



SNADNÝ ZPŮSOB, JAK ZAČÍT
**Uživatelská příručka
k Bitcoinu**

Vítej v uživatelské příručce k Bitcoinu!

Díky této příručce jsi nyní jen krůček od toho, aby ses naučil, jak se stát nezávislým uživatelem Bitcoinu, který se umí o své prostředky zodpovědně postarat. Budoucnost financí a technologií čeká jen na Tebe!

Pouze několik jednoduchých kroků Ti stačí k tomu, aby ses vydal na cestu za bitcoinovým dobrodružstvím. Nauč se provádět transakce a bezpečně uchovávat své prostředky.

Gratulujeme Ti k zodpovědnému přístupu.

Je čas vydat se na cestu za poznáním vzrušujícího světa Bitcoinu!

OBSAH

Jak mohu získat bitcoin?.....	4
Nástroje pro práci s digitálními penězi.....	7
Nastavení hardwarové peněženky.....	9
Správa zálohování.....	17
Lightning network.....	25

JAK MOHU ZÍSKAT BITCOIN?

Bitcoin lze získat mnoha způsoby. Nejpopulárnějším je jeho nákupna kryptoměnových burzách za tradiční měny (např. koruny, dolary, eura).

V bitcoinech můžeš také přijímat platby za zboží nebo služby.

Zkus požádat svého zaměstnavatele o vyplácení mzdy nebo její části v bitcoinech.

Nezapomínej, že i když jsou burzy oblíbeným a snadným způsobem, jak získat bitcoin, nedoporučují se pro jeho dlouhodobou úschovu. Majetek uložený na burze není plně Tvůj, protože nemáš pod kontrolou privátní klíče k peněžence. Proto se říká:

“NEMÁŠ-LI VLASTNÍ KLÍČE, NEVLASTNÍŠ ANI MINCE”.

Z právního hlediska nejsi vlastníkem prostředků uložených na burze, jsi pouze oprávněn vznést nárok na jejich výběr.

Zajisti bezpečnost svých bitcoinů tím, že je budeš ukládat na vlastní hardwareovou peněženku.



JAK MOHU ZÍSKAT BITCOIN?

Nakupuj nebo vydělávej

Mzdy se liší, ale všichni vyděláváme peníze prací a naše práce se měří v hodinách. Jestliže čas jsou peníze, pak je zde několik návrhů závislých na tom, kolik času/peněz chceš investovat do Bitcoingu. Pomohou Ti zjistit, jak hravý můžeš být a kdy je čas přejít na něco serióznějšího:

jednahodina:

experimentuj s transakcemi, testuj různé online aplikace,

jeden den:

rozhodni se, kterou bezplatnou aplikaci si nainstaluješ do svého chytrého telefonu,

dva týdny:

rozhodni se, kterou hardwarovou peněženku si pořídíš,

jeden měsíc:

poříď si kovovou destičku/kapsli, aby sis vytvořil trvalou zálohu výchozí fráze (seedu) pro obnovení přístupu k peněžence. V případě ztráty hardwarové peněženky pak můžeš svůj majetek lehce získat zpět.

Bitcoin se, stejně jako každá tradiční měna, dělí na dílčí jednotky. Každý bitcoin představuje neuveritelných sto milionů satoshi (100 000 000 SATS). Díky tomu je možné koupit bitcoin i za zlomek koruny.

NÁSTROJE PRO PRÁCI S DIGITÁLNÍMI PENĚZI

BEZPEČNÉ

HARDWAROVÁ PENĚZENKA
generování a autorizace
blockchainových transakcí



ZABEZPEČENÉ

KOVOVÝ RECOVERY SEED
odolné řešení pro záznam a úschovu seedu

UNIVERZÁLNÍ

LIGHTNING NETWORK
rychlé platby na dosah ruky



NASTAVENÍ HARDWAROVÉ PENĚZENKY

Moderní počítače a chytré telefony jsou sice schopné provádět kryptografické algoritmy potřebné pro používání Bitcoinu, ale ze své podstaty jsou nezabezpečené.

Tato zařízení provádějí různorodé úkoly – pořizují fotky nebo prohlížejí web – a obecně platí, že čím více toho zařízení umí, tím více má bezpečnostních slabin.

SLOVNÍČEK POJMŮ

PRIVÁTNÍ KLÍČ
velmi silné heslo

HARDWAROVÁ PENĚZENKA

Hardwarová peněženka je elektronické zařízení, které může provádět omezený počet úloh: vytvoření hesla, výpočet bitcoinové adresy a ověření transakce. Omezením funkčnosti zařízení se snižuje riziko úspěšného pokusu o hackerský útok.

