Bitcoinová síť a transakční vrstva Lightning Network

Tomáš Hanzelka

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav informatiky a umělé inteligence

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tomáš Hanzelka**
Osobní číslo:	**A18041**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Softwarové inženýrství**
Forma studia:	**Prezenční**
Téma práce:	**Bitcoinová síť a transakční vrstva Lightning network**
Téma práce anglicky:	**The Bitcoin Network and Transaction Layer Lightning Network**

Zásady pro vypracování

1. Proveďte rešerši na dané téma.
2. Zaměřte se na možnosti těžení v síti Bitcoin, popište současné možnosti těžení.
3. Prozkoumejte transakční vrstvu Lightning Network a možnosti její implementace.
4. V praktické části implementujte vlastní Lightning Network uzel pomocí vhodného nástroje.
5. Analyzujte navržené řešení z pohledu ekonomického a energetického.

Forma zpracování bakalářské práce: **Tištěná/elektronická**

Seznam doporučené literatury:

1. STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. 2., rozšířené vydání. Praha: Grada Publishing, 2018. Finance pro každého. ISBN 978-80-271-0742-1.
2. M. ANTONOPOULOS, Andreas. Mastering Bitcoin: Programming the Open Blockchain. 2. 2020.
3. M. ANTONOPOULOS, Andreas, Olaoluwa OSUNTOKUN a René. Mastering the Lightning Network: A Second Layer Blockchain Protocol for Instant Bitcoin Payments. 2019.
4. AMMOUS, Saifedean. The Bitcoin Standard: The Decentralized Alternative to Central Banking.

Vedoucí bakalářské práce: **doc. Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **15. ledna 2021**
Termín odevzdání bakalářské práce: **17. května 2021**

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
DĚKAN
L.S.

prof. Mgr. Roman Jašek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 7. 5. 2021

Tomáš Hanzelka v. r.
podpis studenta

ABSTRAKT

Cílem práce je ukázat Bitcoin jako otevřenou technologii, která může být pro lidi užitečným nástrojem a ukázat, na jakých technologických principech je Bitcoin postaven. V práci jsou popsány výhody a nevýhody decentralizovaného řešení, kterým Bitcoin je a zároveň je popsáno, jakým způsobem je Bitcoin chráněn před možným útokem. V teoretické části je vysvětlena také funkčnost a bezpečnostní mechanismy nové transakční vrstvy Lightning Network. Praktická část ukazuje použití Lightning Network v praxi s postavením vlastního uzlu, který funguje jako součást decentralizované Bitcoinové sítě. V teoretické i praktické části je kladen důraz na ekonomické hledisko těžby a provozu Lightning Network uzlu.

Klíčová slova: Bitcoin, blockchain, uzel, těžení, těžař, Satoshi, proof of work, Lightning Network, myNode

ABSTRACT

The aim of this work is to display Bitcoin as an open technology that can be a useful tool for people and to demonstrate the technological principles Bitcoin is based on. The work describes the advantages and disadvantages of a decentralized solution, which Bitcoin is, and describes how Bitcoin is protected from possible attacks. The theoretical part also explains the functionality and security mechanisms of a new transaction layer called the Lightning Network. The practical part shows how the Lightning Network is used in practice with the positioning of its own node, which works as part of the decentralized Bitcoin network. In the theoretical and practical part, emphasis is placed on the economic impact of mining and the operation of the Lightning Network node.

Keywords: Bitcoin, blockchain, node, mining, miner, Satoshi, proof of work, Lightning Network, myNode

„The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust. “

Satoshi Nakamoto

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Bitcoin po dobu 12 let své existence ušel dlouhou cestu. Velké množství lidí si nějakou kryptoměnu koupilo, buď jako spekulaci nebo jako novou technologii. Objevují se firmy, které investují část svých volných prostředků do Bitcoinu a jiných kryptoměn. Začínají se objevovat i finanční instrumenty, které umožňují institucím snadnou investici do Bitcoinu. Některé společnosti dokonce začínají umožňovat svým zákazníkům provádět platbu v Bitcoinu.

Bitcoin nemá centrální bod, a to přináší mnoho výhod a nevýhod. Bitcoin jako decentralizovaný systém je komplikovanější než centralizované systémy, a to hlavně kvůli tomu, že musí být zajištěno, aby data byla na všech uzlech systému stejná. Také nesmí docházet ke dvojím útratám jedné transakce, to by mohlo vzniknout kvůli tomu, že by se každý uzel nacházel na jiném místě na světe a obdrží informaci v jiný čas než ostatní uzly. Všechny tyhle problémy musely být vyřešeny, aby mohl Bitcoin jako decentralizovaný systém fungovat.

Cílem práce je vysvětlit tyto základy a principy a představit Bitcoin především jako otevřenou technologii, která umožňuje lidem po celém světě převádět hodnotu jen prostřednictvím internetu a chytrého telefonu bez toho, aniž by museli využívat tradiční finanční nástroje. Tradiční finanční nástroje fungují dobře, ale Bitcoin umožňuje lidem navíc ochránit svoje soukromí a být svou vlastní bankou.

V posledních letech probíhá na Bitcoinu intenzivní vývoj, který umožňuje lidem používat bezpečnější, efektivnější a uživatelsky přívětivější Bitcoinovou síť. Názorným příkladem je Lightning Network, díky které je možné provádět téměř instantní bitcoinové transakce se zanedbatelným poplatkem.

I. TEORETICKÁ ČÁST

1 HISTORIE

Bitcoin jako digitální měna byl popsán v roce 2008 osobou jménem Satoshi Nakamato. Tohle jméno, jak se později zjistilo, je zcela vymyšlené [1].

Po dobu existence Bitcoinu se objevilo několik osob, které označovaly sebe nebo jiné za tvůrce, ale tyto domněnky nebyly nikdy dokázány, jelikož sám Satoshi Nakamato vlastní velké množství Bitcoinových mincí, které by mohl předložit veřejnosti, pokud by chtěl dokázat svoji identitu [2].

Samotný princip a fungování systému byl popsán v tzv. „Bitcoin White Paper“. Dokument má délku asi 8 stran a je v něm popsáno proč Bitcoin vznikl, jaký má účel, jak funguje provádění transakcí, je popsán algoritmus Proof-of-Work, jak se těží, jak se ověřují transakce a jak ochraňuje soukromí. Snahy o stvoření internetových peněz existovaly ještě před vznikem Bitcoinu. Sám Satoshi Nakamoto zmiňuje ve White Paperu projekty b-money a Hashcash, které se pokoušely stát „internetovými penězi“. Satoshi Nakamoto byl předešlými pokusy inspirován a použil některé fungující koncepty právě v Bitcoinu [3].

První verze Bitcoinového software měla pouze 3000 řádků. S postupem času, jak se vyvíjel, zvýšil svůj počet řádku až na 100 000. Tento počet neustále stoupá s tím, jak se Bitcoin dále vyvíjí. Bitcoin je open-source projekt, a proto celý kód Bitcoinu včetně jeho první verze je veřejně dostupný na webu GitHub, jež se stará o uchovávání softwarových projektů [4].

Jako první známá transakce uvnitř bitcoinové sítě, která byla za nějaký reálný produkt, je koupě pizzy, která byla prodána za 10 000 BTC. Transakce proběhla v roce 2010 v USA ve státě Florida. Tento den se zapsal do historie známý jako „Bitcoin Pizza Day“, a je známý především proto, že v dnešní době by tyto mince měly hodnotu milionkrát větší [5].

Se zvyšující se oblíbeností virtuálních měn začaly vznikat první burzy, kde bylo možné nakoupit a prodat mince Bitcoinu za měny jako USD, EUR atp. Po dobu existence bylo mnoho burz již vykradeno hackery [7], a to se na ceně Bitcoinu podepsalo, jelikož taková situace způsobila, krátkodobou nedůvěru a strach [8].

Později se začaly objevovat i směnárny, kde je možné kryptoměny nakoupit mnohem snadněji. Rozdíl mezi směnárnami a burzami je ten, že na burze se pouze setkává nabídka s poptávkou, zatímco směnárna vypíše kurz a za ten mohou lidé nakupovat. Obecně platí, že na burze jsou ceny lepší, protože směnárny provozují svoje služby s většími poplatky. Úplně nejjednodušší způsob nákupu kryptoměn je přes tzv. „Bitcoinomat“. Bitcoinomaty se

nachází ve velkých nákupních centrech. Jedná se o automat, který vypadá podobně jako obyčejný výběrový bankovní automat a funguje velmi podobně. Na automatu zadáte, jaký obnos mincí chcete pořídit, popřípadě kolik chcete utratit peněz. Do Bitcoinmatu vložíte peníze a vyjede vám účtenka s QR kódem, který reprezentuje privátní klíč. Privátní klíč dovoluje obnos mincí utratit. [9].

V poslední době se začaly objevovat obchody a služby, které umožňují příjem kryptoměn. Dnes již existují platební brány, které toto umožňují. Nejznámější z nich je Bitpay, ale existují další, jako například CoinGate a CoinPayments. Dokonce se objevily i open-source projekty jako BTCPay, díky nim je možné, provozovat zcela vlastní platební bránu bez poplatků a na vlastním serveru [10].

V roce 2017 spustil platby za zboží kryptoměnami největší český e-shop Alza.cz. Nejprve bylo dostupné placení jen pomocí Bitcoinu, postupem času rozšířila platbu o placení Litecoinem a dalších kryptoměn [11]. Později začala Alza.cz provozovat Bitcoinomaty ve svých prodejnách [12]. V Praze byla dokonce zprovozněna čerpací stanice s názvem Kryptotank, kde je možné natankovat pohonné hmoty za kryptoměny [13].

2 ZÁKLADNÍ CHARAKTERISTIKA

Ve své nejhlubší podstatě je Bitcoin počítačový program, ale především se jedná o decentralizovaný systém pro převod hodnoty (peněz). V samotném White Paperu je Bitcoin označován jako Peer-to-Peer elektronický peněžení systém, protože Bitcoinová síť nemá žádný centrální bod. Veškeré transakce jsou ověřovány a zapisovány pomocí jednotlivých uzlů v síti. Za uzlem se může skrývat kdokoliv, kdo má zájem zlepšovat bezpečnost Bitcoinové sítě, těžař nebo také prostý uživatel s nainstalovanou peněženkou na elektronickém zařízení [3].

Z toho důvodu, že se jedná o decentralizovaný systém, je velmi těžké zastavit fungování celé Bitcoinové sítě. Na některých z uzlů, je uložena celá databáze transakcí, nazývána jako blockchain. Transakce jsou tvořeny uživateli sítě, kteří mají zájem mezi sebou převést mince. V případě, že by nějaký uzel měl výpadek nebo se dobrovolně odpojil ze sítě, je zde mnoho dalších uzlů, které budou nadále zajišťovat správné fungování sítě [3].

Bitcoin je zcela elektronický systém a neexistují žádné fyzické mince. Komunikace mezi jednotlivými uzly Bitcoinu, které se starají o chod sítě, probíhá prostřednictvím internetu. Jedná se svým způsobem o „internetové peníze“. Jejím základním účelem je převést hodnotu z jedné osoby na druhou [3].

2.1 Asymetrická kryptografie v Bitcoinu

Protokol Bitcoinu je založen na asymetrické kryptografii, která je absolutním základním kamenem celého systému. Asymetrická kryptografie spoléhá na dvojici klíčů nazývaných jako privátní a veřejný klíč. Jednotlivé klíče, které tvoří klíčový pár, jsou matematicky propojené. Výhoda asymetrické kryptografie spočívá v možnosti sdílet veřejný klíč se svým okolím. Okolí může použít veřejný klíč k tomu, aby ověřilo, zda byl použit související privátní klíč bez toho, aniž by byl privátní klíč vyzrazen. To je dáno vlastností asymetrické kryptografie, kdy ověřit použití privátního klíče, je jednoduché. Ovšem zjištění, jaký privátní klíč z veřejného klíče byl použit, je velice výpočetně náročná operace. Různé druhy asymetrické kryptografie jsou založené na různých problémech, které jsou výpočetní silou obtížně řešitelné. Zpravidla se jedná o problémy v oblasti matematiky. Některé problémy spoléhají na problém faktorizace součinu dvou prvočísel, jiné na problém diskrétního logaritmu. Bitcoinový protokol využívá ECDSA, v české literatuře známý pod názvem „Protokol digitálního podpisu s využitím eliptickým křivek“ [14] [15].

2.2 Ostatní základní vlastnosti

Měna je navržena tak, aby byla dělitelná, není třeba posílat vždy celou minci. Bitcoin lze dělit až na 8 desetinných míst. Nejmenší jednotka Bitcoinu se nazývá Satoshi zkráceně sats, která nese název po svém vynálezci. Platí, že 1 BTC = 100 000 000 Satoshi [16]. V případě, že by dělitelnost jedné mince nebyla v budoucnu dostatečná, lze ji zvýšit. Úpravy týkající se Bitcoinového software musí schválit samotná Bitcoinová síť.

Důležitým aspektem celého systému je skutečnost, že počet všech mincí, které budou kdy emitovány do sítě je pevně daný. Bitcoinový protokol počítá s maximálním počtem 21 milionů mincí [16]. Otázka, proč byl systém navržen s konečným počtem mincí je spíše ekonomická. V dnešním světě měny mají přirozenou inflaci, která je navíc považována za zdravou. Určením horní hranice počtů mincí se docílí minimalizace inflace, jelikož nelze emitovat mince jinak, než dovolí Bitcoinový protokol [16].

2.3 Bitcoinová adresa

Adresa slouží uživateli Bitcoinu k příjmu mincí. Uživatel může sdílet veřejnou adresu s ostatními účastníky a nechat si na ni zaslat platbu v Bitcoinech. Díky asymetrické kryptografii je možné sdílet veřejnou adresu bez toho, aniž by uživatel vyzradil svůj privátní klíč.

Veřejná adresa se skládá z náhodných malých nebo velkých písmen a taky číslic o délce 26–35 znaků [17]. Rozsah číslic a znaků je omezen. Pro lepší čitelnost adres se využívá kódování Base58. To zaručuje, že adresa bude reprezentována ve všech znacích anglické abecedy včetně velkých písmen a číslic. Důvod, proč nebylo použito již existující kódování Base64 spočívá v čitelnosti adres. Base58 na rozdíl od Base64 nepoužívá znaky „+“ a „-“ a navíc odstraňuje znaky „0“, „O“, „l“ a „I“, které jsou vzájemně opticky zaměnitelné [18].

Pro zjednodušení použití lze veřejné adresy zakódovat do obrázkového QR kódu. Pomocí aplikace se QR kód naskenuje a dekóduje do formy číslic a písmen a na tu se následně odešle určitý obnos mincí [17].

Veřejnou adresu je možné vygenerovat pomocí libovolné Bitcoinové peněženky. Vznik adresy probíhá tak, že počítač vybere nějaké pseudonáhodné číslo o velikosti 256 bitů a privátní klíč je právě toto 256bitové číslo, které se pro lepší čitelnost a menší délku reprezentuje v hexadecimální soustavě [19].

Postup pro vygenerování veřejné adresy typu P2PKH (Pay-to-Public-Key-Hash) je následující [19]:

- Z příslušného privátního klíče se vygeneruje veřejný klíč o velikosti 256 bitů
- Nad veřejným klíčem provedeme hashovací funkci SHA-256
- Provedeme hashovací funkci RIPEMD-160 nad předchozím hashem
- Přidáme prefix „00“ na začátek přechozího hashe. Ten vyznačuje, jestli se jedná o adresu pro hlavní síť, přičemž pro testovací síť se používá jiný prefix.
- Provedeme 2x hashovací funkci SHA-256 nad předchozím krokem. Vybereme první 4 bajty z výsledné funkce, které přidáme na konec přechozího kroku. Tyto 4 bajty slouží jako kontrolní součet.
- Převedeme výsledek do Base58 formátu
- Výsledná adresa může mít například následující podobu:

1BvBMSEYstWetqTFn5Au4m4GFg7xJaNVN2

2.3.1 Bezpečnost generování privátního klíče

Nejdůležitější částí klíčového páru je privátní klíč, který dává uživateli právo utratit prostředky. Lze z něj dopočítat jak veřejný klíč, tak veřejnou adresu. Privátní klíč nám dovoluje utratit prostředky na adrese, ke které privátní klíč patří. To je dáno tím, že protokol vyžaduje, aby transakce byly podepsány příslušným privátním klíčem a byly síťovými účastníky považovány za validní [3] [20].

Tabulka 1 Příklad veřejné adresy a privátního klíče

Veřejná adresa	`1PboGy49tHUndkwvhpDMGjEvKxVAvz2o6y`
Privátní klíč	`L4wxaAfJDh9BVPMR2Wd1Ahd1STWjZwQa7HTT8HMeg8A7rKoiTNnG`

V případě ztráty privátního klíče jsou prostředky navždy ztraceny. Jelikož je Bitcoin decentralizovaný systém, není zde žádná centrální autorita, která by spravovala klíče a v případě ztráty ho obnovila ze zálohy. Bez vlastnictví privátního klíče neexistuje možnost, jak dokázat protokolu, že jsme vlastníky mincí na přidružené adrese [3]. Proto je nutné, aby byl privátní klíč uchováván na bezpečném místě, kde se nemůže znehodnotit a nejlépe, aby nebyl dosažitelný z online prostoru.

Z hlediska bezpečnosti je potřeba dbát na to, aby vygenerovaný privátní klíč byl co nejvíce náhodný, tím se minimalizuje šance, že by někdo vygeneroval stejný privátní klíč, který bude využíván. To by opět znamenalo, že by mohlo být manipulováno s mincemi, které jsou drženy na příslušné veřejné adrese.

Zpětné dopočítání privátního klíče lze provést pouze útokem hrubou silou. Tím je myšleno, že se budou zkoušet všechny možné kombinace, dokud nebude vygenerován privátní klíč s adresou, na kterou je cíleno. Šance, že se útok hrubou silou povede, je téměř nulová [20]. Je to z toho důvodu, že pokud se uvažuje o délce bitcoinové adresy 160 bitů, tak každý daný bit v adrese může nabývat jak hodnoty „1“ nebo „0“. Pomocí jednoduchého matematického výpočtu lze zjistit, že celkový počet možných adres je 2^{160}.

To znamená, že pokud by byl náhodně vybrán jakýkoliv privátní klíč, je šance 1: 2^{160}, že se trefí právě ten, na který je proveden útok. Pokud by bylo reálně uvažováno o útoku hrubou silou, tak rychlý počítač zvládne vygenerovat kolem 1000 párů klíčů za sekundu. I tak by to počítači o takové výpočetní síle trvalo $2{,}78 \cdot 10^{38}$ let, než by vypočítal všechny klíčové páry všech možných adres.

Každý jedinec má možnost si vytvořit tolik jednotlivých peněženek, kolik potřebuje. Celkový počet dostupných adres, tj. 2^{160} by měl být dostatečný pro celou lidskou populaci i v případě jednorázového použití adres.

Z hlediska soukromí se nedoporučuje užívat jednu adresu na všechny transakce. Moderní Bitcoinové peněženky (jako např. Exodus Wallet [21]) automaticky generují novou adresu po určitém počtu transakcí.

Z výše uvedeného lze vidět, že Bitcoin je z velké části založen na pravděpodobnosti. Jedná se o možnost, jak systém zanechat bezpečný a zároveň otevřený pro všechny.

2.3.2 Uchovávání privátního klíče

Existuje mnoho způsobů, jak chránit privátní klíč před prozrazením nebo znehodnocením. Je vhodné mít zálohované privátní klíče na více zařízeních. Na druhou stranu zde existuje riziko napadení zařízení a prozrazení privátního klíče.

Nejjednodušší způsob, jak uchovat privátní klíč bezpečný, je ho mít zašifrovaný silným heslem. Někteří uživatelé využívají tzv. papírové peněženky. Tu lze vygenerovat na webových stránkách, které tuto službu zdarma nabízí. Na adresu papírové peněženky lze posílat mince. Když uživatel chce utratit nebo odeslat mince jinam, je potřeba pouze

naskenovat privátní klíč, který je reprezentován QR kódem a odeslat na příslušnou adresu [22].

Papírová peněženka nenabízí pohodlí pro uživatele, kteří potřebují často manipulovat se svými mincemi, proto někteří uživatelé využívají softwarové peněženky, které lze nainstalovat na osobní počítač nebo telefon. Softwarové peněženky standardně nabízí daleko větší funkcionalitu oproti papírovým peněženkám. Dokážou například počítat aktuální hodnotu mincí, generovat unikátní adresu pro každou transakci, pohodlně odesílat a přijímat mince nebo třeba generovat zálohy privátních klíčů. Většina dnes dostupných SW peněženek je zcela zdarma. Je potřeba dávat pozor jaké peněžence své prostředky svěřujeme. Vždy může existovat riziko backdooru („zadní vrátka“ v softwaru, které umožňují napadení systému nebo počítače) v softwaru, kvůli kterému bychom mohli prostředky ztratit [21].

Nejsofistikovanější řešení je zakoupení tzv. hardwarové peněženky. HW peněženka je elektronické zařízení, které nabízí stejné možnosti jako SW peněženka s nadstandartními bezpečnostními prvky. Samotné odesílání prostředků se vždy provádí přes uživatelské rozhraní na počítači nebo telefonu, ale potvrzování vždy probíhá na HW peněžence. HW peněženka je navíc chráněná heslem nebo krátkým PIN kódem, který zabraňuje zneužití prostředků při krádeži nebo ztrátě peněženky [23].

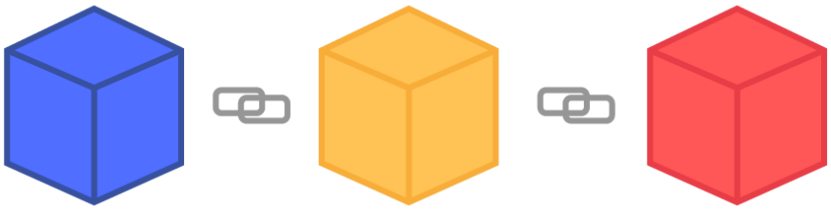
2.4 Blockchain

Blockchain představuje účetní knihu, která uchovává záznamy o všech transakcích, které v Bitcoinové síti proběhly. Rozdíl oproti prosté účetní knize je v tom, že blockchain se nenachází fyzicky pouze na jednom serveru/počítači, někde v bance, který transakce zpracovává. Naopak, tato databáze transakcí je distribuována na mnoha uzlech v síti [17].

Uzel v Bitcoinové síti představuje uživatele Bitcoinového protokolu. Všechny uzly v síti jsou si rovny, neexistuje zde žádná hierarchie, která by upřednostňovala jednotlivé uzly mezi sebou.

V případě, že by se jeden z uzlů vyřadil ze sítě, není to problém. Databáze je totiž uložena na mnoho dalších uzlech. Další výhoda tohoto systému je, že není napadnutelný žádnou třetí stranou. V případě, že by se nějaký stát pokusil o vyřadění uzlů z provozu na jeho území, s Bitcoinovou sítí by to prakticky nic neudělalo a fungovala by normálně dále. Není dán žádný maximální počet uzlů, ale k fungování sítě je potřeba aspoň jeden uzel. Naopak vyšší počet uzlů posiluje nezávislost celé sítě [24].

Blockchain se skládá z jednotlivých bloků. Blok představuje datovou strukturu, která obsahuje údaje o provedených transakcí. Jednotlivé bloky jsou za sebou řetězeny, tak jak znázorňuje *Obrázek 1 Vizualizace blockchainu*. Nové bloky jsou řetězeny na konec blockchainu. Každý blok obsahuje zcela jedinečné transakce, taktéž každý blok je zcela jedinečný. Obecně platí, že novější bloky obsahují novější transakce. Aby velikost celého blockchainu nerostla do velkých čísel a byla zachována dostatečná decentralizace, je maximální velikost bloku omezena na 1 000 000 Bajtů [24].



Obrázek 1 Vizualizace blockchainu

Každý blok lze jednoznačně identifikovat. Blok má tzv. „Height“ česky výšku. Toto číslo reprezentuje pořadí jednotlivých bloků, jak jdou za sebou. Počátek běhu Bitcoinové sítě je datován při vzniku prvního bloku, který nastal spuštěním Bitcoinového softwaru na prvním zařízení. První blok s výškou 0 je nazýván jako „Genesis block“, což doslova znamená „původní blok“ [24].

Transparentnost a anonymita blockchainu

Jelikož je Bitcoin decentralizovaný a otevřený systém, může si kdokoliv stáhnout celý blockchain na své zařízení a prohlížet veškeré transakce, které kdy byly Bitcoinovou sítí zpracovány [16]. Transparentnost celé sítě je důležitý bezpečnostní prvek. Když je celá historie kýmkoliv viditelná, je obtížně v takové síti vytvářet podvodné transakce, jelikož je zde mnoho dalších účastníků, kteří dohlížejí na správnost transakcí v blockchainu.

Existují webové nástroje nazývané jako „blockchain explorer“, které nabízejí služby nahlížení do blockchainu. Díky nim lze vyhledat jakýkoliv blok nebo transakci, což prakticky znamená, že lze prohlížet veškeré transakce, které za dobu existence Bitcoinu proběhly. Lze taktéž najít informace o tom, z jaké adresy transakce putovala, jaká byla její cílová adresa, její převáděné množství mincí a datum provedení transakce nebo například počet mincí na určité adrese. Není obtížné nahlédnout, kolik mincí se nachází na adrese, na kterou se chystáme poslat transakci, včetně všech transakcí, které mířily na nebo z adresy [25].

