

Vysoká škola logistiky o.p.s.

**Využití technologie Blockchain v
logistických procesech**

(Bakalářská práce)

Přerov 2023

Martin Kolář



Vysoká škola
logistiky
o.p.s.

Zadání bakalářské práce

student

Martin Kolář

studijní program
specializace

LOGISTIKA
Informatika pro logistiku

Vedoucí Katedry bakalářského studia Vám ve smyslu čl. 22 Studijního a zkušebního řádu Vysoké školy logistiky o.p.s. pro studium v bakalářském studijním programu určuje tuto bakalářskou práci:

Název tématu: Využití technologie Blockchain v logistických procesech

Cíl práce:

Na základě identifikovaných vlastností technologie Blockchain ukázat na typových příkladech možnosti jejího využití v logistických procesech s vazbou do příslušných informačních systémů. Typové příklady zhodnotit.

Zásady pro vypracování:

Využijte teoretických východisek oboru logistika. Čerpejte z literatury doporučené vedoucím práce a při zpracování práce postupujte v souladu s pokyny VŠLG a doporučeními vedoucího práce. Části práce využívající neveřejné informace uveďte v samostatné příloze.

Bakalářskou práci zpracujte v těchto bodech:

Úvod

1. Logistické procesy
 2. Moderní informační technologie
 3. Typové příklady využití
 4. Zhodnocení
- Závěr

Rozsah práce: 35 – 50 normostran textu

Seznam odborné literatury:

GROS, I., BARANČÍK, I., ČUJAN, Z.: Velká kniha logistiky. Praha: VŠCHT, 2016. ISBN 978-80-7080-952-5.

MAŘÍK, V. et.al. Národní iniciativa Průmysl 4.0. Konfederace zaměstnavatelských a podnikatelských svazů 2016 [online]. [cit. 2016-10-01] Dostupné z: <http://kzps.cz/wp-content/uploads/2016/02/kzps-cr.pdf>

BASL, J., BLAŽÍČEK, R.: Podnikové informační systémy. Grada 2012. ISBN: 978-80-247-4307-3.

Vedoucí bakalářské práce:

doc. Dr. Ing. Oldřich Kodým

Datum zadání bakalářské práce:

31. 10. 2022

Datum odevzdání bakalářské práce:

29. 4. 2023

Přerov 31. 10. 2022

Ing. et Ing. Iveta Dočkalíková, Ph.D.
vedoucí katedry

prof. Ing. Václav Cempírek, Ph.D.
rektor

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní, a že jsem ji vypracoval samostatně. Prohlašuji, že citace použitých pramenů je úplná, a že jsem v práci neporušil autorská práva ve smyslu zákona č. 121/2000 Sb.; o autorském právu, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

Prohlašuji, že jsem byl také seznámena s tím, že se na mou bakalářskou práci plně vztahuje zákon č. 121/2000 Sb., o právu autorském, právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména § 60 – školní dílo. Beru na vědomí, že Vysoká škola logistiky o.p.s. nezasahuje do mých autorských práv užitím mé bakalářské práce pro pedagogické, vědecké a prezentační účely školy. Užiji-li svou bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat předtím o této skutečnosti prorektora pro vzdělávání Vysoké školy logistiky o.p.s.

Prohlašuji, že jsem byl poučena o tom, že bakalářská práce je veřejná ve smyslu zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, zejména § 47b. Taktéž dávám souhlas Vysoké škole logistiky o.p.s. ke zpřístupnění mnou zpracované bakalářské práce v její tištěné i elektronické verzi. Souhlasím s případným použitím této práce Vysokou školou logistiky o.p.s. pro pedagogické, vědecké a prezentační účely.

Prohlašuji, že odevzdaná tištěná verze bakalářské práce a verze nahraná do informačního systému školy jsou totožné.

V Přerově, dne 29. 4. 2023



.....

Poděkování

Rád bych poděkoval všem, kteří mi pomohli s vytvořením této bakalářské práce. Především bych chtěl vyjádřit své poděkování vedoucímu práce doc. Dr. Ing. Oldřichu Kodymovi, který mi poskytl neocenitelnou podporu, rady a nápady během celého procesu psaní.

Nakonec bych chtěl poděkovat všem, kteří se rozhodli tuto práci číst a věnovat jí svůj čas. Doufám, že vám bude přínosem a poskytne vám nové poznatky a nápady. Vaše podpora a zájem o mou práci mi dodávají motivaci a potvrzují mé úsilí.

Anotace

V této bakalářské práci se zaměřuji na rozvíjející se technologii blockchainu a její následné využití v praktickém prostředí. V teoretické části se zaměřuji na samotné fungování, historii a vývoj blockchainu. Zaměřuji se na vlivy a potencionální využití blockchainu v malých i velkých firmách. V praktické části se věnuji konkrétnímu vytváření vlastní kryptoměny. Zkoumám, jakým způsobem je možné takovou měnu vytvořit a jak ji následně využít. Dále prezentuje příklady a modely, jakým způsobem by mohl blockchain sloužit jako nástroj pro zlepšení efektivity různých typech firem.

Klíčová slova

blockchain, kryptografie, logistické procesy, solana, smart kontrakty

Annotation

In this bachelor thesis I focus on the emerging blockchain technology and its subsequent use in a practical environment. In the theoretical part I focus on the actual functioning, history and development of blockchain. I focus on the influences and potential uses of blockchain in small and large companies. In the practical part, I focus on the actual creation of my own cryptocurrency. I explore how such a currency can be created and how it can be subsequently used. It also presents examples and models of how blockchain could serve as a tool to improve the efficiency of different types of companies.

Keywords

blockchain, cryptography, logistics processes, solana, smart contracts

Obsah

Úvod.....	10
1 Logistické procesy	11
1.1 Logistický řetězec	11
1.2 Plánování logistiky.....	12
1.3 Nástroje využívané v logistice	13
1.4 Logistika a Blockchain.....	14
1.4.1 Kryptografie.....	15
1.4.2 Symetrické šifrování	15
1.4.3 Asymetrické šifrování	16
1.4.4 Hašovací šifrování	17
1.4.5 Typy BlockChainu.....	18
1.4.6 Zabezpečení	19
1.4.7 Transparentnost.....	19
1.5 Základní principy kryptoměn.....	19
1.6 Bitcoin	21
1.6.1 Vývoj cen.....	21
1.6.2 Rozdíly mezi Bitcoinem a jinými kryptoměnami.....	22
1.6.3 Technologie Bitcoinu.....	22
1.6.4 Proces těžby a ověřování	23
1.6.5 Proof-of-work	24
1.6.6 Výhody a nevýhody obchodování s Bitcoinem	25
1.6.7 Regulace Bitcoinu po celém světě.....	26
1.6.8 Budoucnost Bitcoinu.....	26
1.6.9 BTC místo klasické fiat měny	27
1.6.10 Ethereum	28
1.6.11 Historie a vývoj.....	29

1.6.12	ETH jako platidlo.....	30
1.6.13	Shrnutí výhod a nevýhod.....	31
2	Moderní informační technologie.....	32
2.1	Vlastní kryptoměnový token.....	32
2.1.1	Výběr Blockchainu.....	32
2.1.2	Využití mincí.....	33
2.1.3	Vytvoření kryptoměny.....	34
2.1.4	Zosobnění vlastní kryptoměny.....	38
2.1.5	Distribuce mincí.....	43
2.2	Smart kontrakty.....	43
2.3	DApps.....	45
2.4	NFT.....	46
2.4.1	Příklady.....	46
3	Typové příklady využití.....	48
3.1	Sledování zásilek.....	48
3.1.1	Příklad.....	49
3.2	Fakturace a platby.....	49
3.2.1	Příklad.....	50
3.3	Řízení skladů.....	51
3.3.1	Příklad.....	52
3.4	Ochrana před paděláním.....	53
3.4.1	Příklad.....	54
3.5	Využití blockchainu v různých oblastech.....	55
3.5.1	Využití vlastní kryptoměny.....	55
3.5.2	Modelové příklady.....	57
4	Zhodnocení.....	59
	Závěr.....	61

Seznam zdrojů.....	62
Seznam grafických objektů.....	65
Seznam zkratk	66
Seznam příloh	67

Úvod

Tato bakalářská práce se zabývá velmi zajímavou a aktuální tematikou, která nachází stále více uplatnění v oblasti logistiky a logistických procesů. Tato technologie se nazývá blockchain a vyznačuje se svojí decentralizovanou povahou, vysokou dostupností a bezpečností. V práci se je zaměřuji na vysvětlení základních principů blockchainu a jeho aplikaci v logistice, to včetně konkrétních příkladů použití. V první části práce se věnuji teoretickému zázemí této technologie, vysvětlení základních principů fungování blockchainu a jeho klíčové vlastnosti. Dále popisuji jednotlivé typy blockchainů a jejich využití v praxi. Je zde uveden i historický vývoj této technologie, jakožto první využití blockchainu v podobě kryptoměny Bitcoin a Ethereum. V druhé části se zaměřuji na konkrétní aplikace blockchainu a moderní technologie využívané v blockchainovém světě. Zaměřím se na jednotlivé typy a využití jednotlivých dostupných veřejných blockchainů. Podrobně zde vysvětlím, jak vytvořit vlastní kryptoměnu na Solana network blockchainu. V třetí části práce uvádím jednotlivé příklady využití blockchainu v praxi spolu s modelovými příklady využití jak vlastní kryptoměny, kterou jsem představil v druhé kapitole, tak další příklady pro využití samotné technologie pro následné zavedení v téměř jakékoliv firmě, která se potýká s logistickým řetězcem. Závěrem se budu zabývat zhodnocením výhod a nevýhod blockchainu pro logistiku a jeho potenciálu pro budoucnost. Cílem této bakalářské práce je tedy přinést ucelený pohled na využití blockchainu v logistice, zhodnotit jeho výhody a nevýhody a na praktických příkladech poukázat na efektivnost, potenciál a poukázat na jeho jednoduchost pro zavedení do praktického prostředí. Doufám, že tato práce přispěje k lepšímu porozumění využití blockchainu v logistice a pomůže firmám v rozhodování o implementaci této technologie.

1 Logistické procesy

Logistika je oblast řízení toku zboží, informací a služeb od výrobce k zákazníkovi. V podnikání se logistika zabývá plánováním, organizací, řízením a sledováním pohybu zboží a služeb, aby byly k dispozici v požadovaném čase, místě a množství. To zahrnuje řízení nákupů, skladování, přepravu, balení a distribuci. [1]

V současném podnikání má logistika zásadní význam, protože pomáhá firmám optimalizovat náklady, zlepšit efektivitu a zvýšit konkurenceschopnost. Efektivní logistika umožňuje firmám dodávat zboží rychleji a spolehlivěji, což zvyšuje spokojenost zákazníků a vede k opakovaným nákupům. Zároveň umožňuje firmám snižovat náklady na skladování a přepravu, což vede k vyšší ziskovosti a konkurenceschopnosti na trhu.

Logistika také pomáhá firmám řídit zásoby a minimalizovat jejich ztráty, což je důležité zejména v oblasti potravinářství a farmaceutických výrobků. Díky logistice jsou firmy schopny lépe reagovat na poptávku a přizpůsobovat se měnícím podmínkám na trhu. To umožňuje firmám lépe plánovat své aktivity, optimalizovat své procesy a zvyšovat svou výkonnost. [1]

Význam logistiky v současném podnikání je tak velký, že mnoho firem vytváří vlastní oddělení pro logistiku a investuje do moderních technologií a systémů, které umožňují lépe řídit pohyb zboží a služeb. Logistika je také důležitou součástí globálního obchodu, protože umožňuje firmám překonávat vzdálenosti a zajišťovat rychlou a spolehlivou přepravu zboží napříč kontinenty. [2]

1.1 Logistický řetězec

Dodavatelský řetězec je část logistického řetězce, která se věnuje nakupování, skladování a přepravě surovin, polotovarů a hotových výrobků od dodavatelů až ke konečnému spotřebiteli. Dodavatelský řetězec je klíčovou částí logistického řetězce a ovlivňuje značně jeho výkonnost a efektivnost. Dobrá správa dodavatelského řetězce může vést k nižším nákladům na nákup, zvýšené kvalitě zboží a vyšší spokojenosti zákazníků. [2]

Skladování a skladovací systémy jsou součástí logistického řetězce, která se věnuje skladování a správě zásob. Skladovací systémy zahrnují všechny technologie a postupy, které umožňují správné a účinné skladování zboží. Skladovací systémy se dále dělí

na různé druhy, jako například vysokozdvizné vozíky, paletové regály, automatizované skladovací systémy a další. Důležitost správného skladování spočívá v tom, že zboží musí být skladováno bezpečně a efektivně tak, aby bylo kdykoliv k dispozici, a to včetně správné manipulace, sledování a kontroly zásob. [2]

Dopravní řetězec je součástí logistického řetězce, která se věnuje přepravě zboží od jednoho místa k druhému. Dopravní řetězec zahrnuje různé druhy dopravy, jako například silniční, železniční, námořní a leteckou dopravu. Dobře fungující dopravní řetězec zajišťuje efektivní přepravu zboží z místa A do místa B v co nejkratším čase s co nejnižšími náklady. [2]

Zpracování objednávek a plánování výroby je součástí logistického řetězce, která se věnuje zpracování objednávek, plánování výroby a koordinaci dodávek. Tato část logistického řetězce zahrnuje procesy a postupy, které zajišťují správné plánování a řízení výrobního procesu a zásobování. Dobrá správa zpracování objednávek a plánování výroby může vést k efektivnějšímu využití zdrojů a snížení času cyklu. [3]

Řízení informačního toku je součástí logistického řetězce, která se věnuje správě informací o zboží, zásobách, objednávkách a dalších relevantních údajích. Řízení informačního toku zahrnuje použití moderních informačních technologií a systémů, které umožňují efektivní sběr, zpracování, přenos a ukládání informací. Správné řízení informačního toku zajišťuje přesnou a aktuální informaci o stavech zásob, objednávkách a dalších relevantních informacích, což zlepšuje celkovou účinnost a výkonnost logistického řetězce. [3]

1.2 Plánování logistiky

Plánování logistiky je proces plánování a organizace různých aktivit a procesů, které jsou nezbytné k zajištění efektivního a úspěšného pohybu zboží a materiálů od výroby až po konečného zákazníka. Plánování logistiky zahrnuje plánování, organizaci a sledování dodávek, skladování, přepravy a distribuce zboží. [2]

Prvním krokem je stanovení poptávky po zboží nebo službách, které mají být dodány zákazníkům. Tento krok umožňuje určit, jaké množství zboží bude muset být vyrobeno, skladováno a distribuováno. [2]

Po analýze poptávky se plánování zaměří na plánování výroby zboží. To zahrnuje určení, jaké množství zboží bude vyrobeno, jaké suroviny budou potřeba, jaké procesy výroby budou použity a jaký bude časový harmonogram. [2]

Po výrobě zboží se plánování zaměří na skladování zboží. To zahrnuje určení, jaké množství zboží bude skladováno, kde bude skladováno a jaký bude systém skladování.

Poté, co je zboží vyrobeno a skladováno, se plánování zaměří na přepravu zboží. To zahrnuje určení nejefektivnějších a nejbezpečnějších tras pro přepravu zboží a určení nejvhodnějších dopravních prostředků pro přepravu zboží. [2]

Po dokončení plánování logistiky se provádí sledování a kontrola celého procesu. To umožňuje plánovačům logistiky identifikovat a řešit případné problémy, jako jsou zpoždění při přepravě zboží nebo problémy se skladováním. [2]

1.3 Nástroje využívané v logistice

Systémy řízení skladu (WMS) jsou užity pro správu skladových procesů, jako je přijímání a vydávání zboží, inventarizace, monitorování zásob a plánování objednávek. Systémy WMS mohou také sledovat polohu zboží v průběhu procesu, což umožňuje efektivní řízení zásob a minimalizaci ztrát. [4]

Systémy řízení dopravy (TMS) se využívají pro plánování a sledování dopravy zboží od dodavatele až po konečného zákazníka. Systémy TMS umožňují optimalizaci trasy, sledování stavu vozidel a výkonu řidičů a řízení přepravy v reálném čase. [5]

Plánování zdrojů podniku (ERP): Tyto systémy umožňují integrované plánování a řízení všech procesů v podniku, včetně procesů logistiky. ERP systémy umožňují plánování dodávek, správu zásob a sledování výkonu v reálném čase. [2]

Řízení řetězce dodávek (SCM) jsou systémy, které umožňují integrované řízení a optimalizaci všech procesů v řetězci dodávek, od výroby až po konečného zákazníka. SCM systémy umožňují sledování zboží a informací v reálném čase a umožňují spolupráci mezi různými částmi řetězce dodávek. [4]

Prediktivní analýza se využívá pro předpovědět budoucí poptávku a zásoby a umožňuje tak předem plánovat a řídit procesy logistiky. Prediktivní analýza může být použita k optimalizaci procesů zásobování, plánování dopravy a řízení skladových procesů.

Například maloobchodní společnost může využít prediktivní analýzu k předpovídání budoucí poptávky a zásob, aby předem plánovala procesy zásobování a minimalizovala riziko nedostatku zboží v sezónním období jako jsou Vánoce.