DODATEČNÝ displej

Hardwarová peněženka obsahuje vestavěný displej. Ověřování na tomto dodatečném displeji zabraňuje neoprávněnému přístupu a zvyšuje bezpečnost.

PRIVÁTNÍ KLÍČE

Aby byly Tvé mince v bezpečí, hardwarová peněženka izoluje Tvůj privátní klíč v offline šifrované paměti a nikdy Tvé privátní klíče neodešle do počítače, ke kterému je připojena.

Předními značkami hardwarových peněženek jsou v abecedním pořadí:
Bitbox, Blockstream, ColdCard, Foundation, Ledger a Trezor.



NASTAVENÍ HARDWAROVÉ PENĚŽENKY

Co je to hardwarová peněženka
a proč jí potřebuji?

Zprovoznění hardwareové peněženky by nemělo trvat déle než 30 minut.

Připrav si počítač, kus papíru a něco na psaní. Také budeš potřebovat přístup k internetu a chvíli klidu.

Ujisti se, že Tě během tohoto procesu nikdo neruší a nepozoruje – zajistíš tak jeho efektivní průběh.

Většina operací uvedených v této příručce se týká citlivých údajů – doporučujeme je provádět na soukromém místě.

Nezapomínej, že hardwareovou peněženku lze snadno uvést do továrního nastavení. Pokud máš stále obnovovací frázi peněženky, o své mince nepřijdeš – lehce peněženku znova zprovozníš. Pokud se chceš procvičit, můžeš tento krok několikrát zopakovat.



Najdi si klidné místo - vezmi si tužku a papír

Nastavení hardwarové peněženky

Tento proces obvykle začíná instalací softwaru do počítače, který umožnuje pohodlné používání hardwarové peněženky.

Pečlivě postupuj podle pokynů zobrazených na monitoru počítače a na displeji zařízení. Nastav si další zabezpečení přístupu k zařízení (obvykle kód PIN) podle pokynů výrobce. Poté si zapíš slova zobrazená na obrazovce hardwarové peněženky – jedná se o Tvou tajnou obnovovací frázi (seed).

Zabezpečení Tvé obnovovací fráze

Seed je klíčový a je nezbytný pro obnovení prostředků v případě ztráty, poškození nebo zničení hardwarové peněženky. Měl by být uložen na bezpečném místě.

Převod prostředků do hardwarové peněženky

Jakmile je peněženka správně nastavena, můžeš do ní převést bitcoiny z jiné peněženky nebo burzy.

Doporučujeme přečíst si návod k použití dodaný výrobcem, protože se tento postup může lišit v závislosti na modelu peněženky.



Stáhni si aplikaci

Hardware penězenky jsou navrženy tak, aby k privátnímu klíči měl přístup pouze jejich majitel, což zvyšuje jejich úroveň zabezpečení.

Obnovovací fráze (seed) je řada obvykle 12 nebo 24 slov, ve kterých je zakódován Tvůj privátní klíč k penězence. Nezapomínej, že tato slova umožňují přístup k Tvým finančním prostředkům!

SLOVNÍČEK POJMŮ

SEED

privátní klíč sloužící k opětovnému získání přístupu v případě selhání nebo ztráty hardware penězенky.

Seed lze přenášet mezi hardware penězenkami různých výrobců. **V důsledku toho je seed mnohem důležitější než samotné zařízení, které jej uchovává.**

