PRAKTICKÁ PŘÍRUČKA VLASTNÍKA KRYPTOMĚN

HODL ZA ŽIVOTA I PO NĚM

Pavel Urbaczka | Tomáš Elbert

2019 | verze 1.0

Proč

ČEHO CHCEME DOSÁHNOUT

Nemá smysl zde vysvětlovat, jaký potenciál kryptoměny mají a jak mohou změnit svět. Pokud čtete tyto řádky, pravděpodobně již kryptoměny vlastníte a věříte, že jste součástí technologické a finanční revoluce.

Alfou i omegou kryptoměn je, že je můžete mít plně pod kontrolou. Držíte-li privátní klíče k vaší kryptoměně, nepotřebujete souhlas jakékoliv třetí osoby k jejímu převodu a nikdo vám ji bez vaší součinnosti nevezme. Svoboda a nezávislost jsou však pouze jednou stranou mince. Její stinnou stranou je odpovědnost za vlastní chyby, která s sebou často nese kruté a nevratné následky.

Mnoho z nás při správě vlastních kryptoměn nedodržuje základní bezpečnostní doporučení, chybuje při vytváření záloh nebo vynalézá pasti na útočníky, do kterých se pak sami chytí. Stejně tak máme tendenci nepřemýšlet nad tím, co bude, až sami nebudeme, a jestli se někdo k našim kryptoměnám dostane, pokud by se nám něco stalo. Z novin se pak dozvídáme kuriózní příběhy o prohledávání skládek, kde se na vyhozených harddiscích povalují miliony dolarů v bitcoinech, o terapii hypnózou, která má vyvolat zapomenutý PIN či o likvidaci kryptoměnových záloh manželkou při úklidu.

Tento e-book je určen těm z vás, kteří jste v oblasti kryptoměn noví a chcete k nim přistupovat obezřetně. Stejně tak je určen vám, kteří už se v oblasti pohybujete delší dobu, ale zatím jste rizika nakládání s kryptoměnami příliš neřešili anebo jen hledáte inspiraci pro vylepšení vašeho systému uložení a záloh. Ostatně ruku na srdce, kdo s ohledem na mládí těchto technologií není v oboru nováčkem. E-book je nadto určen všem, kterým není lhostejné, co se stane s jejich kryptobohatstvím po smrti.

O čem

CO SE DOZVÍTE

E-book začíná kapitolou „*Tipy a triky*“ obsahující doporučení, jak s kryptoměnami nakládat. Jednotlivá doporučení jsou rozdělena do různých kategorií, a to od obecných až po ty, které se dotýkají specifických technologií. Mnoho z doporučení se netýká pouze kryptoměn, ale obecně bezpečného pohybu v online prostředí. Účelem první kapitoly je poskytnout přehled o specifikách vlastnictví kryptoměn, možných rizicích a souvisejících řešeních. Některá z doporučení jsou zároveň pro ilustraci doplněna odkazy na reálné příběhy těch méně šťastných, kteří se doporučeními neřídili.

Praktickou aplikaci uvedených doporučení si pak představíme v další kapitole „*Jak na to*“. V této části se dozvíte, jak krok za krokem postupovat při tvorbě vlastního systému úschovy a zálohování kryptoměn, tak aby vyhovoval vašim individuálním potřebám.

Třetí částí e-booku je kapitola „*Pro případ smrti*“. Dozvíte se, co se s kryptoměnami stane v případě vaší smrti a jaké kroky ještě za života podniknout, aby s vašimi kryptoměnami bylo naloženo tak, jak si přejete.

Pro zjednodušení v příručce pracujeme s pojmem kryptoměn. Těmito máme nicméně na mysli veškerá kryptoaktiva v širším slova smyslu, tedy nejen virtuální měny, ale rovněž nejrůznější typy digitálních tokenů.

Obsah

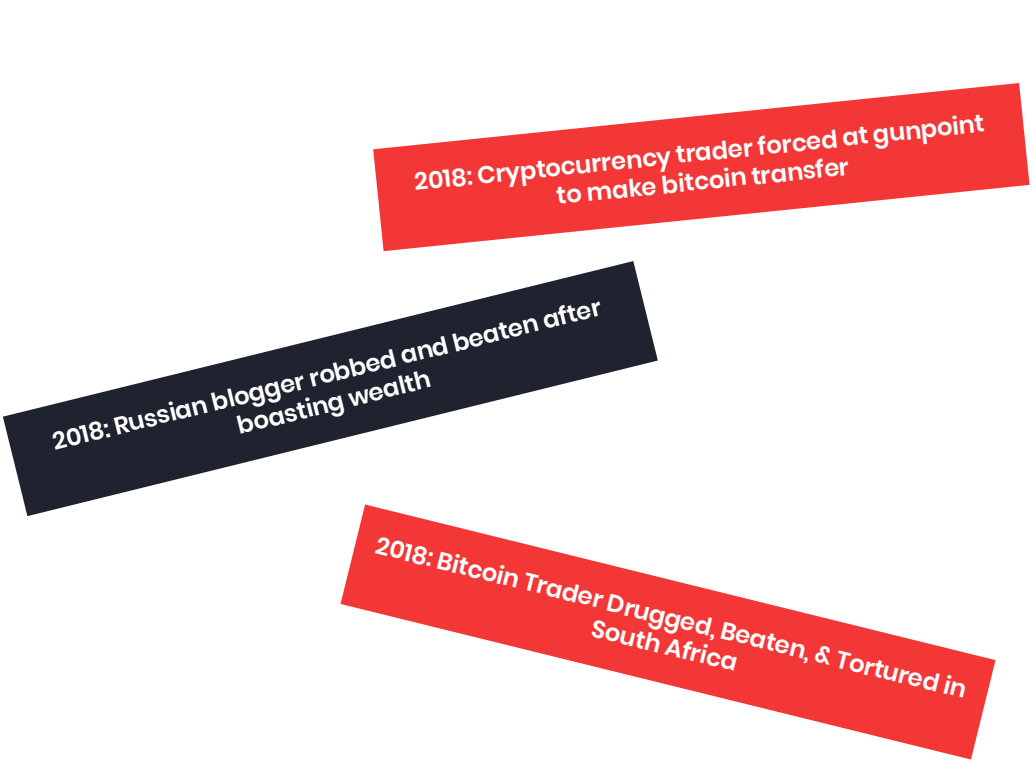
Blockchain Legal

TIPY A TRIKY

1. Obecná doporučení

JAK SE POHYBOVAT V PROSTŘEDÍ INTERNETU

Velká část z následujících doporučení se netýká pouze kryptoměn, ale obecně pohybu v prostředí na internetu. Přestože se vám mohou jevit jako samozřejmé, je dobré si je připomenout. Pro práci s kryptoměnami jsou totiž níže uvedená doporučení úplným základem, bez kterého rozumné úrovně bezpečnosti nikdy nedosáhnete.



obecně

NECHVÁSTEJTE SE

Na veřejnosti neuvádějte, kolik a jakých kryptoměn vlastníte, ani jak moc jste na nich vydělali (či prodělali). Zejména nic takového nepište na sociální sítě.

Nikdy nevíte, jak s takovou informací naloží ostatní. V lepším případě se vystavujete riziku závisti a v horším, že se stanete obětí trestného činu (loupež, vydírání, únos apod.).

CITLIVÉ INFORMACE NEUKLÁDEJTE ONLINE

Chcete-li, aby se k daným informacím nedostaly nežádoucí osoby, nikdy tyto informace neukládejte v online prostředí. Online prostředím je přitom každé prostředí, v rámci kterého dochází k připojení k internetu (služby jako je váš e-mailový účet, úložiště typu dropbox, ale i harddisk počítače připojeného k internetu).

Neexistuje 100% zabezpečení, které by v prostředí internetu zabránilo útoku třetí strany a získání informací. Není-li proto nezbytně nutné uchovávat informace online, je takový postup zbytečným zvýšením rizika hackerského útoku. Obyčejný papír je v řadě případů stále bezpečnější řešení!

POUŽÍVEJTE SPRÁVCE HESEL

Pro registrace ke všem online službám používejte nová a dostatečně silná hesla, která si ukládejte do některého z manažerů hesel.

Opakování stejných hesel nebo používání jednoduchých hesel, která se nám skvěle pamatují, je častým důvodem nabourání bezpečnosti a odcizení kryptoměn (typicky z účtů na kryptoměnových burzách). Vzhledem k tomu, že nikdo z nás si nedokáže zapamatovat velké množství silných hesel, je vhodné používat tzv. správce hesel, jako jsou např. Trezor password manager, LastPass, Keeper, 1Password, apod. Nechcete-li spoléhat na služby poskytovatelů – třetích osob, využijte softwarových řešení, které používají šifrování a lze je uložit na vlastní počítač.

POUŽÍVEJTE 2FA

Kromě hesla zabezpečte své online účty i s pomocí 2FA, jako je Google Authenticator nebo Authy.

Two-factor authentication (2FA) je způsob jak vlastní účty a přístup k informacím dodatečně zabezpečit. Používání 2FA zásadním způsobem zvyšuje vaši bezpečnost, neboť útočník musí kromě primárního hesla překonat i druhou překážku, a sice získání krátkodobě platného sekundárního autentizačního kódu. Tento kód se periodicky generuje například pomocí jedné z uvedených aplikací ve vašem mobilním telefonu.

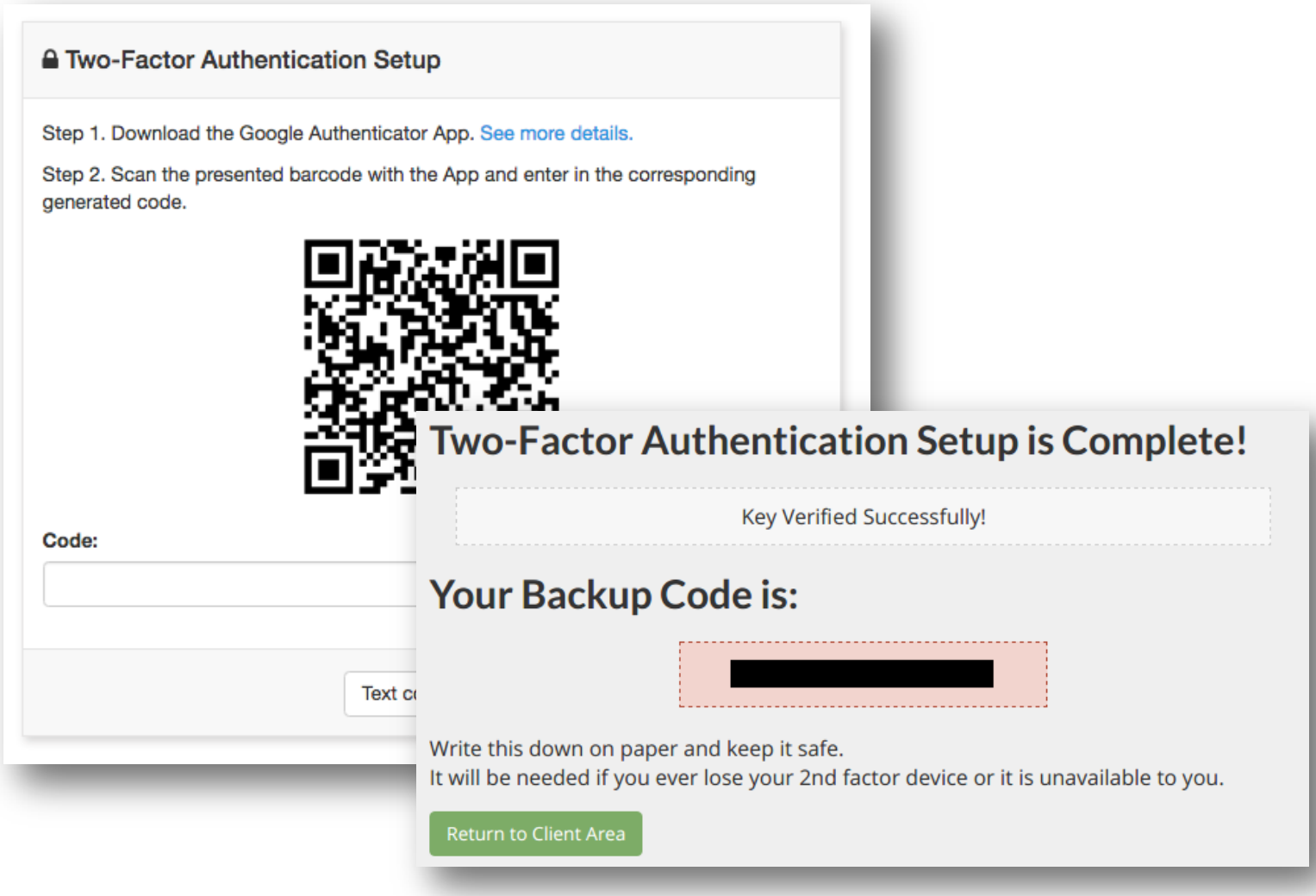
Pokud můžete, je vhodné se vyhnout využívání 2FA prostřednictvím SMS, a to s ohledem na případné možnosti krádeže identity prostřednictvím operátora.

