Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Využití jednodeskových počítačů jako uzel v Lightning Network

Barbora Vinczeová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Barbora Vinczeová

Informatika

Název práce

Využití jednodeskových počítačů jako uzel v Lightning Network

Název anglicky

Use of single-board computers as a node in the Lightning Network

---

Cíle práce

Bakalářská práce je tematicky zaměřena na problematiku kryptoměn.
Hlavním cílem práce je zhodnotit možnosti využití jednodeskových počítačů jako Lightning uzel.

Dílčí cíle práce jsou:
- charakterizovat problematiku jednodeskových počítačů a Lightning uzlu.
- analyzovat stávající řešení,
- formulovat doporučení.

Metodika

Teoretická část bakalářské práce se bude zakládat na analýze a rešerši odborných zdrojů.

V praktické části budou analyzovány jednodeskové počítače a zhodnocena jejich vhodnost pro potřeby Lightning uzlu.

Na základě syntézy teoretických poznatků a výsledků praktické časti budou formulovány závěry práce.

Doporučený rozsah práce

30–40 stran

Klíčová slova

Bitcoin, Blockchain, Lightning Network, node, jednodeskové počítače, kryptoměny.

Doporučené zdroje informací

BLUM, Jeremy. Exploring Arduino: tools and techniques for engineering wizardry. Second edition. Indianapolis: Wiley, [2020]. ISBN 978-1-119-40537-5.

LIN, Shaofeng, Yihan KONG a Shaotao NIE. Overview of Block Chain Cross Chain Technology. In: 2021 13th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA) [online]. IEEE, 2021, 2021, s. 357-360 [cit. 2022-08-10]. ISBN 978-1-6654-3892-6. Dostupné z: doi:10.1109/ICMTMA52658.2021.00083

MONK, Simon. Raspberry Pi cookbook: software and hardware problems and solutions. Third edition. Sebastopol: O'Reilly Media, 2019. ISBN 978-1-4920-4322-5.

Předběžný termín obhajoby

2023/24 LS – PEF

Vedoucí práce

Ing. Michal Stočes, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 11. 8. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 14. 03. 2024

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Využití jednodeskových počítačů jako uzel v Lightning Network" jsem vypracovala samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autorka uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2024 _____

Poděkování

Ráda bych touto cestou poděkovala vedoucímu práce Ing. Michalu Stočesovi Ph.D., za jeho cenné a velmi užitečné rady k vypracování této bakalářské práci. Mé poděkování patří i celé rodině a všem ostatním za veškerou podporu při psaní.

Využití jednodeskových počítačů jako uzel v Lightning Network

Abstrakt

Bakalářská práce se zabývá problematikou využití jednodeskových počítačů jako uzel pro ověřování transakcí v kryptoměnové síti Lightning Network. Teoretická část práce se zaměřuje na analýzu a rešerši jednodeskových počítačů, kryptoměny Bitcoin a vícekriteriální analýzy variant. Praktická část práce se zaměřuje na zhodnocení jednodeskových počítačů pro využití jako uzel v Lightning Network síti. Pro jejich vhodnost jsou provedeny zátěžové testy, kdy jejich výsledky slouží jako podklad pro vícekriteriální analýzu variant. Na základě výsledků analýzy je provedena implementace Lightning Network uzlu na jednodeskovém počítači.

Klíčová slova: Bitcoin, Blockchain, Lightning Network, node, jednodeskové počítače, kryptoměny

Use of single-board computers as a node in the Lightning Network

Abstract

The bachelor's thesis explores the issue of using single-board computers as nodes for verifying transactions in the Lightning Network. The theoretical part of the thesis focuses on the analysis and research of singleboard computers, the cryptocurrency Bitcoin, and multicriteria analysis of options. The practical part of the thesis is focused on evaluating single-board computers for use as nodes in the Lightning Network. Benchmark tests are conducted to assess their suitability, with the results serving as a basis for multicriteria analysis of options. Based on the results of the analysis, an implementation of a Lightning Network node on a single-board computer is carried out.

Keywords: Bitcoin, Blockchain, Lightning Network, node, single board computers, cryptocurrencies

Obsah

1 Úvod

Kryptoměny v dnešní době získávají stále větší popularitu a elektronické finanční transakce se stávají neodmyslitelnou součástí běžného života, tím tak nabývá síť Lightning Network klíčovou pozici v rychlém a efektivním provádění kryptoměnových transakcí. Tato bakalářská práce se zaměřuje na inovativní využití jednodeskových počítačů jako uzlů v síti Lightning Network. Kombinace technologií kryptoměn a jednodeskových počítačů otevírá nové perspektivy v oblasti decentralizovaného financování a umožňuje jednotlivcům přispívat k chodu sítě Lightning Network. Cílem této práce je provést důkladnou analýzu a zhodnocení výkonnosti těchto jednodeskových počítačů ve funkci uzlů v rámci sítě Lightning Network.

S ohledem na rostoucí význam sítě Lightning Network, která slouží k odlehčení hlavního blockchainu Bitcoinu tím, že umožňuje provádět transakce mimo hlavní řetězec. Tím vzniká klíčová otázka výběru optimálního hardwaru pro uzly této sítě. Výběr vhodného jednodeskového počítače je zásadní pro efektivní a spolehlivé fungování uzlu, což má přímý dopad na rychlost a bezpečnost transakcí v síti. V této práci jsou proto porovnávány různé modely jednodeskových počítačů z hlediska jejich výkonnosti, aby se identifikovaly jejich silné a slabé stránky v kontextu použití v Lightning Network. Toto porovnání poskytuje cenné informace pro rozhodování o tom, který hardware je nejvhodnější pro zřízení uzlu v rámci této rychle se rozvíjející sítě.

2 Cíl práce a metodika

Cíl práce

Hlavním cílem práce je zhodnotit možnosti využití jednodeskových počítačů jako Lightning uzel.

Dílčí cíle práce jsou:

- charakterizovat problematiku jednodeskových počítačů a Lightning uzlu,
- analyzovat stávající řešení,
- formulovat doporučení.

Metodika

Teoretická část bakalářské práce se bude zakládat na analýze a rešerši odborných zdrojů. V praktické části budou analyzovány jednodeskové počítače, zhodnocena jejich vhodnost pro potřeby Lightning uzlu pomocí vícekriteriální analýzy variant a následně pro ověření výsledků provedena implementace Lightning uzlu na jednodeskovém počítači. Na základě syntézy teoretických poznatků a výsledků praktické časti budou formulovány závěry práce.

3 Teoretická východiska

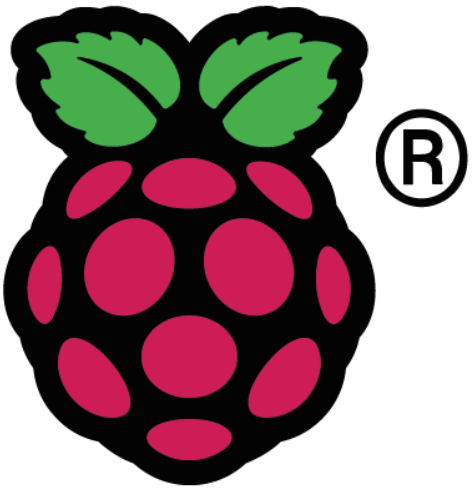
3.1 Jednodeskové počítače

Jednodeskové počítače jsou revolučním krokem v evoluci počítačových technologií. Tato kompaktní, ale výkonná zařízení, která sjednocují všechny základní komponenty počítače na jednom obvodovém panelu, představují zlom v přístupu k výpočetní technice, který se odlišuje od tradičních stolních a přenosných počítačů. Původně byly jednodeskové počítače vyvíjeny jako nástroje pro vzdělávání a hobby projekty, ale jejich význam rychle narůstal a dnes se tyto počítače využívají v široké škále aplikací od domácích multimediálních center, přes průmyslové ovládací systémy, až po výzkumné platformy pro vědecké experimenty. Vývoj jednodeskových počítačů byl poháněn potřebou snížit náklady, zmenšit fyzickou velikost a zároveň zachovat dostatečný výkon pro rozmanité aplikace. Tento trend nastartoval rozmach internetu věcí, kde jsou jednodeskové počítače ideálními kandidáty pro inteligentní ovládací jednotky díky své schopnosti komunikovat s různými senzory a aktuátory v reálném čase. [1] [2]

Historie jednodeskových počítačů sahá až do 70. let 20. století, kdy byly vyvíjeny především pro vzdělávací účely a pro technologické nadšence. Původní myšlenkou bylo vytvořit zařízení, které by bylo jak dostupné, tak dostatečně výkonné pro základní výpočetní úlohy. Během následujících dekád se jednodeskové počítače postupně vyvíjely a stávaly se stále dostupnějšími a výkonnějšími. Klíčovým momentem v jejich historii bylo uvedení Raspberry Pi v roce 2012, které sice znamenalo významný mezník, ale bylo pouze jedním z mnoha kroků v dlouhé evoluci těchto zařízení. Jednodeskové počítače se rychle staly populárními nejen v oblasti vzdělávání a hobby projektů, ale také začaly pronikat do průmyslových aplikací, domácí automatizace, a dokonce i do výzkumných a vývojových projektů. Flexibilita tohoto typu počítačů, možnost programování, přizpůsobení podle specifických potřeb uživatelů a relativně nízké náklady na výrobu a pořízení umožnily jejich široké rozšíření a aplikaci v mnoha různých odvětvích. V posledních letech je lze nalézt v zařízeních od jednoduchých domácích asistentů až po složité průmyslové řídicí systémy, což poukazuje na jejich všestrannost a význam v současném technologickém světě. [1] [2] [3]

3.1.1 Počítač Raspberry Pi

Raspberry Pi, představený nadací Raspberry Pi Foundation, nabízí cenově dostupný, kreditní kartou velikostně srovnatelný počítač, který se snadno připojí k monitoru nebo televizi a ovládá se běžnou klávesnicí a myší. Jedná se o schopné zařízení, které umožňuje lidem všech věkových skupin prozkoumávat oblast výpočetní techniky a učit se programovat v jazycích jako je Scratch a Python. Raspberry Pi je schopné provádět vše, co se očekává od klasického stolního počítače, ať už jde o prohlížení internetu, přehrávání videí ve vysokém rozlišení, tvorbu tabulek, zpracování textu nebo hraní méně náročných her. [4]

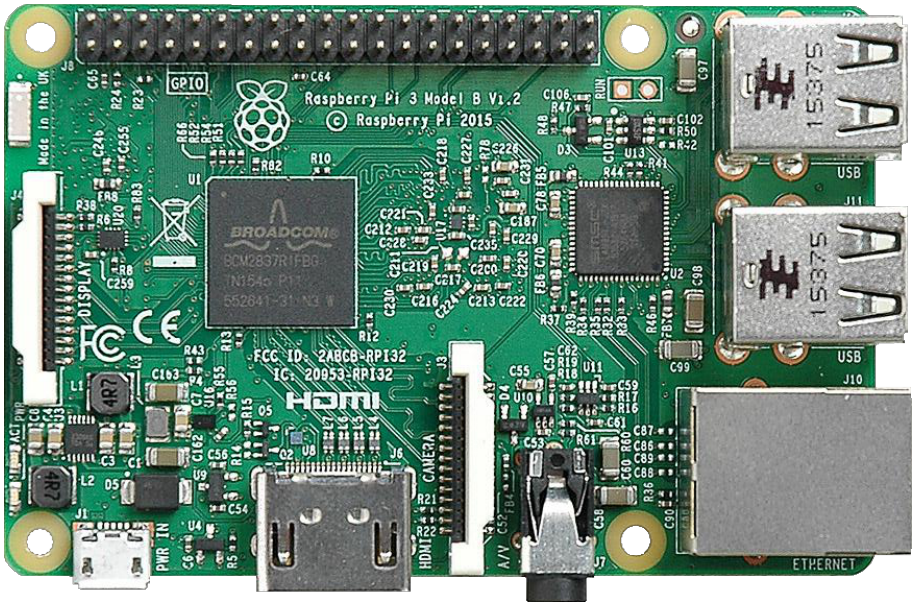


Obrázek 1: Logo Raspberry Pi Foundation [5]

„Počítač Raspberry Pi je dostatečně levný, aby si jej děti mohly koupit za několikatýdenní kapesné, a všechno příslušenství, které ke své činnosti vyžaduje, již v domácnosti pravděpodobně najdete: televizor, kartu SD, kterou lze vytáhnout ze starého fotoaparátu, nabíječku mobilních telefonů, klávesnici a myš. Nepůjčují si jej všichni členové rodiny, ale patří jen dítěti a je dostatečně malý, aby jej dítě mohlo vzít do kapsy a přenést ke kamarádovi. Když se něco pokazí, nic se neděje – stačí vyměnit paměťovou kartu za novou a Raspberry Pi funguje stejně jako po zakoupení. Chcete-li se pustit na dlouhou cestu, na jejímž konci dokážete svůj počítač Raspberry Pi programovat, máte všechny potřebné nástroje, funkce a výukové materiály k dispozici hned poté, co počítač zapnete.“ [6]

Raspberry Pi 3

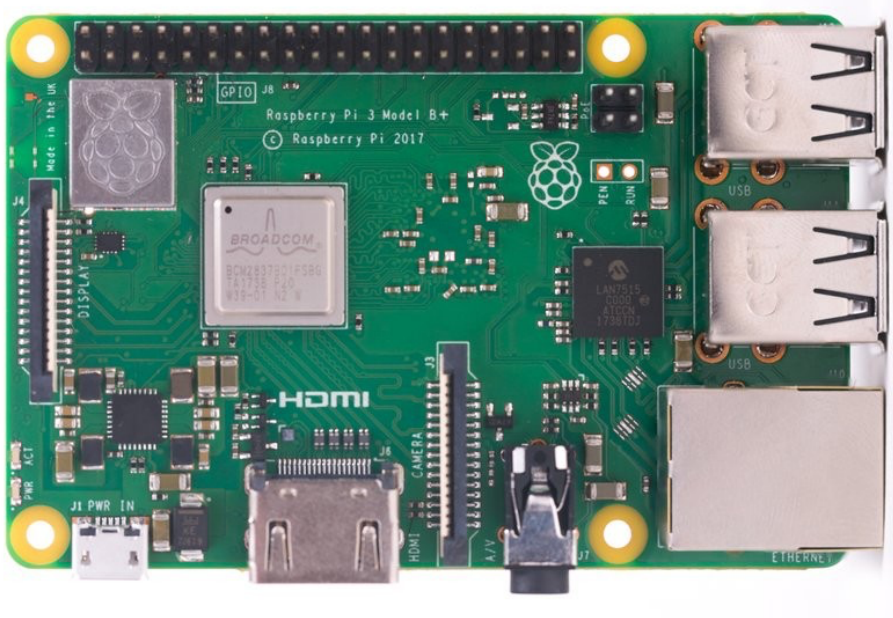
Raspberry Pi 3 představuje významný milník ve vývoji jednodeskových počítačů, přinášejíc výkonnější a univerzálnější platformu. Jeho hlavní a první model, Raspberry Pi 3 Model B, představený v roce 2016 nabídl výrazné vylepšení předešlého modelu s čtyřjádrovým procesorem Broadcom BCM2837 o taktu 1,2 GHz a 1 GB operační paměti splňující standard LPDDR2, což umožnilo rozšířit jeho použitelnost na náročnější aplikace a projekty. Bezdrátové připojení tento model řeší pomocí integrované podpory standardu Wi-Fi 802.11n na pásmu 2,4 GHz a Bluetooth 4.1. Není tedy třeba využívat dalších externích komponent. S rozhraním GPIO poskytujícím 40 pinů, plně funkčním HDMI portem schopným přenášet video až v rozlišení Full HD, 4 USB 2.0 porty pro připojení periferií, Ethernet portem s rychlostí dosahujícím až 100 Mbit/s pro kabelové připojení k internetu a slotem pro microSD kartu pro úložiště se Raspberry Pi 3 Model B stal velmi flexibilním nástrojem. Díky těmto technickým parametrům a pokročilým verzím použitých technologií zaznamenal model velký úspěch mezi vývojáři, učiteli a technologickými nadšenci pro jeho schopnost zvládat složitější výpočetní úkoly. [7]



Obrázek 2: Počítač Raspberry Pi 3 model B [8]

Raspberry Pi 3 Model B+ je dalším významným modelem řady, který byl uveden na trh po původním Modelu B v roce 2018. Tento model přinesl řadu vylepšení a aktualizací, které zvýšily jeho výkon. Počítač nabízí vyšší frekvencí procesoru, která byla zvýšena z původních 1,2 GHz na 1,4 GHz, a vylepšenou konektivitou, včetně rychlejšího Ethernet portu s rychlostí až 300 Mbit/s a pokročilejší Wi-Fi splňující standard 802.11ac na 2,4 GHz

a 5 GHz pásmech. Model B+ tímto vylepšením poskytl uživatelům ještě lepší zážitek. Navíc byla zlepšena energetická efektivita a teplotní management, což umožnilo tomuto modelu zvládat náročnější operace s lepší stabilitou. [9] [10]



