DIPLOMOVÁ PRÁCE

Analýza možností využití technologie distribuovaného registru (DLT) z hlediska významné finanční skupiny působící v ČR

Analysis of the possibilities of using distributed register technology (DLT) from the point of view of a major financial group operating in the Czech Republic

STUDIJNÍ PROGRAM

Projektové řízení inovací

VEDOUCÍ PRÁCE

prof. Ing. Dušan Maga, Ph.D.

BÍZEK

TOMÁŠ

2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Bízek** Jméno: **Tomáš** Osobní číslo: **507476**

Fakulta/ústav: **Masarykův ústav vyšších studií**

Zadávající katedra/ústav: **Institut ekonomických studií**

Studijní program: **Projektové řízení inovací**

II. ÚDAJE K DIPLOMOVÉ PRÁCI

Název diplomové práce:

Analýza možností využití technologie distribuovaného registru (DLT) z hlediska významné finanční skupiny působící v ČR

Název diplomové práce anglicky:

Analysis of the Possibilities of Using Distributed Ledger Technology (DLT) from the Point of View of a Major Financial Group Operating in the Czech Republic

Pokyny pro vypracování:

Cílem práce je analýza přínosu a aplikace technologie distribuovaného registru (DLT) u velké finanční skupiny v ČR. Jedná se o posouzení její vhodnosti a smysluplnosti, zhodnocení slabých a silných stránek, dosavadního využití a určení vhodných adeptů k implementaci.
Teoretická část se zabývá okolnostmi vzniku této technologie, jejím rozdělením a konkrétními oblastmi využití. Popsán bude technický princip fungování.
Praktická část je členěna do dvou částí. První se týká analýzy trhu a trendů DLT technologie, druhá základnímu zhodnocení případu užití DLT technologie ve finančním sektoru a vytipování vhodných adeptů k implementaci pro velkou finanční skupinu v ČR.

Seznam doporučené literatury:

Antonopoulos, A. (2014). Mastering bitcoin. O'Reilly Media, Inc. [online] Available at: https://unglu[1]eit-files.s3.amazonaws.com/ebf/05db7df4f31840f0a873d6ea14dcc28d.pdf
Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. [ebook] Available at: https://bitcoin.org/bitcoin.pdf
Lewis, A. (2018). The Basics of Bitcoins and Blockchains. An Introduction to Cryptocurrencies and the Technology that Powers Them. Mango Publishing Group.

Jméno a pracoviště vedoucí(ho) diplomové práce:

prof. Ing. Dušan Maga, Ph.D. katedra telekomunikační techniky FEL

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) diplomové práce:

Datum zadání diplomové práce: **09.12.2022** Termín odevzdání diplomové práce: **17.08.2023**

Platnost zadání diplomové práce: _____

prof. Ing. Dušan Maga, Ph.D. podpis vedoucí(ho) práce	Mgr. František Hřebík, Ph.D. podpis vedoucí(ho) ústavu/katedry	prof. PhDr. Vladimíra Dvořáková, CSc. podpis děkana(ky)

III. PŘEVZETÍ ZADÁNÍ

Diplomant bere na vědomí, že je povinen vypracovat diplomovou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v diplomové práci.

Datum převzetí zadání _____ Podpis studenta _____

© ČVUT v Praze, Design: ČVUT v Praze, VIC

Bízek, Tomáš. *Analýza možností využití technologie distribuovaného registru (DLT) z hlediska významné finanční skupiny působící v ČR*. Praha: ČVUT, 2023. Diplomová práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií.

MASARYKŮV ÚSTAV
VYŠŠÍCH STUDIÍ
ČVUT V PRAZE

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně. Dále prohlašuji, že jsem všechny použité zdroje správně a úplně citoval a uvádím je v přiloženém seznamu použité literatury. Nemám závažný důvod proti zpřístupňování této závěrečné práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne: 27. 07. 2023 Podpis:

Poděkování

Děkuji vedoucímu práce, panu prof. Ing. Dušanu Magovi, Ph.D. za odborné vedení a cenné rady. Dále bych chtěl poděkovat Vítovi Ferencovi a Tomáši Hrochovi za jejich přátelskou pomoc při závěrečné finalizaci práce.

Abstrakt

Tato diplomová práce analyzuje možnosti využití technologie distribuovaného registru z hlediska významné finanční skupiny působící na finančním trhu v ČR. Nejprve byly získány informace o reálných případech užívání DLT na finančních trzích po celém světě. Následné byly tyto případy užití vyhodnocovány prostřednictvím metody analytického hierarchického procesu a metody komparace. Výsledky ukazují, že existuje několik vhodných adeptů pro implementaci, a to ve všech třech sektorech na finančním trhu v ČR.

Klíčová slova

Kryptoaktivum, technologie distribuovaného registru, DLT, blockchain, finanční trh, Ethereum

Abstract

This thesis analyses the possibilities of using distributed ledger technology from the point of view of a large financial group operating in the financial market in the Czech Republic. First, information on real cases of distributed ledger technology use in financial markets around the world was obtained. Subsequently, these real cases were evaluated using the method of the analytical hierarchy process and the method of comparison. The results show several adepts suitable for implementation in all three sectors of the financial market in the Czech Republic.

Key words

Cryptoassets, distributed ledger technology, DLT, blockchain, financial market, Ethereum.

Obsah

Úvod **5**

1 Úvod do kryptoaktiv a DLT **8**

1.1 Historie kryptoaktiv a DLT 8

1.1.1 Před-bitcoinová doba 8

1.1.2 Rok 2008 – vznik Bitcoinu 9

1.1.3 Rok 2015 – vznik Etherea 10

1.1.4 Období 2017–2018 tzv. ICOs 11

1.1.5 Období po roce 2020 12

1.2 Pojem DLT a pojem a druhy kryptoaktiv 13

1.2.1 DLT 13

1.2.2 Pojem kryptoaktiva 16

1.2.3 Základní rozdělení kryptoaktiv 17

1.2.4 Stablecoin 17

1.3 Právní aspekty kryptoaktiv a DLT technologie 19

1.4 Přínosy a nedostatky DLT technologie 21

2 DLT z technologického hlediska **23**

2.1 Vysvětlení technologické podstaty sítě Bitcoinu 23

2.1.1 Transakce s bitcoinem 24

2.2.2 Odeslání transakce do sítě 24

2.2.3 Těžení a mechanismus konsenzu 24

2.2.4 Bitcoin Core 26

2.2.5 Klíče a adresy 26

2.2.6 Peněženky 27

2.2.7 UTXO 27

2.2.8 Bitcoinová síť 28

2.2.9 Blockchain 28

2.2 Vysvětlení technologické podstaty sítě Ethereum 30

2.2.1 Účty 31

2.2.2 Transakce 32

2.2.3 Gas 32

2.2.4 Smartkontrakty ... 33
2.2.5 Tokeny ... 34
2.2.6 Orákulum ... 35
2.2.7 DApps ... 35
2.2.8 Mechanismus konsenzu ... 35
2.3 Druhy DLT ... 36
2.3.1 Blockchain ... 37
2.3.2 Directed Acyclic Graph ... 38
2.3.3 Holochain ... 41
2.3.4 Tempo ... 42
3 Metodologie ... 45
4 Přehled významného využití DLT technologie v sektorech finančního trhu ve světě ... 47
4.1 Využití DLT technologie na kapitálovém trhu ... 47
4.1.1 Societe Generale-Forge ... 47
4.1.2 Agora ... 48
4.1.3 GS DAP od Goldman Sachs ... 49
4.1.4 Progmat ... 50
4.1.5 Burza SDX ... 50
4.2 Využití DLT technologie v pojišťovnictví ... 51
4.2.1 Blockchain skupiny Allianz ... 51
4.2.2 Krypto-klimatická koalice vedená Lemonade ... 52
4.2.3 Ostatní projekty ... 52
4.3 Využití DLT technologie v bankovním sektoru ... 53
4.3.1 Abra ... 53
4.3.2 BitPesa ... 54
4.3.3 Kate Coin ... 54
4.3.4 Onyx od J. P. Morgan ... 55
4.3.5 Spunta ABI Lab DLT ... 56
5 Vytipování vhodných adeptů k implementaci pro velkou finanční skupinu v ČR ... 57
5.1 Předpoklady rozhodovacího procesu ... 57

5.1.1 Rozhodovací problém a varianty rozhodování 57
5.1.2 Cíle, kritéria, objekty a subjekty rozhodování 57
5.1.3 Stanovení vah kritérií 59
5.2 Rozhodovací proces 60
5.2.1 Hodnocení variant na kapitálovém trhu 61
5.2.2 Hodnocení variant v pojišťovnictví 65
5.2.3 Hodnocení variant v bankovnictví 67
Závěr 72
Bibliografie 74
Seznam obrázků 80
Seznam tabulek 81

Úvod

V roce 2008 člověk jménem Satoshi Nakamoto[1] zveřejnil technologický popis prvního DLT systému Bitcoin a stejnojmenného kryptoaktiva (kryptoaktiva imitující platidla často bývají označovaná jako „digitální měny“) bitcoin nazvaný „Bitcoin: A Peer-to-Peer Electronic Cash System“(Nakamoto 2008), který byl uveden v lednu následujícího roku do provozu, když byl vygenerován první blok stejnojmenné sítě.