2016: Hackers have stolen millions of dollars in Bitcoin – Using only phone numbers

UCHOVÁVEJTE ZÁLOHY 2FA

Při nastavení 2FA je vhodné si offline uchovat zálohy pro případ obnovení (např. vytištěním QR kódu nebo opisem textové podoby zálohy).

Nastavením 2FA obvykle svážete získání autentifikačního kódu s vaším konkrétním zařízením (telefonem). V případě, že telefon ztratíte nebo dojde k jeho zničení, není možné kód získat jiným způsobem než prostřednictvím zálohy. Nemáte-li ji, je nutná zpravidla poměrně složitá a zdlouhavá komunikace s provozovatelem předmětné služby, který by měl řádně ověřit, že o obnovení přístupu žádá skutečně vaše osoba (a nikoliv případný útočník).



UVĚDOMTE SI, ŽE TRANSAKCE NELZE VRÁTIT

Buďte obezřetnější než při obvyklých finančních transakcích. Dávejte pozor, komu a co odesíláte. Používáte-li danou službu poprvé, věnujte alespoň několik minut hledání informací o službě a zkušeností jiných zákazníků dostupných na internetu.

Odhaduje se, že 2,7 až 3,8 mil. bitcoinů je nevratně ztraceno. Jakmile provedete kryptoměnovou transakci na cizí adresu, nevratně ztrácíte kontrolu nad danými prostředky. Neexistuje žádná třetí osoba, která by vám v případě problémů pomohla transakci zvrátit. Vyplatí se tedy vždy pořádně zvážit komu, kam a proč kryptoměnu odesíláte. U kryptoměn jednoznačně platí dvakrát měř a jednou řež!

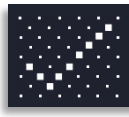
2. Peněženky a způsoby uložení

JAK UCHOVÁVAT KRYPTOMĚNY

Následující doporučení se týkají nakládání s vašimi kryptoměnami, tj. výběru a používání tzv. kryptoměnových peněženek.

Kryptoměnové peněženky spravují údaje, které jsou nezbytné pro zajištění přístupu ke kryptoměnám a jejich převodům. Jedná se zejména o tzv. soukromé a veřejné klíče.

Peněženky



ZVOLTE VHODNOU PENĚŽENKU

Různé typy peněženek s sebou nesou odlišné klady a zápory. Je vhodné zvolit takovou peněženku, která vyhovuje vašim konkrétním potřebám a způsobu využití.

Hardwarová, softwarová i papírová peněženka mají odlišné vlastnosti z hlediska bezpečnosti i způsobů využití. Pro rozdílné účely a objemy je proto vhodné využívat jiné typy peněženek.

Výhodou hardwarové peněženky je zejména offline správa soukromých klíčů v zařízení. Na rozdíl od počítače či mobilního telefonu je zařízení od počátku navrženo tak, aby vaše soukromé klíče chránilo nejen před hackerským útokem, ale i fyzickou ztrátou. Hardwarové peněženky jsou pro běžného uživatele jednoznačně nejbezpečnějším řešením. Současně sofistikované hardwarové peněženky nabízí celou řadu funkcí, od těch pro začínající uživatele po ty pokročilejší.

Softwarové peněženky lze rozdělit na mobilní a desktopové. Oba druhy jsou s ohledem na uchování privátních klíčů v online prostředí nevhodné pro uložení větších částek. Mobilní peněženky se skvěle hodí pro méně hodnotné platby, jako např. za kávu v Paralelní Polis. Lze je vnímat jako obdobu vaší skutečné peněženky. Nenosíte v ní své úspory na penzi, ale máte v ní vždy hotovost na malý nákup a nějaký ten drink. Desktopové peněženky na počítačích připojených k internetu jsou na tom podobně jako mobilní. Desktopová peněženka pro vás nicméně může být atraktivní, pokud se chcete ve větším detailu seznámit s technickým fungováním zvolené kryptoměny. Řada desktopových peněženek vám umožní stáhnout si do počítače celý blockchain (full node) nebo si na vlastní riziko hrát v příkazovém řádku.

Papírové peněženky mohou mít mnoho využití a zároveň i vysoký bezpečnostní standard. Pro většinu lidí je však složité dosáhnout jejich bezpečnostního potenciálu, a proto jsou vhodné způsoby použití poměrně omezené (blíže viz na str. 18).

POUŽÍVEJTE OVĚŘENÁ A SVOBODNÁ ŘEŠENÍ

Pro spolehlivou úschovu kryptoměn používejte vždy řešení, která jsou již náležitě otestovaná a svobodná (např. peněženky, které jsou na trhu delší dobu).

Nové produkty a společnosti mohou slibovat vylepšené funkcionality a pohodlnější řešení. Volba vhodné peněženky je však především otázkou bezpečnosti a „*časový*" test je často tím hlavním vypovídajícím faktorem.

Svobodný software obvykle umožňuje uživatelům používat program pro jakýkoli účel, dále jej distribuovat a také studovat a měnit software díky otevřenému zdrojovému kódu. Právě přístup ke zdrojovému kódu (prvek „*open-source*" dává ostatním programátorům možnost nezávisle ověřit, co program skutečně provádí, najít možné nedostatky v jeho kódu a případně vydat vlastní vylepšené verze.

PENĚŽENKY POŘIZUJTE OD DŮVĚRYHODNÉHO ZDROJE

Jelikož peněženka spravuje vaše kryptoměny, musíte věřit tomu, kdo vám peněženku, ať již softwarovou či hardwarovou poskytl. Útočník může peněženku sám upravit (hacknout) nebo vám rovnou poskytnout zcela falešnou peněženku, a to především za účelem krádeže vašich kryptoměn.

Hardwarové peněženky jsou zpravidla zabaleny v zapečetěném obalu, aby bylo možné ověřit jejich autenticitu, tj. že pochází přímo od výrobce a nebylo s nimi před jejich dodáním manipulováno. Současně je vhodné tyto peněženky pořizovat přímo přes e-shop výrobce, případně přes jiného vysoce důvěryhodného dodavatele. Pořízení hardwarové peněženky z druhé ruky za účelem bezpečného uchování kryptoměn není vhodné. Softwarové peněženky je obdobně nutné stahovat z důvěryhodných zdrojů. Podobně můžete přijít o své kryptoměny při generování papírové peněženky pomocí falešného či pozměněného programu.

2017: Bitcoin gold wallet scam sees fraudsters steal $3.2 million

2018: Man's life savings stolen from hardware wallet supplied by a reseller

BUĎTE OPATRNÍ PŘI VYUŽÍVÁNÍ PROSTŘEDNÍKŮ

Uložení kryptoměn u prostředníka (např. kryptoměnové burzy) s sebou nese výhody i nevýhody. Vydáte-li se touto cestou, dobře zvažte možné důsledky a zejména jakou část svého portfolia chcete tímto zásadním způsobem vystavit riziku.

S vlastní kontrolou nad kryptoměnami se pojí řada rizik. Není proto nic překvapivého, že řada lidí své kryptoměny ukládá u třetích osob, jako jsou kryptoměnové burzy. V takovém případě se však prakticky zcela spoléháte na poctivost a zejména solventnost takového správce. Případů vykradených kryptoměnových burz, ať již člověkem zevnitř nebo zvenčí, je nespočet. Nadto se mohou burzy ocitnout v problémech a insolvenci i z celé řady jiných důvodů. Rovněž pokud máte strach z všudypřítomného pronásledování ze strany NSA, CIA, FBI nebo jen českých exekutorů, dlouhodobě uložit své kryptoměny na burze, kde se v dnešní době zpravidla musíte vcelku důsledně identifikovat, není nejmoudřejší.

Jak říká jeden z nejpřesvědčivějších obhájců Bitcoinu, Andreas Antonopoulos: „*Not your keys? Not your bitcoin.*“. Pokud se vám tato pozice zdá jako přehnaná, uvědomte si, že i z právního pohledu převodem kryptoměny na burzu obvykle přestáváte být vlastníkem konkrétní kryptoměny a vzniká vám pouhá pohledávka za burzou na vydání odpovídající hodnoty. Pokud nadto připustíme, že původním záměrem Bitcoinu bylo vytvořit peer-to-peer platební systém, který lze využívat bez nutnosti prostředníka, pak nechávat jakoukoliv podstatnější kryptočástku na burze je do jisté míry popřením samotného smyslu existence kryptoměn.

POUŽÍVEJTE DOSTATEČNĚ BEZPEČNÝ PIN

Umožňuje-li peněženka nastavení PINu, využijte této možnosti. Nepoužívejte přitom jednoduché PINy, jako jsou např. sekvence (1234) nebo opakovaná čísla (3333). V ideálním případě používejte alespoň šestimístný PIN s různými čísly.

Použitím jednoduchého PINu se výrazně snižuje bezpečnost v případě fyzického získání daného zařízení. Zkouší-li útočník PINy metodou „*brute-force*“, obvykle začíná těmi nejjednoduššími.

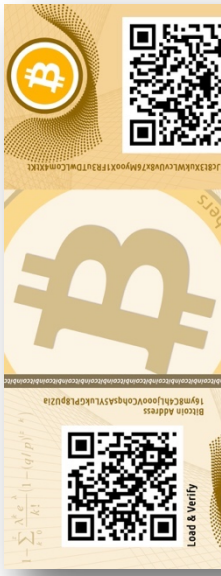
NESPOLÉHEJTE NA JEDINOU TECHNOLOGII

Nesázejte všechno na jednu kartu a nevěřte jen jedné technologii. Diverzifikujte mezi různými druhy peněženek.

Byť se může určitá peněženka jevit jako nejlepší a nejbezpečnější řešení, u každé existuje riziko zneužití, chyby apod. Chcete-li minimalizovat riziko rozsáhlé ztráty, rozdělte své prostředky mezi různé druhy a výrobce peněženek!

BUĎTE OPATRNÍ S PAPÍROVÝMI PENĚŽENKAMI

Nejste-li bezpečnostními experty s potřebnými technickými dovednostmi, vyhněte se používání papírové peněženky pro úschovu větších částek.



Papírové peněženky („*paper wallet*“) jsou historicky populárním řešením, a to nejen pro nízké náklady na jejich výrobu. Mnohdy jsou dokonce považované za „*nejbezpečnější*“ formu úschovy kryptoměny. Jejich problém je však ve splnění předpokladů pro dosažení maximální úrovně bezpečnosti, a sice zejména vytvoření privátních klíčů v bezpečném prostředí (např. důvěryhodný software, dedikovaný offline počítač, zabezpečená tiskárna atp.). Bezpečné vytvoření papírové peněženky tedy rozhodně není triviální, a proto jsou tyto peněženky u větších částek pro běžného uživatele nevhodné. Naopak se však mohou dobře hodit pro darování menších obnosů vašim blízkým.

MĚJTE HARDWARE PENĚŽENKY POD DOHLEDEM

Používáte-li hardwarové peněženky, snažte se je mít pod dohledem a bez přístupu třetích osob.

I když jsou hardwarové peněženky vytvořeny k bezpečnému držení kryptoměn a obvykle jsou chráněny PINem, nelze vyloučit, že chráněná tajemství lze ze zařízení i přesto získat, a to zejména získá-li útočník fyzický přístup k peněžence. Ostatně taková zranitelnost byla již několikrát zjištěna. Výrobci následně, je-li to možné, reagují na zranitelnost vydáním nového firmware.

2018: This team showed weak spots of Ledger and Trezor wallets

3. Zálohy peněženek

JAK PRACOVAT SE ZÁLOHAMI

V posledních letech došlo k významnému posunu z hlediska bezpečnosti správy privátních klíčů, a to především díky dostupné nabídce stále sofistikovanějších a současně uživatelsky přívětivějších hardwarových peněženek. Peněženky nejen stále umožňují nové a nové funkce, ale rovněž snižují riziko lidské chyby. I tak je u většiny hardwarových peněženek při jejich prvotním nastavení nutné vytvoři zálohu.

Vygenerovanou zálohu (anglicky tzv. recovery seed či seed phrase) tvoří obvykle 12 nebo 24 anglických slov. Tato slova jsou nesmírně důležitá. S jejich znalostí, nejsou-li současně využity další nadstandardní bezpečnostní opatření typu heslové fráze (viz dále), je možné obsah peněženky obnovit a získat tím přístup k veškerým v ní uloženým prostředkům. Nakonec tak celá bezpečnost nastaveného řešení může být závislá na způsobu uchování této zálohy. Nejen, že nechcete zálohu ztratit, ale současně k ní nesmí získat přístup žádná nepovolaná osoba. Právě proto je úschově záloh nutné věnovat náležitou pozornost.