Obrázek 3: Počítač Raspberry Pi 3 model B+ [11]

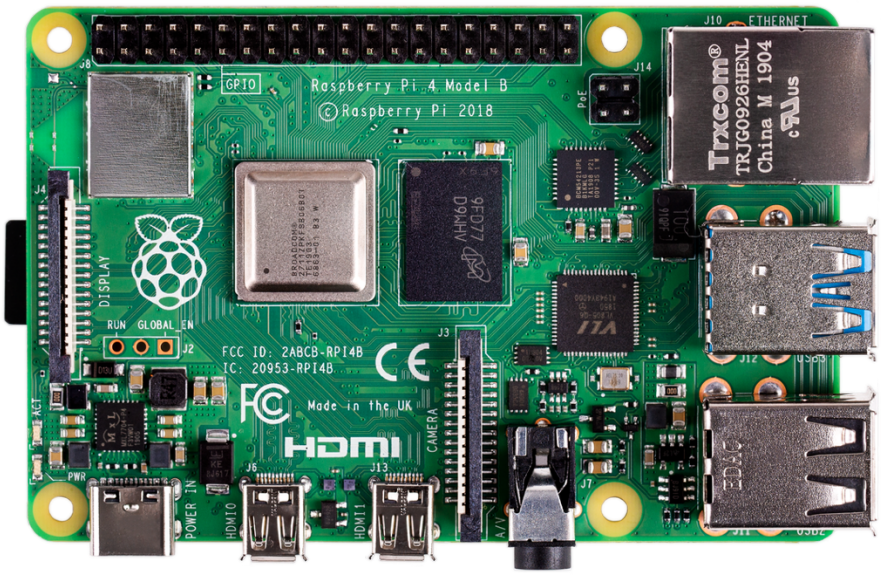
Kromě Modelu B a B+ řada Raspberry Pi 3 zahrnovala i Model A+, který nabízel menší formát a nižší cenu i při zachování klíčových vlastností hlavního modelu. Ačkoliv Model A+ disponoval nižší pamětí RAM a menší konektivitou, jeho kompaktní rozměry a efektivita ho činily ideálním pro projekty, kde byl kladen důraz na velikost a energetickou účinnost. [10]

Raspberry Pi 3 položilo základy pro rozvoj a inovace v oblasti jednodeskových počítačů, přičemž jeho různé modely umožnily uživatelům vybrat si variantu nejvhodnější pro jejich specifické projekty a aplikace. Příchod těchto modelů nejenže rozšířil možnosti použití Raspberry Pi v širším spektru aplikací, ale také připravil půdu pro budoucí generace, které by dále posunuly hranice výkonu, konektivity a různorodosti použití. [7]

Raspberry Pi 4

V roce 2019 byl na trh uvedený model Raspberry Pi 4 Model B, představující první model z generace řady Raspberry Pi 4. Tento model nabízí čtyřjádrový procesor Broadcom BCM2711 s taktem až 1,5 GHz a v době vydaní byl dostupný ve variantách s 1, 2 nebo 4 GB operační paměti. V polovině roku 2020 byla z trhu stažena verze s 1 GB RAM a představena nová verze

s 8 GB. Operační paměť má standard LPDDR4 a pracuje až na frekvenci 3 200 MHz. Model B se vyznačuje rozšířenými možnostmi připojení, včetně 2 microHDMI portů pro připojení 2 monitorů v rozlišení až 4K a s dekódování obrazu ve standardu HEVC/H.265, dvou USB 3.0 portů, dvou USB 2.0 portů, Gigabit Ethernet portu, integrované Wi-Fi využívající standard IEEE 802.11.b/g/n/ac na pásmech 2,4 GHZ a 5 GHz a Bluetooth 5.0. [12]



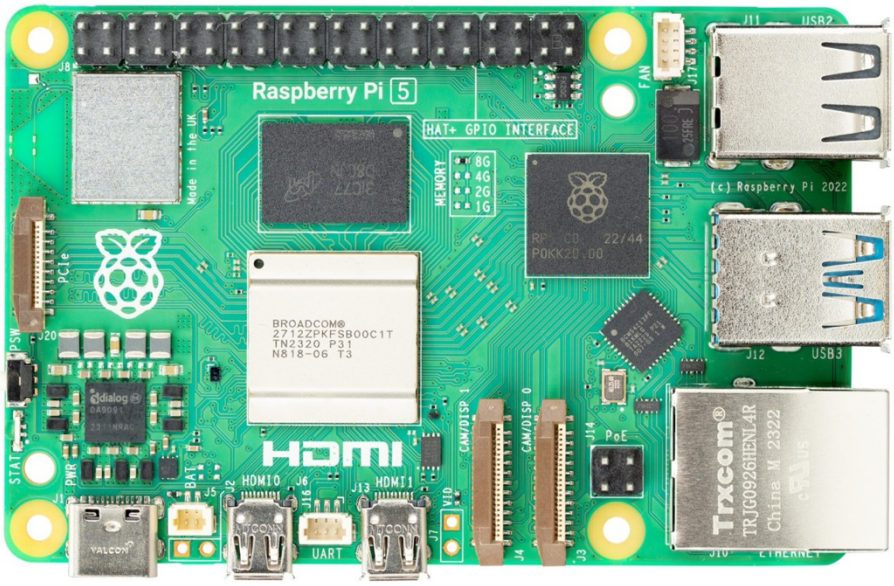
Obrázek 4: Počítač Raspberry Pi 4 model B [13]

Raspberry Pi 5

V druhé polovině roku 2023 byl uvedený na trh nový model s označením Raspberry Pi 5, který představuje další evoluční krok v řadě Raspberry Pi. Jedná se o nejvýkonnější zařízení, které nadace představila. Tento nejnovější počítač přináší řadu vylepšení a inovací, které rozšiřují jeho použitelnost a výkonnost. Jedním z nejvýznamnějších vylepšení je pokročilejší 64bitový čtyřjádrový procesor Arm Cortex-A76 s frekvencí 2,4 GHz, který přináší 2x-3x vyšší výpočetní výkon společně s výrazným nárustem grafického výkonu díky 800MHz grafickému procesoru VideoCore VII. Tato změna je zvláště důležitá pro aplikace vyžadující intenzivní výpočetní práci, jako jsou pokročilé výpočty, strojové učení a zpracování obrazu. Na rozdíl od svého předchůdce podporuje dva monitory připojené přes microHDMI porty současně v rozlišení až 4K s podporou HDR. Kromě vyššího výkonu procesoru byla také u prvního vydaní zvýšena kapacita operační paměti z původních 4 GB na 8 GB. Operační paměť splňuje standard LPDDR4X a pracuje až na frekvenci 4 267 MHz. Raspberry Pi 5 dále pokračuje v tradici vylepšování konektivity, nabízí lepší Wi-Fi připojení

s podporou nejnovějšího standardu Wi-Fi 6 a standardu Wi-Fi 802.11ac na pásmech 2.4 a 5 GHz, což zajišťuje rychlejší a stabilnější bezdrátové připojení. Kromě toho udržuje podporu pro Gigabit Ethernet a vylepšuje portovou nabídku o rychlejší USB 3.0 porty s rychlostí až 5 Gbit/s. Dalším významným rozšířením Raspberry Pi 5 je jeho zdokonalená podpora pro aplikace využívající umělou inteligenci a strojové učení. Tento model je vybaven speciálními hardwarovými a softwarovými vylepšeními, které optimalizují běh AI algoritmů. [14]

Navzdory těmto rozšířením a vylepšením si Raspberry Pi 5 i nadále zachovává základní filozofii Raspberry Pi – nabízet výkonný, ale cenově dostupný počítač, který je přístupný širokému spektru uživatelů. Díky těmto vlastnostem zařízení posouvá hranice toho, co je možné dosáhnout s jednodeskovým počítačem, a stává se lákavou volbou pro řadu aplikací, od domácích projektů přes průmyslové využití až po použití ve výzkumech. [14]

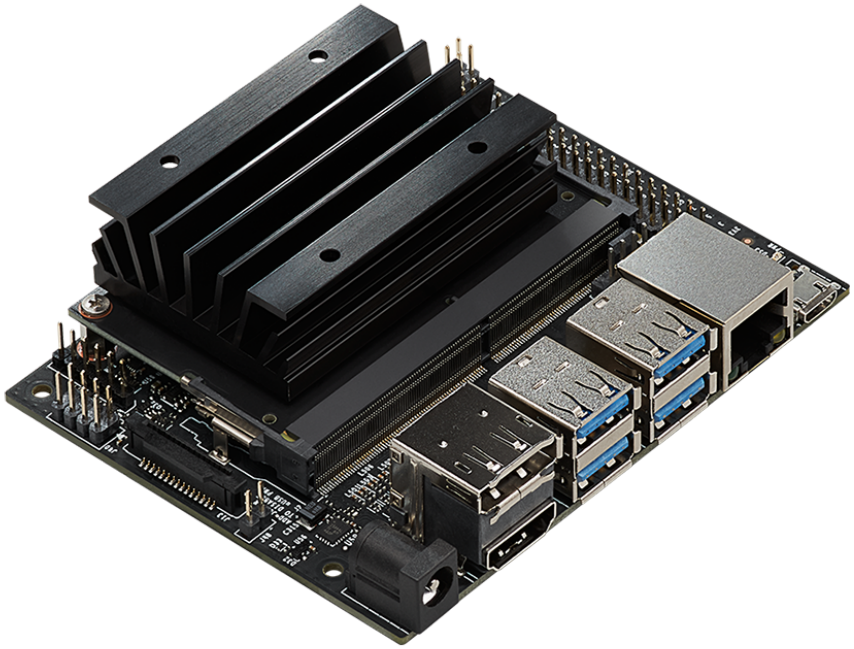


Obrázek 5: Počítač Raspberry Pi 5 [15]

3.1.2 Počítač Jetson Nano

Jetson Nano je kompaktní počítačová platforma vyvíjená společností NVIDIA určená pro vývoj a nasazení aplikací umělé inteligence a strojového učení na koncových zařízeních. Se 128jádrovým grafickým procesorem NVIDIA Maxwell poskytuje Jetson Nano výjimečný výpočetní výkon přesahující půl teraflops, čímž umožňuje uživatelům spouštět moderní AI

modely v reálném čase přímo na zařízení. Tento výkon je doplněn čtyřjádrovým procesorem ARM Cortex-A57. Jetson Nano je vybaveno 4 GB LPDDR4 paměti. Zařízení podporuje microSD karty až do velikosti 128 GB. Co se týče konektivity, Jetson Nano nabízí gigabitový Ethernet, čtyři USB 3.0 porty, HDMI a DisplayPort výstup, 2 MIPI-CSI konektory pro připojení kamery a M.2 Key E konektor pro připojení síťové karty. Pro softwarovou podporu je Jetson Nano kompatibilní s NVIDIA JetPack SDK, což je komplexní balíček, který obsahuje operační systém založený na Linuxu, akcelerované výpočetní knihovny CUDA-X a podporu pro cloudové AI služby. Tato podpora umožňuje vývojářům efektivně vytvářet a nasazovat aplikace, které využívají hluboké učení a umělou inteligenci. [16]



Obrázek 6: Počítač Jetson Nano [17]

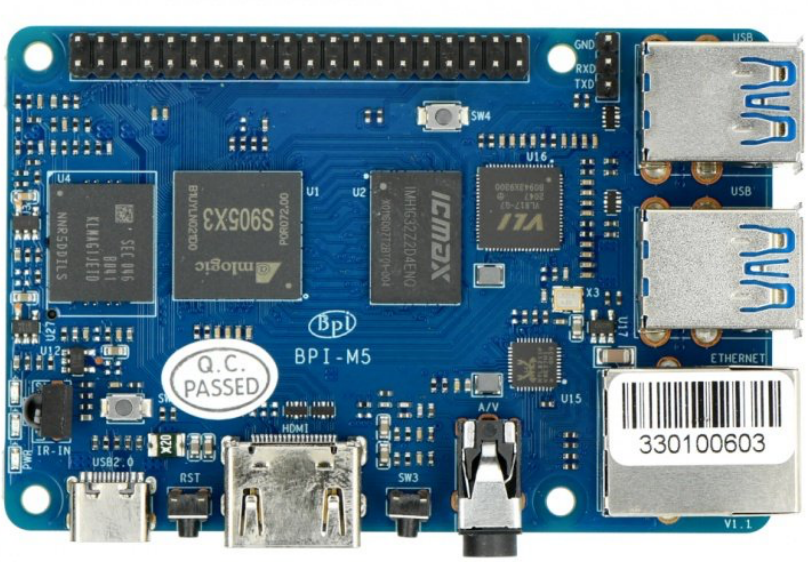
Díky svým schopnostem se Jetson Nano stalo populárním ve světě makerů, ve vzdělávacích institucích a mezi malými podniky pro širokou škálu aplikací, včetně autonomních robotů, systémů rozpoznávání obrazu a inteligentních kamer. Jeho dostupnost, flexibilita a schopnost zvládnout pokročilé úkoly zpracování AI přímo na zařízení bez potřeby cloudové konektivity činí z Jetson Nano ideální platformu pro inovátory a vývojáře, kteří chtějí přesunout hranice možností v oblasti edge computing. [16]

3.1.3 Počítač Banana Pi

Banana Pi je hardwarový projekt s otevřeným zdrojovým kódem, který vede společnost GuangDong BiPai Technology Co., LTD. Projekt se zaměřuje na vývoj desek pro procesory s ARM architekturou a pro mikrokontrolery. Nabízí otevřené softwarové a hardwarové platformy, a tím tak vytváří základní platformy pro technologický vývoj. Nabízí širokou škálu produktů, které integrují hardwarové prostředky pro zpracování hlasu, dat a videa. Vývojáři mají možnost na této hardwarové platformě flexibilně vytvářet různé aplikace. Banana Pi lze využít v oblastech jako je internet věcí, umělá inteligence, průmyslové řízení přes internet, STEAM vzdělávání a další. Snaží se vytvořit ekosystém otevřené komunity a celková technická řešení pro internet věcí. [18]

Banana Pi M5 je výkonný jednodeskový počítač osazený čtyřjádrovým procesorem Amlogic S905X3 Cortex-A55, pracujícím na frekvenci až 2,0 GHz. Jeho výkon je dále podpořen 4GB operační pamětí se standardem LPDDR4 a 16GB eMMC úložištěm, což poskytuje dostatek prostoru a rychlosti pro operace systému a aplikací. K dispozici jsou také čtyři USB 3.0 porty pro rychlé připojení externích zařízení. [19]

Zařízení je vybaveno pouze gigabitovým Ethernet portem a bezdrátová komunikace je řešena buď pomocí dedikované Wi-Fi a BT desky připojené přes GPIO piny nebo pomocí USB dongle. Díky tomuto je zařízení možné využívat Wi-Fi připojení se standardem IEEE 802.11a/b/g/n/ac a Bluetooth verze 5.0. Pro připojení monitoru zde poslouží konektor HDMI 2.1 s rozlišením až 4K s podporou HDR. Grafické zpracování zajišťuje grafický procesor Mali-G31, který spolu s podporou operačních systémů Android a Linux otevírá široké spektrum možností využití od multimediálních aplikací přes vývoj softwaru až po pokročilé výpočetní projekty. [19]

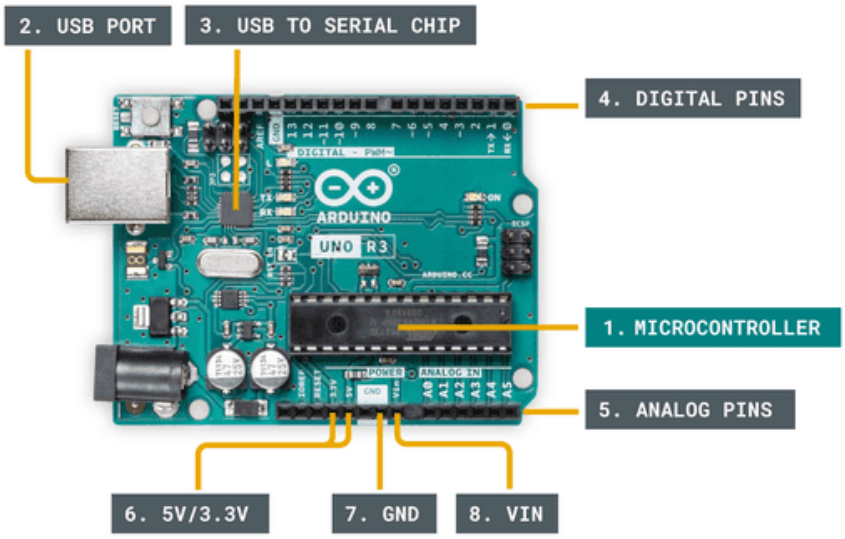


Obrázek 7: Počítač Banana Pi M5 [20]

