Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Využití blockchainových technologií, nejen v kryptoměnách

Jan Bartoš

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Bartoš

Informatika

Název práce

Využití blockchainových technologií, nejen v kryptoměnách

Název anglicky

Uses of blockchain technology, not only in cryptocurrency

Cíle práce

Cílem bakalářské práce je porovnání vývojářských nástrojů blockchainu na základě návrhu metody vícekriteriální analýzy.
Dalším cílem je analýza atributů vývojářských nástrojů blockchainu ovlivňujících jejich použitelnost a vytvoření přehledu dostupných nástrojů.

Metodika

Metodika řešené problematiky bakalářské práce bude založena na studiu a analýze odborných informačních zdrojů.

V praktické části budou analyzovány vlastnosti vývojářských nástrojů blockchainu včetně jejich charakteristik. Poté bude navržena vícekriteriální analýza pro jejich hodnocení. Na základě kombinace teoretických poznatků a výsledků vlastního řešení budou formulovány závěry bakalářské práce.

Doporučený rozsah práce

40

Klíčová slova

blockchain, technologie, vícekriteriální analýza, vývojářské nástroje

---

Doporučené zdroje informací

ANTONOPOULOS, Andreas. Mastering Ethereum: Building Smart Contracts and DApps. Sebastopol, CA: O'Reilly Media, 2018. ISBN 1491971940.

CHOWDHURY, N. *Inside Blockchain, Bitcoin, and Cryptocurrencies. [elektronický zdroj] /.* Milton: Auerbach Publishers, Incorporated, 2019. ISBN 9781000507706.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

Pedersen, Asger & Risius, Marten & Beck, Roman. (2019). A Ten-Step Decision Path to Determine When to Use Blockchain Technologies. MIS Quarterly Executive. 18. 99-115. 10.17705/2msqe.00010.

STROUKAL, D. – SKALICKÝ, J. *Bitcoin a jiné kryptopeníze budoucnosti : historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky.* Praha: Grada Publishing, 2018. ISBN 978-80-271-0742-1.

Předběžný termín obhajoby

2022/23 LS – PEF

Vedoucí práce

RNDr. Alexander Galba

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 19. 6. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 27. 10. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Děkan

V Praze dne 15. 03. 2023

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci " Využití blockchainových technologií, nejen v kryptoměnách" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3.2023 _____

Poděkování

Rád bych poděkoval svému vedoucímu práce, panu RNDr. Alexandru Galbovi, za to, že mi umožnil zpracovávat bakalářskou práci právě u něj. Chtěl bych mu také poděkovat za jeho rady a připomínky během konzultací. Dále bych chtěl poděkovat své mamince, za její podporu a pomoc. Nakonec bych také rád poděkoval komunitě technologie blockchain, jelikož poskytuje svou technologii všem zdarma a snaží se inovovat svět.

Využití blockchainových technologií, nejen v kryptoměnách

Abstrakt

Tato práce se zaměřuje na vícekriteriální rozhodování při výběru vhodných blockchainových vývojářských nástrojů v oblasti zdravotnictví. Práce se skládá z teoretické a praktické části. V teoretické části je popsán blockchain jako technologie, jeho základní principy a funkce. Dále mechanismy, na kterých je tato technologie postavena, a také její využití ve světě. V praktické části je popsána metoda analytického hierarchického procesu a pomocí této metody jsou porovnána na základě několika kritérií jednotlivá blockchainová vývojová prostředí - Bitcoin, Ethereum, Hyperledger Fabric, R3 Corda a Ripple. Z těchto pěti zvolených variant je vybrána ta, která je dle předloženého rozhodovacího procesu nejvhodnější pro oblast zdravotnictví.

Klíčová slova: blockchain, případy užití, vícekriteriální rozhodování, analytický hierarchický proces, zdravotnictví

Uses of blockchain technology, not only in cryptocurrency

Abstract

This thesis focuses on multi-criteria decision-making in the selection of appropriate blockchain development tools in the field of healthcare. The work consists of a theoretical and a practical part. The theoretical part describes blockchain as a technology, its basic principles and functions. Furthermore, the mechanism on which this technology is built, as well as its use in the world. In the practical part, the method of analytical hierarchical process is described and with the help of this method, individual blockchain development environments – Bitcoin, Ethereum, Hyperledger Fabric, R3 Corda and Ripple, are compared based on several criteria. From these five selected variants, the one that is most suitable for the health sector according to the presented decision-making process is selected.

Keywords: blockchain, use cases, multi-criteria decision making, analytical hiearchy process, healthcare

Obsah

Obsah

1. Úvod

Jako relativně mladá technologie má blockchain mnoho teoretický návrhů. Ve své podstatě nabízí odpověď na spoustu problémů moderních technologií. Pokud slyšíme o blockchainu v médiích, je to z většiny případů v oblasti kryptoměn. Základní vlastnosti ale poukazují na mnohem širší využití, která jsou ale ještě v raném věku. Inspirací pro mou práci byl z části zájem o inovaci, kterou tato technologie může nabídnout a také celková filozofie. Satoshi Nakamoto postavil základy unikátní technologii, ke které dal přístup všem, zatímco sám zůstal v anonymitě. Jeho identita je v době psaní této práce stále neznámá a jeho peněženka obsahuje velké bohatství, které je ovšem stále nepřivlastněné. Tato nezištnost vytvořila nespočet následovníků, kteří se snaží zlepšit svět a rozvíjet dále jeho vizi.

Tato práce je rozdělena na několik dílčích kapitol. V teoretické části jsou nejdříve vysvětleny základní principy této technologie, jak funguje, jaké má vlastnosti. Blockchain má mnoho teoretických návrhů, které stále ještě nejsou realizované. Proto je další část věnovaná využitím, které mohou potencionálně zlepšit svět.

Praktická část se soustředí na rozhodování. S rozhodováním se setkáváme na denní bázi. Díky České zemědělské univerzitě se studenti setkávají s metodami řešení komplexnějších rozhodovacích problémů. Jednou z těchto metod je analytický hierarchický proces, který při porovnání variant a kritérií dokáže nabídnout vhodnou variantu řešení a jeho blízké alternativy. Tento proces je využit v rozhodovacím procesu, při výběru vhodného vývojového nástroje blockchainu v oblasti zdravotnictví.

2. Cíl práce a metodika

Cíl práce

Cílem této bakalářské práce je porovnání vývojářských nástrojů blockchainu na základě návrhu metody vícekriteriální analýzy. V teoretické části jsou vysvětleny různé aplikace technologie blockchain, nejen její nejznámější v oblasti kryptoměn. Z tohoto výčtu je vybrána oblast, pro kterou je pomocí analytického hierarchického procesu zvolena vhodná varianta řešení a její blízké alternativy. Tato práce tedy slouží jako shrnutí potencionálních využití a podklad pro další rozhodovatele v oblasti blockchainových řešení.

Metodika

Tato bakalářská práce je tvořena dvěma částmi. První část se skládá z teoretických východisek, která jsou vypracována na základě rešerše dostupných literárních a internetových zdrojů. Nejdříve je popsána problematika technologie blockchain. Následně je vytvořen seznam využití. Tento seznam je podkladem pro výběr oblasti, jež bude předmětem rozhodování v další části.

V praktické části je nejdříve popsána metoda vícekriteriálního rozhodování. Následně je vybrána oblast, ke které je sestrojen profil rozhodovatele, zvolení variant a kritérií. Následuje sestrojení tabulky obsahující data, která vstoupí do analytického hierarchického procesu, ve kterém je provedeno párové porovnání kritérií a variant. Podle tohoto porovnání je každá varianta ohodnocena pro jednotlivá kritéria. Výsledná tabulka obsahuje sumy ohodnocení jednotlivých kritérií a jejich výsledné pořadí.

3. Teoretická východiska

3.1. Blockchain

Blockchain je síť decentralizovaného virtuálního počítače uloženého na více uzlech. Tato síť periodicky produkuje bloky (block), které fungují jako prostředek uchování dat a služeb. Bloky jsou spojené do řetězce (chain). Toto spojení představuje blockchain, jehož účelem je být transparentní databází všeho, co se v dané síti stalo. Můžeme si představit katastr nemovitostí - jeho uživatelé si mohou zobrazit, kdo vlastnil pozemek před nimi, kolik za něj zaplatili a kdy se to stalo. Aplikace uložené na novějších blockchain sítích by i umožňovaly automatický nákup, prodej a následný zápis do sítě. Data už ale nemohou být nikdy změněna, nejen proto přináší mnoho příležitostí.
(STROUKAL D., SKALICKÝ J., 2018)

3.1.1. Blok

Blok je základním stavebním kamenem technologie blockchain. Ukládá v sobě malé množství nejdůležitějších informací, nejčastěji (Nakamoto, S. 2008):

- identifikační číslo
- velikost bloku
- hash předchozího bloku
- hash transakcí uvnitř bloku
- čas vzniku bloku
- Merkleův strom
- počet bitů potřebných pro vyřešení tzv. Nonce (zašifrované číslo, které po vyřešení těžařů blok uzavře)

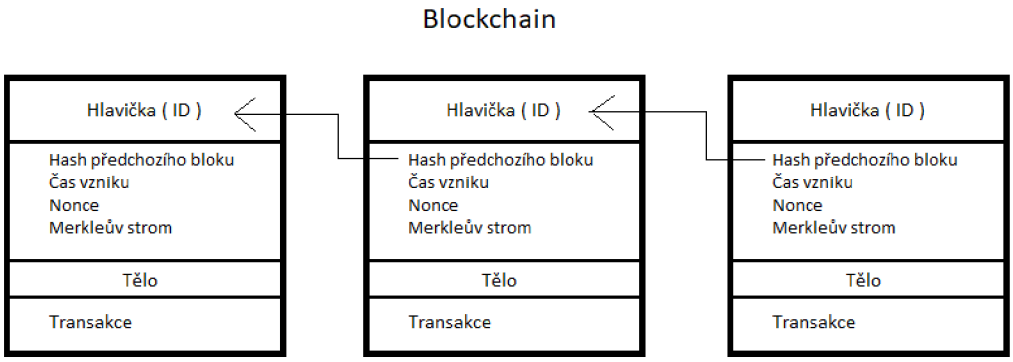
3.1.2. Řetězec

Řetězec spojuje bloky do řady jeden po druhém, bloky jsou spojené právě informacemi, které jsou uložené v hlavičce. Nejnovější blok ukazuje na svého předka a takto to pokračuje až k prvnímu bloku. První blok se nazývá „Genesis block“ a nemá předka (odkazuje se na 0), občas se řetězec větví do více směrů, pracuje se ale jen s nejdelší větví. Zamezí to podvodům, jelikož změna jednoho bloku by znamenala přepočítání všech následníků a nepracovalo by se

s nejdelší větví. Tento řetězec je transparentní, každý se může podívat a verifikovat, co se stalo. (Meynkhard, A. 2019)

Zjednodušené přirovnání by byla kniha, která obsahuje data všech pozemků v ČR a jejich historii. Lze zde zobrazit, kdo vlastnil jaký pozemek, kolik za něj zaplatil a kdy se to stalo. Usnadní to složité předávání informací mezi úřady nebo lidmi. (Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., 2018)

Obrázek 1 – Schéma blockchainu



Zdroj: vlastní zpracování

3.1.3. Kryptografie

Kryptografie se zabývá utajováním komunikace. Jejím cílem je převod zpráv do takové formy, které budou rozumět jen strany, jimž má být zpráva předána. V historii šlo spíše o vytvoření šifry, s postupem vývoje výpočetní technologie se z ní stala matematická disciplína, kde zašifrování a odšifrování za nás řeší počítače.

