

Worldcoin

Andrej Navrátil

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav počítačových a komunikačních systémů

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Andrej Navrátil
Osobní číslo: A22435
Studijní program: B0688A140008 Informační technologie v administrativě
Forma studia: Prezenční
Téma práce: Worldcoin
Téma práce anglicky: Worldcoin

Zásady pro vypracování

- Vypracujte literární rešerši dané problematiky.
- Nastudujte a popište historii, základní vlastnosti a principy kryptoměny Worldcoin.
- Vypracujte srovnávací studii využití, výhod a nevýhod Wordcoin oproti nejběžněji používaným kryptoměnám
- Provedte analýzu dalšího možného využití této kryptoměny, jakož i jejích potenciálních rizik.

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

Seznam doporučené literatury:

1. GIGI. 21 lekcí: co mě naučil pád do bitcoinové králičí nory. Přeložil František ŠIMEK. Praha: Braiins Systems, 2022. ISBN 978-80-908709-0-1
2. GENT, Edd. A Cryptocurrency for the Masses or a Universal ID?: Worldcoin Aims to Scan all the World's Eyeballs. Online. IEEE Spectrum. 2023, roč. 60, č. 1, s. 42-57. ISSN 0018-9235. Dostupné z: <https://doi.org/10.1109/MSPEC.2023.10006664>. [citováno 2024-10-22]
3. GEORGE, A. Shaji; GEORGE, A. S. Hovan a BASKAR, T. *Worldcoin: A Decentralized Currency for a Unified Global Economy*. 2023, roč. 2, č. 2, s. 136-155. Dostupné z: <https://www.allcryptowhitepapers.com/wp-content/uploads/2018/05/Worldcoin-research-whitepaper.pdf>. [citováno 2024-10-22]
4. GUO, Eileen a RENALDI, Adi. *Deception, exploited workers, and cash handouts: How Worldcoin recruited its first half a million test users*. Online. TechReview: MIT Technology Review. Cambridge, Massachusetts, United States: Massachusetts Institute of Technology. April 6, 2022. Dostupné z: <https://www.technologyreview.com/2022/04/06/1048981/worldcoin-cryptocurrency-biometrics-web3>. [citováno 2024-10-22]
5. Francisco, California, United States. Dostupné z: <https://worldcoin.org/> [citováno 2024-10-22]

Vedoucí bakalářské práce: **doc. Ing. Libor Pekař, Ph.D.**
Ústav automatizace a řídicí techniky

Datum zadání bakalářské práce: **4. prosince 2024**
Termín odevzdání bakalářské práce: **9. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Miroslav Matýsek, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 4. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Cílem této bakalářské práce je představit a analyzovat projekt Worldcoin, který představuje inovativní přístup ke kryptoměnám prostřednictvím biometrického ověřování uživatelů. Teoretická část popisuje historii a základní principy fungování Worldcoinu, včetně jeho hlavní myšlenky – vytvoření globální sítě, kde každý člověk může prokázat svou jedinečnost bez nutnosti odhalení osobních údajů. Vysvětluje také funkce specializovaného zařízení „Orb“ pro skenování duhovky oka a možnosti získávání a využití tokenů Worldcoin. Praktická část obsahuje srovnávací studii Worldcoinu s ostatními kryptoměnami z hlediska technologických, ekonomických, uživatelských a regulačních aspektů, identifikující specifické výhody a nevýhody projektu. V závěrečné části zkoumá současné implementace a budoucí potenciál využití v platebních systémech, boji proti AI dezinformacím a možné implementaci univerzálního základního příjmu. Práce kriticky vyhodnocuje rizika spojená se sběrem biometrických dat, regulační výzvy a otázky dlouhodobé udržitelnosti projektu.

Klíčová slova: Worldcoin, biometrické ověřování, blockchain, kryptoměna, digitální identita, důkaz o člověku

ABSTRACT

The aim of this bachelor's thesis is to present and analyze the Worldcoin project, which represents an innovative approach to cryptocurrencies through biometric user verification. The theoretical part describes the history and basic principles of Worldcoin's operation, including its main idea – creating a global network where every person can prove their uniqueness without the need to reveal personal data. It also explains the functioning of the specialized "Orb" device for iris scanning and the possibilities of obtaining and utilizing Worldcoin tokens. The practical part contains a comparative study of Worldcoin with other cryptocurrencies from technological, economic, user, and regulatory perspectives, identifying specific advantages and disadvantages of the project. In the concluding section, it examines current implementations and future potential for use in payment systems, combating AI misinformation, and possible implementation of universal basic income. The thesis critically evaluates risks associated with biometric data collection, regulatory challenges, and questions of the project's long-term sustainability.

Keywords: Worldcoin, biometric verification, blockchain, cryptocurrency, digital identity, proof of personhood

Rád bych tímto poděkoval vedoucímu mé bakalářské práce panu doc. Ing. Liboru Pekařovi, Ph.D. za jeho ochotný přístup a rychlé reakce na mé dotazy. Velmi si vážím veškerých připomínek a cenných rad k práci.

Dále bych chtěl poděkovat své rodině za trpělivost a podporu během celého studia, a zvláště své přítelkyni za povzbuzení v náročných chvílích při psaní této práce.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST.....	13
1 WORLDCOIN – HISTORIE, ZÁKLADNÍ VLASTNOSTI A PRINCIPY	14
1.1 PŘEDSTAVENÍ WORLDCOIN	14
1.1.1 Co je Worldcoin	14
1.1.2 Cíle a vize projektu	14
1.1.3 Koncept důkazu o člověku (Proof-of-Personhood).....	15
1.2 HISTORIE VZNIKU	17
1.2.1 Zakladatelé Sam Altman a Alex Blania	17
1.2.2 Vznik společnosti Tools for Humanity	17
Klíčové milníky vývoje	18
1.3 TECHNOLOGICKÉ ZÁKLADY.....	20
1.3.1 World ID protokol.....	20
1.3.2 Architektura blockchainu	21
1.3.3 Zero-knowledge důkazy	23
1.3.4 Kryptografické principy	24
1.4 ORB – BIOMETRICKÉ OVĚŘOVÁNÍ.....	26
1.4.1 Konstrukce a funkce Orbu	26
1.4.2 Technologie skenování duhovky.....	29
1.4.3 Zpracování biometrických dat.....	32
1.4.4 Bezpečnostní opatření a ochrana dat.....	35
2 TĚŽBA, SMĚNA A PLATBY POMOCÍ WORLDCOIN	38
2.1 ZÍSKÁVÁNÍ WORLDCOINU	38
2.1.1 Přidělování grantu WLD tokenů	38
2.1.2 World App a uživatelské rozhraní.....	39
2.1.3 Rozdíly mezi regiony a zeměmi.....	42
2.2 MOŽNOSTI NÁKUPU A SMĚNY	43
2.2.1 Kryptoměnové burzy	43
2.2.2 Kryptoměnové směnárny	44
2.2.3 Přímě v aplikaci World App	45
2.2.4 Cenový vývoj	45
2.3 VYUŽITÍ PRO PLATBY	46
II PRAKTICKÁ ČÁST.....	47
3 SROVNÁVACÍ STUDIE WORLDCOINU OPROTI OSTATNÍM KRYPTOMĚNÁM.....	48
3.1 3.1 METODOLOGIE SROVNÁVACÍ STUDIE.....	48
3.1.1 Kritéria hodnocení kryptoměn	48
3.1.2 Výběr kryptoměn pro srovnání s Worldcoinem.....	49
3.2 SROVNÁNÍ WORLDCOINU S NEJPOUŽÍVANĚJŠÍMI KRYPTOMĚNAMI	50

3.2.1	Technologické aspekty (konsenzuální mechanismy, škálovatelnost, bezpečnost).....	50
3.2.2	Ekonomické aspekty (tokenomika, distribuce, volatilita).....	55
3.2.3	Uživatelské aspekty (přístupnost, použitelnost, adopce).....	59
3.2.4	Právní a regulační aspekty.....	63
3.3	GRAFICKÉ SROVNÁNÍ VYBRANÝCH ASPEKTŮ KRYPTOMĚN	66
3.4	SHRNUTÍ VÝHOD A NEVÝHOD WORLDCOINU	67
3.4.1	Výhody	67
3.4.2	Nevýhody	68
4	WORLD COIN A WORLD ID: SOUČASNÉ VYUŽITÍ A BUDOUCÍ POTENCIÁL	69
4.1	SOUČASNÉ VYUŽITÍ (2025).....	69
4.1.1	Digitální identifikace v online prostředí.....	69
4.1.2	Spolupráce se seznamovacími aplikacemi	69
4.1.3	Globální expanze.....	69
4.1.4	Mini aplikace dApps v ekosystému.....	70
4.1.5	World Chain	70
4.2	BUDOUCÍ POTENCIÁL.....	71
4.2.1	Platební řešení	71
4.2.2	Standardizace "proof-of-human" neboli PoP	72
4.2.3	Ochrana proti dezinformacím.....	72
4.3	POTENCIONÁLNÍ RIZIKA.....	73
4.3.1	Etické a soukromí ohrožující praktiky při získávání uživatelů	73
4.3.2	Bezpečnostní rizika a zranitelnosti.....	74
4.3.3	Regulační překážky	74
4.3.4	Problémy dlouhodobé udržitelnosti.....	75
4.3.5	Etické problémy "digitální kolonizace"	75
	ZÁVĚR.....	76
	SEZNAM POUŽITÉ LITERATURY	79
	SEZNAM OBRÁZKŮ	84
	SEZNAM TABULEK.....	85
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	86

ÚVOD

V současném digitálním světě, kdy se rozlišení mezi lidmi a umělou inteligencí stává stále obtížnějším, představuje Worldcoin velmi neobyčejný projekt spojující kryptoměnové technologie s biometrickou identifikací.

Teoretická část práce je rozdělena do dvou hlavních kapitol. První kapitola se věnuje historii, základním vlastnostem a principům fungování Worldcoinu. Zabývá se představením projektu, jeho cíli a vizí, včetně revolučního konceptu „důkazu o člověku" (Proof-of-Personhood). Kapitola dále popisuje historii vzniku projektu od jeho zakladatelů až po vznik společnosti Tools for Humanity a klíčové milníky vývoje. Značná pozornost je věnována technologickým základům, zejména protokolu World ID, architektuře blockchainu využívající Layer 2 řešení, implementaci zero-knowledge důkazů a kryptografickým principům zajišťujícím bezpečnost systému. Závěr kapitoly se podrobně zaměřuje na speciální zařízení Orb – biometrické ověřovací zařízení, jeho konstrukci, technologii skenování duhovky, zpracování biometrických dat a bezpečnostní opatření pro ochranu citlivých informací.

Druhá kapitola teoretické části se soustředí na získávání, směny a využití Worldcoinu pro platby. Vysvětluje systém přidělování grantů WLD tokenů, fungování aplikace World App jako primárního uživatelského rozhraní a regionální rozdíly v dostupnosti služeb. Kapitola také poskytuje přehled možností nákupu a směny WLD tokenů prostřednictvím kryptoměnových burz, směnárů a integrovaných funkcí v aplikaci, včetně analýzy cenového vývoje tokenu. Závěr kapitoly hodnotí současné možnosti využití WLD pro přímé platby.

Praktická část práce je zaměřená na komparativní analýzu a hodnocení budoucího potenciálu. První kapitola praktické části představuje rozsáhlou srovnávací studii Worldcoinu s nejpoužívanějšími kryptoměnami na trhu (Bitcoin, Ethereum, Solana, Cardano a Polygon). Studie využívá strukturovanou metodologii hodnocení založenou na čtyřech hlavních kritériích: technologických aspektech, ekonomických aspektech, uživatelských aspektech a právních a regulačních aspektech. Výsledky srovnání jsou prezentovány prostřednictvím tabulek a grafických vizualizací, které umožňují jasnou identifikaci specifických výhod a nevýhod Worldcoinu oproti konkurenčním kryptoměnám.

Závěrečná kapitola se zaměřuje na současné využití Worldcoinu a World ID v roce 2025 a analyzuje jejich budoucí potenciál. Kapitola specifikuje aktuální implementace

technologie v oblasti digitální identifikace, spolupráci se seznamovacími aplikacemi, globální expanzi projektu, vývoj ekosystému Mini aplikací a spuštění vlastního blockchainu World Chain. V části věnované budoucímu potenciálu jsou analyzovány oblasti budoucího využití, včetně platebních řešení s důrazem na partnerství s Visa a vývoj platební karty World Card, možné implementace univerzálního základního příjmu, standardizace konceptu „důkazu o člověku" a využití pro ochranu proti dezinformacím. Kapitola také kriticky hodnotí potenciální rizika, která mohou ohrozit dlouhodobou udržitelnost projektu, včetně etických otázek spojených se sběrem biometrických dat, bezpečnostních zranitelností, regulatorních překážek a problémů dlouhodobé udržitelnosti.

Cílem této bakalářské práce je poskytnout komplexní analýzu projektu Worldcoin, včetně jeho technologických základů, principů fungování, aktuálního využití a potenciálu do budoucna a zároveň srovnat Worldcoin s ostatními kryptoměnami, identifikovat jeho specifické výhody a nevýhody a zhodnotit jeho potenciální rizika.

Vzhledem k proměnlivé povaze tohoto odvětví je práce založena na nejnovějších dostupných informacích k roku 2025, reflektujících aktuální stav vývoje projektu Worldcoin.

I TEORETICKÁ ČÁST

1 WORLDCOIN – HISTORIE, ZÁKLADNÍ VLASTNOSTI A PRINCIPY

1.1 Představení Worldcoin

1.1.1 Co je Worldcoin

Worldcoin představuje inovativní kryptoměnový projekt založený na spojení blockchainu a biometrického ověřování identity, který byl oficiálně spuštěn 24. července 2023. Jedná se o decentralizovanou digitální měnu postavenou na technologii Ethereum (decentralizovaná blockchainová platforma), jejímž cílem je vytvoření globální identitní a finanční sítě dostupné všem lidem bez ohledu na jejich geografickou lokaci či ekonomické zázemí. Projekt usiluje o propojení konceptu decentralizovaných financí s řešením problému rozlišování skutečných lidí od botů (programy navržené k automatickému provádění určitých úkolů) či AI (Artificial intelligence – umělá inteligence) v digitálním prostoru. [1], [2], [5]

Od října 2024 Worldcoin migruje na vlastní blockchain World Chain, který je konstruován pomocí modulární technologické platformy OP Stack (viz. kapitola 1.3.2). [1]

Jedinečnost projektu spočívá v jeho přístupu k verifikaci uživatelů. Na rozdíl od standardních kryptoměnových projektů Worldcoin využívá specializované hardwarové zařízení nazývané "Orb", které skenuje duhovku oka k vytvoření biometrického důkazu jedinečnosti každého člověka. Tento proces umožňuje bezpečnou a soukromí respektující metodu ověření, že každý uživatel je skutečným a jedinečným člověkem, což je hlavní aspekt pro spravedlivou distribuci tokenů (typ digitálního aktiva) a odolnost vůči různým formám podvodů. [2], [6]

1.1.2 Cíle a vize projektu

Worldcoin byl založen s ambiciózní vizí vytvořit první skutečně globální identitní a finanční síť vlastněnou většinou lidstva. Projekt se snaží adresovat několik zásadních výzev současného digitálního světa, přičemž za nejdůležitější považuje [1]:

1. **Finanční inkluze:** Značná část světové populace nemá přístup k bankovním účtům a základním finančním službám. Worldcoin usiluje o vytvoření alternativního finančního systému, který by byl dostupný každému s přístupem k internetu a chytrému telefonu, bez ohledu na jeho ekonomické či geografické podmínky. [1]

2. **Identifikaci v éře AI:** S rozvojem AI je stále obtížnější rozlišit obsah vytvořeným člověkem a umělé inteligence. Worldcoin nabízí technické řešení tohoto problému prostřednictvím svého systému World ID, který umožňuje spolehlivě ověřit lidskost online. [5]
3. **Spravedlivou distribuci hodnoty:** Projekt vychází z předpokladu, že technologický pokrok, zejména v oblasti AI, vytvoří významné ekonomické hodnoty. Worldcoin si klade za cíl zajistit, aby tyto hodnoty byly spravedlivě distribuovány mezi co největší počet lidí, a nikoliv pouze koncentrovány v rukou několika technologických gigantů. [2]
4. **Sybil rezistenci:** V decentralizovaných systémech je zásadním problémem tzv. Sybil útok, kdy jeden aktér vytvoří mnoho falešných identit, aby získal nad systémem kontrolu nebo ovlivnil jeho chování. Často se vyskytuje v decentralizovaných sítích, jako jsou blockchained nebo peer-to-peer (P2P) neboli klient-klient sítě, kde identita není pevně ověřena. Worldcoin nabízí biometrické řešení tohoto problému, které umožňuje ověřit, že každý účastník sítě představuje skutečnou a jedinečnou osobu. [1]

Sam Altman, jeden ze zakladatelů projektu, naznačil potenciální využití Worldcoinu jako infrastruktury pro budoucí univerzální základní příjem (UBI), který by mohl pomoci zmírnit ekonomické dopady automatizace a umělé inteligence. "Cíl je jednoduchý: Globální finanční a identitní síť založená na důkazu o osobě," uvedl Altman. "To se zdá obzvláště důležité v éře AI. Doufám, že Worldcoin může přispět k diskusím o tom, jak sdílet přístup, výhody a řízení budoucích systémů umělé inteligence." [9]

Zatímco kryptoměna Bitcoin řeší problém důvěry v oblasti financí nahrazením důvěry v instituce důvěrou v matematiku a fyziku, Worldcoin se pokouší řešit fundamentálnější problém: důvěryhodnou identifikaci jedinečných lidských bytostí v digitálním prostoru. Bitcoin odstraňuje potřebu důvěřovat centrálním autoritám, zatímco Worldcoin využívá biometrickou technologii k vytvoření důvěryhodného systému digitální identity. [11]

1.1.3 Koncept důkazu o člověku (Proof-of-Personhood)

Proof-of-Personhood (PoP) neboli důkaz o člověku představuje zásadní technologickou inovaci, kterou Worldcoin přináší do ekosystému Web3 (decentralizovaný internet nové generace). Tento koncept řeší kritický problém digitálních sítí – jak zajistit, že každý účastník je skutečná a jedinečná lidskou bytost, nikoliv bot. [3]

Blockchainové sítě využívají různé konsenzuální mechanismus, což je způsob, jakým se účastníci decentralizované sítě dohodnou na tom, která data (např. transakce) jsou platná a mají být zapsána do blockchainu – tedy jak dosáhnou shody bez potřeby centrální autority. Na rozdíl od tradičních kryptoměn, které používají konsenzuální mechanismy jako Proof-of-Work (PoW) – „důkaz práce“, nebo Proof-of-Stake (PoS) – „důkaz držení“, Worldcoin zavádí zcela nový přístup založený na biometrické verifikaci. Projekt pro tento účel vyvinul Privacy-Preserving Proof-of-Personhood Protocol (PPPoPP), který využívá skenování duhovky oka k vytvoření kryptografického důkazu, že daná osoba je skutečným člověkem v rámci sítě. [1]

PoP získává na významu zejména kvůli rychlému vývoji umělé inteligence. Jak AI modely jako ChatGPT dosahují stále pokročilejších schopností generovat obsah nerozeznatelný od lidského, tradiční metody rozlišování mezi lidmi a automatizovanými systémy (jako CAPTCHA) se stávají neefektivními. Worldcoin argumentuje, že biometrické ověření představuje nejspolehlivější metodu, jak tento problém řešit v globálním měřítku. [7], [1]

Praktické využití konceptu PoP zahrnuje:

- Prevence podvodů a botů na sociálních sítích
- Zajištění spravedlivé distribuce kryptoměn
- Umožnění spravedlivého online hlasování
- Vytvoření základu pro potenciální distribuci UBI
- Efektivnější alokace omezených zdrojů

Koncept PoP představuje zajímavou evoluci oproti konsenzuálním mechanismům jako PoW používaným Bitcoinem. Zatímco Bitcoin využívá výpočetní sílu k zajištění bezpečnosti sítě a dosažení konsensu, což Satoshi Nakamoto¹ nazval "distribuovaným časovým serverem", Worldcoin zavádí biometrickou verifikaci jako způsob identifikace jedinečných účastníků. [11]

¹ Satoshi Nakamoto je pseudonym používaný osobou nebo skupinou osob, která vytvořila Bitcoin, publikovala jeho whitepaper v roce 2008 a vyvinula původní implementaci Bitcoinu. Pravá identita Satoshiho Nakamota zůstává neznámá, neboť tvůrce zmizel z veřejné komunikace v roce 2011.