3.1.4 Mikrokontroler Arduino

Od svého zrodu v roce 2005 se Arduino stalo jednou z nejvýraznějších značek ve světě elektroniky a návrhu vestavěných systémů. Rodina Arduino zahrnuje širokou škálu mikrokontrolerových desek, které se liší svými výkonnostními charakteristikami, velikostí a cenou. Mezi nejznámější modely se řadí Arduino Uno, které je často považován za vstupní bod pro začátečníky, Arduino Mega, které nabízí více I/O pinů a paměti pro náročnější projekty, a Arduino Nano, oblíbené pro jeho kompaktní velikost ideální pro integrované aplikace. [21]

Ačkoliv se všechny desky Arduino od sebe liší, existuje několik klíčových komponent, které lze nalézt na prakticky každé z nich (viz Obrázek 8). [21]



Obrázek 8: Popis klíčových komponent počítačů Arduino [22]

V srdci každého Arduina je mikrokontrolér (MCU). Všechny původní desky, včetně Arduino Uno, používají 8bitový mikrokontrolér Atmel ATmega založený na architektuře AVR. Například Arduino Uno používá ATmega 328P. Lze si ho představit jako malý počítač navržený k vykonávání pouze specifického počtu úkolů. USB port slouží k připojení desky Arduino k počítači. Čip USB na sériovou linku je důležitou součástí, protože pomáhá překládat data, která pocházejí například z počítače, do palubního mikrokontroleru. To umožňuje programovat desku Arduino z počítače. Digitální piny využívají binární logiku a jsou běžně používány pro spínače a zapínání/vypínání LED diody. Analogové piny dokážou číst analogové hodnoty s rozlišením 10 bitů (0-1023). Piny 5 V, 3,3 V slouží k napájení externích komponent. GND se používá k dokončení obvodu, kde je elektrická úroveň na 0 voltech. VIN znamená Vstupní napětí, kam se může připojit externí zdroj napájení. V závislosti na desce Arduino se dá najít mnoho dalších komponent. Zmíněné položky se obecně nacházejí na jakékoliv desce Arduino. [21] [23]

Arduino Portenta H7 se řadí mezi nejvýkonnější modely rodiny Arduino, nabízí ještě větší výkon a flexibilitu pro profesionální vývojáře. Tento model kombinuje vysokou výpočetní kapacitu s bohatou sadou periférií, jenž jej činí ideálním pro náročné aplikace, jako jsou průmyslová automatizace, prediktivní údržba a umělá inteligence. Portenta H7 obsahuje dva procesory, které umožňují paralelní zpracování úloh. To znamená, že je schopný zároveň provozovat kód vyšší úrovně a úlohy v reálném čase. Například je možné spouštět

zkompilovaný kód pro Arduino spolu s kódem pro MicroPython a nechat obě jádra vzájemně komunikovat. Funkčnost Portenta je dvojí – může fungovat jako jakákoli jiná vestavěná mikrokontrolerová deska nebo jako hlavní procesor vestavěného počítače. Jako příklad lze použít Portenta Vision Shield, aby se H7 proměnilo v průmyslovou kameru schopnou provádět algoritmy strojového učení v reálném čase na živých videích. Mikrokontroler Portenta H7 umožňuje programování v jazycích vyšší úrovně a s umělou inteligencí při provádění operací s nízkou latencí na přizpůsobitelném hardwaru. [24]

Základem mikrokontroleru H7 je dvoujádrový STM32H747, obsahující Cortex M7 pracující s frekvencí 480 MHz a Cortex M4 s frekvencí 240 MHz. Komunikace mezi jádry je zajištěna mechanismem Remote Procedure Call, díky němuž je možné plynule volat funkce na opačném procesoru. Bezdrátové připojení je zajištěno konektorem Murata 1DX dual WiFi a Bluetooth verzí 5.1. Jednou z nejzajímavějších funkcí Portenta H7 je možnost připojení externího monitoru pro vytvoření vlastního vestavěného počítače s uživatelským rozhraním. To je umožněno díky GPU na čipu procesoru STM32H747. Kromě GPU tento čip obsahuje také dedikovaný JPEG kódovač a dekodér. [24]

3.2 Kryptoměna Bitcoin

Tato první a nejznámější digitální měna byla vynalezena v roce 2009 osobou nebo skupinou osob pod pseudonymem Satoshi Nakamoto reagující na finanční krizi z roku 2008. Cílem bylo vytvořit nezávislou měnu, která by nebyla pod kontrolou žádné vlády nebo finanční instituce a která by umožňovala bezpečný a anonymní přenos hodnoty přes internet. Bitcoin je založen na principu "digitálního zlata" s omezenou nabídkou 21 milionů mincí, podobně jako je omezené množství zlata. Bitcoin se dá rozdělit na menší jednotky, z nichž nejmenší je satoshi, který představuje jednu stomiliontinu Bitcoinu (0,00000001 BTC), zatímco další jednotky jako mBTC (millibitcoin) a µBTC (microbitcoin nebo bit) představují tisícinu a miliontinu Bitcoinu. [25]

Základem měny Bitcoin je technologie blockchain, která funguje jako decentralizovaná síť bez centrální autority. Tato síť zaznamenává všechny transakce v blockchainu, což je veřejná a nezměnitelná účetní kniha. Těžba Bitcoinu, proces ověřování transakcí a přidávání nových bloků do blockchainu, je prováděna těžaři, kteří za svou práci obdrží nově vytvořené Bitcoiny. Tento mechanismus slouží jako základní bezpečnostní a operační komponenta celé

sítě. Bitcoin se rychle stal populárním investičním aktivem a je známý svou vysokou volatilitou. Jeho hodnota se v průběhu let výrazně zvyšovala, což přitáhlo pozornost jak retailových, tak institucionálních investorů. Tato volatilita však také znamená, že cena Bitcoinu může v krátkém čase prudce stoupat i klesat. To představuje riziko pro investory. [25]

Bitcoin a blockchain technologie čelí výzvám, včetně regulačních otázek, otázek týkajících se škálovatelnosti a environmentálních obav spojených s energetickou náročností těžby. Bitcoin je také terčem kritiky kvůli možnému využívání pro nelegální aktivity vzhledem k anonymní povaze transakcí. Budoucnost Bitcoinu zůstává předmětem diskusí. Někteří experti vidí v Bitcoinu budoucí dominantní měnu pro digitální transakce, zatímco jiní upozorňují na jeho omezení a nejistou budoucnost. Bitcoin otevřel dveře pro vývoj dalších kryptoměn a stimuloval výzkum v oblasti blockchainových technologií, čímž významně ovlivnil moderní finanční systémy. [25]

3.2.1 Kryptoměnové peněženky

Kryptoměnové peněženky jsou klíčový prvek v digitálním finančním ekosystému a hrají nezastupitelnou roli v transformaci způsobu, jakým lidé uchovávají, obchodují a pracují s kryptoměnami. Kryptoměnové peněženky fungují jako most mezi starým a novým světem, umožňují uživatelům přenášet, uchovávat a obchodovat s kryptoměnami.

Existují celkem 4 typy peněženek:

a) online peněženky,
b) mobilní peněženky,
c) hardwarové peněženky,
d) papírové peněženky.

Online peněženky jsou digitální nástroje, které umožňují uživatelům spravovat své kryptoměny prostřednictvím internetu. Jsou dostupné na různých online platformách a často poskytují snadný přístup ke kryptoměnám bez nutnosti instalace dodatečného softwaru, a to pouze za použití webového prohlížeče či aplikace. Online peněženky se vyznačují rychlými transakcemi a jednoduchým uživatelským rozhraním. Avšak jejich bezpečnost je klíčovým aspektem a uživatelé musí být obezřetní při výběru spolehlivé platformy a implementaci bezpečnostních opatření. [26]

Výhody jsou:

- rychlost transakcí umožňuje okamžité platby,
- ideální pro uchovávání menších částek kryptoměn.

Nevýhody jsou:

- plná kontrola třetí strany nad bezpečností a správou peněz,
- zvýšené riziko bezpečnostních hrozeb v online prostředí.

Mobilní peněženky jsou navrženy pro chytrá zařízení, jako jsou mobilní telefony a tablety, a umožňují uživatelům mít své kryptoměny stále po ruce. Tato mobilní zařízení se stávají přenosným a efektivním prostředkem pro uskutečňování transakcí. Mobilní peněženky bývají často propojeny s technologiemi jako NFC, což umožňuje uživatelům provádět bezkontaktní platby. Klíčovou výhodou mobilních peněženek je jejich schopnost rychle a pohodlně uskutečňovat transakce v reálném čase. Pro bezpečnost těchto peněženek je nezbytné využívat biometrické autentizace a šifrování dat. [26]

Výhody jsou:

- snadná použitelnost a dostupnost kdykoli,
- možnost využití QR kódu pro rychlé skenování plateb.

Nevýhody jsou:

- zranitelnost mobilních zařízení vůči malware a virům,
- riziko ztráty finančních prostředků při kompromitaci telefonu.

Hardwarové peněženky jsou fyzická zařízení, která poskytují offline úložiště pro privátní klíče kryptoměn. Tyto peněženky eliminují riziko online útoků a jsou obvykle považovány za jedno z nejbezpečnějších úložišť pro kryptoměny. Hardwarové peněženky bývají odolné vůči malware a jiným kybernetickým hrozbám. Uživatelé mohou přistupovat k jejich kryptoměnám pouze při připojení zařízení k počítači nebo jinému zařízení s internetovým připojením. To zajišťuje maximální bezpečnost a ochranu digitálních aktiv. [26]

Výhody jsou:

- maximální bezpečnost díky oddělení od online prostředí,
- plná kontrola nad privátními klíči uživatele.

Nevýhody jsou:

- obtížnější dostupnost a vyšší pořizovací náklady,
- pro začátečníky může být používání složité.

Papírové peněženky představují jednu z nejstarších forem uchovávání kryptoměn. Jsou to fyzické dokumenty nebo QR kódy obsahující privátní klíče. Tato forma uložení privátních klíčů je odolná vůči online hrozbám, protože není připojena k internetu. Ačkoliv jsou papírové peněženky považovány za bezpečné, uživatelé musí dbát na jejich fyzickou ochranu, protože ztráta nebo poškození papíru může vést ke ztrátě přístupu k digitálním aktivům. [26]

Výhody jsou:

- maximální bezpečnost offline uchování,
- jednoduchost použití a nízké náklady.

Nevýhoda je:

- pomalejší provedení transakcí v porovnání s online peněženkami.

3.2.2 Blockchain

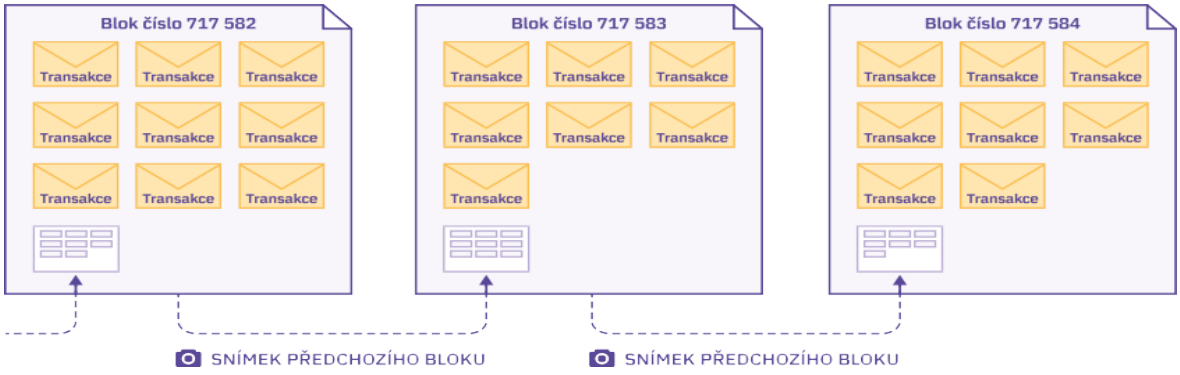
Blockchain představuje pokročilou technologii distribuované databáze, která je základem pro decentralizované sítě typu P2P (Peer-to-Peer). Tato síť umožňuje uživatelům provádět transakce přímo mezi sebou bez potřeby zprostředkovatele, což vede k větší efektivitě a snižuje riziko manipulace. V rámci blockchainu je každá transakce zaznamenána do bloku, který je následně ověřen a přidán do řetězce bloků pomocí nezávislých ověřovacích mechanismů. [27]

Proof of Work je metoda, která vyžaduje od účastníků, často označovaných jako těžaři, vykonání složitých výpočetních úloh, aby mohli přidávat nové bloky do blockchainu. Transakce vytvořená bitcoinovou peněženkou je podepsána soukromým klíčem a odeslána do sítě, kde je každým uzlem ověřena a přidána do dočasného úložiště zvaného mempool. Těžaři pak konkurují o to, kdo jako první vytěží nový blok, přičemž vítězný těžař zařadí vybrané transakce s nejvyššími poplatky do nového bloku a odstraní je z mempoolu. Jako odměnu obdrží nově vytvořené bitcoiny a transakční poplatky. Nově vytěžený blok je následně zaslán do sítě, kde je každým uzlem prověřen a připojen k existujícímu blockchainu. Po této validaci je transakce považována sítí za potvrzenou a kompletní. Tento proces nejenže zajišťuje bezpečnost a integritu databáze, ale také řeší problém dvojitého utrácení, protože

každá jednotka hodnoty může být utracena pouze jednou. Dochází pouze k převodu Bitcoinu mezi účty, nikoli k jeho duplikaci. [27] [28]

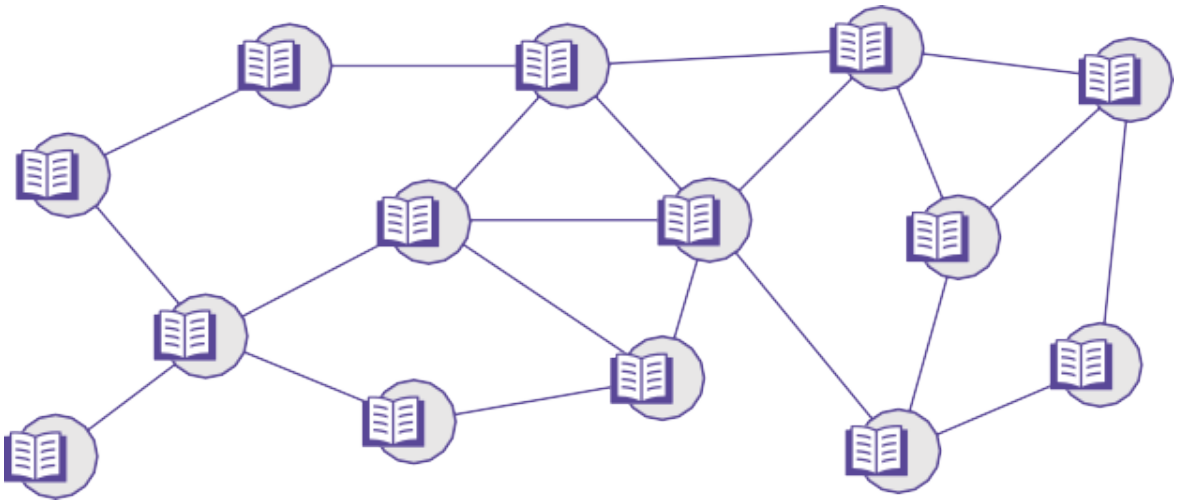
Na rozdíl od tradičních P2P sítí, kde data jsou sdílena formou kopírování mezi uživateli, blockchain ukládá informace o transakcích trvale a nezměnitelně. Díky tomu lze historii transakcí snadno ověřit a sledovat, což zvyšuje transparentnost a důvěru v systém. Výsledkem je robustní infrastruktura, která umožňuje bezpečné a transparentní provádění digitálních transakcí bez závislosti na centralizovaných autoritách. [27]

Blockchain není nic jiného, než tzv. decentralizovaná účetní kniha, která obsahuje všechny transakce, jež kdy byly pomocí této sítě odeslány. Blockchain se skládá z jednotlivých bloků. První blok s pořadovým číslem 0 byl vytvořen tvůrcem Bitcoinu. Jednotlivé bloky na sebe navazují pomocí hashů toho předešlého, což tvoří řetězec. Každý uzel, který nový blok obdrží a uzná, že je platný, si ho přidá na konec svého řetězce. Zároveň smaže transakce v něm obsažené ze svého mempoolu. [25]



Obrázek 9: Architektura blockchainové technologie [25]