3.1.4. Šifrování

Šifrování umožňuje bezpečnou komunikaci dvou stran bez toho, aby citlivé informace spadly do rukou třetí, nezvané strany. Zlehčuje to také předání informací, protože se nemusí používat prostředník, jako například banka. Všeobecně máme několik způsobů šifrování, všechna šifrování používají klíč. Klíč přeměňuje data, tak aby z nich nešla extrahovat informace, klíč se také využívá druhým směrem, a to při rozšifrování nečitelných dat na srozumitelná.

3.1.4.1. Symetrické

Používá stejný klíč k zašifrování i odšifrování dat.

3.1.4.2. Asymetrické

Asymetrické využívá veřejného klíče a privátního. Veřejný klíč se používá k zašifrování dat, k jejichž rozšifrování je ale potřeba právě klíče privátního. Tento způsob přidá další dimenzi, proto je bezpečnější a využívá se častěji. Asymetrický způsob využívají například digitální nebo hardwarové peněženky.

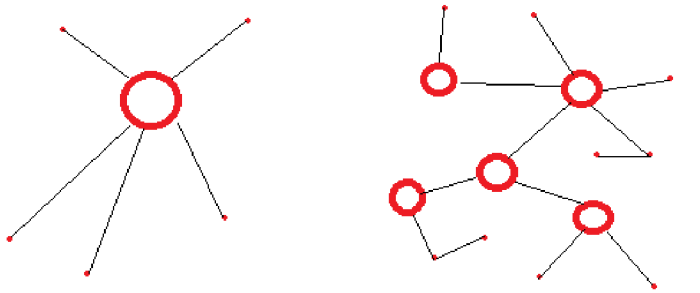
3.2. Decentralizace

Kontrola nad systémem je dána všem uživatelům místo jedné entity (například: firmy, jednotlivci, skupiny). Centralizovaným systémem jsou například banky, kde každá transakce jde přes prostředníka, jímž je právě banka. Tyto transakce se pak musí ověřit a ve výsledku to stojí dost času a energie. Oproti tomu v blockchain síti máme přehled o všech transakcích v reálném čase a ověřování nových se nahrazuje tzv. „těžením“, je to velmi rychlé a energeticky čím dál méně náročné. Zabraňuje to také korupci, jelikož zápisy dat jsou nevratné.

Novodobým příkladem je americká firma Contura Energy, která je dodavatelem uhlí. Jejich systém fungoval na základě platebních kreditů, které vydávala banka jako záruku platby pro kupce. Ačkoli tento systém je dost bezpečný, je ale pomalý a neefektivní, proto se rozhodli jít decentralizovanou cestou, která redukuje čas zprocesování až o polovinu. Chytré kontrakty obejdou původně potřebnou verifikaci člověka. Kvůli transparentnosti také obě strany ihned ví, jak na tom jsou. (Veramallu V., 2021)

Blockchain, má stejný účel jako databáze, slouží k uchování informací a dat. Liší se ale v důležitém bodu. Databázi totiž modifikuje a spravuje centrální entita. Transakce je převedení hodnot z jednoho účtu na druhý, a to oproti blockchainu, kde tuto akci může provést každý uživatel. Jak ale zajistit, že každý uživatel bude jednat čestně a pracovat jen s transakcemi, které může uskutečnit? Blockchain využívá mechanismus konsenzu. Ten vyžaduje souhlas všech účastníků, kteří se musí shodnout na jedné přidané, nebo změněné hodnotě v reálném čase. (STROUKAL D., SKALICKÝ J., 2018)

Obrázek 2 - Vizualizace rozdílu systémů



Zdroj: vlastní zpracování

3.3. Konsenzuální algoritmy

3.3.1. Proof of work (PoW)

Jelikož je blockchain decentralizovaný, bylo třeba vymyslet způsob, jak přidat do této sítě důvěru, která bude zajišťovat chod celku. První podobný mechanismus použil Bitcoin se svým „Proof of work“, který využívá tzv. těžení. Pro přidání nového bloku do řetězu se vyšle každému těžaři (počítač, který se těžení účastní) matematická operace, která je náročná na vypočtení, ale snadná na ověření. Svou odpověď řešitel vyšle k ověření, a pokud dojde více jak polovina počítačů ke stejnému výsledku, bude řešení uznáno a zapsáno do řetězu. Řešitel poté dostane odměnu. Tento způsob naráží na určité nedostatky, pokud by někdo získal nadpoloviční většinu, mohl by převzít kontrolu nad sítí a zkorumpovat ji. Bitcoin je ale natolik rozsáhlý, že dnes je to u něj téměř nemožné. Transakce v této síti nejsou instantní, jelikož toto ověřování je v rámci desítek minut. Toto dlouhé počítání také využívá obrovské množství energie, dnes je to v rámci setin procent světové spotřeby. (Nakamoto, S. 2008)

3.3.2. Proof of stake (PoS)

Modernější alternativa PoW, která je využívaná Ethereem. Oproti svému předchůdci je méně náročná na spotřebu energie. Místo vkládání peněz do hardwaru pro výpočet matematické operace investují uživatelé do sázek. Sázejí na to, že nějaký blok bude zapsaný do řetězu. Pokud mají pravdu, dostanou odměnu proporcionální k výši jejich sázky. Tato sázka slouží jako záloha, že validátor bude čestný a bude pracovat správně. Jeho slabinou je tzv. 51% útok, který může nastat, když nějaká entita ovládá více jak 50 % těžařů v síti, a

může tím měnit řetězec. Docílit tohoto by ale bylo opět velice náročné a drahé. (Ethereum, 2014)

3.3.3. Proof of elapsed Time (PoET)

Tento mechanismus zamezuje velké spotřebě energie, vytváří efektivnější systém loterie, kde se každý verifikovaný účastník může ucházet a má stejnou pravděpodobnost výběru. Poté je všem uzlům v síti vytvořen náhodný časový úsek, během něhož čekají. Ten uzel, který má nejkratší čas, vyhraje a vytvoří blok. Dále tento vyřešený blok zapíše do sítě. Na rozdíl od PoW to umožňuje uzlům v době čekání pracovat na něčem jiném, což zvyšuje efektivitu sítě. Oproti Proof of Stake není tento systém založený na soutěži, ale je náhodný. Využívá ho například Hyperledger Sawtooth pro podniky v oblasti dodavatelských řetězců. (Corso A., 2019)

3.3.4. Proof of capacity (PoC)

Využívá přebytečných kapacit na těžařských hardwarech. Vyhýbá se tím velké spotřebě energie, protože spolu uzly nemusí soutěžit. Místo opakovaného hashování, jako například v Proof of Work, se uloží list všech možných řešení na těžařské zařízení. A to ještě předtím, než začne samotné těžení. Čím větší je kapacita hard disku, tím více hodnot může být uloženo, to vede k více možnostem. (Debus J., 2017)

3.3.5. Proof of Activity (PoA)

Usiluje o kombinaci toho nejlepšího z Proof of Work a Proof of Stake. Těžařský proces začíná stejně jako v Proof of Work. Po nalezení nebo vytěžení nového bloku se pak změní v Proof of Stake. Nový blok obsahuje pouze header a adresu odměny těžaře. Poté se vytvoří nová skupina ověřovatelů, jejichž úkolem je zvalidovat tento blok. Čím více coinů tito uživatelé mají, tím větší je jejich pravděpodobnost výběru jako validátora. Když všichni účastníci podepíšou nový blok, dokončí ho a přidají do blockchainu. V případě, že někteří z účastníků nemohou blok podepsat a dokončit ho, je vytvořena nová skupina a proces se opakuje do té doby, dokud není naplněno potřebné číslo podepsání. Odměna je poté rozdělena mezi těžaře a validátory. Tento mechanismus využívá například Decred. (Debus J., 2017)

3.4. Kryptoměny

3.4.1. Bitcoin

Bitcoin položil otázku, zda-li je pro převody a držení peněz potřeba prostředníka, jímž je například banka. Do bank vkládáme svou důvěru a za tuto službu i platíme. Zakladatelé Bitcoinu chtěli vymyslet způsob, jak tyto procesy obejít. Vymysleli tedy důmyslný matematický systém, který právě toto má vyřešit. (Nakamoto S. 2008)

3.4.2. Čím je Bitcoin podložen

Jeho množství je omezené, a to na 21 milionů BTC. Nejde tedy vytvořit nové jako u jiných měn. Je to srovnatelné s drahými kovy, jako například zlato. Další výhodou ale je fakt, že je dělitelný na velmi malé části. Jeden Bitcoin jde rozdělit až na 100 milionů částí.

V dnešní době ještě stále nebyly vytěženy všechny Bitcoiny, nové se přidávají do oběhu pomocí těžení. Ze začátku se dalo vytěžit nejvíce, a to až přibližně 50 BTC. Tato odměna se ale stále zmenšuje kvůli tzv. Bitcoin halving a je tedy otázka, zda-li se těžařům tento proces vyplácí. Hodně z nich je názoru, že i když na tom dnes prodělají, cena BTC v budoucnu stoupne natolik, že v budoucnosti budou jejich výnosy převyšovat náklady. (CHOWDHURY N., 2019)

3.4.3. Bitcoin halving

Po každých 210 tisících blocích, které se vytěží, se odměna sníží o polovinu. Stalo se to například v roce 2020, kdy se odměna snížila z 12,5 Bitcoinů za blok na 6,25. Další takováto událost se čeká v roce 2024. Takto to bude pokračovat až do roku 2140, kdy se odměna změní na 0, další BTC už vytěžit nepůjdou a celkový počet bude omezený na 21 milionů BTC. Těžaři ale budou moci vydělávat na poplatcích za výpočty transakcí. (PRITZKER Yan, 2020)

3.4.4. Peněženky

Kryptoměnové peněženky mají podobný smysl jako ty, do kterých dáváme hotovost. Na rozdíl od normálních peněženek v sobě ale nemají žádnou hodnotu. Mají v sobě důkaz, že provedené platby na Blockchainu byly jejich. Peněženka projde historii veřejných transakcí a vyhodnotí, jaké množství měny v sobě obsahuje. Při odesílání kryptoměny někomu jinému podepíše transakci svým privátním klíčem. Pro příjem stačí jen transakci přijmout. Existují tři

typy kryptoměnových peněženek (Jokić, S., Cvetković, A.S., Adamović, S., Ristić, N. and Spalević, P., 2019):

- Softwarové peněženky jsou uložené v počítačích. Tuto možnost nabízejí nejvíce kryptoměnové burzy a pro přístup k peněžence u burz nám stačí přihlašovací údaje. Výhodou tedy je, že se o ně nemusíme starat. Existují také funkce, které umožňují platby skrz NFC v mobilu, snadnou správu, nákup a prodej kryptoměn. Nevýhodou je bezpečnostní riziko, spočívající v existenci prostředníka transakce. Pokud by byla burza napadena, můžeme kryptoměny ztratit.
- Hardwarové peněženky nabízí bezpečnější přístup. Dnes už to jsou velmi malá zařízení, která připojíme skrz USB konektor. V době psaní této práce je to nejpoužívanější druh peněženky. Podepsání transakce peněženkou funguje většinou automaticky, zamezuje se tak hackerskému útoku. Hackerský program by zaznamenával vše, co píšeme na klávesnici, a poté by měl přístup k našim privátním klíčům. Existují i jiné útoky, jedním příkladem je program, který při zkopírování adresy nějaké kryptoměnové peněženky vymění adresu za jinou, odkud si kryptoměnu vybere. Je tedy doporučené před transakcí zkontrolovat, jestli je adresa správně. Při posílání větších částek se doporučuje udělat testovací transakce s malou hodnotou.