Zálohy

ZÁLOHU ZAZNAMENÁVEJTE OFFLINE

Zálohy zaznamenávejte a ukládejte mimo prostředí internetu, zejména ne v e-mailu, dropboxu apod.

Uložíte-li zaznamenaná slova v elektronické podobě online, vystavujete se zcela zbytečnému riziku, že k nim získá přístup neoprávněná osoba (o čemž se navíc obvykle ani nedozvíte). Neopomíjejte, že online prostředí tvoří i harddisk ve vašem počítači, který využíváte byť i jen příležitostně k prohlížení internetu. Ideální způsob pro zaznamenání zálohy tak může být propiska a papír, jak popisujeme na další stránce.

DÁVEJTE POZOR PŘI VYTVÁŘENÍ ZÁLOHY

Pořizujte zálohu, jen jste-li sami a v uzavřeném prostoru bez kamer. Slova zálohy při zapisování nevyslovujte nahlas.

Uvědomte si, že stěny mají doslova uši i oči. Ve veřejném prostoru je mnoho kamer a všude kolem nás jsou zařízení zaznamenávající zvuk. Okamžik zapisování zálohy je sám o sobě bezpečností riziko, věnujte mu tedy náležitou pozornost. Okamžitě po pořízení zálohy ji uložte tak, aby k ní neměly přístup jiné osoby.

ZÁLOHU UCHOVÁVEJTE VE VHODNÉ PODOBĚ

Slova zálohy zaznamenejte na papír nebo ještě lépe na jiné materiály, které nepodléhají zkáze (typicky vyražení slov do kovových destiček).

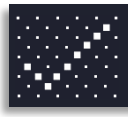
Záloha slouží především pro vás, a to pro případ, že se s peněženkou cokoliv stane (ztráta, vymazání při aktualizaci firmwaru, fyzická destrukce, odcizení apod.). V takovém případě budete rádi za to, že máte zálohu bezpečně uschovanou a v čitelné podobě. Pro zajištění použitelnosti i po delší době je vhodné používat prostředky, které není možné jednoduše smazat (např. propiska na místo obyčejné tužky). Za ideální lze považovat produkty, které chrání zálohu i před vnějšími vlivy (oheň, voda apod.), jako je např. Cryptosteel a další.

POUŽÍVEJTE BEZPEČNOSTNÍ OBÁLKY

Pro uchování záloh používejte tzv. bezpečnostní obálky, a to ideálně ty, které obsahují unikátní identifikační číslo.

Dostane-li se jiná osoba k vaší záloze, může získat přístup k předmětným kryptoměnám. Stačí přitom, aby si zálohu vyfotila, opsala nebo zapamatovala. Může se tak jednoduše stát, že při následné kontrole existence zálohy vůbec nepoznáte, že někdo s vaší zálohou v mezidobí manipuloval. Proto je vhodné využívat tzv. bezpečnostní obálky, které obvykle slouží k zasílání cenných a tajných zásilek a jsou navrženy tak, aby bylo možné vždy ověřit, zda (ne)došlo k neoprávněné manipulaci. Tyto obálky jsou neprůhledné a zalepené tak, že je nutné je při otevření nevratně porušit.

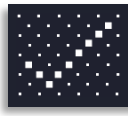
Unikátní identifikátor bezpečnostní obálky (viz např. níže na obrázku číslo 703737100) si při uložení zálohy poznamenejte. Během následné kontroly můžete jeho porovnáním ověřit, zda nedošlo k otevření a výměně obálky za jinou. Obálku je ze stejného důvodu vhodné podepsat.



PRAVIDELNĚ ZÁLOHY KONTROLUJTE

Stanovte si termíny, ve kterých zkontrolujete existenci vašich záloh a skutečnost, že s nimi v mezidobí nemanipulovala neoprávněná osoba.

Při jakkoliv bezpečném nastavení systému uložení záloh může nastat situace, kterou jste nepředvídali. Zálohu například může někdo odcizit, může dojít k jejímu poškození nebo ztrátě. Abyste snížili riziko ztráty uschovaných prostředků, je dobré jednou za čas existenci záloh zkontrolovat, tedy minimálně ověřit, že je nadále čitelná a nikdo k ní nezískal v mezidobí přístup.



ZÁLOHY UCHOVÁVEJTE NA BEZPEČNÉM MÍSTĚ

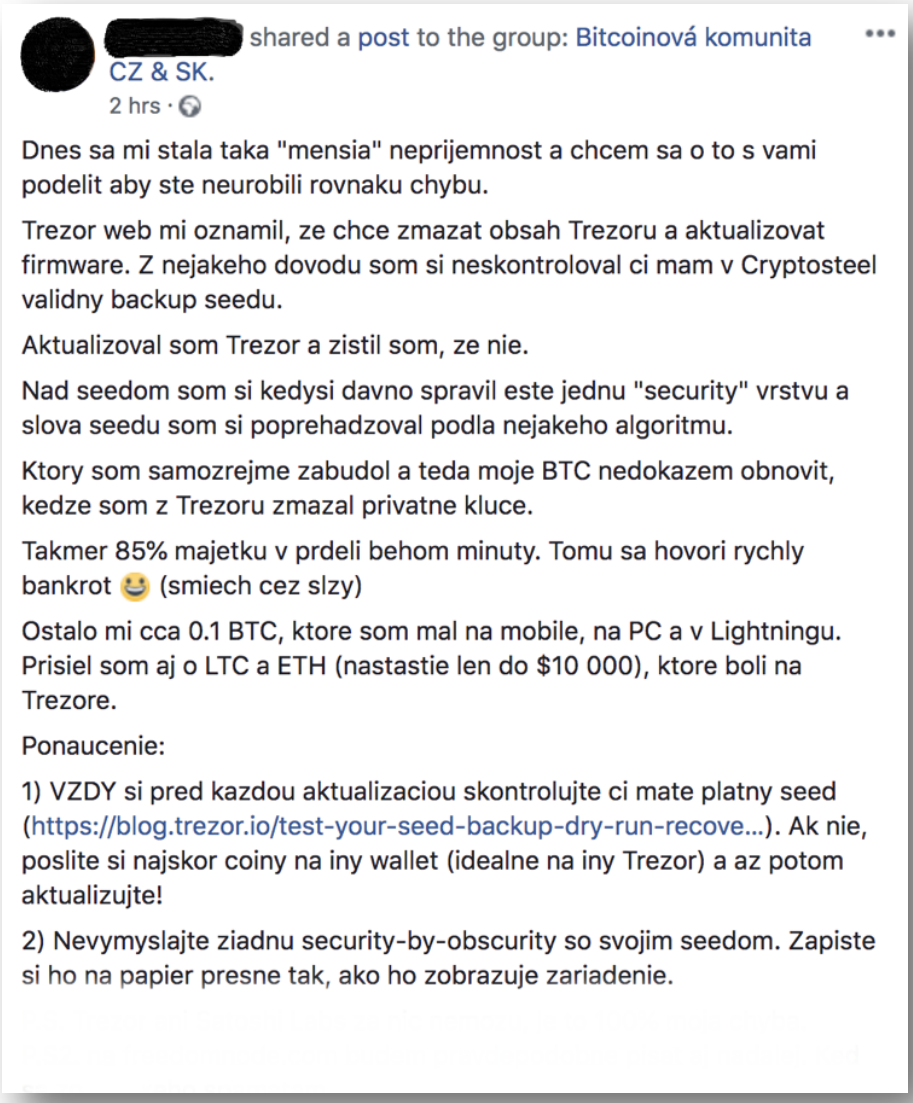
Vyberte vhodné umístění pro uložení záloh, a to takové, ke kterému existuje omezený přístup.

Mezi přijatelná umístění patří zejména trezory, uzamykatelné skříňky, bezpečnostní schránky pro uložení zbraně, depozitní schránky v bance nebo úschova u důvěryhodného notáře či advokáta.

NEVYMÝŠLEJTE VLASTNÍ BEZPEČNOSTNÍ VYLEPŠENÍ

Zůstaňte u ověřených řešení a kombinujte pouze standardní bezpečnostní opatření. Nesnažte se za pomoci vlastní invence řešení dělat složitější.

Lidová tvořivost často nezná hranic a lidé se následně chytají do vlastních pastí. Typickým případem jsou úmyslně přeházená slova zálohy, skrytí slov zálohy v souvislém textu apod. V okamžiku, kdy „*vylepšení*“ vymýšlíte, zdá se vše perfektní, samozřejmé a funkční. Až budete ale zálohu chtít vy nebo vaši pozůstalí využít, na řešení si buď nevzpomenete nebo na něj nikdo nepřijde.


[redacted] shared a post to the group: Bitcoinová komunita CZ & SK.
2 hrs ·

Dnes sa mi stala taka "mensia" neprijemnost a chcem sa o to s vami podelit aby ste neurobili rovnaku chybu.

Trezor web mi oznamil, ze chce zmazat obsah Trezoru a aktualizovat firmware. Z nejakeho dovodu som si neskontroloval ci mam v Cryptosteel validny backup seedu.

Aktualizoval som Trezor a zistil som, ze nie.

Nad seedom som si kedysi davno spravil este jednu "security" vrstvu a slova seedu som si poprehadzoval podla nejakeho algoritmu.

Ktory som samozrejme zabudol a teda moje BTC nedokazem obnovit, kedze som z Trezoru zmazal privatne kluce.

Takmer 85% majetku v prdeli behom minuty. Tomu sa hovori rychly bankrot (smiech cez slzy)

Ostalo mi cca 0.1 BTC, ktore som mal na mobile, na PC a v Lightningu. Prisiel som aj o LTC a ETH (nastastie len do $10 000), ktore boli na Trezore.

Ponaucenie:

1) VZDY si pred kazdou aktualizaciou skontrolujte ci mate platny seed (https://blog.trezor.io/test-your-seed-backup-dry-run-recove...). Ak nie, poslite si najskor coiny na iny wallet (idealne na iny Trezor) a az potom aktualizujte!

2) Nevymyslajte ziadnu security-by-obscurity so svojim seedom. Zapiste si ho na papier presne tak, ako ho zobrazuje zariadenie.

NEROZDĚLUJTE ZÁLOHU NA VÍCE ČÁSTÍ

Nedělte svou zálohu na několik částí, které následně uložíte na odlišná místa.

Mnoho lidí svou zálohu rozděluje na několik částí (např. dvě části po 6 nebo 12 slovech), které následně uloží na odlišná místa. Předpokládají, že tímto postupem zvyšují bezpečnost provedené zálohy. Rozdělení klíčů však bezpečnost ve skutečnosti snižuje. S polovinou daných slov již za použití dnes dostupných technologií totiž lze získat přístup k daným prostředkům, byť je to obtížné a časově náročné. Rozdělením zálohy tak vystavujete zálohu dvojnásobnému riziku zneužití (záloha je na dvou místech). Využijte proto jiných opatření, kterými můžete dosáhnout zamýšleného cíle. Vhodné jsou například heslové fráze nebo multisignature adresy, jak uvádíme dále.

NESPOLÉHEJTE NA JEDNO UMÍSTĚNÍ

Nenechávejte zálohy ke všem svým kryptoměnám na jednom místě nebo u jedné osoby. Využijte více lokací nebo osob.

Našli jste skvělé místo nebo osobu pro uložení svých záloh? Výborně. A teď zkuste vzít v úvahu, že se stane něco, co jste nebyli schopni předvídat a dané místo nebo osoba byly kompromitovány. V takovém případě budete rádi, že jste zálohy k části vašich kryptoměn měli uloženy jinde. To, co platí u diverzifikace peněženek, platí i u diverzifikace míst, na kterých jsou uloženy zálohy, resp. osob, u kterých jsou uloženy (a to i v případě, že se jedná o banku, notáře nebo advokáta).

4. Pokročilejší postupy

JAK DÁLE ZVÝŠIT BEZPEČNOST

Cítíte-li se technicky zdatní nebo máte s ohledem na rozsah vašeho kryptomajetku zájem na sofistikovanějších řešeních? Inspirujte se následujícími doporučeními a zvyšte tak bezpečnost vašeho základního řešení.

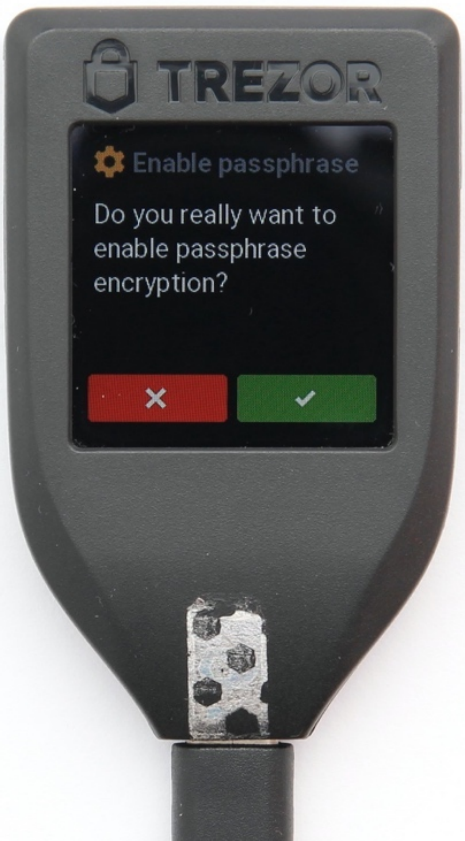
Pokročilí

POUŽÍVEJTE HESLOVÉ FRÁZE

Doplňte vaše řešení o tzv. „*passphrase*“, resp. česky „*heslovou frázi*“.