V důsledku distribuované povahy blockchainu je dosaženo situace, kdy je identická kopie účetní knihy uchována na každém uzlu sítě. Tato účetní kniha může být přirovnána k evidenci, kde jsou jednotlivé listy s transakcemi systematicky zařazovány. Na všech uzlech je celosvětově udržována naprosto shodná verze této knihy. [25]



Obrázek 10: Struktura blockchainové sítě [25]

Hlavní význam blockchainu je spatřován v jeho decentralizaci. Je charakterizován tím, že žádná centrální autorita nemá nad sítí kontrolu, není možné generovat bitcoiny bez odpovídajícího základu, provádět neférové transakce (které by byly ostatními uzly detekovány a odmítnuty), ani úplně vypnout bitcoinovou síť. Vystačí se situací, kdy je uchován alespoň jeden funkční uzel s aktuální verzí blockchainu, který po obnovení sítě umožní distribuci účetní knihy ostatním uzlům. [25]

3.2.3 Bitcoinový uzel

Bitcoinový uzel je základním stavebním prvkem decentralizované sítě. Každý uzel uchovává kopii celého blockchainu a účastní se jeho aktualizace a ověřování. Uzly jsou rozděleny do několika kategorií na základě úlohy, kterou v síti plní. Plné uzly ověřují všechny bloky a transakce a odmítají ty, které porušují pravidla sítě, čímž pomáhají udržovat bezpečnost a integritu sítě. Těžařské uzly kombinují ověřování transakcí s procesem těžby nových bloků. [29]

3.2.4 Lightning Network

Bitcoinový blockchain nabízí velký potenciál pro distribuované účetní knihy, ale jako samostatná platební platforma není schopen pokrýt celosvětové obchodování. Jeho design není škálovatelný pro zpracování objemu globálních finančních transakcí, protože by významně zatěžoval kapacitu sítě. Lightning Network (LN) představuje inovativní řešení pro zvýšení škálovatelnosti a efektivity Bitcoinu, které řeší klíčové problémy spojené s jeho schopností zpracovávat velký objem transakcí. Jako druhá vrstva, která je postavena nad Bitcoinovým

blockchainem, LN umožňuje uživatelům provádět transakce mimo hlavní blockchain, což vede k výraznému zrychlení transakčních časů a snížení poplatků. [29] [30]

Základem LN jsou platební kanály, které umožňují dvěma stranám provádět libovolný počet transakcí bez nutnosti zaznamenávat každou z nich na blockchainu. Tyto kanály jsou vytvářeny tak, že obě strany vloží určité množství bitcoinů jako zálohu do společné multisig adresy, což je speciální typ bitcoinové adresy, která vyžaduje více než jeden soukromý klíč k autorizaci transakce. Stav kanálu se aktualizuje s každou transakcí, ale tyto aktualizace jsou zaznamenány pouze mezi oběma stranami a ne na hlavním blockchainu. To výrazně zvyšuje rychlost a snižuje náklady na transakce. [25] [30]

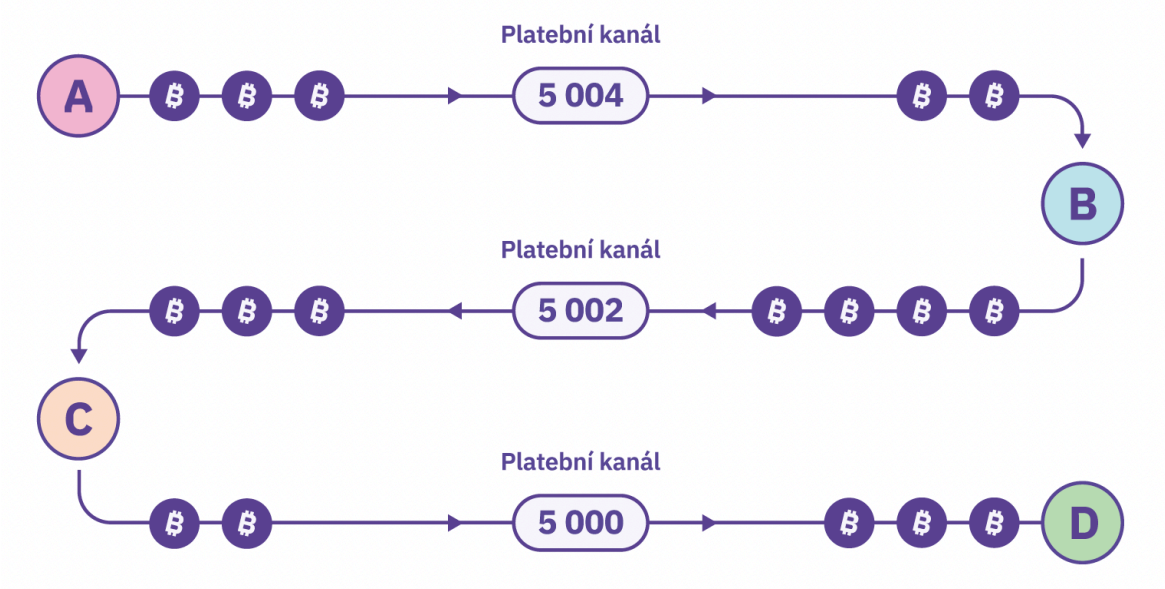
Klíčovým konceptem, který LN používá pro zabezpečení transakcí, jsou Hashed Time-Locked Contracts (HTLCs), což jsou speciální typy platebních kanálů, které přidávají mechanismus pro vytvoření důvěry mezi stranami. Díky tomu může odesílatel platby zajistit, že příjemce dostane peníze pouze v případě, že splní určenou podmínku do stanoveného časového limitu. Pokud podmínka není splněna, prostředky se vrátí zpět odesílateli. To umožňuje bezpečné a důvěryhodné provádění transakcí bez nutnosti důvěřovat protistraně nebo třetí straně. [25]

Důležitou charakteristikou LN je také síťová topologie, která umožňuje transakce mezi uživateli, kteří nemají přímý platební kanál. Díky tzv. "multi-hop" platebním trasám mohou bitcoiny cestovat po více propojených platebních kanálech, což umožňuje komplexní síťovou infrastrukturu, kde každý uživatel může potenciálně dosáhnout každého jiného uživatele v síti. Toto propojení vytváří bohatou síťovou strukturu, kde jsou transakce směrovány dynamicky na základě dostupnosti a kapacity kanálů. [25]

Příkladem může být, kdy Alice potřebuje poslat 5 000 satoshi Davidovi, ale s ní nemá přímý platební kanál. Má však kanál s Bobem, Bob má kanál s Cyrilem a Cyril s Davidem. Platba se tedy uskuteční přes tuto řetězovou cestu, a protože si každý uzel účtuje poplatek za platbu, musí Alice poslat o tuto částku více. Alice tedy pošle Bobovi 5 004 satoshi, Bob

přepošle 5 002 satoshi Cyrilovi a Cyril předá 5 000 satoshi Davidovi. V tomto procesu Bob a Cyril slouží jako prostředníci, které umožní Alici převod k Davidovi. [25]

Dalším zásadním aspektem těchto plateb je, že se buď provedou celé, nebo vůbec, což zajišťuje, že pokud platba neprojde v plné výši, satoshi se vrátí zpět k odesílateli. To zabraňuje riziku, že by prostředníci, jako je Bob či Cyril, zadrželi satoshi bez dokončení transakce. [25]



Obrázek 11: Schéma platební transakce v LN [25]

Lightning Node je specifický typ uzlu v rámci Lightning Network, který umožňuje uživatelům vytvářet a spravovat platební kanály, provádět transakce a směrovat platby v síti. Tyto uzly hrají klíčovou roli v operacích Lightning Network síti, neboť udržují síťovou konektivitu a pomáhají v routování plateb po síti. Uzly v Lightning Network musí být neustále online, aby mohly reagovat na žádosti o platbu a aktualizovat stavy kanálů, což je zásadní pro udržení bezpečnosti a funkčnosti sítě. Uživatelé, kteří provozují vlastní Lightning uzel, mohou získávat poplatky za směrování transakcí pro ostatní uživatele, což přináší finanční motivaci pro udržování kvalitního a spolehlivého uzlu. [29] [30]

Vzhledem k těmto vlastnostem se LN jeví jako slibná technologie pro řešení problémů škálovatelnosti Bitcoinu a může hrát klíčovou roli v jeho budoucím vývoji jako digitální měny. Přestože LN je stále relativně nová technologie a vyvíjí se, její potenciál pro transformaci

platebních systémů a podpora mikroplateb představuje významný krok vpřed v evoluci kryptoměn. [29] [30]

3.3 Vícekriteriální analýza variant

Teorie a modely vícekriteriální analýzy variant se zaměřují na problémy výběru nejvhodnější varianty nebo variant z množiny přípustných možností. Rozhodovatel by měl přistupovat k výběru co nejobjektivněji, přičemž mu v tom pomáhají různé metody a postupy analýzy. Někdy je možné oddělit osobu zadavatele od analytika, což má své výhody i nevýhody. Analytik často není ovlivněn výsledkem a může být objektivnější, ale nemusí být plně seznámen se všemi detaily úlohy. Výsledkem je doporučení nejlepší varianty, která ale nemusí být vždy prakticky nejvhodnější, zejména při malých rozdílech v hodnocení. Modely vícekriteriální analýzy umožňují vyhodnocení variant podle více kritérií a hledání optimálních nebo kompromisních řešení. Přístupy k vícekriteriálnímu rozhodování se liší podle charakteru množiny variant či přípustných řešení. [31]

Podle způsobu jejího zadání lze modely rozlišit na následující 2 skupiny:

- modely vícekriteriálního hodnocení variant, které jsou zadány pomoci konečného seznamu variant a jejich ohodnocení podle jednotlivých kritérií,
- modely vícekriteriální optimalizace, které mají množinu variant s nekonečně mnoho prvky vyjádřenou pomocí omezujících podmínek a ohodnocení jednotlivých variant je dáno jednotlivými kriteriálními funkcemi.

V rámci modelů vícekriteriální analýzy je pevně stanovená diskrétní množina *m* variant, které se hodnotí podle *n* kritérií. Cílem je identifikovat variantu, která je na základě těchto kritérií celkově nejlépe hodnocená, najít kompromisní řešení, seřadit varianty od nejlepších po nejhorší, nebo eliminovat varianty, které nejsou efektivní. Varianty jsou konkrétní rozhodovací možnosti, předmět vlastního rozhodování, které jsou realizovatelné a nejsou logickým nesmyslem. Kritérium je hledisko hodnocení variant, které může být kvalitativní nebo kvantitativní. Výběr kritérií je klíčovým prvkem ve vícekriteriální analýze. Kritéria by měla být nezávislá a měla by komplexně pokrývat všechny relevantní aspekty rozhodování, avšak jejich počet by neměl být příliš velký, aby se zachovala přehlednost. [31]

4 Vlastní práce

4.1 Výběr vhodného zařízení

Pro efektivní provoz uzlu v síti Lightning Network jsou nezbytné určité minimální technické požadavky. LN uzel vyžaduje stabilní a trvalé internetové připojení, adekvátní kapacitu paměti RAM a dostatečně velké úložiště pro uchování celého blockchainu. Pro Lightning Network je rovněž důležitá odezva, jelikož uzly musí být schopny rychle zpracovat transakční data, aby zůstaly synchronizovány se sítí.

Doporučovaný požadavek je mít alespoň 2 GB RAM a 1 TB úložiště pro uchování kompletního blockchainu (v době psaní práce má velikost přibližně 550 GB). Přičemž je preferováno větší úložiště pro delší dobu provozu bez nutnosti rozšiřování úložiště z důvodu zvětšování Blockchainu. S ohledem na velikost Blockchainu je vhodné zvolit externí uložiště, které bude připojené k počítači pomocí USB rozhraní. Z hlediska rychlosti zápisu a čtení dat je vhodnější využít SSD disk namísto disku plotnového či SD karty.

Jednodeskové počítače Raspberry Pi 5 ve verzi s operační pamětí 8 GB, Raspberry Pi 4 model B ve verzi s operační pamětí 8 GB, Raspberry Pi 3 model B+, Jetson Nano ve verzi s operační pamětí 4 GB a Banana Pi M5 byly vybrány pro testování Lightning Network uzlů na základě jejich specifikací s ohledem na doporučené požadavky. Specifikace jednotlivých jednodeskových počítačů byly podrobněji probrány v Kapitole 3.1. Srovnání jejich parametrů je uvedeno v Tabulce 1.

Tabulka 1: Srovnání parametrů jednodeskových počítačů

Zařízení	Procesor	RAM	Rychlost USB	Cena[1]
Raspberry Pi 3 model B+	BCM2837B0 Cortex-A53 64-bit (1 400 MHz)	1 GB	480 Mb/s	939 Kč
Raspberry Pi 4 model B	BCM2711 Cortex-A72 64-bit (1 500 MHz)	8 GB	5 000 Mb/s	2 019 Kč
Raspberry Pi 5	BCM2712 ARM Cortex-A76 64-bit (2 400 MHz)	8 GB	5 000 Mb/s	2 155 Kč
Jetson Nano	NVIDIA T210 ARM Cortex-A57 64-bit (1 430 MHz)	4 GB	5 000 Mb/s	4 799 Kč
Banana Pi M5	Amlogic S905x3 ARM Cortex-A55 64 - bit (1 500 MHz)	4 GB	5 000 Mb/s	2 349 Kč

4.2 Zátěžové testy a porovnání

Pro detailní testování a porovnání výkonu vybraných jednodeskových počítačů byly využity dva renomované zátěžové testy – *Sysbench* a *Geekbench*. Tyto testy jsou zásadní pro objektivní hodnocení schopností každého zařízení. Při testování LN uzlů je zejména důležitý výsledek výkonu CPU a operační paměti, neboť tyto komponenty hrají klíčovou roli v rychlosti zpracování transakcí a celkové schopnosti uzlu udržovat souběžnost s blockchainovou sítí.

Použití nástrojů *Sysbench* a *Geekbench* pro testování výkonu počítačů umožňuje uživateli získat komplexní a víceúrovňové porozumění jejich schopnostem. Tato analýza výkonu pomáhá určit, která konfigurace jednodeskového počítače je nejvhodnější pro provozování uzlu v síti Lightning Network. Zajišťuje, že uzly budou moci efektivně a spolehlivě zpracovávat LN transakce, a tím podporuje celkovou stabilitu a výkon LN sítě.

[1] ceny jsou uvedené z internetových obchodů RPishop.cz a Alza.cz k 18.1.2024

4.2.1 Zátěžové testy pomocí Sysbench

Sysbench[2] je flexibilní a všestranný nástroj pro zátěžové testy, který umožňuje uživatelům provádět komplexní a detailní testy zaměřené na různé aspekty systémového výkonu, jako je výkon procesoru, paměti, vstupně-výstupních a databázových operací. *Sysbench* poskytuje podrobné výsledky pro každý z těchto testů, což umožňuje hluboký vhled do toho, jak každý počítač zvládá specifické výpočetní a paměťové nároky.