1.2 Historie vzniku

1.2.1 Zakladatelé Sam Altman a Alex Blania

Worldcoin byl založen Samem Altmanem a Alexem Blaniou, dvěma výraznými osobnostmi z oblasti technologií a AI [9]. Sam Altman, Altman, současný generální ředitel OpenAI – výzkumná laboratoř v oblasti AI, která vyvinula ChatGPT. Před svým působením v OpenAI byl Altman prezidentem Y Combinatoru, prestižního startupového akcelérátoru, a krátce působil i jako generální ředitel společnosti Reddit. [7]

Altman dlouhodobě projevoval zájem o koncept UBI a jeho potenciální roli v budoucím světě transformovaném umělou inteligencí. "UBI je pro mě zajímavý i bez ohledu na AI," uvedl Altman v rozhovoru. "Je to myšlenka, která oslovuje mnoho lidí. Pokud máme společnost dostatečně bohatou na to, aby ukončila chudobu, pak máme morální povinnost zjistit, jak to udělat". [9]

Alex Blania, druhý ze zakladatelů, se stal generálním ředitelem společnosti Tools for Humanity, která stojí za vývojem Worldcoinu. Blania nastoupil do projektu přímo po dokončení magisterského studia fyziky na California Institute of Technology, kde se zaměřoval na výzkum neuronových sítí a teoretické fyziky. Pro Blaniu představoval Worldcoin první profesionální zkušenost, což vedlo k tomu, že mu Altman poskytl mentory a kouče pro rozvoj manažerských dovedností. Mezi jeho kouči byl například Matt Mochary, který dříve mentoroval samotného Altmana a zakladatele Coinbase (jedna z nejvýznamnějších kryptoměnových burz) Briana Armstronga. [9]

Třetím spoluzakladatelem byl Max Novendstern, který dříve pracoval ve společnosti Wave (společnost zaměřená na mobilní peněžní služby v Africe). Novendstern však v červenci 2021 projekt opustil. [8]

Oba hlavní zakladatelé přinesli do projektu doplňkové perspektivy – Altmanovy zkušenosti s rozvojem AI a jeho zájem o socioekonomické dopady technologického pokroku se doplňují s Blaniovým technickým zázemím a výzkumnými zkušenostmi v oblasti fyziky a AI.

1.2.2 Vznik společnosti Tools for Humanity

Worldcoin byl vyvíjen a spravován společností Tools for Humanity (TFH), která byla založena specificky pro tento účel. Jedná se o společnost se sídlem v San Franciscu

v Kalifornii (USA), která má také dceřinou společnost Tools for Humanity GmbH sídlící v Německu. [1]

Společnost TFH byla zodpovědná za vývoj klíčových komponent Worldcoinu během jeho víceleté testovací fáze. Nejdůležitějšími výstupy jejího vývoje byly biometrické zařízení Orb a aplikace World App, která slouží jako peněženka a rozhraní pro interakci s ekosystémem Worldcoin. [1]

V roce 2022 byla založena nezisková organizace World Foundation jako neutrální správce protokolu Worldcoin. Tato organizace je registrovaná na Kajmanských ostrovech a nemá žádné vlastníky ani akcionáře. World Foundation také vlastní dceřinou společnost nazvanou World Assets Limited, která je zodpovědná za vydávání Worldcoin tokenů (WLD) alokovaných pro komunitu Worldcoin. [1]

Mise společnosti TFH byla definována jako "vybudování spravedlivějšího ekonomického systému", přičemž tato vize se promítla do způsobu, jakým byl Worldcoin navržen a vyvíjen, s důrazem na globální dostupnost, soukromí a spravedlivou distribuci. TFH postupně přesouvá odpovědnost za protokol Worldcoin na World Foundation. [1]

Klíčové milníky vývoje

Vývoj projektu Worldcoin lze rozdělit do několika fází, které formovaly jeho současnou podobu:

Rané fáze výzkumu a vývoje (2019-2020): Projekt byl původně koncipován jako "bitcoin project" s cílem volně distribuovat kryptoměnu lidem po celém světě. V této fázi byly vytvořeny první prototypy Orbu, které byly značně odlišné od současné verze – měly například slot (úložný prostor/otvor) pro vydávání fyzických mincí obsahujících kryptografické klíče k bitcoinu. [9]

Alpha fáze (květen 2021–leden 2022): První fáze testování začala v květnu 2021. Během této fáze byli uživatelé zapojeni prostřednictvím webové aplikace a za ověření své identity jim bylo rezervováno WLD v hodnotě 20 USD. [1]

Beta fáze (listopad 2021–červenec 2023): V listopadu 2021 začala beta fáze s vydáním první mobilní aplikace Worldcoin. V průběhu této fáze se aplikace postupně stávala dostupnou ve více zemích (např. Keňa, Ghana, Súdán, Norsko aj.). Mezi únorem 2022 a květnem 2023 mohli všichni jedinci, kteří se ověřili prostřednictvím Orbu, nárokovat 25

Beta WLD tokenů. Od května 2023 do oficiálního spuštění byl systém modifikován tak, že každý ověřený jedinec mohl nárokovat 1 Beta WLD token za kalendářní týden. [1]

Dosažení milníku 1 milionu ověřených uživatelů (leden 2023): V lednu 2023 oznámila společnost TFH, že technologie Orb byla použita k verifikaci více než jednoho milionu unikátních lidí. Tento milník demonstroval růst technologie a její přijetí v různých regionech světa. [6]

Významné investiční kolo (květen 2023): V květnu 2023 projekt oznámil získání investice ve výši 115 milionů dolarů vedenou společnostmi Blockchain Capital, a16z crypto a Bain Capital Crypto. Toto financování poskytlo projektu potřebné zdroje pro přípravu oficiálního spuštění. [19]

Oficiální spuštění (24. července 2023): Worldcoin a jeho nativní token WLD byly oficiálně spuštěny 24. července 2023. K tomuto datu projekt deklaroval více než 2 miliony verifikovaných uživatelů a plány na rozšíření sítě Orbů do 35 měst ve 20 zemích po celém světě. [10]

Regulatorní výzvy (srpen 2023): Krátce po spuštění projektu se Worldcoin setkal s regulatorním odporem v několika zemích, včetně Německa, Francie, Argentiny a Velké Británie, především kvůli obavám z praktik sběru dat. Úřady v Keni dokonce nařídily pozastavení operací Worldcoinu a provedly razii skladu využívaného společností TFH. [10]

Migrace na World Chain (říjen 2024): V říjnu 2024 Worldcoin oznámil migraci z Optimismu na novou síť nazvanou World Chain, která se stala hlavní platformou pro přístup a využití WLD tokenů. [1]

1.3 Technologické základy

1.3.1 World ID protokol

World ID je decentralizovaný digitální identitní protokol, který představuje technologické jádro ekosystému Worldcoin, které realizuje koncept důkazu o člověku v praxi při zachování vysoké míry soukromí. [4]

Protokol World ID je v podstatě digitální pas, který umožňuje uživateli prokázat, že je jedinečnou a skutečnou osobou, aniž by musel odhalit svou totožnost. K ověřování používá biometrickou technologii, konkrétně tzv. AI-safe Proof of Personhood neboli důkaz o osobě odolný vůči AI, který je vydáván zařízením Orb. [4]

Fungování World ID protokolu spočívá v následujícím procesu [1]:

1. Uživatel si stáhne aplikaci World App a vygeneruje pár kryptografických klíčů – veřejný a soukromý.
2. Uživatel navštíví lokaci s Orbem, kde proběhne skenování jeho duhovky.
3. Orb zpracuje biometrická data lokálně a vytvoří jedinečný hash (matematická funkce pro převod vstupních dat do malého čísla), který je porovnán s databází, aby se zajistilo, že daný člověk ještě nebyl registrován.
4. Pokud je ověření úspěšné, veřejný klíč uživatele je přidán do množiny ověřených identit na blockchainu.

Pro následné používání své identity uživatel nevyužívá přímo svá biometrická data, ale kryptografické metody známé jako zero-knowledge důkazy (ZKP), které umožňují prokázat, že je vlastníkem ověřené identity, aniž by odhaloval konkrétní identifikační údaje. [1]

Tyto důkazy lze generovat přímo z mobilního zařízení uživatele a mohou být integrovány s třetími stranami pomocí Software Development Kitu (SDK) - soubor nástrojů, které vývojářům umožňují vytvářet aplikace pro konkrétní platformu, operační systém nebo programovací jazyk. [1]

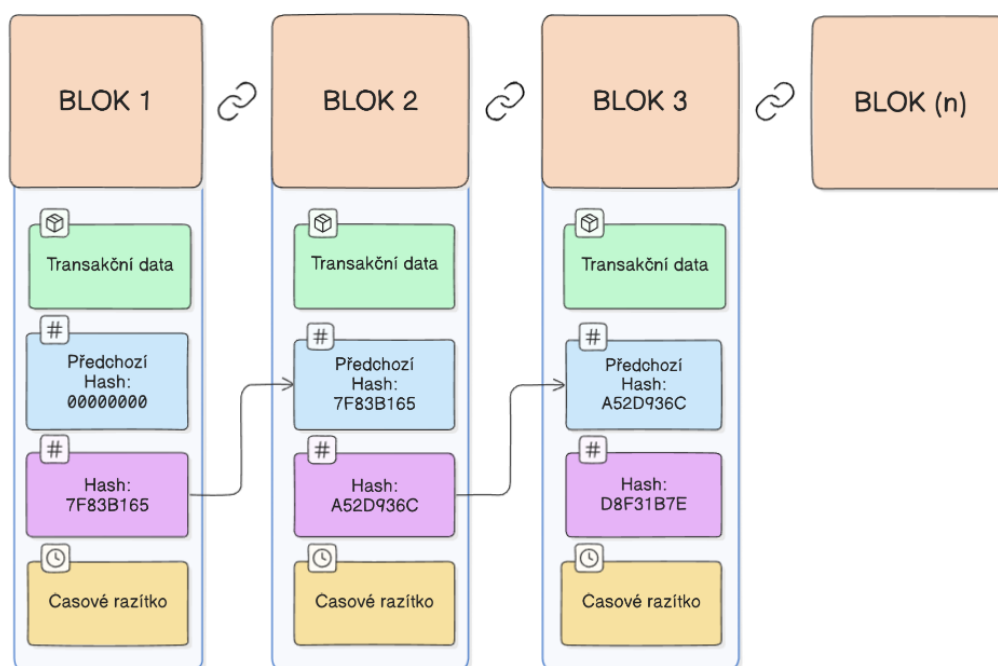
World ID umožňuje tzv. "Sign in with Worldcoin" funkci, která poskytuje bezproblémové přihlašování k webovým stránkám, mobilním aplikacím a decentralizovaným aplikacím (dApps)². Uživatelé mohou soukromě sdílet své ověření

² Decentralizované aplikace (dApps) - aplikace běžící na blockchainu bez centrální kontroly

osoby, včetně telefonního čísla pro usnadnění, nebo biometrických údajů pro maximální úroveň jistoty. [4]

1.3.2 Architektura blockchainu

Blockchain představuje hlavní technologii stojící za Worldcoinem a dalšími kryptoměnami. Jedná se o distribuovanou databázi nebo digitální účetní knihu, která ukládá informace v blocích, které jsou kryptograficky propojeny a zabezpečeny. Každý blok obsahuje sadu transakcí (přesun digitálních aktiv mezi dvěma adresami v blockchainové síti) a odkaz (hash) na předchozí blok, čímž vytváří řetězec bloků – odtud název "blockchain". Tato struktura zajišťuje, že data nemohou být zpětně změněna bez změny všech následujících bloků a souhlasu většiny sítě. [4]



Obrázek 1 Zjednodušené schéma bloků v blockchainu

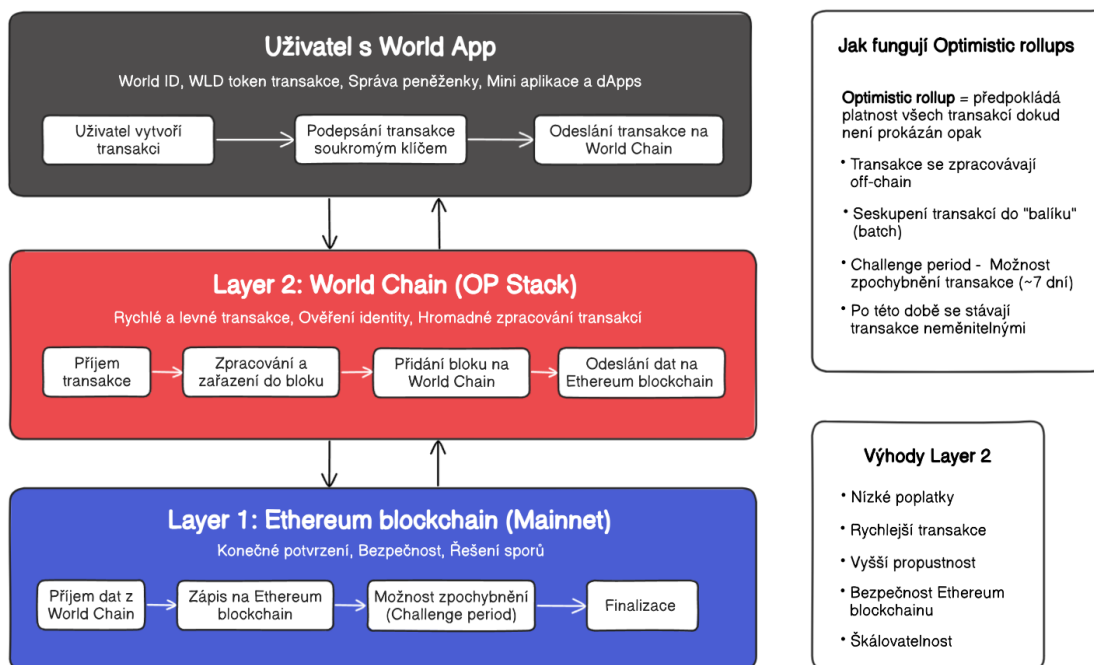
(zdroj: vlastní)

Worldcoin staví svou infrastrukturu na osvědčené a robustní technologii blockchainu Ethereum, což mu poskytuje výhody stabilního a bezpečného ekosystému s rozsáhlou vývojářskou komunitou. Token WLD funguje na hlavní síti Ethereum (Mainnet), vytvořený podle standardu ERC-20, což je široce používaný protokol zajišťující kompatibilitu s většinou kryptoměnových peněženek a burz. [5]

Pro zajištění efektivního každodenního fungování a optimalizaci transakčních nákladů využívá Worldcoin tzv. vrstvené (L2) řešení (viz. Obrázek 2). Původně to byl Optimism, škálovací řešení postavené nad Ethereum, které výrazně snižuje transakční poplatky a zvyšuje rychlost transakcí. Od října 2024 je hlavní platformou pro přístup a využití WLD tokenů síť World Chain, která je také založena na technologii OP Stack nad Ethereum (modulární open-source framework (technologický základ) od společnosti Optimism). [1]

Architektura World Chainu kombinuje on-chain (přímo na blockchainu) a off-chain (mimo blockchain) komponenty. Zatímco blockchain slouží jako veřejná, neměnná vrstva pro ukládání a verifikaci dat, složitější výpočty a zpracování dat probíhají mimo blockchain. Například biometrické zpracování a vytváření hashů probíhá lokálně na Orbu, zatímco blockchain uchovává pouze informace o ověřených identitách. [1]

Pro optimalizaci nákladů na transakce a škálovatelnost využívá World Chain tzv. "zk-rollup" přístup, kdy se více transakcí zpracovává hromadně, což výrazně snižuje množství dat, která je třeba zapisovat na hlavní blockchain. Tento přístup umožňuje, aby náklady na registraci jednoho uživatele byly zlomkem toho, co by stály na samotném Ethereum. [1]



Obrázek 2 Zjednodušené znázornění architektury Worldcoin

(zdroj: vlastní)

1.3.3 Zero-knowledge důkazy

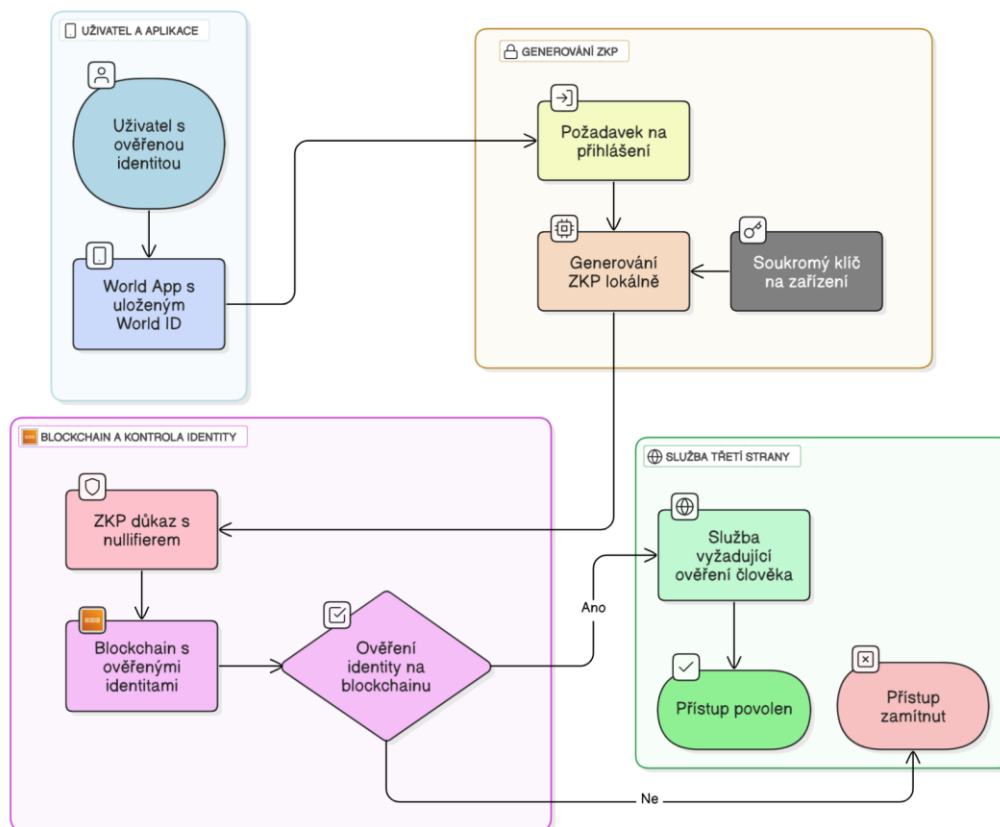
ZKP představují klíčovou kryptografickou technologii v protokolu World ID, která zásadně přispívá k ochraně soukromí uživatelů. Tato metoda umožňuje jedné straně prokázat pravdivost tvrzení bez odhalení jakýchkoliv dalších informací. [1]

V ekosystému Worldcoin slouží ZKP k vytvoření důkazu, že uživatel je registrovaným členem sítě s ověřenou identitou, aniž by byla odhalena jeho skutečná identita nebo biometrická data. Po získání World ID může uživatel generovat tyto důkazy přímo z aplikace World App, čímž prokazuje vlastnictví soukromého klíče odpovídajícího veřejnému klíči v množině ověřených identit, zároveň však chrání svou anonymitu. [1], [2]

Worldcoin využívá specifický typ ZKP známý jako důkaz Groth16, který je implementován v rámci protokolu Semaphore (protokol umožňující anonymní ověření příslušnosti ke skupině a tvorbu zpráv nebo akcí, bez odhalení identity). Tyto důkazy umožňují uživatelům dokázat, že znají soukromý klíč k jednomu z veřejných klíčů v on-chain identitním souboru, aniž by odhalili, který konkrétně. [1]

Worldcoin implementuje specifický typ ZKP známý jako důkaz Groth16 v rámci protokolu Semaphore. Pro prevenci vícenásobného využití stejné identity (např. pro opakované nárokování tokenů) systém využívá tzv. "nullifiery" - jedinečné identifikátory generované z kombinace soukromého klíče uživatele a kontextu akce. [1]

Pro lepší pochopení procesu ZKP slouží následující diagram, který znázorňuje jednotlivé kroky ověření identity:



Obrázek 3 Diagram ověření identity uživatele pomocí World App a ZKP

(zdroj: vlastní)

Tento proces eliminuje potřebu sdílet citlivá data a představuje kompromis mezi transparentností blockchainu a ochranou soukromí, který je pro fungování systému Worldcoin zásadní.