Z toho důvodu je Bitcoin nazýván jako pseudoanonymní. Všechny transakce jsou dohledatelné, problém je v určení vlastníků jednotlivých adres. Pokud není možné spojit adresu s fyzickou osobou nebo institucí, lze považovat transakce z ní provedené za anonymní. V opačném případě se anonymita Bitcoinu ztrácí.

3 TĚŽENÍ V BITCOINOVÉ SÍTI

Mining, česky těžení, je důležitá činnost v Bitcoinovém protokolu, která se stará o správné fungování celé sítě. Těžaři, jakožto osoby, které se snaží vytěžit Bitcoin, jsou ekonomicky motivování k těžení Bitcoinu.

Úkolem těžaře je zvolit množinu nepotvrzených transakcí, které zatím nejsou zapsané v blockchainu a vytvořit z nich tzv. „kandidátní blok“. Nepotvrzené transakce se nachází v tzv. „memory poolu“ (mempool). Každý těžař si udržuje seznam nepotvrzených transakcí právě ve svém memory poolu, aby měl k dispozici transakce, kterými může naplnit kandidátní blok. Kandidátní blok představuje blok, který má zájem těžař vytěžit a zařadit na konec blockchainu [16] [17] [24].

Po vytvoření kandidátního bloku je hlavní úkolem těžaře svůj blok vytěžit. Pokud se mu povede vytěžit blok, zařadí ho na konec blockchainu a předává ostatním uzlům zprávu o nově vytěženém bloku. Uzly si aktualizují svoji verzi blockchainu o nově vytěžený blok a těžaři, kteří jsou také uzly, si odstraní ze svého memory poolu transakce, které již byly potvrzeny v aktuálně vytěženém bloku. Nedávalo by smysl nadále uchovávat transakce, které jsou již zapsány v blockchainu, a tím pádem považovány za proběhlé. Uzly tuto zprávu šíří dál, dokud zprávu o nově vytěženém bloku neobdrží každý uzel v síti [24].

Z toho lze usoudit, že těžaři fungují v síti jako procesní prvek, který validuje transakce a jsou přímo odpovědní za správné fungování sítě.

3.1 Ekonomická motivace těžařů

Vytěžením bloku obdrží těžař odměnu. Odměna se skládá ze dvou částí. První část je definována samotnou sítí a lze ji nalézt v každém bloku jako první transakci. První transakce v bloku nazývána jako „Coinbase“ transakce převede na adresu těžaře počet mincí, který je zrovna definován jako odměna za vytěžení bloku. Coinbase transakce emituje nové mince do sítě [16] [17] [24].

Druhá část odměny se skládá z poplatků za provedení transakce. Zpravidla veškeré transakce jsou zatíženy poplatkem. Poplatek určuje odesílatel transakce a je zcela na odesílateli, jakou výši poplatku zvolí. V případě, že by odesílatel zvolil příliš malý poplatek, riskuje, že by jeho transakce nebyla zvolena do kandidátního bloku, a tím pádem by se při vytěžení nového bloku nemusela objevit v blockchainu. Zvýšením poplatku motivujeme těžaře k tomu, aby zvolili tuto transakci, protože z ní získá větší zisk. Díky tomu jsou transakce s větším

poplatkem zpracovány rychleji. Těžař při vytěžení bloku obdrží veškeré poplatky z transakcí, které zakomponoval do nově vytěženého bloku. Těžař je tedy čistě ekonomicky motivován, aby vybíral transakce s největšími poplatky [17].

3.1.1 Úprava složitosti těžby

Proces těžení bloků se v síti neustále opakuje, a tím jsou potvrzovány nové transakce. Bitcoinová síť se snaží o to, aby byl nový blok vytěžen každých 10 minut, a tím pádem, aby nové mince vznikaly stejným tempem. Aby byla emise nových mincí předvídatelná, síť upravuje složitost pro vytěžení podle toho, jak rychle byly v minulosti vytěženy předchozí bloky. Každých 2 016 bloků se přehodnocuje složitost pro těžbu bloků. Při předpokládané délce vytěžení jednoho bloku 10 minut to znamená, že síť upravuje složitost přibližně každé 2 týdny [24].

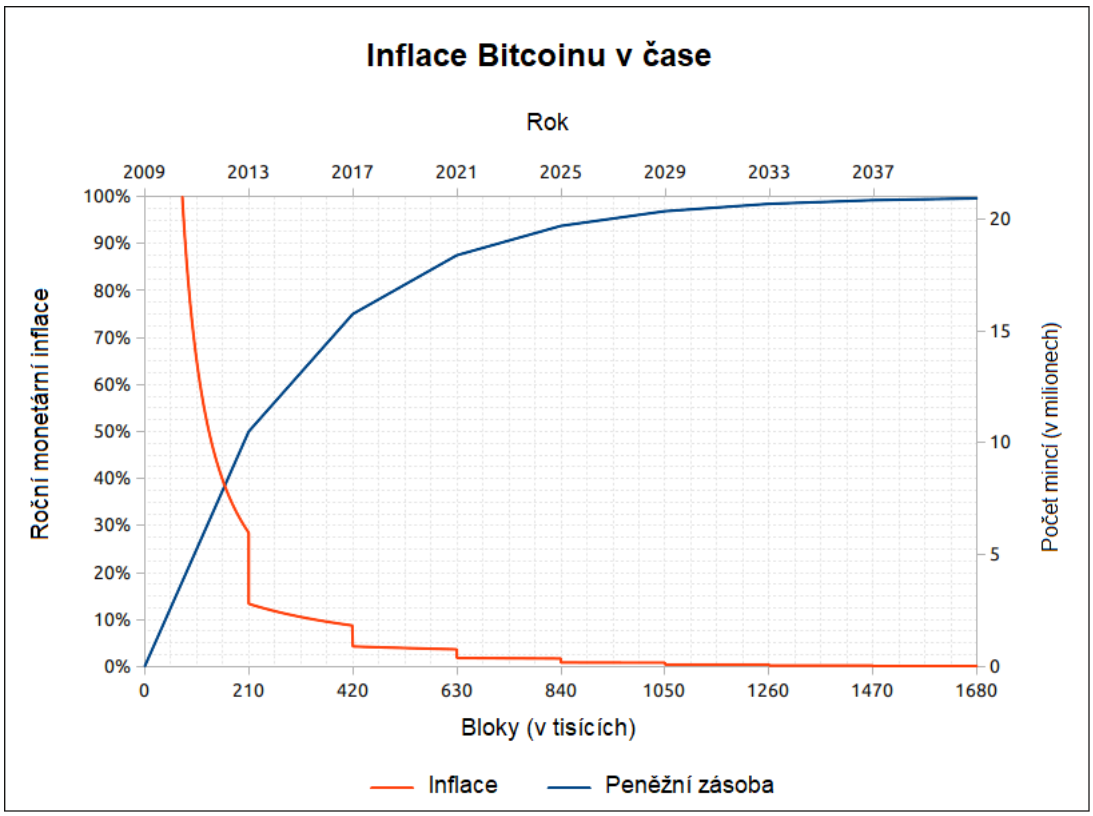
V případě, že by se těžily bloky příliš rychle, zvýší se složitost pro vytěžení bloku, a následkem toho bude vytěžení bloků náročnější. Pokud by naopak nastala situace, že by se těžaři již dále neúčastnili těžby a těžení nových bloků by bylo příliš pomalé, což by znamenalo, že potvrzování transakcí by bylo taktéž pomalé, složitost se sníží. Díky tomu se dosahuje požadovaného časového intervalu 10 minut pro vytěžení jednoho bloku. I kdyby se v síti nacházely jen jednotky těžařů, na funkčnost bitcoinové sítě by to nemělo vliv, a to z toho důvodu, že síť je schopná se přizpůsobit aktuálnímu těžícímu výkonu v síti [24].

3.1.2 Půlení odměny

Odměna za vytěžení bloku není po celou dobu stejná. V počátcích fungování Bitcoinu byla odměna za vytěžení bloku 50 BTC. Bitcoinový protokol odměnu za vytěžení bloku v čase zmenšuje. Úprava odměny je událost, která se nazývá jako „halving“, česky půlení. Každých 210 000 bloků se odměna za vytěžení zmenší na polovinu. To vychází na časový rámec přibližně 4 let. Aktuálně (leden 2021) je odměna za blok 6,25 BTC. Vzhledem k tomu, že se odměna každé čtyři roky zmenšuje, zmenšuje se i emise nových mincí. Počet nově vytvořených mincí zpomaluje tím, jak se zmenšuje odměna za blok [26].

Jelikož je celková peněžní zásoba mincí omezena a víme, jak často nastává vytěžení nového bloku, lze s celkem velkou přesností odhadnout, kdy nastane vytěžení veškerých mincí. Stejně tak je možné předpovědět, kolik mincí bude vytěženo za 10 let. Aktuálně již bylo vytěženo přes 88 % všech mincí a toto tempo bude každé půlení jen zpomalovat. Konec těžby nových mincí je odhadováno na rok 2140 [26].

Kvůli neustále zpomalující se emisi nových Bitcoinů se stejným tempem snižuje vnitřní inflace Bitcoinů. Monetární inflace se zcela zastaví, až bude vytěžen poslední blok s odměnou. Po tomto momentě nebudou generovány nové mince do sítě a odměna za blok se bude skládat pouze z poplatků jednotlivých transakcí v bloku [16]. *Obrázek 2 Průběh těžby a inflace Bitcoinu v čase* názorně ukazuje, jak se emise nových mincí v čase zpomaluje. Kolem roku 2037 budou už téměř všechny mince vytěženy, stejně tak bude inflace Bitcoinu téměř nulová.



Obrázek 2 Průběh těžby a inflace Bitcoinu v čase [27]

3.1.3 Proces uzavření bloku

K tomu, aby bloky nebyly těženy nepřetržitě, bylo potřeba udělat těžbu náročnou. Toho je docíleno tím, že těžaři musí vytvořit hash bloku, který odpovídá pravidlům složitosti. V praxi je třeba splnit řadu pravidel, aby byl těžařův blok přijat celou sítí, jako například zařadit pouze validní transakce, těžit s určenou složitostí, a především musí odpovídat hash bloku [24].

Hash bloku je další a poslední unikátní identifikátor bloku. Když se těžař snaží vytěžit svůj blok, hashuje funkcí SHA-256 celou hlavičku bloku, která obsahuje především metadata spolu s tzv. nonce. Nonce je obyčejné číslo bez speciálního významu, která se spolu s ostatními informacemi hashuje [28].

Tím, jak se zvyšuje složitost, je požadováno po těžařích, aby výsledný hash byl číselně menší. To má za následek menší pravděpodobnost, že bude nalezen správný hash [24]. V praxi to lze pozorovat na vzhledu hashů předchozích bloků, kde lze vidět mnoho nulových hodnot na začátku hashe, jako ukazuje *Tabulka 2 Příklad hashe bloku*.

Tabulka 2 Příklad hashe bloku

Hash bloku 674024
00000000000000000038a9593d03263cdcefc9e2484c6a3feb09f81bae6621b

Pokud by hash nesplňoval podmínky aktuální složitosti pro vytěžení bloku, byl by sítí odmítnut. Úkolem těžaře je měnit nonce nejrychleji, jak mu hardware dovoluje a snažit získat hash bloku, který bude menší než aktuálně určená složitost. V případě, že nalezne nonce, která spolu po zahashování hlavičky bloku odpovídá složitosti, je blok vytěžen. Taková nonce se nazývá „golden nonce“ [28] [29].

Vzhledem k obtížnosti nalezení správného hashe, musí těžař vyzkoušet obrovské množství různých nonce, než nalezne tu, která vede k požadovanému hashi. Často se stává, že jiný z těžařů vytěží blok dříve. Pokud se tak stane, je potřeba, aby těžař zkontroloval, jestli se některá z transakcí v novém bloku nenachází v jeho kandidátním bloku a pokud ano, musí znovu poskládat kandidátní blok a zkoušet různé nonce úplně od začátku.

Uhodnutí nonce může nastat během pár sekund po začátku těžby. Stejně tak, je možné, že těžba bloku bude trvat mnohem déle než ideálních 10 minut. Nejde nijak ovlivnit pravděpodobnost uhodnutí golden nonce. Pokud by hledání správného hashe trvalo příliš dlouho, síť upraví po vytěžení 2016 bloků složitost pro těžbu [24].

3.2 Cíl a složitost

Target česky cíl, představuje největší možný hash, který těžař musí poskytnout pro vytěžení bloku. Při prvním spuštění sítě byl cíl nastaven na hodnotu:

0x00000000FFFF0000000000000000000000000000000000000000000000000000 (1)

Toto hexadecimálně znázorněné číslo představuje největší možný hash, který je možný použít v bitcoinové sítě při příslušné složitosti pro vytěžení bloku [31].

Se zvyšujícím se výpočetním výkonem těžařů, který se udává v hashích za sekundu (H/s, někdy také hashrate), se zvyšovala složitost. Samotná složitost má také své číselné

vyjádření pro lepší interpretaci náročnosti vytěžení bloku. V anglické literatuře se tato hodnota nazývá „difficulty“ a je vyjadřována v dekadické soustavě [30].

Pojmy cíl a složitost jsou navzájem propojeny. S větší složitostí se zmenšuje požadovaný hash neboli cíl. Je to dáno tím, že omezováním horní hranice hashe, se zmenšuje pravděpodobnost těžaře na nalezení správného hashe pro vytěžení bloku. Nejmenší složitost je vyjadřována číselně jako „1“. Čím vyšší složitost, tím toto číslo roste [30]. Vzorec pro spočítání aktuální složitosti je:

$$Aktuální\ složitost\ = Nejvyšší\ možný\ target \div\ Aktuální\ target \quad (2)$$

Konkrétní výpočet:

$$0x00000000FFFF0000000000000000000000000000000000000000000000000000 \div 0x0000000000404CB000000000000000000000000000000000000000000000000 \cong \mathbf{16307,4} \quad (3)$$

Těžař při spočítání hashe zkontroluje, zda hash je menší nebo minimálně stejný jako cíl. V případě, že je hash menší a splnil ostatní podmínky, je blok vytěžen a on získává odměnu [28].

Tabulka 3 Porovnání hashů pro vytěžení bloku

Cílový hash (target)	0000000000000000000d4833adbfb465d4cfb57c2918b830db228cf1b217d99f
Hash nesplňující podmínky pro vytěžení	0000000000000000000f9807c7c506ae1813490e4ba675f843d5a10e0baacdb8
Hash splňující podmínky pro vytěžení	0000000000000000000080974a14e6ef47d97c476a7a5ab62ff8e80e2c68d7baa

Tabulka 3 Porovnání hashů pro vytěžení bloku ukazuje, že hash pro vytěžení musí být číselně menší. Může také nastat situace, že hash splňující podmínky, bude obsahovat rovnou větší počet nul na začátku. To je ovšem méně pravděpodobné.

3.3 Struktura bloku

Blok uvnitř blockchainu je možné obecně rozdělit na dvě části. První z nich je hlavička bloku, která obsahuje ty nejdůležitější informace o bloku. Druhá část, nazývaná jako tělo

bloku, obsahuje z velké části jen data transakcí, které byly do bloku uloženy těžařem [32] [33].

Kromě samotných transakcí se nachází v bloku i jiné informace, které slouží uzlům k tomu, aby ověřovaly, že byly splněny všechny podmínky pro oprávněné vytěžení bloku a nebyl například vytěžen blok s jinou složitostí, než zrovna byla nastavena v celé síti. Další data v hlavičce usnadňují orientaci v blockchainu nebo hledání transakcí v jednotlivých blocích [24].

3.3.1 Hlavička bloku

Hlavička bloku obsahuje především metadata bloku rozdělených do šesti částí. Všechny bity jsou uloženy způsobem Little-endian. Ukládání bitů způsobem Little-endian znamená, že nejméně významné bity se ukládají na paměťové místo s nejnižší adresou. Opakem Little-endian je Big-endian. Big-endian naopak ukládá nejvíce významný bit na paměťové místo s nejnižší adresou. Celkově hlavička zabírá 80 bajtů v bloku. Mimo ukládání důležitých metadat, je hlavička bloku důležitá i v procesu těžení. Když se těžaři snaží vytěžit blok, hashují právě celou hlavičku bloku a snaží se vygenerovat hash, který bude odpovídat aktuální složitosti [32].

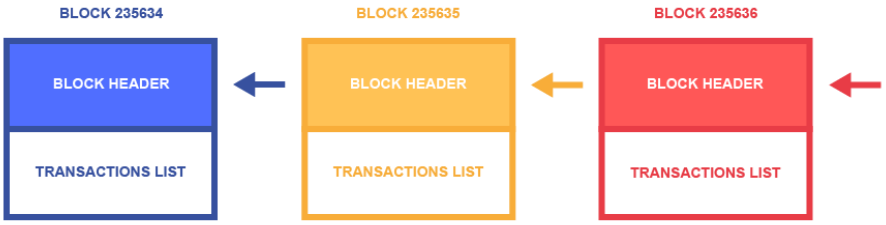
Verze bloku

Jako první se v hlavičce bloku ukládá informace o verzi bloku. Informace o verzi bloku se mění, když těžař upgraduje na novou verzi Bitcoinového softwaru. Některé nové funkce Bitcoinového protokolu jsou dostupné až s novou verzí. Verze bloku poskytuje ostatním účastníkům protokolu informaci o tom, jak mají s blokem nakládat a jaké funkce mohly být v bloku použity. Pro verzi bloku byly vyhrazeny v hlavičce celkem 4 bajty [32] [34].

Hash minulého bloku

Hash minulého bloku je hash, kterým byl vytěžen předchozí blok a zároveň ukazuje na předešlý blok. Tímto způsobem je celý blockchain propojen dohromady, tak jak zobrazuje *Obrázek 3 Propojení blockchainu pomocí hashů bloků*. Jeden blok vždy ukazuje na předešlý. Podobně jako datová struktura známá jako „spojovaný seznam“.

Samotný hash bloku pro daný blok je vždy k nalezení až v bloku následujícím. Hash bloku má velikost 32 bajtů. To je dáno tím, že hashovací funkce SHA-256 tvoří výstup o velikosti 256 bitů [32].



Obrázek 3 Propojení blockchainu pomocí hashů bloků

Nonce

V každém bloku lze taky nalézt informaci o nonce, která vede k vytěžení bloku. Informace o nonce je velice důležitá. Kvůli tomu, že je nonce uložena v každém bloku, si může jakýkoliv účastník sítě ověřit, zda hash bloku odpovídá hlavičce bloku. V případě, že by kdokoliv měl zájem si validnost vytěžení bloku ověřit, spočítá hash pro hlavičku bloku spolu s uvedenou nonce. Pokud hash bloku nesouhlasí, ostatní těžaři ví, že něco není v pořádku a blok by tím pádem nemuseli přijmout jako součást blockchainu. Kdyby ostatním těžařům tato informaci nebyla známa, nebylo by možné ověřit, že těžař neprávem vytěžil blok [34].

Je to právě nonce, kterou se těžaři snaží uhádnout pro vytěžení bloku, jelikož všechny ostatní informace v hlavičce jsou těžaři známy předem. Nalezení nonce je extrémně složité, naopak ověření, že je nonce správná, je rychlý proces [28] [29].

Čas

V hlavičce nesmí chybět informace o čase. Konkrétně o tom, kdy byl blok vytěžen. Informace o čase vytěžení je vhodná v případě, že je potřeba se podívat, jak je blok starý. Čas je kódován do 4 bajtů [35].

Při hashování hlavičky bloku (těžení) je potřeba měnit tuto hodnotu podle toho, jak se čas mění. Když se těžařovi povede vytěžit blok, zapsaná hodnota času v bloku odpovídá času vytěžení [32] [35].

Bits

Pro ověření, zda byl blok vytěžen s požadovanou složitostí se v bloku uchovávají tzv. „bits“. Jedná se o zápis cíle v úsporném formátu, který zabírá pouze 4 bajty. Jelikož je cíl jen číslo

v hexadecimálním formátu, tak se bits reprezentují buď v hexadecimální nebo dekadické soustavě [31] [35].

V hexadecimálním formátu mohou vypadat bits následovně: 0x0e154a4b (prefix „0x“ značí, že číslo je uvedeno v hexadecimálním formátu). Bits se skládají ze dvou částí. První část, která má velikost 1 bajtu (první dva znaky), je exponent. Druhá část, která má velikost zbývajících 3 bajtů, je koeficient. Pokud chceme přepočítat bits na cíl, tak exponent značí počet odsazení nulovými bajty zprava. Ve výše uvedeném případě je exponent „0e“, což je v dekadické soustavě číslo 14. Kvůli tomu, že dvě hexadecimální číslice tvoří jeden bajt, tak musíme číslo 14 zdvojnásobit. Tím pádem máme 28 nul v hexadecimálním formátu. Nyní už je jen potřeba přidat koeficient na nejvyšší bajty zleva. To znamená vzít koeficient „154a4b“ a nahradit jim 6 počátečních nul nalevo. Postup lépe vystihuje *Tabulka 4 Získání targetu (cíle) z hodnoty bits* [24].

Tabulka 4 Získání targetu (cíle) z hodnoty bits

Výchozí bits	0x0e154a4b
Exponent	0x0e
Koeficient	0x154a4b
1. Vytvoření nulového odsazení	0x00000000000000000000000000000000
2. Vložení koeficientu	0x154a4b0000000000000000000000

Pokud by byly ještě přidány nuly před číslo, tak aby mělo velikost 32 bajtů, cíl by vypadal následovně:

0x00000000000000000000000000000000154a4b0000000000000000000000 (4)

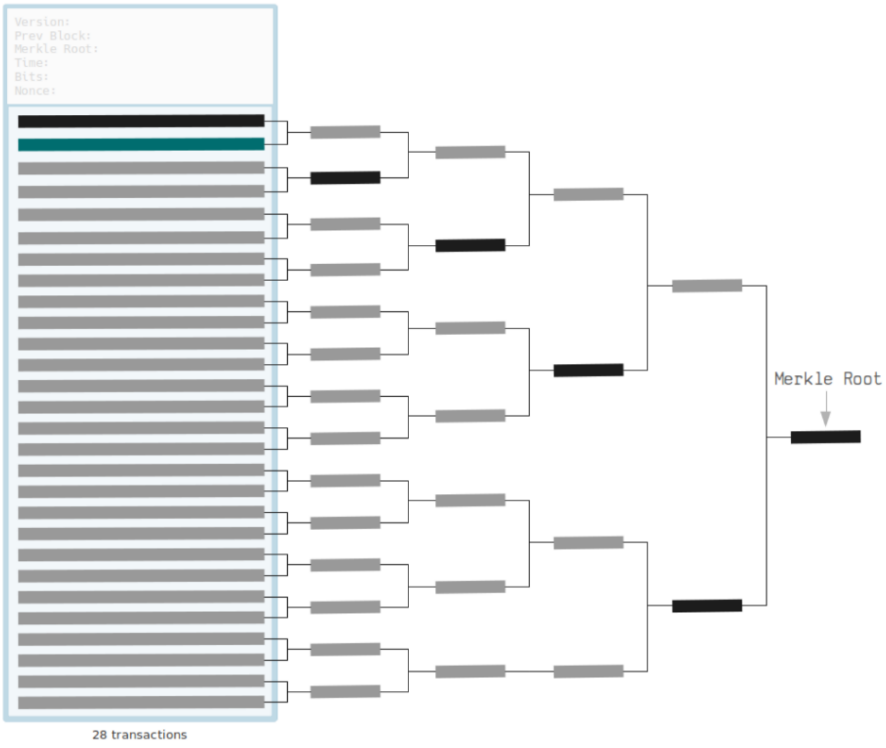
Lze si všimnout, že za koeficientem se nachází jen nulové hodnoty, přesnost cíle není úplná. To bitcoinovému protokolu nevadí. Díky zápisu ve formátu s koeficientem a exponentem se šetří místo v bloku o celých 28 bajtů.

Merkle root

Jedna z nejdůležitějších informací v hlavičce je kořen hashovacího stromu v anglického literatuře nazýváno jako „merkle root“. V podstatně se jedná o hash všech transakcí v bloku, který se získá postavením „merkle tree“, což se česky překládá jako hashovací strom [33].

Merkle root nám udává otisk všech transakcí v bloku. Nabízí se možnost, že není třeba tvořit hashovací strom a ten postupně hashovat, ale můžeme jednoduše spojit všechny transakce dohromady a ty zahashovat. Hashovací strom má ovšem jednu velkou výhodu. Díky kořenu hashovacího stromu, je možné jednodušeji ověřit, jestli se určitá transakce nachází v bloku [33].

Hashovací strom se tvoří tak, že se vezme jeden pár ID transakcí, které se v bloku nachází výlučně vedle sebe, ty se zahashují, hashe se spojí dohromady a opět zahashují. Tohle se provede po párech pro všechny transakce v bloku. Tímto procesem je získána přesně polovinu hashů oproti počtu transakcí v bloku. Výsledné hashe všech párů transakcí se znovu seřadí po párech, spojí a zahashují. Opět je získána celkem polovinu hashů z předchozí poloviny. Tento proces se opakuje, dokud se počet nezredukuje na jediný hash, který reprezentuje otisk všech transakcí v bloku nazývaný jako merkle root [3] [37].