  Velkou nevýhodou hardwarových peněženek je možná ztráta, a to jak fyzické peněženky, tak hesla k ní. Většina peněženek má obnovovací frázi nebo kombinaci slov. Při krádeži nebo ztrátě peněženky nám obnovovací fráze peněženku zpřístupní. Starší peněženky toto neumožňovaly, a než se tato technologie zpopularizovala, mnoho takových peněženek bylo také ztraceno. Některé zdroje odhadují, že až k 10 % Bitcoinů nebude už nikdy přístup. Jedním z předních výrobců hardwarových peněženek je česká firma SatoshiLabs.
- Papírové peněženky se dnes už téměř nepoužívají, mohou být lehko odcizené, poškozené, nebo ztracené. V podstatě jde o zapsání klíče na papír nebo jeho vyrytí do kovu.

3.4.5. Satoshi Nakamoto

Jedním z rizik investorů Bitcoinů zůstává záhada jeho tvůrce nebo tvůrců. Člověk nebo skupina vystupující pod pseudonymem Satoshi Nakamoto vlastní peněženku s přibližně 1,1 miliony BTC, což je přibližně 5 % všech Bitcoinů. Tato peněženka ale není už velmi dlouhou dobu aktivní a nikdo neví, kdo se pod tímto pseudonymem schovává. Kdyby se tvůrce nebo tvůrci rozhodli tyto Bitcoiny prodat, udělalo by to z nich jedny z nejbohatších lidí

na planetě. V době psaní této práce by se tato částka pohybovala kolem 18 miliard dolarů (1 BTC = 17 tisíc USD). Otázkou by také bylo, jaká burza by dokázala takovou částku uskutečnit a jaký cenový dopad by to mělo na ostatní držitele BTC. (Hayes A. 2023)

3.5. Ethereum

3.5.1. Chytré kontrakty

Chytré kontrakty rozšiřují základní programovací podmínky. V základu je to kus kódu, který zkontroluje počáteční stav transakce a poté ji i vyplní. Jako analogie se používá prodejní automat. Nejdříve je vybrán produkt, náš výběr poté spustí program, který vyžaduje peníze. V momentu, kdy jsou peníze vloženy, automat zkontroluje, jestli je částka dostatečná, a rozhodne o vydání produktu. V chytrých kontraktech má tento proces vysokou úroveň zabezpečení a také dobré šifrování. Identita zákazníka je chráněna, protože transakce ji nutně nevyžadují. Kontrakty ale mohou proběhnout, i když nejsou přímo vyvolány, jako například výplata zaměstnancům, kde kontrakt zkontroluje, jestli má zaměstnavatel dostatečnou sumu peněz na výplatu, a výběr peněz zaměstnancům umožní až od určitého data. (ANTONOPOULOS A. 2018)

3.5.2. Transparentnost

V dnešní době je ve světě mnoho takových programů, téměř všechny ale vyžadují účast nějakého prostředníka. Chytré kontrakty slouží jako tento prostředník, jsou ale transparentní a každý se může podívat, jak fungují a k čemu slouží. Navíc po jejich ukončení zapíše transakci do blockchainu, kde už nemůže být změněna a každý si ji může zobrazit. Tento způsob je velmi rychlý a nevyžaduje žádnou administraci. Chytré kontrakty přidávají také vyšší úroveň zabezpečení a mají efektivní šifrování. (Dannen C. 2017)

Tradiční kontrakty mají pravidla, která se dají vyložit více způsoby. V realitě je na tom postaven justiční systém. Dvě poroty u soudu by mohly dojít k různým rozsudkům. Chytré kontrakty mají přesný výsledek a ve dvou stejných případech dojdou ke stejnému výsledku.

Další výhodou je, že Ethereum je open-source. Mimo zápis v blockchainu si tedy můžeme zobrazit, jak funguje proces a co přesně dělají chytré kontrakty.

3.5.3. Důvěra

Můžeme si představit situaci, kdy s někým uzavřeme dohodu, nemáme ale jistotu, že po jejím uzavření druhá strana svůj závazek dodrží. Chytrý kontrakt zajistí, že druhá strana svůj závazek dodrží, jelikož nejdříve zjistí, zda-li druhá strana má dostatečné prostředky, a na konci dohody zajistí i vyplnění závazku. (Dannen C. 2017)

3.5.4. Spotřeba energie

Ethereum podobně jako ostatní kryptoměny získávají kritiku za vysokou spotřebu energie způsobenou těžením a ověřováním transakcí. Vývojáři Eterea již od začátku věděli, že PoW spotřebovává až moc energie, proto už od začátku pracovali na implementaci nového mechanismu a nechali souběžně s Proof of Work běžet jejich nedokončený Proof of Stake. V roce 2022 došlo k dlouho plánovanému spojení těchto dvou odvětví a velkému snížení spotřebované energie.

Pro představu celkových průměrných spotřeb můžeme využít následující tabulku:

Tabulka 1 - Porovnání spotřeby energie

firma	průměrná roční spotřeba energie v TWh	porovnání s PoS Ethereum
Youtube	244	94 000x více
Bitcoin	100	38 000x více
Netflix	94	36 000x více
Ethereum PoW	78	30 000x více
PayPal	0,26	100x více
Ethereum PoS	0,0026	1x (snížení o více než 99%)

Zdroj: Ethereum, W., 2014. https://ethereum.org/en/energy-consumption/

I po tak velké redukci spotřeby se vývojáři Ethereum snaží dále přibližovat k co nejmírnějším dopadům na životní prostředí. (Ethereum W., 2014)

3.5.5. Sharding

Sharding vznikl už v databázích, je to architektura rozdělení databáze na více míst, které nazýváme oddíly. Každý oddíl má stejné schéma, ale jiná data. Takovéto rozdělení snižuje zahlcení systému a výpočetní náročnost serveru. V budoucnosti budeme moci mít Ethereum klienty i v laptopech nebo mobilech, což zvýší bezpečnost, jelikož čím větší bude decentralizace, tím menší škodu může způsobit potencionální útok. Ethereum toto chce implementovat v roce 2023. (Dannen C. 2017)

3.5.6. Open source

Ethereum vyšlo společně s programovacím jazykem Solidity, který umožňuje programovat chytré kontrakty a přispívat k blockchain systému. Vydání tohoto vývojářského prostředí otevřelo dveře i novým kryptoměnám, dnes se tedy můžeme setkat s různými kryptoměnami založenými na Ethereu. (Dannen C. 2017)

3.6. Využití mimo kryptoměny

3.6.1. Logistika

I v dnešní době nastávají velké problémy se sledováním cesty produktu od výrobců k finálnímu bodu spotřeby. Převoz materiálu a výrobků má spoustu kroků. Musí se kontrolovat standardy, platit cla. Vyžaduje to tedy velké množství byrokratických procesů a přenosů informací, které by mohly být vyřešeny chytrými kontrakty. Také si můžeme představit situaci, kdy je maso rozvezeno do více obchodů, poté se ale zjistí, že je zkažené, nebo obsahuje zdraví nebezpečnou látku. Stáhnutí této potraviny je o dost pomalejší, než kdyby informace předání všem odběratelům byla veřejně přístupná a ošetřena chytrým kontraktem, který by všechny upozornil.

Podobný princip je aplikovatelný i na různá léčiva a léky. Léky na předpis bychom si tedy mohli vybrat všude na světě, protože by existoval chytrý kontrakt, který ověří, zdali na něj má kupující nárok. (Veramallu V., 2021)

3.6.2. dApps

Decentralizované aplikace fungují na blockchain síti místo jednoho centrálního serveru. Je to stejný princip jako s měnou, uživatelé nechtějí, aby jejich aplikace byla spravována jednou entitou, která nad ní má plnou moc. V dnešní době je to velmi aktuální a diskutovaná záležitost. Můžeme si vzít jako příklad firmu sociální sítě Twitter. Ten se rozhodl cenzurovat určité účty, například i účet bývalého prezidenta USA. Ať už to byla správná nebo špatná volba, decentralizované aplikace se snaží podobným věcem zabránit. Jedním z průkopníků těchto aplikací je dnes dokonce právě i jeden ze zakladatelů Twitteru.

Centrálně spravované aplikace mohou být napadeny hackerskými útoky. Velmi často se na internetu setkáváme se zprávami o úniku informací. Další výhodou je tedy ochrana

osobních údajů, jelikož nemusíme předkládat informace navíc a o správu a předání se postarají chytré kontrakty. (Dannen C. 2017)

Tento koncept je ale stále ještě nový. Aby uspěl, musí se vyřešit hned několik problémů. Vývojáři se bojí, že jakmile se aplikace jednou zhotoví a vypustí, bude pak těžko modifikovatelná. Problém může také nastat v momentě, kdy aplikace získá na takové popularitě, že blockchain síť nebude mít dostatek výpočetní síly. Tato síť totiž závisí na počtů uzlů a jejich výpočetní síle. V centrálně spravované aplikaci by se výpočetní síla dala navýšit lépe.

3.6.3. Web 3.0

Web 3.0 je další iterací „world wide webu“, na které se dnes pracuje. Je to jeden z příkladů dApps. Jeho vlastnosti ještě nejsou pevně dané, předpokládá se ale, že by byl decentralizovaný. Jejich uživatelé by jednali a obchodovali přímo mezi sebou bez nutnosti nějakého prostředníka. Každý by mohl přispívat k vývoji a nabízet služby. Obsahoval by také prostor pro umělou inteligenci, která by pomocí strojového učení optimalizovala přesnost a rychlost výsledků pro uživatele. (Dannen C. 2017)

3.6.4. Virtuální realita a hry

Klíčová změna by byla založená na principu Zero knowledge proof. Je to proces, který se snaží obejít předání důležitých informací. Místo toho se snaží dokázat, že uživatel tyto informace doopravdy vlastní.