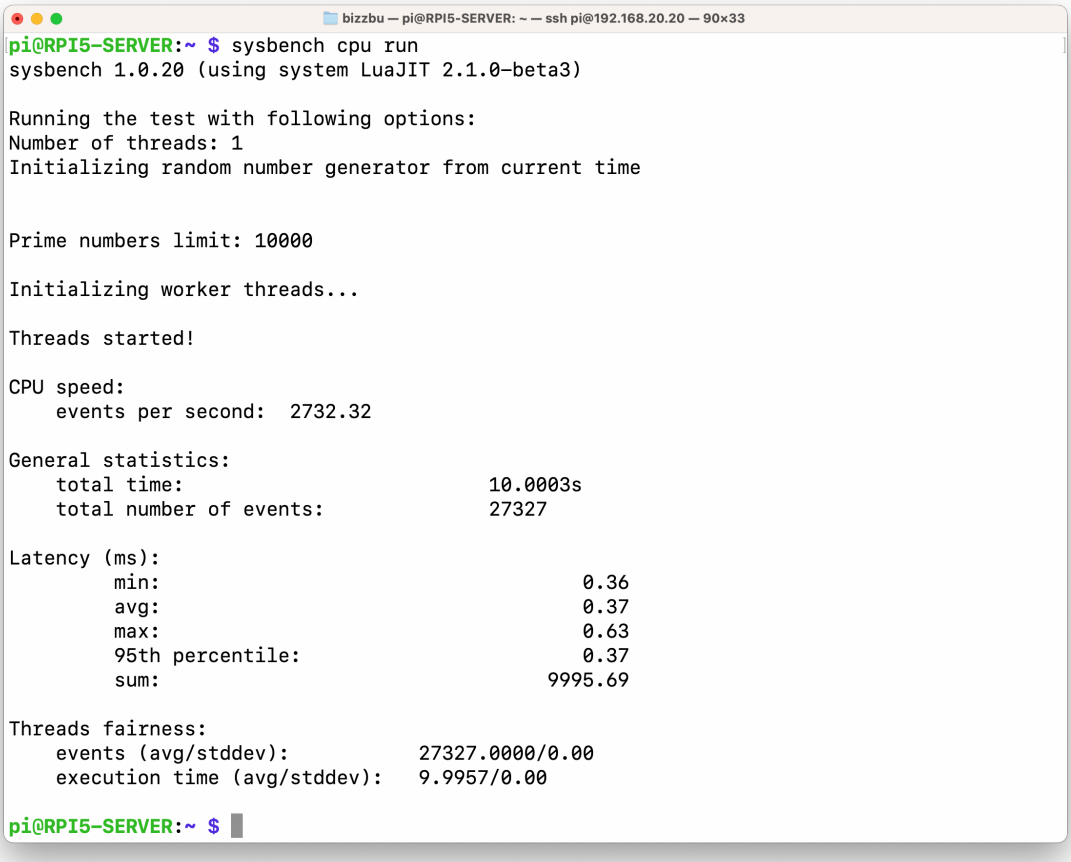
Tento zátěžový test poskytuje řadu konfigurovatelných parametrů, které umožňují uživatelům přizpůsobit testování svým potřebám. Lze nastavit celkový počet pracovních vláken, omezit celkový počet požadavků a celkovou dobu provádění testu v sekundách. Je možné konfigurovat dobu zapínání, průměrnou rychlost transakcí, čekací dobu pro inicializaci vláken, velikost zásobníku pro každé vlákno a interval pro periodické hlášení statistik. Kromě toho nabízí možnosti pro ladění, validaci výsledků, pomoc s nápovědou, nastavení úrovně podrobnosti výstupu a určení percentilu pro měření doby provádění. Pokud si uživatel parametry nespecifikuje, test je prováděn s výchozími hodnotami (viz Tabulka 2).

Tabulka 2: Výchozí hodnoty testu Sysbench

Parametr	Popis parametru	Výchozí hodnota
--threads	Počet pracovních vláken	1
--events	Počet požadavků	0 (bez limitu)
--time	Celková doba provádění testu v sekundách	10
--warmup-time	Doba zapínání	0
--rate	Průměrná rychlost transakcí	0 (bez limitu)
--thread-init-timeout	Čekací doba pro inicializaci vláken v sekundách	30
--thread-stack-size	Velikost zásobníku pro každé vlákno	32 KB
--report-interval	Interval pro periodické hlášení statistik	0
--verbosity	Úroveň podrobnosti výstupu	4
--percentile	Percentil pro měření doby provádění	95 %

[2] Nástroj je dostupný v repositáři na adrese https://github.com/akopytov/sysbench

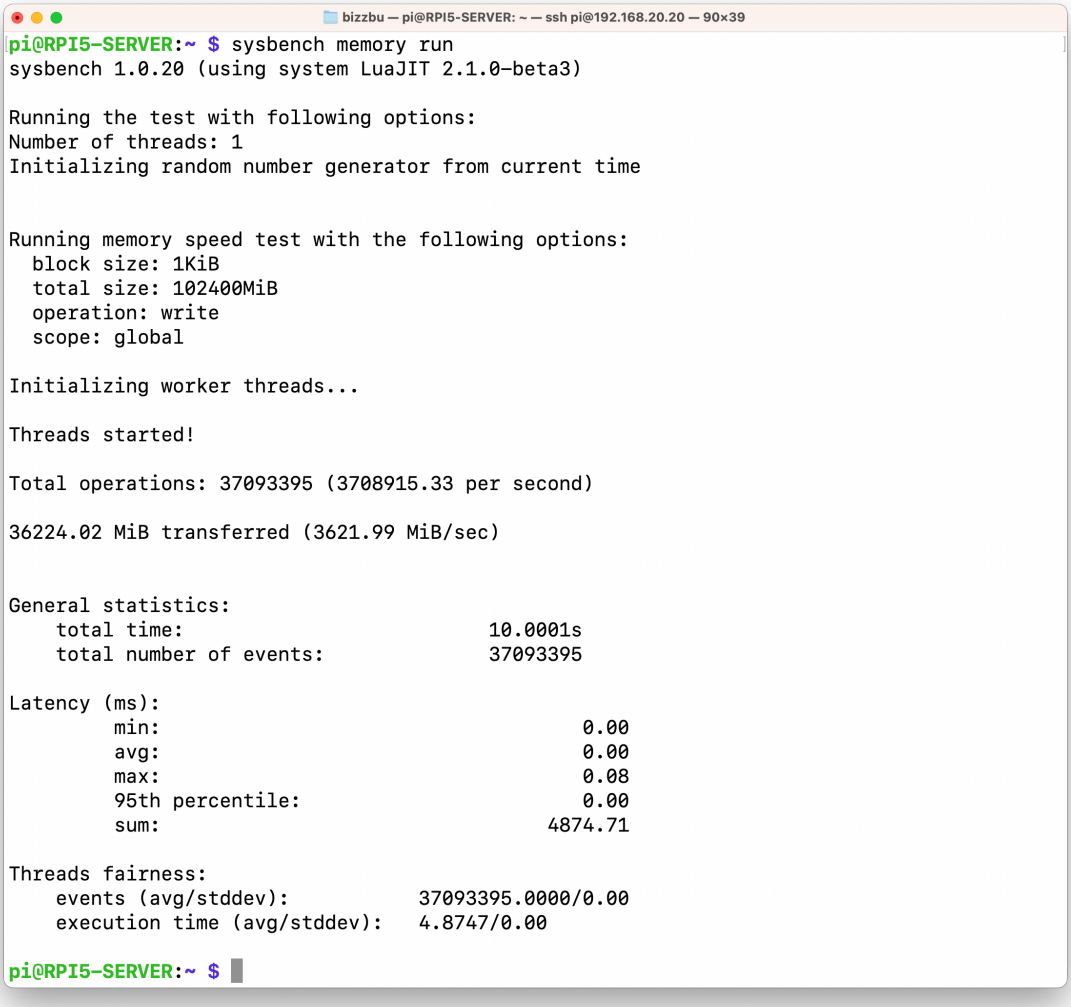
Výsledky zátěžového testu z příkazového řádku ukazují výkon procesoru na Raspberry Pi 5 (viz Obrázek 12). Během desetisekundového testu, který využíval jedno vlákno, bylo provedeno 27 327 operací souvisejících s výpočtem prvočísel. Procesor dosáhl rychlosti 2 732,32 událostí za sekundu. Tento výsledek je pro testování nejzásadnější. Latenceměla minimální hodnotu 0,36 ms, průměrnou 0,37 ms a maximální 0,63 ms. 95 % operací bylo dokončeno rychleji než 0,37 ms. Celkový součet všech latencí byl 9 995,69 ms, což naznačuje, že zátěž byla během testu rovnoměrně rozložena, jak ukazuje nulová standardní odchylka u průměrné doby provádění operace.



Obrázek 12: Výsledek CPU benchmarku Sysbench na RPi 5 [vlastní zpracování]

Dále byl proveden benchmark operační paměti (viz Obrázek 13). V tomto testu jsou důležité 2 výsledky, a to počet operací za sekundu a rychlost přenosu. Výstupy ze zátěžového testu paměti provedeného na Raspberry Pi 5 ukazují, že během desetisekundového testu bylo dosaženo 37 093 395 operací, což odpovídá rychlosti zápisu přes 3,7 milionu operací za sekundu. Během tohoto časového období bylo zpracováno 36 224,02 MiB dat, přičemž rychlost

přenosu dosáhla 3 621,99 MiB/s. Test vykázal nulovou latenci, což značí okamžitý přístup k paměti a její výjimečný výkon. Vysoká rychlost a nízká latence naznačují, že zařízení je velmi vhodné pro aplikace s náročným využitím paměti, jako je ukládání a manipulace s daty blockchainu.



Obrázek 13: Výsledek RAM benchmarku Sysbench na RPi 5 [vlastní zpracování]

Tyto dva testy byly provedeny na všech vybraných jednodeskových počítačích s výsledky zapsanými v Tabulce 3. Nejobstojněji si vedl počítač Raspberry Pi 5, který dominoval ve všech třech kategoriích. Zatímco nejhůř na tom byl počítač Jetson Nano. Ten zaostával v obou výsledcích testu operační paměti. I když Jetson Nano splňuje doporučené požadavky pro provoz LN uzlu, tak v těchto benchmark testech je vidět, že jeho hlavní silnou stránkou není výpočetní výkon CPU, ale počítač je spíše optimalizován na výkon paralelního výpočtu pomocí jader GPU.

Tabulka 3: Výsledky testů nástrojem Sysbench

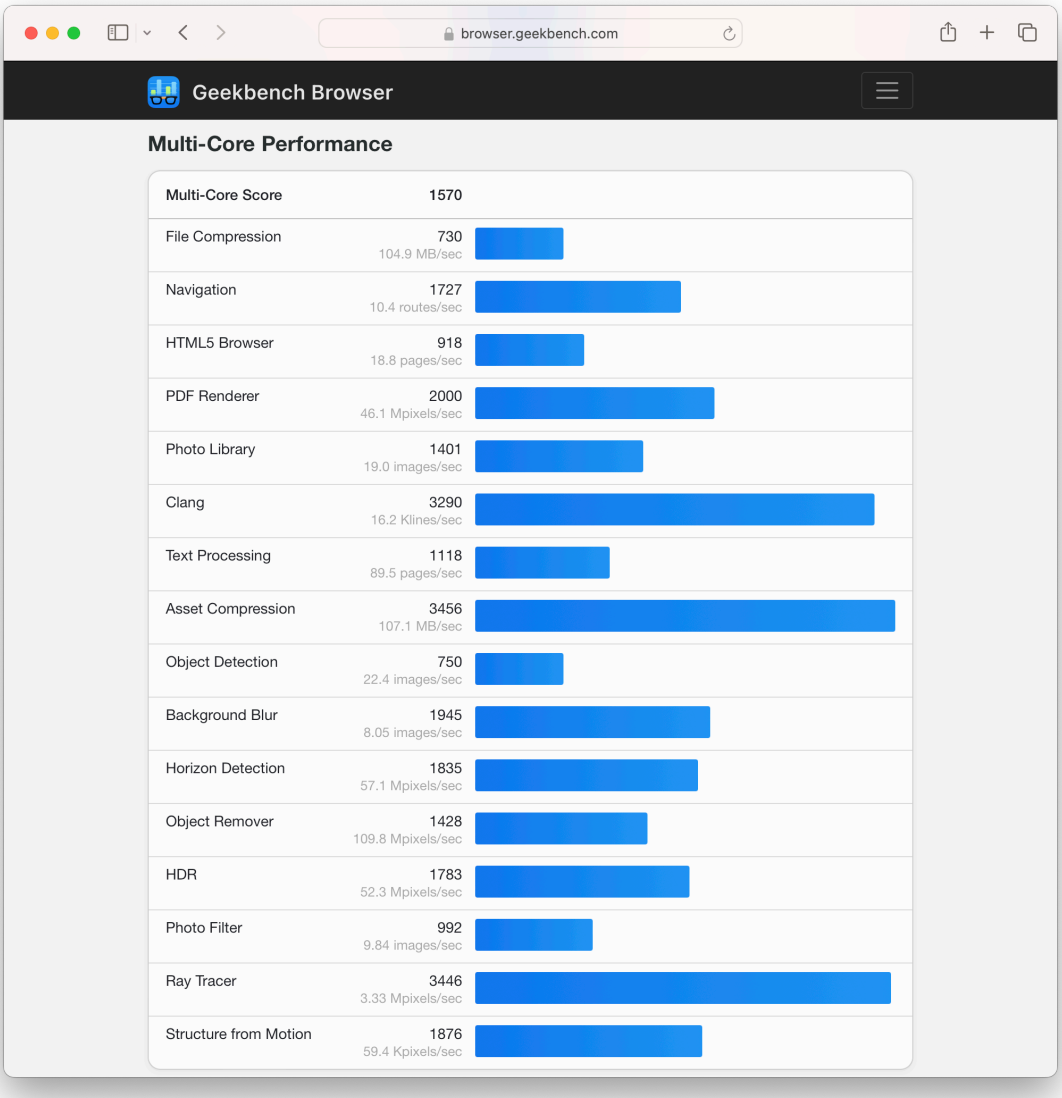
Zařízení	CPU Benchmark (událostí/s)	RAM Benchmark (operací/s)	RAM Benchmark (MiB/s)
Raspberry Pi 3 model B+	579,33	1 037 855,29	1 013,53
Raspberry Pi 4 model B	1 772,42	2 485 823,95	2 427,56
Raspberry Pi 5	2 732,32	3 708 915,33	3 621,99
Jetson Nano	7 47,24	855 356,25	835,31
Banana Pi M5	856,34	2 005 011,58	2 489,13

4.2.2 Zátěžové testy pomocí Geekbench

Geekbench[3], na druhou stranu, nabízí širší perspektivu výkonu systému tím, že provádí řadu referenčních testů, které simulují různé skutečné výpočetní úlohy. *Geekbench* měří výkon procesoru a paměti prostřednictvím různých workloadů, které odrážejí běžné operační scénáře, a výsledkem je jednoduché kompozitní skóre. Toto skóre je užitečné pro rychlé srovnání mezi různými systémy, protože poskytuje okamžitě srozumitelný přehled o celkovém výkonu daného zařízení. *Geekbench* skóre také pomáhá identifikovat, jak dobře může zařízení zvládat paralelní úlohy a multitasking, což jsou důležité aspekty pro LN uzly, které potřebují efektivně zpracovávat množství transakcí a údajů v reálném čase.

Tento benchmark na rozdíl od *Sysbench* neposkytuje uživateli možnost test konfigurovat. Jediná volba konfigurace spočívá v jeho výstupu – zda uživatel chce výsledky ve formátu CSV, HTML, JSON či ryze textovém výstupu. Výsledky testu se automaticky nahrávají na web, který je přístupný široké veřejnosti, a z tohoto důvodu je zde také možnost modifikace výsledek na web nenahrávat. To jsou ale všechny možné konfigurace tohoto benchmarku. Test měří maximální výkon jednoho jádra, a poté měří maximální výkon při zatížení všech jader procesoru. V práci je pracováno s vícejádrovým výsledkem (viz Obrázek 14).

[3] Nástroj je dostupný v repositáři na adrese https://www.geekbench.com/



Obrázek 14: Výsledek benchmarku Geekbench na RPi 5 [vlastní zpracování]

Zátěžový test byl proveden na všech vybraných jednodeskových počítačích s průměrnou dobou testu 30 minut. Výsledek testů je vidět v Tabulce 4. Nejobstojněji si zde vedl počítač Raspberry Pi 5 stejně jako u předešlého testu. Počítač dosahoval téměř dvojnásobného výsledku oproti druhému nejlepšímu počítači, který v tomto testu byl Jetson Nano, i když mu v předešlém testu vyšly výsledky nejhůře. Nejhoršího výsledku dosáhl počítač Raspberry Pi 3, kde výsledky tohoto testu zapříčinilo celkové stáří modelu.

Tabulka 4: Výsledky testů nástrojem Geekbench

Zařízení	Vícejádrové skóre
Raspberry Pi 3 model B+	170 bodů
Raspberry Pi 4 model B	689 bodů
Raspberry Pi 5	1 570 bodů
Jetson Nano	798 bodů
Banana Pi M5	691 bodů

4.3 Vícekriteriální analýza variant

Pro výběr nejvhodnějšího jednodeskového počítače byla zvolena vícekriteriální analýza variant. Obsahuje všechny potřebné nástroje pro volbu optimální varianty.

Varianty jsou:

- Raspberry Pi 3 model B+,
- Raspberry Pi 4 model B,
- Raspberry Pi 5,
- Jetson Nano,
- Banana Pi M5.

Kritéria jsou:

- CPU Benchmark (událostí/s),
- RAM Benchmark 1 (operací/s),
- RAM Benchmark 2 (MiB/s),
- vícejádrové skóre,
- rychlost USB,
- pořizovací cena.

Tato kritéria jsou důležitá pro technické zhodnocení jednodeskových počítačů. Výsledek zátěžových testů CPU a RAM přímo ovlivňuje schopnost systému zpracovávat úlohy a

multitaskování, zatímco rychlost USB určuje efektivitu přenosu dat, která je zásadní pro práci s Blockchainem. Cena je důležitá pro určení nákladů na pořízení zařízení. Porovnávání těchto hodnot umožňuje vybrat optimálnější zařízení pro využití pro provozování uzlu v Lightning Network síti.