První roky se s Bitcoinem nakládalo jako s alternativním projektem, když naprostá většina veřejnosti dle mého soudu počítala s tím, že tento projekt nebude mít dlouhodobou životnost. Cena bitcoinu se pohybovala až do roku 2011 pod jedním americkým dolarem (dále jen „dolar“) za jeden bitcoin, kdy přišel první významnější růst a cena za jeden bitcoin vystoupala až na 31 dolarů, aby se následně propadla pod 5 dolarů za jeden bitcoin. Těchto vln spočívajících v rapidním růstu a následném pádu ceny bitcoinu bylo postupem času mnoho, přesto znamenaly ve výsledku celkový růst jeho hodnoty. Například roce 2012 se cena dostala na 1000 dolarů, aby se propadla na 45 dolarů, v roce 2017 se hodnota dostala těsně pod 20 000 dolarů, poté se propadla na přibližně 6000 dolarů (Javůrek 2018).

Poslední vlnu jsme mohli sledovat v období 2020–2022, kdy se cena za jeden bitcoin vyšplhala na 64 000 dolarů, ale následně spadla na přibližně 19 000 dolarů (DeMatteo 2022). V roce 2022 tvoří bitcoin stále polovinu tržní kapitalizace všech kryptoaktiv, jež se vyšplhala v první polovině roku 2021 na 3 bilióny dolarů, ke konci roku 2022 se ustálila na 1 biliónu dolarů (Statista 2022).[2] Toto poslední období (2020–2022) je spjaté se zájmem finančních institucí o kryptoaktiva, která nejenom začínají do kryptoaktiv investovat, ale rovněž se snaží zkoumat a využívat nové tech-

[1] Pravděpodobně se jedná o pseudonym.
[2] Informace ohledně tržní hodnoty kryptoaktiv je třeba brát s rezervou vzhledem k tomu, že trh je stále velmi neregulovaný a nestandardizovaný a cena některých kryptoaktiv bývá nadsazována.

nologie, které kryptoaktiva přinesla. Jedná se především o technologii distribuovaného registru (dále jen „DLT“), jehož nejznámějším druhem je blockchain. Rovněž jsme svědky po celém světě, včetně EU, nové regulace kryptoaktiv, která v některých případech nahrává velkým finančním institucím, protože na subjekty emitující kryptoaktiva či poskytující s nimi související služby klade nové požadavky, jako jsou personální či kapitálové požadavky anebo náklady na compliance, které jsou snadněji splnitelné pro stávající finanční instituce. V EU bylo dokonce publikováno nové nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy (dále jen „MiCA“)(Evropská unie 2023), které v mnoha případech zvýhodňuje stávající finanční instituce. MiCA například akceptuje povolení, jež některé finanční instituce obdržely pro poskytování některých finančních služeb i pro poskytování jim ekvivalentních kryptoslužeb. Dále některé finanční subjekty jako banky dle MiCA vůbec nepotřebují mít licenci pro vydávání tzv. stablecoinů, zatímco ostatní subjekty takové povolení mít musí. MiCA rovněž limituje pravomoc vydávat a nabízet tzv. tokeny elektronických peněz jen na stávající subjekty finančního trhu s příslušnou licencí.

Z těchto důvodů je třeba technologie kryptoaktiv, zejména DLT, nadále zkoumat a hledat pro ně uplatnění i pro stávající velké finanční instituce v ČR, neboť MiCA přináší velkou příležitosti a trh se velmi rychle mění. Kdo se nepřizpůsobí či nevyužije příležitostí, může na trhu velmi rychle ztratil svoji pozici. Proto jsem si jako cíl své práce zvolil zmapování dosavadního využití DLT finančními subjekty po celém světě a nalezení jejich potenciální využitelnosti i pro nejmenovanou českou finanční skupinu, která se zabývá poskytováním finančních služeb ve všech sektorech finančního trhu (tedy v pojišťovnictví, bankovnictví a na kapitálovém trhu). Věřím, že práce přispěje k většímu využívání DLT finančními subjekty v ČR.

TEORETICKÁ ČÁST

1 Úvod do kryptoaktiv a DLT

Vzhledem k cíli mé práce je nezbytné popsat základní aspekty kryptoaktiv a technologie distribuovaného registru, jako jsou okolnosti jejich vzniku a jejich následný vývoj, terminologie a druhy, ale i právní aspekty. Rovněž se v této kapitole zabývám silnými a slabými stránkami těchto technologií a historií tržní kapitalizace kryptoaktiv, neboť se jedná o důležité aspekty, které využiji v následném mapování dosavadního využití kryptoaktiv subjekty finančního trhu.

1.1 Historie kryptoaktiv a DLT

Smyslem této kapitoly není podat vyčerpávající informace o historii kryptoaktiv a DLT, ale spíše zmínit nejdůležitější milníky ve vývoji těchto technologií.

1.1.1 Před-bitcoinová doba

Pokud jde o uchovávání záznamů o transakcích, tak ty sahají až do starověku, například do starověké Mezopotámie. V novodobé historii se koncepce nezměnitelného řetězení bloků obsahujících informace s kryptografickou hashovací funkcí objevuje v disertační práci Ralpha Merklea z roku 1979, ve které popisuje, jak mohou být informace spojené do stromové struktury, dnes známé jako tzv. Merkleův strom. Významná je rovněž disertační práce Davida Chauma z roku 1982, v níž zmiňuje mnoho elementů blockchainu, který popisuje mj. jako distribuovaný počítačový systém sloužící k vedení evidence, jenž může být založený, spravovaný vzájemně se podezřívajícími skupinami (Sherman et al. 2019). David Chaum se rovněž zabýval vytvořením digitálních peněz a v roce 1989 vytvořil společnost DigiCash, která se zabývala právě vydáváním digitálních peněz s využitím asymetrické kryptografie, když mj. využívala již soukromé a veřejné klíče (Frankenfield 2021). Již před vznikem Bitcoinu vznikaly koncepty digitálních měn a obdobných kryptoaktiv. Mezi ně lze zařadit studii inženýra Wei Daie B-Money z roku 1998 (Dai 1998), kde popisuje digitální měnu odesílanou mezi nevysledovatelnými anonymními digitálními pseudonymy. V roce 1998 vyšla rovněž studie o kryptoměně Bit Gold od Nicka Szaboa (SHARMA 2021), která se natolik podobá technickému popisu Bitcoinu, publikovanému o deset let později, že se

dodnes spekuluje, zda Nick Szabo není Satoshi Nakamoto. Každopádně mezi Bitcoinem a Bit Goldem existují rozdíly, jako je jiná koncepce obtížnosti těžby obou kryptoaktiv či že Bit Gold neměl fungovat jako měna sama o sobě, ale jako měna rezervní.

1.1.2 Rok 2008 – vznik Bitcoinu

Klíčovým milníkem rozmachu kryptoaktiv je rok 2008, kdy osoba jménem Satoshi Nakamoto[3] zveřejnila technologický popis prvního kryptoaktiva a stejnojmenné sítě Bitcoin nazvaný „Bitcoin: A Peer-to-Peer Electronic Cash System“ (Nakamoto 2008), která byla uvedena v lednu následujícího roku do provozu, když byl vygenerován její první blok. V rámci Bitcoinu kombinoval Satoshi Nakamoto několik předchozích inovací a konceptů digitálních peněz, jako jsou B-Money z roku 1998 a anti-spamový software HashCash používající algoritmus[4] Proof-of-Work (Back 1997), aby se mu podařilo vytvořit plně decentralizovaný elektronický peněžní systém, který se nespoléhá na centrální autoritu v případě vydávání těchto peněžních prostředků nebo vypořádání transakcí s nimi (jako je tomu typicky u zákonných platidel centrálních bank). Za hlavní inovaci se zde považuje využití distribuovaného výpočetního systému, který Nakamoto nazývá algoritmus „*Proof-of-work*“ a jenž zjednodušeně řečeno provádí schvalování transakcí přibližně každých 10 minut, umožňující decentralizované síti uživatelů tohoto systému shodnout se na stavu transakcí s kryptoaktivem bitcoin. Tento algoritmus vyřešil dosavadní problém decentralizace kryptoaktiv (kryptoaktiva imitující platidla často bývají označovaná jako „digitální měny“), který spočívá v tzv. dvojí útratě (anglicky „double-spending problem“), kdy stále stejné kryptoaktivum může být utraceno jeho vlastníkem více než jednou a příjemce platby si tuto skutečnost nemůže nikterak ověřit. Tento problém byl do té doby řešen právě centrálními institucemi ověřujícími ve své evidenci pravost transakcí. Satoshi Nakamoto rovněž vyřešil problém tzv. byzantských generálů, který spočívá v pokusu shodnout se mezi více subjekty na provedení určité akce nebo stavu systému prostřednic-

[3] Pravděpodobně se jedná o pseudonym.
[4] Algoritmus je pracovní postup, který má tyto povinné vlastnosti: Rezultativnost, konečnost, elementárnost a determinovanost (Lessner et al. 2020).

tvím výměny informací skrze nespolehlivou a potenciálně zkompromitovanou (komunikační) síť, tedy decentralizovaně, aniž by k tomu využily centrální autoritu[5]. Toto inovativní řešení lze využít například i pro dosažení konsenzu pro decentralizované hlasování ve volbách či pro decentralizované vedení rejstříků či evidencí majetku (Antonopoulos 2017).