1.3.4 Kryptografické principy

Worldcoin staví na několika základních kryptografických principech, které zajišťují bezpečnost, soukromí a důvěryhodnost celého systému [1]:

Asymetrická kryptografie:

- Využívá páry veřejných a soukromých klíčů
- Když si uživatel vytvoří účet Worldcoin, aplikace vygeneruje pár kryptografických klíčů
- Veřejný klíč se používá k vygenerování QR kódu, který Orb přečte před skenováním duhovky
- Soukromý klíč zůstává pod kontrolou uživatele a je nezbytný pro podepisování transakcí a prokazování vlastnictví WLD tokenů

Hašování:

- V případě Worldcoinu se sken duhovky převádí na řetězec čísel známý jako hash
- Využívá jednosměrnou funkci, což činí prakticky nemožným znovu vytvořit původní obraz
- Tato ochrana funguje i v případě, že by byl hash kompromitován
- Worldcoin používá specificky hašovací funkci Poseidon nad skalárním polem BN254 (typ eliptické křivky používané v kryptografii, s čísly o velikosti 254 bitů)

Commitment schémata a Merkleho stromy:

- **Commitment** lze chápat jako způsob, jak se "zavázat" k určité hodnotě, aniž by byla odhalena (např. uživatel se zaváže ke své biometrické identitě)
- Umožňuje pozdější odhalení hodnoty (Uživatel později může prokázat, že je vlastníkem těchto dat)
- **Merkleho stromy** jsou datové struktury umožňující efektivní a bezpečné ověření velkého množství dat
- V kontextu Worldcoinu jsou tyto struktury používány k ukládání a ověřování identity uživatelů v síti

Off-chain výpočty s on-chain verifikací:

- Tento přístup kombinuje výhody soukromí a efektivity off-chain zpracování
- Zároveň využívá bezpečnost a transparentnost blockchainu
- Složité výpočty probíhají mimo blockchain, zatímco jejich výsledky jsou ověřovány na blockchainu

Batch processing (dávkové zpracování):

- Technologie pro efektivní zápis velkého množství nových uživatelů na blockchain
- Vytváří dávkové důkazy, které verifikují správnost zápisu celé množiny uživatelů najednou
- Tímto způsobem se náklady na transakce rozprostřou mezi mnoho uživatelů
- Výrazně zvyšuje efektivitu celého systému a podporuje škálovatelnost

Tyto principy společně vytvářejí pevný technologický základ, který umožňuje Worldcoinu fungovat jako bezpečný, soukromí respektující a efektivní ekosystém. [1]

1.4 Orb – biometrické ověřování

1.4.1 Konstrukce a funkce Orbu

Orb představuje unikátní hardwarové zařízení ve tvaru koule, které tvoří technologický základ pro biometrické ověřování identity v ekosystému Worldcoin. Jeho primárním účelem je skenování duhovky oka uživatelů pro vytvoření unikátního biometrického identifikátoru, který poté využívá World ID. [6]



Obrázek 4 Zařízení Orb

(zdroj: [1])

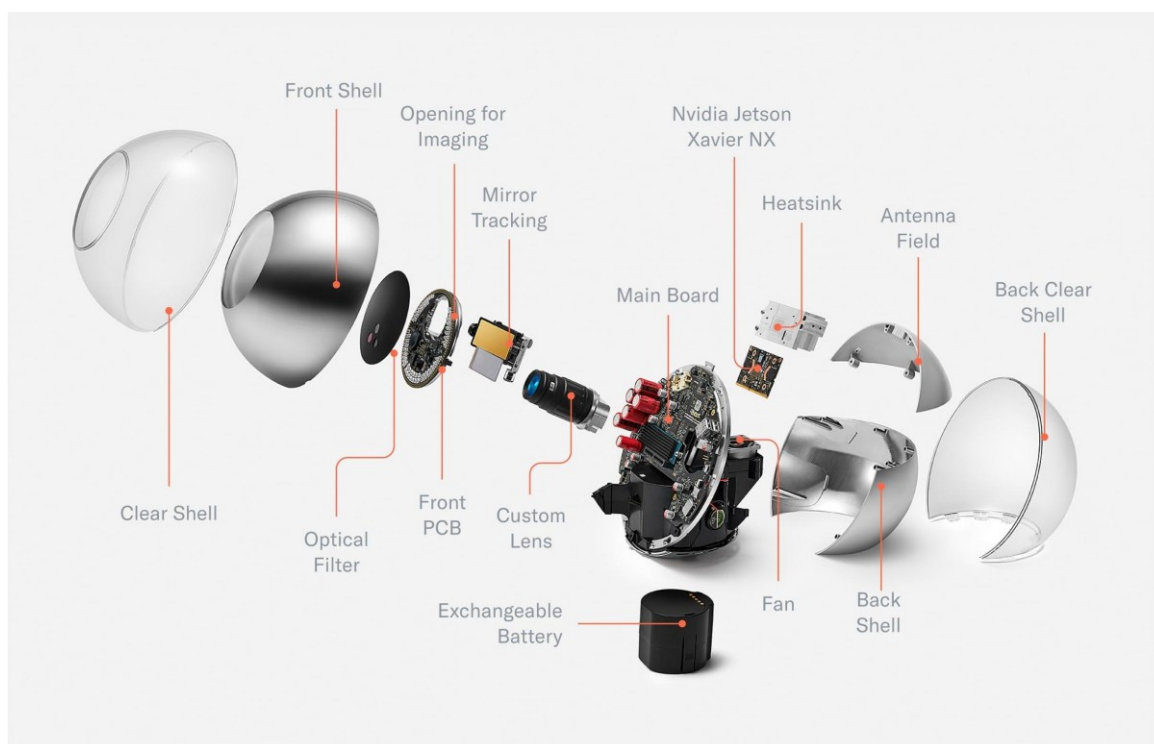
Z designového hlediska je Orb navržen jako sférický objekt s chromovým povrchem a skleněným otvorem v přední části, který umožňuje optickému systému uvnitř zařízení zachytit detailní snímky duhovky. Kouli navrhoval Thomas Meyerhoffer, který byl prvním designérem najatým Jonym Ivem v Applu (legendární designér iMacu, iPodu a iPhoneu). Samotný kulový tvar a náklon osy o 23,5 stupně (stejně jako Země) má symbolizovat globální povahu projektu Worldcoin a jeho ambici sloužit všem lidem planety. [2], [6], [9]

Technicky se Orb skládá z několika klíčových komponent [6]:

1. **Hlavní výpočetní jednotka** – založená na čipu Nvidia Jetson Xavier NX, který poskytuje dostatečný výkon pro zpracování biometrických dat v reálném čase
2. **Optický systém** – zahrnující teleobjektiv s úzkým zorným polem a 2D gimbalové zrcadlo³

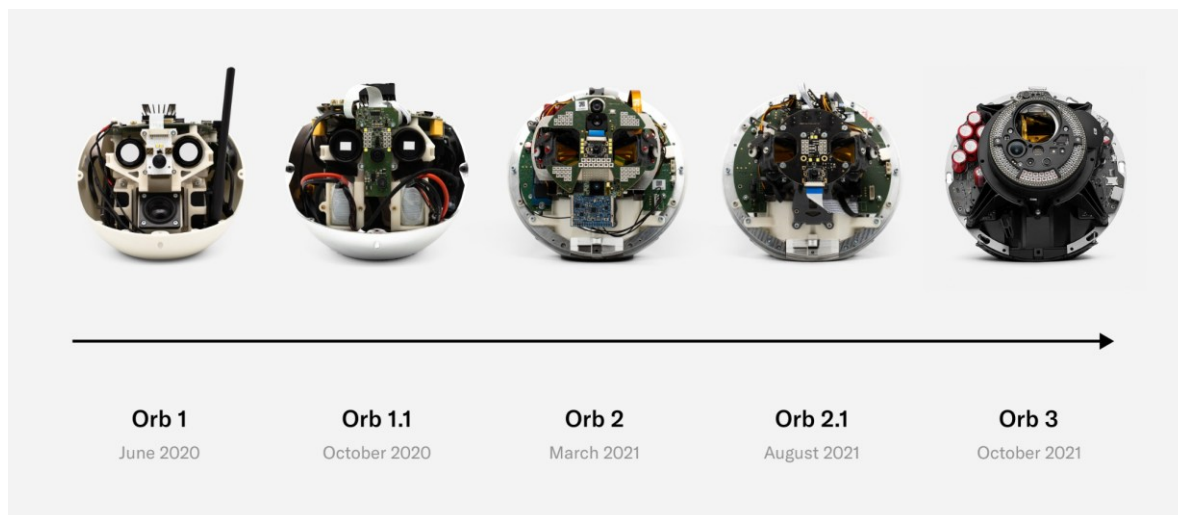
³ Gimbal = mechanické zařízení umožňující volnou rotaci připojené součásti, v tomto případě zrcadla, kolem dvou (2D) nebo tří (3D) navzájem kolmých os.

3. **Soustava kamer a senzorů** – multispektrální kamery včetně širokoúhlé kamery, termální kamery a 3D Time-of-Flight kamery (měří vzdálenost k objektům vysíláním světelných pulzů (obvykle infračervených) a měřením času, za který se světlo odrazí zpět do snímače)
4. **Osvětlovací systém** - 79 infračervených LED diod různých vlnových délek (740nm, 850nm a 940nm) pro optimální snímání duhovky
5. **Bezpečnostní systémy** – včetně zabezpečeného prvku (secure element) pro podepisování dat a detekce neoprávněné manipulace
6. **Komunikační rozhraní** – Wi-Fi, volitelné LTE a GPS modul
7. **Vyměnitelná baterie** – vyrobená z Li-Ion článků typu 18650 s kapacitou přibližně 100Wh



Obrázek 5 Rozklad komponentů orbu

(zdroj: [1])



Obrázek 6 Tři roky výzkumu a vývoje Orbu

(zdroj:[1])

Proces ověření identity prostřednictvím Orbu funguje následovně [6]:

1. Příprava uživatele

- Uživatel se postaví před zařízení Orb (ve vzdálenosti na délku paže) a hledí přímo do zařízení

2. Detekce a zachycení snímku

- Širokoúhlá kamera zachytí scénu a neuronová síť detekuje pozici očí.
- Následně gimbalové zrcadlo nasměruje teleobjektiv na duhovku oka pro zachycení detailního snímku
- Tento snímek je okamžitě zpracován pomocí neuronových sítí běžících na výpočetní jednotce Orbu

3. Ověření a vytvoření hash kódu

- Systém ověří, že se jedná o skutečného člověka (nikoli o fotografii apod.)
- následně vytvoří unikátní hash kód duhovky, který je porovnán s databází již registrovaných uživatelů

1.4.2 Technologie skenování duhovky

Technologie skenování duhovky implementovaná v Orbu představuje pokročilý biometrický systém, který využívá specifických vlastností lidské duhovky pro vytvoření unikátního

identifikátoru. Worldcoin zvolil duhovku jako primární biometrickou údaj z několika důvodů [1]:

1. **Vysoká entropie dat** – duhovka obsahuje výrazně více unikátních rysů než jiné biometrické metody
2. **Stabilita v průběhu života** – struktura duhovky zůstává relativně neměnná po celý život
3. **Extrémně nízká míra falešných shod** – pravděpodobnost, že dvě různé duhovky budou vyhodnoceny jako shodné je téměř nulová
4. **Odolnost proti podvodům** – duhovku je výrazně obtížnější zfalšovat než například otisk prstu

Orb využívá k zachycení detailního obrazu duhovky specializovaný optický systém.

Hlavní komponenty tohoto systému zahrnují [6]:

- **Teleobjektiv s úzkým zorným polem** – přibližně 5° zorné pole, optimalizovaný pro snímání v blízkém infračerveném spektru
- **Globální závěrka kamery** – eliminuje pohybové rozmazání, což je kritické pro zachycení mikroskopických detailů v textuře duhovky
- **Tekutá čočka** – umožňuje rychlé automatické zaostření řízené neuronovými sítěmi
- **Infračervené osvětlení** – synchronizované pulzní osvětlení různých vlnových délek pro optimální kontrast a detailnost snímku
- **2D gimbalové zrcadlo** – dynamicky upravuje zorné pole kamery, čímž výrazně zvyšuje prostor, v němž může být úspěšně provedeno skenování



Obrázek 7 Teleobjektiv a gimbalový systém

(zdroj:[1])

Orb dosahuje velmi vysokého rozlišení než standardy používané v běžných systémech pro rozpoznávání duhovky. Tato vysoká kvalita snímků je zásadní pro minimalizaci chybovosti při identifikaci a zajištění co nejširší použitelnosti systému pro různé typy uživatelů. Systém je navržen tak, aby fungoval spolehlivě za různých světelných podmínek a s různými typy duhovek, včetně tmavých, které mohou být problematické pro snímání ve viditelném spektru. [6]



Obrázek 8 Srovnání kvality snímku duhovky z Orbu versus běžný standard

(zdroj:[1])

Pro ověření pravosti snímané duhovky (tzv. liveness detection, neboli „detekce živosti“) využívá Orbu kombinaci multispektrálního snímání a neuronových sítí běžících v reálném čase. Tyto technologie dokážou rozpoznat a odmítnout potenciální pokusy o podvod, jako je například použití fotografie, kontaktních čoček nebo jiných metod, které by mohly obejít biometrické ověření. [6]

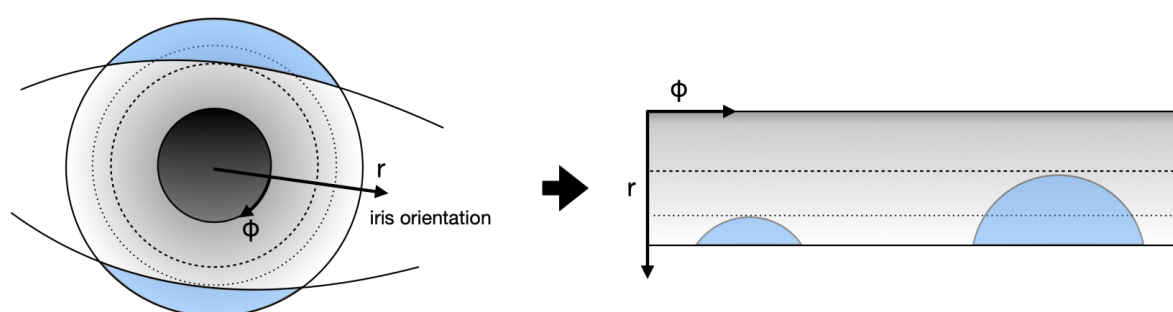
1.4.3 Zpracování biometrických dat

Zpracování biometrických dat v systému Worldcoin je navrženo s důrazem na maximální ochranu soukromí uživatelů. Po zachycení snímku duhovky prostřednictvím Orbu následuje komplexní proces zpracování, který transformuje raw (surová) biometrická data do formy, která zachovává anonymitu a zároveň umožňuje spolehlivou identifikaci jedinečnosti osoby. [1]

V první fázi zpracování je snímek duhovky segmentován pomocí pokročilých algoritmů počítačového vidění. Tento proces identifikuje a izoluje klíčové oblasti oka – duhovku, zornici a skléru (bělmo). Za tímto účelem Worldcoin vyvinul model založený na architektuře DeepLabv3+ (systém pro segmentaci obrazu vyvinutý společností Google) s páteří sítí MobileNet v2 (neuronová síť navržena pro mobilní zařízení k dosažení vysoké

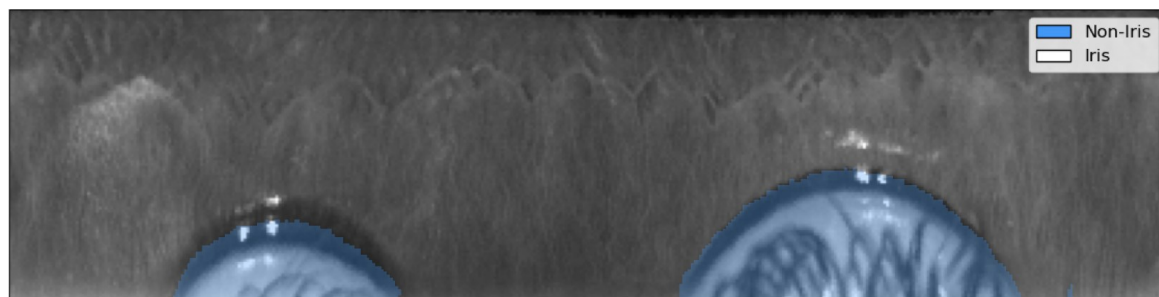
přesnosti při nízké výpočetní rychlosti), který dokáže efektivně izolovat relevantní oblasti oka. [1]

Následuje normalizace, která převádí prstencovou oblast duhovky do standardizovaného obdélníkového formátu. Tento proces eliminuje variace způsobené různou velikostí duhovky, dilatací zornice nebo pozicí oka v záběru. Normalizované snímky duhovky jsou následně zpracovány pomocí banky Gaborových filtrů – matematické nástroje, které rozpoznávají vzory a textury v obraze pomocí vlnových funkcí v různých směrech a měřítkách. [1]



Obrázek 9 Proces transformace kruhové duhovky do obdélníkového formátu

(zdroj:[1])

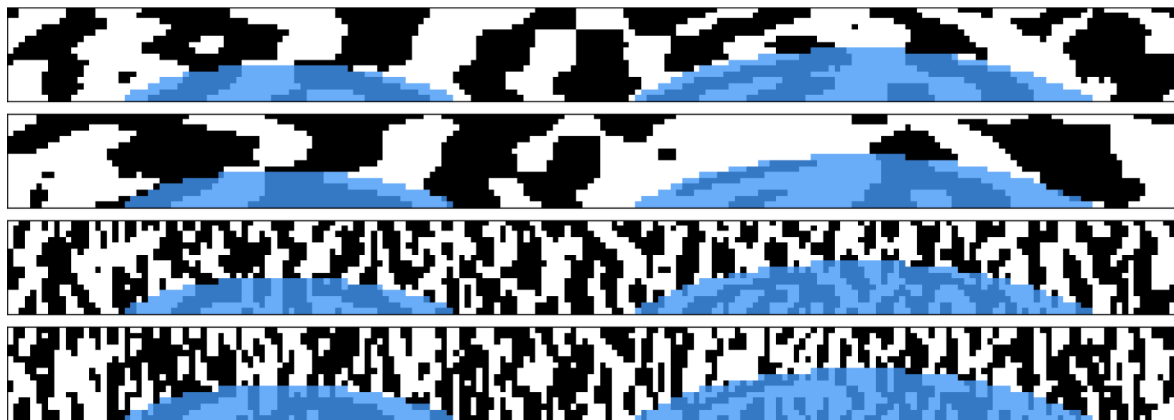


Obrázek 10 Výsledek normalizace

(zdroj:[1])

Zásadním krokem je generování tzv. "IrisHash" - kryptografického otisku duhovky. Tento proces využívá Gaborovy filtry, které jsou aplikovány na normalizovaný obraz duhovky. Výsledkem jsou složité matematické hodnoty. Z těchto hodnot si vezme jen informaci o tom, kde přesně se nachází vzory v duhovce, a převede ji do jednoduchého binárního kódu. Tento postup záměrně ignoruje informaci o tom, jak jsou jednotlivé části

duhovky světlé nebo tmavé, protože jas snímku se může měnit podle osvětlení nebo kontrastu. [1]