Obrázek 4 Vizualizace merkle tree [36]

Když by bylo třeba ověřit, jestli se daná transakce nachází v bloku není nutné složitě znovu rekonstruovat celý hashovací strom. V prvním patře na úrovni dvou transakcí, z nichž je jedna ověřována, jestli se nachází v bloku, jsou obě transakce spojeny dohromady a zahashovány. Díky tomu je možné se posunout o patro výše. Nyní byl získán jeden hash, který je vypočítán v předchozím patře a potřebujeme druhý, aby bylo možné se posunout zase o patro výše. Druhý hash se získá tak, že je zažádán nějaký uzel o jeho zaslání. Uzly

uchovávají všechny hashe hashovacího stromu každého bloku. Oba hashe jsou spojeny dohromady a zahashovány. To znamená opět posun o patro výše ve stromu. Proces se opakuje, dokud není dosaženo nejvyššího patra stromu, což je zmiňovaný „merkle root“. Vypočtený merkle root je porovnán s hodnotou, která je napsaná v bloku, v kterém je hledána transakce. Jestliže jsou shodné, je zřejmé, že transakce se v bloku nachází. V celém procesu nebylo potřeba veškeré hashe transakcí v bloku, ale vždy jen druhý hash v páru pro daný list stromu. Lepší pochopení poskytuje *Obrázek 4 Vizualizace merkle tree* .

Kvůli hashování jednotlivých pater, které přímo ovlivňují patra vyšší, by jediná výměna transakce v bloku za jinou úplně změnila hodnotu merkle root. Je to dáno výstupní charakteristikou hashovací funkce. Dokonce i změna pořadí transakcí v bloku mění merkle root. To je dáno tím, že by se pro nějaký pár transakcí úplně změnil výsledek hashovací funkce a taková změna by se projevila v každém vyšším patře až do merkle rootu [37].

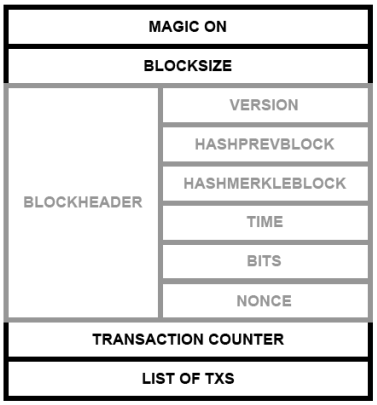
3.3.2 Tělo bloku

Tělo bloku obsahuje pouze z velké části především transakce, které se těžař rozhodl zařadit do svého bloku. Transakce jsou rozpoznatelné podle svého ID. Zkráceně se používá výraz TXID neboli „transaction ID“. TXID jsou jen hashe transakcí, ale jedna transakce je speciální a nazývá se tzv. „coinbase transakce“. Ta se nachází v těle jako první ze všech transakcí. Coinbase transakce předává těžaři odměnu za vytěžený blok, a ještě všechny poplatky transakcí v bloku, které do bloku zařadil. Coinbase transakce nevede z žádného bodu, je vygenerována samotnou sítí a převedena na adresu těžaře. Ten s prostředky může naložit podle své vůle [35] [38].

Mimo samotné transakce obsahuje blok mimo hlavičku i další užitečné data. Hned na začátku každého bloku je uloženo tzv. „magic number“. Vždy má hodnotu „0xD9B4BEF9“ a slouží jako identifikátor pro síť, že se jedná o produkční verzi blockchainu a ne testovací. Dále slouží jako ukazatel začátku bloku. Magic number má velikost 4 bajtů [38].

Blok obsahuje i informaci o své velikosti. Konkrétně značí, kolik bytů se vyskytuje v celém bloku právě po této informaci o velikosti. Číslo velikosti bloku může nabývat velikosti až 4 bajtů [38].

Poslední ukazatel značí, kolik transakcí se nachází v bloku. Je to prostý čítač transakcí. Má vyhrazeno 1 až 9 bajtů. Po čítači transakcí následují v bloku už jen samotné transakce [38].



Obrázek 5 Struktura bloku

Obrázek 5 Struktura bloku ukazuje strukturu bloku, kde hlavička je označená šedou barvou a tělo černou.

3.4 Proof of Work

Tím, že je síť decentralizovaná, vznikají problémy s důvěrou mezi jednotlivými uzly a jejich verzí blockchainu, které je potřeba podle nějakého mechanismu řešit. Tento mechanismus se v anglické literatuře nazývá Proof of Work, česky přeložitelný jako „důkaz práce“ [3].

Může nastat situace, že se některý z těžařů snaží v síti podvádět. Udělá to například tak, že se snaží do bloku zařadit transakce, které nejsou validní třeba tím, že odesílatel transakce neměl dostatečné množství prostředků pro provedení transakce.

Jakmile by těžař blok vytěžil, transakci by umístil do bloku a blok by zařadil na konec blockchainu. Problém pro podvodníka je v tom, že těžaři po vytěžení bloku distribuují informaci o vytěženém bloku dalším těžařům. Kdyby si podvodný blok nechal těžař jen pro sebe, ostatní těžaři by nemohli vědět o tom, že transakce uvnitř bloku byly provedeny, a tudíž by k žádnému podvodu nedošlo. Jakmile by informaci o novém bloku obdrželi, všimli by si, že některé transakce jsou podezřelé.

Síť těžařů se může rozhodnout, že verzi blockchainu s nevalidní transakcí budou ignorovat a budou pokračovat na svém blockchainu jako obvykle. Lze si to představit jako rozdvojení blockchainu na dvě různé verze – verzi, kterou mají všechny ostatní uzly a verzi od podvodníka, kteří ostatní uzly ignorují [3].

Jelikož těžení bloků stojí těžaře nějaké zdroje, konkrétně elektrickou energii, je pro ně nevýhodné podvádět, protože podvádění je stojí peníze. V případě, že by nějaký těžař podváděl, vytvořila by se další verze blockchainu a ostatní těžaři by se rozhodli právě pro ten blockchain, ve kterém bylo provedeno více práce. Jinak řečeno, ten blockchain, který obsahuje více bloků [3]. Mohlo by se stát, že by se podvádějícímu těžaři povedlo uzavřít i ještě další blok tentokrát nefalešný, ale jeho snaha o vytěžení dalšího bloku ho zase stála další elektrickou energii a pokud nemá většinový hashovací výkon celé sítě, není možné, aby uzavíral více bloků, než všichni ostatní těžaři v síti dohromady. Ostatní těžaři by podvodnou verzi blockchainu, která má menší počet bloků, nakonec opustili a vrátili se k originálnímu, kde byl vykonán větší důkaz práce, tedy kde bylo vytěženo více bloků.

3.5 Zabezpečení sítě elektrickou energií

Tímto jsme se dostali k důležitému zranitelnému bodu celého blockchainu. Kdyby nějaký těžař vlastnil 51 % hashovacího výkonu celé sítě, mohl by s celým blockchainem manipulovat, protože by se jeho blockchain skládal z největšího počtu bloků, a to je vždy to hledisko, podle kterého těžaři různé verze blockchainů posuzují [3] [39].

Zneužití většinového hashovacího výkonu sítě k provedení podvodné transakce se považuje za útok, který je v literatuře popsán jako „51 % attack". V dnešní době není úplně reálný. Není úplně možné během krátké doby získat enormní hashovací výkon. Celkový výkon sítě je tak velký, že by potřebné prostředky pro získání aspoň jeho poloviny stály velké množství peněz. Kromě velkého množství těžících strojů by bylo potřeba také enormní množství elektrické energie, který jedinec ani skupina nemá možnost bez povšimnutí získat [39].

Podle nejnovějších těžících strojů Antminer S19 Pro, lze těžit s příkonem 3250 W přibližně 110 Terahashů za sekundu [40]. S aktuálním výkonem celé sítě přibližně 155 Exahashů za sekundu [41] bychom k dosažení 51 % výkonu sítě potřebovali přibližně 718 636 těchto strojů s celkovým příkonem 2,34 GW. Pro představu, celkový výkon jaderné elektrárny Temelín je 2,11 GW [42].

Kromě toho, že by se těžař mohl pokusit uzavřít nevalidní transakci do bloku, by se mohl pokusit změnit transakci již v uzavřeném bloku, například někde uprostřed blockchainu. I tato situace je řešena pomocí Proof of Work.

Již bylo zmíněno, že při těžení bloku se hashuje celá hlavička bloku, která obsahuje i hash předchozího bloku. Když bude zahashována hlavička včetně nonce, hashe a dalších informací v hlavičce předchozího bloku, bude hledán hash, který odpovídá aktuálnímu cíli.

Pokud by si těžař změnil jedinou transakci v bloku, úplně by změnil hodnotu merkle rootu, a tím pádem i hashe celého bloku. Hash bloku by měl úplně jinou podobu, neodpovídal by cíli a ostatní těžaři by toto vytěžení bloku nepovažovali za validní. Jediná možnost, která zbývá manipulátorovi, je znovu hledat nonce. Manipulátorovi by se mohlo povést najít nonce pro blok, ve kterém chtěl provést podvodnou transakci, ale to není jediný problém, který by musel řešit.

Jelikož jednotlivé bloky ukazují vždy na hash předešlého bloku, byla by struktura blockchainu narušena, a to z toho důvodu, že blok následující by ukazoval na hash bloku, který by neshodoval s hashem bloku, ve kterém byla provedena podvodná transakce. Podvodník by musel znovu nalézt správnou nonce (hash) i pro další blok. Jakmile by nalezl nonce, tak by musel hledat další nonce, dokud by nenalezl nové nonce i pro všechny bloky až na konec blockchainu (viz. 3.3.1 Struktura bloku).

Změna jedné transakce by pro manipulátora znamenala hledání nových nonce pro všechny následující bloky. Proces by byl náročný na zdroje, a ještě k tomu by jeho verze blockchainu byla v budoucnosti zamítnuta sítí, jelikož na originálním blockchainu by vznikaly nové bloky, jež by tvořily delší blockchain než blockchain zmanipulovaný. Hledání jediné nonce je velmi obtížné a hledat nonce samostatně pro sérií bloků, je téměř nemožné.

Pomocí Proof of Work se síť ochraňuje před útočníky, kteří chtějí narušit integritu sítě. Jedná se o mechanismus ochrany „databáze“, která je distribuována na více zařízeních najednou. Změna blockchainu stojí útočníka nemalé prostředky a vzhledem k tomu, že v rámci sítě je blockchain transparentní, jsou těžaři motivování, aby zachovali korektní chování a tím správné fungování celého blockchainu a transakční sítě. Neférové chování nepřináší zisk, ale ztrátu v podobě zbytečně propálené elektrické energie [24].

3.6 Historie těžení

Obecně je potřeba k těžení pouze výpočetní techniku, která je schopná produkovat hashe SHA-256. Zároveň musí být hashovací neboli těžící stroj připojen k internetu, aby mohl v případě vytěžení bloku, šířit oznámení o vytěžení bloku ostatním uzlům [28].

V počátcích se Bitcoin těžil jen na procesorech stolních počítačů [43].Tento proces těžby fungoval a dovoloval každému, si nějaký počet Bitcoinů natěžit. Protože záměr těžařů je mít co největší zisk a toho mohou dosáhnout pouze tím, že zvýší svůj hashovací výkon, začali hledat způsoby, jak těžení udělat efektivnějším a rychlejším.

Objevila se možnost těžit pomocí grafických karet, jelikož ty mohou výpočet hashe mnohokrát zrychlit. Je to dáno tím, že standartní stolní počítač má v dnešní době 4–8 procesorových jader, zatímco grafická karta má těchto jader jednotky tisíc. Jádra grafické karty nejsou sice tak univerzální jako ty procesorové, ale na druhou stranu je jich mnohem více. Díky masivní paralelizaci výpočtů na grafických kartách se těžební výkon sítě mnohonásobně zvýšil [44].

V praxi to vypadalo tak, že lidé nakoupili několik grafických karet a ty najednou zapojily do jedné základní desky pomocí PCI-E sběrnice. Pro zapojení více karet do jedné desky za používá název „rig“. Rigy obsahovaly 2-8 karet, většinou ale 4 kusy grafických karet [43] [44].

S postupem času se těžba vyvinula ještě do pokročilejší podoby. Začaly se objevovat FPGA (Field Programmable Gate Array), které dokázaly zvýšit výpočetní výkon hashe opět několikanásobně. FPGA jsou programovatelné hradlové pole, jež můžou být naprogramovány pro výpočet nějakého problému. Nevýhoda pole je, že musí být před použitím naprogramovány a nejsou použitelné hned z výroby, jako je to např. u těžení na procesoru nebo grafické kartě [43] [44].

V poslední řadě se objevily zařízení nazývané jako ASIC (Application Specific Integrated Circuit, česky zákaznický integrovaný obvod). Jedná se o čip, který je přesně vyroben na zakázku a jeho funkcionální pružnost je velmi malá. Většinou zvládne provést jen úzký soubor výpočtů, tím pádem se hodí většinou jen pro určitou aplikaci. ASIC zařízení, není schopno provozovat operační systém a není možné spustit na něm nějaký software. V případě využití pro těžbu Bitcoinu, zvládne tyto zařízení produkovat kvanta hashů za sekundu [43] [44]. Jedná se o čistě jednoúčelové zařízení. ASIC jsou tedy prozatím poslední vývojový stupeň těžby Bitcoinu.

To ale neznamená, že by se zařízení dále nevylepšovala. Vylepšování ASIC spočívá v tom, že se vylepšuje výrobní proces litografie čipů. Jednotlivé tranzistory v čipu se zmenšují a díky tomu je dosaženo menší spotřeby nebo vyššího výkonu při stejné spotřebě. To znamená, že těžba je pro těžaře, který vlastní ASIC s efektivnějším čipem, výhodnější.

3.7 Těžební pool

Zpočátku byl Bitcoin těžen jednotlivci. Ti si spustili těžící SW na svém počítači a když měli štěstí, vytěžili blok a dostali za něj odměnu. Vytěžení bloku je náhodná událost, ale pokud těžař chtěl zvýšit šanci na vytěžení bloku, musel zvýšit svůj hashovací výkon. Mohlo se stát, že se mu několik dnů nepodařilo vytěžit ani jeden blok a v jiné chvíli zase mohl vytěžit rovnou několik bloků najednou. Situace přála vždy těm, kteří měli větší hashovací výkon.

Proto vznikly uskupení, které se nazývají „pooly“. Úkolem poolu je spojit mnoho těžařů a jejich výpočetní výkon dohromady, a tím mnohonásobně zvýšit šanci, se kterou mohou vytěžit blok. V dnešní době je prakticky nemožné vytěžit blok bez toho, aniž by se těžaři nacházeli v poolu. Respektive šance, že taková situace nastane, je velmi nízká [45].

Téměř všichni těžaři nyní těží v nějakém poolu, protože je to pro ně vzájemně výhodnější. Pokud některý z tisíců těžařů v poolu vytěží blok, odměnu si rozdělí podle toho, jak každý přispěl do poolu svým hashovacím výkonem. Ten, kdo přispěl do poolu výkonem 2 % z celkového výkonu poolu, dostane odměnu, která se rovná 2 % z celkové odměny za vytěžený blok. Samotný pool si bere malou provizi za poskytnutí služby [44].

V dnešní době existuje desítky různých poolů. Historicky první pool je český Slush Pool, který aktuálně vytěží kolem 4,04 % všech bloků v Bitcoinové síti a přibližně takovým těžebním výkonem přispívá také do Bitcoinové sítě [46]**.** Největší pooly vytěží až kolem 17 % všech bloků, přičemž se tyto hodnoty v čase mění [46]. Může se stát, že se v určitý čas nevyplatí některým těžařům těžit, což může nastat z důvodu zdražení elektřiny nebo náhlé změně ceny za jednu minci. V tom případě je pro těžaře výhodnější vypnout těžící stroje, aby pro ně těžba nebyla ztrátová.

3.8 Ekonomické hledisko těžby

Těžba není vhodná pro kohokoliv na světě. Jsou dva faktory, které ovlivňuji výhodnost těžby. První faktor je cena energie. Jelikož procesory, grafické karty a ASIC jsou elektronické zařízení, tak při své činnosti spotřebovávají elektrickou energii. Pro těžaře je důležité, aby konečná hodnota vytěžených Bitcoinů byla vyšší než cena za koupenou elektrickou energii. V opačném případě by se jednalo o ztrátovou činnost.

Druhý faktor se týká ceny Bitcoinu. Aby těžař měl z těžení zisk, musí prodat mince, které vytěžil. Když by měl levnou energii, ale cena za jednu minci by byla nízká, nemusí se mu

těžení vyplatit. Těžař těžko ovlivní cenu Bitcoinu, proto mu pouze zbývá udržovat cenu za energii co nejníže.

Ve skutečnosti se musí vzít na vědomí ještě jeden faktor. Těžební stroje jako ASICy stojí nějaký obnos prostředků (např. v únoru 2021 stojí ASIC miner Antminer S19j $5017 [47]). Proto musí být konečná cena všech mincí snížena o cenu za zakoupenou energii a cenu za těžební stroje kladná, jinak se nejedná výdělečnou činnost. Rovnice pro zjištění, jestli těžení bylo ziskové je:

$$V = (P_m \cdot C_m) - (P_e \cdot C_e) - (P_z \cdot C_z) \tag{5}$$

Kde:

V – Celkový zisk/ztráta

P_m – Počet vytěžených mincí

C_m – Cena za jednu minci

P_e – Počet kilowatthodin, které byly použity k těžbě

C_e – Cena za jednu kilowatthodinu

P_z – Počet zakoupených strojů

C_z – Cena za jeden stroj

Kvůli těmto faktorům, které ovlivňují těžbu, neprobíhá těžba rovnoměrně všude po světě. Těžba se vyplatí především tam, kde je nízká cena za elektřinu. Jelikož cena těžby v celé Evropě je ve srovnání s USA nebo Čínou velmi vysoká, není těžba až tak v Evropě rozšířena. Největší podíl na těžbě Bitcoinu má Čína a USA, kde je cena za jednu kilowatthodinu elektřiny nejvíce přívětivá [48]. Například v roce 2020 byla v Číně cena za 1 kWh po přepočtu na koruny 1,81 Kč. Nabízí se ještě možnost využití přebytků energie z obnovitelných zdrojů, především solární a vodní energie, které nemohou být uloženy.

Těžba sama o sobě produkuje mimo velký hluk, který jen dán hlučnosti chladících ventilátorů, také znatelné množství tepla. Někteří jedinci, kteří těží Bitcoin nebo jiné kryptoměny, využívají odpadní teplo z těžebních strojů pro jisté účely. Na internetu lze najít příklady, kde někteří lidé využívají pro vytápění skleníků, domů, nebo jiných užitkových budov právě odpadní teplo z těžebních strojů [49].

4 PROCES ZPRACOVÁNÍ TRANSAKCE

Požadavek transakce je obecně vytvořen v nějaké peněžence, která chce převést prostředky do jiné. Samotná peněženka funguje jako uzel v síti. Jakmile je transakce zadána, peněženka přidá do transakce informace o cílové adrese a výši poplatku [24]. Výše poplatku může být různá, záleží na odesílateli, jestli je pro něj priorita, aby transakce byla rychle zpracována. Pokud pro něj rychlost není priorita, může nastavit menší poplatek.

Nyní je potřeba transakci kryptograficky podepsat, a proto je potřeba využít vlastností asymetrické kryptografie. Pokud je podepisován soubor, který bude poslán přes internet a potvrdit tím jeho pravost, je třeba vytvořit hash souboru a ten zašifrovat pomocí privátního klíče. Jedná o se o opačný proces jako při zasílání šifrovaných dat přes internet, kdy se šifruje pomocí veřejného klíče. Transakce podepsána privátním klíčem putuje dál k dalším uzlům, ke kterým je uzel peněženky připojen [3] [24] [50]. Peněženka může být připojena k více uzlům současně.

Jakmile transakce dorazí k dalším uzlům, ty ověří, jestli je transakce validní, a to především jestli z adresy neodchází větší počet mincí, než je na ni uloženo. Také ověří, jestli je transakce správně podepsaná pomocí veřejného klíče odesílatele, jestli se odesílatel nesnaží utratit mince, které již byly utraceny v minulosti atp. Pokud by byly nalezeny nějaké nesrovnalosti, transakce se zavrhne. Pokud jsou všechny potřebné informace o transakci ověřeny, uzel transakci opět odešle dalším k uzlům, ke kterým je připojen. Proces přeposílání transakcí skrz uzly probíhá až do té doby, než všechny uzly nemají informaci o odeslané transakci [24].

Uzel nemá představu o tom, jestli předešlý uzel transakci vytvořil, nebo ji jen přeposílá. Těchto transakcí protéká skrz uzly několik za sekundu a jejich úkolem je informaci o transakci šířit dál napříč celou Bitcoinovou sítí. Je žádoucí, aby každý uzel ověřoval transakce v síti a tím byla zaručena jejich korektnost [24].

Když transakce dorazí k těžaři, je zařazena do jeho memory poolu. Jestli je pro něj poplatek z transakce dostatečně atraktivní, je zařazena do jeho kandidátního bloku. Když se blok povede vytěžit, je transakce navždy zapsána v blockchainu [28]. Transakce se považuje za provedenou po vytěžení několika dalších bloků, a to z toho důvodu, že by pro případného útočníka bylo velice náročné vytěžit několik bloků za sebou.

Po vytěžení bloku je potřeba provést stejný proces šíření informace v rámci sítě, jako v případě informace o transakci. Těžař, který vytěžil blok odešle informaci o vytěženém

bloku dalším uzlům, na které je napojen. Uzly informaci zpracují a ověří, jestli byl blok korektně uzavřen. Ověří jednotlivé transakce v právě vytěženém bloku, a jestli jsou všechny informace správné, začnou opět šířit informaci o bloku dalším uzlům, dokud všechny uzly neobdrží informaci o nově vytěženém bloku [3] [24] [28].

5 ŠKÁLOVATELNOST SÍTĚ

Jelikož doba těžby jednoho bloku je uměle omezena stejně jako velikost bloku, není kapacita Bitcoinové sítě nekonečná. V počátcích celé sítě byly transakce velmi levné, jelikož bloky nebyly zdaleka tak naplněné transakcemi, jak je tomu nyní. Těžaři museli zařazovat do bloku všechny transakce co mohli, aby dosahovali co největšího výdělku. S tím, jak Bitcoin získával na popularitě, se začínal plnit mempool a s ním i bloky [52] [53].

Dnes lze pozorovat stav, kdy jsou skoro všechny bloky zaplněny, tak jak protokol dovoluje [53]. Navíc kvůli zaplněnému mempoolu se na zařazení transakce do bloku musí čekat. Pokud odesílatel nenastaví vyšší poplatek, který těžaře motivuje k zařazení transakce do bloku více než transakce s menším poplatkem, bude jeho transakce zpracována za dlouhou dobu. Zpracování může trvat hodiny a při vyšším vytížení i dny. Transakce o malé hodnotě někdy může stát na poplatku daleko více, než je její hodnota. To celé komplikuje používání Bitcoinu k mikroplatbám [53].

Aktuální transakční kapacita Bitcoinové sítě je kolem 3-6 transakcí za sekundu. To odpovídá zhruba 2000-3000 transakcí za blok [53]. Vývojáři Bitcoinu si začali uvědomovat, že tenhle stav není do budoucna udržitelný. Bitcoinový protokol sice obdržel několik nových vylepšení, které zajišťují větší efektivitu sítě, ale bylo potřeba vymyslet jiný systém, který by dovoloval dále používat Bitcoin i na menší transakce.

5.1 Lightning Network

Lightning Network (LN) má být řešením pro provádění nejen mikroplateb v Bitcoinové síti. Jedná se o zcela novou transakční vrstvu, která funguje tzv. „off-chain“ [54]. Tím je myšleno, že pro provedení transakce není potřeba využívat blockchain. Je to právě zápis transakce do blockchainu, co dělá transakce drahými.

Transakce na Lightning Network jsou zpracovány téměř instantně. Reálně dokáže transakce dorazit v rámci jednotek sekund. Poplatky jsou buď žádné nebo velmi malé. Záleží na tom, přes kolik uzlů transakce putuje. Jednotlivé uzly si berou velmi malý poplatek za přesměrování transakce. Na rozdíl od těžení je „routing“, neboli přesměrovávání transakce, činnost, která není tak ekonomicky výdělečná (viz. 7.4 Ekonomické a energetické hledisko provozu uzlu). Jedná se spíše malou odměnu za pomoc při provedení transakce. Transakční kapacita Lightning Network je teoreticky neomezená, výhodou může být i mnohonásobně menší energetická náročnost [54].

Samotná nová transakční vrstva není povinnost. Je zcela na uživateli, zda chce využívat výhod Lightning Network, anebo zůstane u přes 10 let ověřených „on-chain“ transakcí.

5.1.1 Základní princip Lightning Network

Lightning Network se snaží transakce vypořádávat off-chain v rámci kanálů, které jsou otevírány mezi dvěma uživateli. Uživatelé si otevřou kanál mezi sebou, jelikož jsou si vědomi, že budou mezi sebou posílat transakce častěji. V tomto kanálu jsou schopni provádět transakce tak často, jak jen chtějí a v případě, že budou transakce posílat jen mezi sebou, je poplatek za transakci nulový [54] [55].

Otevření kanálu ovšem není zdarma. Provádí se transakcí na blockchainu, tím pádem transakce podléhá poplatku za vytěžení. Po vytěžení již jsou všechny transakce prováděny off-chain. Jakmile se někdo z účastníků v platebním kanálu rozhodne kanál uzavřít, nebo se oba shodnou na uzavření kanálu, zapíše se konečný stav mezi dvěma uživateli do blockchainu, přičemž si mohli mezi sebou vyměnit i tisíce transakcí, ale v blockchainu se objeví jen počáteční a konečný stav [54].