Doba po vzniku bitcoinu byla poznamenaná mnoha milníky, například první obchod s bitcoinem byl zaznamenán v roce 2010, když bylo za 2 pizzy zaplaceno 10 000 bitcoinů. Tento milník je dodnes oslavován po celém světě jako tzv. „Pizza day" (Jones 2023). V roce 2011 se objevila nová konkurenční kryptoaktiva a stejnojmenné sítě jako jsou namecoin a litecoin (někdy označovaný jako stříbro v souvislosti s bitcoinem, který se označuje jako zlato) a hodnota bitcoinu poprvé přesáhla 1 dolar. V roce 2013 stál jeden bitcoin už 1000 dolarů. V tomto období vznikají první kryptoburzy, kryptopeněženky a další služby související s kryptoaktivy a také se čím dál více mluví o podvodech s kryptoaktivy a jejich krádežích. K jedné z největších došlo v roce 2014 při útoku na tehdejší největší kryptoburzu Mt. Gox, při němž bylo ukradeno 850 000 bitcoinů.

1.1.3 Rok 2015 – vznik Etherea

Plattforma Ethereum vznikla v období, kdy technologie kryptoaktiv již získaly určitou reputaci a byla snaha najít využití pro tyto technologie i mimo jejich využití jako „kryptoměn". Proto na konci roku 2013 přišel mladý programátor Vitalik Buterin (Sobol 2022) s myšlenkou rozšířit schopnosti sítě Bitcoin a protokolu Mastercoin[6], jeho cílem bylo vytvořit Turingovsky kompletní blockchain pro všeobecné použití (Antonopoulos a Wood 2019). Šlo by tedy o blockchain, který by neměl specifický účel, ale bylo by možné na něm vytvářet i nové aplikace. Pokud se Bitcoin omezoval jen na evidenci své „kryptoměny", pak protokol Etherea nabídl kromě své vlastní stejnojmenné „kryptoměny" mnohem více případů jejího užití, jako jsou smartkontrakty,

[6] Protokol, který rozšiřoval funkcionalitu sítě Bitcoin o tzv. smart kontrakty.

decentralizované aplikace či vytváření nových kryptoaktiv. 30. července 2015 byl vytěžen první blok blockchainu Ethereum a záhy se jeho vlastní „kryptoměna“ ether stala dle tržní kapitalizace druhým největším kryptoaktivem.

1.1.4 Období 2017–2018 tzv. ICOs

Období následujících let po vzniku Etherea lze charakterizovat jako vlnu růstu, kdy odhadovaná tržní kapitalizace všech kryptoaktiv vystoupala v roce 2017 téměř k 800 mld. dolarům z přibližně 15 mld. v předchozím roce, aby následně klesla až na nějakých 120 mld. dolarů v roce 2019 (viz obrázek 1). Toto období je spjaté s fenoménem tzv. prvotního nabízení mincí (anglicky „initial coin offering“ či „ICO“). ICO lze tedy definovat jako způsob, kterým společnost získává prostředky na svůj rozvoj prostřednictvím emise vlastních kryptoaktiv, se kterými mohou být spojena i práva, například vlastnické právo k budoucímu produktu či přístup k službě.

První ICO se uskutečnilo v roce 2013 a jednalo se o již výše zmiňovaný Matercoin, jehož tvůrce vybral na vývoj tohoto protokolu od veřejnosti bitcoiny v té době v přepočtu za 600 tisíc USD za stejnojmenná kryptoaktiva a další výhody v rámci nově vytvořeného protokolu. Z ICO se stal postupem času trend, kdy ICO pořádalo i Ethereum, které vybralo 18 milionů USD (Merre 2021). V roce 2018 se uskutečnila největší ICO emise kryptoaktiva EOS, kdy se v roce 2018 vybralo 4,1 mld. USD. Pomyslná „bublina“ ICO postupem času splaskla vzhledem k tomu, že orgány dohledu jako Komise pro cenné papíry v USA začaly některé ICO kvalifikovat jako regulované prvotní nabízení cenných papírů veřejnosti (tzv. „initial public offering“ či „IPO“) (Frankenfield 2022b) nebo je rovnou zakazovat jako v Číně (Vaswani 2017). Rovněž je třeba mít na paměti, že ICO bylo pro investory velmi rizikové, protože naprostá většina z nich byla vysoce ztrátová, když například dle výzkumu Haffkeho a Frombergera (Haffke a Fromberger 2020) více než 60 procent analyzovaných ICO ztratilo svou hodnotu nebo více než 75 procent své původní hodnoty do 180 dnů od jejich první nabídky veřejnosti.

Obrázek 1 – Agregovaná tržní kapitalizace kryptoaktiv a objem transakcí

Zdroj: Coinmarketcap.com

1.1.5 Období po roce 2020

Po roce 2020 opět zažíváme výrazný růst souhrnné tržní kapitalizace kryptoaktiv, když v polovině roku 2021 vzrostla až ke 3 bilionům dolarů, ale ke konci roku 2022 klesla zhruba 1 bilion dolarů. Důvodů tohoto růstu bývá udáváno vícero (Locke 2021). Já za dva hlavní faktory tohoto růstu pokládám zvýšený zájem institucionálních investorů ohledně investování do kryptoaktiv, kdy například začínají vznikat investiční fondy investující do kryptoaktiv či nové společnosti zabývající se kryptoaktivy, například krypto-směnárny vstupují na burzu (Raphael Auer & Marc Farag & Ulf Lewrick & Lovrenc Orazem & Markus Zoss 2022). Rovněž je patrný zvýšený zájem o kryptoaktiva ze strany běžných, retailových investorů, kteří během pandemie covidu-19 obecně více investují prostřednictvím nových aplikací jako je Robinhood od stejnojmenné společnosti. Do tohoto období je třeba rovněž zařadit vzestup nových technologií či inovací, jako jsou NFT („non-fungible tokens“, česky nezastupitelné tokeny), které v podobě certifikátu o vlastnictví pronikají do umění, DeFi („decentralised finance“, česky decentralizované finance), tedy decentralizované kvazifinační služby s kryptoaktivy či komunity, jako jsou DAO (decentralizované autonomní organizace), což je *organizace, která je řízena počítačovým kódem a programy. Jako taková má schopnost fungovat autonomně, bez potřeby centrální autority… DAO je decentrali-*

zovaná a autonomní. Je decentralizovaná, protože žádný subjekt nemá pravomoc přijímat a prosazovat rozhodnutí. A je autonomní, protože může fungovat samostatně (Binance 2020).

1.2 Pojem DLT a pojem a druhy kryptoaktiv

V této kapitole se věnuji základnímu popisu DLT a jejím klíčovým znakům. Dále uvádím definici kryptoaktiv a jejich základní rozdělení. Není ambicí této kapitoly podat úplný výčet všech druhů kryptoaktiv, spíše se zde zaměřuji na ty relevantní pro praktickou část mé práce.

1.2.1 DLT

Existuje mnoho definic DLT, například dle nové legislativy Evropské unie (2022) se jedná o technologii*, která umožňuje provozování a používání distribuovaných registrů, což je úložiště informací, které vede evidenci o transakcích a které je sdíleno prostřednictvím souboru DLT síťových uzlů a synchronizováno mezi nimi pomocí mechanismu konsensu*. DLT síťovým uzlem pak *je zařízení nebo proces, které jsou součástí sítě a které obsahují úplnou nebo částečnou repliku evidence o všech transakcích v distribuovaném registru*.