Bezpečnost peněženky lze zásadním způsobem zvýšit za použití heslové fráze. Heslová fráze hraje roli při vytvoření vašich klíčů, přičemž k obsahu peněženky se dostanete pouze při její znalosti. Znění heslové fráze si můžete nastavit sami, a to obvykle v pokročilém nastavení některých hardwarových peněženek. Pro heslovou frázi se doporučuje použít několik spolu nesouvisejících slov.

Při použití heslové fráze samotná znalost zálohy nestačí k získání přístupu k daným kryptoměnám. Používání heslové fráze vede k možnosti dodatečného zabezpečení, a to např. tak, že na jedno místo uložíte znění zálohy a na jiné místo znění heslové fráze. Získá-li útočník přístup k jedné z těchto lokací, nebude schopen předmětné kryptoměny odcizit. Na druhou stranu je nutné si uvědomit, že bez znalosti heslové fráze se ke kryptoměnám nedostanete ani vy sami. Zapomenutí nebo nesprávné nastavení fráze (záměnou znaků apod.) tak může mít fatální důsledky!



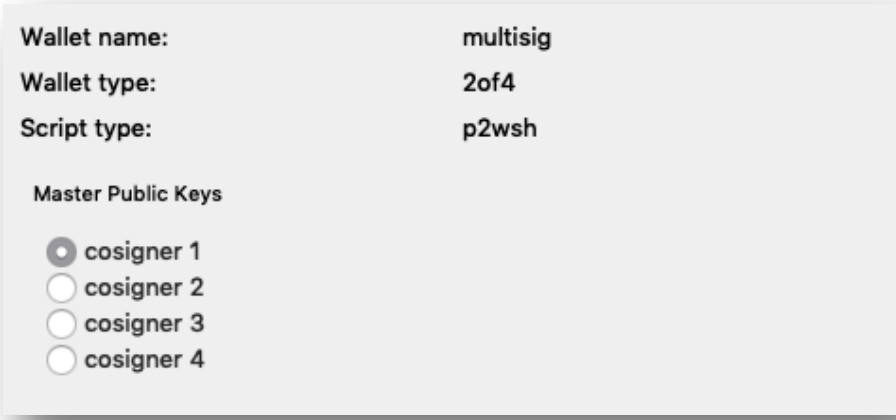
POUŽÍVEJTE MULTISIGNATURE ADRESY

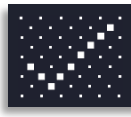
Uchovávejte kryptoměny na multisignature adresách.

Další možností, jak diverzifikovat riziko koncentrace tajemství na jedné lokaci, resp. u jedné osoby, je využití tzv. multisignature adres. Tyto adresy umožňují, aby k nakládání s prostředky bylo využito více privátních klíčů.

U multisignature adres lze nastavit, kolik podpisových oprávnění (privátních klíčů) k nim náleží a kolik z nich je nezbytných k provedení transakce. Příkladem může být nastavení multisignature peněženky, ke které existují celkem 4 podpisová oprávnění (tj. 4 samostatné peněženky se samostatnou zálohou a případně i heslovou frází), z nichž k provedení transakce je nezbytná autorizace minimálně 2 z nich. V praxi pak při provádění transakce jeden držitel podpisového oprávnění vytvoří a podepíše transakci a následně ji pošle k autorizaci ostatním oprávněným. Transakce může být přitom provedena pouze tehdy, pokud dojde k autorizaci minimálně od kterýchkoliv 2 držitelů podpisových oprávnění. Držiteli více privátních klíčů (oprávnění) přitom samozřejmě může být i stejná osoba. Využití multisignature adres umožňuje jak diverzifikaci lokací k uložení záloh, tak i diverzifikaci osob, které disponují podpisovým oprávněním.

Aktuálně bohužel neexistuje mnoho uživatelsky přívětivých řešení, která by umožnila nastavení multisignature peněženky s využitím hardware peněženek. Lze tak nicméně učinit například pomocí softwarové peněženky „*Electrum Bitcoin Wallet*“, kterou lze nalézt na webové adrese electrum.org.



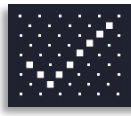


ULOŽTE ZÁLOHU NA VÍCE MÍSTECH

Nebojte se být paranoidní, a ukládejte zálohy v kopiích na více lokacích.

Osvědčené 3-2-1 pravidlo pro tvorbu záloh říká, že byste měli mít vždy alespoň tři „*kopie*“. Tyto kopie by měly být alespoň na dvou různých typech médií a alespoň jedna kopie by měla být uložena na samostatném místě (offsite). Máte-li tedy privátní klíče například v hardwarové peněžence (1. kopie), k hardwarové peněžence jste zapsali zálohu na papír (2. kopie), druhou papírovou zálohu (tj. 3. kopii) byste měli uložit na separátní lokaci.

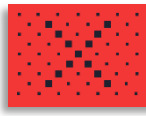
Uložení zálohy na určitou lokaci s sebou nese nepředvídatelné riziko její ztráty nebo zničení. Vytvořením a uložením kopie zálohy na jiné místo je toto riziko sníženo. Na druhou stranu je nutné si uvědomit, že se tímto zároveň zvyšuje riziko zneužití ze strany třetích osob, protože nyní máte své tajemství uloženo na dvou místech (resp. u dvou osob).



ULOŽTE HESLOVÉ FRÁZE NA JINÉ MÍSTO

Uložte znění heslové fráze na jiné místo než s ní související peněženku (ve fyzické podobě) nebo zálohu.

Bezpečnost peněženky či zálohy lze zásadním způsobem zvýšit za použití heslové fráze. Tuto vyšší bezpečnost byste však zcela nevyužili, pokud byste heslovou frázi uchovávali na stejném místě jako související peněženku či zálohu. Výhodou použití heslové fráze je právě skutečnost, že ji můžete uložit na jiném místě. Ten, kdo získá přístup k peněžence či její záloze, totiž bez znalosti heslové fráze nemůže předmětné prostředky nijak zneužít.



VYHNĚTE SE „*DEAD MAN'S SWITCH*“

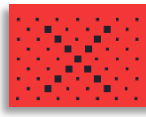
Vzhledem k současnému stavu technologií a některých problematických a nepředvídatelných důsledků je lepší se pro účely automatického převodu kryptoměn konceptu dead man's switch vyhnout.

„*Dead man's switch*“ je pojistkou pro případ smrti či např. dlouhodobého bezvědomí. V online světě tato opatření zpravidla fungují tak, že vám ve zvoleném intervalu, např. jednou za měsíc chodí e-mail s odkazem, který pokud po delší dobu neprokliknete (nenavštívíte), aktivuje automatické úkony, jako je např. odeslání předem připravené zprávy či přímo kryptoměny na zvolené adresy.

Využití automatizovaných mechanismů pro převody kryptoměn v případech, jako je smrt, jsou lákavým postupem. Bohužel však v současnosti tyto postupy s sebou nesou řadu rizik, které je obtížné nebo které vůbec nelze eliminovat. V prvé řadě může dojít ke spuštění automatizovaných procesů, aniž byste to zamýšleli (např. stále žijete, ale nemáte faktickou schopnost provést pravidelné úkony, které zajišťují, že automatizované procesy se nezahájí). Případně, využijete-li externí osoby či mechanismy jako zdroje vstupní informace, tzv. „*oracles*“, ty v klíčový okamžik mohou poskytnout nepravdivé informace.

Automatizované mechanismy pro samotný převod kryptoměn rovněž předpokládají, že vaši blízcí mají svoji adresu na všechny druhy kryptoměn, které jim chcete odkázat, umí s kryptoměnami sami nakládat a v neposlední řadě, že budou držet a mít dobře zálohované privátní klíče ke všem takto poskytnutým adresám. Nadto byste museli mechanizmus nezřídka aktualizovat s ohledem na změny ve vašem kryptoměnovém portfoliu. Využití „*dead man`s switch*“ a jeho implementace pomocí všeslibujících chytrých kontraktů (smart contracts) tedy prozatím raději dejte k ledu.

„*Dead man's switch*“ však může být naopak vhodný pro předání informací vašim pozůstalým o tom, co a jak mají dělat v případě vaší smrti, tedy pro předání návodu, tak jak jej popisujeme dále nebo informace o místě uložení návodu. Informace poskytnuté prostřednictvím „*dead man's switch*“ by nicméně neměly být vysoce citlivé a v žádném případě by neměly obsahovat vaše tajemství (zálohy, hesla, PINy atp.). Snadné řešení pro vytvoření automatického mechanizmu lze nalézt například zde https://www.deadmansswitch.net/, případně lze obdobně využít některé správce hesel.



NEPŘEŽEŇTE TO SE SLOŽITOSTÍ

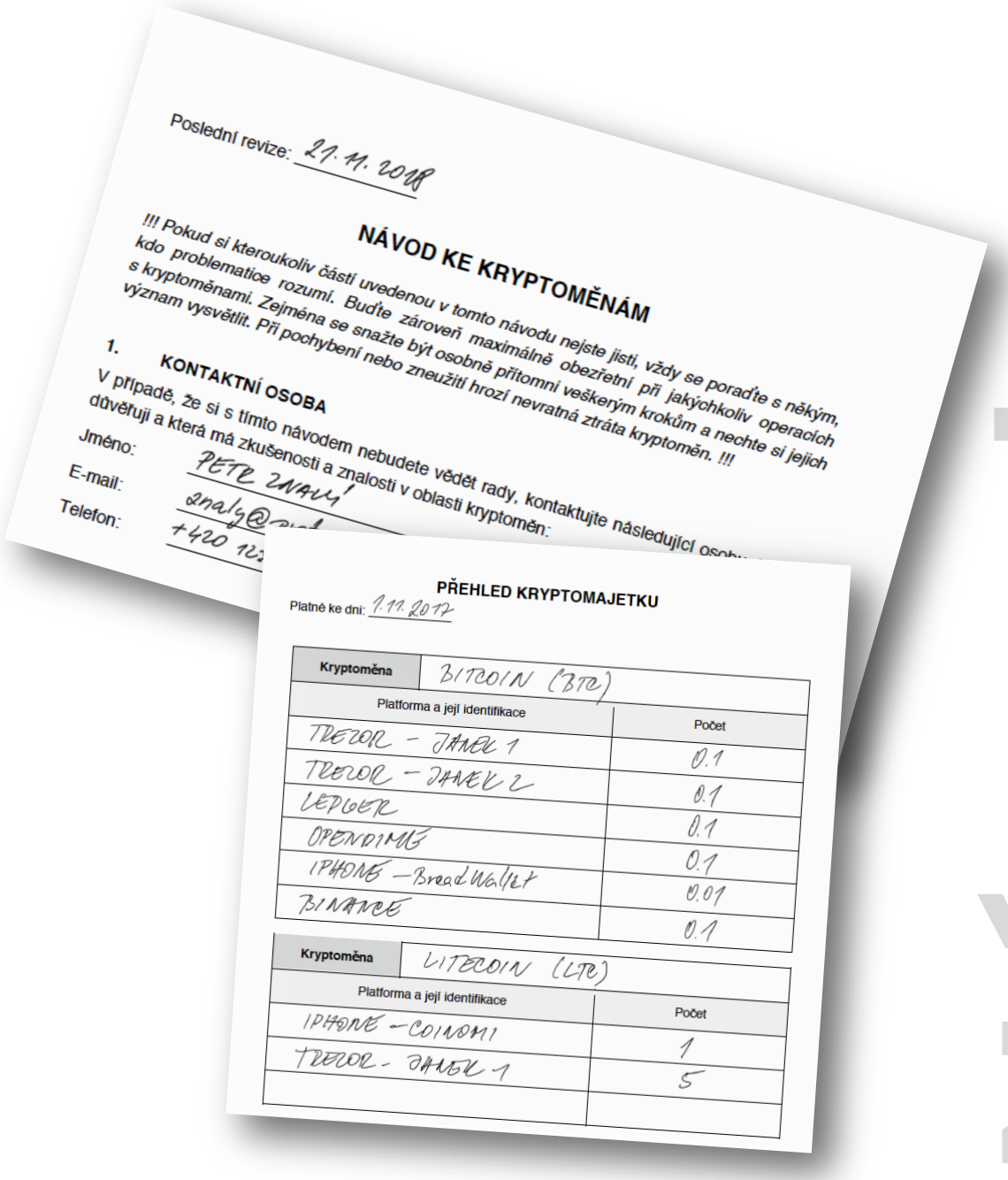
Vlastní řešení nastavte s ohledem na hodnotu uložených kryptoměn a existujících rizik. Mějte rovněž na paměti, že dokonalé zabezpečení neexistuje.