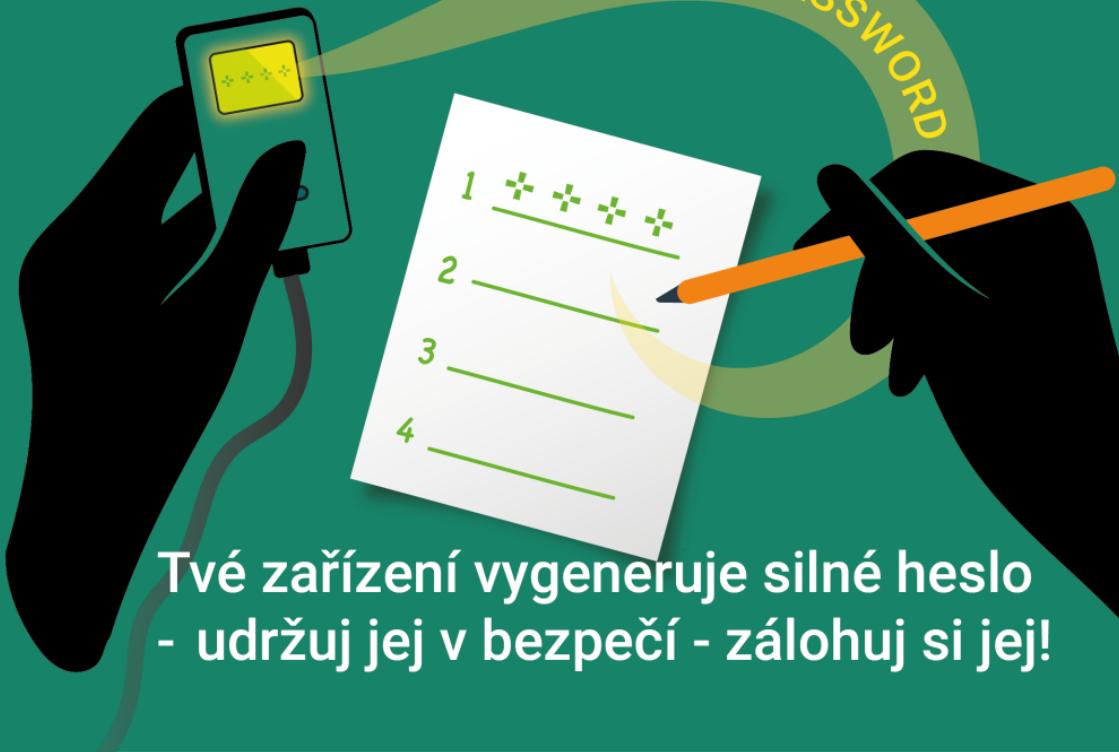
Ztratil jsi hardware penězenu? Nebo přestala fungovat? Nebo bys ji chtěl vyměnit za jiný model? Žádný problém! Stačí zadat svůj seed do nové peněz enky a získáš znova plný přístup ke svým prostředkům.

Chraň si svůj seed, protože je to jediný způsob, jak získat zpět přístup ke svým finančním prostředkům v případě, že ztratíš privátní klíč, heslo nebo hardware penězenu.

Bez seedu nenávratně ztratíš své bitcoiny a možnost je spravovat.

POZOR!

NIKDY NEVYTVAŘEJ DIGITÁLNÍ KOPII (FOTOGRAFIE, TEXTOVÁ ZPRÁVA, E-MAIL) SE SVÝM SEEDEM. NIKDY TAKÉ NEČTI NAHLAS SVŮJ SEED A NEZAPISUJ JEJ DO POČÍTAČE PŘIPOJENÉHO K INTERNETU!



Tvé zařízení vygeneruje silné heslo
- udržuj jej v bezpečí - zálohuj si jej!

SPRÁVA ZÁLOHOVÁNÍ

Proč potřebuji zálohu své obnovovací fráze (seedu)?

Jsi jediný, kdo má přístup k Tvému seedu, proto si nezapomeň vytvořit zálohu. Správa zálohy je jednoduchá a bezpečná, pokud zůstane v režimu offline.

Elektronická zařízení málodky vydrží déle než 10 nebo 20 let, proto nejsou vhodnou volbou pro dlouhodobé ukládání prostředků.

Záloha seedu poskytuje účinnou ochranu v případě chyb souvisejících s aktualizacemi softwaru a firmwaru.

Obnovení přístupu pomocí seedu trvá jen několik minut.

Zajisti, aby Tvůj seed nebyl nikdy zveřejněn, nahrán nebo umístěn na internetu. Svá hesla si nikdy nefoř a neukládej v digitální podobě!



P
A
S
S
W
O
R
D



P
A
S
S
W
O
R
D

SPRÁVA ZÁLOHOVÁNÍ

V případě poškození nebo ztráty
peněženky potřebuješ bezpečnou zálohu,
aby s k ní mohl znovu získat přístup

Hardwareová peněženka generuje obnovovací frázi (seed) offline – nikdy se z HW peněženky nenahrává na internet, protože peněženka není připojena k internetu. Díky tomu je toto zařízení mnohem bezpečnější než aplikace v telefonu nebo počítači.

Svůj seed si nikdy nefot!

Pamatuj, že fotky může někdo vidět nebo k nim získat přístup i bez Tvého vědomí!