1.4 Logistika a Blockchain

Blockchain je distribuovaný, decentralizovaný a veřejný systém, který slouží k ukládání a ověřování záznamů transakcí. Každý uživatel v síti má přístup k knize, která obsahuje kompletní historii všech transakcí, a každá transakce v síti je ověřována a zapsána do systému v reálném čase. [6]

Každá transakce je v blockchainu reprezentována pomocí bloku, který obsahuje digitální podpis, tedy hash, transakce a hash předchozího bloku. Díky této kryptografické konstrukci je zajištěna nezpochybnitelnost předchozích transakcí, protože jakýkoliv pokus o manipulaci s existujícími daty by vedl k změně hashe a tedy i k odlišnému stavu bloku. [6]

Tento decentralizovaný systém eliminuje potřebu centralizované autority, která by mohla být náchylná k útokům a využití dat vlastní pro své vlastní zájmy. Každý uživatel má v síti plnou kontrolu nad svými daty a transakcemi, a žádný záznam nelze vymazat nebo upravit bez souhlasu většiny ostatních uživatelů. [6]

Blockchain se původně proslavil jako základní technologie pro kryptoměny, ale dnes má mnoho dalších využití v různých oblastech, jako jsou finance, logistika, výroba, zdravotnictví a další. Díky svému decentralizovanému a bezpečnému charakteru představuje blockchain inovativní způsob, jak ukládat a spravovat data v digitálním světě. [7]

1.4.1 Kryptografie

Kryptografie a Blockchain jsou propojeni tím, že kryptografie je technologie používaná k zabezpečení kryptoměn. Kryptografie je věda o zabezpečení informací před neautorizovaným přístupem a používá se k ochraně soukromých klíčů a transakcí v kryptoměnových sítích. [6]

Kryptoměny, jako je například Bitcoin, používají kryptografii pro zabezpečení transakcí a ověřování platností peněžních převodů. Tyto kryptoměny používají asymetrickou kryptografii, která umožňuje uživatelům vytvořit digitální podpis, který ověřuje jejich identitu, a tím potvrdit platnost transakce. [6]

Další typ kryptografie používané v kryptoměnách je hashování, které zabezpečuje integritu dat v transakcích. Hashování vytváří jedinečnou kontrolní hodnotu, která identifikuje obsah transakce, a která se přidává k transakci jako součást ověření. [8]

Vzhledem k tomu, že kryptoměny jsou digitální a decentralizované, musí být zabezpečeny proti podvodům a zásahům zvenčí. Kryptografie poskytuje prostředky k dosažení této bezpečnosti a zajištění, že peníze zůstanou v bezpečí a vlastnictví uživatele, který je vlastní. [9]

Základem kryptografie je algoritmus, který slouží k šifrování a dešifrování zpráv. Šifrování znamená přeměnu původního textu na kódovanou podobu, která není čitelná bez znalosti klíče. Dešifrování je naopak proces, kterým se kódovaná zpráva přemění zpět na původní text. Pro zajištění bezpečnosti je klíč důležitý, protože bez znalosti správného klíče není možné zprávu dešifrovat. Existují různé druhy šifrovacích algoritmů, například symetrické, asymetrické a hašovací. [8]

1.4.2 Symetrické šifrování

Symetrické šifrování je technika kryptografie, při které se používá stejný klíč pro šifrování a dešifrování dat. Tento klíč musí být tajný a musí být sdílen mezi odesílatelem a příjemcem zprávy. Pokud útočník získá tento klíč, může dešifrovat všechna data, která byla pomocí něj šifrována. [10]

Symetrické šifrování se často používá pro šifrování kratších zpráv a také pro šifrování dat, která se přenášejí na krátkou vzdálenost, například v síti LAN nebo mezi zařízeními Bluetooth. [10]

Při symetrickém šifrování se původní zpráva nejprve rozdělí na menší bloky a každý blok se následně zašifruje pomocí klíče. Po přenesení zašifrovaných dat na druhou stranu se použije stejný klíč k jejich dešifrování. Pokud se klíč dostane do rukou neoprávněné osoby, mohou být data snadno dešifrována. [10]

Symetrické šifrování má několik výhod, jako je rychlost šifrování a dešifrování, jednoduchost implementace a nízké náklady na výpočetní výkon. Nicméně má také několik bezpečnostních problémů, jako je například problém se sdílením klíče mezi odesílatelem a příjemcem. Dalším problémem může být fakt, že každý blok zprávy se šifruje stejným klíčem, což umožňuje útočníkům provést útok "known plaintext". [10]

1.4.3 Asymetrické šifrování

Asymetrické šifrování, známé také jako veřejný klíčový systém, je metoda kryptografie, která využívá dvou odlišných klíčů pro šifrování a dešifrování zpráv. Jedním klíčem je veřejný klíč, který je široce dostupný pro každého, a druhým klíčem je soukromý klíč, který je uchovávan v bezpečí u uživatele. [10]

V asymetrickém šifrování se zpráva šifruje pomocí veřejného klíče, který je k dispozici pro každého, a poté je dešifrována soukromým klíčem, který má pouze příjemce zprávy. Tímto způsobem je zajištěna bezpečnost přenášených dat, protože kromě příjemce nikdo jiný nemá přístup k soukromému klíči. [10]

Asymetrické šifrování se používá k různým účelům, jako je například ochrana přenášených dat při online transakcích, zabezpečení komunikace mezi uživateli na internetu, ověřování identity a digitalizaci podpisu. [10]

Další výhodou asymetrického šifrování je, že umožňuje digitální podpis, který umožňuje ověřit původního autora dokumentu a ochránit dokument před manipulací. Při digitálním podpisu je použit soukromý klíč, aby se zpráva podepsala, a poté se podepsaná zpráva předá s veřejným klíčem, aby se ověřilo, že zpráva byla podepsána oprávněnou osobou. [10]

Nicméně, asymetrické šifrování má také několik nevýhod. Jednou z nevýhod je, že je pomalejší než symetrické šifrování, což znamená, že pro velké objemy dat může být pomalé. Další nevýhodou je, že klíče jsou mnohem větší než u symetrického šifrování, což může mít dopad na efektivitu a účinnost přenosu dat. [10]

V posledních letech se asymetrické šifrování stalo nezbytným nástrojem pro zabezpečení online komunikace a obchodování. Protože přenos dat na internetu se stává stále důležitějším, je nutné zajistit, aby byly tyto informace chráněny před neoprávněným přístupem. [10]

V současné době se výzkum v oblasti asymetrické kryptografie zaměřuje na nalezení nových algoritmů, které jsou rychlejší a bezpečnější než současné algoritmy. Cílem je vytvořit bezpečné a efektivní kryptografické metody, které mohou být použity k zabezpečení komunikace v různých oblastech, jako je například finance, zdravotnictví nebo vládní instituce. [10]

Asymetrické šifrování je tedy klíčovým nástrojem pro zabezpečení přenosu dat na internetu a jeho význam se bude s neustále rostoucím počtem online transakcí a komunikace dále zvyšovat. [10]

1.4.4 Hašovací šifrování

Hašovací kryptografie je obor kryptografie, který se zabývá vytvářením hašovacích funkcí, které umožňují rychlou a efektivní kontrolu integrity dat. Hašování je proces, který převádí libovolně velký vstupní text na kratší výstupní řetězec, který se nazývá hash. Tento hašovací algoritmus umožňuje ověřit, zda byly data změněny nebo poškozeny, protože pokud jsou data změněna, pak se hašovací funkce změní. Hašovací funkce se také používají k ukládání hesel a ověřování, zda uživatel zadává správné heslo. [11]

Hašovací kryptografie se také používá pro ochranu soukromí a zabezpečení proti útokům. Například v bezpečnostních kamerových systémech se hašovací funkce používají k anonymizaci obrazových dat, takže je možné zachovat soukromí osob, které se nacházejí na záběru. [11]

Hašovací kryptografie má několik výhod. Jednou z nich je, že hašovací funkce jsou rychlé a efektivní, což umožňuje snadné ověřování integrity dat. Další výhodou je, že hašovací funkce jsou jednosměrné, což znamená, že je obtížné zpětně vypočítat vstupní data z haše. Pokud útočník získá hašovou hodnotu, nemůže zpětně vypočítat původní data, což ztěžuje útok. [11]

Tento typ kryptografie je důležitý nejen pro bezpečnost osobních, ale také pro ochranu citlivých informací v oblasti ekonomiky, výzkumu, vojenství a mnoha dalších oblastech. Kryptografie se stává stále důležitější s rostoucím množstvím informací, které jsou ukládány a přenášeny digitální cestou. [11]

1.4.5 Typy BlockChainu

Blockchain je decentralizovaná databáze, která umožňuje ukládání a sdílení informací v reálném čase mezi mnoha účastníky. Existují tři hlavní druhy blockchainů: privátní, veřejné a průmyslové.

Privátní blockchainya jsou uzavřené sítě, které jsou provozovány pouze jedním subjektem nebo organizací. Tento typ blockchainu umožňuje subjektům řídit, kdo má přístup k datům a kdo má právo provádět transakce. Privátní blockchainya jsou často používány v korporátním prostředí, kde je důležité zajistit bezpečnost dat a zároveň udržovat vysokou úroveň důvěrnosti. [7]

Veřejné blockchainya jsou otevřené sítě, které umožňují komukoli připojit se a provádět transakce. Tento typ blockchainu je založen na principu decentralizace, kde jsou data uložena a ověřována mnoha různými účastníky sítě. Veřejné blockchainya jsou často používány pro kryptoměny, jako je například Bitcoin nebo Ethereum. [7]

Průmyslové blockchainya jsou navrženy pro specifické průmyslové účely a používají se k usnadnění transakcí mezi různými subjekty v daném průmyslu. Tento typ blockchainu umožňuje zvýšení efektivity a účinnosti v různých průmyslových odvětvích, jako jsou například energetika, doprava, zdravotnictví nebo správa majetku. [12]

Každý typ blockchainu má své výhody a nevýhody. Privátní blockchainya jsou vhodné pro korporátní prostředí, kde je důležité zajistit bezpečnost dat a zachovat důvěrnost, veřejné blockchainya jsou vhodné pro decentralizované kryptoměny a průmyslové blockchainya jsou vhodné pro průmyslové odvětví a usnadnění transakcí mezi různými subjekty.

1.4.6 Zabezpečení

Transakce v kryptoměnách jsou zabezpečeny pomocí kryptografie. Každá transakce je podepsána digitálním podpisem, což umožňuje ověřit, že transakce byla skutečně provedena majitelem kryptoměny. Tyto digitální podpisy jsou vytvořeny pomocí privátních klíčů, které jsou tajné a pouze majitel kryptoměny by měl mít přístup k nim. Tím se zajišťuje, že transakce jsou legitimní a mají správného majitele. [13]

Kromě toho jsou transakce uloženy v distribuované databázi, známé jako blockchain. Blockchain je řetězec bloků, které obsahují transakce. Každý blok je ověřen pomocí kryptografických technik a přidán k řetězci. To znamená, že jakékoli změny v bloku by byly viditelné a zrušily by jeho platnost. Tím se zajišťuje, že bloky jsou nezměnitelné a nedají se podvrhnout. [13]

1.4.7 Transparentnost

Kryptoměny jsou transparentní, protože každá transakce je zveřejněna v blockchainu. To znamená, že kdokoli může vidět, kdo posílá kryptoměnu a komu je posílána. Tato úroveň transparentnosti znamená, že kryptoměny jsou obtížnější pro použití v nelegálních činnostech, jako je praní špinavých peněz, protože každá transakce je zaznamenána a zveřejněna. [13]

Blockchain umožňuje použití tzv. "chytrých smluv", což jsou digitální smlouvy, které se automaticky aktivují a uplatňují se na základě určitých podmínek. Tyto smlouvy mohou být programovány tak, aby prováděly určité akce v závislosti na určitých událostech. To může být užitečné pro různé obchodní transakce, jako je například uzavírání sázek nebo pojišťovacích smluv. [13]

1.5 Základní principy kryptoměn

Kryptoměny jsou digitální měny, které fungují na základě decentralizovaného systému, který je založen na technologii blockchain. Základní principy kryptoměn zahrnují peer-to-peer (P2P) síť a proces miningu. [13]

Kryptoměny jsou open source, často jsou vyvíjeny a spravovány komunitou uživatelů. Tím se zajišťuje transparentnost a bezpečnost vývoje, protože kdokoli může přispět k vylepšení softwaru a pomoci při odhalování chyb a zranitelností. [7]

Kryptoměny jsou navrženy tak, aby byly bezpečné a soukromé. Transakce jsou chráněny šifrováním, což znamená, že jsou zabezpečeny proti neoprávněnému přístupu a změnám. Soukromí uživatelů je chráněno tím, že transakce jsou anonymní a nejsou spojeny s reálnými jmény. [7]

Většina kryptoměn má omezenou nabídku, což znamená, že existuje pouze omezené množství mincí, které mohou být vytvořeny. Tento princip zajišťuje stabilitu hodnoty kryptoměn, protože nedochází ke znehodnocení měny v důsledku nekontrolovaného vytváření nových mincí. [7]

Decentralizace kryptoměn znamená, že neexistuje žádný centrální autoritativní orgán, který by měl kontrolu nad vývojem, transakcemi a použitím kryptoměn. To umožňuje uživatelům kryptoměn nezávislost a kontrolu nad svými finančními prostředky. [13]

P2P sítě jsou základním principem kryptoměn, protože umožňují přenos kryptoměn přímo mezi uživateli bez zprostředkování třetí stran, jako jsou banky nebo platební brány. V P2P sítích jsou uživatelé spojeni přímo s ostatními uživateli, kteří používají stejnou kryptoměnu a tvoří tak síť, která ověřuje a zaznamenává transakce. [13]

Mining je proces, při kterém jsou nové kryptoměny vytvářeny a ověřovány v blockchainu. Uživatelé, kteří se zapojí do miningu, řeší složité matematické problémy, aby mohli ověřovat transakce a tím získat odměny v podobě nových kryptoměn. Mining zajišťuje bezpečnost a integritu blockchainu tím, že ověřuje transakce a vytváří nové bloky, které jsou přidávány k řetězci transakcí. [13]

Tyto principy poskytují uživatelům kryptoměn svobodu a kontrolu nad svými finančními transakcemi a umožňují vytváření nových možností pro platební systémy a investiční příležitosti. [13]

1.6 Bitcoin

Kryptoměny jsou digitální měny, které využívají kryptografii pro zabezpečení transakcí a řízení tvorby nových jednotek této měny. Jedním z průkopníků v oblasti kryptoměn je Bitcoin, který byl poprvé představen v roce 2009 a dodnes zůstává největší a nejznámější kryptoměnou. [14]

Bitcoin byl vytvořen jako alternativa k tradičním měnám, které jsou ovládány centrálními bankami a vládami. Bitcoin umožňuje přímé převody peněz mezi lidmi bez nutnosti prostředníka a zajišťuje vysokou úroveň anonymity a bezpečnosti. [14]

Jako průkopník v oblasti kryptoměn se Bitcoin setkal s mnoha výzvami a kontroverzemi. Jeho decentralizovaná povaha a absence regulace však také přilákala pozornost investorů a obchodníků, kteří využívají Bitcoin k investicím a obchodování. [14]

V dnešní době existuje mnoho dalších kryptoměn a blockchainových projektů, ale Bitcoin si stále udržuje své místo jako přední kryptoměna. Jeho vliv na finanční a technologický svět je stále velmi významný a budoucnost Bitcoinu a kryptoměn jako celku je stále plná nejistot a nevyzpytatelnosti. [14]

1.6.1 Vývoj cen

Cena Bitcoinu se v průběhu let neustále mění a zaznamenala několik významných výkyvů. V prvních letech existence Bitcoinu byla cena velmi nízká, často pod 1 dolar. Postupně však začala růst a v roce 2013 se cena jednoho Bitcoinu poprvé dostala nad 1 000 dolarů. Následoval však prudký pokles ceny a v roce 2015 byla cena Bitcoinu opět pod 300 dolary. [15]

V roce 2017 došlo k dalšímu období růstu ceny Bitcoinu a v prosinci téhož roku se cena dostala až na téměř 20 000 dolarů za Bitcoin. Tento růst byl však velmi rychlý a krátkodobý a cena Bitcoinu se brzy vrátila na nižší úroveň. V následujících letech se cena Bitcoinu stabilizovala na úrovni mezi 5 000 a 10 000 dolary. [15]

Tržní kapitalizace Bitcoinu, tedy hodnota všech vydaných Bitcoinů, se také neustále mění. V roce 2009 byla tržní kapitalizace Bitcoinu nulová, ale postupně začala růst a v roce 2017 se dostala na téměř 300 miliard dolarů. Následoval však opět prudký pokles a v roce 2018 byla tržní kapitalizace Bitcoinu pod 100 miliard dolary. V současné době

se tržní kapitalizace Bitcoinu pohybuje okolo 1 bilionu dolarů. Podrobnější informace o vývoji cen BTC, lze nalézt v grafu v příloze A. [15]

Vývoj ceny a tržní kapitalizace Bitcoinu je ovlivňován mnoha faktory, jako je poptávka po Bitcoinu, regulace, konkurence a celkový stav trhu s kryptoměny. Cena Bitcoinu je velmi nestabilní a výrazně se může měnit během krátkého časového období. [15]

1.6.2 Rozdíly mezi Bitcoinem a jinými kryptoměny

Bitcoin využívá technologii blockchainu, která umožňuje decentralizované ukládání a ověřování transakcí. Nicméně, existují i další kryptoměny, které využívají jiné verze nebo modifikace blockchainu, jako například Ethereum, Litecoin nebo Ripple. [16]