Když to s komplikovaností svého řešení přeženete, může se vám stát, že bude tak „*bezpečné*“, že se k vašim prostředkům jednou nedostanete ani vy sami. Vždy tedy zvažte, zda stojí za to přidat další prvek, který řešení dělá složitějším. Ne vždy je nejkomplikovanější řešení tím nejbezpečnějším. Obecně platí, že pro většinu lidí jsou vhodná standardní a jednoduchá řešení, u nichž je nejlepší poměr uživatelské přívětivosti a bezpečnosti nebo chcete-li řešení zvolená na základě nákladově-výnosové (cost-benefit) analýzy.

5. K návodu

PRO SEBE I PRO OSTATNÍ

Dokument, který nazýváme „*návodem*“, je důležitou součástí každého složitějšího řešení. O tom, proč byste měli návod použít, se dozvíte více v další kapitole s názvem „*Jak na to*“.



Poslední revize: 27. 11. 2018

NÁVOD KE KRYPTOMĚNÁM

!!! Pokud si kteroukoliv částí uvedenou v tomto návodu nejste jisti, vždy se poraďte s někým, kdo problematice rozumí. Buďte zároveň maximálně obezřetní při jakýchkoliv operacích s kryptoměnami. Zejména se snažte být osobně přítomni veškerým krokům a nechte si jejich význam vysvětlit. Při pochybení nebo zneužití hrozí nevratná ztráta kryptoměn. !!!

1. **KONTAKTNÍ OSOBA**

V případě, že si s tímto návodem nebudete vědět rady, kontaktujte následujícího osobu, kterou důvěřuji a která má zkušenosti a znalosti v oblasti kryptoměn:

Jméno: PETR ZNALÝ

E-mail: znaly@

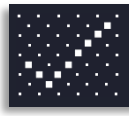
Telefon: +420

PŘEHLED KRYPTOMAJETKU

Platné ke dni: 1. 11. 2017

Kryptoměna	BITCOIN (BTC)
Platforma a její identifikace	Počet
TREZOR – JANEK 1	0.1
TREZOR – JANEK 2	0.1
LEDGER	0.1
OPENDIME	0.1
IPHONE – BreadWallet	0.01
BINANCE	0.1

Kryptoměna	LITECOIN (LTC)
Platforma a její identifikace	Počet
IPHONE – COINOMI	1
TREZOR – JANEK 1	5



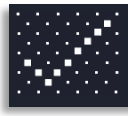
NÁVOD ULOŽTE TAM, KDE BUDE S JISTOTOU NALEZEN

Návod uložte u osoby nebo na místo, kde se v případě vaší smrti včas najde.

Návod je zcela zbytečný, pokud jej po vaší smrti nikdo nenajde. Veškeré vaše úsilí by v takovém případě bylo k ničemu. Proto k návodu nelze přistupovat stejně jako k zálohám peněženek, tedy jako k extrémně zabezpečenému tajemství!

Vhodné je uvažovat o úschově u lidí, kteří se o vaší smrti dozví jako první, tj. vašich blízkých, kamarádech apod., případně u osob, které hrají roli v rámci procesu vypořádání dědictví (např. notář). Co se týká místa, můžete návod zanechat například u sebe doma nebo u blízké osoby, kde předpokládáte, že jej vaši blízcí nepochybně objeví. Techničtější alternativou pak je pro distribuci návodu využít shora popsaný mechanismus „*dead man's switch*".

Návod zejména neschovávejte do trezoru nebo bezpečnostní schránky v bance, neboť k těmto místům se mohou vaši blízcí dostat až při vypořádání dědictví. I přestože je většina dědických řízení skončena do jednoho roku, ve světě kryptoměn se jedná o relativně dlouhou dobu. Nadto není vyloučeno, že právě vaše dědické řízení se protáhne na několik let.



POŘIZUJTE NÁVOD OFFLINE

Pro zvýšení bezpečnosti sepište návod pomocí běžných psacích prostředků, tedy nikoliv na počítači připojeném k internetu.

I u návodu platí, že chcete-li zvýšit pravděpodobnost, že se o obsahu návodu nikdo předem nedoví, vyplňujte jej offline za použití psacích prostředků.

VZDĚLÁVEJTE SVÉ BLÍZKÉ V OBLASTI KRYPTOMĚN

Pokuste se své blízké alespoň obecně seznámit s fungováním kryptoměn a jejich riziky.

Vzpomínáte si na první zásadu, „*Nechvástejte se*“. Tato zásada do jisté míry platí i ve vztahu k vašim blízkým. Nicméně zcela zatajit existenci jakéhokoliv kryptomajektu rovněž nemusí být nejlepším řešením. Vaši blízcí by měli mít minimálně tušení, že jste mohl něco zanechat a že je dobré pátrání po návodu vůbec započít. Rovněž se bude hodit, pokud si nebudou myslet, že Bitcoin, potažmo kryptoměny, jsou dobré tak leda pro drogové dealery či hackery.

Pokud máte ve vaše blízké důvěru, rovněž zvažte, zda s nimi návod krok po kroku neprojít. Může se ukázat, že některé části návodu nejsou tak nad slunce jasné, jak jste se sami domnívali a stejně tak můžete zjistit, že jste na některou podstatnou informaci v návodě zapomněli. Pro tyto účely lze rovněž zvážit použití návodu, který nebude obsahovat konkrétní klíčové informace o rozsahu kryptomajetku či o místě uložení jednotlivých tajemství.

NÁVOD NEUKLÁDEJTE NA STEJNÉM MÍSTĚ JAKO ZÁLOHY

Návod neukládejte spolu se zálohami nebo peněženkami na stejná místa, resp. u stejných osob.

Úroveň zabezpečení u záloh, peněženek a jiných tajemství (heslové fráze, master heslo k manažeru hesel apod.) je zásadně odlišná od úrovně zabezpečení uložení návodu. Návod by vaši blízcí měli být schopni najít i v případě, že netuší, o co je jedná. Oproti tomu přístup k ostatním tajemstvím má být výrazně složitější.

Uschovejte návod na více místech, resp. u více osob.

Nalezení návodu je zcela klíčové pro úspěch vašeho plánu. Doporučujeme proto návod pořídit dvakrát, ideálně třikrát. Vždy se může stát, že se zároveň s vámi stane něco i dané osobě nebo lokaci.

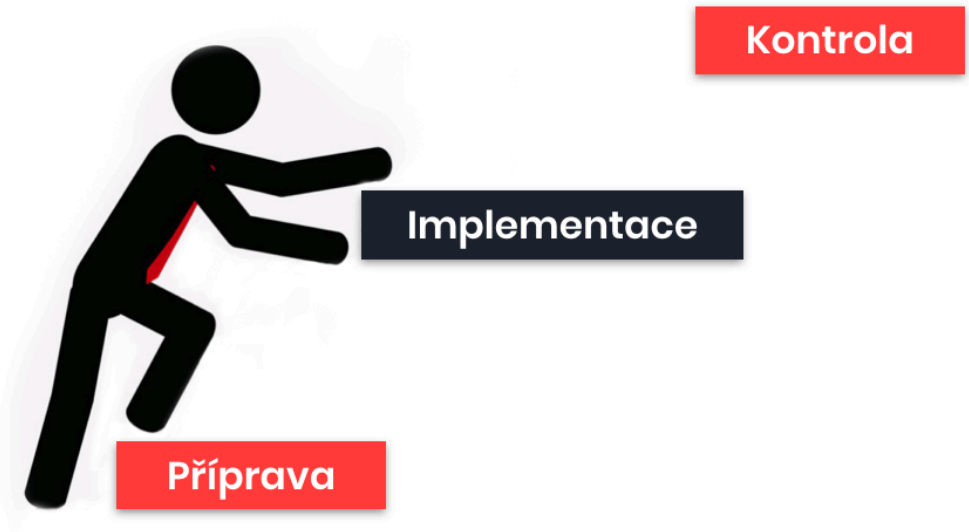
Blockchain Legal

JAK NA TO

Jak na to

Z TEORIE DO PRAXE

Nyní již znáte základní doporučení, kterými se lze řídit při zabezpečení vašich kryptoměn. S touto znalostí můžeme přistoupit k další části, a sice, jak tato bezpečnostní opatření skutečně uvést do praxe. Další postup jsme pro přehlednost rozdělili do tří fází: příprava, implementace a průběžná kontrola.



Praxe

1. Příprava

CO JE TŘEBA SI ROZMYSLET

Jakou hodnotu mají mé kryptoměny a jakou mohou mít v blízké budoucnosti?

Pro kryptoměny v hodnotě stovek korun či několika málo tisíc nemusíme vymýšlet řešení s multisignature adresami a uložením záloh v depozitní schránce v bance. Zcela jinak budu pravděpodobně přistupovat k hodnotám pohybujícím se v řádech milionů Kč. Nezapomeňte ale, že hodnota vašich kryptoměn se může v čase dramaticky měnit. Abyste nemuseli své řešení neustále upravovat, je vhodné počítat s vyšší než aktuální hodnotou a nastavit řešení spíše robustněji.

Mezi kolik typů peněženek chci své kryptoměny diverzifikovat a jak? Případně, chci využít uložení u třetích osob?

Rozmyslete si, kolik peněženek a jakého typu byste chtěli využít. Z vašeho rozhodnutí následně vyplyne, kolik různých záloh nebo zařízení budete muset bezpečně uložit.

Jaká důvěryhodná místa, na které můžu uložit zálohy nebo peněženky, mám k dispozici?

Vhodné je zvolit alespoň dvě na sobě nezávislá místa, abyste v případě úspěšného útoku nepřišli o veškeré prostředky.

Které osobě mohu důvěřovat, že poradí mým pozůstalým, pokud se mi něco stane?

Zvolte minimálně jednu důvěryhodnou osobu, která se v oblasti kryptoměn orientuje a bude schopna a ochotna pomoci vaším pozůstalým získat přístup k vašim kryptoměnám a rovněž jim poradit ohledně jejich dalšího uchovávání nebo zpeněžení.

Na základě výše uvedeného vytvoříte základní kostru řešení uchování vašich kryptoměn spočívající v rozvržení kryptoměn ve vztahu k různým technologiím a volbě způsobů a míst, na kterých budete ukládat vaše tajemství, jako jsou návod, zálohy, heslové fráze, nebo peněženky.

2. Implementace

K VĚCI

V rámci této fáze byste měli vytvořit (pořídit) peněženky a zálohy a uložit je na bezpečná místa. Dále byste měli vytvořit dokumentaci skládající se z návodu a přehledu kryptomajetku a uložit je na vhodné místo.

Vytvoření peněženek a záloh

Ve vztahu ke každé peněžence by měla být vytvořena záloha (je-li to u ní možné). Pro účely vytvoření zálohy můžete použít vzor, který naleznete v příloze č. 1 této příručky.

VZOR – PŘÍLOHA Č. 1

Nezapomeňte k záloze vždy zapsat datum jejího pořízení, název kryptoměn, kterých se týká, a využívaný software (jedná-li se o peněženku na telefonu nebo desktop zařízení) nebo hardware (jedná-li se o hardwarovou peněženku).

Do poznámky můžete napsat veškeré další informace, které byste měli vy nebo jiná osoba získat spolu s danou zálohou, případně jakékoliv další informace, které uznáte za vhodné (např. pokud vzor nebude zcela vyhovovat). Může se jednat například o informace k postupu při použití zálohy, místě uložení peněženky, přístupovým údajům do telefonu či počítače nebo kde hledat heslovou frázi.

Vytvoření návodu

VZOR – PŘÍLOHA Č. 2

Vytvoříme-li nádherné a funkční řešení, ale nikde si jej v detailu nepopíšeme, riskujeme, že:

a) Zapomeneme, jaké řešení je (zvláště, je-li složitější povahy).

b) Něco se nám stane a naši pozůstalí jej nebudou schopni rekonstruovat.

c) V lepším případě extrémně zkomplikujeme situaci naším blízkým hledáním přístupů a trvající nejistotou o rozsahu zanechaného kryptoměnového majetku.

V prvních dvou případech hrozí nevratná ztráta prostředků. Ve třetím případě si naši blízcí po smrti najmou Sherlocka Holmese vyškoleného v oboru kryptoměn a ten s vynaložením podstatného úsilí úspěšně vystopuje, co po vás zbylo a jak se k tomu bezpečně dostat.

Uvedeným scénářům snadno předejdete prostřednictvím pořízení návodu, tedy jakousi „*mapou pokladu*“, kterou uložíte na vhodné, přiměřeně dostupné, místo.