SLOVNÍČEK POJMŮ

KOVOVÁ ZÁLOHA
trvalá kopie
obnovovací fráze
(seedu) z kovu

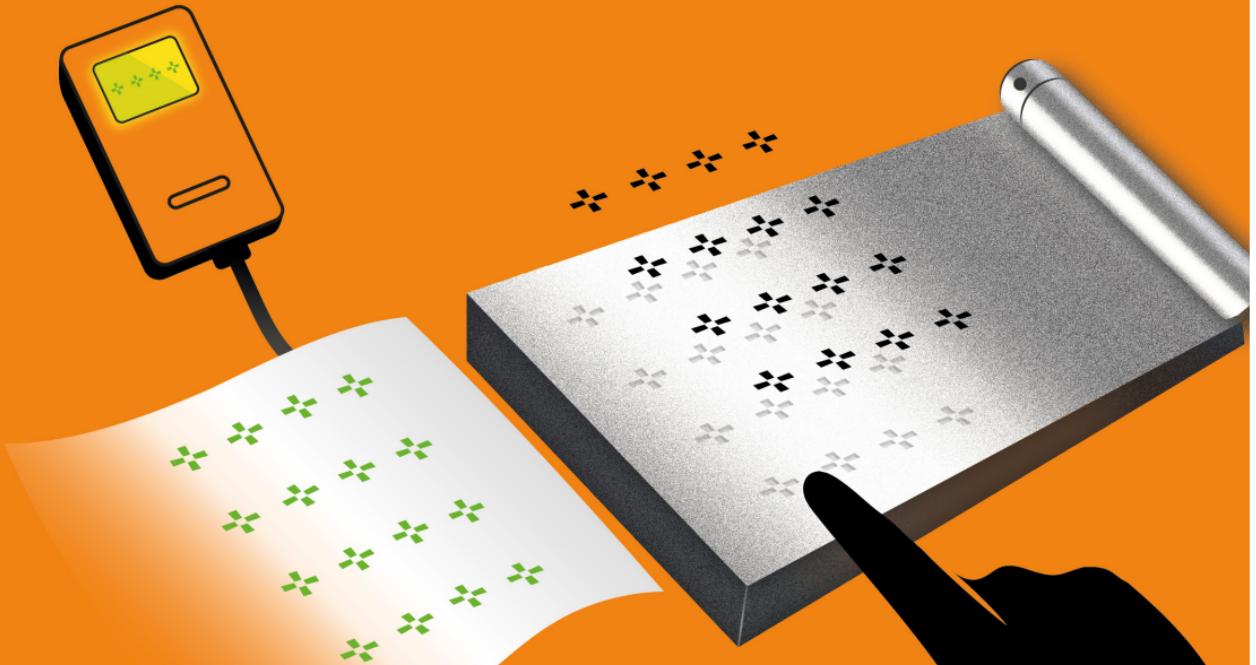
K tomuto seedu by neměl mít přístup nikdo jiný než Ty. Je uložen v šifrované paměti hardwareové peněženky od okamžiku její aktivace. Při té příležitosti byla připravena první papírová kopie Tvého seedu.

Chraň svůj seed – vytvoř si jeho trvalou kovovou zálohu.

Vytvoření takové zálohy trvá přibližně 30 minut.

Díky tomu ochráníš svůj seed před nebezpečím, jakým je voda, požár, elektrický výboj nebo fyzická degradace v průběhu času.

Zakup si hotovou kovovou zálohu nebo se podívej na online výukové programy, kde najdeš návody pro kutily. Můžeš také využít návody dostupné na youtube.com/@Cryptosteel.



Připrav si vhodné nástroje

Vytvoření kovové zálohy obnovovací fráze (seedu) zajišťuje trvanlivost a vyšší odolnost proti poškození ve srovnání s jinými způsoby ukládání.

Kovové zálohy jsou vysoce odolné vůči elektrickým šokům, ohni, vodě a fyzické degradaci v průběhu času.

KOVOVÁ ZÁLOHA JE NEJLEPŠÍM ZPŮSOBEM, JAK OCHRÁNIT SVŮJ SEED V PŘÍPADĚ NEPŘEVÍDATELNÝCH SITUACÍ.

Cryptosteel je patentovaný, snadno použitelný a mimořádně odolný nástroj.

Alternativním způsobem uchování seedu je jeho ruční vyražení na kovovou destičku ve formě teček. Tento způsob je i přes jeho velkou časovou náročnost hodně používán. Po dešifrování představují tečky privátní klíče nebo seed.

Pokud dáváš přednost levným řešením typu DIY (udělej si sám), můžeš si koupit sadu gravírovacích nástrojů, kovovou destičku a vyrýt na ni svůj seed. Toto řešení však může být méně bezpečné kvůli méně kvalitním materiálům a horší čitelnosti.



Vytvoř si kovový recovery seed

Ujisti se, že záloha Tvého seedu funguje dříve, než ji budeš skutečně za několik dní, měsíců nebo let potřebovat.