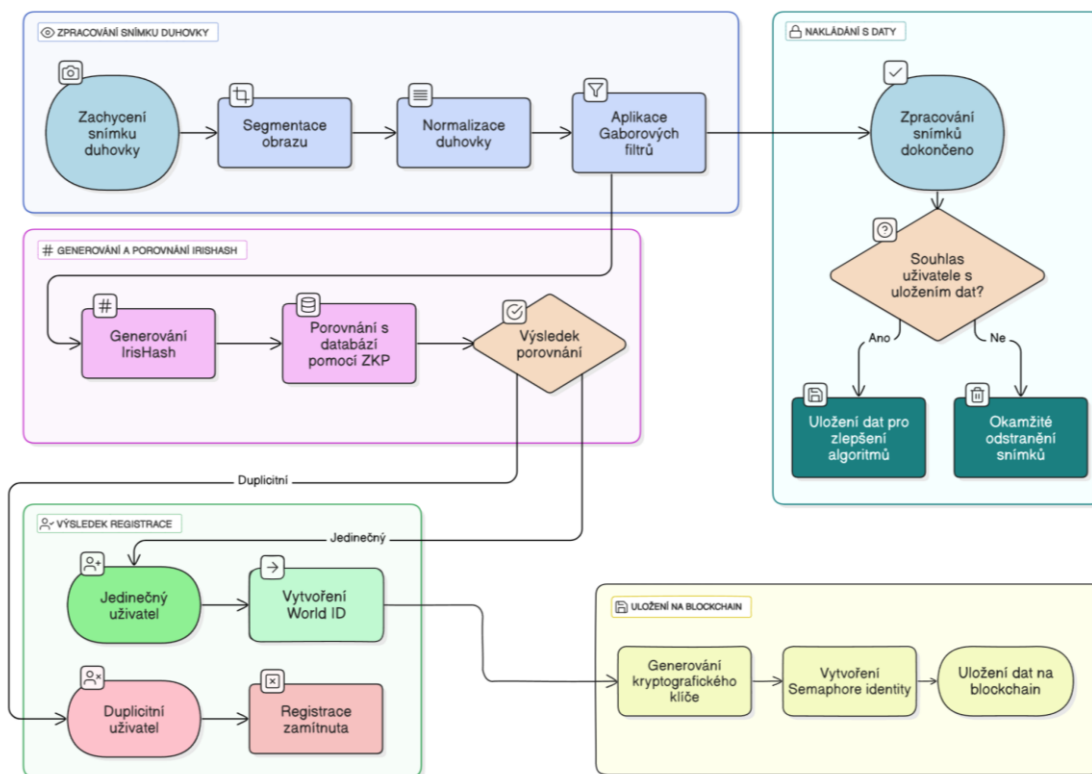
Obrázek 11 Konkrétní příklad anonymizovaného iris kódu

(zdroj:[1])

Výsledný IrisHash obsahuje více než 10 000 bitů informací a zůstává uložen lokálně na Orbu. Místo sdílení tohoto hashe je používán k ověření, zda daný hash již existuje v databázi Worldcoinu, k čemuž se využívají ZKP. Pokud algoritmus najde shodu, indikuje to, že daná osoba se již pokoušela o registraci. Pokud shodu nenajde, jedinec prošel kontrolou jedinečnosti a může pokračovat v registraci. [1]

Důležitým aspektem zpracování dat je, že původní snímky duhovky jsou standardně okamžitě po zpracování odstraněny. Uživatelé mají možnost explicitně souhlasit s uchováním jejich biometrických dat pro účely zlepšení algoritmů, ale tato volba není výchozím nastavením a vyžaduje aktivní souhlas. [1]

Pro srozumitelnou vizualizaci toku zpracování biometrických dat od skenování duhovky až po vytvoření digitální identity nám slouží následující diagram:



Obrázek 12 Proces zpracování biometrických dat v systému Worldcoin

(zdroj: vlastní)

1.4.4 Bezpečnostní opatření a ochrana dat

Worldcoin implementuje vícevrstvý přístup k bezpečnosti a ochraně biometrických dat zpracovávaných prostřednictvím Orbu. Tato opatření jsou navržena tak, aby adresovala oprávněné obavy týkající se soukromí a bezpečnosti, které jsou nevyhnutelně spojeny se sběrem a zpracováním citlivých biometrických informací.

Hardwarová bezpečnost Orbu

Orb je navržen s několika úrovněmi ochrany [6], [1]:

- **Zabezpečený boot proces** – zajišťuje, že zařízení může provozovat pouze autorizovaný firmware
- **Trusted Execution Environment (TEE)** – poskytuje izolované prostředí pro zpracování citlivých dat, což zabraňuje jejich úniku i v případě kompromitace operačního systému
- **Secure Element** – specializovaný čip pro bezpečné ukládání kryptografických klíčů a podepisování dat
- **Systém detekce neoprávněné manipulace** – může zařízení deaktivovat při zjištění pokusu o fyzický průnik

Bezpečnost přenosu dat

Pro ochranu dat během přenosu mezi Orbem a infrastrukturou Worldcoinu jsou implementována komplexní opatření [1]:

- **End-to-end šifrování** – zajišťuje, že data nemohou být zachycena a dešifrována třetí stranou
- **Digitální podpisy** – data přenášená z Orbu jsou digitálně podepsána bezpečnostním prvkem, což umožňuje ověřit jejich původ a integritu
- **Minimalizace přenášených dat** – z Orbu jsou přenášeny pouze nezbytně nutné informace, nikoliv samotná biometrická data

Ochrana soukromí uživatelů

Pro ochranu dat během přenosu mezi Orbem a infrastrukturou Worldcoinu jsou implementována široká bezpečnostní opatření [1]:

- **Lokální zpracování** – biometrická data jsou zpracována přímo na Orbu, což eliminuje rizika spojená s přenosem těchto citlivých informací
- **Okamžité odstranění dat** – snímky duhovky jsou ve výchozím nastavení okamžitě po zpracování odstraněny
- **Vyžadován explicitní souhlas** – pro případné uchování biometrických dat za účelem zlepšení algoritmů je vyžadován výslovný souhlas uživatele

- **Využití Zero-Knowledge Proofs (ZKP)** - celý ekosystém Worldcoinu využívá technologii ZKP

Regulatorní soulad

V oblasti regulatorního souladu se Worldcoin zavazuje k dodržování relevantních předpisů o ochraně dat [3]:

- **Soulad s GDPR** – společnost deklaruje zpracování dat v souladu s obecným nařízením o ochraně osobních údajů
- **Data Protection Officer (DPO)** - Worldcoin zaměstnává pracovníka pro ochranu údajů, který dohlíží na soulad s předpisy
- **Posouzení dopadu (DPIA)** - společnost provádí systematické hodnocení rizik a jejich zmírňování prostřednictvím posouzení dopadu na ochranu osobních údajů

I přes tato bezpečnostní opatření se projekt setkal s regulatorními problémy, které již byly nastíněny v předchozí kapitole 1.2 věnující se jeho historickému vývoji. Tyto problémy ukazují složitost implementace biometrických technologií v globálním měřítku.

2 TĚŽBA, SMĚNA A PLATBY POMOCÍ WORLDCOIN

2.1 Získávání Worldcoinu

2.1.1 Přidělování grantu WLD tokenů

Worldcoin implementuje systém distribuce své kryptoměny založený na "user grants" (uživatelských grantech). Grant tedy znamená přidělení (darování) určitého množství WLD tokenů uživatelům, kteří se verifikovali v systému pomocí Orbu. [1]

Systém distribuce WLD tokenů [16]:

- Celková maximální nabídka: 10 miliard WLD tokenů (pevný limit)
- Cíl Worldcoin Foundation: rozdělit min. 60 % tokenů mezi uživatele
- K začátku června 2025: distribuováno přes 575 milionů WLD tokenů
- Počet ověřených uživatelů: 12+ milionů
- Hodnota WLD (k 4. 6. 2025): ~1,2 USD [12]

Základní principy distribuce [1]:

1. **Inkluzivita:** Každý jedinečný člověk je oprávněn nárokovat granty
2. **Rovnost:** Všichni ověření uživatelé mohou nárokovat stejné množství tokenů
 - Nezávisí na geografické lokaci či ekonomickém zázemí
 - Výjimka: některé jurisdikce (např. Čína) z regulačních důvodů [3]
3. **Udržitelnost:** Granty jsou poskytovány opakovaně, s hodnotou klesající v čase
 - Motivuje k včasnému zapojení do sítě

Typy grantů [1]:

1. **První grant** po verifikaci Orbem
 - Počáteční hodnota: 1 WLD token
 - Představuje první část distribuce novým uživatelům
2. **Opakující se granty**
 - Dostupné pro nárokování každý měsíc
 - Pro již verifikované uživatele

System je navržen s pevným limitem 10 miliard WLD tokenů, což zajišťuje jejich omezenou nabídku, ale neomezuje škálování sítě, jelikož každý token je dělitelný na menší jednotky, podobně jako u bitcoinu. Tato dělitelnost umožňuje provádět mikrotransakce i při rostoucí hodnotě tokenů a zvyšujícím se počtu uživatelů. Postupné uvolňování grantů podporuje udržitelnost ekosystému, zabráňuje centralizaci moci a rychlému vyčerpání zdrojů, což přispívá k dlouhodobé stabilitě celého projektu. [1]

Mechanismus nárokování WLD grantů

Proces nárokování WLD tokenů prostřednictvím World App zahrnuje několik kroků [16]:

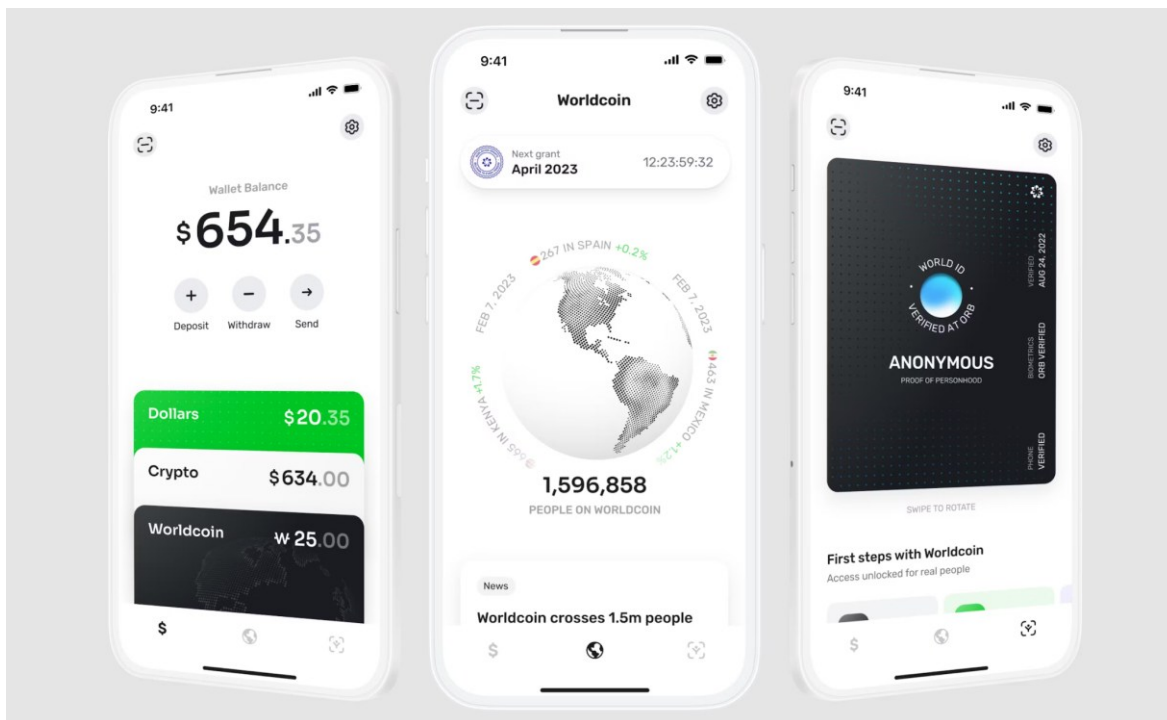
1. **Stažení a instalace World App** – Pro zapojení do protokolu Worldcoin musí uživatelé nejprve stáhnout World App, první peněženkovou aplikaci, která podporuje vytvoření World ID.
2. **Verifikace pomocí Orbu** – Uživatelé mohou získat Worldcoin pomocí World App, která umožňuje uživatelům získat Worldcoin naskenováním jejich očí pomocí Orbu. Tento proces ověřuje jedinečnost každého uživatele a to, že je skutečnou lidskou bytostí. [12]
3. **Nárokování tokenů** – Po úspěšné verifikaci mohou uživatelé přímo v aplikaci nárokovat své WLD tokeny. Aplikace uživatelům připomíná, kdy je k dispozici nový grant, který si mohou nárokovat pomocí svého ověřeného World ID. [12]
4. **Správa získaných tokenů** – Po získání WLD tokenů mohou uživatelé tyto tokeny uchovávat v aplikaci, směňovat je za jiné kryptoměny, nebo je použít v rámci ekosystému Worldcoin.

2.1.2 World App a uživatelské rozhraní

World App představuje primární uživatelské rozhraní pro interakci s ekosystémem Worldcoin. Tato mobilní aplikace byla vyvinuta společností Tools for Humanity jako první frontend pro World ID a je dostupná pro platformy iOS i Android. Aplikace byla navržena tak, aby poskytovala bezproblémový přístup ke globální decentralizované finanční infrastruktuře. [1], [16]

World App plní několik funkcí v rámci ekosystému Worldcoin. Primárně slouží jako úložiště pro World ID. Aplikace umožňuje uživatelům bezpečně a anonymně prokázat, že jsou jedinečným člověkem v online prostředí pomocí World ID, používat digitální aktiva, přistupovat k Mini Aplikacím a nárokovat si tokeny Worldcoin. [1], [16]

Zároveň funguje jako plnohodnotná kryptoměnová peněženka, která umožňuje přijímat, uchovávat a odesílat WLD tokeny i další podporované kryptoměny. Pro uživatele v oprávněných zemích aplikace také slouží jako prostředek pro nárokování pravidelných grantů ve formě WLD tokenů. [1]



Obrázek 13 Ukázka rozhraní aplikace World App

(zdroj:[16])

World App implementuje moderní bezpečnostní architekturu založenou na tzv. smart kontraktech („chytré kontrakty“). Smart kontrakt je digitální program na blockchainu, který automaticky vykoná stanovené podmínky bez potřeby prostředníka. Konkrétně využívají Smart kontrakty SAFE (Smart Account For Everyone), které fungují jako digitální peněženka s rozšířenými bezpečnostními prvky a zjednodušeným uživatelským rozhraním. [16]

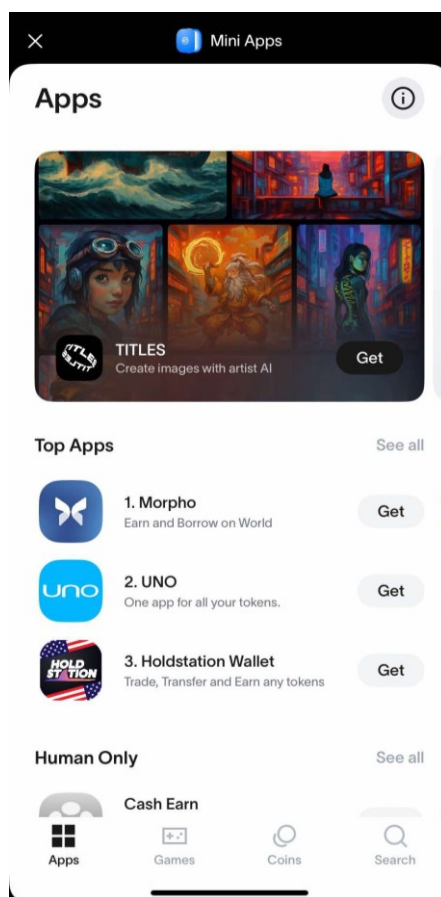
Platební funkce [16]:

- Peer-to-peer platby mezi uživateli
- Využití systému Ethereum Name Service (ENS):
 - Převod komplexních kryptografických adres na zapamatovatelná jména (podobně jako doménový systém na internetu)
 - Zjednodušení transakcí s ERC-20 tokeny v ekosystému Ethereum

Směnárenské funkce [16]:

- Integrace protokolu Uniswap
 - Decentralizovaná směnárenská platforma
 - Umožňuje výměnu kryptoměn přímo v aplikaci
 - Eliminuje potřebu externích služeb

Součástí aplikace je také přístup k Mini Aplikací, kolekci integrovaných aplikací třetích stran navržených pro rozšíření funkcionality ekosystému a zvýšení každodenní produktivity uživatelů (AI asistenti, platební aplikace, eSim a jiné) [38].



Obrázek 14 Ukázka Mini Apps v aplikaci World App

(zdroj: vlastní)

Zásadním prvkem World App je důraz na soukromí a bezpečnost uživatelů. Aplikace implementuje řadu pokročilých technologií a přístupů, které společně vytvářejí bezpečné prostředí respektující soukromí pro uživatele. [16]

Minimalizace sběru dat [16]:

- Nevyžaduje osobní informace (např. jméno, e-mailová adresa nebo telefonní číslo) pro základní funkce (např. vytvoření účtu, přístup do aplikace apod.)

Ochrana biometrických dat [16]:

- Implementace principu osobní úschovy dat (personal custody)
 - Informace pro generování kódu duhovky uchovány pouze na zařízení uživatele
 - Žádná biometrická data nejsou ukládána na Orbu
 - Uživatelé mají plnou kontrolu nad svými daty

Autentizační mechanismy [16]:

- Technologie **Face Auth**
 - Biometrická autentizace obličeje (porovnává záznam s původním)
 - Zajištění, že pouze původní verifikovaná osoba může používat své World ID

Výhody pro ověřené uživatele [16]

Ověření držitelé World ID získávají v aplikaci přístup k několika výhodám, které zvyšují uživatelský komfort:

- Transakce bez poplatků
- Bezpečnější převody ověřeným uživatelům
- Přístup k výukovým kurzům
- Prioritní nepřetržitá zákaznická podpora v několika světových jazycích

2.1.3 Rozdíly mezi regiony a zeměmi

Míra dostupnosti Worldcoinu se napříč jednotlivými regiony a zeměmi výrazně liší, a to v důsledku rozdílů v regulacích, logistice a strategickém zaměření.

Nejvýznamnější regionální omezení představovala dostupnost WLD tokenů v USA. Z důvodu regulační nejistoty se Worldcoin rozhodl nespouštět distribuci tokenů v USA, avšak od 30. dubna 2025 projekt Worldcoin (nyní známý jako World) oficiálně spustil distribuci WLD tokenů ve většině států USA. Uživatelé se mohou ověřit prostřednictvím zařízení Orb

a následně obdržet WLD tokeny. Výjimkou zůstává stát New York, kde distribuce WLD tokenů prostřednictvím aplikace World App nadále není dostupná kvůli regulačním omezením, nicméně obyvatelé se stále mohou ověřit pomocí orbu a získat tak World ID (viz kapitola 4.1.3). Podobně projekt není dostupný v Číně kvůli regulačním omezením, avšak zde není možné provést ani samotnou verifikaci. [1], [10], [38]

V současnosti jsou Orby dostupné ve více než 35 městech po celém světě, včetně významných center jako Hong Kong, Tokio, Singapur, Soul, Paříž, Lisabon, Mexico City, São Paulo, Nairobi, New York a San Francisco. Hongkong má odlišný právní systém než pevninská Čína, což umožňuje provoz Orbů navzdory omezením platným v Čínské lidové republice. [7]

2.2 Možnosti nákupu a směny

2.2.1 Kryptoměnové burzy

Online tržiště pro přímé obchodování kryptoměn mezi uživateli, kde burza slouží jako prostředník a zajišťuje bezpečnost transakcí.

Oficiální spuštění Worldcoinu 24. 7. 2023 přineslo token WLD na významné kryptoburzy, což zajistilo okamžitou likviditu a viditelnost projektu v kryptoměnovém ekosystému.

Aktuálně je Worldcoin dostupný na více než 100 různých burzách, přičemž dominují burzy Binance a Bithumb podle denního objemu obchodů s WLD tokeny. WLD je nově dostupný i na české kryptoměnové burze Coinmate, kde jej lze obchodovat přímo za CZK. [12]

Stručný postup nákupu:

1. Zaregistrujte se na vybrané burze
2. Ověřte svou identitu
3. Vložte peníze – fiat měnu (CZK, EUR, USD aj.) nebo kryptoměnu
4. Vyhledejte WLD v obchodní sekci
5. Zvolte vhodný obchodní pár a nakupte

Obchodování v párech znamená, že jedna měna (nebo kryptoměna) je vždy obchodována vůči jiné měně nebo kryptoměně. Tyto dvě měny společně tvoří "obchodní pár".