Jak by mohl takový návod vypadat? Jako inspiraci pro vytvoření vašeho návodu jsme připravili vzor, který je přílohou č. 2 této příručky. Návod obsahuje několik sekcí, a sice:

1) Kontaktní osoba

Návod vytváříte primárně pro své blízké pro případ, že se vám něco stane. Proto dává smysl jako první informaci, kterou si vaší blízcí v návodě přečtou, uvést osobu, na kterou se mohou obrátit s žádostí o pomoc.

Neuvedete-li důvěryhodnou kontaktní osobu, hrozí, že vaši blízcí (nejsou-li znalí oblasti kryptoměn) se obrátí na osoby, které jejich nevědomosti a zranitelnosti snadno zneužijí ve svůj prospěch. Stejně tak mohou vaši blízcí zcela bezelstně některé citlivé informace uveřejnit při snaze získat pomoc v situaci, ve které si absolutně neví rady. Lze například předpokládat uveřejnění zálohy na online fórech s dotazem, jak s uvedenými slovy naložit.

2) Přehled majetku

Tato část návodu obsahuje informaci, kde lze nalézt přehled vašeho kryptomajektu. Vzhledem k tomu, že přehled může být aktualizován častěji než návod, může být praktické jej ukládat na odlišných místech.

Přehled kryptomajetku, který je průběžně aktualizovaný, může zjednodušit mnoho praktických problémů při vypořádání kryptomajetku po vaší smrti. Nejenže díky němu budete mít sami průběžný přehled o tom, co kde máte, ale zároveň usnadníte práci vašim blízkým při zjišťování, co po vás vlastně zůstalo a po čem je dobré pátrat. Díky sepsání přehledu kryptomajetku si rovněž ověříte, že jste při vytváření záloh a návodu na žádné „*coiny*" nezapomněli. V neposlední řadě vám pak vedení aktuálního přehledu zjednoduší způsob nakládání s kryptomajetkem v rámci tzv. „*pořízení pro případ smrti*", jako je především závěť, případně dědická smlouva či dovětek (viz dále).

Pokud i přes výše uvedené přehled kryptomajetku nebudete chtít vyhotovit, můžete tuto část návodu zcela vypustit.

3) Hesla, PINy, 2FA

Pokud se řídíte doporučeními uvedenými v úvodní části této příručky, je takřka jisté, že si nepamatujete všechna svoje hesla a používáte manažer hesel. Tato část slouží k tomu, aby vaši blízcí získali možnost dispozice s vašimi přístupovými údaji a hesly a PINy, které mohou být nezbytné zejména k získání přístupu na platformy třetích osob.

Není-li používání manažera hesel navázáno na další bezpečnostní opatření (např. používání hardware tokenu, funkce, ke které je možné využít také třeba hardwarovou peněženku Trezor), lze doporučit uschování tzv. master hesla stejně jako by se jednalo o zálohu kryptoměnové peněženky. Master heslo je extrémně citlivé, neboť pokud se k němu dostane neoprávněná osoba, může získat přístup k veškerým vašim heslům.

4) HW, papírové a SW peněženky

Cílem těchto sekcí je uvést, na kterých místech a případně u kterých osob jsou uschována tajemství, která se s nimi pojí (tj. zálohy, heslové fráze nebo případně peněženky ve fyzické podobě).

5) Kryptoměnové burzy

Tato část vysvětluje, jakým způsobem se blízcí mohou dostat k přístupu na vaše účty u třetích osob, jako jsou zejména provozovatelé kryptoměnových burz či jiných online účtů (pokud takové účty využíváte).

6) Postup

Tato část je skutečně projevem povahy návodu jako „*mapy k pokladu*“. Chcete-li to svým blízkým zjednodušit ještě více, napište jim zde krok za krokem, jak mají postupovat. Současně si tak ověříte, že jste na žádné přístupové údaje či jiné podstatné informace ve svém návodu nezapomněli.

2017: Těžce dosažitelné dědictví. Virtuální majetek si Češi berou do hrobu

“V řízení o pozůstalosti notář nepátrá po majetku, který dědicové neoznačí, případně který není evidován ve veřejných seznamech či rejstřících. Bude-li některý z dědiců tvrdit, že zemřelý vlastnil např. kryptoměnu, pak za současného stavu je téměř nemožné ověřir to bez znalosti přístupových údajů”.

viceprezident notářské komory Pavel Bernard

Vytvoření přehledu kryptomajetku

VZOR – PŘÍLOHA Č. 3

Co se týče přehledu kryptomajetku, tento by měl zachycovat vaše prostředky na všech peněženkách a rovněž možné vklady u třetích osob (zejména prostředky na kryptoměnových burzách), a to k určitému dni, který v dokumentu uvedete.

Možný vzor naleznete v příloze č. 3 této příručky. Návrh předpokládá seřazení pod dílčí kryptoměny, nicméně lze to samozřejmě udělat i tak, že jej seřadíte dle dané platformy či zařízení. Nezapomeňte vždy uvést dostatečnou identifikaci (např. jméno HW peněženky, pokud disponujete větším počtem).

Výborně! Jak ale poznáte, že zvolené nastavení je to *„správné“*? Těžko. Asi se totiž nebudete pouštět do ostrého testování vlastním úmrtím nebo zničením hardwarových peněženek, ke kterým jste vytvářeli zálohy. Můžete nicméně vyzkoušet alespoň to, že si představíte (vymyslíte) několik variant situací, které se mohou stát a pokusíte se zahrát si na osobu, která by se k vašim prostředkům měla dostat, případně na osobu, která by k vaším prostředkům neměla dostat, ale chtěla by. Vaše opatření rovněž můžete v anonymizované podobě vyzkoušet na vašich blízkých.

3. Kontrola

SKORO BYCHOM ZAPOMNĚLI

Poslední fází uvedení vašeho řešení do života je jeho průběžné udržování a aktualizace. Za tímto účelem je vhodné nastavit si pravidelné intervaly, ve kterých budete kontrolovat, zejména, že: (1) Aktuální stav odpovídá informacím v návodu (tedy především způsob uložení, místa a určené osoby); (2) Zálohy jsou stále přístupné a čitelné a nebylo s nimi neoprávněně manipulováno; (3) A koneckonců i to, že vaše kryptoměny stále leží na stejných adresách.

Blockchain Legal

PRO PŘÍPAD SMRTI

PRO PŘÍPAD SMRTI

NEŽIJEME VĚČNĚ

K čemu to je?

Pokud jste došli až sem, gratulujeme. Už tak jste udělali dost a pravděpodobně také víc než velká část ostatních kryptomajitelů. Snížili jste riziko, že své kryptoměny ztratíte nebo vám je někdo ukradne a zároveň jste zajistili, že vaše kryptoměny se jednou společně s vámi neodeberou do věčných lovišť.

Máte-li zájem rozšířit své řešení ještě o jeden další krok, kterým je určení, co konkrétního se stane s kryptoměnami po vaší smrti a s tím související zjednodušení celého pozůstalostního (dědického) řízení, pak právě pro vás je tato kapitola.

Účelem této části nicméně není podrobně vás provést celým procesem dědického řízení a vysvětlit vám veškeré detaily a rizika s procesem spojená. To vám může lépe a ve vztahu k vašemu konkrétnímu případu vysvětlit notář nebo advokát, bude-li vás to zajímat. My bychom vám naopak rádi nabídli jednoduchou a nenáročnou alternativu k tomu, že se na úvahy o vaší pozůstalosti a její případnou úpravu zcela vykašlete. Pro tyto účely jsme zvolili z různých pořízení pro případ smrti nejběžnější formu, tj. závěť. Tuto poslední vůli navíc můžete vytvořit sami a s relativně minimem rizik.

2018: The Matthew Mellon Ripple treasure disappeared into thin air

Dědictví

Co se stane, když nic neudělám?

Pokud neprovedete určité zákonem předpokládané úkony, pak se o celé dědictví a související řízení postará zákonná úprava. Ta v prvé řadě stanoví, kdo a v jakém rozsahu zdědí vaši pozůstalost včetně kryptoměn a stane se tak jejich novým vlastníkem. Zákonná úprava svěří ústřední roli v celém procesu notář, který částečně plní roli soudu. V případě sporů mezi dědici o tom, kdo, co a v jakém rozsahu dědí, se však může celý proces protáhnout i na řadu let.

Kdo tedy dědí, když nikoho neurčíte? Občanský zákoník stanoví tzv. zákonnou posloupnost, v rámci které definuje preferované dědické třídy. Dědických tříd je celkem šest a vždy se dědí a postupuje pouze podle jedné z nich. Pro ilustraci se podívejme na první tři z těchto tříd, podle kterých se obvykle dědictví rozděluje:

1) První třída: Dědí děti a manžel, a to každý stejným dílem. Platí ale, že sám manžel v rámci první třídy dědit nemůže.
2) Druhá třída: Dědí manžel, rodiče a tzv. osoby spolužijící (typicky partner), manžel minimálně polovinu, ostatní stejným dílem. Osoby spolužijící nicméně samy v rámci druhé třídy dědit nemohou.
3) Třetí třída: Dědí sourozenci (stačí jeden společný rodič) a osoby spolužijící. Podíly přecházejí na děti sourozenců.

Závěť

Co je závěť a jaké má formy:

Jedna z možností, jak naložit se svými kryptoměnami pro případ smrti je pořízení závěti. Záměrně se zde nevěnujeme jiným možnostem, jako jsou dědická smlouva, darování pro případ smrti nebo odkaz. Tyto složitější koncepce, které nicméně mohou být pro určité případy vhodnější, lze doporučit konzultaci s notářem nebo advokátem.

Závěť je jednání, kterým můžete určit jednu nebo více osob za své dědice, tedy ty osoby, na které přejdou vaše práva a závazky (majetek i dluhy), podíl na nich nebo konkrétní majetek pomocí tzv. odkazu. Účelem závěti je, že se svým jměním naložíte jinak, než by za vás udělal zákon (tedy ve smyslu shora uvedených dědických tříd). Zároveň platí, že závěť nemusíte pořizovat ohledně veškerého svého majetku a lze ji tedy kombinovat s postupem dle zákona. Neuplatní-li se k části vašeho jmění závěť, zpravidla se automaticky dědí dle zákonné posloupnosti.

Závěť lze pořídit zejména v následujících formách:

1) Notářský zápis: Nejbezpečnější je jít za notářem a pořídit závěť notářským zápisem. Výhodou je nejen právní poradenství, kterého se vám při pořízení notářského zápisu od notáře dostane, ale rovněž zaznamenání informace o závěti do tzv. Evidence právních jednání pro případ smrti, jak vysvětlujeme dále. Komu se ale chce chodit k notáři, že?

2) Vlastní rukou: Alternativně můžete napsat závěť vlastní rukou. Celé znění závěti však musí být nejen podepsáno ale i sepsáno vlastní rukou.

3) Před svědky: Není-li závěť napsaná vlastní rukou (např. si ji vytisknete), musíte se vlastní rukou podepsat a před dvěma svědky současně přítomnými výslovně prohlásit, že daná listina obsahuje vaši poslední vůli. Pozor! Svědky nemohou být dědicové, jejich osoby blízké (rodina, partner apod.) ani vykonavatel závěti.

V příloze naleznete jednoduchý vzor závěti, který obsahuje dvě základní varianty, a sice:

1) Specifikaci konkrétních věcí (např. kryptoměn), které odkážete konkrétním osobám.

   Tato varianta předpokládá, že jmění neuvedené v závěti se bude dědit dle zákona.

2) Obecné rozdělení vašeho jmění na podíly, s tím, že každý dostane podíl ve stejném rozsahu.

   Tato varianta předpokládá, že všechno vaše jmění se dědí podle závěti.

Vykonavatel závěti:

Závěť zároveň obsahuje ustanovení o vykonavateli závěti. Kdo to je a proč jsme jej do vzoru zahrnuli? Vykonavatel závěti je osoba, která dbá o řádné splnění poslední vůle. V rámci své role mimo jiné spravuje pozůstalost (do ukončení dědického řízení, není-li ustanoven správce dědictví) nebo uděluje pokyny správci pozůstalosti potřebné k řádné správě pozůstalosti.

Zjednodušeně řečeno se tedy jedná o osobu, která by měla dohlížet nad procesem rozdělení dědictví dle závěti. V případě kryptoměn by tak měla dohlížet zejména na to, že s kryptoměnami je nakládáno tak, aby v průběhu nedošlo k jejich odcizení nebo ztrátě. Má-li vykonavatel křišťálovou kouli, může se i pokusit předejít znehodnocení konkrétní kryptoměny v souvislosti s propadem její ceny.

Prakticky by vykonavatel závěti měl být přítomen dílčím úkonům, jako je získání záloh, rekonstrukce peněženek apod. Vykonavatel by při těchto úkonech měl dohlédnout, aby citlivé informace neunikly k neoprávněným osobám.