OTESTUJ SI SVOU ZÁLOHU IHNED, MÍSTO ABYS PŘEDPOKLÁDAL, ŽE JE SPRÁVNÁ.

Pro dokončení zálohování se ujisti, že Tě seed nezklame, až ho budeš nejvíce potřebovat.

TEST

- Převed' malé množství prostředků na svůj zálohovaný seed
- Resetuj zařízení
- Proved' proces obnovení

Test proběhl úspěšně, pokud máš po procesu obnovy přístup ke svým prostředkům. Gratulujieme! Tvá záloha je správně provedena a umožní Ti v budoucnu v případě potřeby obnovit přístup k Tvým prostředkům.

DŮLEŽITÉ!

Pouze otestovaná záloha zajistí budoucí přístup k Tvým prostředkům. Obnovení peněženky není možné, pokud je seed nesprávný.



Otestuj svou záložní kopii

LIGHTNING NETWORK

Lightning Network je druhá vrstva Bitcoinu. Funguje tak, že uzamyká peníze v blockchainu a vydává odpovídající částku ve vrstvě nad Bitcoinem. To umožňuje provádět bitcoinové transakce téměř okamžitě – v podstatě rychlostí Tvého internetového připojení.

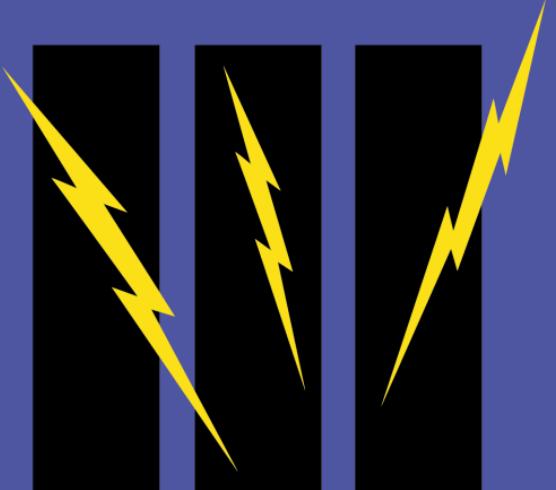
SLOVNÍČEK POJMŮ

LIGHTNING NETWORK
(zkráceně **LIGHTNING**)
druhá vrstva bitcoinové
sítě, která slouží k rychlým
a snadným transakcím.

Lightning Network vytváří přímé platební kanály mezi uživateli a umožňuje tak provádět transakce téměř v reálném čase. Není třeba potvrzovat každý převod na blockchainu. To umožňuje nižší poplatky a okamžité platby.

Lightning Network je nezávislá síť, která díky rychlým a levným transakcím usnadňuje používání Bitcoinu v každodenním životě v bezpočtu aplikací.

Lightning Network byla integrována do celé řady aplikací. Jejich sortiment je široký a dynamicky se vyvíjí, mění se podle potřeb, preferencí uživatelů a nového technologického vývoje.



LIGHTNING NETWORK

Čas nakupovat!

LIGHTNING NETWORK

STÁHNI SI APLIKACI

Aby sis mohl vyzkoušet výhody a prozkoumat možnosti Lightningu, vybrali jsme pro Tebe aplikace hot wallet (peněženka připojená k internetu), které si můžeš nainstalovat do svého chytrého telefonu. Cryptosteel doporučuje dvě možnosti: Wallet of Satoshi (pro začátečníky) a Breez (vyžaduje určité technické znalosti).

Pokud plánuješ provést své první transakce přes Lightning, je pro Tebe **Wallet of Satoshi** vhodnou volbou. Jedná se o peněženku spravovanou třetí stranou nabízející snadné použití, a proto je doporučována začínajícím uživatelům. Aplikace je připravena k použití ihned po instalaci.

Wallet of Satoshi si můžeš stáhnout z webové stránky
walletofsatoshi.com



Měl by ses však zaměřit na používání peněženky, kterou máš plně pod svou kontrolou, jakou je například **Breez**. V takovém případě zaplatíš za otevření Lightning kanálů, což Ti ale umožňuje zachovat si větší kontrolu nad svými prostředky. Pokud se rozhodneš pro aplikaci Breez, bude Ti za otevření kanálu účtován malý poplatek (obvykle menší než 21 korun).

Breez si můžeš stáhnout z oficiální webové stránky
breez.technology



Nezapomeň, že aplikace Wallet of Satoshi i Breez jsou dobré a osvědčené možnosti pro Lightning Network.



Stáhni a nainstaluj si aplikaci

V Lightningové peněžence jsou uloženy bitcoiny z Tvé hlavní peněženky. Začátečníkům doporučujeme operovat s menší částkou, aby se seznámili s fungováním Lightningu a provedli svou první transakci. Vyhraď si na to přibližně 20 minut času.