Hry se dají rozdělit podle rozsahu informací, a to jestli hráči mají plnou informaci o dění, nebo ne. Příkladem hry s plnou informací jsou například šachy. Každý hráč má veškerou informaci o dění na šachovnici. Hrou s neúplnou informací jsou například Lodě, kde jeden hráč má informace pouze o poloze svých lodí. O rozložení protivníka ale informaci nemá. V dnešní době by informace obou hráčů zpracoval server, který nám informaci o protivníkově poloze pošle, a až herní program nám je zatají. V blockchain hře založené na Zero knowledge proof bychom server nepotřebovali a ani neobdrželi protivníkovy důležité informace. O předání informací by se postaraly chytré kontrakty, které proběhnou až v momentech, kdy by k předání muselo dojít. Když tento princip rozvineme, můžeme dostat jak herní, tak virtuální svět, který by nikdy neskončil.

Můžeme si představit situaci, kdy si chceme ve virtuálním světě něco koupit. Systém musí tedy rozhodnout, jestli máme dostatek peněz. Důležité ale je, že systém nemusí vědět

identitu člověka, který chce transakci uskutečnit, a kolik má peněz na účtu. Jako analogii můžeme použít tunel, který má uprostřed dveře. Tyto dveře k otevření vyžadují kód. Abychom někoho přesvědčili, že kód doopravdy máme, musíme tunelem projít. Jen takto dokážeme někoho přesvědčit, že máme správný kód. Velkou výhodou tedy je, že ve virtuálním světě by byla naše osobní data zabezpečena.

3.6.5. Zdravotnictví

Jedno z nejrozsáhlejších využití technologie blockchain můžeme nalézt v oblasti zdravotnictví. Jedním z příkladů je ukládání a předávání dat pacientů. Díky tomuto způsobu mohou pacienti mít větší kontrolu nad svými daty a zároveň tím snižují riziko manipulace těchto dat. Tímto způsobem uložení si mohou i lékaři předávat informace skrz chytré kontrakty.

Dalším příkladem je sledování dodavatelského řetězce léků. Lepší sledování umožňuje pacientům obranu před padělanými, popřípadě zdraví nebezpečným lékům.

Blockchain může zlepšit sledování epidemie, popřípadě pandemie. Nezávislé instituce a státní statistické úřady mohou lépe kontrolovat průběh a rychleji reagovat na změny. (Bamakan, S.M.H., Motavali, A. and Bondarti, A.B., 2020.)

3.6.6. E-government

Blockchain nabízí perspektivní budoucnost elektronického volebního systému. Z jeho charakteristiky vyplývá transparentní sčítání hlasů, protekce identity občana a krok blíže k zamezení manipulace s hlasy. (Lykidis, I., Drosatos, G. and Rantos, K., 2021)

3.6.7. NFT („Non-fungible token“)

Je to důkaz o vlastnictví, použitelný například v umění, nebo nemovitostech. „Non-fungible“ popisuje věc, která je nezaměnitelná a její hodnota je spíše v její unikátnosti. Z toho vyplývá, že oproti ostatním tokenům je tento unikátní, nedělitelný a je nemožné ho padělat. Lze ale převádět vlastníka tohoto tokenu. Tyto tokeny jsou prodávány na internetových trzích. Je to velmi dobrá možnost pro začínající umělce, kteří zde mohou svá díla prodat. Také by to mohlo usnadnit a zpřehlednit pronajímání autorských práv. (Wang Q., Li R., Wang Q., Chen S., 2021)

Dobře vytvořené NFT by mělo mít následující vlastnosti:

- Ověřitelnost – zjištění existence a vlastníka tokenu by mělo být snadné.

- Transparentnost – transakce a obchody mají být vždy možné a viditelné.
- Dostupnost – systém NFT bude vždy umožňovat obchody.
- Odolnost – historie transakcí a vlastníka by neměla být zmanipulovatelná.

3.6.7.1. Možnosti

Tabulka 2 - Oblasti využití NFT

Herní průmysl	Zatím nejvyvinutější oblast, už dnes existují hry založené na vytváření a používání různých kosmetik nebo zvířat. Uživatelé vytváří majetek, který mohou prodat nebo používat. Tento systém podporuje přirozený ekosystém hry, který přináší výhody jak vývojářům, tak hráčům.
Zábavní průmysl	NFT mohou nahradit tradiční lístky svou digitální podobou. V dnešní době vkládáme důvěru třetí straně. Objevuje se mnoho případů, kdy lidé přeprodávají lístky dalším, a dokonce je okrádají, když stejnou kopii pošlou více lidem. NFT nastolují větší úroveň bezpečnosti, lístky nemohou být kopírovány. Bezpečný přeprodej zajistí chytré kontrakty.
Sběratelské předměty	Charakteristika NFT přímo vystihuje možnost vlastnictví. Předkládá důkaz vlastnictví digitálního předmětu. Už dnes se můžeme setkat s digitálními trhy prodávajícími umění nebo známky. Jedním z příkladů je například portál „opensea.io“. V dnešní době musí začínající umělci promovat své produkty na webech třetí strany a často i musí zaplatit poplatek jen za vystavení. Přes NFT trh tedy snižují náklady. Tradičně by prodejem jejich díla výdělek často skončil. NFT ale mohou být naprogramována tak, aby při prodeji nebo pronájmu dostávali licenční poplatek.
Metaverse	Metaverse je virtuální prostředí se sdíleným prostorem pro uživatele, i když je zatím na počátcích svého dění, už dnes si můžeme představit, jaký přínos by měl blockchain a NFT. Blockchain přináší decentralizaci tohoto světa a NFT vytváří systém unikátních předmětů, které se v tomto prostoru můžou vyměňovat a prodávat.

Pro úspěšnou adopci NFT se musí vyřešit následující problémy:

3.6.7.2. Zpracování

Z pohledu využitelnosti nacházíme hned několik problémů. Jeden z nich je pomalé zpracování. Prodej a nákup NFT je úzce spjatý s kryptoměnovou platformou na které je vytvořený, jelikož to je další transakce na blockchainu. Vyřešení tohoto problému vyžaduje přeměnu systému a jeho optimalizaci. (Wang, Q., Li, R., Wang, Q. and Chen, S., 2021)

3.6.7.3. Vysoké ceny validace

V blockchainu existuje takzvaný „gas“, je to poplatek placený validátorům transakce za jejich služby. Zveřejňování a prodej NFT způsobí nahrávání dat do blockchain sítě. NFT transakce jsou dražší než normální, protože spotřebují více výkonu. Ceny takového zpracování mohou být v řádech stovek korun. V průběhu psaní je průměrná cena „gas“ 15.94 dolarů. Cena se každým rokem snižuje. Oproti minulému roku to je velmi významný rozdíl, až o 86 % (119 dolarů). (Wang, Q., Li, R., Wang, Q. and Chen, S., 2021)

3.6.7.4. Vztah ke státům

Typicky se můžeme setkat se dvěma hlavními problémy - legalitou a daněním. Jelikož je tato technologie nová, není moc zákonů upravujících její procesy do hloubky. Státy dnes musí používat již vyšlé zákony, které mohou být nejasné ve vztahu vůči digitálnímu majetku. Některé státy se snaží vytvořit vhodnější zákony, zatímco například Čína nebo Indie se rozhodly NFT co nejvíce omezit.

Prodeje tradičního umění nebo pozemků jsou velmi dobře ošetřeny z hlediska daní. Státy ještě ale nemají dostatečné podklady pro danění virtuálního majetku. Většina NFT jsou postaveny na neúplné anonymitě. Pokud uživatel nespojil svou peněženku se svou identitou, nelze ho nést odpovědným vůči danění, pokud ale svou identitu jednou odkryje nebo odkryl, lze zpětně nalézt celou historii jeho provedených nezdaněných transakcí.
(Wang, Q., Li, R., Wang, Q. and Chen, S., 2021)

4. Vlastní práce

4.1. Vícekriteriální rozhodování

Při rozhodování podle jednoho kritéria je komplexita snadno řešitelná a intuitivní, pokud se bude rozhodovat o stejném produktu na základě jeho ceny, bude preferována cena nižší. Můžeme si ale představit, že když do úlohy vstoupí další kritéria, toto rozhodnutí už nebude jednoduché a nelze zaručit, že bylo správné, a to kvůli rostoucí komplexitě při kombinování kritérií. V tento moment do procesu přijde vícekriteriální rozhodování, právě ono umožní zvážit a porovnat různá kritéria vůči vytčenému cíli. Výsledkem rozhodování je tedy nalezení vhodné varianty a seřazení alternativ. V praktické části této práce je zprvu definován problém, vytvořím přehled alternativ a poté jsou shrnuta kritéria, podle kterých jsou porovnáva. Následně je použita analytická hiearchická metoda a jsou okomentovány výsledky. Přestože tato metoda používá subjektivní hodnocení preferencí kritérií, bude snahou se co nejvíce přiblížit objektivnímu postupu za pomoci studií o kritických faktorech v oblasti zdravotnictví. (Ramík J. 1999)

4.1.1. Varianta

Jsou to konkrétní možnosti o kterých rozhodujeme, pokud je před nás postaven nějaký problém. Pokud možnosti nejsou již předurčené, musí se provést analýza dostupných variant, které budou vstupovat do rozhodovacího procesu. Jedním z procesů před vstupem do AHP je porovnání těchto variant pomocí bodového hodnocení. Je to částečně kvůli kontrole, zda-li nedochází k tzv. Dominanci variant. V případě, že jedna varianta dominuje nad jednou nebo více variantami, lze zjednodušit celý proces tím, že je před vstupem odstraněna. Jako příklad je možné si představit výběr mobilu, který si chceme koupit. Je-li v našem příkladu mobil A lepší nebo stejný ve všech kritériích (delší výdrž baterie, lepší rozlišení, menší cena) než mobil B, není třeba o druhém mobilu vůbec uvažovat, jelikož vždy bude preferován mobil A před B. (Ramík J. 1999)

4.1.2. Kritéria

Jsou faktory, podle kterých se vybrané varianty posuzují. Jsou úzce spjaté s cílem našeho rozhodování. Pokud se rozhoduje o mobilu s nejlepším fotoaparátem, nebude bráno v

potaz kritérium jako operační systém. Kritéria se dělí na dva typy.

Prvním je kvantitativní kritérium, neboli číselné. Jsou to objektivní metriky, jako například délka výdrže baterie nebo cena.

Druhým je kvalitativní kritérium, to mohou tvořit dotazníky, které obsahují slovní odpovědi jako například: "Operační systém mobilu mi přijde spíše srozumitelný." Před vstupem do rozhodování, se musí kvantifikovat dle bodovací stupnice.