Díky tomuto mechanismu umožňuje Lightning Network značně ulevit blockchainu. Nevýhodou zůstává nutnost provedení aspoň dvou on-chain transakcí (obyčejná bitcoinová transakce zapsaná v blockchainu), kterýma se zapisuje počáteční a konečný stav platebního kanálu.

K vytvoření platebního kanálu se využívá vlastností transakcí a peněženek, bez kterých by kanály nemohly existovat.

5.1.2 Multisig adresa

Jedním ze základních kamenů platebního kanálu je tzv. multisig adresa. Jedná se obyčejnou adresu s tím rozdílem, že k utracení prostředků na dané adrese je potřeba více soukromých klíčů. V Lightning kanálu se využívá multisig adresa ve formátu „2 z 2“. To znamená, že je potřeba obou soukromých klíčů k utracení prostředků. Existují multisig adresy i s jiným nastavením. Pro platební kanál, kde zpravidla figurují dva účastníci se nejvíce hodí formát 2 z 2. Multisig adresa, má za úkol zabránit utracení prostředků druhou stranou bez povolení, a tedy k ochraně obou stran v platebním kanálu [56].

5.1.3 Časové zámky

Časové zámky, v anglické literatuře označované jako „Time-Locks“, slouží opět k ochraně proti zpronevěření prostředků jednou ze stran platebního kanálu.

Časové zámky zabraňují utracení mincí po nějakou dobu. Když je v nějaké transakci použit časový zámek, musí strana, která obdržela mince po nějakou dobu čekat, než je bude moci opět utratit [57].

Existují dva typy časových zámků. První typ nazývaný jako CheckLockTimeVerify (CLTV), zamyká mince na přesně daný čas v budoucnosti. Druhý typ nazývaný jako CheckSequenceVerify (CSV), zamyká mince na dobu přibližnou. Jakmile je zapsán do blockchainu CSV zámek nad určitou transakcí, musí příjemce mincí čekat určitý počet bloků, které mají být vytěženy, než může mince utratit [57].

5.1.4 Hashové hodnoty a secret

Posledním stavebním kamenem Lightning Network jsou hashové hodnoty a tzv. „secret“. Opět mají za cíl chránit uživatele před zpronevěřením prostředků druhou stranou.

Secret je obdoba privátního klíče. Jde pouze o velmi dlouhé číslo, které je nemožné uhodnout. Hashová hodnota je právě hash secret. Získání hashové hodnoty naznačuje následující rovnice [57]:

$$H = Hash(R) \tag{6}$$

Kde:

H – hashová hodnota

R – secret

5.1.5 Provádění transakcí v rámci kanálu

Pokud se dva účastníci rozhodnou vytvořit mezi sebou platební kanál, musí jako první poslat určitý obnos mincí na multisig adresu, od které má každý z účastníků jeden ze dvou privátních klíčů. Tato transakce, která je zapsána na blockchainu, je nazývána jako „funding transaction“. V platebním kanále může každá strana kanálu utratit jen tolik mincí, kolik poslala pomocí funding transakce na multisig adresu [57].

Po provedení funding transakce si obě strany vytvoří secret a vymění si mezi sebou jeho hashovou hodnotu. Poté může jakákoliv ze stran posílat peníze z jedné strany na druhou

[57]. Provedení transakce off-chain v rámci Lightning Network se nazývá „commitment transaction“. Poslední commitment transakce vždy reprezentuje aktuální stav kanálu.

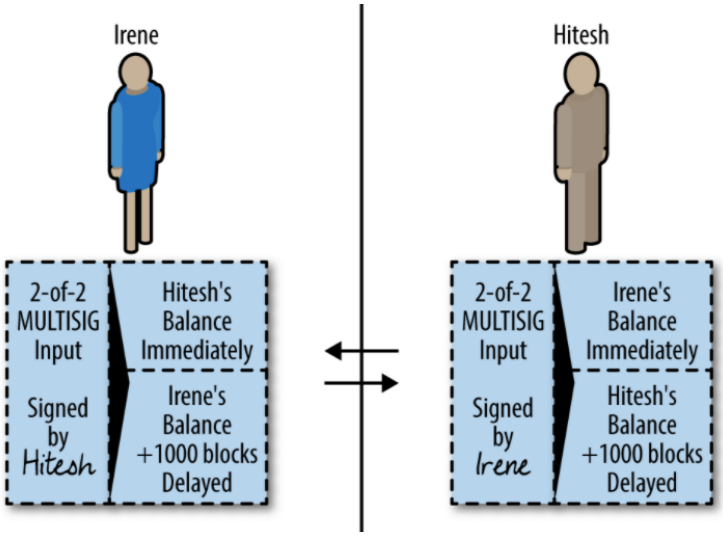
Po otevření kanálu pomocí funding transakce se ihned provede commitment transakce, která určuje stav prostředků na obou stranách kanálu. Kdykoliv se může jeden z účastníků rozhodnout, že chce kanál uzavřít a jeho poslední stav, který je v poslední commitment transakci uložen, zapsat na blockchain [55] [57].

5.1.6 Ochrana prostředků v kanálu

Existuje riziko, že by se jeden z účastníků kanálu mohl rozhodnout ukončit kanál a na blockchain nechat zapsat commitment transakci, která nereprezentuje poslední stav kanálu, ale bude zvýhodňovat jednoho z účastníků tím, že si nechá zapsat větší počet mincí, než jaký ukazuje poslední stav kanálu. Útočník by tím pádem mohl poslat na blockchain předešlou commitment transakci, ve které měl větší počet mincí než v následující.

Proto jsou v platebním kanálu využívány časové zámky, hashové hodnoty a secret [57]. Předpokládejme, že každá ze stran vložila pomocí funding transakce 5 BTC do multisig adresy.

Pokud se například strana A rozhodne poslat straně B 2 BTC, aby stav kanálu byl 3 BTC pro stranu A a 7 BTC pro stranu B, tak musí provést commitment transakci. 7 BTC obdrží protistrana ihned, zbývající 3 BTC může odesílatel utratit také, ale musí čekat 1000 bloků, než bude moct prostředky utratit on-chain. Zbývající 3 BTC může utratit i strana B, ale pouze pokud ví secret strany A. To slouží jako pojistka před zpronevěrou prostředků [57] [59].



Obrázek 6 Asymetric Revocable Commitments [60]

V případě, že by se strana B rozhodla, že chce aktualizovat stav kanálu tak, aby obě strany měly 5 BTC, tedy poslat 2 BTC straně A, musí si obě strany vytvořit nový secret a jejich hash si opět vyměnit. Také si musí vyměnit secret z minulé commitment transakce. Následně jedna ze stran vytvoří commitment transakci. Všechny transakce v obousměrných kanálech jsou tvořeny speciálně pomocí „Asymmetric Revocable Commitments“ [57] [59].

Díky těmto asymetrickým commitmentům obdrží každá ze stran stejnou transakci podepsanou protějškem, kterou mohou obě strany kdykoliv nechat zapsat na blockchain a tím uzavřít platební kanál. Nevýhodou pro každou ze stran je to, že pokud by se rozhodly uzavřít kanál zapsáním commitment transakce na blockchain, musely by čekat 1000 bloků [57] [59], než budou moct mince utratit, jako ukazuje obrázek *Obrázek 6 Asymetric Revocable Commitments*.

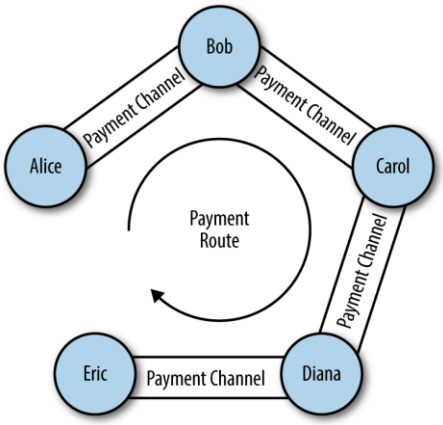
Strana A by se mohla pokusit provést podvod a ukončit kanál neférově tím, že by na blockchain poslala předposlední commitment transakci, která je pro stranu A výhodnější, jelikož v předchozím stavu měla větší počet mincí. Problémem je pro ni, že nemůže utratit mince z adresy po dobu 1000 bloků, protože jsou mince na adrese zamčené pomocí časového zámku [54] [57] [59].

Navíc strana B má po dobu 1000 bloků možnost vybrat všechny prostředky kanálu pro svůj prospěch, protože vlastní secret z minulé transakce, který si museli vyměnit při vytvoření nové commitment transakce [57] [59].

Pomocí tohoto mechanismu je zajištěno, aby obě strany kanálu byly férové, v opačném případě ztratí všechny prostředky v kanálu. Strana B musí na podvod reagovat sama, mechanismus se neděje automaticky [59].

5.1.7 Vícekanálové transakce

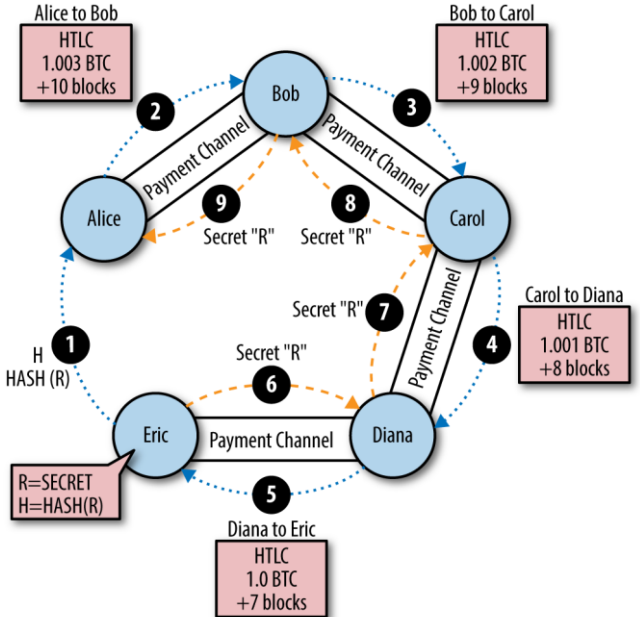
Jednou z největších výhod Lightning Network je možnost posílat off-chain transakce přes více kanálů. Uvažujme situaci, kdy Alice má otevřený kanál s Bobem a Bob má otevřený kanál s Carol. Pokud by Alice chtěla zaplatit pomocí Lightning Network Carol, nemusí nutně otevírat nový kanál, který by ho stál zbytečné poplatky. Je možné využít obou otevřených kanálů k poslání transakce Carol od Alice. Kanály je možné napojovat dále, a na základě toho tvořit dlouhé platební struktury jako zobrazuje *Obrázek 7 Vícekanálová transakce* [58].



Obrázek 7 Vícekanálová transakce [60]

5.1.8 Hash time lock contracts

Pro vypořádávání vícekanálových transakcí byly vytvořeny tzv. „Hash time lock contracts“ (HTLC). Jedná se o domluvu mezi dvěma stranami v platebním kanálu, do které se zamknou prostředky po nějakou dobu [54] [55].



Obrázek 8 Využití HTLC ve vícekanálové transakci [60]

Kontrakt popisuje, že strana A zaplatí straně B, pokud strana B zná secret. Pokud strana B neposkytne správný secret a uplynula uzamykací doba, tak jsou prostředky převedeny zpátky straně A, která HTLC vytvořila [58].

Uvažujme příklad, který ukazuje *Obrázek 8 Využití HTLC ve vícekanálové transakci*, kdy Alice chce zaplatit Ericovi. Alice má otevřený kanál se Bobem, Bob s Carol, Carol s Dianou a Diana s Ericem.

1. Jako první Eric vytvoří secret a z něj hashovou hodnotu. Tu přes bezpečný komunikační kanál předá Alice, od které čeká platbu.
2. Alice vytvoří z hashové hodnoty HTLC a ten předá Bobovi. Tím se zavazuje Bobovi zaplatit, pokud předloží secret. Prostředky jsou vytvořením HTLC zamknuté v kontraktu.
3. V dalším kanálu Bob vytvoří opět HTLC a zamkne do něj prostředky. Ty se uvolní Carol, pokud předloží secret. Secret, který všichni účastníci musí předložit, je stejný pro všechny účastníky vícekanálové transakce. Tímto způsobem se vytvoří celkem 4 HTLC v jednotlivých kanálech od Alice až k Ericovi.
4. Jakmile si zamknou prostředky i v poslední kanálu mezi Dianou a Ericem, Eric si všimne, že se jedná o platbu, kterou očekává od Alice, a to kvůli tomu, že rozpozná, že se jedná hashovou hodnotu, kterou poskytl Alice.
5. Eric poskytne Dianě secret a tím se převedou prostředky od Diany k Ericovi.
6. Když Diana zaplatila Ericovi, ráda by také dostala zpět své prostředky, které zaplatila Ericovi. Proto využije secret, který od Erica získala a nechá si zaplatit od Carol. Tento proces se opakuje v každém kanálu, přes který putuje platba, dokud Bob nezíská secret od Carol a tím dostane platbu od Alice.

Tímto způsobem je možné převést prostředky přes několik kanálů, a to bez toho, aby si účastníci museli vzájemně důvěřovat. Díky HTLC byly prostředky vždy bezpečně uzamknuty a v případě selhání vícekanálové platby bylo možné navrátit prostředky odesílateli [54] [55] [58].

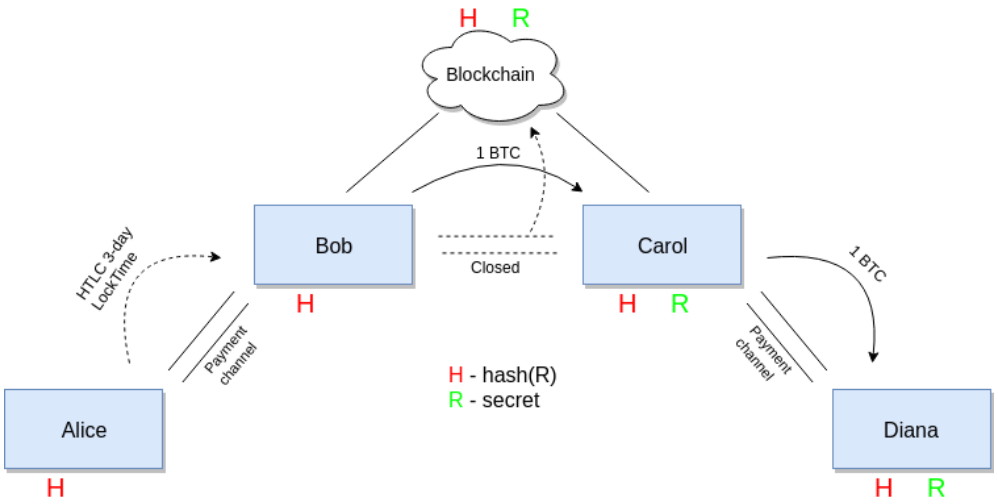
V rámci přesměrovávání platby nazývaného jako „routing“, si každý z uzlů vzal malý poplatek. To je nazýváno jako „routing fee“. Přesměrovávací poplatek je vždy předen znám odesílateli [54].

Výhodou pro účastníky je i zvýšená anonymita. Účastníci kanálu vidí jen na sebe navzájem. Nemají možnost nahlédnout jaké platby probíhají v jiných kanálech. Jediné, co je viditelné pro celou bitcoinovou síť, je počáteční (funding) transakce a také tzv. „settlement“ transakce, která ukončuje kanál. A to z toho důvodu, že tyto dvě transakce je třeba zapsat na blockchain [54].

5.1.9 Bezpečnost vícekanálových transakcí

V případě, že by nastala situace, že by se jeden z kanálu, přes který vede transakce, porouchal, je situace řešitelná [61].

Obrázek 9 Rozbitá vícekanálová transakce popisuje nefunkční kanálovou cestu, kdy Alice posílá platbu Dianě přes Boba a Carol a jeden z uzlů ve vícekanálové transakci přestane reagovat vlivem poruchy nebo záměrně.



Obrázek 9 Rozbitá vícekanálová transakce [61]

V tomto případě přestane Bob reagovat hned potom, co Diana vyzradila svůj secret Carol, a tím pádem byla první platba v kanálu vypořádána. Carol by ráda získala zpět prostředky, které zaplatila. Jelikož Bob nereaguje, uzavře Carol kanál pomocí poslední commitment transakce, což je HTLC kontrakt, který ji předtím Bob předal a pošle kontrakt na blockchain. Carol může použít kontrakt a získat z něj prostředky, jelikož má k dispozici secret od Diany z minulé kanálové transakce. Zbývá pouze vypořádání se mezi Alice a Bobem [54] [61].

Bob se neozývá, ale má díky časovému zámku v kontraktu několik dní na to, aby začal komunikovat a vypořádal se s Alice. Pokud by to nestihl do vypršení časového zámku, může Alice získat zpátky všechny prostředky, které měl původně obdržet Bob. Když se Bob znovu objeví, může si zjistit secret z blockchainu, který tam kvůli uzavření kanálu poslala Carol [61].

Jediný, kdo v téhle situaci riskuje ztrátu prostředků je buď Alice nebo Bob. Ostatní účastnící vícekanálové transakce jsou se svými prostředky v bezpečí. Proto se doporučuje používat Lightning Network především pro méně hodnotné transakce [54] [61].

5.1.10 Druhy implementací Lightning Network

V roce 2016 byl sepsán standard BOLT (Basis of Lightning Technology). Ten má za úkol ucelit specifikaci protokolu a umožnit spolupráci uzlů nezávisle na implementaci. Následně bylo vytvořeno několik různých implementací, každá se liší použitím jiného programovacího jazyka [62] [63].

lnd

Nejpoužívanější implementací je lnd. Byla vytvořena firmou Lightning Labs a je napsána v programovacím jazyky Go a podléhá licenci BSD-MIT [63].

c-lightning

Další významnou implementací je c-lightning. Dle názvu lze rozpoznat, že je napsána v programovacím jazyku C [63].

Eclair

Implementace Eclair byla vytvořena francouzskou firmu ACINQ. Z francouzského jazyka pochází také název implementace – Eclair neboli „blesk“. Implementace je napsána v programovacím jazyku Scala a je dostupná pod licencí Apache License 2.0 [63].

Electrum

Důležitou implementací Lightning Network je také od Electrum. Tato známá SW peněženka funguje již dlouho na počítači nebo mobilním telefonu. Vývojáři implementovali do peněženky podporu Lightning Network v programovacím jazyce Python. Tato implementace je dostupná pouze pro uživatele peněženky Electrum [63].

Rust-Lightning

Rust-Lightning je implementace, která vznikla spoluprací Rust Bitcoin komunity a firmou Square, za kterou stojí také zakladatel Twitteru Jack Dorsey. Implementace je dostupná pod licencí Apache 2.0 nebo MIT. Celá implementace je napsána v moderním programovacím jazyce Rust [63].

Další implementace

Existuje ještě řada dalších, avšak ne tak významných implementací jako např. LNP Node, Node-Lightning, lit atd. Mezi nejpoužívanější řešení patří c-lightning, lnd a Eclair [63].

6 VÝVOJ A BUDOUCNOST

Bitcoin, jakožto software, prodělal po dobu své existence mnoho vylepšení. Vývojáři, kteří na něm pracují, se snaží vylepšovat software Bitcoinu podle možných technických a uživatelských potřeb [64].

V minulosti se mluvilo o možnosti zvětšení kapacity jednotlivých bloků. Oproti aktuální kapacitě 1 MB by se velikost mohla zvětšit např. na 10 MB. To by mělo za následek zvýšení počtu transakcí, které mohou být zpracovány v rámci jednoho bloku, a tím pádem zvětšit transakční propustnost. Tento názor nebyl přijat velmi optimisticky. Mohly by se objevit nové problémy – např. některé uzly by nestačily takové množství transakcí zpracovávat a přetížily by se [64] [65] [66]. Také by se větší velikosti bloků nejspíše způsobila menší decentralizaci sítě.

Skupina lidí, která vystupovala pod názvem Bitcoin Unlimited, jež o zvýšení kapacity bloku usilovala, se dokonce odtrhla od hlavního blockchainu v roce 2017 [65]. Začaly tak koexistovat dva blockchainy. Událost rozdělení blockchainu na více větví se nazývá jako „hard fork“. Tímto hard forkem vznikla nová kryptoměna s názvem Bitcoin Cash [65].

Druhá názorová strana, kterou zastupovala drtivá většina sítě, upřednostňovala řešení jménem „Segregated Witness“. To řeší možnost zvýšení kapacity sítě tím, že odstraní z jednotlivých transakcí v bloku podpisová data, která zabírají velkou část kapacity v bloku [66].

Segregated Witness, zkráceně Segwit, přemisťuje podpisová data v blocích do bloků, které obsahují pouze tato podpisová data [66]. To znamená, že každý nový blok má svůj další druhotný blok, který obsahuje pouze podpisová data. Díky tomu by bylo dosaženo uvolnění místa v bloku a bylo by možné naplnit blok více transakcemi. Řešení, které nevyústí v rozdělení sítě na dva blockchainy, a tím pádem dvě různé kryptoměny, se nazývá „soft fork“ [67].

Očekávaným vylepšením Bitcoinového protokolu mají být Schnorrovy podpisy a tzv. „Taproot“. Schnorrovy podpisy existují již několik dekád. Nebyly použity při vytvoření Bitcoinu z toho důvodu, že podléhaly patentu. Ten vypršel v roce 2008. V té době již pravděpodobně vznikal Bitcoin [68].

Schnorrovy podpisy umožňují agregací více podpisů do jednoho, a tím by mohlo být umožněno efektivnější využití kapacity bloku, a navíc přinést trochu větší bezpečnost,

jelikož by podpisová data byly agregovány do jednoho podpisu a nebylo by poznat, jaké podpisy byly agregovány [68].

Taproot by měl umožnit další zvýšení soukromí, a to díky ukrytí podmínek pro utracení prostředků z peněženky [68].

II. PRAKTICKÁ ČÁST

7 VLASTNÍ UZEL V LIGHTNING NETWORK

Vlastní uzel v sítí Lightning Network dovoluje posílat Lightning transakce skrz síť Lightning Network. Již bylo zmíněno, že transakce přes LN jsou velmi levné a jsou obdržovány téměř ihned. Navíc vlastní uzel dovoluje využívat další výhody, který nabízí, jako maximální kontrola nad platebními kanály, větší bezpečnost než využívání Lightning peněženky na telefonu a bonusové aplikace, které většinou softwarový balík pro provoz uzlu nabízí [69].

Existují řešení, které se snaží vylepšit uživatelskou zkušenost a mažou nutnost vlastnictví uzlu. Takové řešení nabízí například mobilní softwarová peněženka BlueWallet. Lze s ní využívat Lightning Network bez nutnosti vytvoření vlastního uzlu. Uživatel se připojuje k uzlu, který provozuje společnost BlueWallet Services, který má již otevřené platební kanály s dalšími uzly. Nevýhodou tohoto řešení je, že musíme s našimi prostředky důvěřovat třetí straně. Naopak výhodou je větší jednoduchost užívání a menší režie, protože odpadá nutnost spravovat platební kanály a dostatečně je zásobovat likviditou [70].

V této práci je popsáno zhotovení vlastního uzlu. Vlastní uzel nabízí maximální možnost přizpůsobení a totální správu prostředků a kanálů. Blíže budou možnosti ovládání, správy a využití uzlu rozepsány v dalších podkapitolách.

7.1 myNode

myNode je softwarový balík založený na operačním systému Raspbian určený pro SBC (Single-board computer) Raspberry Pi nebo Rock64 a snaží se poskytnout prostředí pro snadný provoz jak Bitcoin, tak Lightning uzlu [69].

Pro zhotovení vlastního Bitcoinového a Lightningového uzlu byl zvolen softwarový balík s názvem myNode. Balík je zdarma ke stažení na oficiálních stránkách[1]. Celý projekt je distribuován s cenovou strategií „freemium“, to znamená, že většina základních i nadstandartních funkcí je ke stažení zdarma. V této práci bylo zvoleno řešení myNode, jelikož se jedná o jeden z prvních řešení, které nabízí provozovat svůj vlastní uzel. Navíc myNode poskytuje mnoho dalších aplikací, které rozšiřují možnosti využití uzlu. Jedná se o aplikace, které poskytují Lightning Network platební bránu nebo aplikace, které se zaměřují na soukromí uživatelů Bitcoinu [69].

[1] Ke stažení na: https://mynodebtc.com/

Ostatní specifické služby, které nabízí myNode jsou zpoplatněné a jsou popsány v kapitole 7.3.3 Aplikace. Licence pro prémiové funkce aktuálně stojí $99 a jde o jednorázovou platbu. Všechen kód lze najít na repositáři GitHub, kde lze získat informaci, že velká část je napsána v programovacím jazyce Python a webovém frameworku Flask [69] [71].

myNode je designován k tomu, aby běžel neustále na zařízením jako Raspberry Pi. Je doporučeno být aktivní v jednotlivých otevřených platebních kanálech, aby byla zajištěna bezpečnost prostředků. Kvůli provozu na Raspberry Pi je spotřeba takového uzlu velmi nízká a zařízení může fungovat bez přerušení (viz. kapitola 7.4 Ekonomické a energetické hledisko provozu uzlu) [69].

K provádění transakcí na Lightning Network používá myNode implementaci lnd, která byla popsána v kapitole 5.1.10 Druhy implementací Lightning Network [71].

