou i virtuální vrstvou napříč hardwarem i softwarem. S rozšířením chytrých telefonů se tento způsob ověření uživatele dostává do praktického života běžných uživatelů. (Gašparik, 2014)



Obrázek 1: Vícefaktorová autentifikace (Gašparik, 2014)

S rozvojem a nástupem cloudových služeb, možností internetových služeb spojených s financemi atp. už dnes nedostačuje zabezpečení heslem. S nástupem bankovních aplikací se nejdříve uživatelé seznámili s použitím certifikátů jako autentizačního nástroje. V korporátní sféře zase existuje povědomí o přihlašování pomocí speciálních hardwarových tokenů. Těmito netradičními způsoby identifikace uživatele a jejich vhodným použitím se zabývá vícefaktorová autentizace (MFA). (Jiroušek, 2006)

Vícefaktorová autentizace (anglicky *multifactor authentication*, zkráceně MFA) je v informatice metoda ochrany přístupu k prostředku (například webu či informačnímu systému) založená na kombinaci zabezpečení ve třech oblastech (takzvaných *„faktory“*):

1. **„Znalostní faktor“** – u této metody se jedná prakticky o cokoli, co uživatel dokáže uchovat v paměti. Typickým příkladem je heslo a PIN, ale patří sem i výběr obrázků, nakreslení gesta/znaku či osobní otázky („Jméno matky za svobodna“). (Gašparik, 2014)
2. **„Faktor vlastnictví“** – faktor zahrnuje zjednodušeně to, co lze nosit v kapse nebo peněžence. To zahrnuje například hardwarové tokeny (RSA SecurID, Yubikey), platební karty, mobilní telefony a SIM karty. (Gašparik, 2014)
3. **„Faktor biometrie“** – zabývá se charakteristikou svého nositele. Čtenáře snadno napadne otisk prstu (Touch ID), další možností je například sken očnice nebo rozpoznávání obličeje (například Face ID). (Gašparik, 2014)

Hardwarové (HW) tokeny

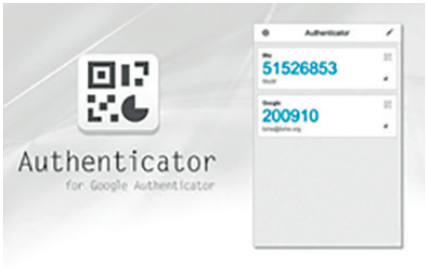
V korporátní a soukromé sféře jsou hardwarové tokeny převládajícím způsobem realizace autentizačních tokenů. Klasickým představitelem je v dnešní době kryptoměn hardwarová peněženka na kryptoměnu Trezor.

Obrázek 2: Hardwarová autentifikace, nástroj Trezor (Lavrinčík, 2018)

Softwarové (SW) tokeny

Levným trendem, řešícím některé nevýhody svých hardwarových protějšků, jsou softwarové autentifikace.

Jedná se typicky o aplikaci na chytrém telefonu (OS Android, iPhone, Windows Phone aj.). Použití je shodné. Software v telefonu se spáruje s autentizačním serverem a od té doby generuje klíče, kterým autentizační protějšek rozumí.



Obrázek 3: Softwarová autentifikace (Lavrinčík, 2018)

Ověření SMS zprávou

Jedním z dalších prvků, jak zvýšit bezpečnost přístupu k citlivým datům nebo bankovním účtům, je využít ověření SMS zprávou. Způsob zahrnuje použití většinou zadání uživatelského jména a hesla. V druhém kroku je transakce označena identifikačním číslem a přímo k ní je generovaný kód složený z různých znaků; aby se zvýšila bezpečnost, mívá zpravidla kód velmi časově omezenou platnost (například 10 minut a méně).

Zabezpečení hardwarovým klíčem

V informačních a komunikačních technologiích se jedná o samostatné zařízení (obvod) připojované externě k počítači pomocí USB, USB-C nebo jiného komunikačního portu k počítači. Hardwarový klíč přidává počítači buď novou funkci, nebo odblokuje zablokovanou funkci. Často je tato funkce využívána na ověření platnosti licencí u speciálních aplikací. Některé bankovní nebo finanční instituce u vyšších účtů nabízejí tento způsob k autorizaci klienta k internetovému bankovnictví nebo investičnímu portálu.

Obrázek 4: Hardwarový klíč (Gašparik, 2014)

Příklady

Běžným příkladem použití vícefaktorového zabezpečení je přihlášení k internetovému bankovnictví nebo použití kreditní karty k platbě na internetu.