Bitcoin má pevně stanovený limit na počet mincí, který může být vytvořen (21 milionů), což vede k omezení množství Bitcoinů v oběhu a může mít vliv na cenu. Na druhou stranu, existují i kryptoměny, které mají různé limity na množství mincí, které mohou být vytvořeny, nebo dokonce nemají žádný limit, jako například Dogecoin. [16]

Rychlost transakcí se může lišit v závislosti na kryptoměně a použité technologii. Například Bitcoin transakce mohou být pomalejší kvůli omezené kapacitě sítě, zatímco jiné kryptoměny, jako například Solana, umožňují velmi rychlé transakce. [16]

Některé kryptoměny, jako například Ethereum, mají větší důraz na možnost tvorby chytrých smluv a vytváření decentralizovaných aplikací, zatímco jiné kryptoměny, jako například Monero, kladou větší důraz na soukromí a anonymitu. [16]

Bitcoin je nejznámější kryptoměnou a má nejvyšší úroveň přijetí a popularizace mezi běžnými uživateli. Nicméně, existují i další kryptoměny, které získávají na popularitě a jsou přijímány obchodníky a platformami. [16]

1.6.3 Technologie Bitcoinu

Blockchain je základní technologií, na které je postaven Bitcoin a mnoho dalších kryptoměn. Blockchain je decentralizovaný systém, který umožňuje ukládání a ověřování transakcí v distribuované síti počítačů. Transakce jsou seskupovány do bloků, které jsou následně přidávány do řetězce bloků, což vytváří nezměnitelnou a transparentní záznamovou knihu. [16]

V případě Bitcoinu, blockchain slouží k ukládání všech transakcí, které jsou prováděny mezi adresami Bitcoinu. Každá transakce je ověřována pomocí matematického algoritmu

nazývaného "hash", který již nelze změnit. Tyto ověřené transakce jsou pak seskupeny do bloků, které jsou přidány do blockchainu a jsou tak trvale uloženy v celé síti počítačů. Jedním z hlavních důvodů, proč je blockchain tak důležitý, je jeho decentralizovaná povaha. To znamená, že žádná jednotlivá osoba nebo organizace nemá kontrolu nad blockchainem. Namísto toho je síť řízena množstvím uživatelů, kteří spolupracují na ověřování transakcí a udržování integrity sítě. [17]

Dalším důležitým prvkem blockchainu je jeho bezpečnost. Pokud by někdo chtěl změnit nebo zfalšovat jednu transakci, musel by změnit všechny následující bloky v blockchainu. To je v praxi téměř nemožné, protože by to vyžadovalo úpravu všech kopií blockchainu, které existují v síti. [17]

Blockchain je důležitou technologií nejen pro Bitcoin, ale i pro mnoho dalších oblastí, jako je například finanční sektor, průmysl a logistika. Blockchain umožňuje bezpečné a transparentní ukládání dat, a to bez potřeby centrální autority. To má velký potenciál pro transformaci mnoha odvětví a vytváření nových aplikací a služeb. [17]

1.6.4 Proces těžby a ověřování

Těžba Bitcoinu je proces, při kterém se používá výpočetní síla k řešení matematických problémů a ověřování transakcí v síti Bitcoinu. Tento proces je nezbytný k udržení bezpečnosti a integrity sítě. [18]

Těžba probíhá tak, že počítače v síti se snaží najít řešení matematického problému, který je součástí každé nové transakce. Pokud některý z počítačů v síti najde řešení, tak transakce je ověřena a přidána do blockchainu. Těžba také slouží k vytváření nových Bitcoinů za každý nový blok přidávaný do blockchainu dostává těžbař odměnu v podobě několika nových Bitcoinů. [19]

Proces ověřování transakcí v síti Bitcoinu se nazývá "proof-of-work" (důkaz práce). Jde o proces, který využívá výpočetní sílu počítačů k ověření transakcí v síti. Každý blok v blockchainu obsahuje hashovou hodnotu předchozího bloku, což zajišťuje, že každý blok v řetězci je svázán s předchozím a vytváří nezměnitelný záznam transakcí. [19]

Při ověřování transakcí je třeba vyřešit matematický problém, který je složitý a náhodný, ale snadno ověřitelný. Tento proces se skládá z mnoha výpočtů, které musí být vyřešeny, aby byla transakce ověřena. Těžbaři soutěží o řešení těchto problémů a ten, kdo je vyřeší

jako první, má právo přidat transakci do blockchainu a obdrží odměnu v podobě nově vytvořených Bitcoinů. [19]

Proces těžby a ověřování transakcí v síti Bitcoinu je důležitý pro udržení bezpečnosti a integrity. Díky decentralizované povaze sítě a "proof-of-work" algoritmu, který je náročný na výpočetní sílu, je Bitcoin relativně bezpečná kryptoměna. [19]

1.6.5 Proof-of-work

"Proof-of-work" (důkaz práce) je algoritmus používaný v mnoha kryptoměnách pro ověřování transakcí a udržování integrity a bezpečnosti sítě. Jedná se o proces, při kterém se počítače v síti snaží vyřešit matematický problém, který je složitý a náhodný, ale snadno ověřitelný. [19]

Základem "proof-of-work" je to, že těžaři v síti musí vynaložit určitou množství výpočetní síly k řešení matematického problému. Tento problém může být například nalezení náhodného čísla, které když se použije jako součást transakce a následně se na něj aplikuje hashovací funkce, výsledek bude mít určité vlastnosti. Pokud výsledek nemá požadované vlastnosti, těžaři musí změnit náhodné číslo a pokračovat v procesu, dokud nebudou schopni najít výsledek s požadovanými vlastnostmi. [19]

Tento proces je náročný na výpočetní sílu, protože vyžaduje neustálé testování náhodných čísel, dokud nebyl nalezen výsledek s požadovanými vlastnostmi. Zároveň je však snadno ověřitelný, protože ostatní počítače v síti mohou jednoduše ověřit, zda byl výsledek správně vyřešen. [19]

Jedním z hlavních důvodů použití "proof-of-work" algoritmu je to, že tento proces vytváří závod v těžení, kdy těžaři soutěží o to, kdo jako první vyřeší matematický problém a přidá transakci do blockchainu. Těžař, který vyřeší problém jako první, obdrží odměnu v podobě nově vytvořených Bitcoinů a transakce je potvrzena v blockchainu. Tento proces také pomáhá udržovat bezpečnost sítě tím, že ztěžuje útoky na síť, protože útočník by musel vynaložit velké množství výpočetní síly na řešení matematického problému a získání kontroly nad sítí. [19]

Nicméně, "proof-of-work" algoritmus má také své nevýhody. Jednou z hlavních nevýhod je vysoká spotřeba energie vynaložená na těžbu. Tento proces vyžaduje mnoho výpočetní síly, která se často získává z vysokého výkonu hardwaru, jako jsou speciální ASIC čipy, které jsou navrženy specificky pro těžbu kryptoměn. Tyto ASIC čipy jsou velmi

energeticky náročné a těžaři jsou nuceni vynakládat velké množství elektrické energie, což může být problematické z hlediska ekologického a finančního. [19]

1.6.6 Výhody a nevýhody obchodování s Bitcoinem

Rizika:

Cena Bitcoinu je velmi nestabilní a může se rychle měnit. To znamená, že investoři mohou snadno ztratit své investice, pokud cena Bitcoinu klesne. Proto je důležité pečlivě sledovat trh a provádět analýzy před každým obchodem.

Bitcoin a další kryptoměny jsou zranitelné vůči kybernetickým útokům, jako jsou hacking nebo phishing. Pokud útočníci získají přístup k vaší digitální peněženke nebo obchodní platformě, mohou odcizit vaše bitcoiny.

Regulace kryptoměn se stále vyvíjí a může se výrazně lišit v závislosti na zemi. Existuje riziko, že vlády mohou přijmout regulace, které mohou ovlivnit cenu Bitcoinu a jeho obchodování.

Trh s Bitcoinem je decentralizovaný a neexistuje centrální autorita, která by ho řídila. To znamená, že je náchylný k manipulaci trhu a spekulaci.

Pokud ztratíte své heslo nebo digitální peněženku, nemůžete získat zpět své bitcoiny. Je důležité chránit své heslo a digitální peněženku před ztrátou. [20]

Výhody:

Investice do Bitcoinu může být velmi výnosná, pokud provedete správnou analýzu trhu a provádíte správné obchody.

Bitcoin můžete snadno převést na jinou měnu nebo digitální peněženku. To znamená, že můžete snadno provádět transakce a převádět své bitcoiny.

Bitcoin je decentralizovaný a neexistuje centrální autorita, která by ho řídila. To znamená, že je nezávislý na bankovním systému a může být používán po celém světě.

Transakce Bitcoinu jsou relativně anonymní, což znamená, že nejsou spojeny s vaším osobním účtem nebo identitou [20]

1.6.7 Regulace Bitcoinu po celém světě

Stav regulace Bitcoinu po celém světě se liší v závislosti na zemi. Některé země přijaly Bitcoin s otevřenou náručí, zatímco jiné se snaží jeho používání omezit nebo regulovat. V některých zemích, jako je Japonsko a Jižní Korea, jsou kryptoměny zcela legální a jsou považovány za běžnou formu platby. V Japonsku byla dokonce vytvořena speciální legislativa, která stanoví pravidla pro provozovatele kryptoměnových burz a upravuje způsob zpracování transakcí s kryptoměnami. [21]

Na druhé straně některé země, jako je Čína zakázaly čínským občanům používat kryptoměny jako Bitcoin. V roce 2021 Čína také zakázala těžbu kryptoměn, což vedlo k poklesu výkonu Bitcoinové sítě. [21]

V USA a v Evropě existuje různá regulace pro kryptoměny. V USA Komise pro cenné papíry a burzy stanovila, že některé kryptoměny by mohly být považovány za cenné papíry a měly by být regulovány stejně jako akcie. Evropská unie uvedla, že kryptoměny by měly být podrobeny stejným pravidlům jako tradiční finanční instituce, a to z hlediska prevence praní špinavých peněz a financování terorismu. [21]

1.6.8 Budoucnost Bitcoinu

Bitcoin a kryptoměny obecně jsou stále relativně novou technologií a jejich budoucnost je stále nejistá. Existuje však několik možných vývoju a trendů, které by mohly ovlivnit budoucnost Bitcoinu. [7]

S nárůstem popularity Bitcoinu a kryptoměn se očekává zvýšená regulace ze strany vlád a státních orgánů. To by mohlo ovlivnit cenu a dostupnost kryptoměn a mohlo by to také vést k většímu přijetí a legitimizaci kryptoměn jako investičního nástroje.

I když Bitcoin je stále více vnímán jako investiční nástroj, může se stát, že se bude více používat jako platidlo. To by mohlo vést k většímu rozšíření Bitcoinu mezi obchodníky a spotřebiteli a mohlo by to také zvýšit stabilitu ceny Bitcoinu. [7]

Bitcoin je stále nejznámější a největší kryptoměnou, ale existuje mnoho dalších kryptoměn, které se snaží získat větší podíl na trhu. Pokud by se jedné z nich podařilo překonat Bitcoin v populárnosti a hodnotě, mohlo by to znamenat velkou změnu v kryptoměnovém prostředí. [7]

Bitcoin a kryptoměny jsou často vnímány jako alternativa tradičním investicím, jako jsou akcie a dluhopisy. Pokud by došlo k velkému hospodářskému otřesu nebo krizi, mohlo by to vést k většímu zájmu o kryptoměny jako bezpečné útočiště pro investory. [7]

Budoucnost Bitcoinu a kryptoměn je stále nejistá a závisí na mnoha faktorech. Nicméně, Bitcoin a kryptoměny jsou stále velmi zajímavým a inovativním trhem s mnoha potenciálními výhodami a riziky. Budoucnost může být ovlivněna regulacemi vlád, technologickými inovacemi, přijetím většího počtu lidí a společností a dalšími faktory. [7]

V posledních letech jsme viděli rostoucí zájem a přijetí Bitcoinu a kryptoměn ze strany velkých finančních institucí a společností, jako jsou PayPal, Visa, Mastercard, Tesla a další. Tento trend může vést k dalšímu nárůstu ceny Bitcoinu a dalších kryptoměn. [7]

Další možnou budoucností může být rozvoj decentralizovaných finančních aplikací a dalších decentralizovaných služeb využívajících blockchain technologii. Tyto aplikace mohou poskytnout nové možnosti pro investování, půjčování a správu financí.

V každém případě je důležité být obezřetný a pečlivě zvažovat rizika a výhody při investování do Bitcoinu a kryptoměn. Je také důležité sledovat vývoj regulací a trendů, aby se minimalizovala rizika a maximalizovaly výhody. [7]

1.6.9 BTC místo klasické fiat měny

Jedním z klíčových faktorů pro nahrazení klasické měny Bitcoinem je adopce. Bitcoin se stává stále populárnější a více lidí ho používá pro různé účely, jako jsou nákupy, investice a mezinárodní platby. Pokud bude tento trend pokračovat, může se Bitcoin stát více běžnou a uznávanou měnou. [22]

Klasická měna je obvykle považována za stabilní, zatímco Bitcoin může být velmi volatilní. Pokud Bitcoin chce nahradit klasickou měnu, musí být stabilnější a méně náchylný k výkyvům v cenách. [22]

Bitcoin je decentralizovanou měnou, z čehož vyplývá, že neexistuje centrální autorita, která by mohla garantovat jeho bezpečnost. To znamená, že existuje větší riziko ztráty Bitcoinu v důsledku hackerských útoků nebo technických problémů. Pokud by měl Bitcoin nahradit klasickou měnu, musel by být více zabezpečený a mít lepší ochranu. [22]

Bitcoin a kryptoměny jsou stále velmi nedostatečně regulovány a legislativa se může měnit. Pokud by měl Bitcoin nahradit klasickou měnu, musí být regulován podobně jako klasické měny. [22]

Bitcoin a kryptoměny stále mají několik výzev, které musí překonat, existují potenciální faktory, které by mohly vést k tomu, že se stane alternativou klasické měny. Nicméně, zda se to stane, závisí na mnoha faktorech a bude se to vyvíjet v průběhu času. [22]

1.6.10 Ethereum

Ethereum je decentralizovaná open-source blockchainová platforma, která umožňuje vytváření a spouštění decentralizovaných aplikací a smart kontraktů. Ethereum bylo vytvořeno v roce 2014 Vitalikem Buterinem, který měl za cíl vytvořit platformu, která by umožnila tvorbu aplikací, které byly byly odolné vůči cenzuře, falšování a útokům hackerů. Ethereum se také snaží být přínosem pro tvůrce obsahu, vývojáře, podniky a spotřebitele, kteří chtějí využít decentralizovaných technologií. [23]

Hlavním prvkem Ethereum je blockchain, který slouží jako veřejná a distribuovaná databáze transakcí. Každý uživatel sítě má přístup k celé historii transakcí a aktuálnímu stavu sítě. Ethereum se také vyznačuje možností programovat smart kontrakty. [23]

transakce v síti a pro odměny pro těžáře. Těžba Etheru probíhala pomocí "proof-of-work" algoritmu, ale v roce 2022 síť přešla na "proof-of-stake" algoritmus, který je šetrnější k životnímu prostředí a umožňuje těžbu bez nutnosti vysoké výpočetní kapacity. [23]

Ethereum se také vyznačuje možností vytváření vlastních kryptoměn pomocí standardu, což umožňuje tvorbu vlastních kryptoměn a tokenů pro různé účely, například jako firemní platidlo. [23]

Celkově lze tedy říci, že Ethereum je platforma, která umožňuje vytváření decentralizovaných aplikací a smart kontraktů, a která slouží jako základ pro vývoj nových kryptoměn a tokenů. Ethereum se snaží poskytnout uživatelům a tvůrcům obsahu větší svobodu, bezpečnost a efektivitu při využívání decentralizovaných technologií. [23]

1.6.11 Historie a vývoj

Historie vzniku a vývoj sítě Ethereum se datuje do roku 2013, kdy Vitalik Buterin, kanadsko-ruský programátor, začal pracovat na své vlastní blockchainové platformě, která by umožnila tvorbu decentralizovaných aplikací a smart kontraktů. Buterin se inspiroval Bitcoinem, ale chtěl vytvořit platformu, která by byla více programovatelná a umožňovala tvorbu komplexnějších aplikací. [24]

V roce 2014 Buterin spolupracoval s dalšími vývojáři na vytvoření Etherea, které bylo oficiálně uvedeno na trh 30. července 2015 a od té doby se stala jednou z největších a nejpopulárnějších blockchainových platforem na světě. [24]

Během prvních let vývoje bylo Ethereum vystaveno několika technickým výzvám, včetně útoků hackerů a problémů s škálovatelností. V roce 2016 byl však představen plán na zavedení nového konsenzuálního algoritmu, "proof-of-stake", který by měl být energeticky úspornější a umožnit rychlejší a efektivnější zpracování transakcí. [24]

V roce 2017 se Ethereum stalo populární platformou pro vývoj nových kryptoměn a tokenů pomocí standardu ERC-20. To vedlo k boomu, kdy společnosti využívaly síť Ethereum k financování svých projektů. Tento trend však také přilákal mnoho podvodníků, a tak byla v roce 2017 vydána řada opatření a regulací, aby se minimalizovaly rizika pro investory. [24]