7.1.1 Hardwarové požadavky myNode

Minipočítač

K provozu uzlu je potřeba výpočetní technika, na které bude provozován operační systém od balíku myNode. Minipočítač bude po instalaci myNode kontrolovat transakce a bloky, které se budou objevovat v bitcoinové síti [24].

Samotný balík nabízí instalační soubory pro minipočítače Raspberry Pi 4 a RockPro64. Minipočítače by měly mít aspoň 4 GB operační paměti. Pro experimentování lze nainstalovat balík i na virtuální počítač, který bude běžet ve VirtualBoxu. Balíček je možné nainstalovat i na starší zařízení jako Raspberry Pi 3 a Rock64, přičemž instalace na tyto zařízení není doporučována, a to z toho důvodu, že jejich výkon není dostatečný a mohly by nastat výkonnostní problémy. Jiné minipočítače nejsou podporovány [69].

Napájecí adaptér

Kromě samotného minipočítače je potřeba i další hardware. Aby mohl počítač fungovat, je třeba napájecí adaptér. Adaptér musí poskytovat napětí a proud 5,1 V a 3 A stejnosměrného proudu o celkovém výkonu 15,3 Wattů s konektorem USB-C [72].

MicroSD karta

Pro nahrání celého operačního systému je potřeba microSD karta, která se vloží do mikropočítače. Její kapacita by měla být aspoň 16 GB.

Z karty se po vložení do microSD konektoru počítače bude spouštět operační systém od balíku myNode. Proto je určená minimální kapacita, aby se celý operační systém se všemi aplikacemi na kartu vešel [69].

Disk

Zbytek dat se ukládá na externí disk, který je připojený přes sběrnici USB. Podle dokumentace myNode lze použít buď HDD (Hard Disk Drive) nebo SSD (Solid State Drive) [69]. Obecně je doporučeno používat SSD, a to především proto, že prostředí poběží daleko rychleji a bude mnohem více responzivní. To je dáno tím, že SSD nemá žádné pohyblivé části a kvůli tomu může přistupovat k uloženým datům na disku daleko rychleji než HDD [73]. Důležité je, aby disk měl kapacitu alespoň 1 TB. Je to z toho důvodu, že se na něj bude stahovat celý blockchain, který samotný zabírá přes 300 GB. Přesto by nebyl dostatečný ani disk s kapacitou 500 GB, jelikož bloky, adresy a transakce se musí indexovat, aby v nich bylo možné rozumnou rychlostí vyhledávat. Indexy zabírají další místo na disku [69].

Je možné použít jak interní disk s externím boxem, který umožňuje disk pomocí USB připojit k minipočítači nebo taky rovnou externí disk, který má připojovací kabel od výroby [69].

Ostatní požadavky

K tomu, aby se mohlo zařízení synchronizovat s blockchainem, je potřeba připojení k internetu [24]. Obě podporované zařízení mají Ethernet port, kde je možné je pomocí internetového kabelu s konektorem RJ45 připojit k internetu [72] [74].

Doporučuje se zařízení vybavit lepším chlazením. Oba počítače jsou prodávány bez dodatečného chlazení a spoléhají na chlazení pasivní. Výše uvedené minipočítače jsou celkem výkonné a v teplém prostředí může být jejich výkon nepříjemně ovlivňován kvůli „throttlingu“. Ten snižuje takt procesoru počítače, aby zůstal dostatečně chladný. Tím se snižuje rychlost běhu systému [75].

Throttling lze řešit pomocí dodatečného chlazení. Pasivní chlazení lze podpořit tzv. heatsinky (žebrovaný kovový chladič). Ty se nalepí na ty části počítače, které generují nejvíce tepla a tím se podpoří výměna tepla mezi čipem a okolím. Heatsinky je vhodné doplnit aktivním chlazením ve smyslu ventilátoru, který urychluje odvádění tepla ze zařízení [76]. Nevýhodou je hlučnost ventilátoru.

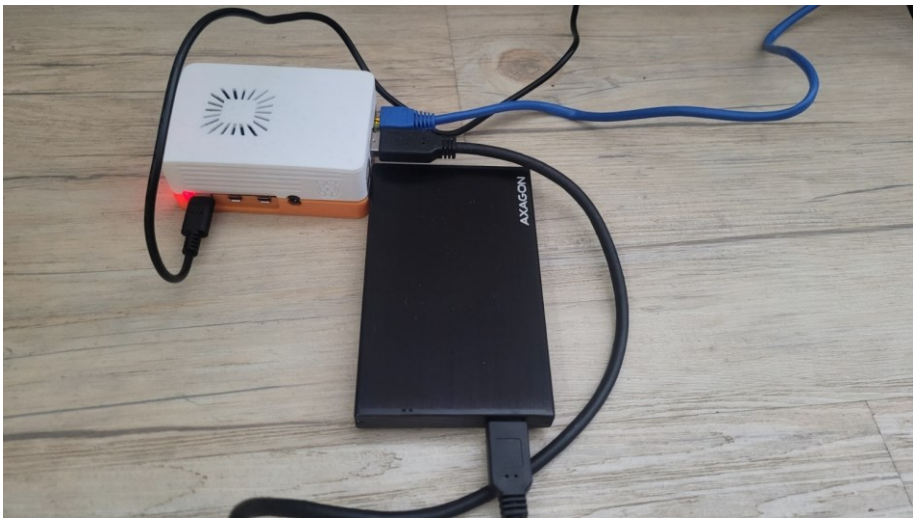
Další možností může být vložení celého mikropočítače do krabičky, která ochraňuje celé zařízení zvenčí.

7.1.2 Použitý hardware

V této práci byl zvolen minipočítač Raspberry Pi 4 se 4 GB RAM, a to především z důvodu jeho snadné dostupnosti. Počítač RockPro64 je velmi obtížně dostupný na českém trhu.

Z důvodu rychlosti systému byl použit SSD značky Kingston, konkrétně model A400 s kapacitou 960 GB. Jde o tradiční SSD nižší třídy, které je plně dostatečné pro práci s vlastním Lightning uzlem.

Disk je připojen přes SATA sběrnici k externímu boxu. Samotný externí box nepotřebuje přídavné napájení a je napájen přímo z minipočítače. Externí box je značky Axagon. Modelové označení je EE25-XA6.



Obrázek 10 Použitý HW k provozu uzlu

V poslední řadě je zařízení uloženo v ochranné krabičce, která byla zhotovena na 3D tiskárně. Krabička nebyla zhotovena vlastním úsilím, ale byla zakoupena na internetu. Krabička obsahuje malý ventilátor, který je připojen k počítači a z něj je také napájen. Ventilátor má konstantní rychlost. Na místech, které vyzařují teplo, jsou připevněny heatsinky, které pomáhají s chlazením počítače. *Obrázek 10 Použitý HW k provozu uzlu* ukazuje všechny použité komponenty.

7.1.3 Alternativy myNode

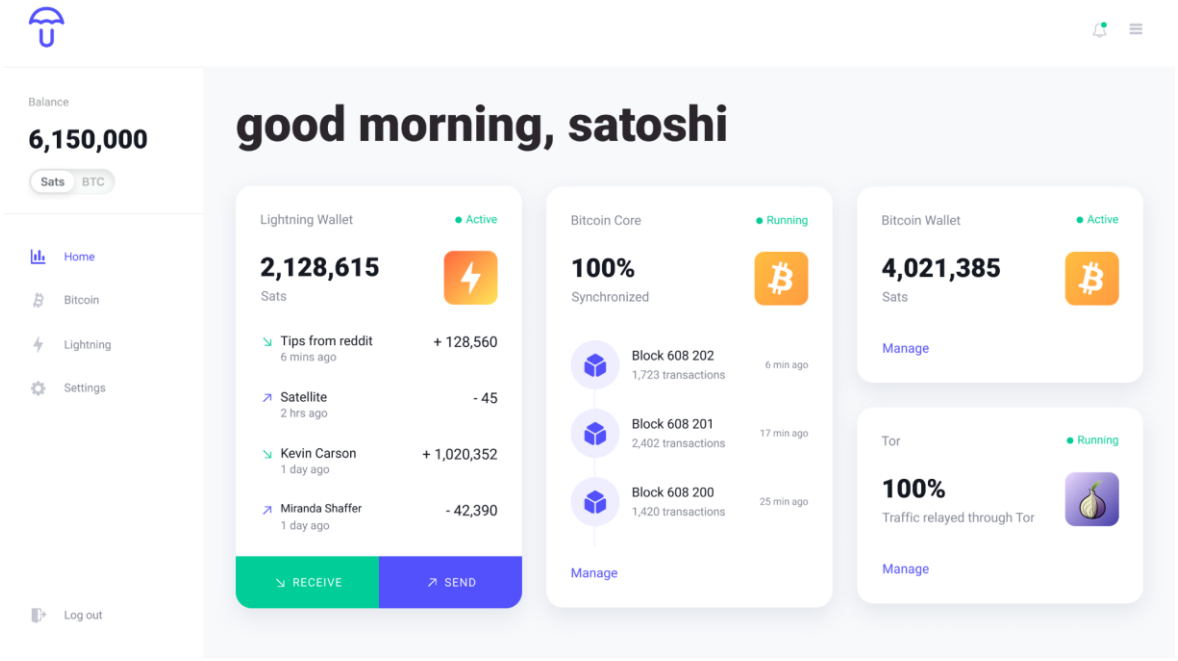
Kromě myNode lze najít i alternativní řešení, které poskytují funkcionalitu Bitcoin a Lightning uzlu. Všechny řešení jsou zpravidla open-source. To je velice důležité, protože

je nežádoucí, abychom svěřovali své prostředky softwaru, o kterém nevíme, jak bude pracovat.

Umbrel

Mezi nejznámější alternativy se řadí Umbrel. Balík Umbrel poskytuje funkcionalitu Bitcoinového uzlu a mimo to zvládá i Lightning transakce. Umbrel je možné nainstalovat na minipočítač typu Raspberry. Potřebný hardware je velmi podobný tomu, který je potřeba k zprovoznění řešení myNode [77].

Výhodou Umbrel je jeho velmi jednoduché a vkusné uživatelské rozhraní (viz. *Obrázek 11 Uživatelské rozhraní balíčku Umbrel*). V tomto ohledu je vhodnější pro začátečníky, jelikož se snaží být jednoduchý pro použití. Navíc Umbrel nabízí mnoho dalších aplikací, které můžou být na počítač nainstalovány, a tím pádem rozšiřovat možnosti, které uzel může nabídnout (jedná se o podobné nebo stejné aplikace jako jsou popsány v kapitole 7.3.3 Aplikace) [77].



Obrázek 11 Uživatelské rozhraní balíčku Umbrel [77]

I přes lákavé uživatelské rozhraní nebylo řešení Umbrel pro tuto práci zvoleno. Umbrel je stále mladý projekt na rozdíl od myNode a existuje riziko, že se v něm bude vyskytovat mnoho neodhalených chyb.

RaspiBolt

Podobnou funkcionalitu, jako řešení myNode nebo Umbrel, dokáže zprostředkovat i RaspiBolt. Toto řešení má za cíl také nabídnout vlastní Lightning a Bitcoin uzel, který bude

běžet na minipočítači Raspberry Pi. Instalace a nastavení uzlu se neobejde přes zadávaní příkazů přes příkazovou řádku a pro méně zkušené uživatele může toto být problémem. Je ovšem doporučený pro zkušené uživatele. Z toho důvodu nebyl zvolen pro tuto práci. Uživatel, který nemá zkušeností s Linuxem a příkazovým řádkem riskuje, že může svou chybou ztratit prostředky [78].

Nodl

Nodl je další ze série možných uzlových řešení na Bitcoinové síti. Nodl nabízí rovnou hardware s předinstalovaným systémem. Řešení se snaží být plně upravovatelné pro zkušené uživatele a také bere v potaz soukromí uživatelů. Toto řešení nebylo vybráno, protože na internetu nebyla nalezena dokumentace, která by popisovala ovládání uzlu. Dalším odrazujícím faktorem je vysoká cena, za kterou se zařízení prodává ($529) [79].

7.2 Příprava a instalace

Před instalací samotného softwaru myNode je třeba stáhnout instalační soubor systému pro konkrétní počítač z oficiálních stránek[2] myNode. V tomhle případě se jednalo o verzi pro Raspberry Pi 4. Systém je potřeba nahrát na paměťovou kartu, která se bude vkládat do počítače.

Pro nahrání paměťové karty se v dokumentaci doporučuje použít nástroj Balena Etcher nebo Raspberry Pi Imager [69]. Oba nástroje jsou zdarma ke stažení na platformy Windows, Linux nebo macOS. V tomto případě byl použit nástroj Balena Etcher[3].

Kartu je vložena do počítače, který má čtečku paměťových karet a je provedeno flashnutí karty pomocí nástroje a instalačního souboru, který byl stažen. Oba nástroje se snaží být, co nejjednodušší.

Bylo zvoleno jen cílové zařízení (karta) a instalační soubor, který je na kartu nahrán. Během chvíle se na kartu nahraje systém, to ovšem platí pro rychlé počítače. Na pomalejším stroji může nahraní systému na kartu trvat i desítky minut.

K zařízení se musí připojit všechen potřebný hardware, což v tomto případě znamená pouze disk. Dále je třeba zařízení připojit k internetu pomocí Ethernet kabelu. Potom zbývá jen připojit napájecí kabel a zařízení se ihned zapne a systém se spouští – tzv. bootuje.

[2] myNode ke stažení: myNode Download (mynodebtc.com)
[3] BalenaEtcher ke stažení: https://www.balena.io/etcher/

Jakmile zařízení nabootuje, je dostupné k přístupu z lokální sítě. Celé zařízení se ovládá přes webový server, který je spuštěn na zařízení. K přístupu do webového rozhraní lze použít URL „mynode.local“. Do webového rozhraní je možné přistoupit z jakéhokoliv zařízení, které má k dispozici webový prohlížeč a nachází se ve stejné síti. Přístup přes URL „mynode.local“ nemusí být vždy spolehlivý, někdy se stane, že přístup přes URL z důvodu chyby nefunguje a je třeba přistoupit pomocí IP adresy, kterou přiřadil zařízení místní DHCP (Dynamic Host Configuration Protocol) server. IP adresu lze zjistit například v routeru sítě. Zařízení vysílá do sítě svůj název a je možné ho najít pod názvem „myNode“ (viz. *Obrázek 12 Zjištění IP adresy myNode v routeru*).

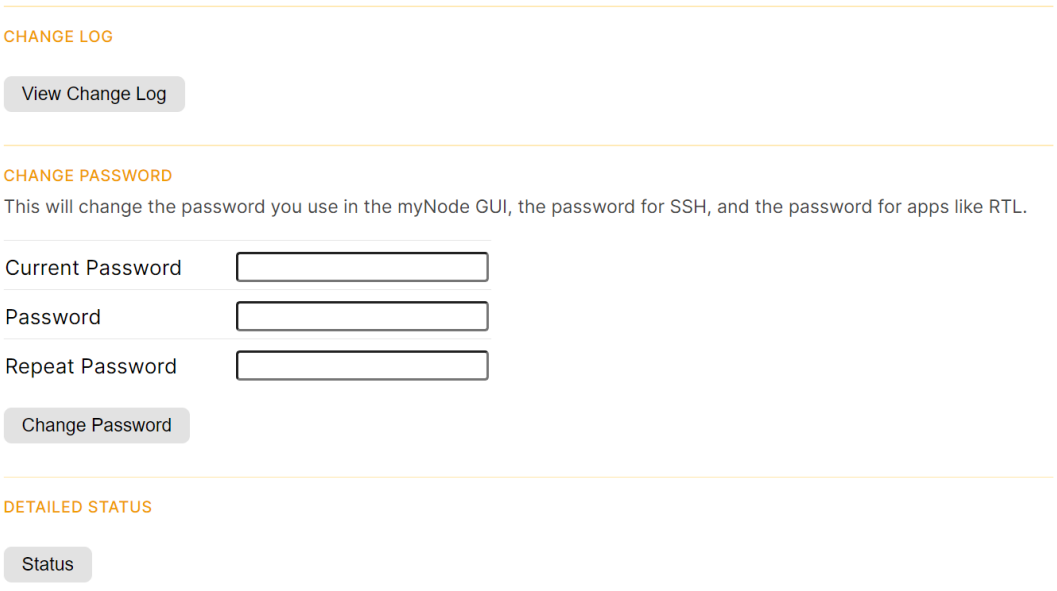
Obrázek 12 Zjištění IP adresy myNode v routeru

Po přístupu na webový server zařízení se zobrazí uvítací obrazovka, kde lze vložit klíč, který zpřístupní všechny prémiové funkce nebo pokračovat na verzi zdarma, což bylo využito v tomto případě.

Obrázek 13 Stahování blockchainu na myNode

Hned poté se začne zařízení synchronizovat s blockchainem. To znamená, že začne stahovat celý blockchain na připojený disk. Kvůli velké velikosti blockchainu může tento proces trvat řadu dní. Prostředí myNode ukazuje uživateli, v jaké fázi se synchronizace s blockchainem nachází, konkrétně ukazuje, kolik bloků již bylo z celkového počtu bloků staženo (viz. *Obrázek 13 Stahování blockchainu na myNode*). Při vypracovávaní této práce se zařízení synchronizovalo celých 14 dní.

Po stažení celého blockchainu se ukáže výchozí menu, z kterého se ovládá uzel. Doporučuje se ihned po stažení změnit výchozí heslo, kterým se přistupuje k uzlu, aby se zamezilo

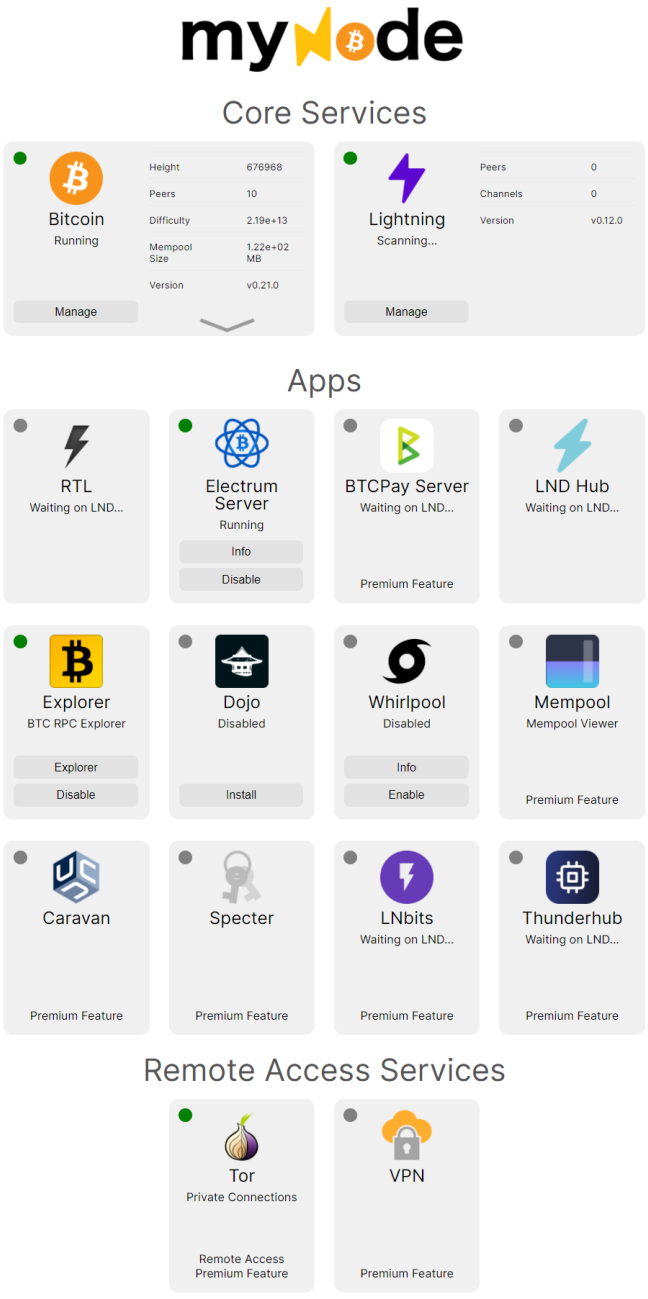


Obrázek 14 Změna hesla v nastavení myNode

zneužití prostředků. Změnu hesla lze provést v nastavení uzlu, konkrétní formulář pro změnu hesla zobrazuje *Obrázek 14 Změna hesla v nastavení myNode*.

7.3 Ovládání uzlu

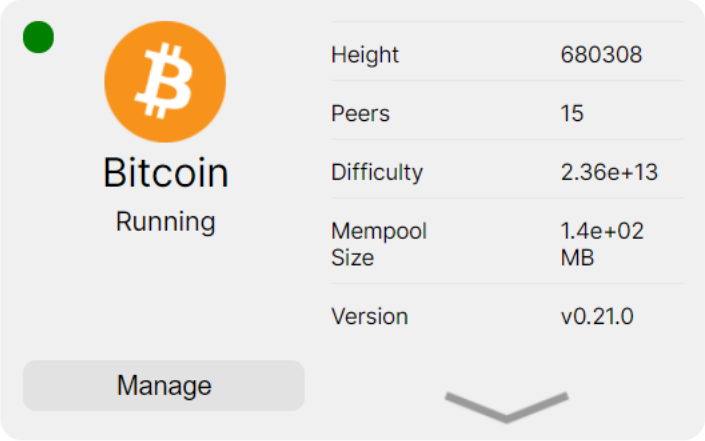
Ve výchozím menu, které ukazuje *Obrázek 15 Výchozí menu myNode*, je možné spustit všechny aplikace, které balíček myNode nabízí. Pokud uživatel chce využívat jen vytváření kanálů a Lightning transakcí, nemusí všechny aplikace využívat. Slouží jako možnost rozšíření možností toho, co Bitcoinový uzel nabízí.



Obrázek 15 Výchozí menu myNode

7.3.1 Bitcoinový uzel

Ve vrchní části menu se nachází pod nadpisem „Core Services“ základní ukazatele uzlu. Levá část poskytuje informace o Bitcoinovém uzlu a aktuálním dění v blockchainu a mempoolu jako např. „Height“, což je číslo naposled vytěženého bloku. Dále „Peers“, který ukazuje, ke kolika dalším uzlům je náš uzel napojen. To souvisí s tím, že Bitcoin je decentralizovaná platforma, a je nutné stáhnout blockchain od jiných uzlů, kteří ho na svém zařízení uchovávají [24].



Obrázek 16 Informace poskytující Bitcoinový uzel

Údaj difficulty značí aktuální složitost pro vytěžení bloku. Z obrázku lze vidět, že prostředí uzlu zobrazuje toto číslo v exponenciálním formátu. To z toho důvodu, že toto číslo je v dnešní době obrovské, a proto se volí kompaktnější formát [30].

Mempool size udává sumu velikosti transakcí v mempoolu, které čekají na to, až budou těžařem zařazeny do blockchainu [24].

Poslední údaj „Version“ značí verzi softwaru Bitcoin Core. Jde o původní bitcoinovou peněženku, která byla používána především v počátcích Bitcoinu. Bitcoin Core požadoval pro posílání transakcí vlastní uzel neboli „full node“, a to z toho důvodu, aby mohl ověřovat transakce například při odesílání mincí. Později byly vyvinuty způsoby, které nevyžadují k používání peněženky provozovat full node, a tím pádem stahovat celý blockchain na zařízení. V dnešní době má Bitcoin Core místo jako full node implementace, případně je vhodný pro uživatele, kteří nechtějí důvěřovat ostatním účastníkům sítě (uzlům), ale chtějí mít maximální kontrolu nad svými prostředky [80].

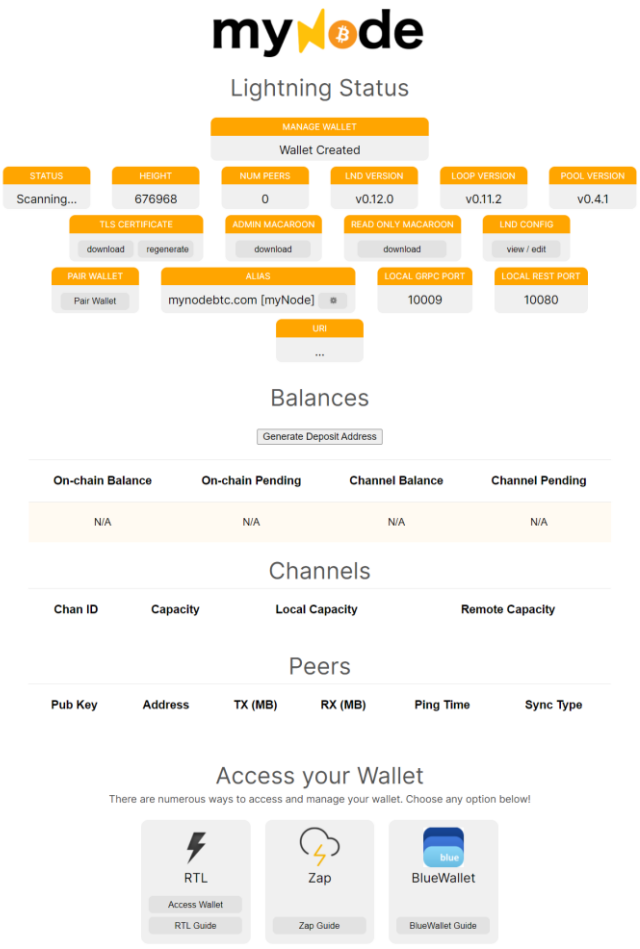
Mimo tyto ukazatele, které ukazuje *Obrázek 16 Informace poskytující Bitcoinový uzel*, lze po rozkliknutí šipky sledovat poslední vytěžené bloky s informací o tom, kdy byly vytěženy a kolik obsahují jednotlivé bloky transakcí. Pomocí tlačítka „Manage“ lze dokonce sledovat,

na které uzly je naše zařízení připojené. Pokud uživatel není v síti, která má veřejnou IP adresu, připojuje se uzel k ostatním uzlům především přes síť Tor.