SHRNUTÍ

- Za rizikové objekty na internetu můžeme považovat primárně počítačové viry, červy, trojské koně a další. Některé napadají soubory v počítači, některé emailovou poštu, některé dokáží prohlížet kontakty a jedny z těch nejmodernějších dokáží odposlouchávat, jaké znaky jsou vkládány prostřednictvím klávesnice do počítače.
- Při práci na internetu musíme být velice obezřetní, jakým způsobem pracujeme s daty na internetu, zejména kde a jaká data (hesla) vkládáme a jakým způsobem dbáme na zabezpečení těchto dat.
- Vícefaktorová autentizace je termín, který se objevuje v souvislosti se zabezpečeným řízením přístupu (k internetu nebo k cloudovým službám). Jedná se o poměrně širokou oblast, která proniká fyzickou i virtuální vrstvou napříč hardwarem i softwarem.

Kontrolní otázky a úkoly

1. *Pokuste se definovat způsoby zabezpečení a ochrany dat v rámci sítě internet.*
2. *Vyjmenujte příklady internetových služeb nebo serverů, kde se dá využít vícefaktorová autentifikace.*
3. *Vyjmenujte příklady internetových služeb nebo serverů, kde se dá využít zabezpečení s ověřením SMS zprávou.*

3 PRÁCE SE ZABEZPEČENÍM A DATY NA INTERNETU

3.1 Kryptoměny

Díky sílící popularitě plateb na internetu a zejména výměn ať už malých, nebo velkých částek na velkou vzdálenost se nedoporučuje používat kreditní kartu. Od devadesátých let vznikla řada projektů virtuálních a digitálních měn, které by z důvodu většího zabezpečení a anonymity mohly českou korunu zastoupit (příklad: Fazole, PayPal atp.).

Prvním projektem, který měl cestu těžkou a trnitou, ale stal se celosvětovým fenoménem zejména při internetových platbách, je kryptoměna Bitcoin. (Bitcoin Firsts – Bitcoin Wiki)

V současné době se můžeme v odborné literatuře nebo při platebním styku setkat s pojmem kryptoměna (zákon č. 284/2009 Sb., o platebním styku). Označení kryptoměna vyjadřuje, že měna využívá poznatky 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 1000 kryptoměn, z nichž nejznámější, nejpoužívanější a nejstarší je Bitcoin – více informací na www.coinmarketcap.com. Mezi další obchodovatelné kryptoměny patří Litecoin, Dogecoin, Dash, Quark, Ethereum a další. Rozdíl mezi klasickou měnou Fiat a kryptoměnou Bitcoin bychom mohli shrnout do přehledné tabulky níže. Za nejvýznamnější inovaci můžeme považovat to, že každá peněženka je pseudoanonymní (není dohledatelný majitel, pouze jednotlivé transakce), můžeme ji darovat, nelze ji zdanit a dohledat jejího majitele.

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.

Tabulka 1: Rozdíl mezi klasickou měnou FIAT a kryptoměnou (Lavrinčík, 2018)

Vznik Bitcoinu se datuje do roku 2008, kdy Satoshi Nakamoto publikoval dokument popisující protokol Bitcoin. 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, 15. prosince 2017 Bitcoin dosahuje historicky nejvyšší hodnoty 19 970 USD za 1 BTC. (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. Při práci s Bitcoinem se používá zkratka BTC. Vzhledem k současnému kurzu 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 pouze 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. (Bter.com: BitCoin and Crypto-currency Exchange Platform)

Obrázek 5: Historický vývoj ceny Bitcoinu (Bter.com: BitCoin and Crypto-currency Exchange Platform)

Jelikož se jedná o nehmatatelnou měnu, k uchovávání Bitcoinu se 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 má svoje jedinečné číslo v síti, může například vypadat následovně: 14ECFC5r6DYsfW-3Gqo4GucLxDFcHeGdsdb. (Jak začít s Bitcoiny na btctipcz)

Pro dosažení 100% bezpečnosti při práci s kryptoměnou je nutnou pečlivě hlídat tzv. privátní klíče. Kryptoměny jsou v současné době ideálním nástrojem pro bezpečné pseudoanonymní nebo zcela anonymní platby. (Bitcoin: A Peer-to--Peer Electronic Cash System)

Když se chystáme vytvořit transakci mezi dvěma peněženkami, potřebujeme bitcoinovou adresu, což je veřejná 160bitová hash generovaná pomocí protokolu digitálního podpisu s využitím eliptických křivek ECDSA (Bitcoin P2P e cash paper). 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. ("from:'Satoshi Nakamoto'")

Příklady

Jako příklad uvádíme společnosti v Olomouci, které akceptují platby Bitcoinem: Gappa Solutions s.r.o., ONYX engineering, Bitcoinmat (Vault 42), ATM btc (Šantovka), Okrasná školka Droždín, Brondo restaurant pizzeri, Salva Quardia, Ftipny Tricko, Vlasové studio Petra Now, EREC future s.r.o., Masáže Radomír Navrátil.