V roce 2018 bylo Ethereum vystaveno dalším technickým problémům, včetně pomalého zpracování transakcí a vysokých poplatků. To vedlo k diskusím o nutnosti provést hard fork sítě, což by znamenalo rozdělení sítě na dvě větve. Nakonec se však vývojáři rozhodli pro další inovace a vylepšení stávající sítě, aby se minimalizovaly problémy a umožnilo větší škálovatelnost. [24]

V současné době se Ethereum nachází ve fázi Ethereum 2.0, která byla spuštěna v prosinci 2020. Ethereum 2.0 je navrženo tak, aby umožnilo vyřešení stávajících problémů se škálovatelností a zlepšilo energetickou efektivitu sítě. [24]

S vývojem sítě Ethereum se také rozvíjí ekosystém decentralizovaných aplikací a smart kontraktů, které využívají možnosti, které platforma nabízí. Díky rozvoji decentralizovaných aplikací na Ethereum můžou uživatelé používat decentralizované

burzy, půjčovat si a investovat do kryptoměn, vydělávat peníze na likviditě a mnoho dalšího. Síť Ethereum také umožňuje tvorbu NFT (Non-Fungible Tokens), které slouží k zaznamenání vlastnictví digitálních artefaktů, jako jsou například digitální umělecká díla. [24]

Celkově lze říci, že síť Ethereum se v průběhu let vyvinula v jednu z nejvýznamnějších a největších blockchainových platform na světě. A to díky inovativnímu konceptu, možnostem tvorby decentralizovaných aplikací, smart kontraktů, a silnému ekosystému vývojářů a uživatelů. [24]

1.6.12 ETH jako platidlo

Ether (ETH) je kryptoměna využívaná jako platidlo v síti Ethereum. Její hlavní funkce je umožňovat platby za transakce v rámci sítě a také sloužit jako odměna pro těžaře, kteří přispívají k zabezpečení a správě sítě. [24]

Ether je navržen jako digitální token, který je omezený počtem existujících jednotek. Celkový počet ETH je omezen na 18 milionů nových jednotek ročně, což znamená, že množství ETH v oběhu je omezeno. Toto omezení poskytuje mechanismus pro udržení hodnoty ETH a zajišťuje, že nedojde k inflaci množství ETH v oběhu. [24]

Ether je také používán pro placení poplatků za transakce v síti. Tyto poplatky jsou zahrnuty v každé transakci v síti Ethereum a jsou použity k placení těžařům, kteří potvrzují a zpracovávají transakce. Poplatky jsou určovány podle aktuální poptávky a nabídky na síti, což znamená, že v době vysoké poptávky po transakcích jsou poplatky vyšší. [24]

V rámci sítě Ethereum může být ETH také využit pro tvorbu a správu smart kontraktů. Smart kontrakty jsou programy, které jsou uloženy na blockchainu a jsou naprogramovány tak, aby automaticky prováděly určité akce při splnění určitých podmínek. Tyto smart kontrakty mohou být využity k provedení různých operací, jako jsou například transakce, platby a uzavírání obchodů. [24]

Celkově lze tedy říci, že ETH má v síti Ethereum důležitou funkci jako platidlo pro transakce, platbu poplatků a tvorbu a správu smart kontraktů. Jeho omezené množství a průběžně se měnící hodnota jsou klíčovými faktory, které ovlivňují jeho hodnotu na trhu. [24]

1.6.13 Shrnutí výhod a nevýhod

Výhody kryptoměn zahrnují rychlost transakcí, nízké poplatky, bezpečnost a možnost uskutečňovat transakce bez nutnosti používat tradiční finanční instituce. Kryptoměny mohou být přínosné zejména pro lidi, kteří nemají přístup k bankovním účtům. Kromě toho, kryptoměny jsou decentralizované a nejsou ovládány centrálními institucemi.

Nevýhody kryptoměn zahrnují nestabilitu cen a nejistotu kolem jejich hodnoty. Tyto měny jsou stále často spojovány s nelegálními aktivitami, jako jsou praní špinavých peněz. Kromě toho, kryptoměny jsou stále regulovány různými způsoby v různých zemích a existují rizika spojená s používáním této formy digitálního platidla. V poslední době se také objevily otázky týkající se environmentálního dopadu kryptoměn kvůli obrovské spotřebě energie, kterou vyžaduje proces těžby Bitcoinu a dalších kryptoměn.

2 Moderní informační technologie

2.1 Vlastní kryptoměnový token

Motivace pro vytvoření vlastní kryptoměny může být různá. Někteří lidé chtějí vytvořit kryptoměnu jako investiční nástroj, který by mohl mít potenciál pro růst a zisk. Další motivací může být vytvoření kryptoměny, která by se zaměřovala na konkrétní oblast nebo problém a umožňovala snadnou a rychlou platbu za specifické produkty nebo služby.

Cíle vytvoření vlastní kryptoměny se mohou lišit v závislosti na motivaci. Pokud je cílem vytvořit investiční nástroj, může být cílem zajistit co největší růst a stabilitu hodnoty kryptoměny, aby byla atraktivní pro investory. Pokud je cílem vytvoření kryptoměny pro specifický účel, jako například pro platby v určité oblasti, cílem může být poskytnout snadné a rychlé platby za produkty nebo služby.

Dalším cílem může být poskytnout uživatelům více kontrolu nad jejich finančními transakcemi a umožnit decentralizované řízení měny, bez zásahu vlád a finančních institucí. Vytvoření vlastní kryptoměny může také pomoci s rozvojem nových technologií, jako jsou smart kontrakty a blockchain, což může mít potenciál pro využití v různých odvětvích.

2.1.1 Výběr Blockchainu

Výběr vhodné blockchain technologie pro vytvoření vlastní kryptoměny je klíčovým rozhodnutím, které ovlivní celkovou funkčnost, bezpečnost a výkonnost kryptoměny. Existuje mnoho různých blockchain technologií, jako jsou Bitcoin, Ethereum, Solana a mnoho dalších.

Bitcoin (BTC), Solana (SOL) a Ethereum (ETH) jsou tři z nejpobulárnějších blockchain technologií, které se používají pro tvorbu kryptoměn. Zde jsou některé klíčové rozdíly mezi BTC, SOL a ETH, které je třeba zvážít při tvorbě vlastní kryptoměny.

Jedním z kritérií pro výběr správného blockchainu je škálovatelnost neboli počet transakcí za sekundu. BTC a ETH se potýkají s omezenou škálovatelností a mohou zpracovat pouze omezený počet transakcí za sekundu, zatímco SOL nabízí vysokou

škálovatelnost a umožňuje vývojářům vytvářet aplikace, které mohou zpracovávat větší objemy dat.

Dalším z kritérií je samotná rychlost transakcí a zápisu na blockchain. SOL je známý svou rychlostí zpracování transakcí, což z něj dělá ideální volbu pro aplikace, které vyžadují rychlé zpracování dat. BTC a ETH jsou pomalejší a mohou trvat několik minut až hodin, než transakce bude zpracována.

V neposledním řadě je třeba se zaměřit na otázku bezpečnosti samotného blockchainu, kdy BTC a ETH jsou dlouhodobě prověřenou a stabilní technologií s dobrou bezpečností historií, zatímco SOL je novější technologií s méně zkušenostmi.

Nakonec je třeba se zamyslet nad možným budoucím vývojem, kdy ETH a SOL jsou známé pro svou podporu smart kontraktů, které umožňují vývojářům vytvářet složité aplikace a automatizovat transakce.

Výběr mezi BTC, SOL a ETH pro tvorbu vlastní kryptoměny závisí na konkrétním účelu a požadavcích projektu. Pokud je cílem vytvořit digitální měnu, pak BTC a ETH jsou pravděpodobně lepší volbou. Pokud je však cílem vytvořit výkonnou blockchainovou platformu pro aplikace s vysokou škálovatelností a rychlostí, pak SOL by mohl být lepší volbou.

2.1.2 Využití mincí

Vlastní kryptoměna může být využita jako platba za zboží a služby. Můžeme ji integrovat do svého obchodu a umožnit zákazníkům zaplatit za nákup pomocí vaší kryptoměny. Podobně jak Alza integrovala BTC jako validní prostředek platby.

Vlastní kryptoměna může být také využita jako nástroj pro financování projektů. Například, pokud máte projekt, který chcete financovat, můžete vytvořit a prodat svou vlastní kryptoměnu, abychom získali finanční prostředky.

Vlastní kryptoměna může být využita jako nástroj pro odměňování lidí za určité služby. Například, lze odměňovat vlastní zaměstnance kryptoměnou, kterou následně mohou směnít za produkty, které firma vyrábí namísto tvorby různých kuponů.

Vlastní kryptoměnu lze využít jako prostředek pro transakce mezi partnery. Pokud máte partnera v jiné zemi a chcete s ním obchodovat, můžete použít svou vlastní kryptoměnu, abychom snížili náklady na transakce a usnadnili obchodování.

Vlastní kryptoměnu lze také využít jako ziskový nástroj. Například, pokud máme projekt, který má potenciál růstu, můžeme vytvořit a prodat svou vlastní kryptoměnu, abychom následně získali zisk z růstu hodnoty mince, která se opírá o růst projektu.

Tyto příklady ukazují, že vlastní kryptoměna může být využita pro mnoho různých účelů a může poskytovat řadu výhod pro uživatele. Je však důležité mít na paměti, že úspěch využití vlastní kryptoměny závisí na mnoha faktorech, jako jsou tržní podmínky, konkurence a efektivní marketingová strategie.

2.1.3 Vytvoření kryptoměny

Ze všeho nejdříve je potřeba vytvořit prostředí ve kterém, lze danou kryptoměnu vytvořit. Osobně jsem si pro ukázkou vybral Solanu a to z důvodu, že Solana má nejrychlejší odezvu ze všech kryptoměn na trhu a nejnižší poplatky. Důvod, proč jsou poplatky v rámci halířů a celková rychlost transakcí je díky své škálovatelnosti, která je na velmi vysoké úrovni.

Samotná Solana network funguje na programovacím jazyku, který se jmenuje Rust. Jedná se o moderní, bezpečný a vysoko výkonný programovací jazyk, který byl vyvinut pro internetový prohlížeč Mozilla. Jeho hlavním zaměřením je poskytnout vývojářům nástroje, které umožní psát vysoko výkonný a spolehlivý kód. Rust byl navržen tak, aby řešil některé z největších problémů, které trápí vývojáře v jiných jazycích, jako jsou chyby v paměti, datové závislosti a další. Jedním z nejvýraznějších rysů Rustu je jeho bezpečnost. Rust přináší nové přístupy k řešení problémů v paměti, což umožňuje vývojářům psát kód bez starostí o chyby v paměti, které jsou častou příčinou zranitelností a bezpečnostních incidentů. Dalším významným rysem Rustu je jeho podpora pro souběžné programování. Rust obsahuje nástroje, které usnadňují psaní souběžného kódu, což umožňuje vývojářům psát vysoko výkonné programy, které mohou využívat více procesorů a jader. [25]

Osobně celý proces v rámci testování a zkoušení různých příkazů a stahování knihoven, které jsou z mnohdy pochybný zdrojů, provádím na virtuálním počítači s Linuxem. Konkrétně s verzí Ubuntu 21.10, která je momentálně nejnovější. Po vytvoření virtuálního počítače je třeba stáhnout aktuální drivery. To lze jednoduše udělat skrze příkaz: `sudo apt update`. Následně je potřeba stáhnout cargo package s nejnovější nástroji, které Solana Network využívá. Což lze udělat jednoduše zadáním příkazu níž.

```
sh -c "$(curl -sSfL https://release.solana.com/v1.15.2/install)"
```

Následně po nainstalování všech potřebných nástrojů je třeba virtuální počítač třeba restartovat pro správné chování všech nově stažených nástrojů.

Dalším krokem je vytvoření prvotní peněženky, která slouží k placení poplatků za založení tokenu, vytvoření mincí a následné transakce. Poplatky jsou v rámci halířů a jsou odvozeny od vytíženosti blockchainů. Prvotní peněženku lze jednoduše vytvořit pomocí příkazu:

```
solana-keygen new
```

Tento příkaz následně udělá několik věcí. První tou hlavní vytvoří pro nás ve virtuálním počítači json soubor, který uchovává tzv. seed, tento seed slouží jako privátní klíč, jenž se následně kombinuje s naším veřejným klíčem. Veřejný klíč je ten, s kterým budeme nadále operovat a skrze něj posílat kryptoměny.

Seed kryptoměnové peněženky je důležité uchovávat v bezpečí, protože se jedná o klíč k veškerým kryptoměnovým prostředkům. Seed obvykle sestává z 12 až 24 slov, které slouží k obnově peněženky v případě ztráty nebo poškození. Existuje několik možností pro uchovávání seedu.

Seed můžete napsat na kus papíru a uschovat na bezpečném místě. Tento způsob je bezpečný, protože se seed nenachází na internetu a nemůže být hacknut, ale existuje riziko ztráty nebo poškození papíru.

Hardwarové peněženky jsou fyzická zařízení, která uchovávají seed offline. Tento způsob je velmi bezpečný, protože seed není nikdy uložen online a není tedy ohroženo hackery.

Pokud používáte online peněženku, seed by měl být uložen v bezpečném souboru na vašem počítači a měl by být chráněn heslem. Pokud však máte podezření na kompromitaci vašeho počítače nebo hesla, měli byste okamžitě převést své kryptoměny na jinou adresu a zabezpečit své seed novým heslem.

Seed může být rozdělen na více částí a uložen na různých místech, aby se minimalizovalo riziko ztráty nebo krádeže. V tomto případě musíte zajistit, aby každá část byla uložena v bezpečí a že máte přístup ke všem částem, když budete chtít obnovit svou peněženku.

Po uložení privátního klíče je potřeba na náš veřejný klíč poslat kryptoměnu, která bude složít jako úhrada na poplatky spojené s využíváním Solana Network blockchainu. K tomu je potřeba si vytvořit účet na burze.

Nejznámější a nejpoužívanější burza kryptoměn, která se momentálně využívá, je Coinbase. Na této burze samotný účet funguje jako kryptoměnová peněženka, přes kterou můžeme zakoupit a následně poslat kryptoměnu do peněženky, skrze náš veřejný klíč, na virtuálním počítači. Není potřeba nijak vysoký obnos, stačí zakoupit a poslat minimální možný počet pro transakci pro poslání, což zde na burze je SOL v hodnotě 35 korun.

Pro další pracování a tvoření změn do blockchainu je třeba stáhnout balíček nástrojů Rustu. To lze jednoduše udělat skrze příkaz:

```
curl https://sh.rustup.rs -sSf | sh
```

Následně je potřeba nainstalovat linuxové developerské nástroje, které nesmírně ulehčují celou práci s následným vytvořením vlastní kryptoměny. Nástroje lze nainstalovat skrze příkazy:

```
sudo apt install libudev-dev  
sudo apt install libssl-dev pkg-config -y  
sudo apt install build-essential -y
```

Když se spustí aplikace, která potřebuje komunikovat s periferním zařízením, například kryptoměnovou peněženkou, knihovna libudev-dev umožňuje aplikaci získat informace o připojených zařízeních. Aplikace může získat informace o zařízení pomocí jeho identifikátorů, například pomocí identifikátoru USB rozhraní, identifikátoru Bluetooth zařízení nebo identifikátoru sériového portu. V našem případě se jedná o veřejný a privátní klíč.

Knihovna libudev-dev poskytuje sadu funkcí, které umožňují aplikaci získávat informace o periferních zařízeních, jako jsou například seznamy připojených zařízení, jejich vlastnosti a informace o stavech zařízení. Tyto funkce umožňují aplikaci dynamicky reagovat na změny v konfiguraci periferních zařízení.

V případě kryptoměnových peněženek knihovna libudev-dev umožňuje aplikaci komunikovat s připojenou peněženkou a provádět transakce s kryptoměnami. Aplikace může použít informace poskytované knihovnou k ověření, že komunikuje s kryptoměnovou peněženkou a že provádí platbu kryptoměnou na správný účtu.

Libssl-dev je balíček pro Ubuntu, který obsahuje soubory a knihovny pro OpenSSL. OpenSSL je open-source implementace protokolů SSL a TLS, které zajišťují šifrování pro komunikaci přes internet.

Konkrétněji, OpenSSL poskytuje funkce pro vytváření a ověřování digitálních certifikátů, šifrování dat pomocí různých kryptografických algoritmů, včetně symetrických a asymetrických, a také pro kontrolu integrity a autenticity dat pomocí hashovacích funkcí. Tyto funkce jsou velmi důležité pro zabezpečení komunikace mezi klientem a serverem, například v internetových bankovních aplikacích, komunikačních aplikacích nebo kryptoměnových aplikacích.

V souvislosti s kryptoměny se libssl-dev často používá v různých aplikacích, jako jsou kryptoměnové peněženky, kryptoměnové burzy nebo miningové programy. Tyto aplikace používají OpenSSL pro zabezpečení komunikace mezi uživatelem a blockchainem nebo peněženkou.

Build-essential je balíček softwarových nástrojů pro kompilaci a sestavování aplikací v operačním systému Ubuntu nebo jiném systému založeném na Debianu. Tento balíček obsahuje základní nástroje potřebné pro kompilaci aplikací, včetně překladačů, knihoven a dalších nástrojů, které jsou nezbytné pro vývoj softwaru v jazyce C a dalších jazycích.