Tor využívá ke komunikaci přes internet několik uzlů. Komunikace přes uzly je šifrována, kvůli tomu samotné uzly nevědí, jaké informace přes něj protékají (s výjimkou posledního uzlu, který komunikuje s cílovým serverem). Šifrování je několikanásobné, když uživatel zadá požadavek, který se bude šířit přes Tor, ten následně putuje např. přes 3 uzly. Na prvním uzlu je první šifrovací vrstva dešifrována a požadavek poslán na další uzel. Další uzel opět dešifruje další šifrovací vrstvu atd. Až poslední uzel, který pošle na cílový server, vidí kompletně dešifrovaná data [81].

7.3.2 Lightning uzel

Druhá část uzlu se skládá z Lightning Network. Před používáním samotného Lightning Network je potřeba vytvořit peněženku. Prostředí nám vygeneruje tzv. „seed“, který slouží jako předloha pro generování privátních klíčů. Je nutné seed bezpečně uchovávat, nejlépe



Obrázek 17 Podrobnosti LN uzlu

na místo, kde není dosažitelný z online prostoru, proto je vhodné opsat si seed například na papír a uložit na místo, kde nemůže být znehodnocen nebo ukraden. V případě ztráty seedu a selhání zařízení by byly ztraceny i všechny prostředky v peněžence, protože ze seedu se generují všechny privátní klíče v peněžence [24].

Po bezpečném uložení seedu je možné prohlížet nastavení Lightning uzlu a rovnou začít vytvářet kanály a posílat transakce. K statusu Lightning uzlu se lze dostat pomocí tlačítka „Manage“ pod nadpisem Lightning.

Následně se ukáže prostředí (viz. *Obrázek 17 Podrobnosti LN uzlu*), kde je možné získat důležité informace o uzlu a případně ho i konfigurovat. Lze například nastavit implementaci Lightning Network lnd, popř. připojit peněženku k uzlu, přes kterou lze ovládat uzel. Lze zde najít informace, které slouží k připojení k uzlu jako porty a URI. Mimo to je možné stáhnout zálohu všech otevřených kanálů a vytvořit adresu na příjem mincí, které slouží k posílání transakcí v kanálech. Samozřejmostí je informace o otevřených kanálech a jejich kapacitách.

Tato sekce je vhodná pro konfiguraci Lightning uzlu a rychlou informaci o kanálech. Samotné ovládání Lightning uzlu není prováděno v této sekci, ale v aplikaci Ride the Lightning, která je popsána v kapitolách 7.3.3 Aplikace, 7.3.4 Vytvoření platebního kanálu, 7.3.5 Podrobné informace o kanálu a 7.3.6 Provedení Lightning transakce.

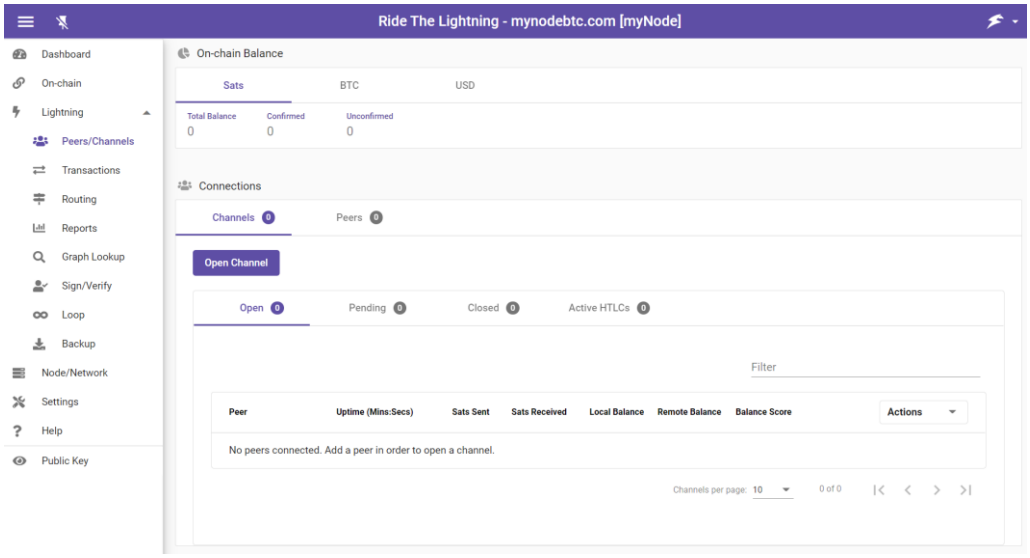
7.3.3 Aplikace

Většina nutných nebo velmi užitečných aplikací jsou dostupné i ve free verzi. Nadstandartní aplikace jsou k dispozici pouze v premium verzi [69]. Nejedná se ovšem o aplikace, bez kterých by uzel nebylo možné pohodlně používat. Většinou jde o aplikace, které velká část uživatelů nepotřebuje, naopak mohou být výhodné pro uživatele, kteří si například zakládají na soukromí nebo chtějí zcela využívat možnosti, které balíček myNode poskytuje.

Ride The Lightning

Jedna z nejdůležitějších aplikací je Ride The Lightning (RTL). Aplikaci lze otevřít po té, co je vytvořena Lightning peněženka. Je dostupná i ve free verzi [69] [82].

Prostředí aplikace RTL, které ukazuje *Obrázek 18 Prostředí Ride The Lightning*, slouží ke kompletní správě kanálů, likvidity, routingu, zálohy kanálů atd [82]. Není nutné používat toto prostředí, pokud si uživatel přeje ovládat svůj uzel přes jinou např. mobilní aplikaci jako Zap, BlueWallet atd.



Obrázek 18 Prostředí Ride The Lightning

Electrum Server

Electrum Server je aplikace, která je také dostupná ve free verzi. Poskytuje možnost používání obyčejné Bitcoin peněženky. Používání Electrum Serveru má ale výhodu v tom, že daná peněženka (např. mobilní) používá pouze uzel, který běží na zařízení s myNode. Všechny transakce se ověřují pouze a jenom na vlastním serveru. To zajišťuje nadstandartní soukromí [83].

BTCPay Server

Jednou z velkých výhod premium verze myNode je BTCPay server. Samotný BTCPay Server je open-source projekt, který je zdarma, ale jeho používání v rámci myNode je omezeno pouze na premium verzi [69] [84].

BTCPay Server je platební brána, která umožňuje generovat příkazy pro platbu. Lze ji například implementovat do eshopu a následně si nechat platit v Bitcoinu. Výhodou je, že poskytovatel platební brány je sám uživatel, a proto se neplatí žádné poplatky provozovateli platební brány. BTCPay server dokáže generovat platby podle aktuální ceny Bitcoinu a podporuje i platbu v Lightning Network. Jedná se o vyspělou platební bránu, která poskytuje široké možnosti [84].

LND Hub

LND Hub je řešení pro Lightning peněženku BlueWallet, která sama o sobě neposkytuje možnost otevírání kanálů. Všechny kanály otevírá a zavírá provozovatel peněženky BlueWallet. Tím je dosaženo lepší uživatelské zkušenosti. LND Hub umožňuje spravovat vlastní uzel, který je napojený na uzel od BlueWallet. Následně je možné, aby se jiní uživatelé připojili na uzel provozovatele myNode a mohou posílat transakce přes kanály, které má otevřené provozovatel uzlu BlueWallet. Nevýhodou je poskytování dostatečné likvidity pro všechny uživatele, kteří jsou napojení na uzel myNode. Jinak by se mohlo stát, že by platba nemusela být uskutečněna [69] [70] [85].

RPC Explorer

Velmi užitečnou aplikací je RPC Explorer. Jde o obyčejný prohlížeč blockchainu a je dostupný ve free verzi. Díky němu je možné prohlížet všechny transakce, které se na bitcoinové síti staly. Explorer využívá faktu, že balík myNode provozuje full node, a tím pádem má lokálně k dispozici celý blockchain, který se aktualizuje podle toho, jak jsou těženy nové bloky [69] [86].

Díky Exploreru není nutné důvěřovat službám, které prohlížeč blockchainu taky nabízí, ale je možné prohlížet blockchain lokálně přímo ze zařízení myNode. Nevýhodou je menší rychlost vyhledávání a prohlížení, což je dáno výkonem zařízení, na kterém se balík myNode provozuje [69] [86].

Dojo a Whirlpool

Dojo a Whirlpool jsou aplikace zaměřené na soukromí uživatele Bitcoinu. Whirlpool poskytuje tzv. „mixování“ mincí. V podstatě se jedná o službu, která dokáže anonymizovat transakce. Transakce v bitcoinové síti jsou všechny transparentní a při identifikaci adresy se anonymita ztrácí. Mixování dokáže mince přenést přes řadu transakcí a tím zmátnout někoho, kdo by se snažil transakce identifikovat. Pro maximální soukromí je potřeba využívat i Dojo, jelikož samotný Whirlpool neposkytuje maximální soukromí [85].

Mempool

Prohlížeč mempool slouží podobně jako Explorer k sledování transakcí. Jedná se o prémiovou funkci, díky ní lze zjistit, kde se transakce, kterou uživatel chce vyhledat, nachází. Nabízí podobnou funkcionalitu jako webový prohlížeč blockchainu dostupný na URL adrese „mempool.space“. Na tomto webu je možné sledovat aktuální vytížení

mempoolu, aktuální poplatky na blockchainu, a navíc web poskytuje plnohodnotný prohlížeč blockchainu [69] [87].

Uživatel může díky aplikaci Mempool zjistit výši poplatku, kterou má zvolit pro svou transakci nebo například prohlížet poplatky v předchozích blocích. Mimoto ukazuje těžbu bloků v reálném čase [87].

Caravan

Caravan je prémiová aplikace, která má za cíl usnadnit správu multisig peněženek. Samotný Caravan nespravuje privátní klíče, ale pouze poskytuje rozhraní pro snadnou útratu mincí na multisig adresách [69] [88].

Specter

Podobně jako Caravan se i Specter snaží o snadnou správu prostředků na multisig adresách. Specter dokáže také využívat benefitů full nodu. Oproti Caravan nabízí o něco lepší uživatelské rozhraní a širší možnosti. Jedná se o prémiovou funkci [69] [89].

LNbits

LNbits je další Lightning peněženka, která nabízí možnost správy více Lightning peněženek najednou. Zajímavá je možnost fungování jako jednoduchá platební brána pro prodej lístků na událost. LNbits dokonce nabízí provoz Lightning Network uzlu jako pokladny. Prodavač může vložit údaje o platbě například v českých korunách a systém vygeneruje Lightning fakturu, která může být ihned proplacena kupujícím [90].

LNBits toho umí daleko více, ale užívání je zatíženo prémiovou verzí myNode. Mimo implementaci v myNode je projekt open-source [69].

Thunderhub

Podobně jako Ride The Lightning nabízí Thunderhub možnost správy vlastního Lightning uzlu. Uživatelské rozhraní je velmi intuitivní a jednoduché. Thunderhub umí reprezentovat události na uzlu ve formě grafů a také zaznamenává transakce, které byly routovány přes Lightning uzel [91].

Implementace v myNode je zatížena prémiovou licencí, jinak je projekt open-source a k dispozici v jiných balíčkách jako RasbiBlitz, Umbrel nebo BTCPay Server. [69] [91]

VPN

Pro vzdálený přístup do uzlu obsahuje balíček myNode i VPN (Virtual Private Network). VPN je řešena implementací OpenVPN, díky níž lze přistoupit k uzlu a ovládat ho kdekoliv na světě, i když se uživatel nachází mimo lokální síť, ve které se uzel nachází [69].

Tor

K podobnému účelu jako VPN slouží i Tor. Pomocí něj je možné se taktéž připojit k uzlu, když se uživatel nachází mimo síť uzlu [69]. Výhodou je, že komunikace po síti Tor je automaticky šifrována. To znamená, že je přístup k uzlu bezpečný i například na veřejných Wi-Fi. Tor k přístupu používá tzv. „onion URL“, což je speciální URL adresa, která provádí přenos dat pouze přes Tor síť [81].

7.3.4 Vytvoření platebního kanálu

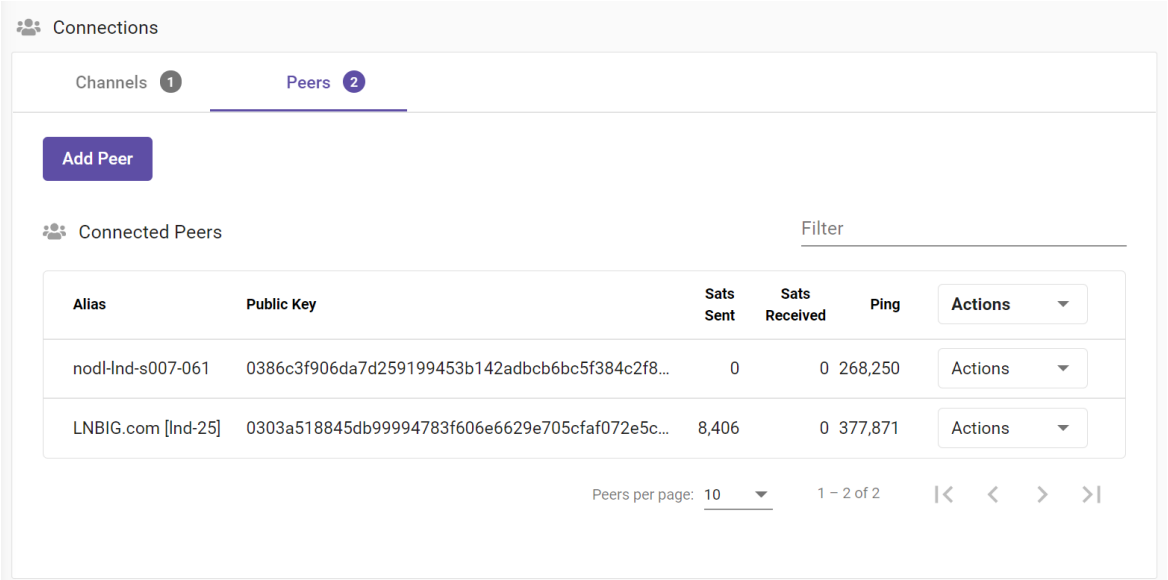
K vytvoření platebního kanálu je třeba získat veřejný klíč Lightning uzlu, díky němuž je možné navázat spojení s jiným uzlem a následně i otevřít platební kanál. Předpokladem pro vytvoření kanálu je dostatečný zůstatek na Lightning peněžence uzlu [92].

Pokud uživatel neví, ke kterému uzlu se má připojit, může použít služby, které indexují Lightning uzly jako např. „1ml.com“. Tato služba poskytuje informace o tom, kolik je aktuálně uzlů v Lightning Network, celkovou kapacitu kanálů, počet platebních kanálů a kapacitu jednotlivých kanálů. Kromě toho služba indexuje uzly s největší kapacitou nebo největším počtem kanálů. Tato informace může přijít vhod, když je potřeba vytvořit platební kanál [93].

Tím, že se uzel připojí na jiný uzel s velkým počtem kanálů, se zvyšuje šance, že platba pomocí Lightning Network projde přes více platebních kanálů k cílovému uzlu. Pokud by uzel, na který se uživatel připojí, neměl otevřené téměř žádné kanály, existuje velké riziko, že nebude moct provádět transakce skrz celou Lightning Network.

Po zvolení uzlu, ke kterému se chce uživatel připojit, je nutné použít prostředí nebo příkazový řádek k provedení propojení uzlů. V případě uzlu myNode, lze použít aplikaci Ride The Lightning. Po přidání uzlu jako peeru se uzly navzájem vidí a komunikují [93].

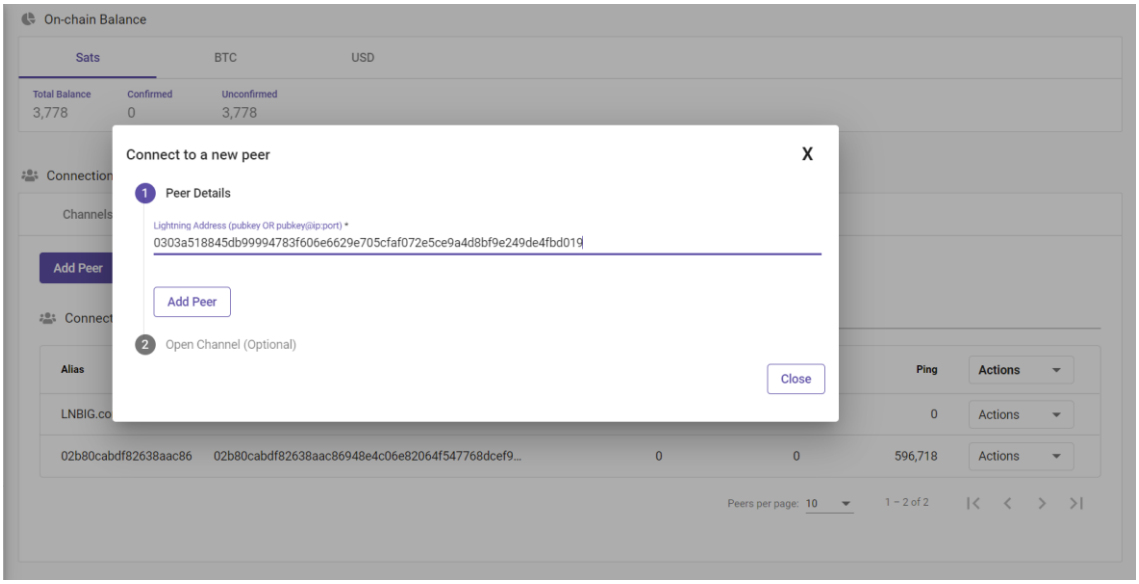
Uzel se snaží připojit k ostatním uzlům v Lightning Network sám. Proto lze vidět v tabulce peerů další uzly (viz. *Obrázek 19 Zobrazení připojených peerů v RTL*), které se sami od sebe napojily. V případě, že se chce uživatel připojit ke konkrétnímu uzlu, který nemá mezi peery, musí jej explicitně přidat mezi peery.



Obrázek 19 Zobrazení připojených peerů v RTL

Po přidání mezi peery nabídne prostředí Ride The Lightning vytvoření kanálu. Není nutné rovnou otvírat kanál, pokud si tak uživatel nepřeje. *Obrázek 20 Připojování k peerům v Ride The Lightning* znázorňuje, jak probíhá připojování k dalšímu uzlu v síti LN.

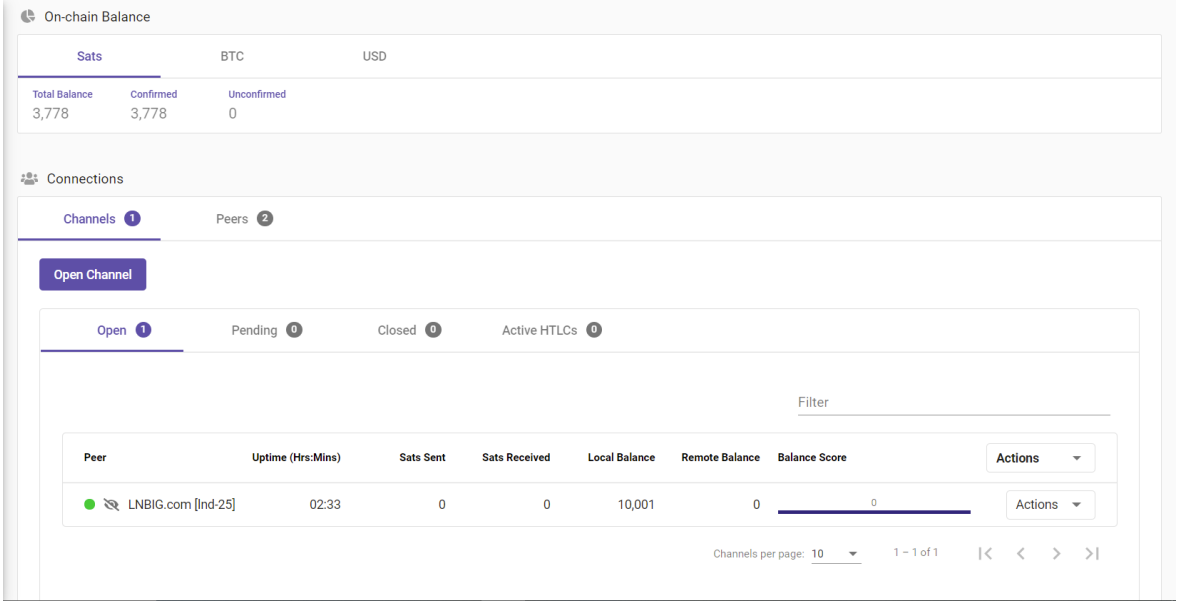
Jelikož vytvoření platebního kanálu vyžaduje zapsání transakce na blockchain, transakce je zatížená poplatkem, proto je vhodné upravit výši poplatku pro transakci, která otevírá kanál.



Obrázek 20 Připojování k peerům v Ride The Lightning

Prostředí nabízí možnost úpravy výši poplatku pro vytvoření kanálu a zkušenější uživatelé mohou využít chvíle, kdy je mempool prázdný a ušetřit na poplatcích [93].

Po otevření kanálu je nutné počkat na schválení z druhé strany. Uzly nemají důvod zamítat otevření kanálu, pokud do něj sami nevkládají prostředky. Při schválení žádosti o otevření kanálu se změní stav kanálu z „Pending“ na „Active“.



Obrázek 21 Zobrazení aktivních kanálů v Ride The Lightning

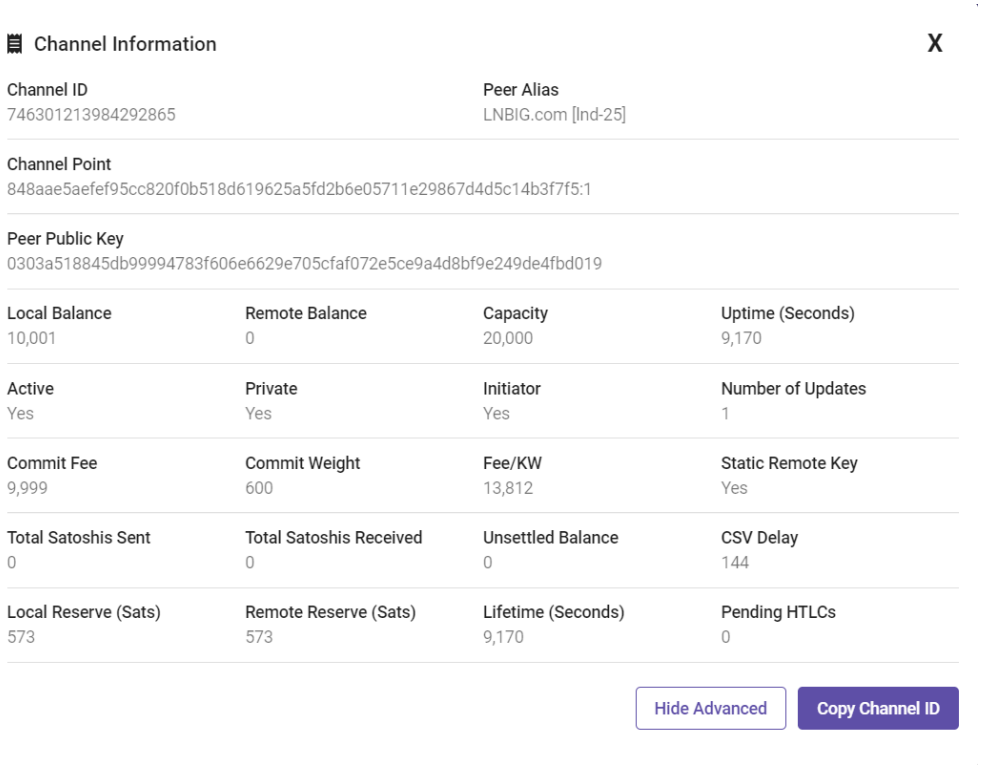
V tuto chvíli už lze kanál plně využívat k placení v rámci Lightning Network. Existuje možnost vytvořit kanál jako soukromý, což zabraňuje ostatním účastníkům sítě možnost routovat transakce přes tento kanál. Soukromý kanál je vhodný pro uživatele, kteří nechtějí, aby ostatní účastníci měli informaci o existenci kanálu [94].

Prostředí zobrazuje užitečné informace o jednotlivých kanálech tak, aby používání bylo jednoduché. Tabulku se seznamem kanálu zobrazuje *Obrázek 21 Zobrazení aktivních kanálů v Ride The Lightning*. U každého kanálu ukazuje „Local Balance“ a „Remote Balance“. Local balance značí, kolik je možné odeslat v rámci kanálu z vlastní strany. Naopak Remote balance značí, kolik prostředků může vlastní uzel přijmout v rámci kanálu, a to je velice důležité. Kdyby Remote balance byla malá, tak by přes tento kanál nebylo možné přijmout více prostředků, než je právě Remote balance [92].

7.3.5 Podrobné informace o kanálu

Když je kanál vytvořen, je možné zobrazit všechny podrobné informace o kanálu.