Vykonavatel závěti je dobrovolná funkce. Osoba, kterou v závěti určíte, může z funkce kdykoliv odstoupit. Proto je vhodné předem určit vykonavateli závěti i odměnu, která mu připadne za řádný výkon jeho povinností.

Nepominutelní dědicové:

Při pořízení závěti je zároveň nutné si dát pozor na to, že zákon při dědění zvýhodňuje některé osoby nazvané nepominutelnými dědici.

Nepominutelnými dědici jsou výhradně děti zůstavitele a pokud tyto nedědí, tak jejich potomci.

Nepominutelní dědicové musí v rámci dědictví získat tzv. povinný díl, kterým je u (i) nezletilého nepominutelného dědice ¾ jeho zákonného dědického podílu (tedy toho, který by dostal, kdyby žádná závěť neexistovala) a u (ii) zletilého nepominutelného dědice ¼ jeho zákonného dědického podílu. Vyhnout se těmto omezením lze pouze prostřednictvím tzv. vydědění, a to pouze v zákonem vymezených případech.

Uložení závěti:

U závěti platí totéž, co u návodu. Závěť, která se po vaší smrti nenajde, jako by nebyla.

V úvahu, tak připadají obdobná místa jako u návodu. Pokud chcete mít stoprocentní jistotu, pak je vhodné využít služeb notáře, který při přijetí závěti do úschovy tuto zaeviduje shodně jako při pořízení závěti formou notářského zápisu v Evidenci právních jednání pro případ smrti. Existence závěti v této centrální evidenci vedené notářskou komorou bude vždy kontrolována notářem, který bude pověřen soudem k úkonům v daném dědickém řízení.

Daně a jiné výdaje v rámci dědického řízení

I pokud nejste přímo libertarián či anarchokapitalista, je pravděpodobné, že nejste fanouškem daňové povinnosti. Možná rovnou považujete odvod daně za krádež za bílého dne. Proto vás jistě potěší, že dědická daň byla již v roce 2014 zrušena. Zanecháte-li tedy svůj kryptomajetek dědicům (ať již se jedná o fyzickou nebo právnickou osobu), žádnou daň z ní tyto osoby odvádět nebudou.

V rámci dědického řízení se nicméně platí odměna notáři za vedení dědického řízení. Ta je stanovena dle vyhlášky Ministerstva spravedlnosti a odvíjí se od hodnoty dědictví. Pro hrubou představu, při hodnotě 20 mil. Kč se odměna bude pohybovat v závislosti na dalších okolnostech (výší nákladů spojených s přípravou podkladů pro soud) kolem 50.000,- Kč. U hodnoty odpovídající 1 mil. Kč se odměna notáře bude pohybovat kolem 14.000,- Kč.

Blockchain Legal

PŘÍLOHY

Vzorové dokumenty

PRO TROCHU INSPIRACE A ABY VÁM RUKA NEUPADLA

Na následujících stránkách naleznete vzorové dokumenty, které by vám mohly přijít vhod při uvadění informací uvedených v této příručce do praxe.

Prosím, mějte nicméně na paměti, že vzorové dokumenty slouží pouze pro inspiraci a při jejich případném vyplňování je vždy nutné zohlednit konkrétní okolnosti. Jinými slovy, berte tyto vzory s rezervou a při práci s nimi zapojte selský rozum!

Editovatelné verze všech dokumentů naleznete zde.

Datum: _____

Kryptoměna: _____

SW (HW): _____

Recovery seed:

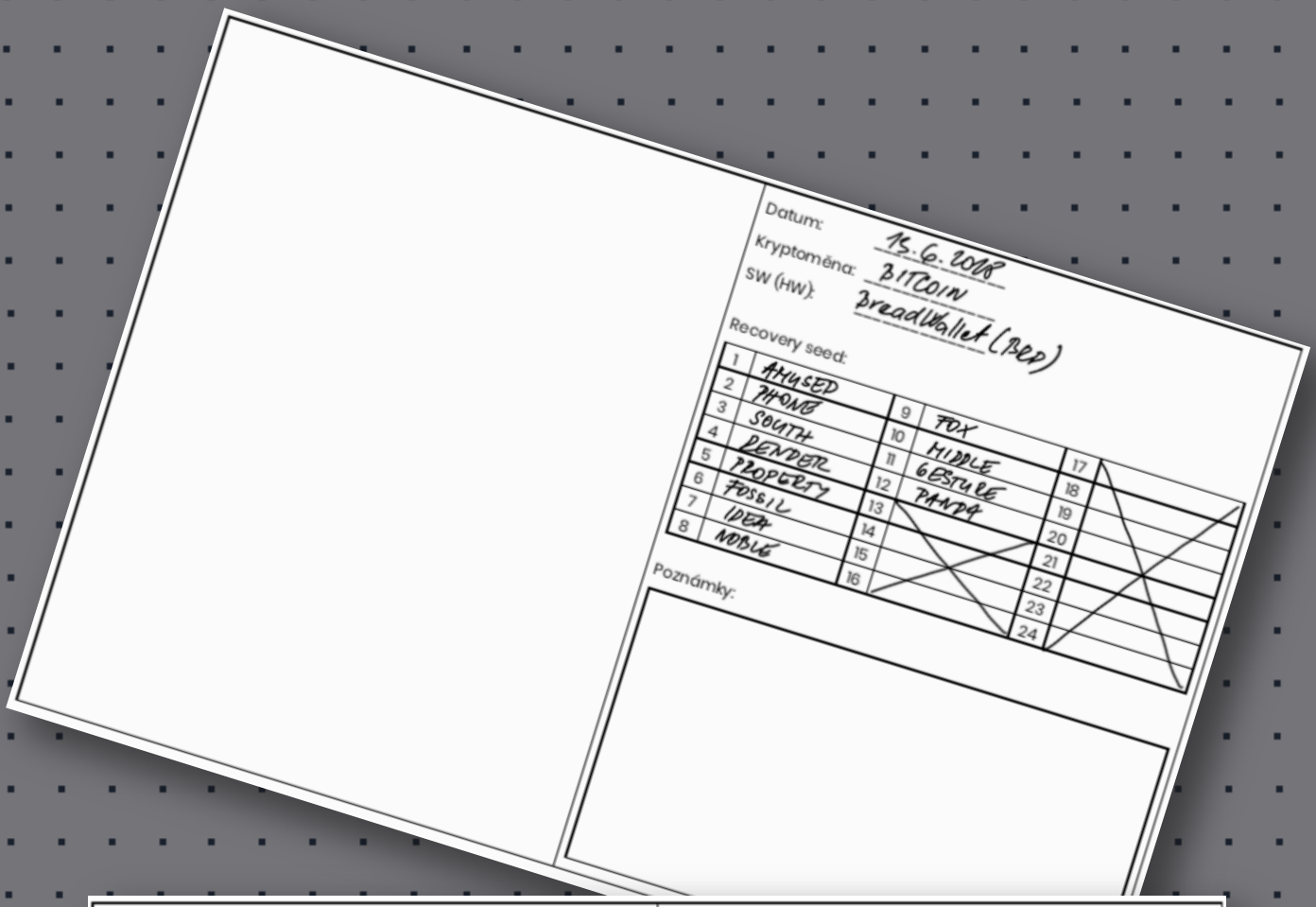
1		9		17	
2		10		18	
3		11		19	
4		12		20	
5		13		21	
6		14		22	
7		15		23	
8		16		24	

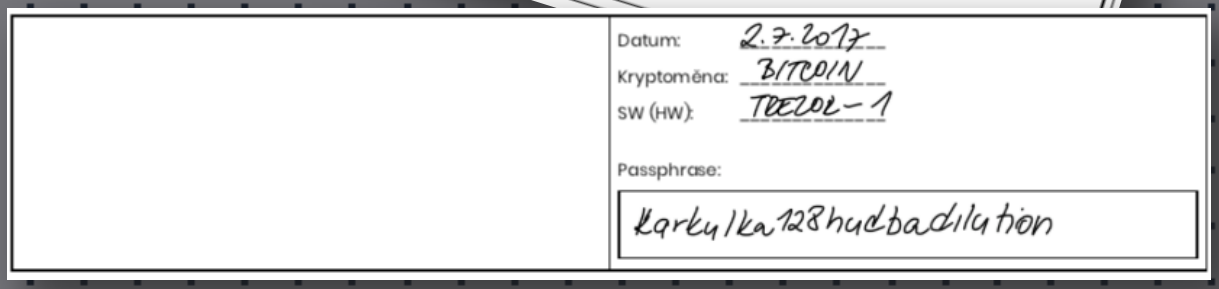
Poznámky:

PŘÍLOHY – Vzor zálohy

	Datum: _____ Kryptoměna: _____ SW (HW): _____ Passphrase:
	Datum: _____ Kryptoměna: _____ SW (HW): _____ Passphrase:
	Datum: _____ Kryptoměna: _____ SW (HW): _____ Passphrase:

UKÁZKA


Datum: 15.6.2018
Kryptoměna: BITCOIN
SW (HW): BreadWallet (BRD)
Recovery seed:
1 ARMSED
2 PHONE
3 SOUTH
4 RENDER
5 PROPERTY
6 FOSSIL
7 IDEA
8 NOBLE
9 FOX
10 MIDDLE
11 GESTURE
12 PANDA
13
14
15
16
17
18
19
20
21
22
23
24
Poznámky:


Datum: 2.7.2017
Kryptoměna: BITCOIN
SW (HW): TREZOR – 1
Passphrase:
karkulka128hudbadilution

Poslední revize: _____

VZOR - PŘÍLOHA Č. 2

NÁVOD KE KRYPTOMĚNÁM

!!! Pokud si kteroukoliv částí uvedenou v tomto návodu nejste jisti, vždy se poraďte s někým, kdo problematice rozumí. Buďte zároveň maximálně obezřetní při jakýchkoliv operacích s kryptoměnami. Zejména se snažte být osobně přítomni veškerým krokům a nechte si jejich význam vysvětlit. Při pochybení nebo zneužití hrozí nevratná ztráta kryptoměn!!!

1. KONTAKTNÍ OSOBA

V případě, že si s tímto návodem nebudete vědět rady, kontaktujte následující osobu, které důvěřuji a která má zkušenosti a znalosti v oblasti kryptoměn:

Jméno: _____

E-mail: _____

Telefon: _____

2. PŘEHLED MAJETKU (KRYPTOMĚNY)

V příloze tohoto návodu naleznete přehled mých kryptoměn a způsob jejich uložení.

Alternativně:

Aktuální přehled mých kryptoměn a způsob jejich uložení naleznete zde:

Umístění: _____

Kontakt: *tel.: _____, e-mail: _____*

Obálka: _____

3. HESLA, PINy, 2FA

3.1. Hesla a PINy

Veškerá hesla, PINy a další autentifikační údaje, které využívám k přístupu do různých služeb, jsou dostupná _____, a to za použití přihlašovacích údajů, které naleznete zde:

Umístění: _____

Kontakt: tel.: _____, e-mail: _____

Obálka: _____

3.2. 2FA

Zálohy ke všem 2FA jsou v papírové podobě uloženy v _____

_____

_____

4. HW PENĚŽENKY

Veškeré zálohy k HW peněženkám jsou uchovávány dle následujícího popisu. Je-li uvedeno, že využívám passphrase, pak je k použití zálohy nezbytná i znalost dodatečného „*hesla*".

4.1. Název HW peněženky: _____

4.1.1. *Recovery seed*

Umístění: _____

Kontakt: tel.: _____, e-mail: _____

Obálka: _____

4.1.2. *Passphrase*

Umístění: _____

Kontakt: tel.: _____, e-mail: _____

Obálka: _____

5. PAPÍROVÉ PENĚŽENKY

Veškeré papírové peněženky, které používám pro uložení kryptoměn, jsou uchovávány dle následujícího popisu.

5.1. Název kryptoměny: _____

Umístění: _____

Kontakt: tel.: _____, e-mail: _____

Obálka: _____

6. SW PENĚŽENKY

6.1. Název kryptoměny: _____; Typ peněženky: _____

Recovery seed

Umístění: _____

Kontakt: tel.: _____, e-mail: _____

Obálka: _____

6.2. Název kryptoměny: _____; Typ peněženky: _____

Recovery seed

Umístění: _____

Kontakt: tel.: _____, e-mail: _____

Obálka: _____

7. KRYPTOMĚNOVÉ BURZY

Informace o zůstatcích na kryptoměnových burzách jsou uvedeny v dokumentu s přehledem mého kryptomajetku.

Identifikační údaje a další informace nezbytné k přístup k účtům jsou uvedené v bodu 3 tohoto návodu (hesla, PINy, 2FA).