Dalším krokem je stáhnutí všech potřebných zdrojových kódů a nástrojů pro samotnou manipulaci s veřejným blockchainem Solany. Instalace toho balíčku se provádí skrze příkaz:

```
cargo install spl-token-cli
```

Jedná se o opravdu velký balíček, který trvá několik desítek minut na nainstalování, ale je nezbytný pro jakoukoliv následnou práci s blockchainem. Následně už nezbyvá nic jiného než vytvořit vlastní kryptoměnu. Pro vytvoření kryptoměny stačí zadat následující příkaz:

```
spl-token create-token
```

Tento příkaz vytvoří samotnou kryptoměnu, jenž vypadá jako shluk náhodných čísel a písmen: "7Hcs4RFNaf4esNu4SN8WmyauCntkvT8ryct2fmH84X1F". Což takto samo o sobě nijak vábně nevypadá, ale jedná se o adresu, díky které můžeme danou kryptoměnu najít na samotném blockchainu. Tato adresa je již nenávratně zapsána do blockchainu a nelze ji nijak vymazat.

Nadále je potřeba vytvořit peněženku pro novou kryptoměnu, která bude sloužit pro další distribuci nové kryptoměny. Vytvořit takovou peněženku můžeme skrze příkaz:

```
spl-token create-account adresa kryptoměny  
(7Hcs4RFNaf4esNu4SN8WmyauCntkvT8ryct2fmH84X1F)
```

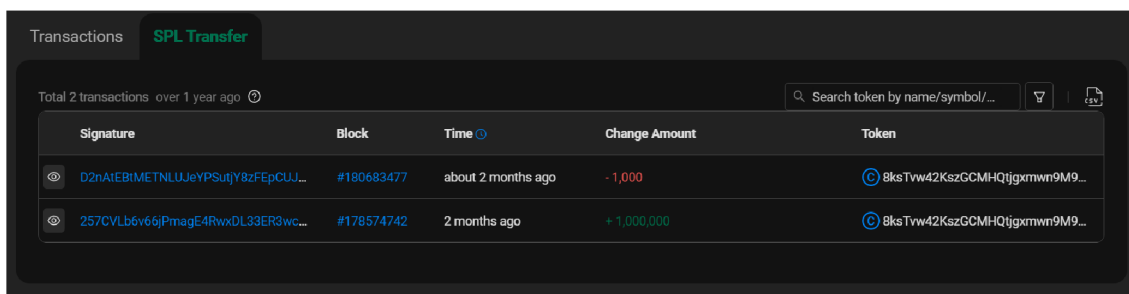
Poslední, co zbývá je vytvořit samotné mince. Mince lze jednoduše vytvořit skrze příkaz:

```
spl-token mint adresa tokenu (7Hcs4RFNaf4esNu4SN8WmyauCntkvT8ryct2fmH84X1F)  
počet mincí (ku příkladu 100 000) veřejný klíč peněženky
```

Tímto krokem jsme vytvořili sto tisíc mincí, které následně můžeme rozdistribuovat na jakoukoliv jinou peněženku podporující kryptoměnu SOL. Mince můžeme rozesílat skrze příkaz:

```
spl-token transfer --fund-recipient --allow-unfunded recipient  
7hcs4RFNaf4esNu4SN8WmyauCntkvT8ryct2fmH84X1F (tokenová adresa) 20 (počet  
mincí které chceme poslat) CE4uDb9Zoghe7xFtRhBpoMVxfVo6UZ4uj4oQfVwph5zY  
(adresa peněženky na kterou chceme kryptoměnu poslat)
```

Pokud transfer byl úspěšný, tak redistribuované mince by měly být během pár sekund na zadané peněžence. Toto si můžeme ověřit v samotné peněžence anebo na stránkách třetích stran jako je solana.fm apod., které sbírají veškerá data o pohybu na blockchainu.



The screenshot shows a transaction history for 'SPL Transfer' on Solana Explorer. It displays two transactions:

Signature	Block	Time	Change Amount	Token
D2nA1EBIMETNLUJeYPSutjY8zFepCUJ...	#180683477	about 2 months ago	-1,000	8ksTvw42KszGCMHQ1jgxmwn9M9...
257CVLb6v6jPmagE4RwxDL33ER3wc...	#178574742	2 months ago	+1,000,000	8ksTvw42KszGCMHQ1jgxmwn9M9...

Obr. 2.1 Výstup vytváření kryptoměny

Zdroj: vlastní zpracování z [26]

2.1.4 Zosobnění vlastní kryptoměny

Následný krok je relativně dobrovolný a tím je pojmenování a nahrát profilovou fotku naší kryptoměny. Momentálně se naše kryptoměna nachází ve stavu, kdy je nerozeznatelná a dohledatelná pouze skrze adresu tokenu.

Vzhledem ke změnám, které před pár měsíci hlavní vývojáři udělali, již nelze měnit název a profilovou fotku skrze fork na githubu. Tuto změnu udělali kvůli automatizaci

a možnosti automatického upravování vlastních kryptoměn bez nutnosti čekat na schválení od správců na githubu.

Pro změnu je potřeba nějaký programovací nástroj využívající programovací jazyk TypeScript. Osobně využívám program Visual studio code od Microsoftu. Mimo tohoto programu je třeba stáhnout nejnovější Node.js, což jsou ovladače a nástroje pro operace s JavaScriptem. A následně je třeba ve Windows terminálu potřeba stáhnout přídatné balíčky pro Node.js a to konkrétně těmito příkazy:

```
npm install -g ts-node  
npm install -g typescript
```

Tyto přídatné balíčky umožňují spouštět příkazy tvořené v TypeScriptu přímo do nodů Javascriptu. Následně je potřeba napsat kód, který nám dovoluje dělat změny přímo na samotném blockchainu. V následující ukázce je script, který se napojuje do blockchainu a upravuje hodnoty vlastní kryptoměny.

```

import * as mpl from "@metaplex-foundation/mpl-token-metadata";
import * as web3 from "@solana/web3.js";
import * as anchor from '@project-serum/anchor';
export function loadWalletKey(keypairFile: string): web3.Keypair {
1   const fs = require("fs");
2   const loaded = web3.Keypair.fromSecretKey(
3     new Uint8Array(JSON.parse(fs.readFileSync(keypair-
4 File).toString())));
5   return loaded;}
6 async function main() {
7   console.log("Kontrola");
8   const myKeypair = loadWalletKey('C:\\Users\\Desk-
9 top\\krypto\\src\\key.json')
10  console.log(myKeypair);
11  console.log(myKeypair.publicKey.toBase58())
12  const mint = new web3.PublicKey("CE4uDb9Zoghe7xFtRhBpoMVx-
13 fVo6UZ4uj4oQfVwph5zY")
14  const seed1 = Buffer.from(anchor.utils.bytes.utf8.encode("meta-
15 data"));
16  const seed2 = Buffer.from(mpl.PROGRAM_ID.toBytes());
17  const seed3 = Buffer.from(mint.toBytes());
18  const [metadataPDA, _bump] = web3.PublicKey.findProgra-
19 mAddressSync([seed1, seed2, seed3], mpl.PROGRAM_ID);
20  const accounts = {
21    metadata: metadataPDA,
22    mint,
23    mintAuthority: myKeypair.publicKey,
24    payer: myKeypair.publicKey,
25    updateAuthority: myKeypair.publicKey,}
26  const dataV2 = {
27    name: "VS logistiky",
28    symbol: "$VSLG",
29    uri: "https://raw.githubusercontent.com/vslg_crypto/main/meta-
30 data.json",
31    sellerFeeBasisPoints: 0,
32    creators: null,
33    collection: null,
34    uses: null}
35  const args = {
36    createMetadataAccountArgsV2: {
37      data: dataV2,
38      isMutable: true
39    }
40  };
41  const ix = mpl.createCreateMetadataAccountV2Instruction(accounts,
42  args);
43  const tx = new web3.Transaction();
44  tx.add(ix);
45  const connection = new web3.Connection("https://api.mainnet-beta.so-
46 lana.com");
47  const txid = await web3.sendAndConfirmTransaction(connection, tx,
48  [myKeypair]);
49  console.log(txid);}
50  main();

```

První tři řádky slouží pro import balíčků, které pomáhají kódu správné fungování. První příkaz importuje balíček "mpl-token-metadata" od Metaplex Foundation, což je knihovna pro práci s metadaty digitálních aktiv a tokenů na blockchainu Solana. V této knihovně jsou definovány různé typy a funkce pro práci s těmito metadaty.

Druhý příkaz importuje balíček "solana/web3.js", jenž je knihovna pro práci s blockchainem Solana. Tato knihovna poskytuje různé funkce a typy, jako například vytváření Solana účtů, podepisování transakcí a další.

Třetí příkaz importuje balíček "project-serum/anchor", jedná se o knihovnu pro tvorbu decentralizovaných aplikací na blockchainu Solana. Tato knihovna poskytuje různé funkce pro vytváření a ovládání programů, jako jsou například smart kontrakty, na Solana blockchainu.

Začínáme s funkcí "loadWalletKey", která načte privátní klíč primární peněženky naší kryptoměny ze souboru ve virtuálním PC. Funkce bere jeden argument "keypairFile", což je řetězec, který představuje cestu k souboru s privátním klíčem na virtuální PC.

V této funkci se nejprve importuje modul file systému z nodu, který umožňuje čtení a zápis souborů. Poté se spustí "readFileSync", která načte obsah souboru synchronně, tj. program bude čekat, dokud se soubor neotevře a nenačte jeho obsah do paměti. Funkce "toString()" pak převede načtená data na řetězec.

Načtený řetězec obsahuje privátní klíč ve formátu "JSON". Tento klíč se pak převede na čitelnou verzi pro TypeScript a použije se jako argument pro vytvoření nového klíčového páru web3.Keypair pomocí metody "fromSecretKey()". Tento krok umožňuje podepsání nového kontraktu na blockchainu, aby ho předala dál pro následné potvrzení.

Funkce "loadWalletKey", načte privátní klíč účtu. Tento klíč se používá k autentizaci transakce, která vytváří nový token. Dále se vytvoří nová instance web3.PublicKey, což je veřejný klíč cílového účtu, který má být naplněn novými tokeny.

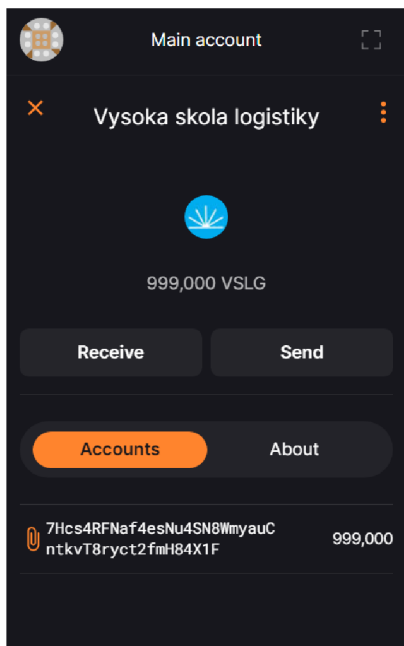
Poté se vytváří několik seedů pomocí bufferů, které se používají k výpočtu veřejné adresy programu. Tyto seedy se pak používají k výpočtu veřejné adresy programu a účtu pro metadata pomocí metody "findProgramAddressSync()".

Poté se vytvoří objekt accounts, který obsahuje údaje o účtech, které se používají v transakci. Tyto účty jsou poté použity k vytvoření nových tokenů pomocí metody

"createCreateMetadataAccountV2Instruction()", která vytváří instrukci pro program Metaplex na vytvoření nových tokenů s konkrétními metadaty.

Vytvořená instrukce se pak přidá do nové transakce. Tato transakce se podepíše privátním klíčem. Nakonec se pomocí instance "web3.Connection" připojíme na blockchain a transakce se odešle pomocí "sendAndConfirmTransaction()". Funkce main vypíše ID transakce, aby uživatel mohl ověřit, že transakce byla úspěšně odeslána na blockchain a byla zpracována.

Celkově tedy tento kód vytváří a odesílá transakci na Solana blockchain, která vytváří nový token s metadata informacemi o naší kryptoměně a umožňuje ji zosobnit. Zjednodušeně zosobnění kryptoměny lze docílit pomocí této funkce "createCreateMetadataAccountV2Instruction()" ze specifikovaných dat a účtů jako je adresa kryptoměny, privátní a veřejný klíč. Privátní klíč účtu, který se používá k podepisování transakce, je načítán ze souboru pomocí funkce "loadWalletKey()" umístěném ve virtuálním počítači. V případě úspěchu se vypíše ID transakce, čímž se potvrdí úspěšné nahrání dodatečných informací na blockchain.



Obr. 2.2 Výstup vlastní kryptoměny

Zdroj: vlastní zpracování

2.1.5 Distribuce mincí

Jednou z možností distribuce kryptoměn je forma "Initial Coin Offering" (ICO). Jedná se o proces, při kterém vývojáři kryptoměny prodávají mince potenciálním investorům výměnou za jiné kryptoměny, jako je například Bitcoin nebo Ethereum. Tyto mince jsou obvykle prodávány za speciální cenu nebo s různými slevami pro brzké investory.

Další z často využívaných možností je Airdrop. Jde o proces, při kterém vývojáři kryptoměny rozdávají zdarma mince nebo tokeny určitému počtu uživatelů, kteří splňují určitá kritéria, jako je například následování určitého účtu na sociálních sítích nebo registrace na webové stránce.

Některé málo známé burzy umožňují nabídku nových projektů, které následně mají možnost tyto burzy využít jako startovací můstek pro velké a frekventované burzy. Distribuce mincí kryptoměny na burze zahrnuje nabídku mincí kryptoměny k nákupu na burze, což umožňuje lidem nakoupit mince kryptoměny výměnou za fiat měnu nebo jiné kryptoměny.

2.2 Smart kontrakty

Smart kontrakty jsou digitální programy uložené na blockchainu, které umožňují automatické vykonávání podmínek a pravidel. Tyto kontrakty jsou programovány tak, aby se provedly automaticky, jakmile jsou splněny předem definované podmínky. Mohou být použity k provedení různých operací, jako jsou například transakce, platby a uzavírání obchodů. [27]

Smart kontrakty jsou navrženy tak, aby byly transparentní, nezpochybnitelné a nezměnitelné. Jsou uloženy v blockchainu, což znamená, že jsou viditelné a přístupné pro každého, kdo má přístup k blockchainu. Smart kontrakty jsou také nezpochybnitelné a nezměnitelné, protože jsou zapsány v blockchainu a každá změna by vyžadovala změnu celého blockchainu. [27]

Smart kontrakty umožňují lidem provádět obchody a transakce bez potřeby tradičních prostředníků, jako jsou například banky a notáři. Tyto kontrakty umožňují snížení nákladů a času potřebného k dokončení obchodu, protože jsou plně automatizované a nevyžadují zprostředkovatele. [27]

Smart kontrakty také zvyšují důvěru mezi účastníky obchodu, protože jsou programovány tak, aby se provedly pouze v případě splnění předem stanovených podmínek. To znamená, že každý účastník obchodu ví, co může očekávat a jaká jsou pravidla. Smart kontrakty také umožňují snadnější dodržování zákonů a předpisů. [27]

Příkladem použití smart kontraktů mohou být například uzavírání pojištění, kde smart kontrakt automaticky vyplácí náhrady v případě, že se stane určitá událost, například havárie vozidla. [27]

Smart kontrakty se stávají stále důležitější součástí blockchainových sítí, jako je Ethereum, a jejich využití má obrovský potenciál. Vývoj smart kontraktů v síti Ethereum se soustředí na rozšíření funkcionality a zlepšení efektivity. V současné době se pracuje na vylepšení programovacího jazyka Solidity, který je používán pro psaní smart kontraktů. To by mělo vést ke zlepšení bezpečnosti a zjednodušení psaní smart kontraktů. [27]

Další vývoj v oblasti smart kontraktů se zaměřuje na využití umělé inteligence a strojového učení k vylepšení efektivity a automatizace. Tyto technologie by mohly umožnit vytvoření smart kontraktů, které jsou schopny učit se a přizpůsobovat se různým podmínkám a situacím. [27]

S vývojem smart kontraktů se také vynořují nové možnosti pro využití blockchainu a decentralizace. Smart kontrakty mohou pomoci vytvořit nové ekonomické modely a způsoby spolupráce, které jsou decentralizované a autonomní. To může vést k vytvoření nových možností pro rozvoj aplikací, podnikání a dalších oblastí. [27]

V současné době se vývoj smart kontraktů zaměřuje na vylepšení jejich bezpečnosti, efektivity a automatizace. S rostoucím využitím blockchainu a decentralizace se očekává, že bude stále více příležitostí pro využití smart kontraktů v různých oblastech. [27]

2.3 DApps

DApps (Decentralized Applications) jsou aplikace postavené na blockchainových sítích, jako je Ethereum. Tyto aplikace se liší od tradičních aplikací tím, že jsou decentralizované a provozovány na blockchainu, což znamená, že jsou nezávislé na jakémkoliv centrálním autoritářském systému. Tento decentralizovaný charakter dApps přináší řadu výhod, jako je větší bezpečnost, transparentnost. [24]

DApps mohou být použity v mnoha oblastech, jako jsou finance, hry, sociální sítě, tržště, pojištění a další. Mezi nejvýznamnější příklady dApps patří Uniswap, Aave, Compound a MakerDAO v oblasti financí, CryptoKitties a Decentraland v oblasti her. Status a Brave v oblasti sociálních sítí a webových prohlížečů. [24]

Jednou z nejvýznamnějších výhod je zvýšená bezpečnost. Díky blockchainové technologii jsou data v dApps uložena a ověřována mnoha uživateli, což zvyšuje jejich transparentnost a důvěryhodnost. [24]

DApps také nabízejí možnosti financování a spolupráce mezi uživateli. Provozovatelé dApps mohou financovat své projekty pomocí tzv. "Initial Coin Offerings" nebo tokenů. Uživatelé mohou investovat do projektů, které se jim líbí, a využívat služeb, které nabízejí. Takto vznikají nové ekonomické modely, které jsou založeny na spolupráci a decentralizaci. [24]

Význam dApps stále roste, a to zejména díky rostoucímu zájmu o blockchainovou technologii a decentralizaci. DApps nabízejí nové možnosti pro využití blockchainu v různých oblastech a mohou přinést významné inovace do tradičních průmyslových odvětví. Například v oblasti financí mohou dApps umožnit nové způsoby pro peer-to-peer platby, nebo automatizované investování a obchodování. V oblasti zdravotnictví a farmacie mohou dApps pomoci vylepšit řízení lékařských záznamů a poskytovat bezpečný přístup k citlivým zdravotním datům. [24]

DApps také přinášejí nové příležitosti pro tvorbu a využívání digitálních aktiv a tokenů, což může vést k vzniku nových ekonomik a podniků, které jsou založené na blockchainové technologii. Například dApps mohou umožnit vytvoření decentralizovaných tržšť pro nákup a prodej digitálního obsahu, jako jsou hudba, filmy nebo digitální umění. [24]

V neposlední řadě mají dApps také potenciál přinést významné inovace do oblasti sociálních sítí a komunikace. Například mohou umožnit nové způsoby pro bezpečné a soukromé sdílení informací a komunikaci mezi uživateli. [24]

2.4 NFT

NFT (Non-Fungible Token) je speciální druh kryptoměnového tokenu, který reprezentuje unikátní digitální aktivum. Zatímco běžné kryptoměnové tokeny jsou fungibilní a vzájemně zaměnitelné (jeden bitcoin je stejný jako jiný bitcoin), NFT jsou neopakovatelné a mají jedinečné vlastnosti a charakteristiky. [24]

NFT jsou používány k tokenizaci digitálních aktiv jako jsou například digitální umělecká díla, videa, hudba, hry, virtuální pozemky a další digitální obsah. Tyto aktivity jsou poté uloženy na blockchainu a stávají se tak jedinečnými, neopakovatelnými a ověřitelnými.