Nejběžnější páry pro WLD [12]:

- WLD/USDT: Kupujete WLD za stablecoin Tether (nejčastější)
 - Stablecoin je kryptoměna navázaná na stabilní aktivum (např. dolar, zlato, nebo jiná kryptoměna), která si udržuje stálou hodnotu a slouží pro minimalizování cenové volatility (výkyvy v čase)
- WLD/BTC: Kupujete WLD za Bitcoin
- WLD/ETH: Kupujete WLD za Ethereum
- WLD/KRW: Kupujete WLD za korejský won (populární na Bithumb)

Burzy jsou vhodné pro aktivnější obchodníky, investory s větším objemem prostředků a uživatele, kteří chtějí využívat pokročilé obchodní strategie a nástroje.

2.2.2 Kryptoměnové směnárny

Online služba, která umožňuje jednoduchou a rychlou výměnu mezi různými kryptoměnami nebo mezi kryptoměnami a fiat měnami. (např. Changelly, ShapeShift aj.) Na rozdíl od kryptoměnových burz, směnárny fungují jako přímí zprostředkovatelé směny. Tyto platformy jsou oblíbené zejména mezi začátečníky díky své jednoduchosti, rychlosti a absenci nutnosti zadávání obchodních příkazů. [39]

Mezi známé zahraniční směnárny podporující WLD patří například SimpleSwap, SwapSpace či CEX.IO, kde lze WLD snadno směnit například za USDT, BTC nebo EUR.

Na českých směnárnách (např. Simplecoin, Anycoin) zatím podpora Worldcoinu zavedena nebyla. [40]

Stručný postup směny:

1. Vyberete vstupní kryptoměnu (kterou posíláte)
2. Vyberete výstupní kryptoměnu (kterou chcete získat)
3. Zadáte množství nebo cílovou adresu peněženky
4. Směnárna zobrazí směnný kurz a poplatky
5. Odešlete své kryptoměny na adresu poskytnutou směnárnou
6. Směnárna vám odešle požadovanou kryptoměnu na vaši adresu

2.2.3 Přímo v aplikaci World App

Pro uživatele s WLD tokeny ve World App je proces směny relativně jednoduchý. Mohou buď převést své tokeny na externí burzu, nebo využít integrované směnářské funkce přímo v aplikaci World App, jak již bylo zmíněno v kapitole 2.1.2. [5], [7]

2.2.4 Cenový vývoj

Cenový vývoj WLD tokenu od jeho spuštění v červenci 2023 prošel několika změnami [8].

Nejvyšší hodnoty (all-time high) dosáhl WLD v březnu 2024, kdy jeho cena vystoupala až na 11,72 USD. Tento cenový vrchol mohl být způsoben kombinací rostoucího zájmu o projekty spojené s umělou inteligencí, rozšiřující se uživatelské základny a obecného růstu na kryptoměnových trzích v daném období. [12]

K začátku června 2025 se cena WLD pohybovala kolem 1 USD. [12]

Z pohledu návratnosti investic (ROI) vykázal WLD za poslední období následující výsledky. Za jeden měsíc došlo k nárůstu o 23,5 %. Za šest měsíců byl zaznamenán pokles o 66,93 %. Za jeden rok token ztratil hodnotu o 76,31 %. [8]

Z pohledu budoucích predikcí někteří analytici očekávají, že WLD by mohl v dlouhodobém horizontu dosáhnout minimální ceny 1,7 USD v roce 2027 a 3,62 USD v roce 2032, avšak tyto předpovědi jsou pouze spekulativní a skutečný cenový vývoj bude záviset na mnoha faktorech (např. regulatorní vývoj, míra adopce projektu, tempo verifikace nových uživatelů, celková situace kryptoměnového trhu a vývoj konkurenčních technologií). [8]

Všechna uvedená data jsou zpracována ke dni 4. června 2025.



Obrázek 15 Cenový vývoj tokenu WLD od spuštění až do 4. června 2025

(zdroj:[12])

2.3 Využití pro platby

V současné době jsou možnosti využití WLD tokenu pro přímé platby stále ve vývoji, přičemž primární funkcí tokenu je správa a zapojení se v ekosystému Worldcoin spíše než každodenní platební nástroj. Ačkoliv přímá akceptace WLD u obchodníků není ještě široce rozšířena, některé platformy a služby již umožňují platby v WLD. Aplikace Emporium, dostupná v rámci World App, umožňuje uživatelům užívat WLD tokeny u známých obchodníků, jako jsou Apple, Amazon a Starbucks. V aplikaci také naleznete mini aplikaci Cash App, která dovoluje obchodníkům vytvářet QR kódy pro příjem kryptoměnových plateb, včetně WLD. [1], [16]

II PRAKTICKÁ ČÁST

3 SROVNÁVACÍ STUDIE WORLDCOINU OPROTI OSTATNÍM KRYPTOMĚNÁM

3.1 3.1 Metodologie srovnávací studie

3.1.1 Kritéria hodnocení kryptoměn

Pro účely identifikace specifických výhod a nevýhod Worldcoinu v porovnání s nejpoužívanějšími kryptoměnami budou stanovena následující hodnotící kritéria, která strukturuji celou srovnávací analýzu:

- **Technologické aspekty** – hodnotí technickou implementaci kryptoměn, včetně konsenzuálních mechanismů, škálovatelnosti sítě a bezpečnostních prvků. Posuzuje efektivitu infrastruktury a odolnost vůči různým typům útoků, což je zásadní pro dlouhodobou udržitelnost a funkčnost projektu.
- **Ekonomické aspekty** – analyzují tokenomiku (jak token funguje v rámci ekonomického systému projektu), distribuční mechanismy a monetární politiku projektů. Zahrnuje hodnocení celkové nabídky tokenů, inflační či deflační charakter měny a volatilitu, která přímo ovlivňuje využitelnost jako uchovatele hodnoty a platebního prostředku.
- **Uživatelské aspekty** – hodnotí přístupnost, použitelnost a celkovou míru adopce kryptoměn. Toto kritérium zahrnuje faktory jako vstupní bariéry, transakční rychlost, uživatelská přívětivost a rozsah ekosystému, které jsou klíčové pro praktické využití a rozšíření projektu.
- **Právní a regulační aspekty** – posuzuje regulační status, právní výzvy, geografická omezení a compliance postupy (dodržování nebo soulad s pravidly, předpisy, zákony, normami apod.) jednotlivých kryptoměn. Toto kritérium je zvláště relevantní pro Worldcoin vzhledem k jeho využití biometrických dat.

Jedním ze stěžejních aspektů hodnocení kryptoměn je jejich schopnost fungovat bez důvěry v centrální autoritu. Hlavním problémem, který Bitcoin a další kryptoměny řeší, je právě otázka důvěry. U Worldcoinu je tato otázka obzvláště zajímavá vzhledem k jeho modelu kombinujícímu decentralizovanou kryptoměnu s centralizovaným prvkem biometrické verifikace. [11]

3.1.2 Výběr kryptoměn pro srovnání s Worldcoinem

Cílem této analýzy je porozumět tomu, v čem se Worldcoin liší od již zavedených blockchainových platforem.

Za tímto účelem byly vybrány kryptoměny, které reprezentují různé technologické přístupy a využívají odlišné způsoby zabezpečení, zpracování transakcí i zapojení uživatelů. Díky této různorodosti můžeme lépe posoudit, jaké má Worldcoin postavení v kryptoměnovém prostředí. V závorce za názvem každé kryptoměny je uvedena zkratka jejího tokenu:

1. **Bitcoin (BTC)** - první a nejrozšířenější kryptoměna založená na technologii blockchain, která slouží primárně jako digitální zlato a uchovatel hodnoty. Bitcoin představuje standard, vůči kterému lze hodnotit inovativnost Worldcoinu. [14]
2. **Ethereum (ETH)** - platforma pro vytváření dApps s vlastním nativním tokenem, která přechodem na PoS mechanismus zlepšila svou udržitelnost. Protože Worldcoin funguje jako ERC-20 token na Ethereum blockchainu, je jejich hodnocení vzájemně provázané – výkon a možnosti Worldcoinu jsou přímo závislé na Ethereum infrastruktuře. [15], [1]
3. **Worldcoin (WLD)** - projekt kombinující kryptoměnu s biometrickou verifikací identity, zaměřený na globální finanční inkluzi a řešení problému Sybil útoků. Worldcoin představuje hlavní předmět této studie. [1]
4. **Solana (SOL)** - vysokorychlostní blockchain s inovativním konsenzuálním mechanismem Proof-of-History (PoH) - umožňuje ověřit pořadí a čas událostí v blockchainu („důkaz historie“), je zaměřený na maximální propustnost a nízké transakční poplatky. Solana je důležitým referenčním bodem pro hodnocení výkonnostních parametrů Worldcoinu. [21]
5. **Cardano (ADA)** - blockchain platforma s vědeckým přístupem k vývoji, využívající formálně verifikované protokoly a mechanismus PoS Ouroboros. Cardano nabízí zajímavé srovnání z hlediska akademického a přísnému přístupu k vývoji. [22]
6. **Polygon (MATIC)** - škálovací řešení pro Ethereum, které využívá technologii Layer 2 (podobně jako Worldcoin, viz. Obrázek 2) k výraznému zvýšení

propustnosti transakcí a snížení poplatků. Polygon umožňuje rychlé a levné transakce na blockchainu Ethereum, čímž zlepšuje škálovatelnost a přístupnost dApps a DeFi (Decentralized Finance) projektů (poskytování finančních služeb bez potřeby tradičních zprostředkovatelů, např. banky). [26]

3.2 Srovnání Worldcoinu s nepoužívanějšími kryptoměnami

3.2.1 Technologické aspekty (konsenzuální mechanismy, škálovatelnost, bezpečnost)

Konsenzuální mechanismy

Konsenzuální mechanismy představují základ každé kryptoměny, určující způsob, jakým se účastníci sítě shodnou na platnosti transakcí.

Bitcoin využívá původní PoW mechanismus, který vyžaduje řešení složitých matematických problémů k ověření bloku transakcí. Tento přístup zajišťuje vysokou bezpečnost, ale za cenu vysoké energetické náročnosti a omezené škálovatelnosti. Bitcoinový konsenzuální mechanismus se za více než dekádu prokázal jako mimořádně odolný vůči útokům, což potvrzuje jeho robustnost [19]. PoW systém (těžba) je v Bitcoinu implementován jako způsob realizace distribuovaného časového serveru, který umožňuje nezávislé potvrzování pořadí transakcí. [11], [14]

Ethereum původně také využívalo PoW, ale v roce 2022 úspěšně přešlo na PoS mechanismus v rámci aktualizace známé jako "The Merge". Tento přechod výrazně snížil energetickou náročnost sítě (podle oficiálních údajů o více než 99,9 %) a položil základy pro budoucí vylepšení škálovatelnosti. PoS mechanismus Etherea vyžaduje od validátorů (účastníci blockchainové sítě, kteří ověřují a potvrzují transakce, aby mohly být přidány do blockchainu) složení zálohy (stake) minimálně 32 ETH, což zajišťuje ekonomickou motivaci k poctivému ověřování transakcí. [15], [18]

Worldcoin využívá modifikovaný PoS mechanismus, který je detailně popsán v kapitole 1.3.2. Tato architektura umožňuje Worldcoinu těžit z bezpečnostních vlastností Ethereum blockchainu a zároveň dosahovat vyšší propustnosti a nižších transakčních poplatků. Kombinace s biometrickou verifikací přidává další vrstvu zabezpečení celého ekosystému. [16], [13]

Solana implementuje unikátní kombinaci PoS a PoH mechanismů. PoH funguje jako "kryptografické hodiny", které vytvářejí časové razítko pro každou transakci, což umožňuje

paralelní zpracování a výrazně zvyšuje propustnost sítě. Tento přístup umožňuje Solaně dosahovat teoretické propustnosti až 65 000 transakcí za sekundu, což je řádově více než u tradičních blockchainů. Kombinace těchto mechanismů však přináší vyšší nároky na hardware validátorů, což může vést k určité míře centralizace. [21][27][28]

Cardano využívá vlastní PoS protokol Ouroboros, který je prvním vědecky recenzovaným a matematicky ověřeným konsensuálním algoritmem. Systém Ouroboros funguje jako digitální hodinky, které rozdělují čas na větší úseky (epochy) a menší úseky (sloty), a v každém malém časovém úseku je náhodně vybrán jeden účastník, který je odpovědný za přidání bloku do blockchainu (slot leader). Tento přístup zajišťuje energetickou efektivitu při zachování vysoké úrovně bezpečnosti a decentralizace. Cardano klade důraz na formální verifikaci svých protokolů, což minimalizuje riziko chyb v kódu, ale může zpomalovat implementaci nových funkcí. [22], [32]

Polygon jako Layer 2 řešení pro Ethereum využívá kombinaci vlastního PoS konsensuálního mechanismu s kontrolními body zaznamenanými na hlavním Ethereum blockchainu. Tento hybridní přístup umožňuje Polygonu těžit z bezpečnostních záruk Etherea a zároveň dosahovat výrazně vyšší propustnosti a nižších poplatků. Validátoři Polygonu musí stakovat (uzamknout/zálohovat) MATIC tokeny jako záruku poctivého chování, což vytváří ekonomické podněty pro zajištění bezpečnosti sítě. [26]

Škálovatelnost

Škálovatelnost je schopnost blockchainu zvládat víc transakcí a uživatelů bez snižování výkonu nebo zvýšení nákladů. Jde tedy o zásadní předpoklad pro praktické využití kryptoměn v masovém měřítku.

Bitcoin má v základní vrstvě (Layer 1) omezenou propustnost přibližně 7 transakcí za sekundu (TPS), což vyplývá z velikosti bloku 1 MB a průměrného času vytvoření bloku 10 minut. Pro zlepšení škálovatelnosti byla vyvinuta řešení druhé vrstvy jako Lightning Network, umožňující téměř okamžité mikrotransakce mimo hlavní blockchain. Lightning Network je stále v rané fázi vývoje, ale s rostoucím počtem uzlů a kanálů se stává stále významnějším prvkem Bitcoinového ekosystému. [11], [14], [27]

Ethereum ve své základní vrstvě momentálně dosahuje propustnosti přibližně 15-30 TPS, což představuje zlepšení oproti Bitcoinu, ale stále omezení pro globální adopci. Ethereum řeší vyšší škálovatelnost (stovky až tisíce TPS) prostřednictvím "rollupů" druhé vrstvy (Optimistic a ZK-rollupy). Dalším plánovaným krokem ke zvýšení škálovatelnosti je

sharding (rozdělení sítě na menší části), který má být zaveden v budoucích aktualizacích. [15], [27]

Worldcoin, díky implementaci na Optimism Layer 2, může dosahovat výrazně vyšší propustnosti než základní vrstva Etherea a s rozvojem a optimalizacemi může rychlost dorovnat nebo překonat některé L2 vrstvy. Tento přístup umožňuje efektivní zpracování velkého množství transakcí při zachování nižších poplatků, což je velmi důležité pro zamýšlené globální využití. [1]

Solana je známá svou extrémně vysokou propustností dosahující teoreticky až 65 000 TPS díky kombinaci PoS a PoH mechanismů a paralelnímu zpracování transakcí pomocí technologie Gulf Stream (optimalizace zpracovávání transakcí a zvyšování propustnosti sítě). Tato vysoká propustnost je dosažena částečně díky vyšším hardwarovým nárokům na validátory, což může představovat kompromis mezi výkonem a decentralizací. V praxi Solana běžně zpracovává 2 000-3 000 TPS, což je stále výrazně více než tradiční blockchainya. [21], [27]

Cardano implementuje škálovatelnost postupně v rámci svého plánovaného vývoje. V současné implementaci dosahuje propustnosti kolem 20 TPS. Pro další zlepšení škálovatelnosti Cardano vyvíjí Layer 2 řešení nazývané Hydra, které by mělo umožnit zpracování tisíců transakcí za sekundu rozložením zátěže do několika paralelních kanálů. Cardano také plánuje implementaci shardingu v rámci své vývojové mapy. [22], [32]

Polygon jako Layer 2 řešení pro Ethereum dosahuje maximální propustnosti až 7 000 TPS. Toto výrazné zlepšení oproti základní vrstvě Etherea je dosaženo díky samostatnému blockchainu s vlastním konsensuálním mechanismem, který periodicky ukládá souhrnné informace na Ethereum blockchain [31]. Polygon nabízí také různé typy škálovacích řešení, včetně Polygon zkEVM, což je ZK-rollup technologie, která dále zvyšuje propustnost a snižuje náklady. [26], [29]

Bezpečnost

Bitcoin je považován za nejbezpečnější blockchain z hlediska odolnosti vůči útokům, což je dáno enormním množstvím výpočetního výkonu v síti a dlouhou historií bez úspěšných útoků na základní protokol. Bezpečnostní model je založen na ekonomické motivaci těžařů a decentralizaci sítě. Síla Bitcoinu spočívá v číslech – „Vires in Numeris“ – což se projevuje v prakticky neprolomitelné kryptografické ochraně a matematických principech, na kterých je postaven. [11], [14]

Ethereum po přechodu na PoS zajišťuje bezpečnost prostřednictvím ekonomických stimulů pro validátory, kdy špatné chování může vést ke "slashingu" (ztrátě části nebo celé zástavy). Bezpečnostní model Etherea je komplexnější než u Bitcoinu, ale s rostoucím počtem validátorů se stává robustnějším. [15], [18]

Worldcoin těží z bezpečnostních vlastností Ethereum blockchainu, na kterém staví, a přidává dodatečnou vrstvu bezpečnosti prostřednictvím biometrické verifikace uživatelů pomocí skenování duhovky zařízením Orb. Tento unikátní přístup řeší problém Sybil útoku, což je problém, se kterým se potýkají ostatní kryptoměny. [1]

Solana využívá ekonomické stimuly pro zajištění bezpečnosti sítě, podobně jako další PoS blockchainy. Validátoři musí stakovat SOL tokeny jako záruku poctivého chování. Specifickým bezpečnostním rizikem Solany je vyšší technická náročnost validace, která může vést k určité centralizaci validátorů, což potenciálně snižuje bezpečnost sítě. Solana v minulosti čelila několika výpadkům sítě z důvodu technických problémů, což vyvolalo otázky ohledně stability a zralosti implementace. [21]

Cardano klade mimořádný důraz na bezpečnost prostřednictvím formálně verifikovaného vývoje a matematicky ověřených protokolů. Bezpečnostní model Cardana je založen na protokolu Ouroboros, který poskytuje podobnou úroveň bezpečnosti jako PoW, ale s výrazně nižší energetickou náročností. Cardano také implementuje více vrstev protokolů (Settlement Layer a Computation Layer), což zvyšuje bezpečnost oddělením základních funkcí blockchainu. [22]

Polygon jako Layer 2 řešení kombinuje vlastní bezpečnostní mechanismy s bezpečnostními zárukami poskytovanými Ethereum blockchainem. Bezpečnost sítě je zajištěna validátory stakujícími MATIC tokeny a kontrolními body, které jsou pravidelně zaznamenávány na Ethereum. Tento přístup představuje kompromis mezi absolutní bezpečností a škálovatelností, kdy Polygon obětuje určitou míru bezpečnostních záruk ve prospěch vyšší propustnosti a nižších poplatků. [26], [29]

Tabulka 1 Srovnávací tabulka technologických aspektů kryptoměn

Kryptoměna	Konsenzuální mechanismus	Škálovatelnost (TPS)	Bezpečnost
Bitcoin	Proof-of-Work (PoW)	~7 (Layer 1), vyšší s Lightning Network	Velmi vysoká, dlouhodobě ověřená, decentralizovaná
Ethereum	Proof-of-Stake (PoS)	~15 (Layer 1), > 2000 (Layer 2, záleží na typu)	Vysoká – motivace validátorů pomocí odměn a sankcí (slashing)
Worldcoin	Modifikovaný PoS na Optimism (Layer 2)	~10 (reálně – L2 World Chain) s rozvojem i vyšší	Bezpečnost Etherea + biometrická verifikace (Orb)
Solana	Proof-of-History (PoH) + PoS	~1,000 (L1 reálně), ~65,000 (L1 teoreticky)	Vysoká, ale náchylnost k výpadkům, riziko centralizace
Cardano	Ouroboros (PoS)	~1 (L1 reálně) ~20 (L1 teoreticky), >1,000 (L2 Hydra)	Velmi vysoká, formální verifikace protokolů
Polygon	PoS	~50 (L2 reálně), ~700 (L2 teoreticky)	Bezpečnost Etherea + vlastní síť validátorů