- Vygeneruj adresu pro příjem bitcoinu:
 - Klikni na tlačítko "Recieve" a vyber možnost "Bitcoin On-Chain" v peněžence Wallet of Satoshi
 - nebo "Receive via BTC Address" v aplikaci Breez.
- Zkopíruj adresu do svého počítače.
- Tuto adresu zadej do aplikace své hardwarové peněženky.
- Proveď malou transakci a počkej, dokud nebude potvrzena v blockchainu. Tento převod může trvat až hodinu nebo déle.
- Záleží na velikosti poplatků, které jsi ochoten zaplatit.
- Tvé prostředky máš nyní na své Lightningové peněžence a můžeš tedy provádět okamžité transakce.

Přesné kroky potřebné ke vkladu prostředků na Lightningovou peněženku se mohou lišit v závislosti na zvolené aplikaci. Funkčnost Lightningu je založena na základním principu plného krytí Bitcoinem. Vložením vašich prostředků do Lightningu se z vašeho bitcoinu stane vklad pro Lightning Network. Výběrem prostředků z Lightningu dojde k uvolnění příslušné rezervy do bitcoinové sítě. Veškeré náklady spojené s Lightningem jsou uváděny před potvrzením transakce.

DŮLEŽITÉ!

Bitcoinová síť je mnohem bezpečnější a vhodnější pro dlouhodobé ukládání prostředků. Doporučujeme proto pravidelný výběr bitcoinů z Lightningu a jejich převod na On-chain.



Nabij si svou lightningovou peněženku

LIGHTNING NETWORK

PLAŤ A PŘIJÍMEJ

To nejlepší jsme si nechali na konec. Nyní si můžeš vyzkoušet, jak rychlé a levné jsou transakce přes Lightning. Níže uvedená doporučení Ti umožní bitcoiny nejen utrácet, ale také vydělávat.



www.bitrefill.com

Bitrefill poskytuje velký výběr kupónů, poukázk a dárkových karet k okamžitému nákupu v některých z největších internetových obchodů, maloobchodů a online službách.



shopinbit.com

ShopinBit nabízí více než 800 000 produktů, které si lze zakoupit prostřednictvím Lightningu, včetně mobilních telefonů, notebooků, hodinek, videoher a dalšího zboží.

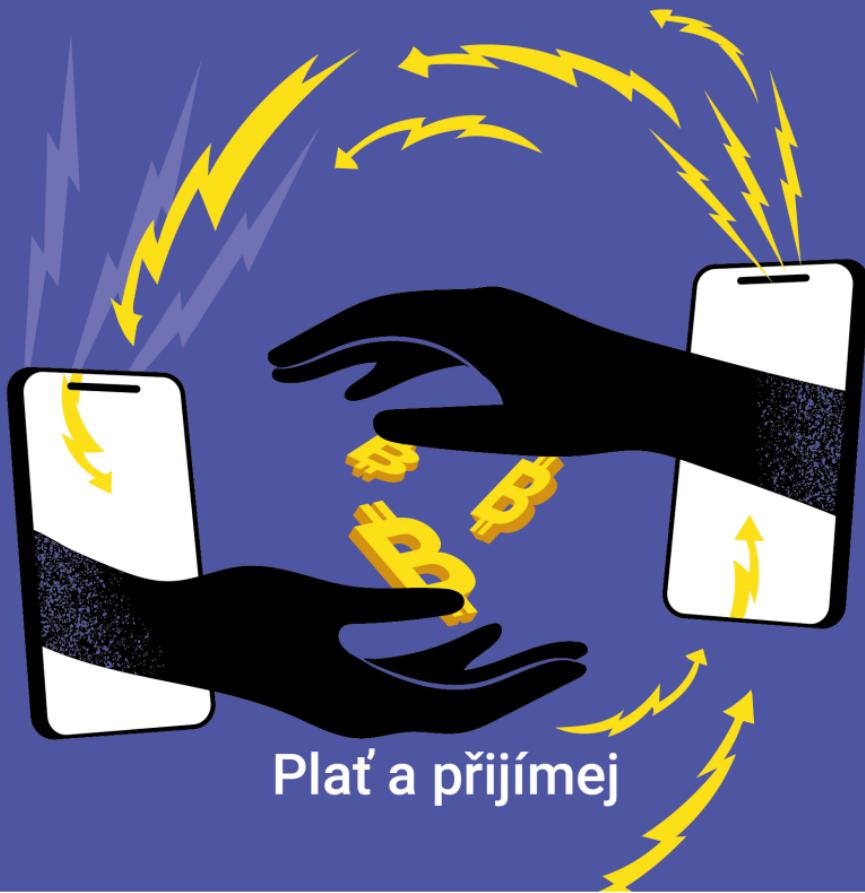
Společnost THNDR vyvinula sérii mobilních her, za jejichž hraní vyplácí odměny v Lightningu. Vyzkoušejte si na svém chytrém telefonu hry Bitcoin Bounce, Bitcoin Bay, Turbo 84, Bitcoin Snake, Tetro Tiles, Club Bitcoin: Solitaire.