Jednotlivé kanály jsou identifikovány pomocí ID kanálu, což je dlouhé identifikační číslo - např. *Obrázek 22 Zobrazení detailních informací kanálu*. Samotný uzel, se kterým je kanál otevřen, má tzv. „alias“. Jedná se o přezdívku uzlu, kterou si může každý uzel libovolně nastavit. K připojení se používá veřejný klíč uzlu, jak bylo popsáno v kapitole 7.3.4 Vytvoření platebního kanálu.



Obrázek 22 Zobrazení detailních informací kanálu

Lze nalézt informaci o tom, jak dlouho kanál existuje, zda je aktivní, privátní nebo kdo byl iniciátor k otevření kanálu.

Důležitou informací je tzv. „commit fee“, což je poplatek za zavření kanálu. Poplatek se odečte od prostředků uzamknutých v kanálu a nedá se v rámci kanálu použít. Poplatek je rezervován pro případ, že by jedna ze stran chtěla „hrubou silou“ zavřít kanál. Uzavření hrubou silou se nazývá jako „force close“. Opakem násilného uzavření je „cooperative close“ [55] [92].

Při násilném uzavření kanálu není možnost zvolit výši poplatku k settlement transakci, která se musí zapsat na blockchain, proto je výše prostředků rezervována jako commit fee. Při kooperativním uzavření kanálu se mohou obě strany dohodnout na výši poplatku pro uzavření kanálu a tím ušetřit na poplatcích [55].

V poslední řadě lze nalézt informaci o tom, kolik transakcí bylo v rámci kanálu provedeno nebo kolik je neproplacených HTLC faktur. Pokud by uživatele zajímala výdělečnost

vzhledem k routování plateb od ostatních účastníků LN, tak je v prostředí možné nalézt informaci označovanou jako „Fee/KW“. Číselná hodnota Fee/KW značí, kolik si uzel účtuje satoshi za přesměrování platby za každých 1000 bajtů velikosti transakce [95].

7.3.6 Provedení Lightning transakce

Po úspěšném otevření kanálu lze konečně odeslat Lightning transakci v rámci sítě. Pro odeslání transakce je nutné, aby příjemce platby vygeneroval platební fakturu. Po vygenerování ji libovolným komunikačním kanálem odešle plátci.

Jako příklad je uvedeno, jak se odesílá platba z myNode na Lightning peněženku vytvořenou pomocí aplikace BlueWallet. Plátce musí buď naskenovat LN fakturu, která je pro pohodlné používání zakódována jako QR kód (viz. *Obrázek 23 Vytvořená LN faktura v peněžence BlueWallet*), anebo může vložit rovnou platební řetězec. Je to právě platební řetězec, který je zakódován do QR kódu.

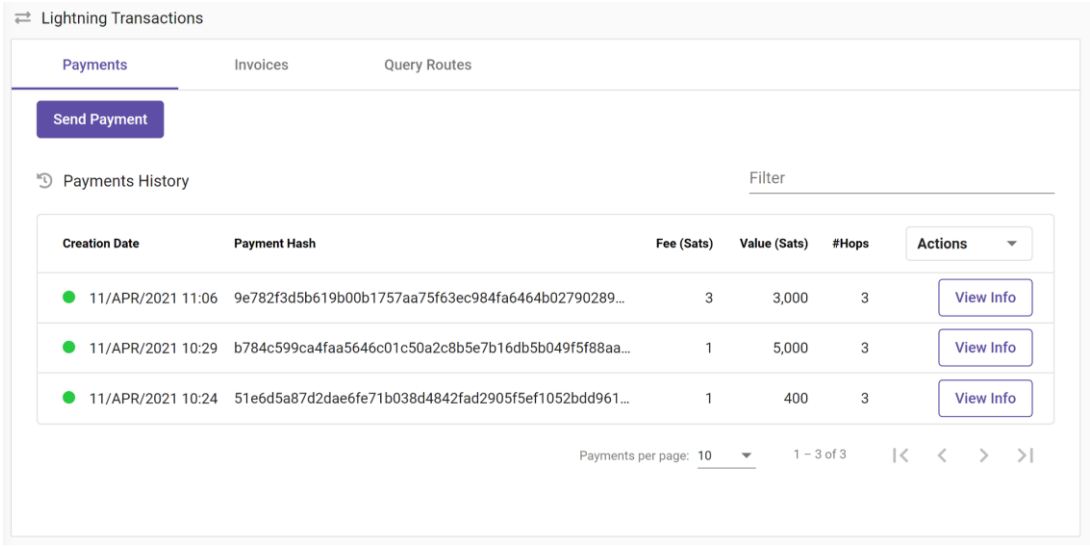
Obrázek 23 Vytvořená LN faktura v peněžence BlueWallet

V případě, že jsou všechny náležitosti platby splněny, jako například dostatečný zůstatek, existence platebních kanálů mezi odesílatelem a příjemcem, je platba provedena. Platba dorazí v rámci sekund a poplatek za transakci se liší podle toho, přes kolik platebních uzlů

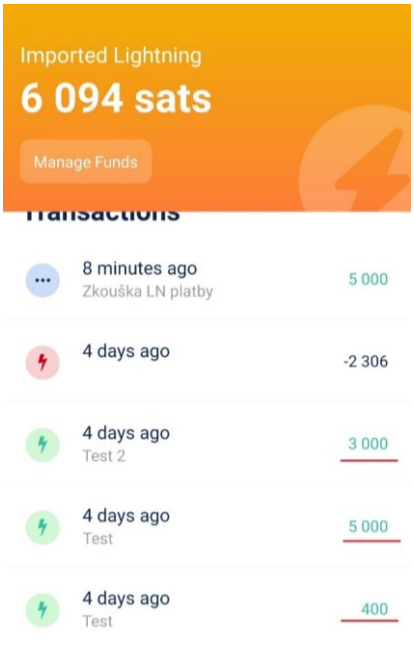
transakce musí putovat. Každý uzel si bere za routování platby malý poplatek. Kdyby byl otevřen platební kanál přímo mezi odesílatelem a příjemcem, poplatek by byl nulový [55].

V našem případě (viz. *Obrázek 25 Přehled LN transakcí v RTL prostředí*) byl poplatek za platbu při provedení tří zkušebních plateb v rozmezí 1–3 satoshi. To při dnešním kurzu ceny Bitcoinu (únor 2021) odpovídá přibližně 1,4 až 4,1 haléřům za transakci.

V prostředí RTL je následně možné zobrazit historii všech provedených plateb. U každé platby je možnost si zobrazit detailní informace, např. lze zjistit přes jaké uzly platba proběhla, přes kolik uzlů platba putovala a také informaci o tom, jaká byla výše poplatku za platbu.



Obrázek 25 Přehled LN transakcí v RTL prostředí



Obrázek 24 Přijaté transakce v peněžence BlueWallet

Přehled přijatých plateb jde samozřejmě nalézt i v aplikaci BlueWallet (*Obrázek 24 Přijaté transakce v peněžence BlueWallet*), kam LN platba směřovala.

7.4 Ekonomické a energetické hledisko provozu uzlu

Díky tomu, že je uzel provozován na minipočítači, je energetická náročnost systému velmi malá. Samotné Raspberry Pi 4 spotřebuje při zátěží kolem 8 Wattů [96].

V případě, že by minipočítač byl celých 365 dní v maximální zátěží, znamenalo by to spotřebování 70,08 kWh energie za rok. To při předpokládané ceně elektřiny 4 Kč/kWh znamenalo, že počítač Raspberry Pi 4 spotřebuje elektrickou energii v hodnotě 230,32 Kč za rok.

Minipočítač ovšem nevyužívá většinu času procesor na maximální výkon. Nejvíce elektrické energie spotřebuje při stahování, kopírování a indexování blockchainu na disk. Následný provoz už není tak energeticky náročný. Počítač sice stahuje a aktualizuje blockchain na disku, tak jak jsou těženy nové bloky, ale jedná se pouze o jednotky MB, které se musí zapsat během hodiny na disk. Proto lze přepokládat, že spotřeba elektrické energie bude ve výsledku mnohem menší. Při vlastním měření pomocí Wattmetru EMOS FHT 9999, vykazoval počítač se zapojeným SSD při obyčejném provozu spotřebu 6 Wattů. Při tomto vytížení by počítač spotřeboval elektrickou energii v hodnotě 210,- Kč za rok.

Nízká spotřeba energie je jeden z hlavních důvodu, proč jsou uzly provozovány na SBC. Provoz uzlu na standardním stolním počítači nebo notebooku by byl mnohonásobně dražší. Ve vlastním měření vykazoval moderní stolní počítač s procesorem AMD Ryzen 3600X a grafickou kartou AMD RX 470 8 GB spotřebu v klidovém stavu podle Wattmetru EMOS FHT 9999, 70 Wattů. Provoz takového počítače by za rok stál při cenně elektrické energie 4 Kč/kWh, 2453,- Kč. Výhodou je i pořizovací cena jednodeskového počítače. Například Raspberry Pi 4 je k dnešnímu datu (22. 2. 2021) možné pořídit přibližně za 1 500,- Kč[4] [72].

Jelikož počítač figuruje jako uzel v síti Lightning Network, může na sebe vydělávat tím, že směřuje transakce přes platební kanály, které navázal s jinými uzly. V kapitole 7.3.6 Provedení Lightning transakce je uvedeno, že v případě transakce, která putovala přes 3 uzly, byl poplatek 1-3 satoshi. Poplatek se může u každého uzlu výrazně lišit. Předpokládejme situaci, kdy je poplatek za přesměrování transakce 1 satoshi.

[4] E-shop nabízející Raspberry Pi 4: Raspberry Pi 4 Model B 4 GB RAM (rpishop.cz)

To by znamenalo, že při přesměrování 10 000 transakcí uzel vydělá 10 000 satoshi. To při dnešním kurzu (únor 2021) znamená výdělek přibližně 136,- Kč. 10 000 transakcí je ovšem dost velké číslo. Znamenalo by to otevření několika desítek kanálů. Každé otevření kanálů je zatíženo nutností zapsat transakci na blockchain a transakce na blockchainu jsou poměrně drahé (dle vytížení sítě může být poplatek za transakci od 10,- do 200,- Kč). Na druhou stranu je pro otevření mnoha kanálů potřeba, ať je navázáno dostatek platebních cest, které ostatní uživatelé LN mohou použít pro provedení svojí platby, a navíc je nutné zásobit všechny kanály dostatečnou likviditou pro provedení transakce. Likviditou je v tomto případě míněno local balance, která je popsána v kapitole 7.3.4 Vytvoření platebního kanálu. Otevření vysokého počtu kanálu a zároveň zásobení likviditou všech kanálů by znamenalo zamknutí prostředků v řádech deseti tisíců korun v platebních kanálech. Některé uzly totiž vyžadují minimální částku v Bitcoinu při otevření kanálu, tak aby kanál zajišťoval dostatečnou likviditu a byl dostatečné kvalitní pro ostatní účastníky sítě.

Můžeme si reálnou situaci namodelovat. Uvažujme příklad, kdy by náš uzel vytvořil aspoň 20 platebních kanálů tak, aby zajistil dobré platební cesty a procházely přes něj transakce, z kterých si budeme moct vzít poplatek. Pro poskytnutí dostatečné likvidity uzavřeme do každého z kanálu 0,01 BTC a předpokládejme, že protější uzel do kanálu také uzavře nějaké prostředky, tak aby transakce mohly procházet skrz kanál oběma směry. To znamená, že musíme uzamknout celkem 0,2 BTC do kanálů. Ignorujme nyní skutečnost, že některé uzly by vyžadovaly uzamknutí více prostředků, některé uzly totiž požadují k uzamknutí i 0,1 BTC, přesto většině velkým uzlům stačí zmíněných 0,01 BTC [93]. Je žádoucí, abychom vytvářeli kanály s největšími uzly, protože tím zvýšíme pravděpodobnost, že transakce bude putovat přes náš uzel a můžeme z takové transakce získat poplatek za přesměrování.

Zamknutí 0,2 BTC do kanálů znamená k dnešnímu kurzu 960 525,- Kč (únor 2021) zajištění prostředků v hodnotě 192 105,- Kč. Poté je možné v rámci kanálů přesměrovávat transakce a získávat z nich malé poplatky. Poplatek za přesměrování platby se skládá ze dvou částí nazývanou jako „base fee“, ta bývá zpravidla 1 satoshi a „fee rate“, která se uzel od uzlu liší. Fee rate značí, kolik si uzel bere z částky procent jako poplatek za přesměrování a pohybuje se u populárních uzlů od 0,0001 % až 0,1 % z transakční částky [93].

Můžeme nastavit poplatek stejný jako na jednom z největších uzlů od společnosti ACINQ, která stojí za vytvořením jedné z Lightning Network implementací s názvem Eclair, tedy

0,0055 % [93]. Je vhodné nenastavovat fee rate moc vysoko, abychom neodradili ostatní účastníky sítě od přesměrování platby přes náš uzel.

Ostatní provozovatelé LN uzlů vykazují, že s výrazně méně než 30 otevřenými kanály dokázali přesměrovat téměř 500 plateb za měsíc [97]. Pokud bychom uvažovali, že v našem případě, kdy máme 20 otevřených kanálů, přesměrujeme 1 000 plateb za měsíc o průměrné hodnotě jedné platby 100,- Kč, znamená to, že bychom přesměrovali za jeden měsíc platby v hodnotě 100 000,- Kč. Získané poplatky z fee rate by byly 5,50 Kč a z fee base 1000 satoshi, což je při dnešním kurzu Bitcoinu 960 525,- Kč (únor 2021) v přepočtu 9,60 Kč. Dohromady jsme z obou poplatků získali za měsíc 15,10 Kč, a pokud bychom přesměrovali stejné množství transakcí všechny další měsíce v roce, získali bychom při stejném kurzu Bitcoinu 181,- Kč za celý rok. To je částka, která sotva postačí na zaplacení elektrické energie, kterou Raspberry Pi za rok spotřebuje (viz. 7.4 Ekonomické a energetické hledisko provozu uzlu).

Pokud bychom ovšem fee rate zvýšili na 1 % (i uzly s tak vysokými poplatky existují), získali bychom z fee rate 1 000,- Kč a 9,60 Kč z fee base (viz. *Tabulka 5 Výdělky z přesměrování transakcí*). Dohromady tedy 1009,60 Kč za měsíc, což znamená získání poplatků v hodnotě 12 115,- Kč za rok při kurzu Bitcoinu 960 525,- Kč. To už je částka, která pokryje i pořizovací náklady Raspberry Pi 4 [72]. Je třeba mít na paměti, že by počet přesměrovaných transakcí byl při vyšším fee rate nejspíše menší.

Tabulka 5 Výdělky z přesměrování transakcí

Předpokládaný kurz za 1 BTC:	960 525 Kč
Hodnota jedné přesměrované transakce:	100 Kč

Počet přesměrovaných transakcí za měsíc	**Fee rate**	**Fee base [Satoshi/transakce]**	**Výdělek z fee rate**	**Výdělek z fee base [Satoshi]**	**Celkový měsíční výdělek**
1000	0,0055 %	1	5,50 Kč	1000	15,10 Kč
1000	0,1000 %	1	100,00 Kč	1000	109,60 Kč
1000	1,00 %	1	1 000,00 Kč	1000	1 009,60 Kč

Při nastavení vyšších poplatků za přesměrování platby se sice dá vydělat i řádově nízké deseti tisíce korun za rok, přesto výdělek zdaleka nestačí na to, aby pokryl uzamčené prostředky v kanálech, a to ani při několikaletém provozu uzlu.

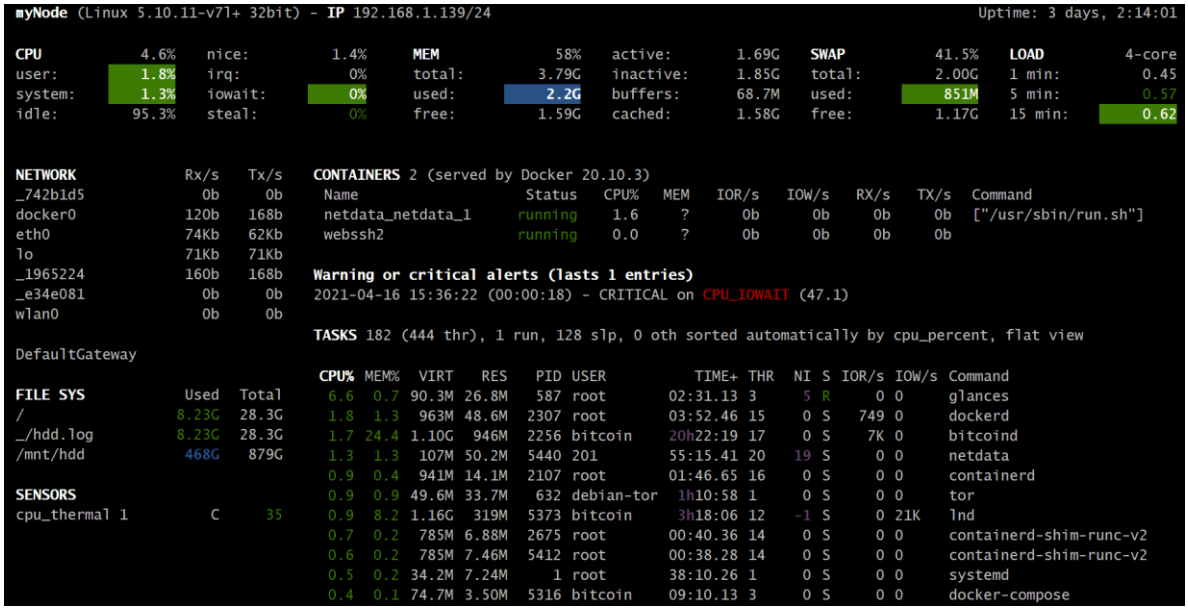
Z toho důvodu se provoz LN uzlu pro výdělek nejeví jako optimální řešení. Uzel je vhodné řešení pro firmy, obchody nebo veřejné osoby, které chtějí nabídnou svým zákazníkům levné a velmi rychlé platby v Bitcoinu. Díky cenové dostupnosti je toto řešení vhodné i pro subjekty s malými finančními možnostmi.

Výhodou takových plateb je osvobození od poplatků platebních bran, které si za zprostředkování plateb účtují malá procenta z převedené částky. Nevýhodou může být větší cenová volatilita Bitcoinu, což může být pro některé subjekty nevhodné.

7.5 Správa a analýza uzlu myNode

Balíček myNode obsahuje několik nástrojů pro sledování stavu a případnou správu uzlu. V nastavení se nachází nástroj Glances, do kterého se lze dostat kliknutím na „Open Glances“ z přehledu zařízení (to je k nalezení ve spodní liště v hlavním menu pod tlačítkem „Status“). Systém nás přesměruje do aplikace Glances.

Glances je monitorovací nástroj napsaný v programovacím jazyce Python a dokáže zobrazit velmi detailní informace o stavu počítače. Zobrazuje data o době běhu počítače, použitém operačním systému, využití operační paměti, swapu, procesoru, kapacity disků podle připojených diskových jednotek, teplotu na procesoru, využití podle běžících procesů,

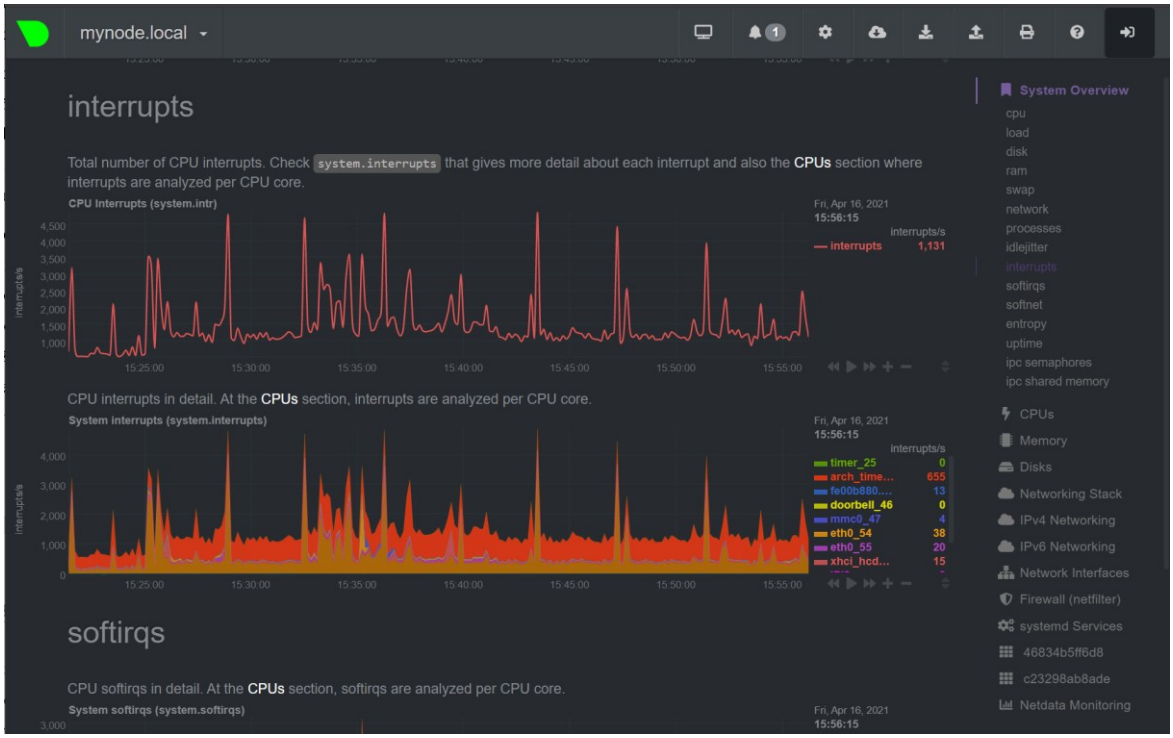


Obrázek 26 Informační přehled nástroje Glances

běžících Docker kontejnerů, kritických chybách a mnoho dalších informací. Všechny informace, které Glances poskytuje, ukazuje *Obrázek 26 Informační přehled nástroje Glances* [98].

Nástroj může být vhodný pro uživatele, který potřebuje ověřit, zda nějaký proces příliš nevytěžuje procesor nebo jestli proces komunikuje po síti. Obecně je vhodný spíše pro vývojáře a pokročilé uživatele, protože všechny informace jsou zobrazeny v „terminálové“ podobě.

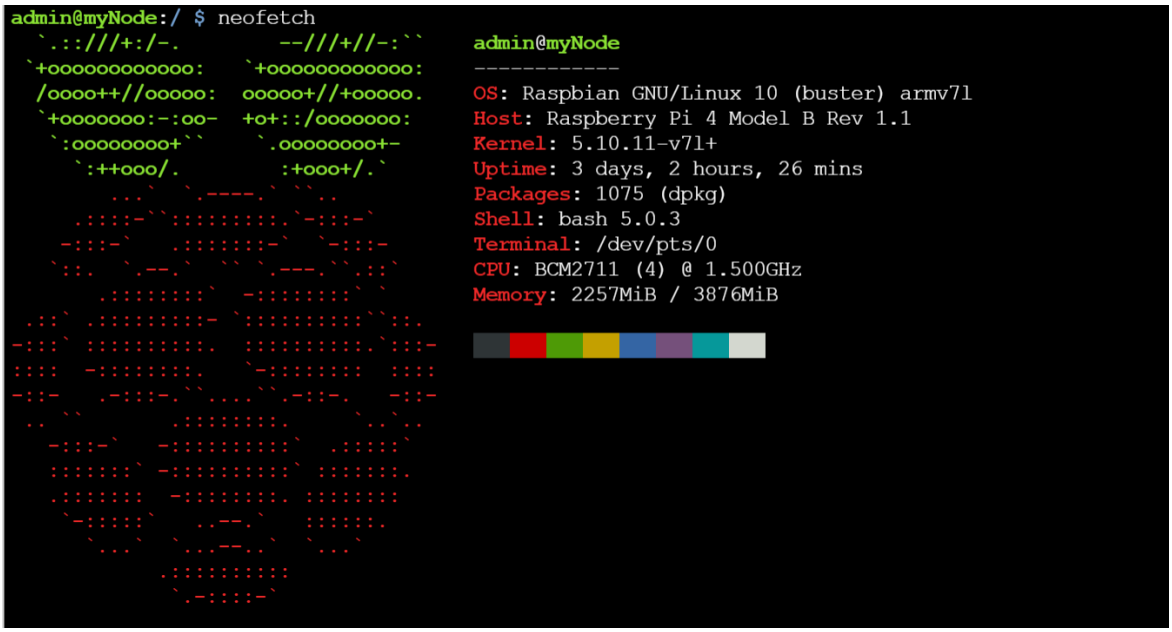
Podobnou úlohu jako Glances se snaží splnit nástroj Netdata. Ten poskytuje mnohem více detailních informací jako například přerušení procesoru a změnu kontextu. Na rozdíl od Glances zobrazuje Netdata všechny data v grafické podobě ve formě grafů. Grafů je několik desítek a jsou rozumně rozdělené podle kategorií v menu (viz. *Obrázek 27 Informační přehled nástroje Netdata*) [99]. Netdata je nutné povolit v nastavení myNode, poté je možné aplikaci spustit a používat.