(zdroj: Zpracováno na základě údajů z [1], [5], [11], [13]-[16], [18]-[22], [26], [27], [29], [32], [41])

Hodnotící škála – Tabulka 1:

Bezpečnost:

- **Velmi vysoká:** Systém má dlouhodobě prokázanou odolnost proti útokům, robustní zabezpečení a minimální zranitelnost
- **Vysoká:** Systém nabízí spolehlivou ochranu, ale s o něco nižší mírou zabezpečení

3.2.2 Ekonomické aspekty (tokenomika, distribuce, volatilita)

Tokenomika a distribuce

Bitcoin má limitovanou nabídku 21 milionů mincí. Díky pevně dané nabídce se Bitcoin stává tvrdou měnou odolnou vůči inflaci. Distribuce probíhá prostřednictvím těžby, kdy jsou nové mince vydávány jako odměna za validaci transakcí. Přibližně každé čtyři roky dochází k "halvingu", kdy se odměna za vytěžený blok snižuje na polovinu. K začátku června 2025 bylo v oběhu přibližně 19,9 milionu BTC. Tento model zajišťuje transparentní a předvídatelnou monetární politiku nezávislou na centrálních autoritách. [11], [17], [14]

Ethereum nemá pevně stanovený maximální limit nabídky, ale po implementaci EIP-1559 (aktualizace protokolu Ethereum) a přechodu na PoS se část poplatků za transakce spaluje, což vytváří deflační tlak při vysokém využití sítě. Distribuce ETH proběhla prvotně prostřednictvím veřejného prodeje v roce 2014, následně pokračovala těžbou a nyní probíhá formou odměn pro validátory. Tento ekonomický model kombinuje prvky inflačního a deflačního systému. [15], [18]

Worldcoin má maximální nabídku 10 miliard tokenů WLD, rozdělených na 75 % pro uživatelskou komunitu a 25 % pro investory a zřizovatele (včetně TFH). Unikátní je distribuce části tokenů prostřednictvím verifikace jedinečnosti člověka pomocí skenování duhovky zařízením Orb. Tento přístup se zásadně liší od tradičních distribučních mechanismů. [1]

Solana nemá stanovený maximální limit nabídky, ale implementuje inflační model začínající na 8 % s postupným snížením na 1,5 %. Významná část tokenů (cca 60 %) byla vyhrazena vývojářskému týmu, investorům a nadaci Solana Foundation a zbylých 40 % pro komunitu. Solana implementuje mechanismus stake poolů (umožňuje více uživatelům spojit své prostředky a účastnit se stakování) pro participaci menších držitelů. [21], [42], [43]

Cardano má maximální nabídku 45 miliard ADA tokenů. Implementuje "treasury model", kdy část nových tokenů je alokována do fondu (treasury), o jehož využití hlasuje komunita. Přibližně 57,6 % všech ADA bylo při spuštění distribuováno mezi investory. [22]

Polygon má maximální nabídku 10 miliard MATIC tokenů. Největší podíl (23,33 %) byl určen na rozvoj ekosystému. Významná část (21,86 %) připadla nadaci Polygon, která podporuje dlouhodobý vývoj projektu. Pro veřejnost bylo vyčleněno 19 % celkové nabídky. Vývojářský tým získal 16 % tokenů jako motivaci pro další rozvoj platformy.

Na síťové operace bylo určeno 12 % tokenů, zatímco poradci obdrželi 4 %. Pro první investory a podporovatele, bylo vyhrazeno celkem 3,80 % tokenů. [26], [29]

Volatilita

Volatilita je míra cenových výkyvů aktiva v čase. U kryptoměn představuje rychlé a často dramatické změny hodnoty, což ztěžuje jejich využití jako platidla, ale zvyšuje jejich přitažlivost pro investory hledající vysoké zisky.

Bitcoin historicky vykazuje vysokou volatilitu, která se s rostoucí tržní kapitalizací postupně snižuje. Během svého vývoje zažil několik významných cenových cyklů s nárůsty a propady o stovky procent v rámci jednotlivých let. Tato volatilita je částečně způsobena pevně danou nabídkou a kolísající poptávkou, ale také charakterem investic a relativní nezralostí trhu ve srovnání s tradičními finančními aktivy. [17]

Ethereum vykazuje podobnou míru volatility jako Bitcoin, což odráží obecný trend na kryptoměnovém trhu. Jeho cenové pohyby jsou ovlivněny nejen spekulativními investicemi, ale i reálným využitím v DeFi aplikacích a NFT (Non-Fungible Token – unikátní digitální token, který dokazuje vlastnictví digitálního aktiva, např. obrázku nebo videa). ekosystému. Přejít na PoS mechanismus a implementace EIP-1559 vytvořily nové ekonomické procesy, které mohou dlouhodobě ovlivnit volatilitu ETH. [17], [18], [24]

Worldcoin, jako novější projekt, zatím vykazuje velmi vysokou volatilitu, což je charakteristické pro méně zavedené kryptoměny s nižší tržní kapitalizací. Cenové pohyby WLD jsou ovlivněny faktory jako tempo verifikace nových uživatelů, regulatorní vývoj a celkové přijetí konceptu. Unikátní distribuce spojená s biometrickou verifikací může potenciálně vést k rovnoměrnější distribuci tokenů. [1], [17]

Solana vykazuje vysokou volatilitu i ve srovnání s ostatními velkými kryptoměnami. Tato volatilita je způsobena rychlým růstem projektu a výkyvy v důvěře investorů v návaznosti na technické výpadky sítě v minulosti. Vysoká koncentrace tokenů v rukou prvních investorů může přispívat k větším cenovým výkyvům. [17], [21]

Cardano vykazuje střední až vysokou volatilitu, typickou pro altcoiny (alternativní kryptoměny jiné než Bitcoin). Jeho cenové pohyby jsou silně ovlivněny oznámeními o vývoji a implementaci nových funkcí. Postupný a opatrný způsob vývoje může vést k odlišné volatilitě než u ostatních projektů. [17], [22]

Polygon jako Layer 2 řešení pro Ethereum je částečně ovlivněn cenovými pohyby ETH, ale zároveň vykazuje i vlastní volatilitu v závislosti na adopci a využití sítě. Volatilita MATIC je typicky vyšší než u ETH vzhledem k nižší tržní kapitalizaci, ale má tendenci odrážet obecné trendy na trhu Layer 2 řešení. Rostoucí adopce Polygonu jako hlavního škálovacího řešení pro Ethereum by mohla vést k postupnému snižování volatility. [17], [29]

Tabulka 2 Srovnávací tabulka ekonomických aspektů kryptoměn

Kryptoměna	Max. nabídka	Distribuce a alokace	Monetární model	Volatilita (roční)	Tržní kapitalizace*
Bitcoin	21 milionů	100 % prostřednictvím těžby; 19,9 mil. BTC v oběhu	Dlouhodobě deflační, halving každé 4 roky	~50 %	~\$2 biliony
Ethereum	Neomezena (~120 mil. aktuálně)	Dříve těžba, nyní staking	Variabilní, potenciálně deflační	~70 %	~\$300 miliard
Worldcoin	10 miliard	75 % pro uživatele (Orb), 25 % pro zakladatele a investory	Kontrolovaná inflace	~120 %	~\$1,8 miliard
Solana	Neomezena (~600 mil. aktuálně)	PoS odměny, ekosystémové granty	Inflační (klesající míra)	~90 %	~\$80 miliard
Cardano	45 miliard	57,6 % veřejný prodej, zbytek vývoj, tým a nadace	Klesající kontrolovaná inflace	~100 %	~\$25 miliard
Polygon	10 miliard	Iniciální distribuce, staking	Kontrolovaná inflace	~80 %	~\$330 milionů

*Údaje o tržní kapitalizaci jsou přibližné a vztahují se k 4. 6. 2025

(zdroj: Zpracováno na základě údajů z [1], [11]-[18], [21], [22], [29], [42], [43])

3.2.3 Uživatelské aspekty (přístupnost, použitelnost, adopce)

Přístupnost a použitelnost

Přístupnost a použitelnost definují, jak snadno mohou běžní uživatelé kryptoměnu používat bez technických znalostí. Zahrnují intuitivní peněženky, srozumitelné rozhraní a jednoduché procesy transakcí.

Bitcoin má rozsáhlou infrastrukturu včetně množství peněženek, burz a služeb, což usnadňuje přístup pro nové uživatele. Zároveň však relativně pomalé transakce a potenciálně vysoké poplatky na základní vrstvě mohou omezovat jeho použitelnost pro každodenní transakce. Lightning Network řeší tyto problémy, ale přidává další vrstvu komplexity. Bitcoin těží z pozice nejstaršího a nejznámějšího kryptoměnového projektu, což zvyšuje povědomí a důvěru u veřejnosti. [11], [14], [20]

Ethereum nabízí široké možnosti využití díky smart kontraktům a dApps. Uživatelská zkušenost se průběžně zlepšuje, ale složitost ekosystému a technické bariéry stále představují komplikaci pro masovou adopci. Vysoké transakční poplatky během období vysokého vytížení sítě byly historicky problémem, který částečně řeší řešení druhé vrstvy. Ethereum vytvořilo rozsáhlý ekosystém zahrnující DeFi, NFT a další aplikace. [15], [18], [24]

Worldcoin se odlišuje zaměřením na přístupnost pro globální populaci, včetně lidí bez přístupu k tradičním bankovním službám. Proces verifikace identity pomocí Orbu vytváří vstupní bariéru, která je kompenzována potenciálními výhodami ověřené identity. Díky fungování na Ethereum infrastruktuře umožňuje Worldcoin uživatelům využívat dApps a další blockchainové služby. Worldcoin nabízí vlastní peněženku World App, která integruje funkce World ID s finančními službami. Tento integrovaný přístup může zjednodušit uživatelskou zkušenost, ale závislost na fyzické verifikaci prostřednictvím Orbu limituje globální dostupnost. [1]

Solana klade důraz na uživatelskou přívětivost a nízké poplatky, což ji činí atraktivní pro běžné uživatele. Díky vysoké propustnosti poskytuje téměř okamžité dokončení transakcí. Solana má rostoucí ekosystém DeFi aplikací a NFT tržišť. Nevýhodou je vyšší technická složitost při provozování validátoru, což může omezovat decentralizaci. [17], [21]

Cardano se zaměřuje na uživatelskou přívětivost prostřednictvím pečlivě navržených peněženek. Důraz na bezpečnost zvyšuje důvěru uživatelů, ale postupný a opatrný přístup k vývoji znamená, že některé funkce byly dostupné později než u konkurence. Cardano má

aktivní komunitu a silné zastoupení ve vzdělávacím sektoru. Projekt spolupracuje s vládami a institucemi v rozvojových regionech, zejména v Africe. [22]

Polygon vyniká kombinací nízkých poplatků, rychlých transakcí a kompatibility s Ethereum ekosystémem. Je atraktivní jak pro koncové uživatele, tak pro vývojáře dApps. Polygon je kompatibilní s většinou populárních Ethereum peněženek, což usnadňuje začlenění nových uživatelů do systému. Ekosystém zahrnuje aplikace od DeFi přes herní projekty až po NFT, což poskytuje uživatelům mnoho možností využití. [26], [29]

Tabulka 3 Srovnávací tabulka uživatelských aspektů kryptoměn

Kryptoměna	Vstupní bariéra	Transakční rychlost	Uživatelská přívětivost	Ekosystém	Globální dostupnost
Bitcoin	Střední (technická znalost)	10+ minut (L1), sekundy (LN)	Zlepšující se	Rozsáhlý, etablovaný	Vysoká
Ethereum	Střední až vysoká	~15 sekund (L1), sekundy (L2)	Komplexní	Nejrozsáhlejší, DeFi, NFT	Vysoká
Worldcoin	Vysoká (vyžaduje Orb)	Sekundy	Dobrá	Rozvíjející se	Omezená (dostupnost Orbů)
Solana	Střední	<1 sekunda	Průměrná	Rostoucí, DeFi, NFT	Vysoká
Cardano	Nízká	~20 sekund	Průměrná	Akademický přístup	Vysoká
Polygon	Nízká	Sekundy	Dobrá	Integrovaný s Ethereum	Vysoká

(zdroj: Zpracováno na základě údajů z [1], [11]-[18], [20]-[22], [26], [29])

Hodnotící škála – Tabulka 3

Vstupní bariéra:

- **Nízká:** Minimální technické požadavky, intuitivní přístup vhodný pro začátečníky
- **Střední:** Vyžaduje základní technické porozumění a orientaci v kryptoměnovém
- **Střední až vysoká:** Komplexnější vstupní proces vyžadující hlubší technické znalosti
- **Vysoká:** Značné technické nebo procedurální překážky limitující snadný přístup

Uživatelská přívětivost:

- **Zlepšující se:** Probíhá aktivní vývoj ke zjednodušení uživatelského rozhraní a procesů
- **Komplexní:** Vyšší složitost vyžadující pokročilejší znalosti a orientaci v ekosystému
- **Průměrná:** Standardní úroveň přívětivosti srovnatelná s běžnými digitálními službami
- **Dobrá:** Nadprůměrně intuitivní rozhraní a procesy

Globální dostupnost

- **Vysoká:** Široce dostupné bez významných geografických nebo technických omezení
- **Omezená:** Dostupnost limitovaná specifickými faktory

Adopce

Adopce kryptoměn označuje míru, jakou jednotlivci, firmy a instituce přijímají a využívají kryptoměny a blockchain technologie ve svých aktivitách, platbách a procesech.

Bitcoin dosáhl nejvyšší míry adopce mezi všemi kryptoměnami. Je akceptován tisíci obchodníky, některé země (El Salvador) jej přijaly jako zákonné platidlo a velké instituce jej zahrnují do svých portfolií. Bitcoin se etabloval jako "digitální zlato" a uchovatel hodnoty, což podpořilo jeho adopci proti inflaci. Lightning Network zvyšuje jeho použitelnost pro každodenní transakce. Adopce Bitcoinu má podobné exponenciální křivky jako jiné síťové technologie v minulosti (např. internet, e-mail apod.). [11], [20], [31]

Ethereum dominuje v oblasti DeFi a NFT, s miliardovými hodnotami v ekosystému. Jeho adopce je silná v technologickém sektoru a mezi vývojáři. Přechod na PoS a plánovaná vylepšení škálovatelnosti mají potenciál dále zvýšit adopci. [18], [24]

Worldcoin je relativně nový projekt s omezenější adopcí. K začátku června 2025 bylo verifikováno přes 12 milionů uživatelů. Potenciál je značný díky zaměření na globální dostupnost a digitální identitu, ale je omezen fyzickou infrastrukturou [16]. World ID si získává popularitu jako ochrana proti botům. [1], [16]

Solana zaznamenala významný nárůst adopce v letech 2021-2025 v oblasti DeFi a NFT. Její nízké poplatky přilákaly vývojáře hledající alternativy k Ethereum. Prosazuje se i v platbách, ale občasné výpadky sítě vyvolávají otázky spolehlivosti. [21], [24]

Cardano buduje adopci prostřednictvím partnerství s vládami a institucemi v rozvojových regionech. Jeho vědecký přístup přitahuje segment trhu oceňující bezpečnost. [22]

Polygon dosáhl významné adopce jako hlavní Layer 2 řešení pro Ethereum. Mnoho dApps bylo přesunuto na Polygon, což přivedlo velké množství uživatelů. Je využíván v oblasti Web3 her a NFT. [29], [30]

3.2.4 Právní a regulační aspekty

Regulatorní prostředí významně ovlivňuje fungování a potenciál kryptoměn v různých jurisdikcích.

Bitcoin má stabilní regulatorní postavení ve většině vyspělých zemí jako digitální komodita nebo aktivum. Jeho decentralizace snižuje riziko zásadních regulatorních zásahů. Regulace se týká primárně regulačních požadavků KYC/AML (Poznej svého zákazníka/Opatření proti praní špinavých peněz) na burzy, nikoliv základního protokolu. [14], [25]

Ethereum čelí složitějším otázkám vzhledem k širšímu využití včetně smart kontraktů a DeFi aplikací. Některé aktivity mohou být považovány za finanční služby vyžadující licencování. Přejít na PoS vyvolal otázky o klasifikaci jako cenný papír. Ethereum Foundation spolupracuje s regulátory na vytvoření jasného právního rámce. [18], [45]

Worldcoin čelí specifickým regulatorním výzvám souvisejícím se sběrem biometrických dat. Projekt již byl předmětem regulatorního zkoumání v některých zemích, především kvůli obavám o ochranu soukromí a soulad se zákony o ochraně osobních údajů jako GDPR. Biometrická verifikace vzbuzuje právní otázky týkající se vlastnictví dat, informovaného souhlasu a možností odstranění či změny již uložených biometrických údajů. Regulatorní nejistota představuje významnou překážku pro globální rozšíření projektu, zejména ve vyspělých ekonomikách s přísnými zákony na ochranu dat. [23]

Solana řeší podobné výzvy jako Ethereum v oblasti tokenů a DeFi aplikací. PoS mechanismus může vyvolávat otázky klasifikace jako investičního produktu. Kvůli kratší historii může čelit vyšší nejistotě než Bitcoin či Ethereum. Nadace Solana pracuje na dodržování předpisů a vytváření pravidel pro vývojáře. [21]

Cardano má proaktivní přístup k regulacím. Spolupracuje s regulátory a vládami na vhodném regulatorním rámci. Implementuje funkce usnadňující compliance, například doplňující údaje pro transakce. Tento přístup může poskytnout konkurenční výhodu. [22]

Polygon jako Layer 2 řešení sdílí výzvy Etherea, ale řeší i specifické otázky jako infrastrukturní poskytovatel. Jeho postavení jako škálovacího řešení může zjednodušit regulatorní situaci. Aktivně spolupracuje na vytváření standardů pro Layer 2 řešení a implementuje funkce pro KYC/AML v zkEVM. [26]

Tabulka 4 Srovnávací tabulka právních a regulačních aspektů kryptoměn

Kryptoměna	Regulatorní klasifikace	Právní výzvy	Geografická omezení	Přístup k regulacím
Bitcoin	Digitální komodita/aktivum	Nízké (etablovaný status)	Minimální (zakázáno v ~10 zemích)	Nepotřebuje zásadní změny, decentralizace brání zásahům
Ethereum	Digitální aktivum, některé tokeny jako cenné papíry	Střední (DeFi, staking)	Minimální	Aktivní spolupráce s regulátory, snaha o právní rámec
Worldcoin	Nejednotná, vyvíjející se	Vysoké (biometrická data)	Významná (pozastaveno v několika zemích)	Zatím regulatorní nejistota, potenciální překážka pro globální přijetí
Solana	Podobně jako Ethereum	Střední	Minimální	Nadace pracuje na compliance a pravidlech pro vývojáře
Cardano	Digitální aktivum	Nízké až střední	Minimální	Proaktivní spolupráce s vládami a regulátory
Polygon	Infrastrukturní řešení	Nízké	Minimální	Implementuje standardy a spolupracuje s regulátory

(zdroj: Zpracováno na základě údajů z [1], [4], [11], [14], [16], [18], [20]-[26], [29]-[31])