Pro zjednodušení si lze pod pojmem DLT síťového uzlu rovněž představit každého řadového uživatele sítě, který má u sebe kopii DLT a DLT prostřednictvím příslušného softwaru používá.

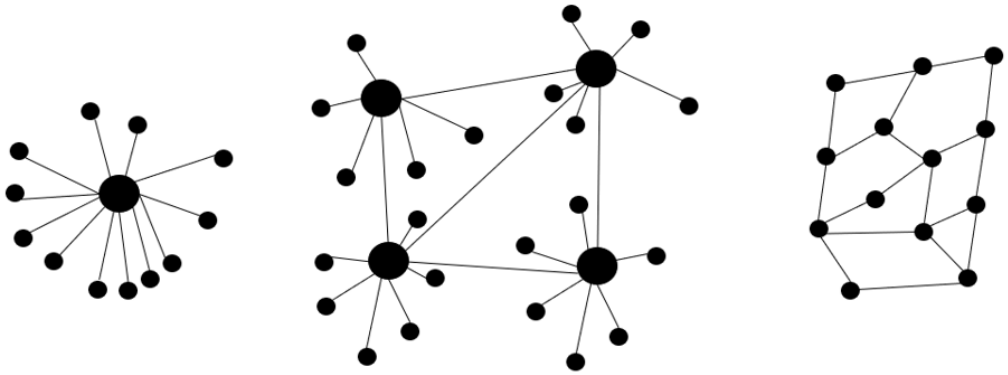
Pojmovými znaky DLT se zabývá podrobně Bashir (2023), ze kterého v této kapitole čerpám. Podle něj lze DLT chápat jako vrstvu distribuované peer-to-peer sítě, která běží na internetu.

1) Hlavním pojmových znakem DLT je dle Bashira skutečnost, že se jedná o distribuovaný systém, tzn. systém, ve kterém jeho dva či více uzlů spolupracují koordinovaně takovým způsobem, aby dosáhly společného výsledku, ale z vnějšího pohledu se

jedná o systém jediný. Jako příklad bývá uváděný vyhledávací systém od společnosti Google. Distribuovaný systém se skládá z uzlů a z komunikačních kanálů, kde uzly mezi sebou komunikují prostřednictvím posílání zpráv. Pro distribuované systémy je příznačné, že ačkoliv některé uzly či propojení mezi nimi jsou chybové, když například posílají nepravdivé zprávy či neposílají vůbec nic, tak distribuované systémy mají k takové chybovosti určitou hladinu tolerance, a fungují i přesto správně.

Problémem při vytváření distribuovaných systémů je skutečnost, že nemohou disponovat třemi klíčovými vlastnostmi najednou. Tuto domněnku poprvé představil Eric Brewer v roce 1998 a nazval ji CAP teorém. Dle něj nemohou distribuované systémy disponovat zároveň a) konzistencí, což je vlastnost, která zajišťuje, že všechny uzly v distribuovaném systému mají jedinou aktuální a totožnou kopii dat, b) dostupností, tedy vlastností spočívající ve skutečnost, že data jsou dostupná v každém uzlu, a to na požadavek uzlu jiného bez prodlení či jiných chyb, c) tolerancí k chybovosti uzlů a propojením popsaným v předcházejícím odstavci. Právě v DLT je konzistence obětována na úkor ostatních dvou vlastností. To znamená, že pro DLT je typické, že existují uzly s odlišnými daty, které se ovšem časem synchronizují, typicky je tomu například u větvení bloků u Bitcoinu v kapitole 2.2.9.

Infrastrukturu informačních technologií lze rozlišovat na centralizovanou, decentralizovanou a distribuovanou. Centralizované infrastruktury fungují na základě vztahu client-server, kde server poskytuje v rámci infrastruktury klíčovou funkci, jako je databáze či aplikační servery a je ovládán centrální autoritou. U decentralizovaných infrastruktur není jediná centrální autorita, nýbrž její role je nahrazena více autoritami. Jako příklad lze uvést společnost, kde si každé oddělení spravuje svou část databáze. V distribuovaném systému žádné autority nejsou, nýbrž data se synchronizují napříč uzly infrastruktury a navenek se infrastruktura chová jako jednolitá (viz obrázek č. 2).



Obrázek 2 – Centralizovaný, decentralizovaný a distribuovaný systém

2) Dalším pojmovým znakem DLT je skutečnost, že to je peer-to-peer síť, tzn. že každý uživatel této sítě je připojen hned k několika dalším uzlům sítě za účelem komunikace, a to bez zprostředkování či kontroly takové komunikace ze strany jakékoliv centrální autority.

3) Zabezpečení prostřednictvím kryptografie za účelem zamezení falšování či zneužití na ní uložených dat.

4) Data lze pouze vkládat do DLT, a to v časově sekvenčním pořadí a je téměř nemožné jednou vložená a validovaná data měnit.

5) Posledním významným znakem DLT je možnost její aktualizace prostřednictvím mechanismu konsenzu, tzn. že data nevaliduje a nepřidává do DLT nějaká centralizovaná autorita, nýbrž jsou přidávána na základě předem stanovených pravidel protokolu, umožňujícím jednotlivým uzlům či uživatelům DLT se shodnout na aktualizaci. Nejznámějšími mechanismy konsenzu jsou mechanismus konsenzu, který používá síť Bitcoin, tzv. proof-of-work a mechismus konsenzu, který používá platforma Ethereum, tzv. proof-of-stake, které blíže popisuji v kapitole 2.

DLT technologii lze rozdělit na několik typů a základním rozlišením je způsob, jak jsou dané záznamy v DLT evidovány. Pokud architektura chronologicky jdoucích záznamů

za sebou tvoří řetězec bloků, pak hovoříme o tzv. blockchainu, což je nejznámější a nejčetněji zastoupená kategorie DLT. Dalšími důležitými druhy DLT jsou Directed Acyclic Graphs, Holochain a Tempo. Druhy DLT se podrobně zabývám v kapitole 2.3.

1.2.2 Pojem kryptoaktiva

Terminologie kryptoaktiv je nejednotná, stále se utváří, a proto se používají různé termíny jako digitální peníze, virtuální měny, kryptoměny, virtuální aktiva či kryptoaktiva. Například v roce 2019 (Blandin, Apolline and Cloots, Ann Sofie and Hussain, Hatim and Rauchs, Michel and Saleuddin, Rasheed and Allen, Jason Grant and Cloud, Katherine and Zhang, Bryan Zheng 2019) se pojem virtuální měna používal v legislativě v USA, Japonska či Kanady, kryptoaktiv v legislativě Německa či Velké Británie, pojem virtuální aktiva v legislativě Mexika a pojem digitální aktiva používala legislativa Francie. Česká legislativa zatím pracuje jen s pojmem virtuální aktiva v zákoně proti praní špinavých peněz (Česká republika 2008), který byl přejat z terminologie Finančního akčního výboru, což je mezinárodní mezivládní organizace, která stanovuje standardy ohledně praní špinavých peněz a boje proti terorismu. Je patrné, že se terminologie postupem času vyvíjí, když na úrovni orgánů Evropské unie byl nejprve používaný pojem virtuální měna, který zdůrazňoval platební funkci některých kryptoaktiv, když se později začalo používat pojmu kryptoaktivum, což vyvrcholilo návrhem nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy (Evropská komise 2020), který zveřejnila Evropská komise v roce 2020. Lze očekávat, že tato terminologie se rozšíří nejenom do členských států Evropské unie, ale i za její hranice, neboť pokud bude tato legislativa schválená, půjde pravděpodobně o nejvýznamnější legislativní akt svého druhu (Evropská unie 2023). Dle čl. 3 odst. 1 bodu 2 MiCA je kryptoaktivum *„digitální zachycení hodnoty nebo práva, které může být převáděno a ukládáno elektronicky pomocí technologie distribuovaného registru nebo pomocí podobné technologie“.* Tato definice je dle mého názoru dostatečně široká, neboť se pod ní vejdou všechna známá kryptoaktiva, zároveň explicitně zmiňuje jako klíčový znak kryptoaktiv technologie distribuovaného registru, avšak v budoucnu bude třeba upřesnit, jaké všechny technologie budou spadat pod podobné technologie technologii distribuovaného registru. Samotný termín kryptoaktivum implikuje, že se jedná

o majetek spjatý s kryptografií, což je mnohem výstižnější nežli například termín virtuální aktivum, kam by mohly spadat například i elektronické peníze dle zákona č. 370/2017 Sb., o platebním styku.

Dále se v souvislosti s kryptoaktivy používá pojem token, který lze definovat jako jednotku kryptoaktiva.