Dále se kritéria dají rozlišit na minimalizační a maximalizační. Je to důležité rozlišit, jelikož při porovnávání kritéria, jako výdrž mobilu a jeho cena, bude u ceny preferováno číslo nižší a u výdrže čas delší. Je tedy třeba převést data na stejnou bodovou stupnici.
(Ramík J. 1999)

4.1.3. Metody stanovení vah kritérií

Váhy kritérií určují jejich důležitost, tyto váhy jsou opět úzce spjaté s řešeným problémem. Když bude znovu použita analogie mobilů, v případě, že se jedná o nákup zařízení, a v jednom rozhodovacím procesu je rozhodovatel omezen finačními prostředky, bude váha kritéria větší, než kdyby peníze problémem nebyly, a jde hlavně o nejlepší mobil na trhu. Váhy tedy určují důležitost jednotlivých kritérií. Jsou rozlišeny hodnotami mezi číslicemi 0 a 1. Čím větší je důležitost kritéria, tím větší číslo bude mít. (Ramík J. 1999)

První metodou, která stojí za zmínku, bude metoda bodovací. Jednotlivá kritéria se posuzují podle číselné stupnice. Při rozhodování je přiřazena ke každému kritériu číselná hodnota. Čím větší hodnota bude, tím větší bude mít důležitost. Touto metodou budou porovnány dominované varianty. (Ramík J. 1999)

Druhou metodou je Saatyho metoda. Využívá párového porovnání kritérií. Místo porovnání všech najednou se porovná každé kritérium po dvojicích, tímto se problém rozdělí na menší problémy. Při mnoha kritériích je těžké rozhodnout, jak je navzájem ohodnotit, když jsou ale porovnána vždy dvě kritéria mezi sebou, je často snažší srovnat, jestli jedno nebo druhé je důležitější, případně stejné důležité. Nevýhodou je, že s každým přidaným kritériem vysoce narůstá počet komparací, které musíme provést. (Ramík J. 1999)

Porovnání probíhá ohodnocením kritérií celými čísly 1,3,5,7,9 následovně:
(lze používat i mezistupně 2,4,6,8)

1 – rovnocenná kritéria *i* a *j*

3 – *i* je slabě preferované oproti *j*

5 – *i* je silně preferované oproti *j*

7 – *i* je velmi silně preferované oproti *j*

9 – *i* je absolutně preferované oproti *j*

Tato porovnání se uspořádají do matice. Na diagonále vzniknou jedničky, jelikož stejná kritéria mají stejnou preferenci. Pod diagonálou vznikne logický opak, znamená to, že pokud bylo *i* slabě preferováno (3) před *j*, bude *j* před *i* preferováno opačně (1/3). Saatyho matice má tuto obecnou podobu (Ramík J. 1999):

$$S = \begin{pmatrix} 1 & \cdots & s_{1n} \\ \vdots & \ddots & \vdots \\ \frac{1}{s_{n1}} & \cdots & 1 \end{pmatrix}$$

Následně je třeba spočítat váhy hodnoty b_i, které se počítají pomocí normalizovaného geometrického průměru řádků této matice následovně (Ramík J. 1999):

$$v_i = \frac{b_i}{\sum_{i=1}^{n} b_i}$$

váhy se poté vypočítají podle vzorce normalizací hodnot b_i

$$bi = \sqrt[n]{\prod_{j=1}^{n} Sij}$$

4.1.4. Konzistence rozhodování

Proces rozhodování vyžaduje vysokou konzistenci, znamená to, že když existují tři objekty rozhodování (například typ mobilu, který bude vybírán). U telefonu A se určí, že je dvakrát lepší než telefon B, poté se o telefonu B řekne, že je třikrát lepší než telefon C. Z konzistence vyplývá, že telefon A by měl být šestkrát lepší než C. V matematice je toto pravidlo nazváno tranzitivitou. Je třeba brát ohled na to, že lidská mysl není nutně konzistentní. Kdyby před nás někdo postavil telefony A a C, mohli bychom jim dát menší, nebo větší váhu, než při párovém porovnání. Konzistenci je třeba zkontrolovat před výpočtem metodou AHP. (Ramík J. 1999)
Index konzistence se označuje jako CI a spočítá se následovně :

$$\mathrm{CI} = \frac{\lambda \max - \mathrm{m}}{\mathrm{m} - 1}$$

λ_{max} - je zde maximální vlastní číslo matice

n - označuje počet kritérií/variant, které tvoří čtvercovou matici.

Aby rozhodování bylo konzistentní, musí být CI <0,1.

4.1.5. Metoda AHP

Analytický hiearchický proces, vytvořený Thomasem L. Saatym, rozděluje problém na menší části. Tyto části poté párově porovná a přiřadí jim číselné hodnoty podle předurčené škály. Po přiřazení čísla každé části je zvolena ta s nejvyšší prioritou. Na ni bude kladen důraz v rozhodovacím procesu. Tento proces se opakuje jak pro porovnání kritérií, tak pro varianty. Na závěr se vynásobí dílčí váhy variant s váhou kritérií. Výsledkem je syntéza preferencí, u které se určí pořadí variant. (Mu E., Pereyra-Rojas M. 2017)

4.2. Komparace vybraných vývojářských nástrojů pro zdravotnický systém.

Tato kapitola se věnuje samotné komparaci blockchainů. Jejím cílem je zvolit nejlepší variantu vývojářského nástroje pomocí metody AHP.

Jako první bude představen profil fiktivního rozhodovatele. Dále bude sestaven výčet variant a poté kritérií. Následně budou porovnány skrz metodu AHP a zformulovány výsledky, případně vhodné alternativy.

Před zpracováním praktické části bylo nutno položit otázku: Vůči jakému sektoru budou tyto platformy porovnávány? Jako příklad bylo vybráno právě zdravotnictví, jelikož zde blockchain poskytuje jedno z nejrozsáhlejších využití. Obsahuje v sobě také částečné využití ostatních sektorů, jako například dodavatelský řetězec, který ve zdravotnictví dokáže sledovat přesun a prodej léků ve velmi komplexním měřítku.

Další využitím je klinické hodnocení léků, kterému nahrává možnost anonymního testování, nebo transparentních a těžko zpochybnitelných výsledků.

Zdravotnické systémy zacházejí s citlivými dokumenty o svých pacientech, tyto dokumenty jsou uložené v centralizovaném systému. Toto může vést k bezpečnostnímu riziku, kdy hackerské skupiny napadnou tyto systémy a požadují peněžní výkupné za předání systému zpět. Tyto reference nebudou brány v potaz v tomto šetření, cílem je pouze poukázat na počet výskytu v médiích. (Hackerským útokům čelily v Česku nemocnice, Národní knihovna či volební web - Novinky. [online]. Copyright © 2003. Dostupné z: https://www.novinky.cz/clanek/internet-a-pc-bezpecnost-hackerskym-utokum-celily-v-cesku-nemocnice-narodni-knihovna-ci-volebni-web-40394428).

Dále se mohou objevit případy, kdy se turista vyskytne v cizí zemi a tamní lékaři budou potřebovat důležité informace o jeho zdraví, alergiích atd. V tuto chvíli by blockchainové sítě byly velmi využitelné, protože chytré kontrakty by tyto informace předaly. Z tohoto důvodu budou uvažovány pouze varianty blockchainů, které toto umožní (vlastnost jménem interoperabilita).

Při tomto využití je vhodno zmínit Estonsko, které za pomocí blockchainu úspěšně digitalizovalo většinu svého zdravotnického systému. Občané mají chytré karty, jejichž prostřednictvím si mohou prohlédnout vládní portály a informace o svých zdravotních záznamech.

"*Používáme blockchain jako další vrstvu bezpečnosti, která nám pomáhá k zajištění integrity zdravotních záznamů. Soukromí a integrita zdravotních informací jsou nejvyšší prioritou pro vládu. Rádi pracujeme s inovativními technologiemi, jako je blockchain, k zajištění bezpečnosti našich záznamů*." (vlastní překlad) – Artur Novek, architekt zdravotních systémů

(Blockchain and healthcare: the Estonian experience - e-Estonia. e-Estonia - We have built a digital society & we can show you how [online].
Dostupné z: https://e-estonia.com/blockchain-healthcare-estonian-experience)

4.3. Profil potencionálního rozhodovatele

V rámci legislativy o digitalizaci státu dostaly státní orgány za úkol vybrat nejlepší variantu a doporučení pro postavení blockchainového systému státu, které budou nemocnice a dodavatelé následně implementovat. Je tedy důležité zvolit jen ty blockchainové systémy, které umožňují komunikaci s ostatními platformami, prostřednictvím výše zmíněných vlastností. Důležitá potencionální rozhodnutí mohou zahrnovat určení kritických faktorů úspěchu, vytvoření standardů a bezpečnostních doporučení, dodržování předpisů a přehled financování.

4.4. Vývojová prostředí a jejich platformy

Vývojová prostředí slouží k vytváření, testování a nasazení aplikací na blockchain. Umožňují snažší přístup k vytváření aplikací v decentralizované struktuře, zatímco poskytují vysokou úroveň bezpečnosti. Lze se setkat, s případem, kdy jedno vývojové prostředí je možné aplikovat na více různých blokchainů. V následujícím rozhodování budou přiřazeny platformám jejich nejpopulárnější nástroje.

4.4.1. Varianty

Popis variant je rozdělen na dvě části, které jsou poté zohledněny ve výběru. První část se soustředí na platformu, kterou nabízí, a druhá na programovací jazyk potřebný pro její implementaci.

4.4.1.1. V1 - Bitcoin

Obecnému smyslu Bitcoinu byla věnována kapitola v teoretické části této práce. Klíčovou výhodou Bitcoinu v oblasti zdravotnictví je jeho úroveň adopce. Je to nejpopulárnější kryptoměna a je v ni kladená největší důvěra. Spolehlivý a rychlý přenos peněz má ve zdravotnictví velký vliv.

Programovacím jazykem je Clarity. Vývojáři Clarity si vzali poučení z chyb jeho alternativ a soustředí se na bezpečnost a snadnost. Jako jeden z příkladů uvedených v dokumentaci se představuje ošetření problému, který se nazývá Parity bug. Právě ten vedl ke ztrátě milionů dolarů Etherea. Tento jazyk se nekompiluje, ale interpretuje. Znamená to, že kód se zapisuje rovnou do řetězu, přesně tak, jak je napsán. Je to z toho důvodu, že kompilování přidává vrstvu komplexity, ve které se může vyskytnou bezpečnostní chyba. Druhým důvodem je, že zkompilovaný jazyk může být těžší na pochopení, zatímco kód, který vypadá tak, jak se spouští, je jednodušší. Další vlastností je vždy přesně daný počet kroků, ve kterém proběhne, což zamezí problémům s nedostatečným financováním transakce.
(Clarity overview, 2023)

4.4.1.2. V2 - Ethereum

Ethereum patří mezi již využívané blockchainy, nabízí tím tedy větší úroveň adopce. Můžeme se setkat s firmami, které pomocí Etherea tvoří blockchainová řešení v oblasti zdravotnictví.