Pro ohodnocení je použita bodovací metoda s maximalizačním charakterem kritéria a použitým intervalem od 1 do 10 včetně, aby bylo zajištěno dostatečné rozlišení mezi variantami a současně umožněno intuitivní a snadno srozumitelné hodnocení. Výsledky zátěžových testů, rychlosti USB konektorů a ceny byly podle jejich hodnot převedeny na body. Kritérium cena bylo normalizováno. Váhy jsou pro všechna kritéria stejné. Hodnocení je uvedeno v Tabulce 5.

Tabulka 5: Vícekriteriální analýza variant

Zařízení	CPU Benchmark	RAM Benchmark 1	RAM Benchmark 2	Více-jádrové skóre	Rychlost USB	Cena	Průměr
Raspberry Pi 3 model B+	2	2	3	1	1	10	3,17
Raspberry Pi 4 model B	6	6	7	4	10	7	6,67
Raspberry Pi 5	10	10	10	10	10	7	9,5
Jetson Nano	3	2	2	5	10	3	4,17
Banana Pi M5	3	5	7	4	10	7	6
Charakter kritéria	**MAX**	**MAX**	**MAX**	**MAX**	**MAX**	**MAX**	

Výsledek vícekriteriální analýzy variant ukázal, že počítač Raspberry Pi 5 je optimálním jednodeskovým počítačem pro provozování Lightning uzlu. Je tedy potřeba přistoupit k praktické implementaci a ověřit, zda tyto závěry odpovídají skutečnému výkonu v reálných podmínkách.

4.4 Implementace Lightning Network uzlu

Provozování vlastního uzlu či Lightning uzlu má několik výhod. Uživatelé nejsou závislí na třetích stranách pro ověřování transakcí, a tím zvyšují své soukromí a bezpečnost. Kromě toho provozování uzlu přispívá k decentralizaci a robustnosti sítě, protože čím více nezávislých uzlů síť má, tím je obtížnější ji cenzurovat nebo napadnout. Provozování Lightning uzlu zase umožňuje uživatelům využívat rychlé a levné transakce poskytova nésítí Lightning Network a podílet se na inovativní vrstvě pro mikroplatby postavené nad Bitcoinem. Tímto způsobem je také možné vydělávat na poplatcích za transakční cesty, které procházejí přes uživatelův uzel.

Pro nezkušené uživatele existuje několik možností zprovoznění LN uzlu v podobě předpřipravených platforem, jako jsou například *Umbrel*, *Citadel*, *RaspiBlitz*, *myNode*, *Embassy* a *Nodl*. *Umbrel* se vyznačuje graficky přívětivým rozhraním a vlastním obchodem s aplikacemi, který umožňuje instalovat mnoho aplikací a nadstaveb. Je ideální pro začátečníky díky své jednoduchosti a souběžně nabízí pokročilé funkce pro zkušenější uživatele. *Citadel*, fork *Umbrelu*, nabízí podobné funkce, ale klade větší důraz na komunitní rozvoj a pravidelné aktualizace. *RaspiBlitz* poskytuje grafického instalačního průvodce, uživatelsky přívětivé rozhraní pro konfiguraci a podporuje rozmanité nadstavby a funkce včetně podpory pro LCD displeje. *Embassy* a *myNode* jsou další alternativy, které nabízejí jednoduché řešení pro správu uzlu, zatímco *Nodl* se zaměřuje na prodej hotových hardwarových řešení s předinstalovaným softwarem pro snadný start. Všechny tyto distribuce již obsahují nakonfigurovaný Bitcoin plný uzel, samotnou implementaci Lightning Network a popřípadě různé nadstavby. Další možností je projekt *RaspiBolt*, který nenabízí již nakonfigurované zařízení nebo operační systém s běžícím LN uzlem, ale poskytuje pokročilejšímu uživateli přehled o tom, jak si Raspberry Pi pro provoz uzlu nakonfigurovat.

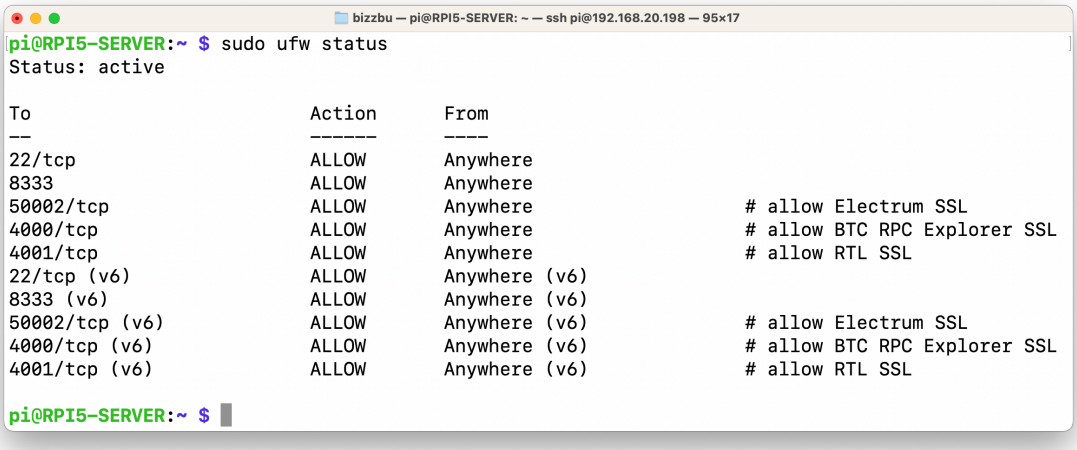
Zkušení uživatelé si mohou sestavit uzel zcela od základu svépomocí. Je třeba vybrat linuxovou distribuci, v ní nejprve provést konfiguraci operačního systému a správně ji zabezpečit. Poté následuje instalace a konfigurace Bitcoin plného uzlu, LN a jejich vzájemné propojení. V rámci provozu je nutné udržovat všechny komponenty aktualizované. Ačkoli je možnost vlastního zprovoznění považována za nejlepší z hlediska kontroly a funkcí uzlu, je vhodná pouze pro pokročilé uživatele. Je důležité si uvědomit, že jakákoli chyba v konfiguraci může mít vážné důsledky. Nejedná se pouze o riziko ztráty peněžních prostředků, ale také o potenciální nefunkčnost uzlu v případě neúspěšné aktualizace komponenty či špatně nastaveného zálohování.

Pro účely této bakalářské práce byla zvolena implementace LN uzlu bez využití již hotových řešení na počítači Raspberry Pi 5. Základem pro implementaci LN uzlu je čistý operační systém Raspberry Pi OS.

4.4.1 Systém a zabezpečení

Pro zabezpečení jednodeskového počítače je klíčové provést několik kroků, které ochrání systém tak, aby nedošlo k nějaké hrozbě. Prvotně je důležité aktualizovat systém na nejnovější verzi, která obsahuje nejnovější bezpečností záplaty. Z hlediska zabezpečení přístupu je

důležité používat uživatele s jiným než výchozím názvem, u kterého je zásadní nastavit silné heslo za pomoci malých, velkých písmen, číslic a speciálních charakterů. Pro bezpečné vzdálené připojení protokolem SSH je důležité zakázat přihlášení jako root a nastavit autentizaci pomocí soukromého klíče, nikoliv hesla. Ideální je správně zabezpečit i lokální firewall sítě na routeru, aby se na počítač dalo přistupovat například jen ze zařízení s konkrétní MAC adresou. Dále je nutné nainstalovat a aktivovat firewall na samotném systému počítači a zakázat jakékoliv jiné než povolené porty: port 22 pro SSH, který umožňuje vzdálený přístup, port 8333 pro Bitcoinový uzel, porty 50002 a 50001 pro Electrum SSL, které umožňují bezpečné připojení ke klientským aplikacím, a porty 4000 a 4001 pro BTC RPC Explorer SSL a RTL SSL, jež jsou využívány pro správu uzlu a pro průzkumníky bloků (viz Obrázek 15).

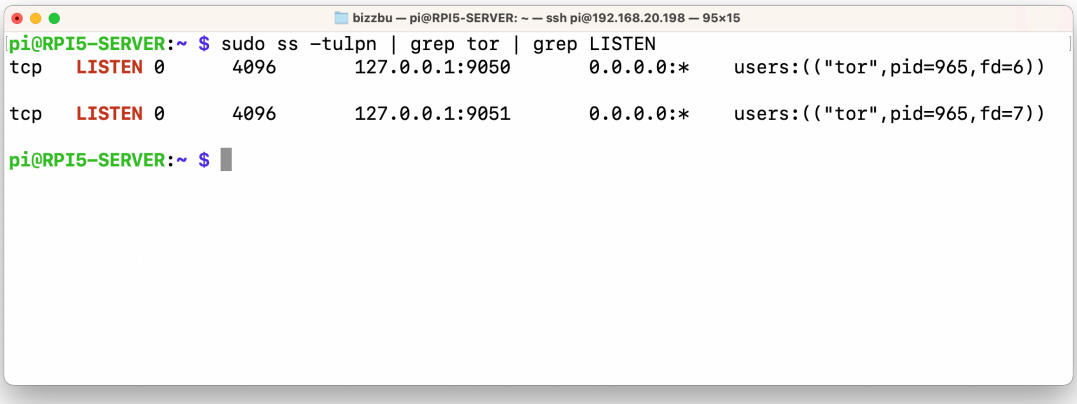


Obrázek 15: Nastavená pravidla na systémovém FW RPi 5

Proti síťovým útokům se dá chránit nástrojem Fail2ban. To je systém prevence průniku chránící proti neúspěšným pokusům o získání přístupu do systému, sledující logy aplikací (například SSH) a detekující vzory chování, které naznačují pokusy o neautorizovaný přístup do systému. Když takový pokus rozpozná, automaticky aktualizuje pravidla systémového firewallu, aby blokoval IP adresu útočníka na určitou dobu. Toto pomáhá chránit systém proti brute-force útokům a dalším druhům síťových útoků. Fail2ban je konfigurovatelný, umožňuje nastavit různá kritéria pro detekci a definovat akce, které se mají provést po detekci útoku. Pokud chceme předejít hrozbě způsobené bezdrátovým rozhraním jako je Wi-Fi či Bluetooth, je vypnutí takového připojení důležitým krokem.

Vzhledem k tomu, že některé služby jsou přístupné z internetu, je nezbytné zabezpečit komunikaci šifrováním a skrýt interní struktury pomocí reversního proxy serveru. Pro jeho zprovoznění je nutné nainstalovat NGINX, vytvořit SSL/TLS certifikát a upravit konfigurační soubor NGINX pro směrování a šifrování provozu. NGINX je zároveň i webový server, proto je důležité webový server zakázat a použít jen reversní proxy server. Tento postup pomáhá ochránit data přenášená mezi uživatelem a serverem.

Na zastínění anonymizace internetového provozu je vhodné využít software Tor Browser. Díky němu je zvýšené soukromí a bezpečnost tím, že anonymizuje internetový provoz a umožňuje uživatelům obejít cenzuru. Tor Browser dosahuje tohoto cíle směrováním datových paketů přes distribuovanou síť tisíců serverů, známých jako uzly Tor. Internetový provoz je posílán přes náhodně vybranou cestu těchto uzlů, přičemž každý uzel zná pouze předchozí a následující uzel v řetězci, nikoli původní zdroj nebo konečný cíl dat. To ztěžuje sledování původu nebo cíle komunikace. Data jsou na každém přeskoků znovu šifrována, což přidává další vrstvu ochrany. Bitcoin Core komunikuje napřímo s Tor Browser službou, aby byl zajištěn veškerý provoz přes síť Tor. Je tedy důležité nastavit Tor tak, aby přijímal pokyny skrze svůj kontrolní port, a to s náležitým ověřením. Toho je docíleno tak, že se v Tor konfiguraci povolí port 9051, který umožňuje interakci s běžícím Tor procesem.



Obrázek 16: Kontrola portů služby Tor na RPi 5 [vlastní zpracování]

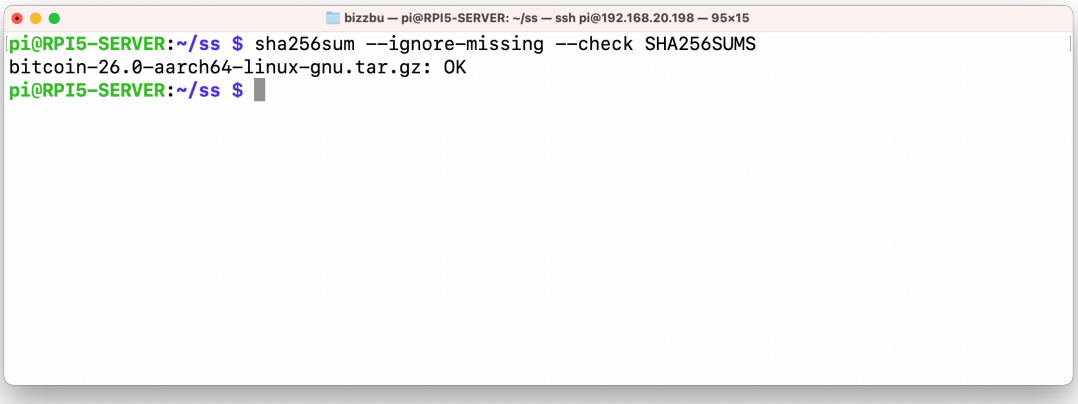
Pokud by se jednodeskový počítač nezabezpečil správně, mohlo by to mít za následek řadu technických a bezpečnostních problémů. Neautorizovaní uživatelé by mohli získat přístup k systému, což by mohlo vést k odcizení citlivých informací a finančních prostředků. Mohli by rovněž instalovat malware nebo ransomware, který by mohl způsobit poškození systému nebo

ztrátu dat. Nepříznivě by to mohlo ovlivnit výkon a dostupnost systému, když by se například zvýšila zátěž sítě kvůli distribuovaným útokům odmítnutí služby. Systém by také mohl být využíván pro nelegální aktivity bez vědomí majitele.

4.4.2 Bitcoin Core služba

V Lightning Network je nezbytné, aby byl pro odesílání transakcí otevírajících nebo zavírajících platební kanály zajištěn přístup do bitcoinové sítě, což vyžaduje provoz plného bitcoinového uzlu. Tento uzel je využíván také pro monitorování potenciálního odeslání již zneplatněného stavu kanálu protistranou. Z toho důvodu je potřeba nainstalovat a nakonfigurovat aplikaci Bitcoin Core.

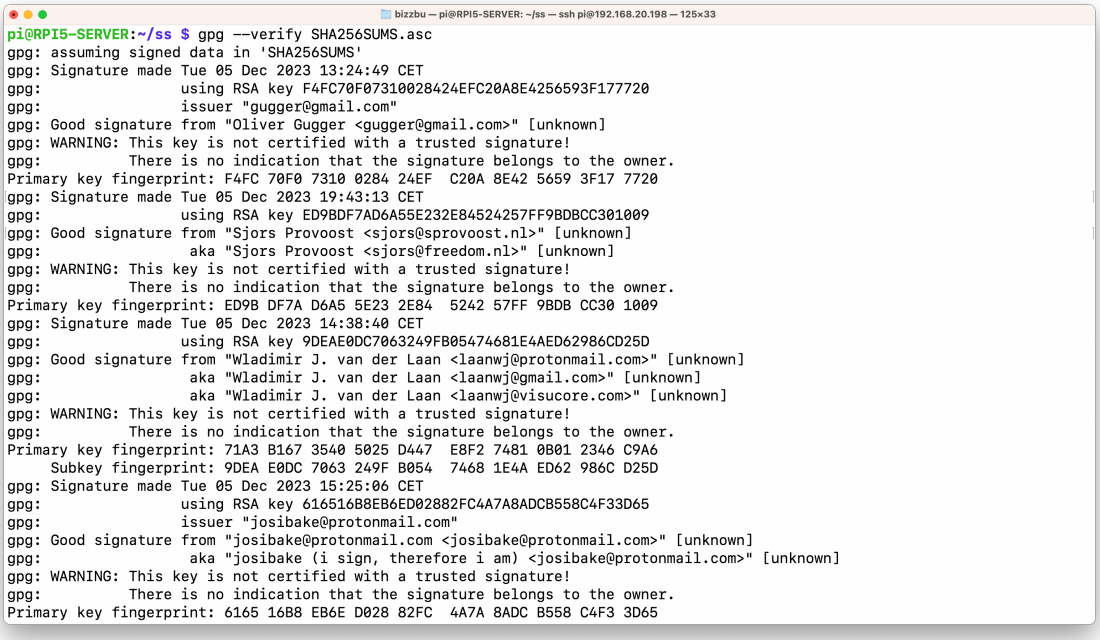
Je zásadní stahovat Bitcoin Core nejnovější verze, a to pouze z ověřených zdrojů. I když je zdroj důvěryhodný, je nutné provést ověření kontrolního součtu a podpisu, aby se předešlo riziku infekce malwarem, manipulace se softwarem nebo jiným bezpečnostním hrozbám, které by mohly ohrozit bezpečnost kryptoměny a soukromí uživatele. K ověření kontrolního součtu, který je stažen společně s Bitcoin Core, se využívá příkaz, který porovná součet souboru a jeho výpočet (viz Obrázek 17).