1.2.3 Základní rozdělení kryptoaktiv

Existuje několik základních rozdělení kryptoaktiv. Nejobecněji lze kryptoaktiva dělit na bitcoiny a altcoiny. Mezi altcoiny patří všechna kryptoaktiva kromě bitcoinu. Toto rozdělení je vzhledem k velké tržní kapitalizaci bitcoinu stále využitelné. V poslední době je významné rozdělení kryptoaktiv, které mimo jiné zmiňuje i Evropský orgán pro bankovnictví (2019) (dále jen „EBA“), a to dle jejich účelu na platební či převodní tokeny, které slouží k převodům či jako platební prostředky a typicky neobsahují žádná práva, další kategorií jsou dle EBA investiční tokeny, se kterými jsou spojena práva, jako jsou vlastnické právo či oprávnění, příkladem by mohl být tokenizovaný derivát či tokenizovaná akcie. Třetí kategorií jsou užitné tokeny, které typicky umožňují přístup k nějakému produktu či službě, příkladem mohou být lístky do kina. V praxi významným dělením bude skutečnost, zda jsou kryptoaktiva regulována předpisy finančního trhu, či nikoliv. Samozřejmě tato taxonomie počítá s tzv. hybridními tokeny, které mohou splňovat znaky více kategorií.

Kryptoaktiva lze rovněž dělit podle zastupitelnosti na tzv. zastupitelné tokeny, kam typicky patří bitcoin či ether, kdy jednotlivé tokeny lze nahradit tokenem stejného druhu, a nezastupitelné tokeny, kam patří například tokenizované certifikáty o uměleckých dílech, tzv. NFT (z anglické non-fungible token), které nelze nahradit tokenem stejného druhu.

1.2.4 Stablecoin

Pro finanční sektor je významná kategorie tzv. stablecoinů, proto o nich pojednávám v samostatné podkapitole. Stablecoiny řeší v rámci „světa“ kryptoaktiv především

problém velké volatility kryptoaktiv, která je typická pro převodní tokeny jako je bitcoin. Proto stablecoiny mají určitý stabilizační mechanismus, který jejich hodnotu stabilizuje prostřednictvím navázáním na nějaké referenční aktivum či kombinaci aktiv. Stablecoiny lze dle stabilizačního mechanismu rozdělit na dvě kategorie, a to na stablecoiny, jejichž hodnota je stabilizovaná tím, že je kryta jiným aktivem či košem aktiv, a na tzv. algoritmické stablecoiny, jejichž hodnota je stabilizovaná prostřednictvím algoritmu.

Pokud jde o první typ stablecoinu, ten typicky jejich vydavatel kryje rezervou v podobě fiat měny, komoditami či jinými kryptoaktivy či jejich kombinací, jež má v úschově. Příkladem byl stablecoin diem. Ohlášení nového stablecoinu diem (Murphy et al. 2022) od stejnojmenné asociace, jejímž hlavním členem byla společnost Meta Platforms (dříve Facebook), se v roce 2019 stalo velkou obavou pro strany mnoha vlád, centrálních bank a orgánů dohledu nad finančním trhem kvůli možnosti praní špinavých peněz, ohrožení finanční stability a vytvoření globálního platebního prostředku, jehož rezervou měl být koš tvořený z několika fiat měn, jako je americký dolar. Potenciální vznik stablecoinu diem byl rovněž i jedním z hlavních důvodů vzniku návrhu Evropské komise nařízení MiCA. Tlak ze strany regulačních a dohledových orgánů se stal tomuto projektu osudným, neboť 31. ledna 2022 asociace Diem na svých stránkách oznámila (Diem Association 2022) prodej práv duševního vlastnictví a dalších aktiv, což znamenalo konec projektu vývoje stablecoinu diem.

Algoritmické stablecoiny (Genç 2023) udržují svou stabilní hodnotu prostřednictvím algoritmu, který funguje obdobně jako měnová politika centrální banky. Když je hodnota stablecoinu vyšší nežli referenční aktivum, vůči kterému udržuje stabilní hodnotu, pak algoritmus zvyšuje počet stablecoinů v oběhu. Pokud je cena stablecoinu nižší nežli cena referenčního aktiva, pak algoritmus stahuje stablecoiny z oběhu. K tomu používá různé mechanismy, jako jsou například pobídky k jejich nákupu ve formě provizí.

1.3 Právní aspekty kryptoaktiv a DLT technologie

Kryptoaktiva a DLT v ČR podléhaly doposud minimální regulaci, což se ovšem v brzké době v důsledku přijímání nové evropské regulace značně změní. Nejvýznamnější dosavadní regulací je zákon proti praní špinavých peněz, kde jsou pro poskytovatele služeb s kryptoaktivy povinnosti jako například identifikovat či kontrolovat své klienty (Česká republika 2008). Významná je z hlediska právního režimu kryptoaktiv rovněž skutečnost, že v ČR nelze dle převažující právní interpretace[7] tokeny vydat podle českého práva jako cenné papíry (tedy jako akcie či dluhopisy), ač osobně zastávám protichůdný názor, když tvrdím, že centrální depozitář může vést evidenci zaknihovaných cenných papírů v DLT podobě v souladu se zákonem podnikání na kapitálovém trhu (Česká republika 2004) a s dalšími právními předpisy. Pro finanční trh v ČR lze jako jedno z nejvýznamnější právních stanovisek uvést stanovisko České národní banky (ČNB) k převodním tokenům, ze kterého vyplývá, že ČNB převodní tokeny a služby s nimi spojené v naprosté většině případů nedohlíží (Česká národní banka 2018).

V rámci balíčku digitálních financí zveřejnila Evropská komise dva návrhy nařízení, které se týkají kryptoaktiv. První z nich, tzv. nařízení o pilotním režimu pro tržní infrastruktury založené na technologii sdíleného registru (Ministerstvo financí ČR, oddělení 3502 – Platební služby a tržní infrastruktura 2022), zavádí pilotní režim pro tržní infrastrukturu založenou na DLT. Konkrétně zavádí tři zvláštní licenční režimy tržní infrastruktury využívající technologii DLT na období šesti let. Tato povolení mohou získat subjekty držící licenci pro obchodníka s cennými papíry, provozovatele regulovaného trhu nebo centrálního depozitáře cenných papírů. Nařízení stanoví také některé regulatorní výjimky pro provozování infrastruktury DLT. Zároveň nařízení staví najisto, že investičním nástrojem může být i investiční nástroj vydaný na DLT.

[7] Srov. DĚDIČ, Jan, ŠOVAR, Jan, MIKULA, Ondřej. Proč podle českého soukromého práva nelze uvažovat o (ICO) tokenech jako o cenných papírech. Právní rozhledy. 2018, č. 15–16, s. 554–556; nebo HOBZA, Martin. ICO a tokeny optikou práva kapitálového trhu: mohou být tokeny investičními cennými papíry? Bulletin advokacie. 2019, č. 3, s. 41–46.

Toto nařízení bude muset být dále adaptováno do české legislativy. Jeho smyslem je umožnit rozvoj využívání technologie DLT na finančních trzích. Typicky půjde o to usnadnit použití DLT při vydávání akcií či dluhopisů. Dle důvodové zprávy tohoto nařízení: *Právní předpisy Unie v oblasti finančních služeb nebyly vytvořeny s ohledem na technologii sdíleného registru a kryptoaktiva a obsahují ustanovení, která mohou vyloučit nebo omezit použití technologie sdíleného registru při emisi, obchodování a vypořádání kryptoaktiv, která jsou považována za finanční nástroje. V současné době také chybí povolená infrastruktura finančního trhu, která by využívala technologii sdíleného registru a poskytovala pro kryptoaktiva, která jsou považována za finanční nástroje, služby v oblasti obchodování nebo vypořádání, případně kombinaci těchto služeb. Rozvoj sekundárního trhu s takovými kryptoaktivy by mohl přinést četné výhody, jako jsou vyšší účinnost, transparentnost a hospodářská soutěž v souvislosti s obchodováním a vypořádáním.* Nařízení má pilotní charakter, tzn. že v roce 2026 budou evropské orgány rozhodovat o jeho prodloužení či revizi.

Druhým významným právním předpisem, který v rámci balíčku digitálních financí zveřejnila Evropská komise, byl návrh nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy, tzv. MiCA, jejíž regulaci mají zjednodušeně řečeno podléhat ta kryptoaktiva, která nebudou podléhat regulaci jiných předpisů na finančním trhu. Půjde typicky o převodní tokeny či o stablecoiny. Návrh v mnoha případech zvýhodňoval stávající finanční instituce, když mj. akceptoval některá povolení, která obdržely pro poskytování některých jiných finančních služeb i pro vydávání a nabízení stablecoinů, zatímco ostatní subjekty si budou muset o obdobné povolení zažádat, či jim návrh dokonce limituje možnost vydávat tzv. tokeny elektronických peněz jen na stávající subjekty finančního trhu s příslušnou licencí instituce elektronických peněz či úvěrové instituce. Právě z těchto důvodů má nařízení MiCA, které bylo schváleno v polovině roku 2023 (Evropský parlament 2023), změnit trh s kryptoaktivy ve prospěch stávajících finančních institucí.