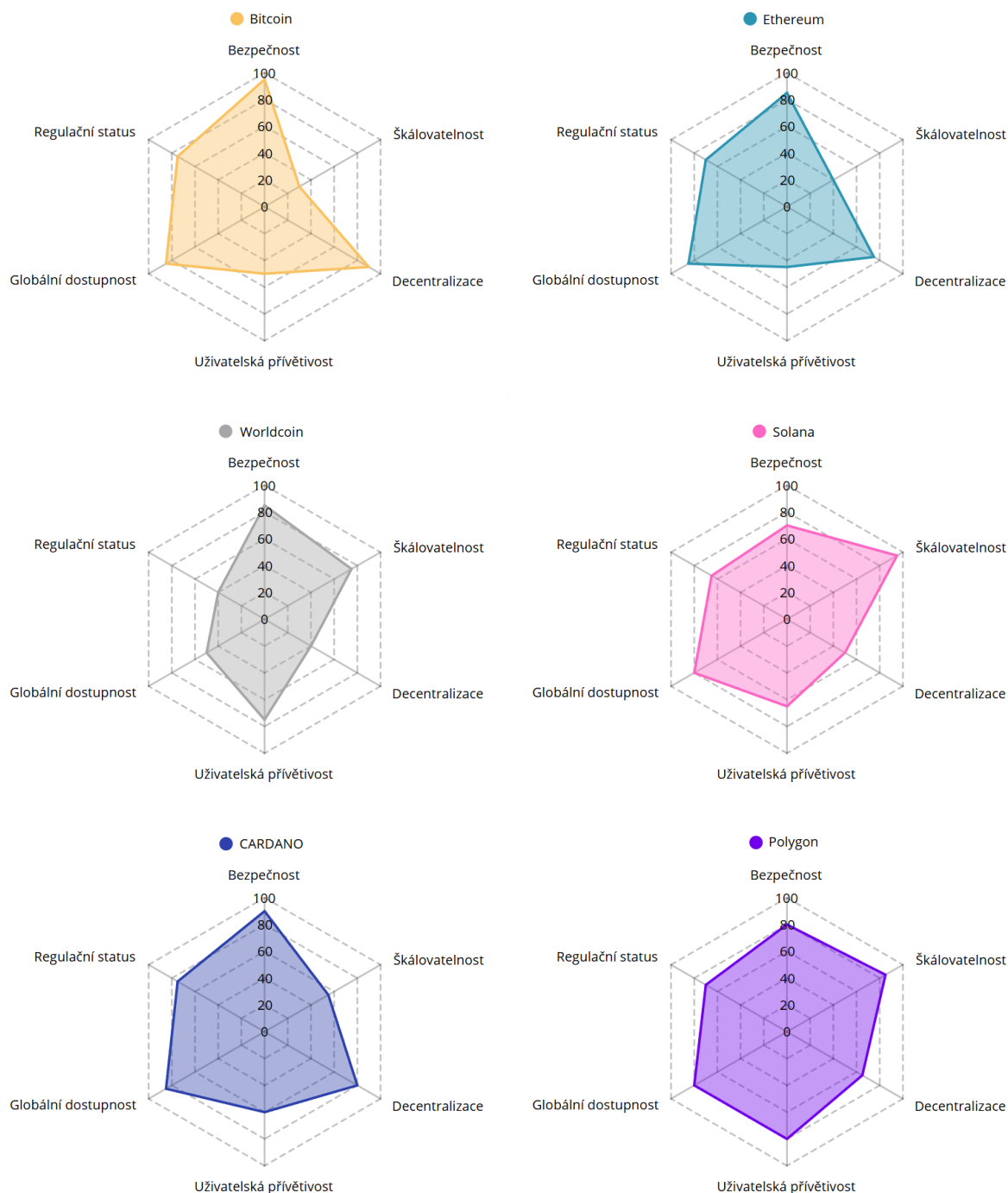
Hodnotící škála – Tabulka 4**Právní výzvy:**

- **Nízké:** Relativně stabilní právní postavení s omezeným množstvím nevyřešených otázek
- **Nízké až střední:** Mírná úroveň právních nejasností, které však nepředstavují zásadní překážku
- **Střední:** Významné nevyřešené právní otázky v některých jurisdikcích nebo oblastech použití
- **Vysoké:** Zásadní právní výzvy ovlivňující fungování nebo budoucí vývoj projektu

Geografická omezení:

- **Minimální:** Legální ve většině jurisdikcí s omezeními jen v několika zemích
- **Významná:** Podstatná geografická omezení včetně zákazů nebo pozastavení provozu ve více jurisdikcích

3.3 Grafické srovnání vybraných aspektů kryptoměn



Obrázek 16 Radarové grafy srovnávající vybrané aspekty kryptoměn

(zdroj: vlastní)

Tyto aspekty byly upřednostněny před jinými díky jejich vyšší relevanci pro celkové hodnocení životaschopnosti projektu a jejich přímému dopadu na uživatelskou zkušenost a adopci. Hodnoty v grafech jsou zpracovány na základě dat a údajů shrnutých z kapitoly 3.

3.4 Shrnutí výhod a nevýhod Worldcoinu

3.4.1 Výhody

- **Efektivní řešení Sybil útoku** – Biometrická verifikace zajišťuje, že každý jedinec může mít pouze jednu identitu v síti, což poskytuje vyšší míru garance jedinečnosti než tradiční kryptoměny založené na ekonomických bariérách
- **Pokročilá ochrana soukromí** – Implementace zero-knowledge proofs umožňuje prokázat jedinečnost identity bez odhalení biometrických dat
- **Potenciál pro spravedlivou distribuci prostředků** – Biometrická verifikace jedinečnosti umožňuje spravedlivou distribuci tokenů mezi skutečné lidi
- **Verifikace lidskosti v éře AI** – Poskytuje mechanismus odolný vůči AI simulacím v době rostoucích schopností umělé inteligence generovat přesvědčivý obsah
- **Integrovaný přístup k identitě a financím** – World App kombinuje funkce identity a finančních služeb v rámci jedné platformy
- **Snadná použitelnost** – Díky vlastní aplikaci World App je systém přístupný i uživatelům bez technických znalostí kryptoměn
- **Možný vysoký výkon transakcí** – Díky implementaci na Optimism Layer 2 nabízí vysokou propustnost a nízké transakční poplatky
- **Potenciál pro AI governance** (soubor pravidel pro provoz AI) – Technologický základ pro systémy, kde je důležité zajistit, že rozhodnutí činí skuteční lidé.
- **Zaměření na globální finanční inkluzi** – Cílí na zpřístupnění finančních služeb lidem bez přístupu k tradičnímu bankovníctví
- **Spravedlivá tokenomika** - 75% celkové nabídky tokenů je určeno pro uživatelskou komunitu (uživatelé, vývojáři, ekosystémové projekty)

3.4.2 Nevýhody

- **Sběr citlivých biometrických dat** – Proces verifikace vyžaduje sběr vysoce citlivých biometrických dat
- **Centralizace procesu verifikace** – Závislost na zařízení Orb vytváří potenciální bod selhání
- **Omezená fyzická dostupnost** – K roku 2025 bylo rozmístěno pouze omezené množství Orbů (866 lokací ve 22 zemích), což limituje možnost uživatelů získat World ID [1]
- **Fyzické bariéry pro škálovatelnost** – Na rozdíl od čistě digitálních kryptoměn je škálovatelnost omezena rychlostí výroby a distribuce fyzických Orbů
- **Nezvratitelnost biometrického sběru** – Na rozdíl od hesel či jiných autentizačních metod nelze biometrické údaje v případě jejich zneužití jednoduše změnit
- **Regulatorní výzvy** – Projekt čelí komplexním regulatorním výzvám kvůli odlišným právním rámcům pro zpracování biometrických dat napříč jurisdikcemi
- **Geografická omezení** – V některých zemích byly operace pozastaveny z regulatorních důvodů, což limituje globální dostupnost
- **Nutnost důvěry v provozovatele** – Uživatelé musí důvěřovat společnosti TFH a operátorům Orbů, že budou dodržovat deklarované postupy ochrany soukromí
- **Vyšší vstupní bariéra** – Proces vyžaduje fyzickou přítomnost u Orbu, což představuje významně vyšší vstupní bariéru než u tradičních kryptoměn
- **Dlouhodobá udržitelnost** – Projekt má zatím neproověřený obchodní model a nejistou dlouhodobou udržitelnost

4 WORLD COIN A WORLD ID: SOUČASNÉ VYUŽITÍ A BUDOUCÍ POTENCIÁL

4.1 Současné využití (2025)

4.1.1 Digitální identifikace v online prostředí

World ID na rozdíl od tradičních metod ověřování, jako jsou hesla, dvoufaktorová autentizace nebo CAPTCHA, nevyžaduje sdílení osobních údajů, které by mohly ohrozit soukromí uživatele. Místo toho využívá ZKP (kapitola 1.3.3), které umožňují prokázat členství v množině ověřených identit bez odhalení konkrétní identity. [1]

World ID nachází praktické uplatnění jako nástroj pro ověření identity na rostoucím počtu populárních online platform. Aktuálně je implementován na sociálních sítích jako Telegram a Reddit, stejně jako v herních prostředích jako Minecraft, kde pomáhá odlišit skutečné uživatele od botů a automatizovaných účtů. [34]

Funkce "Sign in with Worldcoin" představuje alternativu k tradičním přihlašovacím metodám. Implementace je usnadněna prostřednictvím SDK, což přispívá k rozšiřování této funkcionality napříč digitálním ekosystémem. [1]

4.1.2 Spolupráce se seznamovacími aplikacemi

V květnu 2025 společnost Match Group, vlastníci populární seznamovací aplikace včetně Tinderu, Hinge a Match.com, oznámila plán na využívání World ID k ověřování uživatelů na Tinderu v Japonsku. Tato iniciativa představuje významný průlom v aplikaci technologie Worldcoin v oblasti, kde je důvěryhodnost identit zásadním problémem. [35], [1]

Program se zaměřuje na využití World ID jako řešení pro ověřování věku a autenticity profilů, což má zvýšit důvěryhodnost uživatelů a přispět k bezpečnějšímu prostředí online seznamování. Match Group (technologická společnost, která vlastní některé online seznamovací aplikace a služby) vnímá tuto technologii jako prostředek k omezení falešných profilů a zvýšení kvality interakcí mezi uživateli. [1]

4.1.3 Globální expanze

V uplynulých měsících Worldcoin významně rozšířil svou geografickou dostupnost, přičemž významným úspěchem bylo zpřístupnění Orbů v šesti amerických městech: Atlanta,

Austin, Los Angeles, Miami, Nashville a San Francisco. Tato expanze představuje zásadní krok k překonání dřívějších regulatorních překážek na americkém trhu. [36]

Vstup na americký trh následoval po období opatrnosti způsobené regulatorními nejistotami týkajícími se distribuce kryptoměnových tokenů. Worldcoin nyní umožňuje americkým uživatelům nejen verifikovat svou identitu prostřednictvím Orbů, ale také získávat WLD tokeny, což dále rozšiřuje uživatelskou základnu projektu. [36]

K usnadnění globální expanze Worldcoin představil také zařízení "Orb Mini" – kompaktnější verzi původního Orbu, která má zjednodušit proces biometrické verifikace a umožnit rychlejší rozšiřování infrastruktury. [37]

4.1.4 Mini aplikace dApps v ekosystému

World App postupně rozšiřuje své funkce prostřednictvím ekosystému Mini aplikací, které zvyšují užitečnost platformy pro každodenní využití. Tyto Mini aplikace jsou v podstatě webové aplikace otevírané přímo ve World App. [38]

Vývojáři mohou využívat SDK přímo vytvořený pro Worldcoin (MiniKit SDK), který umožňuje těmto aplikacím interagovat s ekosystémem World. Díky tomu mohou aplikace snadno implementovat funkce jako ověření identity pomocí World ID nebo využívat platební systém s WLD tokeny. [38]

Pro podporu růstu ekosystému Mini aplikací spustil Worldcoin v dubnu 2025 program odměn pro vývojáře, který alokuje prostředky ze společného fondu podle počtu World ID verifikovaných uživatelů interagujících s danou aplikací. Mezi populární kategorie patří hry, AI asistenti, finanční aplikace a nástroje pro mezinárodní platby. [37]

4.1.5 World Chain

V roce 2024 Worldcoin významně rozšířil své technologické základy spuštěním vlastního blockchainu World Chain (viz. kapitola 1.3.2).

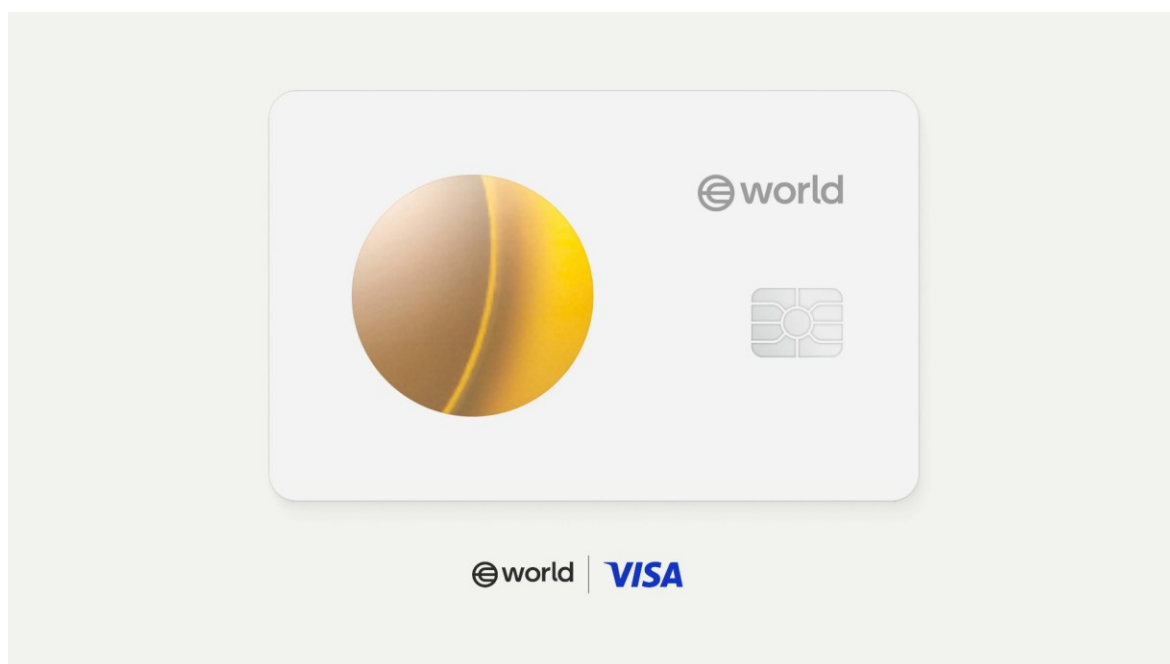
Tento krok k technologické nezávislosti posílil schopnost Worldcoinu adaptovat se na specifické požadavky svého rostoucího ekosystému, především v oblasti rozlišování skutečných lidí od botů a zpracování velkého objemu transakcí při zachování nízkých nákladů.

4.2 Budoucí potenciál

4.2.1 Platební řešení

V květnu 2025 Worldcoin oznámil spolupráci se společností Visa na vývoji "World Card" – platební karty propojující kryptoměnový ekosystém s tradičním platebním systémem. Tato karta, která by měla být dostupná v USA později v roce 2025, propojí aplikaci World App s celosvětovou platební sítí Visa. [36]

Hlavní funkcí World Card bude umožnit uživatelům utrácet WLD tokeny (i jiné kryptoměny) kdekoliv, kde je Visa akceptována, bez nutnosti převedení na fiat měnu. Systém automaticky provede potřebnou směnu v okamžiku transakce, což významně zjednodušuje používání kryptoměn v běžném životě. Karta by měla také nabízet odměnový program zaměřený specificky na služby spojené s AI, přičemž odměny budou vypláceny v tokenech WLD přímo do propojené peněženky. [1], [36]



Obrázek 17 World Card – Worldcoin karta ve spolupráci s VISA

(zdroj: <https://world.org/blog/announcements/world-card-your-digital-assets-accepted-anywhere>)

Univerzální základní příjem (UBI)

Jedním z nejambicióznějších potenciálních využití Worldcoinu je vytvoření infrastruktury pro globální univerzální základní příjem (UBI). Tato vize byla opakovaně zmiňována Samem Altmanem, spoluzakladatelem projektu, a je explicitně zmíněna ve whitepaperu Worldcoinu jako jeden z klíčových případů využití. [1]

Koncept UBI se stává důležitějším v souvislosti s postupující automatizací pracovních pozic a rostoucích schopností AI, které mohou vést k významné změně pracovního trhu. Worldcoin nabízí technologické řešení dvou zásadních výzev spojených s implementací UBI v globálním měřítku [1]:

1. **Identifikace příjemců** – Biometrická verifikace zajišťuje, že každý člověk může obdržet svůj podíl pouze jednou, což eliminuje riziko podvodů a multiplikace identit.
2. **Efektivní distribuce** – Decentralizovaná blockchain infrastruktura umožňuje přímé zasílání prostředků bez závislosti na tradičních finančních institucích, což je zvláště významné v regionech s omezeným přístupem k bankovním službám.

Současný systém pravidelných grantů WLD tokenů pro ověřené uživatele lze vnímat jako zkušební verzi tohoto konceptu, byť v omezené podobě.

4.2.2 Standardizace "proof-of-human" neboli PoP

Vzhledem k rychlému vývoji generativní AI se "důkaz o člověku" stává zásadním pro fungování digitálního světa. Navzdory riziku, že pokročilá AI by mohla vytvářet falešné biometrické údaje pro obcházení PoP systémů, Worldcoin spoléhá na pokročilé softwarové i hardwarové bezpečnostní mechanismy. World ID může sloužit jako globální standard v této oblasti s potenciálem pro široké využití na různých platformách a službách.

Tato standardizace může výrazně zlepšit kybernetickou bezpečnost, online hlasování, přístup k omezeným zdrojům a další oblasti, kde je nutné spolehlivě odlišit lidi od automatizovaných systémů.

4.2.3 Ochrana proti dezinformacím

S rostoucími vývojem AI se problematika dezinformací a deepfakes (AI vytvářející falešné, ale realistické audiovizuální materiály) stává stále naléhavější. World ID by mohl sloužit jako podstatný nástroj pro rozlišování mezi obsahem vytvořeným lidmi a AI, což by pomohlo v boji proti dezinformacím a manipulacím v online prostředí. [37]

Potenciální využití v této oblasti může zahrnovat:

1. **Verifikace původu obsahu** – Označení obsahu, který byl vytvořen verifikovanými lidskými uživateli, což by usnadnilo rozlišení od obsahu generovaného AI
2. **Důvěryhodné zpravodajství** – Integraci World ID do zpravodajských platforem pro zvýšení důvěryhodnosti publikovaných informací
3. **Autentifikace digitálních děl** – Propojení digitálních děl s ověřenými lidskými tvůrci, což by pomohlo v boji proti neoprávněnému využívání AI k napodobování stylu známých umělců či autorů
4. **Bezpečné online volby** – Zajištění, že každý člověk může hlasovat pouze jednou, bez možnosti manipulace automatizovanými systémy
5. **Ověřené recenze** – Zajištění, že recenze produktů a služeb pocházejí od skutečných uživatelů, ne od botů nebo placených falešných recenzí

4.3 Potencionální rizika

Navzdory inovativnímu přístupu a ambiciózní vizi Worldcoinu existuje několik významných rizik, která mohou ohrozit dlouhodobou udržitelnost a společenské přijetí projektu.

4.3.1 Etické a soukromí ohrožující praktiky při získávání uživatelů

Historický vývoj Worldcoinu ukazuje na problematické praktiky při získávání prvních uživatelů, které by mohly negativně ovlivnit důvěru v projekt [3]:

- **Nedostatečný informovaný souhlas** – Podle výzkumu od Eileen Guo a Adi Renaldi mnoho uživatelů v rozvojových zemích nebylo řádně informováno, že jsou "testovacími uživateli" nebo že jejich biometrická data byla použita k trénování algoritmů. Účastníci často nevěděli, že jejich data byla zpracovávána jinak než data budoucích uživatelů.
- **Problematický marketing** – V některých regionech používal Worldcoin klamavé taktiky – například v západní Jávě získávali uživatele pod záminkou "rozdávání sociální podpory". V Súdánu lákali uživatele na soutěže o AirPods (sluchátka od společnosti Apple), protože bylo obtížné "vysvětlit koncept digitálních měn lidem, kteří nemají ani e-mail".

- **Využívání ekonomické zranitelnosti** – Projekt cílil na chudé populace, kde i malá odměna představovala silný motivační faktor. Keňský operátor Bryan Mtembei to označil za "manipulaci a využívání studentů bez jasného vysvětlení".