Programovacím jazykem je Solidity. Je to staticky psaný programovací jazyk zaměřený na chytré kontrakty, a přestože se převážně využívá pro Etehreum, může se aplikovat i na tvorbu u jiných blockchainů. Jedná se o vysokoúrovňový programovací jazyk, což znamená, že se vzdaluje strojovému kódu. Pro programátory by tedy měl být snažší na čitelnost a s pomocí pár řádků dokáže zahrnout více nižších strojových operací. Byl vytvořen jedním ze zakladatelů Eteherea (Gavin Wood), je ovlivněný jazyky jako C++, Python a Javascript. (Solidity 0.8.19 documentation)

4.4.1.3. V3 - Hyperledger Fabric

Hyperledger Fabric je open-source platforma určená pro podnikové aplikace postavené na blockchainu. Jeho výhodou je míra úpravy, kterou lze našemu systému poskytnout, a dá se v mnoha oblastech upravit. Poskytuje velkou míru bezpečí při přístupu k citlivým informacím pacientů, a to kvůli propracovanému systému práv. Je to tedy "permissioned" blockchain, což znamená, že pro přístup vyžaduje povolení. Používá šifrovanou a decentralizovanou architekturu, která přispívá k obraně proti hackerským útokům. Poskytuje relativně velkou míru adopce, velké řetězce jako Walmart, nebo IBM využivají tohoto blockchainu. Jejich komunita v této oblasti spolupracuje, pořádá virtuální setkání a globální forum, na které se mohou firmy připojit a kolaborovat na projektech. (Hyperledger foundation, 2022)

Programovacím jazykem je Golang. Podobně jako Solidity je to staticky psaný vysokoúrovňový programovací jazyk. Vytvořený je v Googlu autory Robertem Griesemerem, Robem Pikem a Kenem Thompsonem. Má podobnou syntaxi jazyku C, což znamená, že jeho pravidla zápisu, jako například kombinace využitelných symbolů a slov, jsou si podobná. Golang je primární jazyk na implementaci na Hyperledger Fabric blockchainu. (Effective Go)

4.4.1.4. V4 - R3 Corda

Podobně jako Hyperledger Fabric vyžaduje povolení k přístupu. Je určena pro soukromý sektor, ve kterém je tato vlastnost kritická. V "permissionelss" blockchainu, nevíme, kdo vlastní uzel, což v institucích způsobí problémy. Oproti jiným platformám se liší v architekuře. Je založena na uzlech, protože každý uzel v síti má jiný pohled na data v síti. V případě nějaké transakce je vztažena pouze na ty, které v ní byly přímo zapojeny, a tím vytváří další úroveň bezpečí. Je open-source s aktivní komunitou.

Programovacím jazykem je Kotlin. Ten je ovlivněný jazyky jako Java, nebo C# a snaží se co nejvíce přizpůsobit uživatelům při jejich denní práci. Designová rozhodnutí vývojářů jsou založena právě na uživatelích. Kotlin se stále vylepšuje, což může způsobit chybu mezi vydáními. (Kotlin Docs)

4.4.1.5. V5 – Ripple

Ripple také vyžaduje oprávnění pro přístup, byl založený v roce 2012 pro podniky. Jeho primární funkcí je zpracování plateb, je podobný bankovnímu systému SWIFT. Velkou výhodou je tedy rychlost převodu a zpracování transakcí za minimálních transakčních

poplatků. V oblastní zdravotnictví může poskytovat dobrou obranu před zneužíváním prodeje léků. Dokumentace Ripplu uvádí jako příklad decentralizovaný trh ScriptCo, který prodává léky za snížené ceny kvůli redukci prostředníků. (XRP Healtchare)

Jeho programovacím jazykem je C++. Oproti ostatním jazykům má vysokou úroveň adopce, byl vytvořen v roce 1985 a prošel již nespočetně vylepšeními. Díky tomu má velmi optimalizovaný průběh kompilování, přívětivé prostředí pro vývojáře a bohaté materiály pro začátečníky.

4.4.2. Kritéria

Jako relativně mladá technologie nemá blockchain pevně určená a změřená kritéria pro porovnání, jeden z hlavních zdrojů, jimž se lze inspirovat, je vědecký článek, který navrhuje právě rámec kritérií na všeobecné porovnání. (Z. Moezkarimi, F. Abdollahei and A. Arabsorkhi, 2019)

Kritéria budou také z části vybírána ze studií o kritických faktorech při implementaci blockchainu ve zdravotnictví. Jedna z těchto studií zvolila různá kritéria a předložila je na zhodnocení expertům z oboru, kteří následně hodnotili jejich důležitost. Mezi položená kritéria patřily i netechnické faktory, jako například podpora řízení nebo vedoucí projektu. Tato kritéria nebudou brána v úvahu, jelikož se zaměřuji především na technickou stránku blockchainu. Dále budou posuzovány vývojářské nástroje, jejich metriky, zapojení komunity a rozsah, kterým dokáží ovlivnit rozhodnutí dle zmíněného profilu. (Bali, S., Bali, V., Mohanty, R.P. and Gaur, D. 2022)

4.4.2.1. K 1 - Transparentnost

Trasparentnost dat jako taková vychází z podstaty blockchainu, zde bude zvažováno spíše to, jaký systém práv daný blockchain má. Pro zdravotnictví je potřeba mít rozdělené, kdo si může zobrazit jaká data. Externí instituce, popřípadě stát, může využít transparentních dat pro statistické výzkumy, přičemž mohou zachovat anonymitu jedinců. Nemocnice ovšem potřebuje mít přesné informace o každém pacientovi, popřípadě mít způsob předání těchto informací jiným nemocnicím, zatímco zachová anonymitu pacienta.

K 1.1 – Typ blockchainu

Typ blockchainu se rozděluje na “permissioned” a “permissionless”, kde bylo blockchainu bez povolení (“permissionless”) dáno nejmenší ohodnocení, zatímco pouze s

povolením dostalo ohodnocení větší. Vyjímkou bylo Ethereum, které nabízí obě možnosti, a dostává tedy nejlepší ohodnocení.

K 1.2 – Typ sítě

Toto dílčí kritérium rozděluje blockchainy na dvě části, veřejnou a privátní. Privátní zde dostala lepší ohodnocení, jelikož obsahuje více využití v oblasti zdravotnictví. Tento typ sítě má rozsáhlejší využití pro systém nemocnic a dodavatelského řetězce. Výhoda veřejného spočívá v lepším sledování statistických měření nezávislých institucí.

4.4.2.2. K 2 – Škálovatelnost

Vyjadřuje v jakém měřítku dokáže blockchain pracovat s transakcemi. Toto kritérium je relativně důležité, jelikož zdravotnické systémy vyžadují relativně rychlý průběh, a to i při velkém objemu dat.

K 2.1 Počet zpracovatelných transakcí

Vyjadřuje maximální počet transakcí, které může blockchain provést za sekundu. Ve srovnání s finančním sektorem většina blockchainových sítí zaostává. Bitcoin je velmi slabý, jeho počet zpracovatelných transakcí je 7. Vedle něj můžeme postavit jinou variantu jako R3 Corda, která má téměř dvěstěnásobek transakcí za sekundu. I R3 Corda ale zaostává za moderními finančními systémy, jako MasterCard, nebo Visa, které mají transakcí několikrát více. U blockchainu se vyskytuje problém jménem Blockchainové trilema, kdy z podstaty této technologie je možné dosáhnout dvou ze tří možností - bezpečnost, škálovatelnost a decentralizace. Zvýšením jedné možnosti ostatní dvě klesají.

K 2.2 Čas potvrzení transakce

Pro potvrzení transakce se musí vytvořit nový blok, tato vlastnost je úzce spjatá s mechanismem konsenzu, který byl zmíněn v teoretické části. Bitcoin zde opět zaostává, jelikož pro vytvoření nového bloku je třeba výpočtu náročné matematické úlohy. Ostatní varianty mají mnohem lepší časy. Je nutno podotknout, že transakce je platná ještě před potvrzením, problém nastává v tom, že si uživatelé mohou být jisti validitou své transakce až po potvrzení více uzly.

K 2.3 Mechanismus konsenzu

Jak bylo zmíněno v dílčím kritériu času potvrzení, mechanismus konsenzu je esenciální částí škálovatelnosti, jelikož diktuje, jakým způsobem jsou transakce zpracovávány. Objevují se stále nové alternativy tohoto mechanismu, vhodnější pro privátní instituce.

4.4.2.3. K 3 – Architektura

I přes svou výhodu nezpochybnitelného uložení dat jsou blockchainy vystaveny bezpečnostním chybám a útokům. Zde je třeba dbát na míru úrovně šifrování, možnosti nastavení práv, aktualizaci protokolů, počtu historických útoků.

K 3.1 – Bezpečnost

Jedna z vlastností blockchainu je schopnost permanentního uložení dat (immutability) do řetězce. Riziko bezpečnostní chyby ve smyslu tohoto dílčího kritéria představují převážně hrozby, které převezmou kontrolu nad sítí, prostřednictví ovládnutí většiny uzlů, popřípadě zahlcení sítě. Dosáhnutí tohoto je ale extrémně náročné a blockchainy jsou proti útokům dobře koncipovány. Je tedy třeba zmínit, že pokud zde nějaký blockchain má nižší ohodnocení, neznamená to nutně, že zranitelnost je veliká, pouze že je teoreticky realizovatelná.

K 3.2 – Interoperabilita

Vyjadřuje schopnost komunikace jednoho blockchainu s jiným. V případě pacienta v cizí zemi, která má ale jiný systém než jeho mateřská země, je schopnost komunikace esenciální pro rychlé předání informací.

4.4.2.4. K 4 – programovací jazyk

K 4.1 – skóre dokumentace

Skóre dokumentace je dílčí kritérium, které bylo ohodnoceno subjektivně po konzultaci s vrstevníky oboru a vlastního zhodnocení, vyjadřuje vlastnosti jako přehlednost, přístupnost a jednoduchost.

K 4.2 – počet vývojářů

Toto dílčí kritérium je vhodné zmínit, jelikož představuje přibližný rozsah aktualizací, komunikace s vývojáři a celkového rozsahu firmy.

K 4.3 – popularita

Zde byla brána v úvahu data jako počet sledujících na sociálních sítích, příspěvky na programovacích stránkách a také celková adopce.

4.5. Kroky výpočtu metodou AHP

4.5.1. Přehled vstupujících dat

Tato tabulka popisuje hodnoty dílčích kritérií, která byla získána pro toto rozhodování. Pro výpočet byl použit program Microsoft Excel.

Tabulka 3 - Dílčí kritéria

						jednotka
Blockchain	**Bitcoin**	**Ethereum**	**Hyperledger**	**R3Corda**	**Ripple**	
K1 - transparentnost						
K1.1 - typ blockchainu	-less	obojí	-ned	-ned	-ned	
K1.2 typ sítě	veřejná	veřejná	privátní	privátní	privátní	
K2 - škálovatelnost						
K2.1 - počet zpracovatelných transakcí	7	15	3500	1678	1500	transakcí/s
K2.2 - čas potvrzení transakce	600	15	4	4	4	sekund
K2.3 - mechanismus consensu	PoW	PoS	BFT	Notary	RPCA	
K3 - architektura						
K3.1 - bezpečnost	1	3	6	4	5	
K3.2 - interoperabilita	malá	velká	velká	střední	střední	
K4 - programovací jazyk	Clarity	Solidity	Golang	Kotlin	C++	
K4.1 - skóre dokumentace	6	8	7	10	8	
K4.2 - počet vývojářů	51-200	51-200	51-200	201-500	<500	pracovníků
K4.3 - popularita/adopce	<5984 k	<3277 k	<110 k	< 90 k	<2750 k	sledujících

Zdroje: vlastní zpracování, za použití následujících zdrojů a dohledání doplňujích informací z internetových zdrojů.