SHRNUTÍ

- Označení kryptoměna vyjadřuje, že měna využívá poznatky 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).
- Při práci s Bitcoinem se používá zkratka BTC. Vzhledem k současnému kurzu je Bitcoin dělen na menší jednotku Satoshi (dle jména zakladatele).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 prostřednictvím mobilní aplikace mít Bitcoiny okamžitě připravené k platbě, ale nehodí se na držení větších obnosů z důvodu bezpečnosti.

Kontrolní otázky a úkoly

1. *Pokuste se definovat pojem kryptoměna.*
2. *Vyjmenujte příklady kamenných obchodů nebo internetových e-shopů, kde akceptují platby kryptoměnou.*
3. *Jmenujte výhody využívání kryptoměn na internetu.*

POUŽITÁ LITERATURA

JIROUŠEK, Radim, 2006. *Principy digitální komunikace*. Voznice: Leda, ISBN 80-7335-084-X.

KERNIGHAN, Brian W, 2019. *Jak porozumět digitálnímu světu: vše, co potřebujete vědět o internetu, bezpečnosti a soukromí*. Přeložil Petr HOLČÁK. Praha: Argo, Zip (Argo: Dokořán). ISBN 978-80-7363-903-7.

LAVRINČÍK, Jan, 2018. *Podnikání na internetu.* 1. vyd. Olomouc: Moravská vysoká škola, o.p.s., 105 s. ISBN nemá.

POKORNÝ, Miroslav a Jan LAVRINČÍK, 2009. *Teorie systémů I*. Olomouc: Moravská vysoká škola Olomouc, ISBN 978-80-87240-09-0.

SCHLOSSBERGER, Otakar, 2012. *Platební služby.* Praha: Management Press, ISBN 978-80-7261-238-3.

Elektronické zdroje

Bitcoin History: The Complete History of Bitcoin [Timeline], 2015 [Online]. History of Bitcoin. [2015-11-09]. Dostupné z www: http://historyofbitcoin.org/

from:'Satoshi Nakamoto, 2015 [on-line]. Mail-archive. [2019-10-10]. Dostupné z www: http://www.mail-archive.com/search?l=cryptography@metzdowd.com&q=from:%22Satoshi+Nakamoto%22

"Zákon č. 284/2009 Sb., o platebním styku, 2009 [Online]. Portál.gov. [2019-10-10]. Dostupné z www: https://portal.gov.cz/app/zakony/download?idBiblio=69225&nr=284~2F2009~20Sb.&ft=pdf.

Bitcoin Firsts - Bitcoin Wiki, 2015 [on-line]. Wiki.it. [2019-10-10].]. Dostupné z www: https://en.bitcoin.it/wiki/Bitcoin_Firsts

Bitcoin P2P e cash paper, 2015 [on-line]. Gmane.org. [2019-10-10].]. Dostupné z www: http://article.gmane.org/gmane.comp.encryption.general/12588/

Bitcoin: A Peer-to-Peer Electronic Cash Systém, 2015 [on-line]. Bitcoin.org. [2019-10-10].]. Dostupné z www: https://bitcoin.org/en/bitcoin-paper/

Bter.com: BitCoin and Crypto-currency Exchange Platform, 2013 [on-line]. Bter.com. [2019-10-10]. Dostupné z www: http://www.bter.com/

GAŠPARIK, Petr. *Vícefaktorová Autentifikace,* 2014 [on-line]. Btctip.cz. [2019-10-10]. Dostupné z www: http://btctip.cz/jak-zacit-s-bitcoiny-2/

Jak začít s Bitcoiny na btctipcz [Timeline], 2015 [on-line]. Btctip.cz. [2019-10-10].]. Dostupné z www: http://btctip.cz/jak-zacit-s-bitcoiny-2/

Senate Committee Listens to Bitcoin Experts, Expresses Open-Mindedness, On Bitcoin, 2013 [on-line]. Onbitcoin.com. [2019-10-10].]. Dostupné z www: http://onbitcoin.com/2013/11/18/senate-committee-listens-bitcoin-experts-expresses-open-mindedness/

PdF UP v Olomouci, Žižkovo nám. 5, 771 40 Olomouc

CENTRUM
CELOŽIVOTNÍHO
VZDĚLÁVÁNÍ

Centrum celoživotního vzdělávání

www.ccv.upol.cz