www.thndr.games

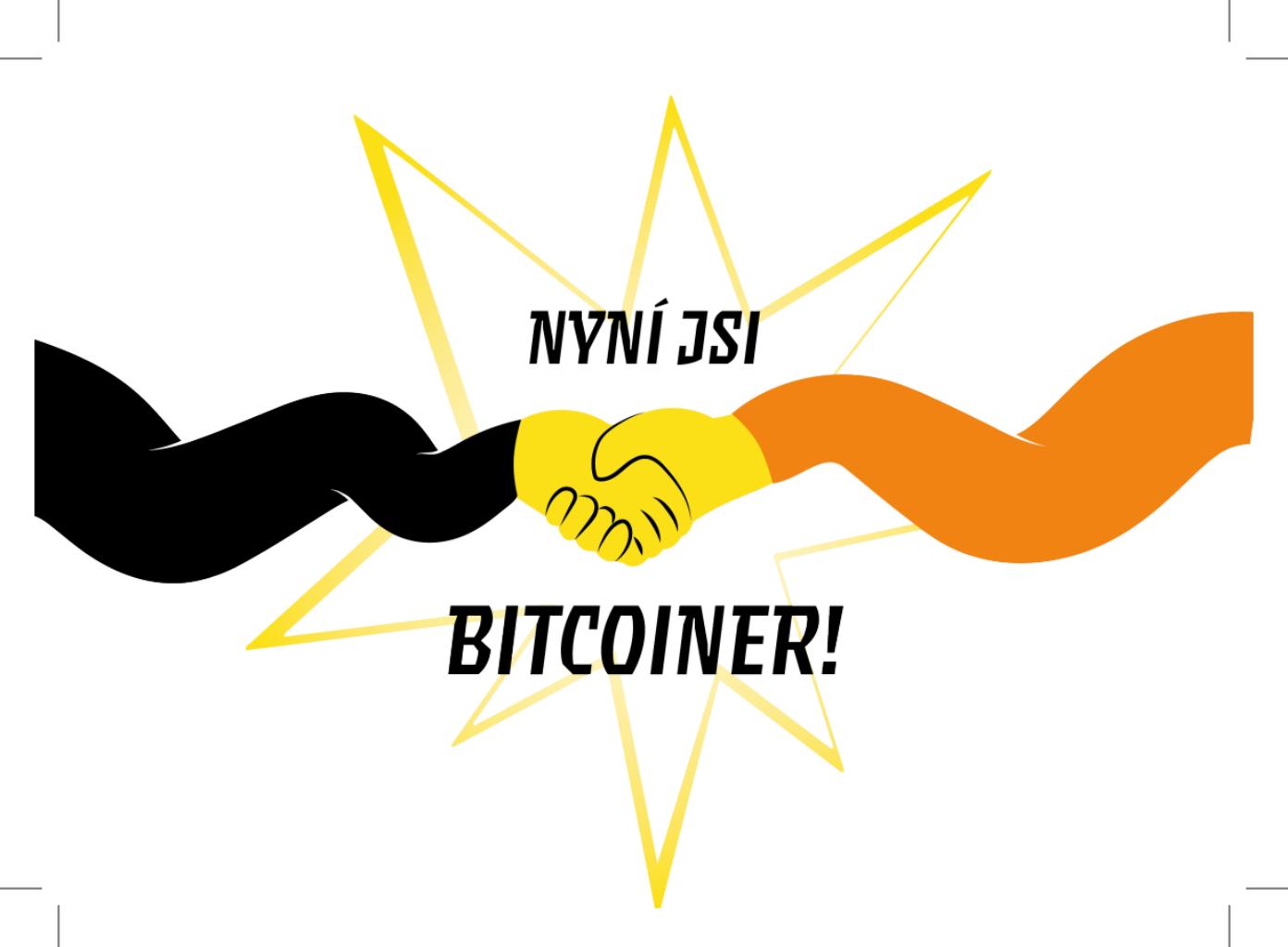
Nostr je budoucnost sociálních médií s otevřeným protokolem. Je odolný vůči ценziře a zajistuje globálně decentralizované publikování na webu. Pomocí Lightningu si mohou jeho uživatelé mezi sebou posílat drobné částky (zapy).