1.4 Přínosy a nedostatky DLT technologie

Dle mého názoru možné přínosy a výhody DLT pro zaznamenávání kryptoaktiv a jiných údajů v sobě implikují i nedostatky. Vždy půjde o konkrétní potřebu, která bude rozhodující, zda zvolit DLT technologii, nebo centralizovaný systém pro ukládání dat, jako jsou tradiční databáze. Níže popisuji základní přehled přínosů a nedostatků DLT technologie a využívání kryptoaktiv:

a) Decentralizace a disintermediace (Natarajan et al. 2017) – toto je smysl vytvoření DLT technologie a její hlavní výhoda. V případě DLT jde o systém pro evidenci, pro jehož fungování nepotřebujeme žádné centrální autority či zprostředkovatele, což v důsledku přináší úspory, zvyšuje rychlost a zlepšuje škálovatelnost. Je ovšem nutné podotknout, že pro komerční subjekty, jež vykonávají zprostředkovatelské funkce, nemusí být decentralizace a disintermediace žádoucí.

b) Rychlost – tradiční finanční infrastruktury se často potýkají s omezeními, když například na burzách se obchoduje pouze v obchodní dny a v určeném čase, mezibankovní platební transakce se ještě donedávna vypořádávaly v ten samý den pouze za poplatek a o víkendech je vypořádání mezi bankami v ČR stále omezené. Například blockchain sítě Bitcoin vypořádává transakce každých deset minut 24 hodin denně 7 dní v týdnu. Potenciál této technologie je ovšem vypořádávat transakce okamžitě. Je známým faktem, že Bitcoin je schopen provést přibližně 7 transakcí za vteřinu a novější DLT jsou schopny realizovat tisíce transakcí za vteřinu. Oproti tomu například americká společnost VISA (Rodrigues 2022) je údajně schopná zprocesovat až 65 000 transakcí za vteřinu.

c) Transparentnost a snadná kontrola údajů registru – všichni členové sítě DLT mohou disponovat svou kopií distribuovaného registru a změny v registru lze činit jen na základě splnění podmínek algoritmu spočívajícího v konsenzu účastníků sítě. Takový registr je snadno auditovatelný.

d) Automatizace a programovatelnost – DLT umožňuje tzv. smartkontrakty, tzn. software umístěný na DLT, který je vykonatelný za splnění předem sta-

novených podmínek (blíže ke smartkontraktům viz kapitola 2.2.4). Ve finančnictví by smartkontrakty šlo například použít pro automatické vyplacení dividend držiteli akcií. Automatizace i programovatelnost jsou ovšem proveditelné i u centralizovaných systémů.

e) Obtížná změnitelnost záznamů – DLT má charakter účetní knihy, kde jsou data navázána na sebe a do níž se zapisuje typicky na základě mechanismu spočívajícího v konsenzu účastníků sítě. Čím starší jsou záznamy, tím obtížnější je možnost jejich změny. Tato architektura ovšem nemusí být vhodná v případě, kdy potřebujeme záznamy změnit, například v případě chybných transakcí.

f) Kybernetická bezpečnost – DLT registry vzhledem k tomu, že jsou distribuované mezi uživateli, nejsou závislé na bezpečnosti nějakého centrálního registru, jako tomu je u centralizovaných databází. Útok na jeden registr nevede k poškození záznamů. Oproti tomu u DLT existují jiné hrozby kybernetických útoků, jako jsou útoky na tzv. kryptopeněženky, kryptoburzy, útoky na ovládnutí řízení DLT apod. Mezi nejvýznamnější možné útoky na DLT je tzv. 51procentní útok, který spočívá v ovládnutí většiny hašovací či výpočetní kapacity určené k vytváření nových bloků DLT, tedy více než 50 procent (Frankenfield 2022a). Takové ovládnutí by mělo za následek možnost vytvářet nové bloky dle požadavků daného útočníka, který by mohl blokovat validaci nových transakcí nebo je měnit a utrácet ve svůj prospěch. Přesto i takový útok by měl malé šance měnit bloky blockchainu zvalidované v minulosti, tedy před samotným útokem.

g) Dostupnost a nižší náklady – Některá kryptoaktiva jako například bitcoin představují pro jejich uživatele snadnější a levnější způsob přeshraničního platebního styku oproti centralizovaným platebním systémům, kde mohou být vyšší poplatky za remitence (Natarajan et al. 2017).

2 DLT z technologického hlediska

Vzhledem k tomu, že cílem mé práce je zhodnotit využitelnost DLT pro finanční sektor a navrhnout prototyp možného využití, nelze opomenout popis DLT z technologického hlediska. Proto se tato kapitola věnuje základním technologickým aspektům DLT na příkladech sítě Bitcoin a platformy Ethereum. Dále je v uveden popis i jiných druhů DLT, než je blockchain, na kterém jsou Bitcoin i Ethereum založené.

2.1 Vysvětlení technologické podstaty sítě Bitcoinu

Cílem této kapitoly není detailně vysvětlit veškeré technikálie Bitcoinu, nýbrž popsat základní technické principy jeho fungování a soustředit se především na technologii DLT. V této kapitole čerpám z publikace nazvané Mastering Bitcoin: Programming the Open Blockchain (Antonopoulos 2017), pokud neuvádím jinak. Jak již bylo uvedeno, Bitcoin je inovativní zejména v použití kryptografických technologických poznatků s technologií distribuovaného registru. Bitcoin je názvem jak pro protokol, tak pro samotné kryptoaktivum, které se prostřednictvím tohoto protokolu převádí mezi jeho uživateli a imituje pro tyto uživatele funkcionalitu peněz. Samotné kryptoaktivum bitcoin existuje oproti tradičním penězům pouze ve virtuální podobě, a nikoliv v podobě hmotné, či digitální, protože je obsažené v samotných transakcích mezi jeho odesílatelem a příjemcem. Tyto transakce jsou evidované chronologicky v blocích, ze kterých se skládá blockchain Bitcoinu, což je druh DLT. Zjednodušeně vyjádřeno se každých deset minut vytvoří nový blok obsahující transakce za posledních deset minut před jeho vznikem. Tento blok se přidá na konec blockchainu, tedy za poslední blok. Uživatelé se na stavu blockchainu dohodnou prostřednictvím mechanismu konsenzu, což je protokol, který umožňuje síti Bitcoin dohodnout se na aktuálním stavu blockchainu, jehož klíčovou součástí je mechanismus proof-of-work (více v kapitole 2.2.3 o těžení bitcoinu). Uživatelé Bitcoinu používají kryptografické klíče, jejichž prostřednictvím mohou s bitcoiny nakládat. Právě tyto klíče bývají uschovávány v tzv. digitálních peněženkách. Bitcoin je distribuovaný peer-to-peer systém, tzn. že v něm komunikují klienti napřímo bez existence centralizovaného serveru

a informace se v rámci tohoto systému rozdistribuují prostřednictvím jednotlivých uživatelů.

2.1.1 Transakce s bitcoinem

Jak již bylo uvedeno, kryptoaktivum bitcoin je obsaženo v transakcích, které defacto informují celou síť, že vlastník konkrétního bitcoinu (či jeho části) ho převedl na vlastníka nového. Ten může bitcoin převádět dál. Každá nová transakce je složená ze vstupů a z výstupů. Vstupy znamenají kryptoaktiva v majetku převodce (na jeho adresách), které použije na výstupy, tedy pro převod do vlastnictví (na adresy) nového vlastníka. Dalšími výstupy mohou být transakční poplatky (incentiva, která získají vítězní těžaři, viz podkapitola 2.2.3 k těžení), nebo vrácení rozměněných kryptoaktiv zpět na adresu původního vlastníka. Zjednodušeně řečeno transakce převádějí hodnotu z transakčních vstupů do transakčních výstupů. Výstupy jedné transakce jsou použity jako vstupy transakce následující.

2.2.2 Odeslání transakce do sítě

Každá transakce má 258 bytů a po jejím vytvoření je odeslána do sítě, kde je následně ověřena a zaevidována na blockchain. Bitcoinová síť je druh peer-to-peer sítě, tzn. že každý uživatel této sítě je připojen hned k několika dalším uživatelům sítě, tzv. uzlům sítě. Transakce je odeslána z jednoho uzlu sítě k nejbližším uzlům, které tuto transakci posílají dalším uzlům, jež tuto transakci ještě neobdržely. Toto posílání transakcí se nazývá zaplavování (angl. „flooding“) a během několika sekund je transakce doručena k většině uzlů v síti. Každý uzel sítě transakci řádně ověří předtím, než ji odešle dál, a zároveň ji uloží do úložiště (tzv. memory pool), kde je zařazená mezi transakce čekající na zařazení do bloku.