(Z. Moezkarimi, F. Abdollahei and A. Arabsorkhi, 2019)

(Bamakan, S.M.H., Motavali, A. and Bondarti, A.B., 2020.)

(Cornelius C. Agbo Qusay H. Mahmoud. 2019)

4.5.2. Tabulka bodového hodnocení dílčích kritérií

Následující tabulka zobrazuje převedení původních hodnot na stejnou bodovou stupnici. Systém přidělení bodového ohodnocení byl zmíněn v předchozí části. Jelikož se ale pracuje s dílčími kritérii, bylo nutno provést párové porovnání pro dílčí kritéria, které je zobrazeno v posledním sloupci váhy.Tabulka dílčích kritérií převedená na bodové ohodnocení

Tabulka 4 - Bodové hodnocení dílčích kritérií

	Bicoin	**Ethereum**	**Hypeledger F.**	**R3 Corda**	**Ripple**	**váhy**
K 1						
K 1.1	5	10	8	8	8	0,5
K 1.2	5	5	8	8	8	0,5
K 2						
K 2.1	1	2	10	5	5	0,45
K 2.2	1	8	10	10	10	0,45
K 2.3	4	6	8	10	8	0,09
K 3						
K 3.1	1	3	6	4	5	0,14
K 3.2	3	9	9	6	6	0,85
K 4						
K 4.1	6	8	7	10	8	0,45
K 4.2	4	4	4	6	8	0,9
K 4.3	10	5	1	1	4	0,45

4.5.3. Bodové hodnocení kritérií

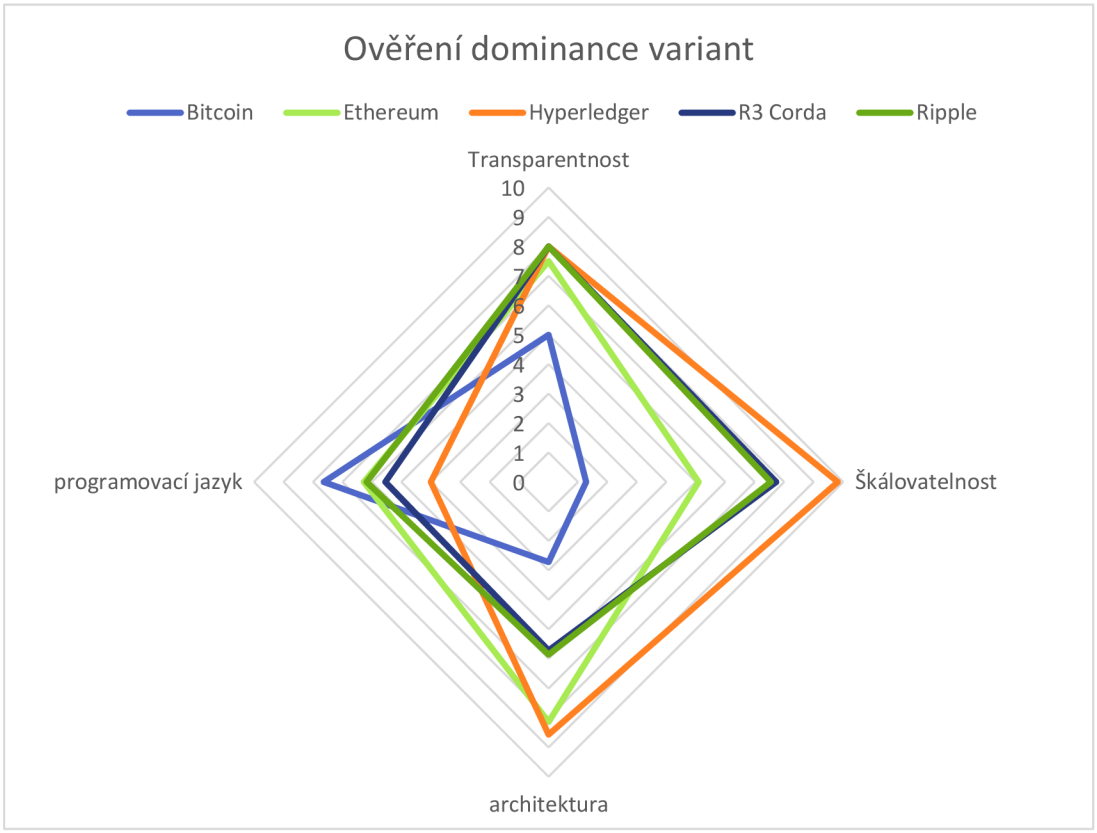
Následující tabulka zobrazuje ohodnocení kritérií dle váženého průmeru dílčích kritérií. Tato tabulka by už mohla vstoupit do metody AHP, nejdřív by ale bylo vhodné ověření dominance variant. Toto ověření porovná, zda-li je nějaká varianta lepší ve všech směrech než některá druhá. V případě, že by se toto potvrdilo, byla by slabší varianta vyřazena, jelikož tento fakt implikuje, že ať budou váhy jakékoliv, jedna varianta bude vždy lepší než druhá, zároveň by to také ulehčilo celý výpočet skrz metodu AHP.

Tabulka 5 - Bodové hodnocení kritérií

	Bicoin	**Ethereum**	**Hypeledger F.**	**R3 Corda**	**Ripple**
K 1	5	7,5	8	8	8
K 2	1,27	5,09	9,82	7,73	7,55
K 3	2,71	8,14	8,57	5,57	5,86
K 4	7,64	6,27	4	5,55	6,18

4.5.4. Ověření dominance variant

Ověření bylo nejprve provedeno pomocí grafického vyobrazení. Ze grafu lze vyčíst, že Ripple a Corda mají velmi podobné ohodnocení a Ripple by potencionálně mohl vyřadit R3 Cordu. Po kontrole s předchozí tabulkou bylo zjištěno, že R3 Corda má o trochu lepší ohodnocení ve škálovatelnosti. Do metody AHP tedy vstupují všechny varianty.



Graf 1 - ověření dominance variant

4.5.5. Párové porovnání kritérií

Následně bude přepočítáno bodové ohodnocení na párové porovnání kritérií dle výše zmíněné stupnice. Pro bližší vysvětlení lze vzít jako příklad kritérium 1 a kritérium 2. Z literálních zdrojů a studie o kritických faktorech úspěchu v oblasti zdravotnictví je možné soudit, že transparentnost dat je slabě až silně preferovaná před škálovatelností.

Tabulka 6 - Matice párového porovnání kritérií

	K 1	**K 2**	**K 3**	**K 4**
K 1	1	4	3	4
K 2	1/4	1	1/3	1
K 3	1/3	3	1	2
K 4	1/4	1	1/2	1

4.5.6. Stanovení vah kritérií

Po určení preferencí dle Saatyho stupnice je možné postoupit k dalšímu kroku, a to k spočítám geometrického průměru každého řádku jednotlivě. Následně lze spočítat váhu každého kritéria vůči ostatním. Tato váha poté bude porovnána s jednotlivými variantami v následujících krocích.

Tabulka 7 - Stanovení vah

	geometrický průměr	**váha kritéria**
K 1	2.632148	0.531398858
K 2	0.537285	0.108471338
K 3	1.189207	0.240086536
K 4	0.594604	0.120043268
celkem	4.953244	1

4.5.7. Párové porovnání variant pro první kritérium

Následující tabulka popisuje podobný proces jako v předchozích dvou tabulkách, je zde ale párově porovnáváno ohodnocení varianty v daném kritériu. Tato tabulka tedy zobrazuje porovnání v kritériu transparentnost.

Tabulka 8 - párové porovnání variant u prvního kritéria

	V1	V2	V 3	V 4	V5
V 1	1	1/5	1/7	1/7	1/7
V 2	5	1	1/3	1/3	1/3
V 3	7	3	1	1	1
V 4	7	3	1	1	1
V 5	7	3	1	1	1

Oproti předchozímu výpočtu u kritérií zde přibývá další sloupec. Tento sloupec násobí dílčí váhy vůči váze kritéria transparentnost.

4.5.8. Stanovení vah variant pro první kritérium

Tabulka 9 - hodnocení variant vůči prvnímu kritériu

	geometrický průměr	dílčí váhy	vážené dílčí váhy
V 1	0,2255	0,034937142	0,018565557
V 2	0,713709	0,110576146	0,058760038
V 3	1,838416	0,284828904	0,151357754
V 4	1,838416	0,284828904	0,151357754
V 5	1,838416	0,284828904	0,151357754
celkem	6,454458	1	0,380041104

4.5.9. Shrnutí jednotlivých výpočtů

Následné tabulky mají stejný průběh. Všechny kroky byly shrnuty do následujícího obrázku.

Obrázek 3 - Shrnutí výpočtů

	transpar	škálovatel	architekru	programovací jazyk	geo	váha	CI	0.02	lambda	4.06
transparentnost	1.00	4.00	3.00	4.00	2.632148	0.531399				
škálovatelnost	0.25	1.00	0.33	1.00	0.537285	0.108471				
architektura	0.33	3.00	1.00	2.00	1.189207	0.240087				
programovací jazyk	0.25	1.00	0.50	1.00	0.594604	0.120043				
					4.953244	1				

transparentnost												
	V1	V2	V3	V4	V5	geom. p.	dílčí váhy	vážené dílčí	CI	0.04	lambda	5.16
V1	1.00	0.20	0.14	0.14	0.14	0.2255	0.034937	0.018566				
V2	5.00	1.00	0.33	0.33	0.33	0.713709	0.110576	0.05876				
V3	7.00	3.00	1.00	1.00	1.00	1.838416	0.284829	0.151358				
V4	7.00	3.00	1.00	1.00	1.00	1.838416	0.284829	0.151358				
V5	7.00	3.00	1.00	1.00	1.00	1.838416	0.284829	0.151358				
						6.454458	1	0.380041				

škálovatelnost												
	V1	V2	V3	V4	V5	geom. p.	dílčí váhy	vážené dílčí	CI	0.04	lambda	5.16
V1	1.00	0.20	0.11	0.14	0.14	0.214446	0.030064	0.003261				
V2	5.00	1.00	0.20	0.33	0.33	0.644394	0.090339	0.009799				
V3	9.00	5.00	1.00	3.00	3.00	3.322699	0.465815	0.050528				
V4	7.00	3.00	0.33	1.00	1.00	1.475773	0.206891	0.022442				
V5	7.00	3.00	0.33	1.00	1.00	1.475773	0.206891	0.022442				
						7.133086	1	0.08603				

architektura												
	V1	V2	V3	V4	V5	geom. p.	dílčí váhy	vážené dílčí	CI	0.01	lambda	5.05
V1	1.00	0.20	0.20	0.33	0.33	0.338504	0.054367	0.013053				
V2	5.00	1.00	1.00	3.00	3.00	2.141127	0.343888	0.082563				
V3	5.00	1.00	1.00	3.00	3.00	2.141127	0.343888	0.082563				
V4	3.00	0.33	0.33	1.00	1.00	0.802742	0.128929	0.030954				
V5	3.00	0.33	0.33	1.00	1.00	0.802742	0.128929	0.030954				
						6.226242	1	0.209132				

programovací jazyk												
	V1	V2	V3	V4	V5	geom. p.	dílčí váhy	vážené dílčí	CI	0.05	lambda	5.21
V1	1.00	2.00	5.00	3.00	3.00	2.459509	0.425177	0.05104				
V2	0.50	1.00	3.00	2.00	1.00	1.245731	0.21535	0.025851				
V3	0.20	0.33	1.00	2.00	1.00	0.668325	0.115534	0.013869				
V4	0.33	0.50	0.50	1.00	1.00	0.608364	0.105168	0.012625				
V5	0.33	1.00	1.00	1.00	1.00	0.802742	0.13877	0.016658				
						5.784671	1	0.103385				

Zdroj: vlastní zpracování

V neposlední řadě je nutné zkontrolovat, zda-li rozhodování bylo konzistentní. Jelikož index konzistence vyšel u každé tabulky nižší než “0,1”, lze tato rozhodování považovat za konzistentní a přejít na další krok. Pokud by nějaký krok nebyl konzistentní, bylo by nutné danou tabulku přepočítat s lepšími hodnotami párového porovnání.