Každé NFT má svůj vlastní digitální identifikátor, který je uložen v blockchainu. Tento identifikátor obsahuje informace o aktivu, jako jsou jeho unikátní vlastnosti, historie vlastnictví a další metadatové informace. Vlastnictví NFT může být převedeno mezi uživateli pomocí kryptoměnových transakcí, což umožňuje obchodování s digitálními aktivy. [24]

NFT jsou využívány v různých oblastech, například v umění a designu. Digitální umělecká díla mohou být tokenizována jako NFT a následně prodávána na speciálních platformách pro digitální umění. NFT jsou také využívány v herním průmyslu, kde hráči mohou vlastnit unikátní digitální předměty a postavy, a v oblasti virtuální reality, kde mohou být tokenizovány virtuální pozemky a budovy. [24]

Mezi nejznámější platformy pro NFT patří například OpenSea, Rarible a SuperRare. Tyto platformy umožňují uživatelům nakupovat, prodávat a obchodovat s NFT. S rostoucím zájmem o digitální aktiva a blockchainovou technologii se očekává, že využití NFT bude dále růst. [24]

2.4.1 Příklady

CryptoKitties – první úspěšný NFT projekt, který umožňuje sbírání a chov digitálních koček.

NBA Top Shot – projekt, který nabízí digitální sběratelské karty s videoklipy z nejlepších okamžiků v historii NBA.

Decentraland – virtuální svět, kde jsou pozemky digitálními aktivy, které lze vlastnit jako NFT a využívat pro vytváření digitálních domů, podobně jako je tomu u hry The Sims.

Axie Infinity – hra, která umožňuje hráčům chovat a bojovat s digitálními bytostmi zvanými Axies, které jsou NFT.

Art Blocks – projekt, který umožňuje umělcům vytvářet unikátní digitální umělecká díla, která jsou NFT a mohou být vlastněna a obchodována.

Bored Ape Yacht Club – projekt, který nabízí sbíratelské digitální obrazy s postavami opic. Tento projekt se stal velmi populárním mezi sběrateli NFT.

3 Typové příklady využití

V logistice se blockchain může využít pro zlepšení transparentnosti, bezpečnosti, efektivity a spolupráce v celém logistickém řetězci. Blockchain může v logistice výrazně zlepšit transparentnost, bezpečnost, efektivitu a spolupráci v celém logistickém řetězci.

3.1 Sledování zásilek

Sledování zásilek je jedním z klíčových procesů v logistice, který umožňuje zákazníkům a logistickým firmám získat přesné informace o tom, kde se zásilka momentálně nachází a jakým způsobem se pohybuje. Blockchain může poskytnout vysokou úroveň transparentnosti a spolehlivosti pro sledování zásilek a umožnit vytvoření decentralizovaného systému, který by mohl být použit v celém logistickém řetězci. [28]

Základem tohoto systému by byly smart contracts. Tyto smlouvy by se používaly pro každou transakci a událost v cyklu zásilky, a to od okamžiku, kdy je zásilka přijata k odeslání, až po okamžik, kdy je doručena. Smart contracts by umožnily automatické zaznamenávání a ověřování každé transakce a události v blockchainu, což by vytvořilo transparentní a bezpečný systém sledování zásilek. [28]

Když je zásilka přijata k odeslání, mohou být vytvořeny smart contracts, které obsahují informace o zásilce, jako jsou například její váha, rozměry a cílová adresa. Tyto informace by byly zaznamenány v blockchainu a odesílatelé by obdrželi jedinečný kód, který by umožnil sledování zásilky. Když je zásilka předána dopravci, mohou být vytvořeny další smart contracts, které by zaznamenaly předání zásilky a informace o dopravci. Každá transakce by obsahovala datum, čas, místo a další údaje, které by byly ověřeny a zapsány v blockchainu. [28]

Při překonávání různých etap cesty by byly vytvářeny další smart contracts, které by zaznamenávaly transakce mezi jednotlivými aktéry v logistickém řetězci, jako jsou přepravní společnosti, celní úřady, skladovací společnosti a další. Tyto smart contracts by umožnily zaznamenávat a ověřovat přesné informace o tom, kde se zásilka nachází, jaké trasy projela a kdo se o ni staral. [28]

Když je zásilka doručena, mohou být vytvořeny další smart contracts, které by zaznamenaly doručení zásilky a informace o příjemci. Tyto informace

by byly zaznamenány v blockchainu a příjemce by obdržel potvrzení o doručení zásilky. Tento proces by umožnil logistickým firmám a zákazníkům sledovat zásilky v reálném čase, což by usnadnilo správu zásilek a zlepšilo celkovou transparentnost a spolehlivost logistického řetězce. [28]

Důležité je také zmínit, že blockchain by umožnil snadné zaznamenávání a ověřování informací o zásilce, což by mohlo pomoci při řešení problémů, jako jsou ztracené nebo poškozené zásilky. Pokud by se vyskytl problém, bylo by možné v blockchainu najít přesné informace o tom, kde a kdy k problému došlo, a kdo byl zodpovědný za danou transakci nebo událost. Využití blockchainu pro sledování zásilek by tedy mohlo zlepšit efektivitu a transparentnost logistického řetězce a zvýšit spokojenost zákazníků. [28]

3.1.1 Příklad

Jedním z příkladů využití blockchainu v logistice je projekt IBM Food Trust, který umožňuje sledování potravinových produktů od zemědělských podniků až po spotřebitele. Tento projekt využívá blockchain k vytvoření decentralizovaného a transparentního systému pro sledování potravin v celém logistickém řetězci. [29]

Každá transakce v logistickém řetězci je zaznamenána v blockchainu, což umožňuje firmám a spotřebitelům sledovat původ potravin, jak byly zpracovány a jak byly distribuovány. Díky tomuto systému mohou spotřebitelé získat přesné informace o tom, kde byly potraviny pěstovány a jak dlouho trvalo, než se dostaly na police obchodů. [29]

Tento projekt již funguje v několika společnostech, jako je například Nestlé a Walmart. Projekt IBM Food Trust také pomáhá firmám lépe kontrolovat kvalitu potravin, snižovat náklady na skladování a zlepšovat řízení rizik v celém logistickém řetězci. [29]

3.2 Fakturace a platby

Blockchain může být využit k zabezpečení těchto procesů a zlepšení jejich efektivitu a spolehlivosti. Jedním z možných způsobů, jak využít blockchain pro fakturaci a platby, je vytvoření smart kontraktů. Tyto smart kontrakty by byly vytvořeny před provedením transakce a obsahovaly by informace o platbách, datumu splatnosti a další relevantní informace. Tyto smart kontrakty by byly následně uloženy v blockchainu, což by zajistilo, že informace o transakci jsou zabezpečeny a nebylo by možné je pozměnit. [30]

Pokud by byla transakce provedena, smart kontrakt by automaticky provedl platbu a informace o platbě by byly uloženy v blockchainu. Tento proces by umožnil oběma stranám transakce přístup k informacím o transakci a zabezpečil by celý proces fakturace a platby. [30]

Další možností, jak využít blockchain pro fakturaci a platby, je vytvoření decentralizovaného systému, který umožní rychlou a bezpečnou výměnu informací a peněz mezi obchodními partnery. Tento systém by umožnil rychlejší a efektivnější zpracování transakcí a snížil by náklady na platební služby a poplatky za transakce. [30]

3.2.1 Příklad

Jedním z příkladů využití blockchainu pro fakturaci a platby je projekt We.trade, který byl vyvinut společnostmi IBM, Deutsche Bank, HSBC, KBC, Natixis, Nordea, Rabobank, Santander a Societe Generale. [31]

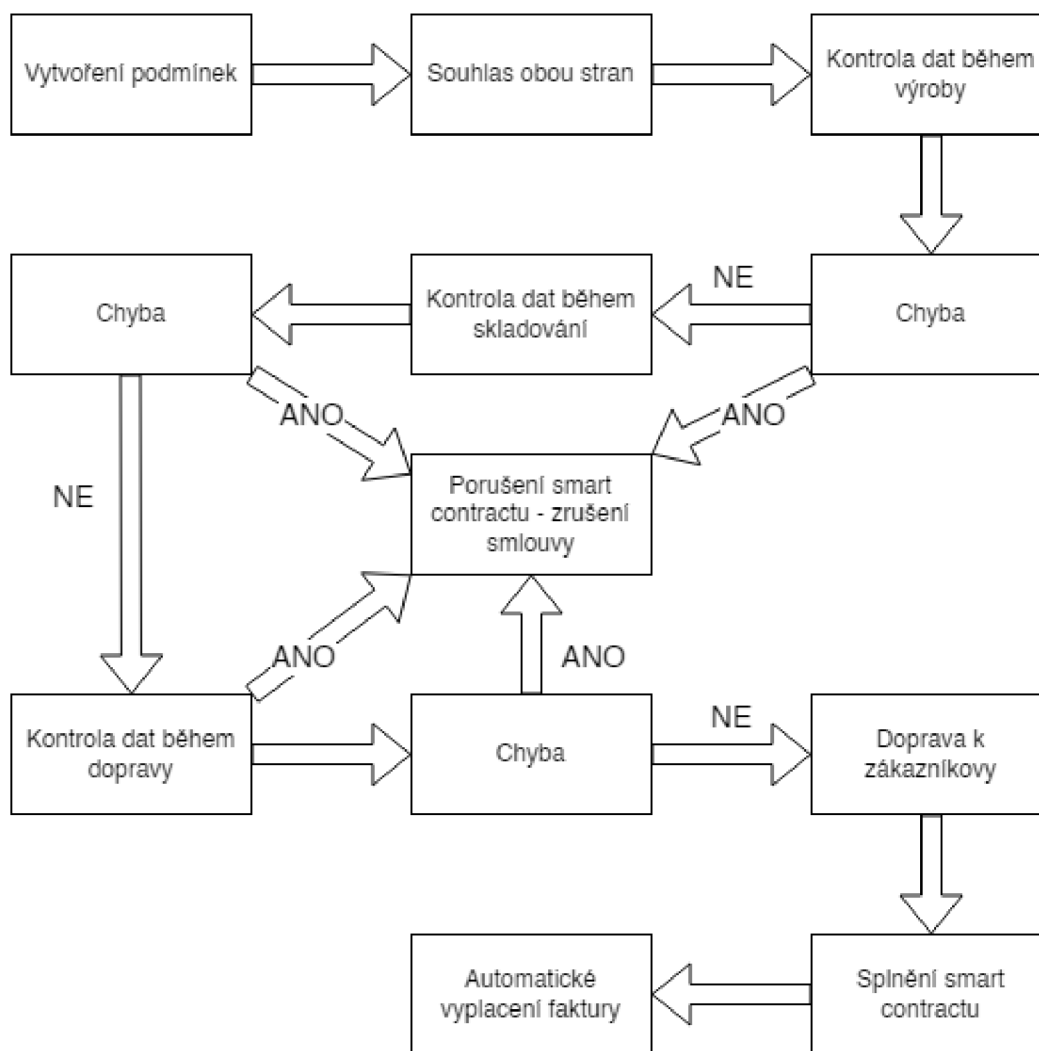
We.trade je decentralizovaným obchodním systémem, který využívá blockchain pro zabezpečení transakcí a zlepšení procesu fakturace a platby. Tento systém umožňuje malým a středním podnikům snadno a bezpečně obchodovat s partnery po celém světě.

Když se podnik rozhodne použít We.trade, musí se nejprve zaregistrovat na platformě a ověřit svou identitu. Poté může vytvořit objednávku a odeslat ji svému obchodnímu partnerovi. Systém We.trade pak vytvoří smart kontrakt, který obsahuje informace o platbě, datumu splatnosti a další relevantní informace. [31]

Obchodní partner poté přijme objednávku a potvrdí ji. Jakmile jsou obě strany transakce spokojeny s podmínkami, systém We.trade automaticky provede platbu a digitální měny, která je uložena v blockchainu. Tento proces umožňuje snadnou a bezpečnou výměnu peněz mezi obchodními partnery a eliminuje riziko podvodů a nedorozumění. [31]

Další výhodou projektu We.trade je to, že umožňuje sledovat celý proces obchodní transakce, včetně fakturace a platby, v reálném čase. To znamená, že obě strany transakce mají přístup ke všem informacím o transakci a mohou sledovat stav transakce kdykoliv během procesu. [31]

Projekt We.trade tedy ukazuje, jak může být blockchain využit k zlepšení procesu fakturace a platby, a přinést výhody pro malé a střední podniky, které se snaží rozšířit své obchodní aktivity na mezinárodní úrovni. [31]



Obr. 3.1 Diagram zapojení blockchainu

Zdroj: vlastní zpracování

3.3 Řízení skladů

Blockchain může také pomoci zlepšit řízení skladů v logistice. Díky systému správy skladů lze snadno sledovat zásoby a jejich pohyb mezi jednotlivými body logistického řetězce, což může pomoci zlepšit efektivitu a snížit náklady. [32]

Prvním krokem k efektivnějšímu řízení skladů je digitalizace dat o zboží. Tyto informace mohou být ukládány do blockchainu, což zaručí, že jsou vždy aktuální a spolehlivé. Například lze vytvořit smart kontrakt, který bude obsahovat informace o objednavce, včetně názvu produktu, množství, ceny a adresy doručení. [32]

Blockchain může pomoci při sledování zásilek od místa výroby až po místo určení. Tento proces může být zabezpečen kryptografickými klíči a digitálními podpisy. Pokud je zásilka přesunuta na jiný sklad, může být tato změna automaticky zaznamenána do blockchainu. To zaručí, že zásilka je vždy zabezpečena a sledována, což umožní rychleji reagovat na případné problémy. [32]

Díky smart kontraktům může blockchain umožnit automatizaci procesů. Například, když doručení zásilky dorazí na sklad, smart kontrakt může automaticky aktualizovat záznam o skladových zásobách. Pokud je zásoba zboží nízká, blockchain může automaticky vygenerovat objednávku na dodavatele a zpracovat platbu. [32]

Blockchain je známý pro své vysoké zabezpečení dat a transparentnost. To znamená, že všechny údaje o zásobách a pohybu zboží jsou ukládány v distribuované databázi, která je nemožné hacknout. Zabezpečení dat tak pomáhá chránit skladové zásoby a zabraňuje možnému podvodu. [32]

Skrze sledování zásilek v reálném čase mohou být zásoby zboží lépe plánovány a optimalizovány. To umožňuje minimalizovat ztráty, omezit počet nevyužitých produktů a zlepšit celkovou efektivitu skladování. Dále mohou být využity algoritmy umělé inteligence, které na základě dat v blockchainu dokážou předvídat poptávku a navrhnout optimální strategii pro řízení skladových zásob. [32]

3.3.1 Příklad

Jedním z příkladů využití blockchainu pro řízení skladů je projekt, který realizovala společnost IBM ve spolupráci s farmaceutickou firmou amerického Pfizeru. [33]