2.2.3 Těžení a mechanismus konsenzu

Transakce se ověří prostřednictvím procesu, který se nazývá těžení (angl. „mining“), jehož výsledkem je zařazení ověřené transakce do bloku blockchainu Bitcoinu (Lewis 2018). Právě v těžení spočívá mechanismus konsenzu Bitcoinu, tzv. proof-of-work.

Proces těžení má dvojí smysl – jednak ověřuje transakce, čímž zamezuje duplikaci či jinému zneužití transakcí a nahrazuje funkci centrální ověřovací autority, zároveň vytváří nové bitcoiny, jako to dělá centrální banka, když vytváří peníze. Je třeba zdůraznit, že hlavním smyslem těžení je právě ověřování transakcí a nové bitcoiny a poplatky slouží jako pobídka pro uživatele sítě, tzv. těžaře, kteří transakce ověřují.

Jednotky bitcoinu se tedy vytvářejí prostřednictvím těžení, kde tzv. těžaři (někteří uživatelé sítě) mezi sebou soupeří v hledání řešení matematické úlohy a zároveň přitom zpracovávají transakce s bitcoiny, za což jsou odměňováni nově vytěženými bitcoiny a poplatky za transakce, k čemuž dochází přibližně každých deset minut, kdy vítězný těžař zjednodušeně řečeno ověří transakce za posledních 10 minut. Protokol bitcoinu rovněž obsahuje algoritmus, který reguluje těžební funkci v podobě obtížnosti řešené matematické úlohy tak, aby docházelo pravidelně k vytěžení nových bitcoinů jednou za deset minut. Protokol rovněž půlí množství bitcoinů vytěžených jednou za 4 roky a je omezen na celkový počet vytěžených bitcoinů na 21 milionů, k čemuž má dojít v roce 2140. Vzhledem k velkému počtu těžařů a složitosti řešené úlohy je těžení energeticky velmi náročné, proto se těžaři organizují do tzv. poolů (angl. pool), ve kterých společně řeší úlohu a dělí si odměnu.

Matematická úloha, kterou se těžaři každých deset minut snaží vyřešit, se nazývá „Proof-of-Work“ a spočívá v hashování hlavy bloku blockchainu a náhodného čísla prostřednictvím SHA256 kryptografického algoritmu do chvíle, kdy je nalezeno řešení odpovídající požadovanému řešenému vzoru. Vítěz této úlohy oznámí nový blok blockchainu do celé sítě Bitcoinu, kde ho ostatní uživatelé jednoduše ověří a přiřadí na konec svého blockchainu.

2.2.4 Bitcoin Core

Bitcoin Core je open source projekt vytvořený komunitou dobrovolníků, jehož kód v programovacím jazyce C++ je volně dostupný na webu.[8] Jedná se o referenční implementaci systému Bitcoin, tzn. že stanoví, jak by každá část Bitcoinu (blockchain, ověřování, peněženky apod.) měla být implementovaná, a typicky funguje jako client (uzel Bitcoinu). Vedle Bitcoin Core existují i další implementace, a to i v jiných programovacích jazycích.

2.2.5 Klíče a adresy

Bitcoin je založený na kryptografii, což je druh matematiky, který se využívá v počítačové bezpečnosti typicky prostřednictvím šifrování textu. Kryptografie se u Bitcoinu používá především pro ověření znalosti tajné informace, aniž by tajná informace byla odhalena (tzv. digitální podpis), či pro ověření autentičnosti údajů (tzv. digitální otisk). Vlastnictví bitcoinu je realizováno prostřednictvím bitcoinových adres, digitálních klíčů a digitálních podpisů.

Digitální klíče představují čísla, která vytvářením digitálního podpisu a digitálních otisků umožňují nakládání s bitcoiny, typicky umožňují jejich prodej a nákup. Digitální klíče tvoří pár, když první z nich se nazývá soukromým a druhý veřejným klíčem. Digitální klíče jsou typicky uloženy ve složkách uživatelů či v jednoduché databázi, tzv. peněžence (angl. „wallet“). Veřejný klíč je matematicky odvozený prostřednictvím funkce násobení eliptické křivky ze soukromého klíče, z něhož ovšem nelze dovodit veřejný klíč. Veřejný klíč se používá k přijímání bitcoinů a soukromý klíč se používá k odesílání či útratě bitcoinů, neboť se jím digitálně podepisují transakce. Kdo drží soukromý klíč, může nakládat s příslušnými bitcoiny, proto se tento klíč nezveřejňuje či nesděluje a používá se místo toho veřejný klíč a digitální podpis, jež mají

[8] https://bitcoin.org/en/bitcoin-core/

funkci demonstrovat, že jejich držitel disponuje soukromým klíčem. Při útratě bitcoinu vlastník předloží svůj veřejný klíč a digitální podpis (oba vytvořené ze soukromého klíče) do nové transakce, díky čemuž umožní každému v bitcoinové síti ověřit si jeho vlastnictví převáděných bitcoinů.

V rámci transakce je veřejný klíč zastoupený svým digitálním otiskem, tzv. bitcoinovou adresou, která je z něj zpravidla odvozená a představuje jediný údaj o příjemci bitcoinu, který plátce v rámci transakce vidí. Bitcoinová adresa reprezentuje příjemce bitcoinu a lze ji připodobnit k platebnímu šeku.

2.2.6 Peněženky

U Bitcoinu se termín peněženka používá pro datové struktury a slouží jako základní uživatelské prostředí, ve kterém jsou uloženy digitální klíče a v němž se s digitálními klíči rovněž nakládá, čímž se v důsledku nakládá s bitcoiny. Existují různé druhy peněženek, nejčastěji se dělí na peněženky softwarové a hardwarové. Softwarové peněženky jsou v digitální podobě ve formě aplikací, zatímco hardwarové peněženky jsou ve formě hardwaru, jako jsou speciální USB disky, kde jsou uloženy virtuální klíče umožňující podepisovat transakce.

2.2.7 UTXO

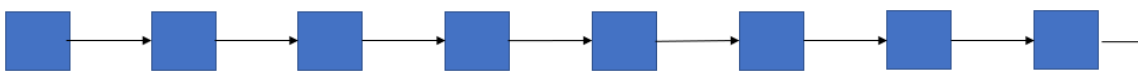
Důležitý pojem pro bitcoin je takzvané UTXO (angl. „unspent transaction output“, ve volném českém překladu „výstup nevyčerpaných transakcí“), což znamená všechny dostupné a utratitelné výstupy transakcí. Součet všech UTXO, tzv. UTXO set, se rovná součtu existujících bitcoinů. UTXO je významné zejména vzhledem k pohledu evidence transakcí, když tzv. bitcoinové peněženky vypočítávají aktuální zůstatek uživatele skenováním blockchainu a agregací hodnoty všech UTXO, které může peněženka utratit pomocí digitálních klíčů, jimiž uživatel v peněžence disponuje. Zůstatek se v Bitcoinu vypočítává prostřednictvím transakcí, a nikoliv prostřednictvím účtů, jako je tomu např. u Etherea, jak bude popsáno níže v kapitole 2.2.1.

2.2.8 Bitcoinová síť

Bitcoin je peer-to-peer síťová architektura fungující na internetu, kde není žádný centralizovaný server, uzly (uživatelé) si jsou rovné a síť je otevřená pro další uzly. Ačkoliv si jsou uzly rovné, mohou zároveň mít v síti odlišné role vzhledem k funkcionalitě, které v rámci sítě vykonávají. Uzel, který vykonává všechny funkcionality Bitcoinu, jimiž jsou směrování dat při přenosu v síti (routing), správa blockchainové databáze, těžba bitcoinů a funkcionalita peněženky, se nazývá plný uzel (angl. „full node“). Většina uzlů bitcoinové sítě ovšem zastává jen některé funkce, což je důležitý poznatek i pro praktickou část mé práce, tedy že jednotliví uživatelé prostřednictvím uzlů mohou vykonávat specifické funkce.

2.2.9 Blockchain

Bitcoin používá druh DLT, který se nazývá blockchain, jedná se o nejznámější dosavadní realizaci DLT. Datová struktura blockchainu tvoří uspořádaný, zpětně propojený seznam bloků a transakcí. Blockchain může mít podobu prostého souboru nebo jednoduché databáze (např. dle Bitcoin Core LevelDB databáze). Každý blok obsahuje transakce (zpravidla ale ne pouze za určité období) a je zpětně propojený s předchozím blokem, tzv. rodičovským blokem (angl. parent block) Jde tedy o blok, který vznikl deset minut před vznikem nově napojeného bloku, čímž nám vzniká řetězec bloků, angl. blockchain, jak je ilustrováno na obrázku 3, kde modré čtverce představují jednotlivé bloky a šipky ukazují chronologické pořadí těchto bloků.