4.3.2 Bezpečnostní rizika a zranitelnosti

Systém Worldcoinu čelí několika potenciálním bezpečnostním rizikům, která mohou ohrozit integritu celého ekosystému [3]:

- **Problémy zařízení Orb** – Byly zaznamenány technické poruchy včetně selhání při rozpoznávání duhovky. Operátor ze Súdánu uvedl: "Mému příteli trvalo celý týden, než zařízení rozpoznalo jeho duhovku". Zařízení také vyžadovala častou údržbu v Německu.
- **Riziko krádeže identity** – V roce 2021 se podnikateli v Indonésii podařilo získat přístup k peněženkám více než 200 uživatelů po jejich verifikaci Orbem a převést jejich prostředky. Worldcoin tvrdí, že po přechodu na mobilní aplikace tento typ podvodu nezaznamenali.
- **Centralizace ověřování** – Závislost na centralizovaném zařízení pro ověřování identity odporuje decentralizačním principům kryptoměn a vytváří potenciální jediný bod selhání.
- **Riziko nelegálního využití** – Evropský parlament upozorňuje, že kryptoaktiva obecně představují riziko praní špinavých peněz a financování terorismu, proto připravuje regulaci MiCA (Markets in Crypto-Assets) pro sledování a identifikaci převodů kryptoaktiv. [46]

4.3.3 Regulatorní překážky

Biometrická povaha Worldcoinu vyvolává zásadní regulatorní otázky, které mohou limitovat jeho globální přijetí [3]:

- **Problematická ochrana osobních údajů** – Sběr biometrických dat podléhá přísným regulacím jako GDPR. Worldcoin sám ve svých dřívějších podmínkách naznačoval možný nesoulad s GDPR.
- **Nejasný právní status** – V některých regionech byly odhaleny potenciálně korupční praktiky, například platby místním úředníkům v Indonésii za každou naskenovanou osobu, označované jako "peníze na kávu a cigarety".

- **Evropský regulační rámec** – Nařízení MiCA vyžaduje transparentnost, ochranu spotřebitelů a monitorování transakcí, což znamená pro Worldcoin dodatečné regulační překážky. [46]

4.3.4 Problémy dlouhodobé udržitelnosti

Model Worldcoinu přistup několik zásadních překážek pro zajištění dlouhodobé udržitelnosti projektu:

- **Fyzické bariéry pro globální rozšíření** – Závislost na fyzických zařízeních Orb omezuje globální pokrytí
- **Nezvrátitelnost biometrické identifikace** – Na rozdíl od hesel nebo jiných forem digitální identity nelze biometrické údaje v případě kompromitace nebo zneužití "resetovat". Toto představuje závažné dlouhodobé riziko pro uživatele, kteří již poskytli svá biometrická data.
- **Ekonomická a investiční nejistota** –Token WLD zaznamenal pokles o více než 70 % za poslední rok (k 4. 6. 2025) [8]

4.3.5 Etické problémy "digitální kolonizace"

Projekt Worldcoin vyvolává závažné etické otázky, které přesahují běžné problémy spojené s kryptoměnami a zasahují do samotných základů společenských hodnot a norem [3]:

- **Krypto-kolonialismus** – Odborníci jako Payal Arora a Pete Howson označují přístup Worldcoinu za formu "krypto-kolonialismu", kdy jsou "blockchainové experimenty vnucovány zranitelným komunitám", které se nemohou bránit.
- **Zacházení s lidským tělem jako s nástrojem** – Kritici poukazují na dehumanizující přístup projektu včetně Edwarda Snowdena (americký whistleblower, bývalý zaměstnanec CIA), který uvedl: "Nekatalogizujte oční bulvy. Ve skutečnosti nepoužívejte biometrii pro nic. Lidské tělo nejsou razítkovací kleště."

ZÁVĚR

Tato bakalářská práce byla zaměřena na komplexní popis a analýzu projektu Worldcoin, který představuje unikátní spojení kryptoměnové technologie s biometrickou identifikací. Cílem práce bylo poskytnout podrobný přehled technologických základů, principů fungování a současného využití Worldcoinu, stejně jako jeho srovnání s ostatními významnými kryptoměnami.

V teoretické části byla prozkoumána historie vzniku projektu od jeho zakladatelů Sama Altmana a Alexe Blanie až po současnost, kdy projekt dosahuje více než 12 milionů verifikovaných uživatelů. Detailně byly analyzovány technologické základy, zejména protokol World ID, architektura blockchainu a implementace zero-knowledge důkazů. Zvláštní pozornost byla věnována biometrickému zařízení Orb, které představuje klíčový prvek celého systému pro ověřování jedinečnosti uživatelů prostřednictvím skenování duhovky oka.

V praktické části práce byla provedena rozsáhlá srovnávací studie Worldcoinu s nejpoužívanějšími kryptoměnami včetně Bitcoinu, Etherea, Solany, Cardana a Polygonu. Srovnání ukázalo, že Worldcoin přináší zcela nový přístup k řešení problému Sybil útoků, ale za cenu vyšších vstupních bariér a závislosti na fyzické infrastruktuře. Zatímco tradiční kryptoměny řeší problém důvěry v oblasti financí, Worldcoin se zaměřuje na výzvu důvěryhodné identifikace lidských bytostí v digitálním prostoru.

Srovnávací studie také identifikovala hlavní výhody Worldcoinu: efektivní řešení problému falešných identit, pokročilá ochrana soukromí prostřednictvím zero-knowledge důkazů a potenciál pro spravedlivou distribuci prostředků. Současně však projekt čelí významným výzvám, včetně regulatorních překážek spojených se sběrem biometrických dat, etických otázek týkajících se postupů získávání uživatelů v rozvojových zemích a fyzických omezení škálovatelnosti.

Analýzou současného využití byla odhalena rostoucí adopce World ID na populárních platformách a významná partnerství, včetně spolupráce s Match Group na ověřování uživatelů Tinderu a s Visa na vývoji platební karty World Card. Tyto spolupráce ukazují praktickou využitelnost technologie a její možnosti pro komerční uplatnění.

Worldcoin představuje ambiciózní pokus o vytvoření globální identitní a finanční infrastruktury, která má potenciál významně ovlivnit budoucnost digitální identity. Úspěch

projektu bude záviset na schopnosti vyřešit současné regulatorní a etické výzvy při zachování technologické inovativnosti a zodpovědnosti vůči společnosti.

SEZNAM POUŽITÉ LITERATURY

- [1] WORLD. *A New Identity and Financial Network*. Online. Dostupné z: <https://whitepaper.world.org/>. [cit. 2025-02-24].
- [2] GENT, Edd. *A Cryptocurrency for the Masses or a Universal ID?: Worldcoin Aims to Scan all the World's Eyeballs*. Online. IEEE Spectrum. 2023, roč. 60, č. 1, s. 42-57. ISSN 0018-9235. Dostupné z: <https://doi.org/10.1109/MSPEC.2023.10006664>. [citováno 2025-02-24].
- [3] GUO, Eileen a RENALDI, Adi. *Deception, exploited workers, and cash handouts: How Worldcoin recruited its first half a million test users*. Online. TechReview: MIT Technology Review. Cambridge, Massachusetts, United States: Massachusetts Institute of Technology. April 6, 2022. Dostupné z: <https://www.technologyreview.com/2022/04/06/1048981/worldcoin-cryptocurrency-biometrics-web3>. [citováno 2025-02-24].
- [4] GEORGE, A. Shaji; GEORGE, A. S. Hovan a BASKAR, T. *Worldcoin: A Decentralized Currency for a Unified Global Economy*. 2023, roč. 2, č. 2, s. 136-155. Dostupné z: <https://www.allcryptowhitepapers.com/wp-content/uploads/2018/05/Worldcoin-research-whitepaper.pdf>. [citováno 2025-02-24].
- [5] BINANCE ACADEMY. *What Is Worldcoin?* Online. 2023. Dostupné z: <https://academy.binance.com/en/articles/what-is-worldcoin>. [cit. 2025-02-24].
- [6] WORLD. *Opening the Orb: A look inside Worldcoin's biometric imaging device*. Online. Dostupné z: <https://world.org/blog/engineering/opening-orb-look-inside-worldcoin-biometric-imaging-device>. [cit. 2025-02-24].
- [7] FORBES. *Worldcoin: The Cryptocurrency That Wants To Scan Your Eyeballs*. Online. Dostupné z: <https://www.forbes.com/advisor/investing/cryptocurrency/what-is-worldcoin/>. [cit. 2025-02-24].
- [8] BLOX. *Worldcoin: everything you need to know about WLD*. Online. Dostupné z: https://weareblox.com/en-eu/worldcoin?utm_medium=search&utm_source=google. [cit. 2025-02-24].
- [9] COINDESK. *The Untold Story of Worldcoin's Launch: Inside the Orb*. Online. Dostupné z: <https://www.coindesk.com/consensus-magazine/2023/07/24/the-untold-story-of-worldcoins-launch-inside-the-orb>. [cit. 2025-02-24].

- [10] IEEE SPECTRUM. *Worldcoin Launched. Then Came the Backlash*. Online. Dostupné z: <https://spectrum.ieee.org/worldcoin-2664361259>. [cit. 2025-02-24].
- [11] GIGI. *21 lekcí: co mě naučil pád do bitcoinové králičí nory*. Přeložil František ŠIMEK. Praha: Braiins Systems, 2022. ISBN 978-80-908709-0-1.
- [12] COINGECKO. *Worldcoin Price*. Online. Dostupné z: <https://www.coingecko.com/en/coins/worldcoin>. [cit. 2025-03-19].
- [13] COINCODEX. *Worldcoin Price*. Online. Dostupné z: <https://coincodex.com/crypto/worldcoin-org/>. [cit. 2025-03-19].
- [14] NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. Online. Dostupné z: <https://bitcoin.org/bitcoin.pdf>. [cit. 2025-03-019].
- [15] ETHEREUM. *Ethereum Whitepaper*. Online. Dostupné z: <https://ethereum.org/en/whitepaper/>. [cit. 2025-03-19].
- [16] WORLD. *The real human network*. Online. Dostupné z: <https://world.org/>. [cit. 2025-03-19].
- [17] COINMARKETCAP. *Today's Cryptocurrency Prices by Market Cap*. Online. Dostupné z: <https://coinmarketcap.com/>. [cit. 2025-04-26].
- [18] ETHEREUM. *The Merge*. Online. Dostupné z: <https://ethereum.org/en/roadmap/merge/>. [cit. 2025-04-26].
- [19] BETZ, Brandy. *Sam Altman's Crypto Project Worldcoin Raises \$115M, Led by Blockchain Capital*. Online. 2023. Dostupné z: <https://www.coindesk.com/business/2023/05/25/sam-altmans-crypto-project-worldcoin-raises-115m-led-by-blockchain-capital>. [cit. 2025-02-24]
- [20] LIGHTNING NETWORK. *Lightning Network – Scalable, Instant Bitcoin/Blockchain Transactions*. Online. Dostupné z: <https://lightning.network/>. [cit. 2025-04-22].
- [21] AKOVENKO, Anatoly. *Solana: A new architecture for a high performance blockchain v0.8.13*. Online. Dostupné z: <https://solana.com/solana-whitepaper.pdf>. [cit. 2025-04-27].
- [22] CARDANO DOCS. Online. Dostupné z: <https://docs.cardano.org/>. [cit. 2025-04-27].

- [23] REUTERS. *Kenya suspends Worldcoin's crypto project over safety concerns*. Online. 2022. Dostupné z: <https://www.reuters.com/world/africa/kenyan-government-suspends-activities-worldcoin-country-2023-08-02/>. [cit. 2025-05-05].
- [24] DEFI LLAMA. *Total Value Locked in DeFi*. Online. Dostupné z: <https://defillama.com/> [cit. 2025-04-28].
- [25] FATF. *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. Online. Dostupné z: <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-rba-virtual-assets-2021.html>. [cit. 2025-05-02].
- [26] NAILWAL, Sandeep; CHAUDHARY, Amit a DENG, Wenxuan. *POL: One token for all Polygon chains*. Online. Dostupné z: <https://polygon.technology/papers/pol-whitepaper>. [cit. 2025-05-02].
- [27] CHAINSPECT. Online. Dostupné z: <https://chainspect.app/>. [cit. 2025-05-02].
- [28] BUZZMAG. *Solana (SOL): Vše, co potřebujete vědět*. Online. 2021. Dostupné z: <https://www.buzzmag.cz/solana-sol/>. [cit. 2025-05-02].
- [29] BINANCE. *Polygon (MATIC)*. Online. 2021. Dostupné z: <https://www.binance.com/en/research/projects/matic-network>. [cit. 2025-05-02].
- [30] POLYGON. Online. Dostupné z: <https://polygon.technology/>. [cit. 2025-05-05].
- [31] FEYEN, Erik; KAWASHIMA, Yusaku a MITTAL, Raunak. *Crypto-Assets Activity around the World Evolution and Macro-Financial Drivers*. Online. 2022. [cit. 2025-05-05].
- [32] ALZA.CZ. *Cardano (VŠE, CO CHCETE VĚDĚT) – Kryptoměna s velkým potenciálem, ale i riziky*. Online. Dostupné z: <https://www.alza.cz/cardano-ada>. [cit. 2025-05-05].
- [33] BITRSS – WORLD CRYPTO NEWS. *Worldcoin Expands in the U.S., Unveils Crypto Visa Card, and Partners with Tinder*. Online. Dostupné z: <https://bitrss.com/worldcoin-expands-in-the-u-s-unveils-crypto-visa-card-and-partners-with-tinder-84949>. [cit. 2025-05-05].
- [34] TECHCRUNCH. *Worldcoin adds integrations with Minecraft, Reddit, Telegram, Shopify and Mercado Libre*. Online. 2023. Dostupné

z: <https://techcrunch.com/2023/12/13/worldcoin-integration-reddit-telegram-shopify/>. [cit. 2025-05-05].

- [35] TECHCRUNCH. *World partners with Tinder, Visa to bring its ID-verifying tech to more places*. Online. 2025. Dostupné z: <https://techcrunch.com/2025/04/30/world-partners-with-tinder-visa-to-bring-its-id-verifying-tech-to-more-places/>. [cit. 2025-05-05].
- [36] ALTCOIN BUZZ. *Worldcoin Launches in U.S. with Eye Scans and Visa Card*. Online. 2025. Dostupné z: <https://www.altcoinbuzz.io/cryptocurrency-news/worldcoin-launches-in-u-s-with-eye-scans-and-visa-card/>. [cit. 2025-05-05].
- [37] BLOCKWORKS. *Sam Altman's Worldcoin gets new Orb Mini and US launch*. Online. 2025. Dostupné z: <https://blockworks.co/news/sam-altman-worldcoin-orb-mini-eye-scan>. [cit. 2025-05-05].
- [38] WORLD. *Mini Apps*. Online. Dostupné z: <https://docs.world.org/mini-apps>. [cit. 2025-05-05].
- [39] MAHESHWARI, Rashi. *What Are Crypto Exchanges And How Do They Work*. Online. Dostupné z: <https://www.forbes.com/advisor/in/investing/cryptocurrency/what-is-a-crypto-exchange/>. [cit. 2025-05-16].
- [40] ANYCOIN. *Měny*. Online. Dostupné z: <https://www.anycoin.cz/currencies>. [cit. 2025-05-16].
- [41] TOKEN TERMINAL. *World Chain WLD*. Online. Dostupné z: https://tokenterminal.com/explorer/projects/worldcoin/metrics/transactions-per-second?utm_source=chatgpt.com. [cit. 2025-05-16].
- [42] COINCODECAP. *A Deep Dive Into SOLANA: SOL Tokenomics Explained*. Online. 2025. Dostupné z: <https://coincodecap.com/solana-sol-tokenomics>. [cit. 2025-05-16].
- [43] KALOUSEK, Ing. Zbyněk. *Může být Solana budoucností kryptoměn?* Online. 2024. Dostupné z: <https://zpravy.kurzy.cz/781516-muze-byt-solana-budoucnosti-kryptomen/>. [cit. 2025-05-16].

- [44] HELIUS. *A Complete History of Solana Outages: Causes, Fixes, and Lessons Learnt*. Online. 2025. Dostupné z: <https://www.helius.dev/blog/solana-outages-complete-history>. [cit. 2025-05-16].
- [45] UNCHAINED. *SEC Investigating Ethereum Foundation Regarding Proof-of-Stake Transition: Report*. Online. 2024. Dostupné z: <https://unchainedcrypto.com/sec-investigating-ethereum-foundation-regarding-proof-of-stake-transition-report/>. [cit. 2025-05-16].
- [46] EUR-LEX. *Evropské nařízení o kryptoaktivech (MiCA)*. Online. 2022. Dostupné z: <https://www.europarl.europa.eu/topics/cs/article/20220324STO26154/rizika-kryptomen-a-prinos-legislativnich-opatreni-eu>. [cit. 2025-05-16].

SEZNAM OBRÁZKŮ

Obrázek 1 Zjednodušené schéma bloků v blockchainu	21
Obrázek 2 Zjednodušené znázornění architektury Worldcoin.....	22
Obrázek 3 Diagram ověření identity uživatele pomocí World App a ZKP	24
Obrázek 4 Zařízení Orb.....	27
Obrázek 5 Rozklad komponentů orbu	28
Obrázek 6 Tři roky výzkumu a vývoje Orbu	29
Obrázek 7 Teleobjektiv a gimbalový systém.....	31
Obrázek 8 Srovnání kvality snímku duhovky z Orbu versus běžný standard	32
Obrázek 9 Proces transformace kruhové duhovky do obdélníkového formátu	33
Obrázek 10 Výsledek normalizace	33
Obrázek 11 Konkrétní příklad anonymizovaného iris kódu	34
Obrázek 12 Proces zpracování biometrických dat v systému Worldcoin.....	35
Obrázek 13 Ukázka rozhraní aplikace World App	40
Obrázek 14 Ukázka Mini Apps v aplikaci World App.....	41
Obrázek 15 Cenový vývoj tokenu WLD od spuštění až do 4. června 2025	46
Obrázek 16 Radarové grafy srovnávající vybrané aspekty kryptoměn	66
Obrázek 17 World Card – Worldcoin karta ve spolupráci s VISA.....	71

SEZNAM TABULEK

Tabulka 1 Srovnávací tabulka technologických aspektů kryptoměn.....	54
Tabulka 2 Srovnávací tabulka ekonomických aspektů kryptoměn	58
Tabulka 3 Srovnávací tabulka uživatelských aspektů kryptoměn	60
Tabulka 4 Srovnávací tabulka právních a regulačních aspektů kryptoměn.....	64

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

2D	Two Dimensional (dvojrozměrný)
3D	Three Dimensional (trojrozměrný)
ADA	Token kryptoměny Cardano
AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
BTC	Bitcoin
CIA	Central Intelligence Agency
CZK	Česká koruna
dApps	Decentralized Applications
DeFi	Decentralized Finance
DPO	Data Protection Officer
DPIA	Data Protection Impact Assessment
dApps	Decentralizované aplikace
ENS	Ethereum Name Service
ETH	Token kryptoměny Ethereum
EUR	Euro
GDPR	General Data Protection Regulation
GPS	Global Positioning System
ID	Identification/Identity
KYC	Know Your Customer
KRW	Korejský won
L1	Layer 1
L2	Layer 2
LED	Light Emitting Diode

LN	Lightning Network
LTE	Long Term Evolution
MATIC	Token kryptoměny Polygon
MiCA	Markets in Crypto-Assets
NFT	Non-Fungible Token
P2P	Peer-to-Peer
PoH	Proof-of-History
PoP	Proof-of-Personhood
PoS	Proof-of-Stake
PPPoPP	Privacy-Preserving Proof-of-Personhood Protocol
QR	Quick Response
ROI	Return on Investment
SDK	Software Development Kit
SOL	Token kryptoměny Solana
SAFE	Smart Account For Everyone
TEE	Trusted Execution Environment
TFH	Tools for Humanity
TPS	Transactions Per Second
UBI	Universal Basic Income
USD	Americký dolar
USDT	Tether
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WLD	Worldcoin token
zkEVM	Zero-Knowledge Ethereum Virtual Machine
ZKP	Zero-Knowledge Proof