8. POSTUP

Doporučený postup pro získání kompletního přístupu k mému kryptomajetku:

1) Požádání kontaktní osoby o pomoc (bod 1)
2) Získání přihlašovacích údajů do password manageru (bod 3.1)
3) Získání a obnova záloh 2FA (bod 3.2)
4) Získání zálohy HW peněženek (bod 4.1.1)
5) Získání passphrase k HW peněžence (bod 4.1.2)
6) Získání přístupu k papírovým peněženkám (bod 5)
7) Získání záloh a obnova zbývajících peněženek (bod 6)

Podpis: _____

Poslední revize: 21. 11. 2018

NÁVOD KE KRYPTOMĚNÁM

!!! Pokud si kteroukoliv částí uvedenou v tomto návodu nejste jisti, vždy se poraďte s někým, kdo problematice rozumí. Buďte zároveň maximálně obezřetní při jakýchkoliv operacích s kryptoměnami. Zejména se snažte být osobně přítomni veškerým krokům a nechte si jejich význam vysvětlit. Při pochybení nebo zneužití hrozí nevratná ztráta kryptoměn. !!!

1. KONTAKTNÍ OSOBA

V případě, že si s tímto návodem nebudete vědět rady, kontaktujte následující osobu, které důvěřuji a která má zkušenosti a znalosti v oblasti kryptoměn:

Jméno: PETR ZNALÝ
E-mail: znaly@protonmail.com
Telefon: +420 123 456 789

2. PŘEHLED MAJETKU (KRYPTOMĚNY)

V příloze tohoto návodu naleznete přehled mých kryptoměn a způ

Alternativně:

Aktuální přehled mých kryptoměn a způsob jejich uložení naleznet

Umístění: 3. ŠUPLÍK U STOLU V PRACOVNĚ MÉHO B
Kontakt: *tel.:* ———, *e-mail:* ———
Obálka: 72681729

3. HESLA, PINy, 2FA

3.1. Hesla a PINy

Veškerá hesla, PINy a další autentifikační údaje, které využívám k
jsou dostupná V APLIKACI LASTPASS (lastpass.com), a t
údajů, které naleznete zde:

Umístění: Depozitní schránka (Komerční banka
Kontakt: tel.: +420 123 456 789, e-mail: banka@
Obálka: A123456789

3.2. 2FA

Zálohy ke všem 2FA jsou v papírové podobě uloženy v Samolepce s nálep
osobní, který je uložen v mém bytě v obývacím pokoji v knihovně.

4. HW PENĚŽENKY

Veškeré zálohy k HW peněženkám jsou uchovávány dle následujícího popisu. Je-li uvedeno, že využívám passphrase, pak je k použití zálohy nezbytná i znalost dodatečného „*hesla*".

4.1. Název HW peněženky: TREZOR – FRANTA

4.1.1. *Recovery seed*
Umístění: Úschova u notáře (Jan Notář, U Notáře 12, Praha)
Kontakt: tel.: +420 123 456 789, e-mail: notar@notar.cz
Obálka: A123456789

4.1.2. *Passphrase*
Umístění: Depozitní schránka (Komerční banka – Praha 1)
Kontakt: tel.: +420 123 456 789, e-mail: banka@banka.cz
Obálka: A123456789

5. PAPÍROVÉ PENĚŽENKY

Veškeré papírové peněženky, které používám pro uložení kryptoměn, jsou uchovávány dle následujícího popisu.

5.1. Název kryptoměny: BITCOIN (BTC)
Depozitní schránka (Komerční banka – Praha 1)
tel.: +420 123 456 789, e-mail: banka@banka.cz
A123 456 789

6.2. Název kryptoměny: BITCOIN (BTC); Typ peněženky: BreadWallet (telefon)

6.2.1. *Recovery seed*
Umístění: knihovna – 2. p
Kontakt: tel.: ———, e-mail: ———
Obálka: A123456789

ŽENKY
toměny: XMR; Typ peněženky: GUI – Desktop

seed
Úschova u notáře (Jan Notář, U Notáře 12, Praha
tel.: +420 123 456 789, e-mail: notar@notar.cz
A123 456 789

7. KRYPTOMĚNOVÉ BURZY

Informace o zůstatcích na kryptoměnových burzách jsou uvedeny v dokumentu s přehledem mého kryptomajetku.

Identifikační údaje a další informace nezbytné k přístup k účtům jsou uvedené v bodu 3 tohoto návodu (hesla, PINy, 2FA).

8. POSTUP

Doporučený postup pro získání kompletního přístupu k mému kryptomajetku:

1) Požádání kontaktní osoby o pomoc (bod 1)
2) Získání přihlašovacích údajů do password manageru (bod 3.1)
3) Získání a obnova záloh 2FA (bod 3.2)
4) Získání zálohy HW peněženek (bod 4.1.1)
5) Získání passphrase k HW peněžence (bod 4.1.2)
6) Získání přístupu k papírovým peněženkám (bod 5)
7) Získání záloh a obnova zbývajících peněženek (bod 6)

Podpis: Jan Podpisil

VZOR - PŘÍLOHA Č. 3

PŘEHLED KRYPTOMAJETKU

Platné ke dni: _____

Kryptoměna	
Platforma a její identifikace	Počet

Kryptoměna	
Platforma a její identifikace	Počet

Kryptoměna	
Platforma a její identifikace	Počet

PŘÍLOHY – Vzor přehledu kryptomajetku

Platforma	
Kryptoměna	Počet

Platforma	
Kryptoměna	Počet

Platforma	
Kryptoměna	Počet

Platforma	
Kryptoměna	Počet

Platforma	BINANCE
Kryptoměna	Počet
BITCOIN (BTC)	0.1
MONERO (XMR)	20
DASH	10

Platforma	LEDGER
Kryptoměna	Počet
BITCOIN (BTC)	0.1
STELLAR (XLM)	20
ZCASH (ZEC)	5

Platforma	
Kryptoměna	

Platforma	
Kryptoměna	

UKÁZKA

PŘEHLED KRYPTOMAJETKU

Platné ke dni: 1.11.2017

Kryptoměna	BITCOIN (BTC)
Platforma a její identifikace	Počet
TREZOR - JANEK 1	0.1
TREZOR - JANEK 2	0.1
LEDGER	0.1
OPENDIME	0.1
IPHONE - Bread Wallet	0.01
BINANCE	0.1

Kryptoměna	LITECOIN (LTC)
Platforma a její identifikace	Počet
IPHONE - COINOMI	1
TREZOR - JANEK 1	5

Kryptoměna	ETHEREUM (ETH)
Platforma a její identifikace	Počet
MYETHERWALLET - TREZOR - JANEK 1	4

ZÁVĚŤ

Já, ***bude doplněno***, r. č.: *bude doplněno*, v době sepsání této závěti trvale bytem: bude doplněno,

pořizuji pro případ mé smrti vědomě, bez nátlaku, po zralé úvaze a svobodně tuto svoji závěť, která představuje a obsahuje moji poslední vůli ohledně mého majetku.

1. POVOLÁNÍ DĚDICŮ

Svými dědici povolávám:

1) *bude doplněno*, nar.: *bude doplněno*, bytem: *bude doplněno*
2) *bude doplněno*, nar.: *bude doplněno*, bytem: *bude doplněno*
3) *bude doplněno*, nar.: *bude doplněno*, bytem: *bude doplněno*

2. POŘÍZENÍ PRO PŘÍPAD SMRTI

Dědice povolávám následujícím způsobem:

1) Dědicem *bude doplněno* povolávám *bude doplněno*.
2) Dědicem *bude doplněno* povolávám *bude doplněno*.
3) Dědicem *bude doplněno* povolávám *bude doplněno*.

Ostatní svůj majetek ponechávám zákonné dědické posloupnosti. Dědicové se mohou dohodnout i na jiné výši dědických podílů.

Alternativně: Každého z dědiců povolávám (a tímto jim vyměřuji podíl na pozůstalosti) k jedné třetině (1/3) mého veškerého jmění/Dědicem veškerého svého jmění povolávám bude doplněno.

3. VYKONAVATEL ZÁVĚTI

Vykonavatelem této závěti povolávám *bude doplněno*, nar.: *bude doplněno*, bytem: *bude doplněno.*

Vykonavatel zajistí a dohlíží (zejména po technické stránce), aby veškeré kryptoměny (např. Bitcoin, Litecoin, Monero apod.), které jsou součástí pozůstalosti, byly rozděleny mezi dědice způsobem stanoveným v této závěti.

Vykonavateli této závěti náleží odměna ve výši *bude doplněno* Kč, a to za každý započatý kalendářní měsíc výkonu funkce, až do pravomocného ukončení řízení o pozůstalosti po mé osobě.

Zůstavitel: V *bude doplněno* dne *bude doplněno*

_____

bude doplněno

4. SVĚDECKÁ DOLOŽKA

Potvrzujeme svým podpisem, že *bude doplněno* před námi současně přítomnými svědky tuto závěť vlastní rukou podepsal a výslovně prohlásil, že tato listina obsahuje jeho poslední vůli.

V *bude doplněno* dne *bude doplněno*

_____
bude doplněno
nar.: *bude doplněno*
bytem: *bude doplněno*

V *bude doplněno* dne *bude doplněno*

_____
bude doplněno
nar.: *bude doplněno*
bytem: *bude doplněno*

ZÁVĚŤ

Já, **Janek Dohodlll**, r. č.: *990103/5259*, v době sepsání této závěti trvale bytem: U Satoshiho 42, Praha 1, 110 00,

pořizuji pro případ mé smrti vědomě, bez nátlaku, po zralé úvaze a svobodně tuto svoji závěť, která představuje a obsahuje moji poslední vůli ohledně mého majetku.

1. POVOLÁNÍ DĚDICŮ

Svými dědici povolávám:

1) Janu Nevdanou, nar.: 25. 11. 1990, bytem: Nakamota Satoshiho 42, Praha 1, 110 00,
2) Martina Nevlastního, nar. 14. 6. 2010, bytem: Nakamota Satoshiho 42, Praha 1, 110 00, a
3) Františka Bločenku, nar.: 12. 3. 1998, bytem: Hala Finney 2014, Praha

2. POŘÍZENÍ PRO PŘÍPAD SMRTI

Dědice povolávám následujícím způsobem:

1) Dědicem 2 bitcoinů (BTC) povolávám Janu Nevdanou.
2) Dědicem 150 moner (XMR) povolávám Martina Nevlastního.
3) Dědicem veškerých zbývajících bitconů (BTC), moner (XMR), etheru (ETH), litecoinů (LTC) a případně jiných kryptoměn, které budu mít ve svém vlastnictví k okamžiku mé smrti, povolávám Františka Bločenku.

Ostatní svůj majetek ponechávám zákonné dědické posloupnosti.

Dědicové se mohou dohodnout i na jiné výši dědických podílů.

Alternativně:

Každého z dědiců povolávám (a tímto jim vyměřuji podíl na pozůstalosti) k jedné třetině (1/3) mého veškerého jmění/Dědicem veškerého svého jmění povolávám Františka Bločenku.

3. VYKONAVATEL ZÁVĚTI

Vykonavatelem této závěti povolávám Petra Znalého, nar.: 2. 8. 1985, bytem: U Trezorky 123/1 Praha.

Vykonavatel zajistí a dohlíží (zejména po technické stránce), aby veškeré kryptoměny (např. bitcoin, litecoin, monero apod.), které jsou součástí pozůstalosti, byly rozděleny mezi dědice způsobem stanoveným v této závěti.

Vykonavateli této závěti náleží odměna ve výši 10.000,- Kč, a to za každý započatý kalendářní měsíc výkonu funkce, až do pravomocného ukončení řízení o pozůstalosti po mé osobě.

Zůstavitel:

V Praze dne 3. 1. 2020

Janek Dohodlll

4. SVĚDECKÁ DOLOŽKA

Potvrzujeme svým podpisem, že Janek Dohodlil před námi současně přítomnými svědky tuto závěť vlastní rukou podepsal a výslovně prohlásil, že tato listina obsahuje jeho poslední vůli.

V Praze dne 3. 1. 2020

Ondřej Vidět
nar.: 8. 6. 1986
bytem: U Vidělů 12, Praha

V Praze dne 3. 1. 2020

Marie Vidělа
nar.: 15. 8. 1989
bytem: U Vidělů 12, Praha

O nás, autoři a licence

KDO JSME

Advokátní kancelář Blockchain Legal jsme založili v roce 2017, a to s ohledem na naše nadšení a zájem o informační technologie a kryptoměny i nedostatečnou nabídku specializovaných právních služeb v těchto oblastech.

NAŠE VIZE

Naším cílem je rozvíjet hodnoty osobní svobody, ochrany soukromí a decentralizace v těsném sepětí s technologiemi.

Autory tohoto e-booku jsou Pavel Urbaczka a Tomáš Elbert, advokáti Blockchain Legal. Komiksové ilustrace vytvořila Marie Butula Cichá.

Blockchain Legal

CYPHERPUNK LAWYERS

blockchainlegal.cz

info@blockchainlegal.cz