5. Výsledky a diskuse

Pro získání výsledků metody AHP byla spočítána suma vážených dílčích variant. Následně byly varianty ohodnoceny pořadovým číslem od největší syntézy preferencí po nejnižší. Výsledky a pořadí byly shrnuty do následující tabulky:

Tabulka 10 - Výsledná tabulka preferencí

varianta	syntéza preferencí	pořadí
Bitcoin	0.085919087	5.
Ethereum	0.176973347	4.
Hyperledger Fabric	0.298317183	1.
R3 Corda	0.217378338	3.
Ripple	0.221412046	2.

Metodou AHP bylo porovnáno pět blockchainových platforem a jazyků. Jako nejlepší varianta na vytvoření blockchainového systému v oblasti zdravotnictví vyšel se znatelným náskokem Hyperledger Fabric. Druhé místo náleží Ripplu, zatímco velmi malý kus za ním zaujímá R3 Corda. Čtvrté místo s větším rozdílem patří Ethereu. Jako poslední se umístil Bitcoin s velmi velkým odstupem od ostatních.

Pokud porovnáním výsledky s původní tabulkou je možné zjistit, že Hyperledger Fabric měl velmi dobré ohodnocení v prvních třech kritériích, zatímco měl nejhorší bodové ohodnocení v kritériu programovací jazyk. Z výsledků tedy lze usoudit, že pro postavení dobrého zdravotnického systému na platformě Hyperledger Fabric bude důležité investovat zdroje do vývojářů, kteří už mají zkušenosti s touto platformou, a zaručí tím úspěšné vybudování tohoto systému, protože Golang jako programovací jazyk není tak dobře adoptovaný jako jeho alternativy.

6. Závěr

Cílem této bakalářské práce bylo porovnání vývojářských nástrojů blockchainu.

V teoretické části byly popsány základní principy blockchainu a byl vytvořen přehled důležitých oblastí využití.

V praktické části byly představeny kroky vícekriteriálního rozhodování pomocí metody AHP. Následně byly charakterizovány varianty a kritéria, které do této metody vstoupily. Poté bylo krok po kroku popsáno rozhodování mezi jednotlivými variantami.

Jako nejvhodnější nástroj vychází Hyperledger Fabric. R3 Corda a Ripple byly jeho blízké alternativy výběru, které nabízí lepší programovací jazyky, a tedy i základy pro postavení alternativní varianty. Na předposledním místě figuruje Ethereum, které nabízí silnou míru škálovatelnosti. Poslední místo náleží Bitcoinu, nejpopulárnější platformě, která i přes silnou adopci nedosahuje takové úrovně využití ve zdravotnictví, jako jeho alternativy.

7. Seznam použitých zdrojů

7.1. Literální

ANTONOPOULOS, Andreas. Mastering Ethereum: Building Smart Contracts and DApps. Sebastopol, CA: O'Reilly Media, 2018. ISBN 1491971940.

Dannen, C. (2017). Introducing ethereum and solidity: Foundations of cryptocurrency and Blockchain Programming for Beginners. Apress. 2017. ISBN 978-1-4842-2534-9

Mu, E., Pereyra-Rojas, M. (2017). Practical decision making an introduction to the Analytic Hierarchy Process (Ahp) using Super Decisions V2. Springer International Publishing. ISB 978-3-319-33860-6

PRITZKER, Yan. Vynález jménem bitcoin. Přeložil Tereza WONGOVÁ. [Praha]: Braiins Publishing, 2020. ISBN 978-80-907975-0-5.

STROUKAL, D. -- SKALICKÝ, J. Bitcoin a jiné kryptopeníze budoucnosti : historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky. Praha: Grada Publishing, 2018. ISBN 978-80-271-0742-1.

7.2. Internetové

Al-Megren, S., Alsalamah, S., Altoaimy, L., Alsalamah, H., Soltanisehat, L. and Almutairi, E., 2018, July. Blockchain use cases in digital sectors: A review of the literature. In *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)* (pp. 1417-1424). IEEE.
Dostupné z: https://www.researchgate.net/profile/Shada-Alsalamah-2/publication/326785973_Blockchain_Use_Cases_in_Digital_Sectors_A_Review_of_the_Literature/links/5b636663458515298ce0c034/Blockchain-Use-Cases-in-Digital-Sectors-A-Review-of-the-Literature.pdf

Bamakan, S.M.H., Motavali, A. and Bondarti, A.B., 2020. A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications*, *154*, p.113385. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S0957417420302098?casa_token=v70eTmVqAlMAAAAA:ZtX4d_gRilP-Yy1RCpajvibrUXwwJZZBN8_UW5mt8F970r5bb_5vohhlJScfVSPtSrjQWcJhuZRQ

Bali, S., Bali, V., Mohanty, R.P. and Gaur, D. (2022), "Analysis of critical success factors for blockchain technology implementation in healthcare sector" Dostupné z: https://doi.org/10.1108/BIJ-07-2021-0433

Clarity Overview | Stacks Docs. Stacks Docs [online]. Copyright © 2023 Stacks Open Internet Foundation. Dostupné z: https://docs.stacks.co/docs/clarity/

Cornelius C. Agbo Qusay H. Mahmoud. Comparison of blockchain frameworks for healthcare applications, 2019 Dostupné z: https://onlinelibrary.wiley.com/doi/pdfdirect/10.1002/itl2.122?casa_token=3r-5Edp-72MAAAAA:T9W3nxgYpLCLmbIqY6IOtYDz2oY5mYm9OdQ8k_6_A96dqxfWbpn_ttGvyvruXu8Z349S5FtDUvcm44WOHg

Corso, A., 2019. *Performance analysis of proof-of-elapsed-time (poet) consensus in the sawtooth blockchain framework* (Doctoral dissertation, University of Oregon).
Dostupné z: https://www.cs.uoregon.edu/Reports/MS-201906-Corso.pdf

Debus, J., 2017. Consensus methods in blockchain systems. *Frankfurt School of Finance & Management, Blockchain Center, Tech. Rep*.
Dostupné z: http://explore-ip.com/2017_Consensus-Methods-in-Blockchain-Systems.pdf

Effective Go - The Go Programming Language. The Go Programming Language [online]. Dostupné z: https://go.dev/doc/effective_go

Ethereum, W., 2014. Ethereum Whitepaper. Ethereum.
Dostupné z: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

Hayes, A. (2023, January 3). Who is satoshi nakamoto? Investopedia, Dostupné z: https://www.investopedia.com/terms/s/satoshi-nakamoto.asp

Hyperledger Foundation. Hyperledger – Open Source Blockchain Technologies [online]. Copyright © 2022 The Linux Foundation Dostupné z: https://www.hyperledger.org/about

Jokić, S., Cvetković, A.S., Adamović, S., Ristić, N. and Spalević, P., 2019. Comparative analysis of cryptocurrency wallets vs traditional wallets. *Ekonomika*, *65*(3), pp.65-75.
Dostupné z: http://scindeks-clanci.ceon.rs/data/pdf/0350-137X/2019/0350-137X1903065J.pdf

Kotlin Docs | Kotlin Documentation. Kotlin Programming Language [online]. Dostupné z: https://kotlinlang.org/docs/home.html

Lykidis, I., Drosatos, G. and Rantos, K., 2021. The Use of Blockchain Technology in e-Government Services. Computers, 10(12), p.168
Dostupné z: https://www.mdpi.com/2073-431X/10/12/168

Meynkhard, A. (2019). Fair market value of bitcoin: halving effect. Investment Management and Financial Innovations.
Dostupné z: https://pdfs.semanticscholar.org/3686/3ee36a6e246b23c5baf2ba1e623ffd1fa832.pdf

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System.
Dostupné z: https://bitcoin.org/bitcoin.pdf
Ramík J. (1999): Vícekriteriální rozhodování – analytický hierarchický proces (AHP). Karviná, Slezská univerzita. Dostupné z: https://www.researchgate.net/publication/39759319_Vicekriterialni_rozhodovani_-_analyticky_hierarchicky_proces_AHP

Solidity — Solidity 0.8.19 documentation. [online]. Dostupné z: https://docs.soliditylang.org/en/v0.8.19/

Veramallu, V., 2021. SUPPLY CHAIN MANAGEMENT INTEGRATION WITH BLOCKCHAIN.
Dostupné z: https://scholarworks.lib.csusb.edu/cgi/viewcontent.cgi?article=2517&context=etd

Wang, Q., Li, R., Wang, Q. and Chen, S., 2021. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447. Dostupné z: https://www.researchgate.net/publication/351656444_Non-Fungible_Token_NFT_Overview_Evaluation_Opportunities_and_Challenges

XRP Healthcare | Web3 | Healthcare Solutions [online]. Copyright ©oj Dostupné z: https://xrphealthcare.com/XRPH-Deck.pdf

Zheng, Z., Xie, S., Dai, H.N., Chen, X. and Wang, H., 2018. Blockchain challenges and opportunities: A survey. International journal of web and grid services, 14(4), pp.352-375. Dostupné z: https://www.researchgate.net/publication/328338366_Blockchain_challenges_and_opportunities_A_survey

Z. Moezkarimi, F. Abdollahei and A. Arabsorkhi, "Proposing a Framework for Evaluating the Blockchain Platform," 2019 5th International Conference on Web Research (ICWR), Tehran, Iran, 2019, pp. 152-160, doi: 10.1109/ICWR.2019.8765280. Dostupné z: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8765280

8. Seznam obrázků, tabulek, grafů a zkratek

8.1. Seznam obrázků

8.2. Seznam tabulek

8.3. Seznam grafů

8.4. Seznam použitých zkratek

PoW – proof of work
PoS – proof of stake
PoET – proof of elapsed time
PoC – proof of capacity
PoA – proof of aktivity
NFC – Near-field communication
BTC – Bitcoin
dApps – decentralized applications
Web – website
NFT – non-fungible token
AHP – analytical hiearchy process
-less – permissionless
-ned – permissioned
RPCA – robust principal component analysis