Obrázek 27 Informační přehled nástroje Netdata

Jelikož je celý balíček myNode postavený na operačním systému Raspbian, což je linuxový operační systém určený pro zařízení Raspberry, dovoluje myNode vstup přes nastavení do terminálu. V terminálu fungují klasické linuxové příkazy, přičemž terminál je vhodný opět pro vývojáře a zkušené uživatele. Po instalaci nástroje „neofetch“, který zobrazuje detaily

linuxové distribuce a systému, na kterém je distribuce nainstalovaná, je možné použít příkaz neofetch pro zobrazení informací (viz. *Obrázek 28 Linuxový terminál na myNode*).



Obrázek 28 Linuxový terminál na myNode

ZÁVĚR

I přesto, že Bitcoin stojí na solidních technických základech a důvěra v něj se za poslední roky výrazně zvýšila, jsou investice do něj stále rizikové. Trh s kryptoměnami je mladý a každý den se objeví nové projekty, které lákají na pohádkové zhodnocení investic. Navíc neexistují regulace, které by zabraňovaly manipulacím trhu v masivním měřítku.

Je třeba být opatrný. Příčky prvních kryptoměn podle tržní kapitalizace se velmi výrazně mění podle aktuálních trendů. Některé kryptoměny mohou přinést svým investorům velké zhodnocení, ale stejně rychle může cena těchto kryptoměn směřovat dolů.

V posledních letech se začíná měnit i vnímaní samotného Bitcoinu. Místo vnímaní Bitcoinu jako prostředku směny, se objevují názory, že by Bitcoin měl být vnímám jako uchovatel hodnoty nebo dokonce jako „digitální zlato“. Pojmenování digitální zlato může znít úsměvně, ale když vezmeme v potaz fakt, že Bitcoinu je omezené množství a v dlouhodobém horizontu si Bitcoin vždy udržel svoji hodnotu, nezní to již tak nerealisticky.

Vnímaní Bitcoinu jako udržitele hodnoty nahrává fakt, že především poslední měsíce lze pozorovat masivní tištění peněz, které v budoucnu může zvýšit míru inflace. Jen za období únor 2020 až únor 2021 se podle agregátu M2 navýšilo množství dolarů v oběhu o více než 20 % [100]. Někteří si tenhle fakt uvědomují a snaží se najít pomyslný bezpečný přístav, ve kterém se jejich vydělané peníze nebudou znehodnocovat.

Za dobu existence Bitcoinu se rapidně zvýšila bezpečnost sítě, která je reflektována hashratem. Se zvyšujícím se hashratem se zvyšuje i elektrická energie potřebná k provedení útoku na Bitcoinovou síť. V dnešní době se takový útok jeví jako skoro nereálný.

Krom zvyšující se bezpečnosti se Bitcoin zlepšuje i technologicky. Lightning Network dovoluje používat Bitcoin jako prostředek směny, což je věc, kterou kritici Bitcoinu rádi zmiňují. Používání Bitcoinu jako prostředek směny v minulosti bránily neustále se zvyšující poplatky, při kterých nedávalo smysl platit za zboží, když platba stála jako polovina hodnoty zboží nebo dokonce více. Dalším problémem bylo i čekání, než byla transakce potvrzena. Tyto problémy vyřešila nová transakční vrstva Lightning Network. Je ale třeba mít na paměti, že se jedná o zkušební provoz a technologie není zatím zcela bez chyb. Kromě Lightning Network pracují vývojáři na dalších vylepšení jako Schnorrových podpisech a Taprootu. Ty opět zvýší efektivitu a soukromí při používání Bitcoinu.

Bude zajímavé pozorovat, jak bude Bitcoin přijat státy, společnostmi a samotnými lidmi a jak lidé s technologií, která jim umožňuje bránit se proti inflaci a realizovat platby svobodně, bez třetích stran, naloží.

SEZNAM POUŽITÉ LITERATURY

[1] STRAY, KARI. Who created Bitcoin. Cointelegraph [online]. 2017, 1 [cit. 2021-3-1]. Dostupné z: https://cointelegraph.com/news/who-created-bitcoin-long-story-short

[2] ALVAREZ, JOSE. Does Satoshi have a million bitcoins? Blockonomi [online]. 2018, 4 [cit. 2021-3-1]. Dostupné z: https://blockonomi.com/who-is-satoshi-nakamoto/

[3] NAKAMOTO, Satoshi. Bitcoin White Paper [online]. 2008, 9 [cit. 2021-3-1]. Dostupné z: https://bitcoin.org/bitcoin.pdf

[4] Bitcoin Github [online]. 2008 [cit. 2021-3-1]. Dostupné z: https://github.com/bitcoin/bitcoin

[5] Bitcoin pizza transaction. Blockchain: Explorer [online]. 2010 [cit. 2021-3-1]. Dostupné z: https://www.blockchain.com/btc/tx/a1075db55d416d3ca199f55b6084e2115b9345e16c5cf302fc80e9d5fbf5d48d

[6] BTCNN. Most Famous Bitcoin Transactions Since its Creation. Btcnn.com [online]. btcnn, 2019, 1 [cit. 2021-3-1]. Dostupné z: https://www.btcnn.com/most-famous-bitcoin-transactions-since-its-creation

[7] CAMPBELL, Scott. Bitcoin exchange MtGox 'faced 150,000 hack attacks every second'. The Telegraph [online]. 2014, 9. 3. 2014, 2 [cit. 2021-3-1]. Dostupné z: https://www.telegraph.co.uk/finance/currency/10686698/Bitcoin-exchange-MtGox-faced-150000-hack-attacks-every-second.html

[8] POLLOCK, Darryn. The Mess That Was Mt. Gox: Four Years On. Cointelegraph [online]. 2018, 9. 3. 2018, 2 [cit. 2021-3-1]. Dostupné z: https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-onchange-MtGox-faced-150000-hack-attacks-every-second.html

[9] Burzy kryptoměn. E15 [online]. 2019, 28. 2. 2019, 1 [cit. 2021-3-1]. Dostupné z: https://www.e15.cz/burza-kryptomen

[10] AGRAWAL, Harsh. Bitcoin Payment Gateways. Coinsutra [online]. 2019, 4 [cit. 2021-3-1]. Dostupné z: https://coinsutra.com/bitcoin-payment-gateways-merchants/

[11] V Alze nyní zaplatíte i Bitcoiny. Alza [online]. 2017 [cit. 2021-3-1]. Dostupné z: https://www.alza.cz/platba-bitcoiny-a-btc-automaty-alza

[12] Alza.cz zavádí prodej kryptoměn ve svých platebních terminálech. Alza [online]. Praha, 2018, 27. 6. 2018 [cit. 2021-3-1]. Dostupné z: https://www.alza.cz/alzacz-zavadi-prodej-kryptomen-ve-svych-platebnich-terminalech

[13] Kryptotank [online]. Praha [cit. 2021-3-1]. Dostupné z: https://kryptotank.cz/

[14] D. COOK, John. Bitcoin key mechanism and elliptic curves over finite fields [online]. 2018, 14. 9. 2018, 1 [cit. 2021-3-1]. Dostupné z: https://www.johndcook.com/blog/2018/08/14/bitcoin-elliptic-curves/

[15] DAS, Ravi. The Mathematical Algorithms of Asymmetric Cryptography and an Introduction to Public Key Infrastructure [online]. 2017, 3. 2. 2017, 2 [cit. 2021-3-1]. Dostupné z: https://resources.infosecinstitute.com/certification/mathematical-algorithms-asymmetric-cryptography-introduction-public-key-infrastructure/

[16] STROUKAL, Dominik a Jan SKALICKÝ. Bitcoin: peníze budoucnosti : historie a ekonomie kryptoměn, stručná příručka pro úplné začátečníky. 2. Praha: Ludwig von Mises institute CZ&SK, 2015. ISBN 978-80-87733-26-4.

[17] FILLNER, Karel. JAK NA BITCOIN [online]. 2. 2014 [cit. 2021-3-4]. Dostupné z: https://btctip.cz/wp-content/uploads/2018/05/jak-na-bitcoin-karel-fillner-aktualizace.pdf

[18] NAKAMOTO, Satoshi. The Base58 Encoding Scheme [online]. 2019, 29. 11. 2019, 1 [cit. 2021-3-4]. Dostupné z: https://tools.ietf.org/id/draft-msporny-base58-01.html

[19] TORE, Tuna. How to generate a Bitcoin address — Technical address generation explanation. Hackernoon [online]. 15. 1. 2020 [cit. 2021-3-4]. Dostupné z: https://hackernoon.com/how-to-generate-bitcoin-addresses-technical-address-generation-explanation-rus3z9e

[20] ROUSE, Margaret. Asymetric cryptography. Techtarget [online]. [cit. 2021-3-4]. Dostupné z: https://searchsecurity.techtarget.com/definition/asymmetric-cryptography

[21] Exodus Wallet [online]. [cit. 2021-3-4]. Dostupné z: https://www.exodus.com/

[22] GAZDA, Adam. Bitcoin Paper Wallet – Co jsou a jak fungují papírové peněženky? Finex [online]. 2019, 17. 8. 2019, 2 [cit. 2021-3-4]. Dostupné z: https://finex.cz/bitcoin-paper-wallet-co-jsou-a-jak-funguji-papirove-penezenky/

[23] Trezor [online]. [cit. 2021-3-4]. Dostupné z: https://trezor.io/

[24] ANTONOPOULOS, Andreas M. Mastering bitcoin: programming the open blockchain. Second edition. Beijing: O'Reilly, 2017. ISBN 978-1491954386.

[25] Blockchain explorer [online]. [cit. 2021-3-4]. Dostupné z: https://www.blockchain.com/cs/explorer

[26] HERTIG, Alyssa. Bitcoin Halving, Explained. Coindesk [online]. 2020, 24. 3. 2020 [cit. 2021-3-8]. Dostupné z: https://www.coindesk.com/bitcoin-halving-explainer

[27] Bitcoin Block Half. Bitcoin Block Half [online]. [cit. 2021-3-8]. Dostupné z: https://www.bitcoinblockhalf.com/images/bitcoin-inflation-chart.png

[28] WALKER, Greg. Mining: How Does Mining Work. Learn Me Bitcoin [online]. [cit. 2021-3-8]. Dostupné z: https://learnmeabitcoin.com/technical/mining

[29] DOHERTY, Frank. The Golden Nonce. Medium [online]. 1. 2. 2019 [cit. 2021-3-8]. Dostupné z: https://fdoherty13.medium.com/the-golden-nonce-c2bac08ce208

[30] WALKER, Greg. What is Difficulty in Bitcoin? Learn Me Bitcoin [online]. [cit. 2021-3-8]. Dostupné z: https://learnmeabitcoin.com/beginners/difficulty

[31] WALKER, Greg. What is Target in Bitcoin? Learn Me Bitcoin [online]. [cit. 2021-3-8]. Dostupné z: https://learnmeabitcoin.com/technical/target

[32] WALKER, Greg. Block Header. Learn Me Bitcoin [online]. [cit. 2021-3-10]. Dostupné z: https://learnmeabitcoin.com/technical/block-header

[33] OUPICKÝ, Jan. Jak funguje Bitcoin [online]. [cit. 2021-3-10]. Dostupné z: http://www.karlin.mff.cuni.cz/~tuma/Aplikace17/Prace/btc_oupicky_oprava.pdf. Univerzita Karlova.

[34] Block hashing algorithm [online]. [cit. 2021-3-10]. Dostupné z: https://en.bitcoin.it/wiki/Block_hashing_algorithm

[35] BACZUK, Jordan. What's in a Bitcoin Block? Medium [online]. 2019, 26. 2. 2019 [cit. 2021-3-10]. Dostupné z: https://medium.com/better-programming/whats-in-a-bitcoin-block-41d0a5d1472f

[36] WALKER, Greg. Merkle tree visualization. Learn Me Bitcoin [online]. [cit. 2021-3-10]. Dostupné z: https://learnmeabitcoin.com/technical/images/merkle-root/merkle-root.png

[37] CHUMBLEY, Alex, Karleigh MOORE a Jimin KHIM. Merkle tree. Brilliant [online]. [cit. 2021-3-10]. Dostupné z: https://brilliant.org/wiki/merkle-tree/

[38] Block structure. Bitcoin.it [online]. [cit. 2021-3-10]. Dostupné z: https://en.bitcoin.it/wiki/Block

[39] FRANKEFIELD, Jake. 51% Attack Definition. Ivestopedia [online]. 6. 3. 2019, 2 [cit. 2021-3-13]. Dostupné z: https://www.investopedia.com/terms/1/51-attack.asp

[40] Antminer S19 Pro. Bitmain [online]. [cit. 2021-3-13]. Dostupné z: https://shop.bitmain.com/release/AntminerS19Pro/overview

[41] Total Hash Rate. Blockchain [online]. [cit. 2021-3-13]. Dostupné z: https://www.blockchain.com/charts/hash-rate

[42] Jaderná elektrárna Temelín. ČEZ [online]. [cit. 2021-3-13]. Dostupné z: https://www.cez.cz/cs/o-cez/vyrobni-zdroje/jaderna-energetika/jaderna-energetika-v-ceske-republice/ete

[43] History of Bitcoin Mining. Bitcoin.it [online]. [cit. 2021-3-16]. Dostupné z: https://en.bitcoin.it/wiki/Mining#History

[44] The History and Future of Bitcoin Mining. Genesis Block [online]. 2021, 3. 3. 2021 [cit. 2021-3-16]. Dostupné z: https://genesisblockhk.com/the-history-and-future-of-bitcoin-mining/

[45] How Long Does It Take to Mine One Bitcoin. CoinMarketCap [online]. 2020, 20. 9. 2020 [cit. 2021-3-16]. Dostupné z: https://coinmarketcap.com/alexandria/article/how-long-does-it-take-to-mine-one-bitcoin#toc-mining-solo-vs-mining-pool

[46] Mining Pools Share [online]. [cit. 2021-3-16]. Dostupné z: https://www.blockchain.com/pools

[47] Antminer S19j Details. Bitmain [online]. [cit. 2021-3-16]. Dostupné z: https://shop.bitmain.com/

[48] Cost of electricity over world. Global Petrol Prices [online]. 2020 [cit. 2021-3-16]. Dostupné z: https://www.globalpetrolprices.com/electricity_prices/

[49] BAYDAKOVA, Anna. Bitcoin Miners Are Heating Homes Free of Charge in Frigid Siberia: 23.8.2019. Coindesk [online]. [cit. 2021-3-16]. Dostupné z: https://www.coindesk.com/bitcoin-miners-are-heating-homes-for-free-in-frigid-siberia

[50] How Bitcoin Transactions Work. Bitcoin.org [online]. [cit. 2021-3-16]. Dostupné z: https://www.bitcoin.com/get-started/how-bitcoin-transactions-work/

[51] How Do Bitcoin Transactions Work? Coindesk [online]. 2020, 18. 9. 2020 [cit. 2021-3-16]. Dostupné z: https://www.coindesk.com/learn/bitcoin-101/how-do-bitcoin-transactions-work

[52] Block Height 250 000. Mempool Space [online]. 3.8.2013 [cit. 2021-3-16]. Dostupné z: https://mempool.space/block/00000000000003887df1f29024b06fc2200b55f8af8f35453d7be294df2d214

[53] Block Height 675 000. Mempool Space [online]. [cit. 2021-3-17]. Dostupné z: https://mempool.space/block/0000000000000000057b6df3f61f96fbdd4b9c4d76fcb975cb0e8a56577d51

[54] POON, Joseph a Thaddeus DRYJA. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments [online]. 2016, 59 [cit. 2021-3-17]. Dostupné z: https://lightning.network/lightning-network-paper.pdf

[55] ANTONOPOULOS, Andreas. Mastering the Lightning Network. Github [online]. 22.9.2019 [cit. 2021-3-17]. Dostupné z: https://github.com/lnbook/lnbook

[56] What Is a Multisig Wallet? Binance Academy [online]. 13.11.2020 [cit. 2021-3-17]. Dostupné z: https://academy.binance.com/en/articles/what-is-a-multisig-wallet

[57] WIRDUM, Aaron Van. UNDERSTANDING THE LIGHTNING NETWORK, PART 1: BUILDING A BIDIRECTIONAL BITCOIN PAYMENT CHANNEL. Bitcoin Magazine [online]. 31.3.2016, 5 [cit. 2021-3-17]. Dostupné z: https://bitcoinmagazine.com/technical/understanding-the-lightning-network-part-building-a-bidirectional-payment-channel-1464710791

[58] WIRDUM, Aaron Van. UNDERSTANDING THE LIGHTNING NETWORK, PART 2: CREATING THE NETWORK. Bitcoin Magazine [online]. 3 [cit. 2021-3-17]. Dostupné z: https://bitcoinmagazine.com/technical/understanding-the-lightning-network-part-creating-the-network-1465326903

[59] ALIEV, Magomed. Lightning network in depth, part 1: Payment channels. Medium [online]. 2018, 5.3.2018, 7 [cit. 2021-3-17]. Dostupné z: https://medium.com/softblocks/lightning-network-in-depth-part-1-payment-channels-b943607950dd

[60] ANTONOPOULOS, Andreas. A Technical Introduction to The Lightning Network [online]. 20.5.2020 [cit. 2021-3-20]. Dostupné z: https://aantonop.io/wearedevsln

[61] ALIEV, Magomed. Lightning network in depth, part 2: HTLC and payment routing. Medium [online]. 2018, 9.3.2018, 7 [cit. 2021-3-20]. Dostupné z:

https://medium.com/softblocks/lightning-network-in-depth-part-2-htlc-and-payment-routing-db46aea445a8

[62] TOWNS, Anthony. Basis of Lightning Technology (BOLT). Github [online]. [cit. 2021-3-20]. Dostupné z: https://github.com/lightningnetwork/lightning-rfc/blob/master/00-introduction.md

[63] An Overview of Lightning Network Implementations. Medium [online]. 2021, 15.3.2021 [cit. 2021-3-20]. Dostupné z: https://medium.com/@fulgur.ventures/an-overview-of-lightning-network-implementations-d670255a6cfa

[64] ACHESON, Noelle. Crypto Long & Short: How Bitcoin Development Is Evolving – And What's Behind It. Coindesk [online]. 2020, 29.11.2020, 8 [cit. 2021-3-20]. Dostupné z: https://www.coindesk.com/bitcoin-protocol-development-incentives-diversity

[65] MAJASKI, Christina. Bitcoin Unlimited Definition. Ivestopedia [online]. 2019, 5.3.2019 [cit. 2021-3-20]. Dostupné z: https://www.investopedia.com/terms/b/bitcoin-unlimited.asp

[66] ČAPEK, Jan. Segregated Witness: Co je SegWit a jak funguje. BTCtip [online]. 2017, 2.3.2017, 4 [cit. 2021-3-20]. Dostupné z: https://btctip.cz/segregated-witness-co-je-segwit-a-jak-funguje/

[67] Hards Forks and Soft Forks Explained. Binance Academy [online]. 2021, 29.4.2021 [cit. 2021-3-20]. Dostupné z: https://academy.binance.com/en/articles/hard-forks-and-soft-forks

[68] TĚTEK, Josef. Schnorrovy podpisy a Taproot: dlouho očekávané upgrady Bitcoinu se blíží! Alza [online]. 2020, 29.11.2020, 12 [cit. 2021-3-24]. Dostupné z: https://www.alza.cz/schnorrovy-podpisy-a-taproot-dlouho-ocekavane-upgrady-bitcoinu-se-blizi

[69] MyNode [online]. [cit. 2021-3-24]. Dostupné z: https://mynodebtc.com/

[70] Bluewallet: Zero Configuration Lightning Payments on Android and iOS. Ice3x [online]. 2019, 1.3.2019 [cit. 2021-3-24]. Dostupné z: https://ice3x.co.za/what-is-bluewallet/

[71] MyNode Github. Github [online]. [cit. 2021-3-24]. Dostupné z: https://github.com/mynodebtc/mynode

[72] RPishop: Raspberry Pi 4 Model B – 4GB RAM. RPishop [online]. [cit. 2021-3-24]. Dostupné z: https://rpishop.cz/raspberry-pi/1598-raspberry-pi-4-model-b-4gb-ram-765756931182.html

[73] VILLINGER, Sandro. SSD vs HDD: What's the difference? Avast [online]. 2019, 27.9.2019 [cit. 2021-3-24]. Dostupné z: https://www.avast.com/c-ssd-vs-hdd

[74] RockPro64 Specification. Pine64 [online]. [cit. 2021-3-24]. Dostupné z: https://www.pine64.org/rockpro64/

[75] JELIČ, Pavel. Thermal throttling: Co to je, jak se projevuje, a jak mu předejít? Jablíčkář [online]. 2020, 6.5.2020 [cit. 2021-3-24]. Dostupné z: https://jablickar.cz/thermal-throttling-co-to-je-jak-se-projevuje-a-jak-mu-predejit/

[76] Understanding Heat Sinks: Functions, Types, & More. Arrow [online]. 31.11.2019 [cit. 2021-3-24]. Dostupné z: https://www.arrow.com/en/research-and-events/articles/understanding-heat-sinks-functions-types-and-more

[77] Umbrel [online]. [cit. 2021-3-24]. Dostupné z: https://getumbrel.com/

[78] RasbiBolt [online]. [cit. 2021-3-24]. Dostupné z: https://stadicus.github.io/RaspiBolt/

[79] Nodl One [online]. [cit. 2021-3-24]. Dostupné z: https://www.nodl.it/nodl-one.html

[80] About Bitcoin Core. Bitcoin Core [online]. [cit. 2021-3-24]. Dostupné z: https://bitcoincore.org/en/about/

[81] Tor Project: About. Tor Project [online]. [cit. 2021-3-27]. Dostupné z: https://www.torproject.org/about/history/

[82] Ride The Lightning. Github [online]. [cit. 2021-3-27]. Dostupné z: https://github.com/Ride-The-Lightning/RTL

[83] Electrum Server Guide. MyNode [online]. [cit. 2021-3-27]. Dostupné z: https://mynodebtc.com/guide/electrum_server

[84] BTCPay Server. Github [online]. [cit. 2021-3-27]. Dostupné z: https://github.com/btcpayserver/btcpayserver#-features

[85] MIKLE, Michal. MyNode – Bitcoin a Lightning full node. Alza [online]. 2019, 1.1.2019 [cit. 2021-3-27]. Dostupné z: https://www.alza.cz/mynode-bitcoin-lightning-full-node-recenze-zkusenosti

[86] BTC RPC Explorer. Github [online]. [cit. 2021-3-27]. Dostupné z: https://github.com/janoside/btc-rpc-explorer

[87] Mempool. Github [online]. [cit. 2021-3-27]. Dostupné z: https://github.com/mempool/mempool

[88] Caravan: Bitcoin Multisig. Github [online]. [cit. 2021-3-27]. Dostupné z: https://unchained-capital.github.io/caravan/#/

[89] Specter. Github [online]. [cit. 2021-3-31]. Dostupné z: https://github.com/cryptoadvance/specter-desktop

[90] LNbits [online]. [cit. 2021-3-31]. Dostupné z: https://lnbits.org/

[91] ThunderHub [online]. [cit. 2021-3-31]. Dostupné z: https://thunderhub.io/

[92] How To Ride The Lightning! Medium [online]. 25.11.2018 [cit. 2021-3-31]. Dostupné z: https://medium.com/@suheb__/how-to-ride-the-lightning-447af999dcd2

[93] 1ML: Lightning Network Search and Analysis Engine [online]. [cit. 2021-3-31]. Dostupné z: https://1ml.com/

[94] FLOWERS, Ryan. Growth of the Bitcoin Lightning Network. Opennode [online]. 2020, 28.10.2020 [cit. 2021-3-31]. Dostupné z: https://www.opennode.com/blog/growth-of-the-bitcoin-lightning-network/

[95] BOLT #2: Peer Protocol for Channel Management. Github [online]. [cit. 2021-3-31]. Dostupné z: https://github.com/lightningnetwork/lightning-rfc/blob/master/02-peer-protocol.md#the-open_channel-message

[96] PILTCH, Avram. Raspberry Pi 4: Review, Buying Guide and How to Use. Tom'sHardware [online]. 2020, 2.4.2020 [cit. 2021-3-31]. Dostupné z: https://www.tomshardware.com/reviews/raspberry-pi-4

[97] User experience with earning satoshi by routing transaction over LN [online]. In: . [cit. 2021-3-31]. Dostupné z: https://www.reddit.com/r/lightningnetwork/comments/lb7pbk/last_month_i_collected_over_7000_sats_in_fees/

[98] Glances: An Eye on your system. Github [online]. [cit. 2021-3-31]. Dostupné z: https://nicolargo.github.io/glances/

[99] Netdata: Monitor every in real time for free with Netdata [online]. [cit. 2021-3-31]. Dostupné z: https://www.netdata.cloud/

[100] M2 Money Stock. Fred: Economic Data [online]. [cit. 2021-3-31]. Dostupné z: https://fred.stlouisfed.org/series/M2SL

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BTC	Bitcoin
ASIC	Application Specific Integrated Circuit, česky zákaznický integrovaný obvod pro specifické použití
MW	Megawatt
MB	Megabajt
HW	Hardware
SW	Software
A	Ampér
V	Volt
GB	Gigabajt
TB	Terabajt
USB	Universal Serial Bus
RAM	Random Access Memory
SSD	Solid-State Drive
HDD	Hard Disk Drive
URL	Uniform Resource Locator
URI	Uniform Resource Identifier
LN	Lightning Network
RTL	Ride The Lightning
P2PKH	Pay-to-Public-Key-Hash
VPN	Virtual Private Network
SBC	Single-board Computer

SEZNAM OBRÁZKŮ

SEZNAM TABULEK