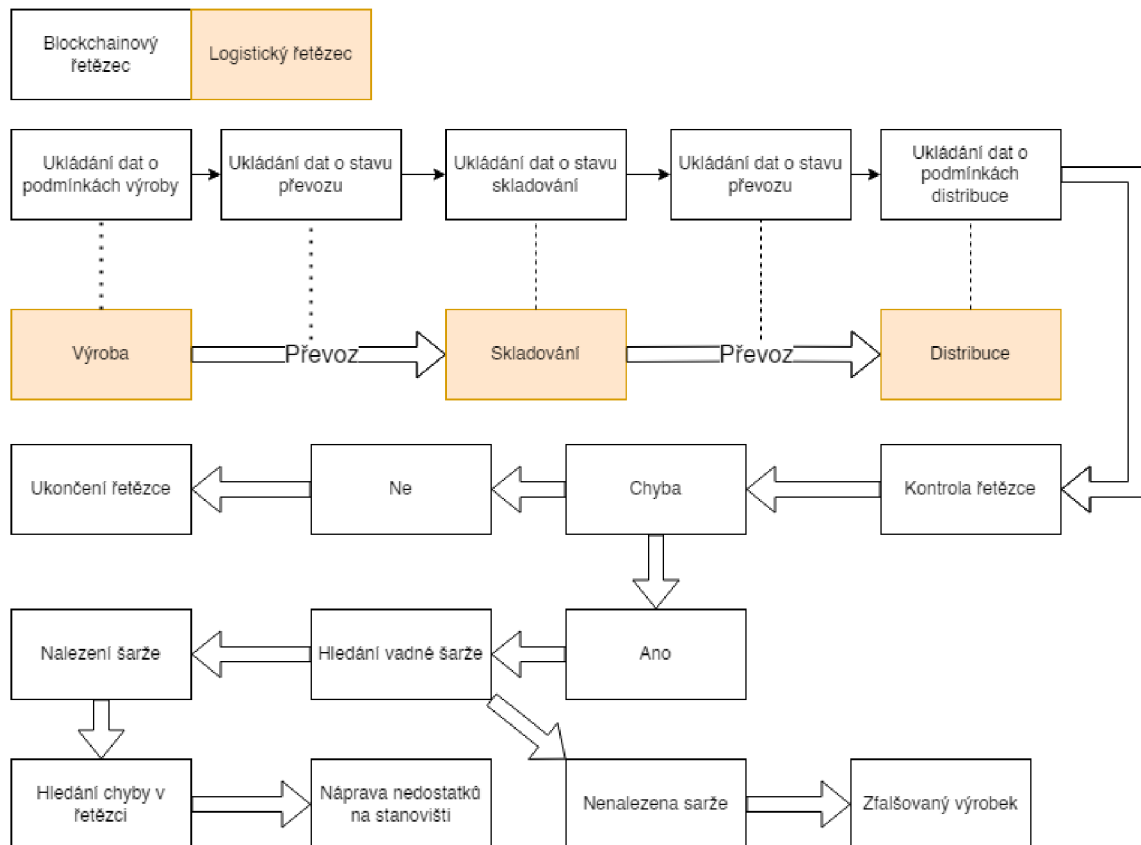
Tento projekt byl zaměřen na využití blockchainu k sledování pohybu léků v rámci dodavatelského řetězce. Hlavním cílem bylo zvýšit transparentnost a spolehlivost informací o léčivech, od jejich výroby až po doručení pacientovi. [33]

V rámci projektu byl vytvořen blockchainový systém, který umožňuje sledovat každou jednotlivou dávku léku od výroby až po distribuci. Každá dávka léku byla vybavena speciální identifikační kódem, který byl uložen v blockchainu společně s informacemi o výrobci, datumu výroby a dalšími údaji. [33]

Díky tomuto systému bylo možné sledovat každý pohyb dávky léku v rámci dodavatelského řetězce. Informace o každé změně majetkového práva byly zaznamenány

v blockchainu, což umožňovalo v reálném čase sledovat stav skladových zásob a předvídat poptávku. [33]

Tento projekt umožnil farmaceutické společnosti Pfizer minimalizovat rizika spojená s falšováním a paděláním léků v dodavatelském řetězci. Transparentnost a spolehlivost informací o pohybu dávek léků v rámci dodavatelského řetězce se podařilo zvýšit bezpečnost a spolehlivost farmaceutických produktů a zároveň efektivněji řídit skladové zásoby. [33]



Obr. 3.2 Diagram zapojení blockchainu

Zdroj: vlastní zpracování

3.4 Ochrana před paděláním

V neposlední řadě může blockchain pomoci ochránit logistický řetězec před paděláním zboží. Lze využít transparentnosti blockchainu a snadno ověřit původ zboží a tím snížit rizika paděláním a podvodů. Blockchain se také využívá k ochraně před paděláním, zejména v oblasti drahých kovů, uměleckých děl a dalších hodnotných produktů.

Tento systém zajišťuje, že každá jednotlivá položka má svůj unikátní digitální otisk a nelze ji padělat nebo změnit. [34]

V rámci tohoto systému se nejprve vytvoří digitální záznam o produktu, který obsahuje jeho unikátní identifikační kód a další údaje, jako je datum výroby, místo výroby, výrobce, Tento záznam se pak uloží do blockchainu, kde je uložen v chronologickém pořadí, což zajišťuje, že nelze měnit žádné informace o produktu. [34]

Díky tomuto záznamu může být produkt sledován v celém procesu od výroby až po prodej. Pokud se produkt změní majitele, například při prodeji, nový majitel produktu může aktualizovat informace v blockchainu a přidat tak nové informace o produktu, například novou adresu majitele. [34]

Tento systém zajišťuje, že každá jednotlivá položka má svůj unikátní digitální otisk, který nelze padělat. V případě, že někdo pokusí se podvodně prodat padělanou položku, může být tato padělaná položka snadno identifikována a odstraněna z trhu. [34]

3.4.1 Příklad

Everledger je blockchainový projekt, který se zaměřuje na ochranu před paděláním drahých kovů a drahokamů, jako jsou diamanty, rubíny nebo safíry. Projekt Everledger byl založen v roce 2015 a používá blockchain pro vytvoření digitálních profilů pro každý drahý kámen, který projde dodavatelským řetězcem. [35]

Každý profil obsahuje jedinečné informace o kameni, jako je jeho původ, historie a fyzické charakteristiky, jako jsou barva, tvar a velikost. Tyto informace jsou následně uloženy v blockchainu a propojeny s kamenem pomocí jedinečného identifikátoru. [35]

Toto řešení umožňuje obchodníkům, spotřebitelům a autoritám rychle a snadno ověřit pravost drahého kamene, což snižuje riziko paděláním a krádeže. Pokud by například kámen byl ukraden, může být rychle identifikován a náležitě vrácen svému majiteli. [35]

Everledger spolupracuje se společnostmi z celého světa, včetně výrobců kamenů, obchodníků s drahými kovy, pojišťovacími společnostmi a vládními institucemi, aby zajistil, že každý kámen, který projde dodavatelským řetězcem, bude sledován a zabezpečen v digitálním profilu. [35]

Projekt Everledger ukazuje, jak blockchain může být využit pro ochranu před paděláním a krádeží drahých kovů a drahokamů. Tento příklad ukazuje, jak blockchain může

být využit pro vytvoření spolehlivých a transparentních informací o produktech v celém dodavatelském řetězci, což zvyšuje důvěru spotřebitelů a snižuje riziko podvodů a krádeží. [35]

3.5 Využití blockchainu v různých oblastech

V oblasti zdravotnictví může být blockchain využit k ukládání a sdílení zdravotních záznamů pacientů. Tato technologie by umožnila lékařům a jiným zdravotnickým pracovníkům okamžitý a bezpečný přístup k informacím o pacientovi, což by zlepšilo rychlost a kvalitu léčby. Zdravotní záznamy by byly ukládány v decentralizované síti, což by umožnilo pacientům mít kontrolu nad svými daty a chránit je před neoprávněným přístupem. Nadále by blockchain mohl být využit k ověřování autentičnosti léků a předcházení padělání léků.

Blockchain technologie může také být využita v oblasti logistiky k sledování dodávek zboží a optimalizaci dodavatelského řetězce. Systém sledování dodávek by umožnil všem účastníkům dodavatelského řetězce sledovat pohyb zboží od výrobce až po konečného spotřebitele. To by umožnilo identifikaci a vyřešení problémů v dodavatelském řetězci a předcházení padělání výrobků. Dále by blockchain mohl být využit k vytvoření chytrých smluv, které by automaticky řídily podmínky dodávky a platby.

Blockchain technologie je již využívána v oblasti finančního sektoru, zejména v oblasti digitálních měn a platform pro obchodování s kryptoměny. Blockchain umožňuje provádět transakce bez potřeby zprostředkovatele, což snižuje náklady a zvyšuje rychlost transakcí. Dále by blockchain mohl být využit pro řízení identity, což by zlepšilo bezpečnost a ochranu osobních dat.

Blockchain technologie by mohla být využita k zabezpečení voleb a umožnit transparentní a bezpečné hlasování. Blockchain by umožnil zaznamenání hlasů bez možnosti padělání nebo manipulace s výsledky volby. To by zvýšilo důvěru ve volby a zlepšilo demokratický proces.

3.5.1 Využití vlastní kryptoměny

Využití vlastní kryptoměny v rámci firem může sloužit jako forma bonusu pro zaměstnance. Tento bonus lze dále využít jako alternativu k běžné fiat měně a následně použít pro nákup firemních produktů a služeb.

Kryptoměna jako bonus pro zaměstnance může být pro firmy zajímavým nástrojem, jak motivovat své zaměstnance. Kryptoměna může být vydaná speciálně pro tuto účel a může být použitelná pouze pro nákup firemního zboží a služeb, čímž firmě naroste využívání interních zdrojů a zvyšovat loajalitu svých zaměstnanců.

Jako alternativa k běžné fiat měně, nebo jako alternativa místo kuponů a stravenek, může mít vlastní kryptoměna několik výhod. Jednou z hlavních výhod je to, že kryptoměna může být snadno převoditelná do běžné fiat měny nebo jiných kryptoměn, což znamená, že zaměstnanci mohou své odměny relativně snadno směnit za peníze. Další výhodou je to, že použití kryptoměny může být mnohem rychlejší a efektivnější než tradiční platební metody.

Použití vlastní kryptoměny pro nákup firemního zboží a služeb může být pro firmy výhodné, protože může navýšit interní spotřebu a zvyšovat využití firemních produktů a služeb. Zároveň může být pro zaměstnance atraktivní, protože jim to dává možnost využívat své odměny na nákup věcí, které potřebují.

Náklady spojené s tvorbou kryptoměny se liší v závislosti na druhu blockchainu, který se používá. Využití veřejného blockchainu může mít diametrálně odlišné náklady ve srovnání s privátním blockchainem. Pokud se zaměříme na Solana network, kterou jsem popsal v předchozí kapitole, tvoří náklady na vytvoření kryptoměny tři základní položky: hardware, software a čas.

Pokud jde o hardwarovou výbavu, postačí základní notebook nebo kancelářská stanice, protože veškeré náročné výpočty probíhají na veřejném blockchainu. V případě, že firma nevlastní žádný hardwarový vybavení, cena se může pohybovat okolo 15 tisíc korun za základní hardware.

Po softwarové stránce, využil jsem bezplatnou verzi Microsoft Visual Studio. Virtuální počítač, který jsem použil, není podle mého názoru nezbytný a využil jsem ho spíše pro ochranu svého hardwaru, protože jsem poprvé vytvářel kryptoměnu. Existují alternativy jako servery od Linode, které nabízejí trial verze po dobu 2 měsíců a umožňují vlastní virtuální počítače. To snižuje potřebu vlastnit výkonný počítač.

Co se týče využití virtuálního počítače, je to výhodná možnost, pokud chcete ochránit svůj hardware nebo potřebujete výkon, který váš počítač nemá. Existují však také cloudové služby, jako například Amazon Web Services nebo Google Cloud Platform, které umožňují pronájem virtuálního serveru na určitou dobu za nízkou cenu. Tyto služby

jsou velmi flexibilní a mohou být použity pro různé účely, jako jsou testování softwaru, hosting webových stránek a mnoho dalšího.

Vytvoření vlastní kryptoměny vyžaduje zvážení mnoha faktorů, které ovlivňují časové náklady. Pokud má člověk zkušenosti s programováním a již dříve vytvářel kryptoměny, může to být rychlé a zvládnutelné i během několika hodin. Nicméně, v případě nedostatku zkušeností a změn na blockchainu, může tvorba kryptoměny trvat i několik týdnů. Osobně kvůli jsem tu svou vytvářel asi týden, a to z důvodu nedávných změn na blockchainu a z nedostatku zkušeností.

Ostatní náklady spojené s tvorbou kryptoměny zahrnují poplatky za samotné vytvoření a vydání mincí. Poplatek za vytvoření kryptoměny je stanoven na 0,0001 SOL, což přibližně odpovídá 1 haléři. Další poplatek se vztahuje k vytvoření samotných mincí, a to 0,000027 SOL, což opět zhruba odpovídá jednomu haléři. Cena poplatku se může lišit v závislosti na vytíženosti sítě a aktuálním kurzu.

3.5.2 Modelové příklady

Firmy by mohly používat blockchain pro zpracování smluv, které by plně splňovaly veškerá nařízení, jenž přikazují směrnice o GDPR. Vzhledem k anonymitě, kterou kryptografie na blockchainu poskytuje, tak by veškeré osobní údaje mohly být zapečetěny na blockchainu a přístup k nim by měla pouze oprávněná osoba.

Jednou z možností, jak využívat blockchain, tak by byla jeho transparentnost. Mohla by vytvářet veřejné a transparentní záznamy o svých aktivitách, které by byly mohly být podpořené o pevná data od přístrojů. Tyto data by následně mohla sloužit jako podpůrný prostředek při nabízení svých služeb na trhu.

Využit blockchain k zajištění správy smluv. Smart contracts by umožnily firmě vytvářet smlouvy s vysokou úrovní automatizace a transparentnosti. Tyto smlouvy by mohly být uloženy v blockchainu a automaticky provádět všechny akce specifikované v smlouvě, což by minimalizovalo rizika spojená s neplněním smlouvy a zajišťovalo spravedlivé rozdělení platby. Další výhodou by bylo velké snížení administrativních nákladů.

Následující modelový příklad ukazuje, jak by mohl být nasazený blockchain pro firmu zabývající se distribucí potravin.

Firma by mohla využít blockchain k zabezpečení identifikace potravin v průběhu celého dodavatelského řetězce, od výrobce až po prodejnu. Každá potravina by byla označena

unikátním kódem a záznam o této potravíně by byl uložen v blockchainu. To umožní firmě sledovat pohyb potravin v reálném čase a zjistit, kde se nacházejí v průběhu celého dodavatelského řetězce.

Další možností, jak by takováto firma mohla využít blockchain je k zabezpečení kvality a bezpečnosti potravin. Když se potravina pohybuje v průběhu dodavatelského řetězce, informace o ní by byly neustále aktualizovány v blockchainu. Dodávky rozvázející potraviny by mohly mít teploměry, které by do blockchainu neustále nahrávaly informace o teplotě, čímž by se zamezilo pochybnostem o kvalitě a bezpečnosti přepravy a zajistilo by se, že dané potraviny jsou bezproblémové pro následnou konzumaci.

Další možností, jak využít blockchain je k zrychlení procesu objednávání, fakturace a plateb. Při využití smart contracts by byly objednávky automaticky zpracovány, fakturovány a platby by byly převedeny v reálném čase. To by ušetřilo čas a náklady na administrativní práce a umožnilo by firmě se soustředit na vlastní podnikání.

Jako jednou z velkých výhod blockchainu, je možnost sledování veškerého pohybu v logistickém řetězci v reálném čase. Toto umožňuje zlepšit a zefektivnit plánování celé firmy. Ku příkladu, pokud by se měla dodávka zpozdít, tak budeme o tomto problému vědět s velkým předstihem a umožní nám to upravit denní ve firmě.

4 Zhodnocení

Blockchainová technologie je velmi zajímavou a perspektivní technologií, která může mít zásadní dopad na různá odvětví a procesy v nich probíhající. Základní myšlenkou blockchainu je vytvoření decentralizovaného a transparentního systému záznamů, který umožňuje ověřování a sledování transakcí a událostí v reálném čase.

Hlavní výhodou blockchainu je jeho bezpečnost a nezměnitelnost záznamů, což znamená, že data jsou chráněna před úpravami nebo paděláním. Blockchainová technologie také umožňuje efektivní řešení problémů spojených s důvěryhodností a transparentností, a to bez nutnosti spoléhat se na prostředníka nebo třetí stranu.

Využití blockchainu se nejčastěji spojuje s kryptoměnami, ale v poslední době se stává stále populárnější v jiných oblastech, jako jsou například logistika, finance, zdravotnictví nebo správa informací. V těchto oblastech blockchainová technologie umožňuje zajištění bezpečnosti dat, transparentnosti procesů, snížení nákladů a zvýšení efektivity.

Nicméně, i když je blockchainová technologie velmi perspektivní, stále existují určité výzvy a problémy, jako jsou například otázky soukromí a ochrany osobních údajů, problémy s výkonem a škálovatelností a nedostatek standardizace. Tyto problémy však nebrání v rozvoji a využívání blockchainu a mnoho firem již úspěšně implementovalo tuto technologii do svých procesů a řeší problémy, které se s ní pojí.

U nás se o tuto problematiku a budoucí vývoj stará seskupení Elektronické asociace České republiky, která se snaží přiblížit a pomoci nasadit blockchain do místních firem. Proslavili se svých blockchainem Notarius, který využívají velké firmy po světě.