Obrázek 17: Ověření kontrolního součtu pomocí příkazu [vlastní zpracování]

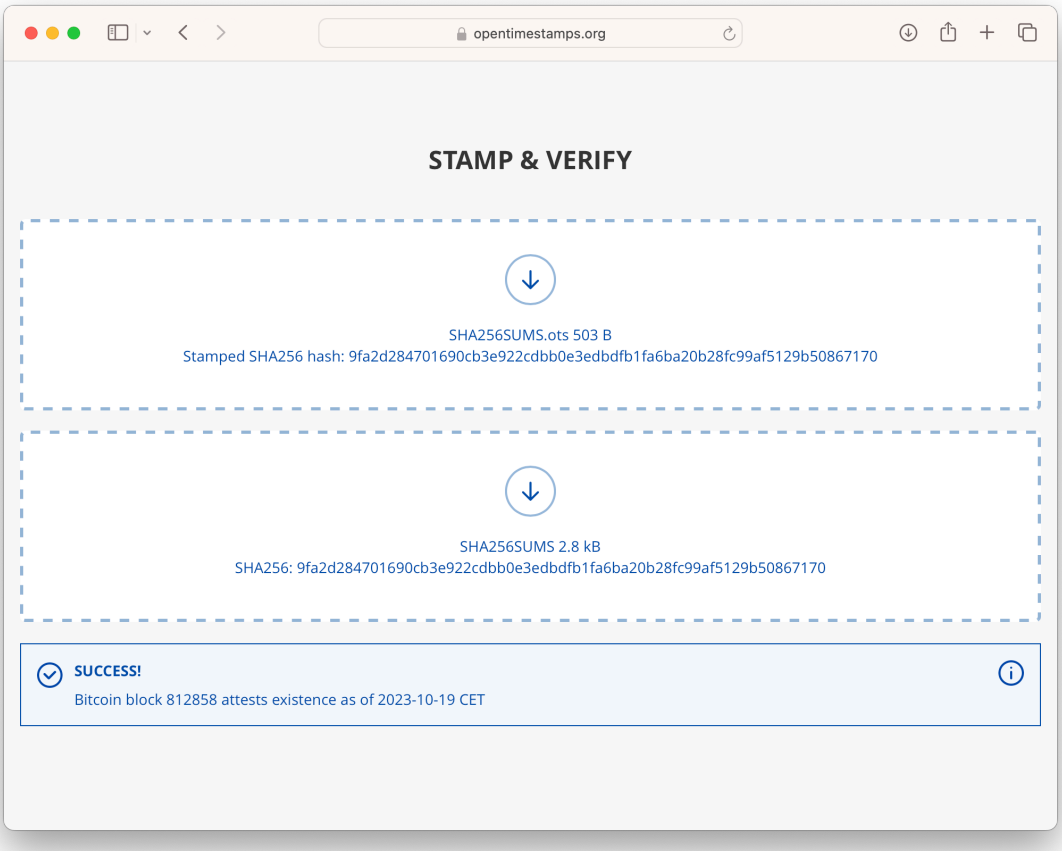
Pro ověření platnosti podpisů u verzí Bitcoin Core, které podepisuje několik jednotlivců každý svým klíčem, je nutné nejprve importovat odpovídající veřejné klíče do databáze GPG klíčů. Pro ověření, že soubor s kontrolními součty je kryptograficky podepsán pomocí klíčů pro vydání, je třeba použít příkaz, který ověří podpisy pro každý z veřejných klíčů, které

podepsaly kontrolní součty. Při kontrole je důležité se ujistit, že alespoň několik podpisů ukazuje očekávaný text, což potvrzuje jejich pravost. Tento krok zajišťuje, že balíček nebyl pozměněn a je bezpečný k použití.



Obrázek 18: Ověření integrity podpisu pomocí příkazu

Pro ověření, že soubor s kontrolními součty pro Bitcoin Core existoval k určitému datu, lze použít protokol OpenTimestamps. Stačí stáhnout soubor SHA256SUMS a jeho timestamp důkaz (SHA256SUMS.ots) z oficiálního webu Bitcoin Core a poté tyto soubory nahrát na webovou stránku OpenTimestamps pro ověření. Pokud je časové razítko ověřeno, web napíše potvrzení, že soubor s kontrolními součty existoval již v době vydání Bitcoin Core.



Obrázek 19: Ověření časového razítka na webu opentimestamps.org [vlastní zpracování]

Z bezpečnostního hlediska je důležité každou službu spouštět přes svého uživatele. Je tedy třeba pro službu s Bitcoin Core vytvořit uživatele s názvem, ze kterého se bude dát vyčíst, že se jedná o uživatele zaštiťující tuto službu. Pro dotazování Bitcoin Core ostatními programy je nutné mít správné přístupové údaje. Aby se předešlo ukládání uživatelského jména a hesla v konfiguračním souboru v prostém textu, je heslo hašováno. Bitcoin Core pak může přijmout heslo, zahašovat ho a porovnat s uloženým hašem, aniž by bylo možné získat zpět původní heslo. Alternativně lze přístupové údaje získat prostřednictvím souboru s příponou *.cookie* ve složce s daty Bitcoinu.

Dále je nutné nastavit konfigurační soubor Bitcoin Core. V něm lze nastavit mnoho parametrů podle potřeb uživatele. Mezi ně patří například parametr *server*, který umožňuje Bitcoin Core fungovat jako server, parametr *rpcuser* a *rpcpassword* pro nastavení autentizačních údajů RPC, parametr *maxconnections* pro limitování počtu peerů, parametr *testnet* pro použití testovací sítě Bitcoinu, parametr *txindex* pro vytvoření kompletního indexu

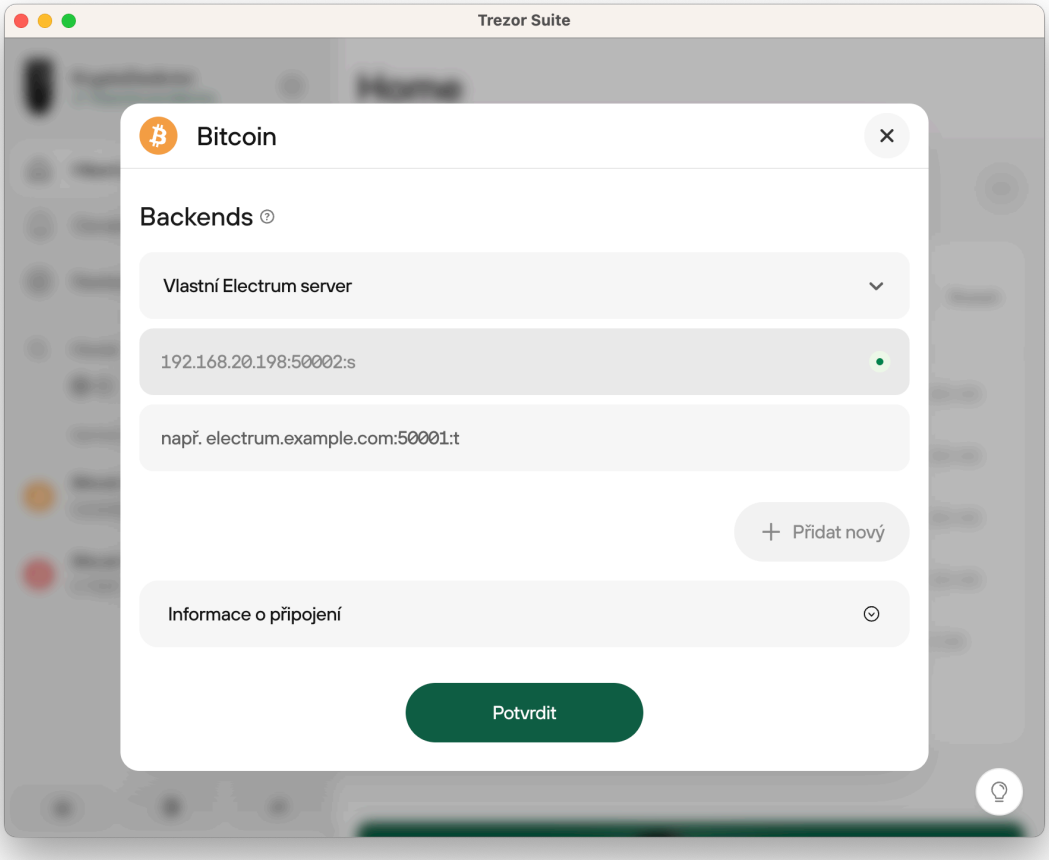
transakcí, a parametr *walletnotify* pro spuštění skriptu při detekci transakce spojené s peněženkou. Také je možné v souboru nastavit složku pro určení místa ukládání dat bitcoinového uzlu. Na internetu jsou k dispozici specializované nástroje, které umožňují odborně vygenerovat konfigurační soubor. Tyto nástroje poskytují uživatelsky přívětivé rozhraní, kde si uživatel vybere různé konfigurační parametry a na základě daných voleb nástroj vytvoří příslušný konfigurační soubor. Pomáhají uživatelům efektivně nakonfigurovat Bitcoin Core bez hluboké technické znalosti všech dostupných parametrů.

Pro automatické spuštění Bitcoin Core po restartu zařízení je možné vytvořit službu v systemd, což je systém pro správu systému a služeb v Linuxu. Tím se vytvoří služba, která zajistí, že Bitcoin Core se automaticky spustí při každém zapnutí počítače. K tomu slouží konfigurační soubor umístěný v */etc/systemd/system/*, který definuje, jak a kdy se má Bitcoin Core spustit. Po spuštění Bitcoin Core dojde k synchronizaci s blockchainem. To je proces, kdy se lokální instance softwaru aktualizuje na nejnovější stav celého blockchainu. Tato synchronizace může trvat až několik dní v závislosti na rychlosti internetového připojení, výkonu počítače a rychlosti disku, jelikož celý blockchain je velmi rozsáhlý a obsahuje všechny transakce od počátku existence Bitcoinu.

Pro integraci Bitcoin Core s peněženkami je nutné nastavit Electrum server jako jejich prostředníka. Ten importuje data z Bitcoin Core a poskytuje je softwarovým peněženkám, které podporují protokol Electrum. Díky tomu je možné využívat desktopové peněženky podporující hardwarové peněženky, ve spojení s vlastním Bitcoin node. Je nezbytné nastavit NGINX reversní proxy server pro přidání šifrování SSL/TLS komunikace Electrs na portech 50001 a 50002, aby byla zajištěna bezpečná výměna dat. Toho se docílí vytvořením dalšího konfiguračního souboru ve složce NGINX konfigurací. Toto nastavení posílí ochranu komunikace a zajistí, že data mezi vaším zařízením a Electrs serverem budou šifrována a tím lépe chráněna před potenciálními útoky. Pro spuštění Electrum serveru je efektivní a výkonnou možností použít Electrs, což je Electrum server psaný v jazyce Rust. V tomto kroku je opět důležité ověřit integritu podpisu, vytvořit službu, která bude Electrs spouštět automaticky při každém startu počítače, a pro ní vytvořit jejího vlastního uživatele, pod kterým bude spouštěna.

Po dokončení instalace, konfigurace a synchronizace Electrs serveru k němu lze jednoduše připojit softwarové peněženky, které umožňují uživatelům spravovat své transakce a prostředky s vyšší úrovní soukromí a bezpečnosti. V aplikaci desktopové peněženky je nutné

vyplnit IP adresu či hostname zařízení, port Electrum serveru a následně zvolit mezi SSL či TLS protokolem (viz Obrázek 20).



Obrázek 20: Připojení Electrum serveru v aplikaci Trezor Suite [vlastní zpracování]

4.4.3 Lightning Network

Pro LN existuje několik implementací, které se dodržují The Basis of Lightning Technology (BOLT) specifikace pro vzájemnou kompatibilitu. BOLT je sada standardních protokolů a pravidel pro Lightning Network, které definují, jak by měly různé implementace LN spolu komunikovat a fungovat. Mezi nejvýznamnější patří LND, Core Lightning a Eclair, každá s unikátními charakteristikami a zaměřením, jenž uživatelům nabízí různé možnosti využití v závislosti na jejich potřebách a technickém prostředí.

LND, vyvinuté společností Lightning Labs, je široce přijímané díky své robustnosti a rozsáhlé dokumentaci. Nabízí komplexní API rozhraní a podporuje různé back-endy, což

uživatelům umožňuje flexibilitu ve výběru konfigurace a širokou škálu aplikací a nástrojů pro správu uzlu. Core Lightning od Blockstream se naopak zaměřuje na pokročilé uživatele s potřebou hlubší konfigurace a optimalizace. Jeho modulární architektura a pluginový systém poskytuje prostor pro vlastní úpravy a specializaci podle specifických požadavků a scénářů využití. Eclair od společnosti ACINQ nabízí jak robustní řešení pro servery a podnikové klienty, tak i mobilní aplikace pro individuální uživatele, čímž zdůrazňuje flexibilitu a přístupnost technologie Lightning Network širšímu spektru uživatelů.

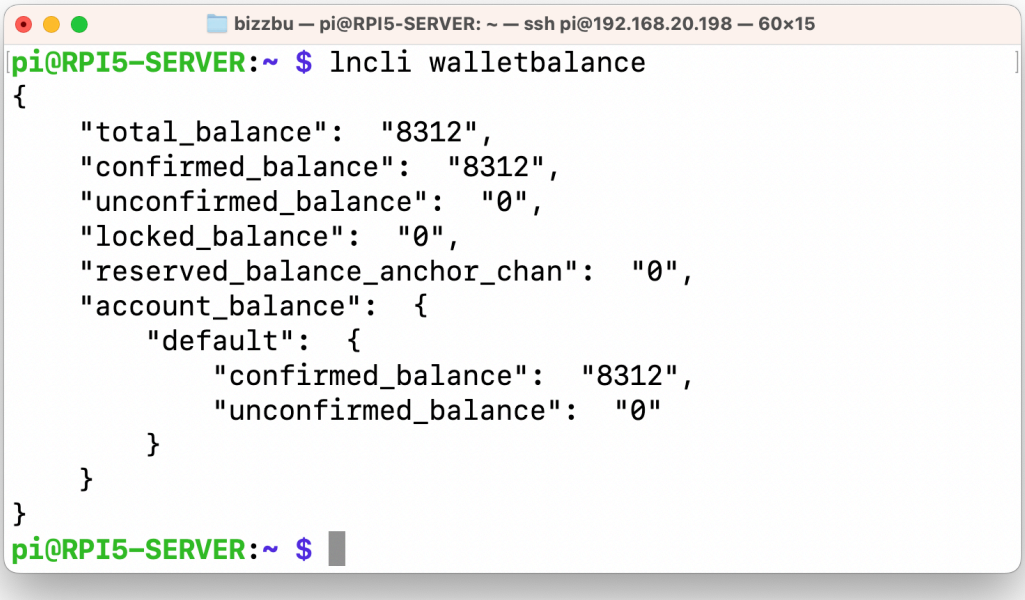
Při instalaci LND je zásadní opět ověřit kontrolní součet, digitální podpisy a časové razítko. Ověření časového razítka potvrzuje, že soubor existoval v určitém čase, což přidává další vrstvu bezpečnostního ověření. Tyto kroky společně zajišťují vyšší úroveň zabezpečení během procesu instalace. Stejně jako u předešlé instalace je nutné vytvořit pro LND službu svého uživatele a zajistit tím větší bezpečnost.

Obrázek 21: Ověření integrity podpisu pomocí příkazu [vlastní zpracování]

LND obsahuje Bitcoin peněženku, která spravuje on-chain a Lightning mince a je chráněna heslem, které je nutné zadat při každém spuštění LND. Tento stav není ideální z hlediska bezpečnosti. Uživatel má tak dvě možnosti, jak postupovat – buď je nutné po každém restartu počítače ručně odemknout LND, nebo je možné heslo uložit na uzlu pro jeho automatické odemknutí. I když druhá možnost nabízí pohodlí, z hlediska zabezpečení není ideální. Existují však metodiky a pokročilé přístupy, které umožňují zabezpečení tohoto procesu bez nutnosti kompromisu na pohodlí či bezpečnosti. Ostatní zmíněné implementace heslo nemají.

Po úspěšném spuštění LND následuje proces vytvoření peněženky, kde je nutné nastavení hesla peněženky a k zaznamenání seed fráze. Seed fráze je sada slov, která slouží k obnově

peněženky v případě ztráty nebo poškození. Proto je zásadní, aby seed fráze byla vždy pečlivě zapsána a uložena na bezpečném místě, protože kdokoli, kdo má k této frázi přístup, může obnovit peněženku a získat tak přístup k prostředkům.