Plat' a přijímej

Protože už víš, jak s Bitcoinem pracovat...



NYNÍ JSI

BITCOINER!

Special thanks to:

Mutant LetterPress, Mariusz Mamcarz, Vlad Costea, Gracjan Pietras, Kateřina Polášková,
JesterHodl.com, Joko and btc21.de

Tato kniha s otevřeným zdrojovým kódem s názvem „Bitcoin User Manual“ (dále jen „Kniha“) je navržena tak, aby poskytovala obecné informace o předmětu, kterým je bitcoin a kryptoměny. Zde se rozumí, že autoři, přispěvatelé, jejich přidružené subjekty a žádní interní nebo třetí poskytovatelé služeb (souhrnně označovaní jako „strany“) neposkytují právní, finanční, investiční ani žádné jiné profesionální rady nebo služby Všechny názory, interpretace, prohlášení nebo tvrzení obsažená v Knize jsou vyhradně názory autora (autori) a přispěvatelů a nemusí nutně reprezentovat ani odrážet názory stran. Strany se výslovně zřikají jakékoli prohlášení nebo záruk, výslovné nebo předpokládané, včetně, ale bez omezení, záruk vhodnosti pro konkrétní účel, prodejnosti a neporušení práv. Kniha je poskytována výhradně pro vzdělávací a informační účely. Informace obsažené v tomto dokumentu nepředstavují nabídku, žádost, doporučení, podporu nebo radu k nákupu, prodeji nebo držení bitcoinů, jakýchkoli jiných kryptoměn nebo cenných papírů nebo jiných finančních nástrojů ve Spojených státech nebo v jakékoli jiné jurisdikci. Takové informace, pokud jsou interpretovány jako žádost nebo nabídka, jsou nezákonní a nejsou zamýšleny stranami. Nic v Knize by nemělo být vykládáno jako poskytování právního, daňového, investičního, finančního nebo jakékoli jiné formy odborného poradenství. Autoři a přispěvatelé Knihy nejsou certifikovanými investičními poradci. Jakékoli minulé výkony, historická data, anekdoty nebo příklady uvedené v knize by neměly být interpretovány jako orientační nebo příslib budoucích výsledků. Autor (autori) a strany prostřednictvím Knihy neposkytují personalizované právní, daňové, finanční nebo investiční poradenství. Poskytnuté informace nejsou určeny k tomu, aby byly použity jako jediný základ pro jakákoliv investiční rozhodnutí, ani by neměly být vykládány jako rady navržené tak, aby vyhovovaly konkrétním potřebám jednotlivce nebo subjektu. Investice do bitcoinu a dalších kryptoměn s sebou nese vlastní riziko, včetně rizika ztráty celé investice. Strany neprohlašují, nezaručují ani nenaznačují, že služby nebo metody obsažené v Knize zabrání čtenáři ve ztrátě investic. Čtenáři se durazně doporučuje, aby si před jakýmkoli investičním rozhodnutím vyzádal rady příslušného profesionálního poradce. Strany nepřebírají žádnou odpovědnost za chyby, opomenutí nebo opačný výklad předmětu tohoto dokumentu a nebudou odpovědné za žádné přímé, nepřímé, následné, zvláštní, exemplární nebo jiné škody z toho vyplývající. Toto vyloučení odpovědnosti se řídí a vykládá v souladu se zákony jurisdikce, ze které je Kniha přístupná, bez ohledu na jakýkoli konflikt zákonů. Jakýkoli spor vzniklý nebo související s vaším používáním Knihy bude posouzenou příslušným státním nebo federálním soudem v uvedené jurisdikci a tímto s takovou jurisdikcí souhlasíte. Vstupem do Knihy nebo jejím používáním potvrzujete a souhlasíte s tím, že jste si přečetli, porozuměli a přijali tyto podmínky. Pokud s těmito podmínkami nesouhlasíte, doporučujeme vám Knihu nečíst ani ji nepoužívat. Vaše používání Knihy svobodně a bez jakékoli formy kompenzace představuje souhlas s těmito podmínkami.

SHOPINBIT



WASABI WALLET



Satsback.com



BitBox

BTCTKVR

LEDGER

chaincamp



Blockstream



SATOSHILABS

POLISH
BITCOIN
ASSOCIATION
EST 2013

SEYSER

btc prague



WALLET
OF SATOSHI

Bitrefil

THNDR





cryptosteel