Blockchain Notarius je služba, která umožňuje uživatelům ověřit a zabezpečit své důležité dokumenty pomocí blockchainové technologie. Tato služba je navržena tak, aby umožnila uživatelům snadno a rychle ověřit původnost a pravost svých dokumentů, aniž by museli spoléhat na důvěru k jakékoli třetí straně.

Blockchain Notarius funguje tak, že uživatel nahrává svůj dokument do systému. Tento dokument je poté zpracován a zakódován do podoby jedinečného kryptografického otisku, který se nazývá hash. Tento hash se pak uloží do blockchainové sítě, která slouží jako neprůstřelný a distribuovaný úložiště pro data. Každý hash je jedinečný a nelze ho změnit, takže jakýkoli pokus o změnu původního dokumentu by okamžitě vyzradil

neplatnost dokumentu. Pro ověření dokumentu stačí uživateli zadat hash dokumentu do webového rozhraní Blockchain Notarius. Systém poté porovná tento hash s hashem uloženým v blockchainu a ověří tak pravost dokumentu. Pokud jsou oba hashe shodné, dokument se považuje za platný a pravý.

Hlavní výhodou používání Blockchain Notarius je, že uživatelé mohou rychle a snadno ověřit pravost svých dokumentů bez toho, aby museli spoléhat na důvěryhodnost jakékoli třetí strany. Navíc výhodou je, že hash dokumentu je uložen v decentralizované blockchainové síti, což znamená, že dokument je zabezpečen proti manipulaci a změně. Tento systém tedy poskytuje nejvyšší možnou úroveň bezpečnosti a důvěryhodnosti.

Další výhodou je, že Blockchain Notarius umožňuje uživatelům snadno a rychle ověřit pravost a původnost dokumentu, což může být užitečné pro různé účely, jako například pro ověření identity, ověření autenticity produktů, ověření zdravotních záznamů a další.

Tento a spousta dalších úspěšných projektů ukazuje na funkčnost a smysl blockchainových technologií, které dokáží na správném místě ušetřit velké firemní prostředky, které následně mohou být využity pro konkurenceschopnost na již nesmírně kompetitivním a přesaturovaném trhu.

Závěr

V této práci se zaměřuji na využití blockchainu v logistických procesech a na zhodnocení efektivity této technologie. Pro demonstraci konkrétních příkladů jsem si vybral veřejný blockchain od Solana Networks, který může pomoci firmám v různých aspektech logistických procesů a vedení firmy. V dnešní době, kdy digitalizace nabízí nové možnosti, může blockchain přinést finančně efektivní řešení a pomoci firmám zvýšit svou konkurenceschopnost na již tak přesyceném trhu. V této práci se budu věnovat konkrétním příkladům využití blockchainu v logistických procesech a ukážu, jak tato technologie může přinést výhody v oblasti transparentnosti, bezpečnosti a snížení nákladů na vedení logistických procesů. Budu také zkoumat nevýhody blockchainu, jako je například pomalost transakcí a náklady na implementaci a údržbu, a porovnávat je s jeho výhodami. Cílem této práce je tedy ukázat, jak blockchain může pomoci firmám zlepšit své procesy a získat konkurenční výhodu na trhu.

Technologie blockchain se vyznačuje vysokou flexibilitou, což znamená, že ji lze využít v různých odvětvích a oborech. Blockchain je schopen řešit mnoho různých problémů, jako je například nedostatek transparentnosti, důvěryhodnosti nebo bezpečnosti v transakcích. Právě proto může být využit v mnoha oblastech, jako jsou například finance, pojišťovnictví, výroba, telekomunikace, zdravotnictví, veřejná správa, nebo logistika. V každém odvětví může blockchain pomoci zlepšit stávající fungování a přinést nové možnosti a funkce, které by jinak nebyly možné. Proto je potenciál růstu blockchainu v různých odvětvích velmi vysoký.

Seznam zdrojů

- [1] Allibert, Schoeller. SchoellerAllibert.com. Schoeller Allibert. [Online] 1. 4 2023. [Citace: 4. 3 2023.] <https://www.schoellerallibert.com/cz/novinky/trhy/pojem-logistika-co-znamen-logistika/>.
- [2] Vyšší odborné vzdělání. *Vyšší odborné vzdělání*. [Online] 19. 8 2020. [Citace: 5. 3 2023.] <https://www.vovcr.cz/odz/ekon/409/page02.html>.
- [3] Systém Online. *Systém Online*. [Online] 8. 7 2011. [Citace: 7. 3 2023.] <https://www.systemonline.cz/rizeni-vyroby/pokrocile-planovani-a-rizeni-vyroby.htm>.
- [4] Systems Applications Products. *SAP*. [Online] [Citace: 15. 3 2023.] <https://www.sap.com/cz/insights/what-is-a-wms-warehouse-management-system.html>.
- [5] Edu. *Edu*. [Online] 13. 9 2021. [Citace: 15. 3 2023.] <https://edu.trans.eu/cz/blog/post/jak-usnadnit-rizeni-dopravy-ve-vasi-spolecnosti>.
- [6] Egera. *Egera*. [Online] 2019. [Citace: 15. 3 2023.] <https://egera.com/cs/co-je-blockchain>.
- [7] Vondrák, Matouš. Finex. *Finex*. [Online] 24. 11 2018. [Citace: 15. 3 2023.] <https://finex.cz/blockchain/>.
- [8] Cryptokingdom. *Crypto kingdom*. [Online] 10. 6 2020. [Citace: 15. 3 2023.] <https://cryptokingdom.tech/cs/magazin/zacatecnik/co-je-to-hash-a-hashovani>.
- [9] Binance. *Binance*. [Online] 2023. [Citace: 15. 3 2023.] <https://academy.binance.com/cs/articles/what-is-cryptocurrency.amp>.
- [10] Khan Academy. *Khan Academy*. [Online] 2023. [Citace: 15. 3 2023.] <https://cs.khanacademy.org/computing>.
- [11] SSL. *SSL*. [Online] 10. 11 2015. [Citace: 15. 3 2023.] <https://www.ssl.com/cs/Nej%C4%8Dast%C4%9Bj%C5%A1%C3%AD-dotazy/co-je-kryptografick%C3%A1-hashovac%C3%AD-funkce/>.
- [12] Automatizace.hw. *Automatizace.hw*. [Online] 24. 7 2022. [Citace: 15. 3 2023.] <https://automatizace.hw.cz/princip-technologie-blockchain-a-problematika-pouziti-v-prumyslu.html>.

- [13] Xtb. *Xtb*. [Online] 2023. [Citace: 15. 3 2023.] <https://www.xtb.com/cz/vzdelavani/kryptomeny-pro-zacatecniky>.
- [14] kryptomagazin. *kryptomagazin*. [Online] 1. 12 2021. [Citace: 15. 3 2023.] <https://kryptomagazin.cz/>.
- [15] Coin Marketcap. *Coin Marketcap*. [Online] 2023. [Citace: 15. 3 2023.] <https://coinmarketcap.com/cs/currencies/bitcoin/>.
- [16] Kriptomat. *Kriptomat*. [Online] 2023. [Citace: 15. 3 2023.] <https://kriptomat.io/cs/kryptomeny/druhy-kryptomen/>.
- [17] Skrblik. *Skrblik*. [Online] 9. 3 2021. [Citace: 15. 3 2023.] <https://www.skrblik.cz/navod/jak-funguje-bitcoin/>.
- [18] Cryptosvet. *Cryptosvet*. [Online] 30. 10 2017. [Citace: 15. 3 2023.] <https://cryptosvet.cz/co-je-to-tezba-bitcoinu/>.
- [19] Bankless. *Bankless*. [Online] 23. 4 2021. [Citace: 12. 3 2023.] <https://bankless.cz/studium/co-je-to-proof-of-work-a-jak-funguje>.
- [20] Chytrý převod. *Chytrý převod*. [Online] 1. 2 2021. [Citace: 15. 3 2023.] <https://chytryprevod.cz/kryptomena-bitcoin-vyhody-nevyhody/>.
- [21] Etoro. *Etoro*. [Online] 2023. [Citace: 15. 3 2023.] <https://www.etero.com/cs-cz/crypto/legality-of-bitcoin/>.
- [22] Plecháč, Petr a Velek , Tomáš. TradeCZ. *TradeCZ*. [Online] 24. 3 2022. [Citace: 15. 3 2023.] <https://www.tradecz.cz/bitcoin-jako-zakonne-platidlo-a-postupna-adopce-kryptomen-ktere-staty-jsou-na-rade/>.
- [23] Ethereum. *Ethereum*. [Online] 2023. [Citace: 15. 3 2023.] <https://ethereum.org/en/what-is-ethereum/>.
- [24] FRANKENFIELD, JAKE. Investopedia. *Investopedia*. [Online] 27. 8 2022. [Citace: 15. 3 2023.] <https://www.investopedia.com/terms/e/ethereum.asp>.
- [25] Rust. [Online] 2023. [Citace: 15. 3 2023.] <https://www.rust-lang.org>.
- [26] Solscan. [Online] 2023. [Citace: 15. 3 2023.] <https://solscan.io/account/7Hcs4RFNaf4esNu4SN8WmyauCntkvT8ryct2fmH84X1F>.
- [27] Smart Contracts. *Ethereum*. [Online] 2. 8 2022. [Citace: 15. 3 2023.] <https://ethereum.org/cs/developers/docs/smart-contracts/>.

- [28] Blockchain could revolutionize logistics. *Forbes*. [Online] 4. 12 2016. [Citace: 15. 3 2023.] <https://www.forbes.com/sites/forbestechcouncil/2019/12/04/blockchain-could-revolutionize-logistics-but-is-the-industry-prepared-to-let-it/?sh=63dca59b11e2>.
- [29] Supply Chain Intelligence Suite. *IBM*. [Online] 2023. [Citace: 15. 3 2023.] <https://www.ibm.com/products/supply-chain-intelligence-suite/food-trust>.
- [30] Søggaard, Jonas Sveistrup. How business blockchains can help streamline procure pay. [Online] 27. 8 2018. [Citace: 15. 3 2023.] <https://www.linkedin.com/pulse/how-business-blockchains-can-help-streamline-procure-pay-søggaard>.
- [31] We trade blockchain. *IBM*. [Online] 2019. [Citace: 15. 3 2023.] <https://www.ibm.com/case-studies/we-trade-blockchain>.
- [32] Why blockchain is a game changer for the supply chain. [Online] 3. 7 2019. [Citace: 15. 3 2023.] https://www.supplychain247.com/article/why_blockchain_is_a_game_changer_for_the_supply_chain.
- [33] The pharmaceutical industry on blockchain. *IBM*. [Online] 2023. [Citace: 15. 3 2023.] <https://www.ibm.com/blockchain/resources/transparent-supply/pharma/>.
- [34] Use blockchain protect against counterfeiting. *Europa*. [Online] 16. 9 2022. [Citace: 15. 3 2023.] https://intellectual-property-helpdesk.ec.europa.eu/news-events/news/use-blockchain-protect-against-counterfeiting-2022-09-16_en.
- [35] Everledger. [Online] 2023. [Citace: 15. 3 2023.] <https://everledger.io>.

Seznam grafických objektů

Obr. 2.1 Výstup vytváření kryptoměny	37
Obr. 2.2 Výstup vlastní kryptoměny	41
Obr. 3.1 Diagram zapojení blockchainu.....	50
Obr. 3.2 Diagram zapojení blockchainu	52

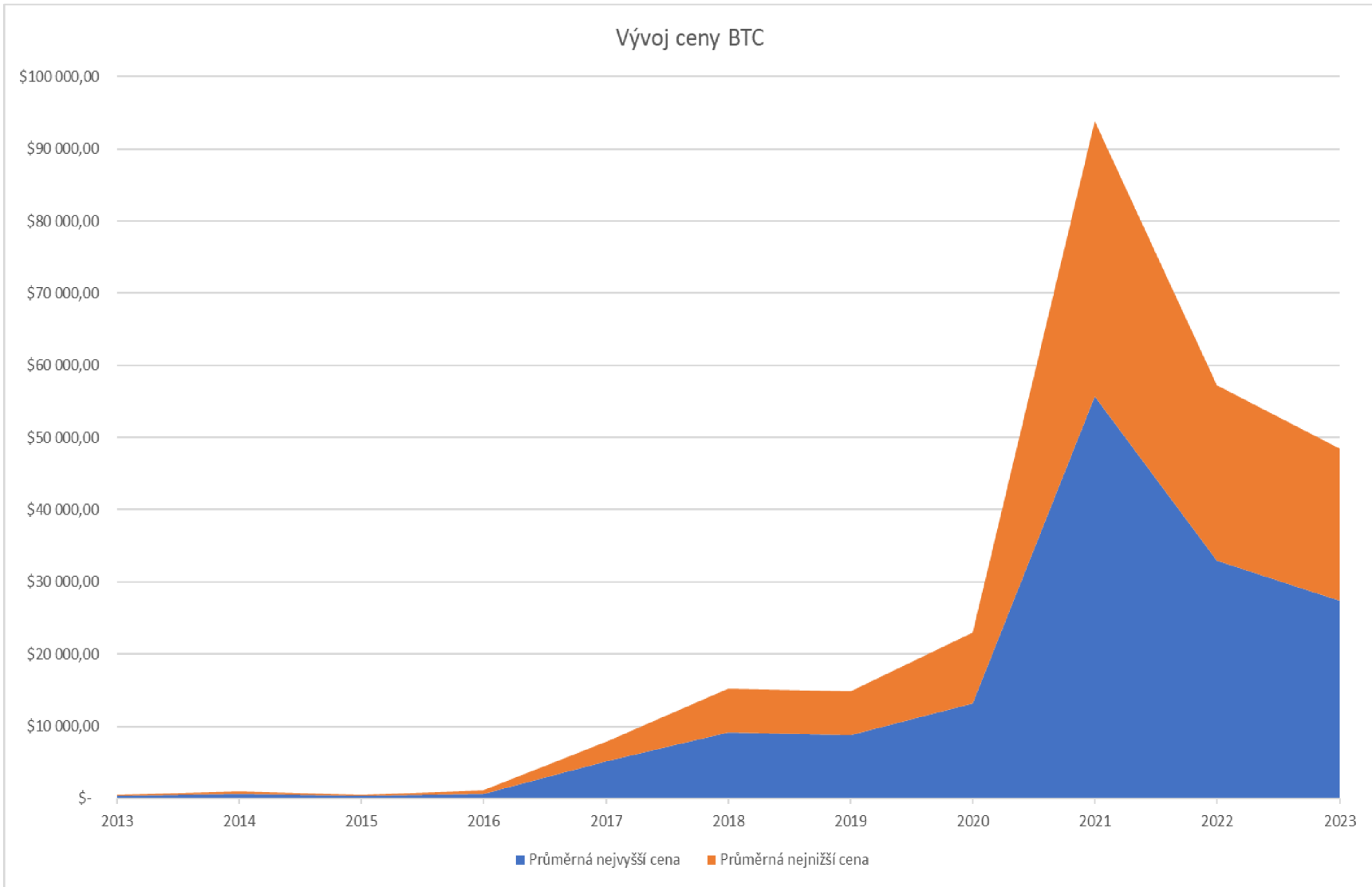
Seznam zkratek

BTC	BitCoin	druh kryptoměny
ETH	Ethereum	druh kryptoměny
SOL	Solana	druh kryptoměny
PC	Personální počítač	nástroj
WMS	Warehouse Management System	system pro správu skladů
TMS	Transport management system	system pro správu přepravy
ERP	Enterprise resource planning	system pro správu podnikový zdrojů
SCM	Supply Chain Management	system pro správu dodavatelského řetězce
LAN	Local Area Network	lokální počítačová síť
P2P	Person to Person	klient-klient
ASIC	Application-Specific Integrated Circuit	druh procesorů pro těžbu kryptoměn
NFT	non-fungible token	nezaměnitelný token
JSON	JavaScript Object Notation	druh dat používaných v javascriptu
ID	identifikační číslo	nezaměnitelné číslo
ICO	Initial Coin Offering	prvotní nabídka tokenů
DApps	Decentralized applications	decentralizované aplikace
GDPR	General Data Protection Regulation	Obecné nařízení o ochraně osobních údajů

Seznam příloh

Příloha A Graf vývoje cen BTC

Vývojový graf ceny BTC



Autor BP	Martin Kolář
Název BP	Využití technologie Blockchain v logistických procesech
Studijní program	IPL
Rok obhajoby BP	2023
Počet stran	50
Počet příloh	1
Vedoucí BP	doc. Dr. Ing. Oldřich Kodym
Anotace	<p>V této bakalářské práci se zaměřuji na rozvíjející se technologii blockchainu a její následné využití v praktickém prostředí. V teoretické části se zaměřuji na samotné fungování, historii a vývoj blockchainu. Zaměřuji se na vlivy a potencionální využití blockchainu v malých i velkých firmách. V praktické části se věnuji konkrétnímu vytváření vlastní kryptoměny. Zkoumám, jakým způsobem je možné takovou měnu vytvořit a jak ji následně využít. Dále prezentuje příklady a modely, jakým způsobem by mohl blockchain sloužit jako nástroj pro zlepšení efektivity různých typech firem.</p>
Klíčová slova	blockchain, kryptografie, logistické procesy, solana, smart kontrakty
Místo uložení	ITC (knihovna) Vysoké školy logistiky v Přerově
Signatura	