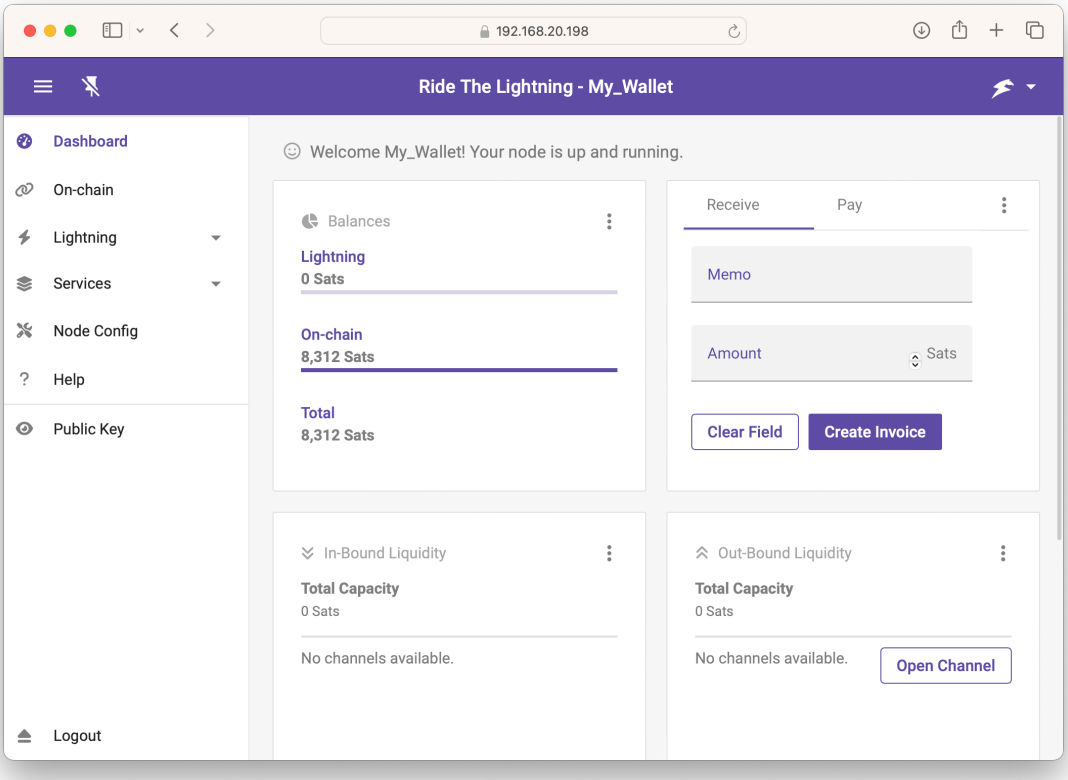


Obrázek 22: Výpis zůstatku LN peněženky [vlastní zpracování]

V posledním kroku je zde možnost, aby si uživatel správu LN uzlu zjednodušil instalací webového rozhraní. Takové webové rozhraní umožňuje uživatelům interagovat s jejich uzlem přes grafické uživatelské prostředí v prohlížeči, což zjednodušuje procesy jako je sledování stavu uzlu, správa platebních kanálů, provádění transakcí, nebo aplikace různých konfiguračních nastavení. Tyto rozhraní poskytují intuitivní a vizuálně přehledný způsob správy uzlu, který je přístupný i pro uživatele bez pokročilých technických dovedností.

Vzhledem k tomu, že RTL je přístupné přes internet, je klíčové před instalací nastavit reverse proxy na portech 3000 a 4001 pro tuto službu. K plynulému a bezproblémovému fungování RTL, napsaného v JavaScriptu, je nezbytná instalace Node.js. Zásadní je také důkladně ověřit bezpečnost zdrojového kódu a ujistit se o jeho bezchybnosti. Pro zvýšení bezpečnosti je nutné vytvořit speciálního uživatele pro správu RTL, což výrazně snižuje riziko neautorizovaného přístupu. Nakonec je nutné přizpůsobit vzorový konfigurační soubor specifickým potřebám uživatele. Navíc je opět potřeba vytvořit službu pro automatické spuštění

RTL při startu systému. Webové rozhraní RTL je dostupné z jakéhokoliv prohlížeče na IP adrese jednodeskového počítače a portu 4001 (viz Obrázek 23).



Obrázek 23: Webové rozhraní RTL [vlastní zpracování]

5 Výsledky a diskuse

Na základě výsledků vícekriteriální analýzy variant je možné usoudit, že Raspberry Pi 5 je nejlepší volbou pro využití v Lightning Network síti z hlediska technických specifikací podložených zátěžovými testy, přičemž Banana Pi M5 a Raspberry Pi 4 Model B jsou dobré alternativy, pokud je počítač Raspberry Pi 5 z nějakého důvodu nemožné použít. Raspberry Pi 3 Model B+ a Jetson Nano jsou méně vhodné volby kvůli jejich nižšímu výkonu v testovaných kritériích (viz Kapitola 4.1.2).

Pro nezkušené uživatele je vhodnější využít již hotová řešení pro zprovoznění LN uzlu, jelikož tyto předkonfigurované platformy snižují složitost nastavení a minimalizují riziko chyb, které by mohly vést k napadení zařízení a krádeži finančních prostředků. Naproti tomu pokročilí uživatelé by měli preferovat samostatnou konfiguraci svého uzlu, neboť jim to umožňuje větší kontrolu a možnost přizpůsobení zařízení podle vlastních potřeb a preferencí, i když tento přístup přináší vyšší požadavky na technické znalosti a zvýšené riziko potenciálních chyb v konfiguraci (viz Kapitola 4.2).

5.1 Využití LN uzlu na jednodeskovém počítači

Jednodeskové počítače nabízejí dostatečný výkon pro provoz Lightning uzlu, přičemž se jeví i jako ekonomické řešení. Pro provozování standardního uzlu postačí běžný jednodeskový počítač v peněžní hodnotě v řádu několika tisíc korun. Navíc jedním z jejich hlavních benefitů je nízká spotřeba elektrické energie a možnost pasivního chlazení, díky čemuž je provoz těchto zařízení velice tichý. Tyto vlastnosti činí toto řešení vhodné pro domácí použití.

Nicméně je třeba počítat s tím, že v domácím prostředí se mohou občas vyskytnout výpadky elektrického proudu nebo internetového připojení, které je možné v případě potřeby řešit pomocí záložních zdrojů. Mohou zde také nastat omezení související s výkonem zařízení, přičemž upgradování jednotlivých komponent na výkonnější verze je zde prakticky nemožné. Jako alternativa se nabízí možnost provozování klasického serveru doma, pokud to podmínky dovolují, což dává plnou kontrolu nad systémem. Pro firemní účely jsou více využívaná cloudová řešení na x86 platformě, která jsou sice nákladnější, ale nabízí komplexní řešení včetně chlazení, napájení, zálohování a zajištění statické IP adresy a garantované dostupnosti. Klíčovou výhodou je možnost dynamického navyšování zdrojů podle aktuálních potřeb.

5.2 Podpora Bitcoin sítě

Účast na fungování Bitcoin a Lightning Network sítě je klíčová pro zabezpečení, efektivitu a budoucí růst obou těchto sítí. Jelikož je Bitcoin decentralizovaná síť, každý, kdo provozuje plný uzel, přispívá k její odolnosti proti útokům a manipulaci, podporuje decentralizaci a pomáhá udržet síť bezpečnou a nezávislou. Provozování uzlu znamená účast v procesu ověřování a potvrzování transakcí. To je zásadní pro ochranu integrity celého systému.

Lightning Network síť přináší inovativní řešení pro rychlejší a levnější transakce, čímž zvyšuje škálovatelnost Bitcoinu a zároveň snižuje zatížení jeho hlavního blockchainu. Každý, kdo se zapojí do podpory těchto sítí, přispívá k silnějšímu, rychlejšímu a cenově efektivnějšímu ekosystému, což má prospěch pro celou komunitu uživatelů těchto přelomových technologií. Taková podpora a účast také stimuluje inovace a rozvoj, což je nezbytné pro adaptabilitu a růst obou technologií. Když vývojáři a firmy vidí silnou a zdravou síť, jsou motivováni k vytváření nových produktů a služeb. Tím se podporuje širší adopce Bitcoinu a udržuje jeho základní principy decentralizace a otevřenosti.

6 Závěr

Cílem bakalářské práce bylo zhodnotit možnosti využití jednodeskových počítačů jako uzlu v Lightning Network síti. V rámci literární rešerše byly přezkoumány a zhodnoceny relevantní zdroje v oblasti zkoumaného tématu. Teoretická část se podrobně zabývala technickým popisem jednodeskových počítačů z řady Raspberry Pi, z rodiny Arduino a počítačů Jetson Nano a Banana Pi M5. Dále se zabývala úvodem do kryptoměnového světa, kde byla detailněji probrána kryptoměna Bitcoin, technologie Blockchain a její druhá vrstva Lightning Network síť. Teoretická část se dále věnovala i vícekriteriální analýze variant, která poskytla hlubší porozumění pro výběr optimálního řešení.

V praktické části byla provedena analýza jednodeskových počítačů a poté byly počítače vybrány s ohledem na doporučené požadavky pro provoz uzlu v síti Lightning Network. Na daných počítačích byly provedeny zátěžové testy, které sloužily jako podklad k vícekriteriální analýze variant. Zá základě jejího výsledků byl vybrán a doporučen nejvhodnější počítač, na kterém byla provedena implementace Lightning uzlu a prozkoumány jeho možnosti zprovoznění.

7 Seznam použitých zdrojů

[1] Steven J. Johnston, Philip J. Basford, Colin S. Perkins, Herry Herry, Fung Po Tso, Dimitrios Pezaros, Robert D. Mullins, Eiko Yoneki, Simon J. Cox, Jeremy Singer, „Commodity single board computer clusters and their applications,“ 2024. [Online]. Dostupné z: https://www.sciencedirect.com/science/article/pii/S0167739X18301833?via%3Dihub.

[2] J. Doerr, „"Low-cost microcomputing: The personal computer and single-board computer revolutions," in Proceedings of the IEEE, vol. 66, no. 2, pp,“ 2024. [Online]. Dostupné z: https://ieeexplore.ieee.org/document/1455131.

[3] A. N. E. Belferd and A. Rahmoun,, „A Single Board Computer and its Cluster Applications," 2022 2nd International Conference on Advanced Electrical Engineering (ICAEE),“ 2024. [Online]. Dostupné z: https://ieeexplore.ieee.org/document/9962136.

[4] „RaspberryPi.com,“ 2023. [Online]. Dostupné z: https://www.raspberrypi.org/help/what-%20is-a-raspberry-pi/.

[5] „RaspberryPi.com,“ 2024. [Online]. Dostupné z: https://www.raspberrypi.com/app/uploads/2022/02/COLOUR-Raspberry-Pi-Symbol-Registered.png.

[6] EBEN UPTON, GARETH HALFACREE, Raspberry Pi - Uživatelská příručka, Brno: Computer Press, 2013.

[7] „RPishop.cz,“ 2024. [Online]. Dostupné z: https://rpishop.cz/raspberry-pi-3b/283-raspberry-pi-3-model-b-64-bit.html.

[8] „Wikimedia.org,“ 2024. [Online]. Dostupné z: https://upload.wikimedia.org/wikipedia/commons/b/b4/Raspberry_Pi_3_Model_B.png.

[9] „RPishop.cz,“ 2024. [Online]. Dostupné z: https://rpishop.cz/raspberry-pi-3b/896-raspberry-pi-3-model-b-plus-64-bit-1gb-ram.html.

[10] „RPishop.cz,“ 2024. [Online]. Dostupné z: https://rpishop.cz/raspberry-pi-3a/1114-raspberry-pi-3-model-a.html.

[11] „RPishop.cz,“ 2024. [Online]. Dostupné z: https://rpishop.cz/wp-content/uploads/2018/03/4350-Raspberry-Pi-3-Model-B-64-bit-1GB-RAM.jpg .

[12] „RPishop.cz,“ 2024. [Online]. Dostupné z: https://rpishop.cz/raspberry-pi-4/2611-raspberry-pi-4-model-b-8gb-ram.html.

[13] „RPishop.cz,“ 2024. [Online]. Dostupné z: https://rpishop.cz/wp-content/uploads/2019/06/6028-Raspberry-Pi-4-Model-B-2GB-RAM.jpg.

[14] „RPishop.cz,“ 2024. [Online]. Dostupné z: https://rpishop.cz/raspberry-pi-5/6498-raspberry-pi-5-8gb-ram.html.

[15] „RPishop.cz,“ 2024. [Online]. Dostupné z: https://rpishop.cz/wp-content/uploads/2023/09/31088-Raspberry-Pi-5-8GB-RAM.jpg.

[16] „NVIDIA.com,“ 2024. [Online]. Dostupné z: https://developer.nvidia.com/embedded/jetson-nano-developer-kit.

[17] „NVIDIA.com,“ 2024. [Online]. Dostupné z: https://www.nvidia.com/content/dam/en-zz/Solutions/intelligent-machines/jetson-nano/nvidia-jetson-nano-developer-kit-2c50-p@2x.png.

[18] „Banana-pi.org,“ 2024. [Online]. Dostupné z: https://docs.banana-pi.org/en/home.

[19] „Banana-pi.org,“ 2024. [Online]. Dostupné z: https://docs.banana-pi.org/en/BPI-M5/BananaPi_BPI-M5.

[20] „Botland.cz,“ 2024. [Online]. Dostupné z: https://cdn3.botland.cz/100851-large_default/banana-pi-m5-4gb-ram.jpg.

[21] „Arduino.cc,“ 2024. [Online]. Dostupné z: https://docs.arduino.cc/learn/starting-guide/getting-started-arduino/.

[22] „Arduino.cc,“ 2024. [Online]. Dostupné z: https://docs.arduino.cc/static/d0c28c5bd0894792476c6052dea5fa63/29114/board-anatomy.png.

[23] J. Blum, Exploring Arduino: tools and techniques for engineering wizardry. Second edition, Indianapolis: Wiley, 2020.

[24] „Arduino.cc,“ 2024. [Online]. Dostupné z: https://docs.arduino.cc/hardware/portenta-h7/.

[25] M. Novák, Lightning Network: Platby budoucnosti, Braiins Publishing, 2023.

[26] S. Jokić, „et al. Comparative analysis of cryptocurrency wallets vs traditional wallets,“ 2024. [Online]. Dostupné z: https://doi.org/10.5937/ekonomika1903065J.

[27] Dominik Stroukal, Jan Skalický, Bitcoin: Peníze budoucnosti, Mises, 2015.

[28] Shaofeng Lin, Yihan Kong, Shaotao Nie, „Overview of Block Chain Cross Chain Technology,“ 2022. [Online]. Dostupné z: doi:10.1109/ICMTMA52658.2021.00083.

[29] S. Nakamoto, „Bitcoin: A Peer-to-Peer Electronic Cash System,“ 2009.

[30] J. Poon, „The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,“ 2016.

[31] T. Šubrt, „Ekonomicko-matematické metody,“ Aleš Čeněk s.r.o, 2019.

8 Seznam obrázků, tabulek, grafů a zkratek

8.1 Seznam obrázků

8.2 Seznam tabulek

8.3 Seznam použitých zkratek

AI – Artificial Intelligence

API – Application Programming Interface

BOLT – Basis of Lightning Technology

BTC – Bitcoin

CPU – Central Processing Unit

CSI – Camera Serial Interface

CSV – Comma-separated values

eMMc – embedded MultiMediaCard

FW – Firewall

GND – Ground

GPG – GNU Privacy Guard

GPU – Graphics processing unit

HD – High-Definition

HDMI – High-Definition Multimedia Interface

HDR – High Dynamic Range

HEVC – High Efficiency Video Coding

HTLCs – Hashed Time-Locked Contracts

HTML – HyperText Markup Language

I/O – Input/Output

IEEE –Institute of Electrical and Electronics Engineers

IP – Internet Protocol

JPEG – Joint Photographic Experts Group

JSON – JavaScript Object Notation

LCD – Liquid Crystal Display

LED – Light-emitting Diode

LN – Lightning Network

LPDDR – Low-Power Double Data Rate

MAC – Media Access Control

MIPI – Mobile Industry Processor Interface

NFC – Near-field Communication

OS – Operating System

P2P – Peer-to-Peer

QR – Quick-response

RAM – Random Access Memory

RPC – Remote Procedure Call

SD – Secure Digital

SSD – Solid-state Drive

SSH – Secure Shell

SSL – Secure Sockets Layer

TLS – Transport Layer Security

USB – Universal Serial Bus

Wi-Fi – Wireless Fidelity