Obrázek 3 – Schéma blockchainu

Každý blok lze identifikovat prostřednictvím haše (angl. hash), což je výstup vzniklý matematickou hashovací funkcí nazvanou SHA256, která převádí vstupní data do re-

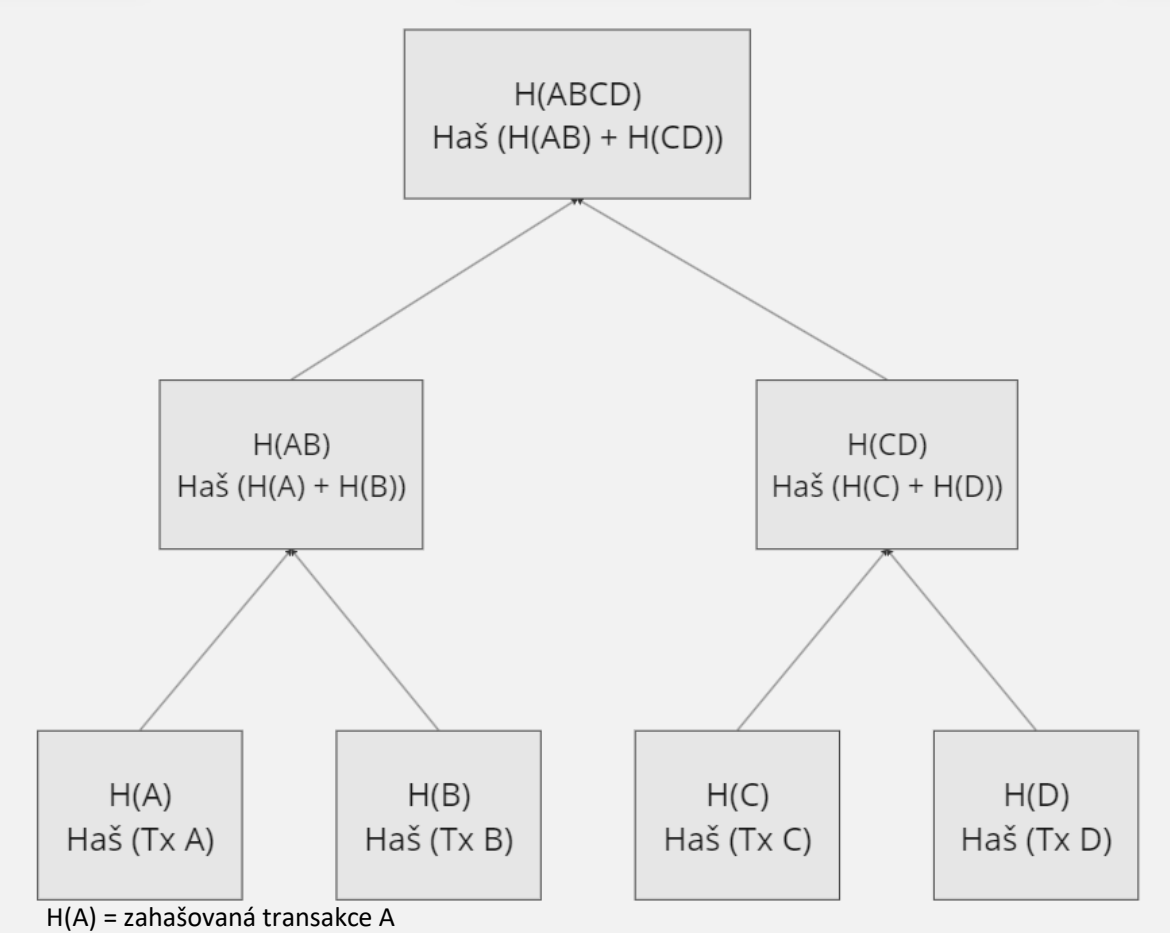
lativně malých čísel. Identifikační haš každého bloku nalezneme v jeho hlavě. Například haš prvního vytěženého bloku je 000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f.
Každý blok má 4 části, údaj o velikosti bloku, údaj o počtu transakcí v bloku, hlavu s identifikačními údaji o bloku, transakce daného bloku, kdy průměrný blok obsahuje 1900 transakcí.

V hlavě bloku nalezneme především haš tohoto bloku a haš rodičovského bloku (tato vlastnost každé hlavy bloku nám vytváří pomyslný řetězec bloků). Haš každého bloku je mj. vypočítán ze svého obsahu, tzn. transakcí i z haše bloku svého rodiče. Jakmile bychom tedy změnili rodičovský blok, dojde ke změně všech navazujících bloků. Tato vlastnost vzhledem k velkému počtu bloků tvoří významnou vlastnost blockchainu, jeho nezměnitelnost.

Přestože každý blok má jen jednoho rodiče, může mít více navazujících bloků, tzv. dětí. Tato problematika vychází z distribuovaného charakteru blockchainu, když je pro něj typické, že se může rozvětvit, což nastává, když více těžařů vytěží téměř naráz nové bloky, což se nazývá rozvětvením (angl. forking). Náprava forkingu spočívá v protokolu Bitcoinu, který zajistí na základě daných pravidel, že se uživatelé v průběhu času synchronizují a určí pouze jednu větev, kterou jeho uživatelé budou používat. K synchronizaci dochází zpravidla již v průběhu následujícího těžení, když nově vytěžený blok určí vítěznou větev, neboť delší validní větev má přednost před větví kratší. Zajímavé je, že situace, kdy současně existuje několik větví blockchainu, je systémem Bitcoinu brána jako validní do chvíle, než se uživatelé synchronizují.

Každý blok v blockchainu obsahuje souhrn všech transakcí v bloku prostřednictvím tzv. Merkleova stromu, což je struktura dat, která se používá nejenom jako souhrn všech transakcí, ale i k usnadnění ověřování transakcí za pomoci SHA256 hašovací funkce. Když každá transakce v bloku je zahašovaná samostatně, následně zahašovaná s hašem další transakce, následně zahašovaná s hašem dalších dvou transakcí, které byly předtím zahašované samostatně a tak dále, až vznikne jediný haš, tzv. Merkelův kořen (angl. Merkle root). Názorně je to ukázáno na obrázku 4. Díky Merkelově

stromu nemusíme znát všechny transakce, ale pouze několik hašů, abychom ověřili, že konkrétní transakce je součástí daného bloku, což významně sníží nároky na výpočet ověřování transakcí.



Obrázek 4 – Schéma Merkleova stromu

2.2 Vysvětlení technologické podstaty sítě Ethereum

Platforma Ethereum byla uvedená do provozu v roce 2015, kdy byl vytěžen její první blok, a technologicky navazuje na síť Bitcoin, proto se v následující kapitole pokusím vysvětlit především její odlišnosti od Bitcoinu. V této kapitole čerpám z publikace nazvané Mastering Ethereum: Building smart contracts and DApps (Antonopoulos a Wood 2019), pokud neuvádím jinak. Ethereum se liší od Bitcoinu zejména účelem, který je mnohem širší, jedná se o platformu umožňující ostatním uživatelům vytvářet

a ukládat různorodá data (vedle vlastního kryptoaktiva ether), a plní tedy hned několik funkcí, neomezuje se pouze na převod jediného kryptoaktiva jako Bitcoin. Ethereum je rovněž schopné načíst kód do svého stavového automatu a spustit tento kód, přičemž výsledné změny stavu uloží do svého blockchainu, touto funkcionalitou připomíná univerzální počítač (dále jen výpočetní funkcionalita Etherea). Ethereum tedy funguje jako decentralizovaný počítač, tzv. virtuální počítač Ethereum (angl. Ethereum Virtual Machine). Ethereum rovněž slouží jako platforma pro tvorbu decentralizovaných aplikací (dále jen „*DApps*“).

2.2.1 Účty

Odlišností Etherea od Bitcoinu je mimo jiné systém založený na účtech, neboť Bitcoin se zakládá na jednotlivých transakcích s UTXO namísto vedení účtů (více k UTXO viz kapitola 2.2.7). V Ethereu existují dva typy účtů, tzv. externě vlastněné účty (angl. „externally owned accounts“), ke kterým přísluší soukromý klíč, jehož držitel má přístup ke kryptoaktivům a smluvním účtům spojených s takovým účtem (viz dále).

Druhým druhem účtu je smluvní účet (angl. „contract account“). Smluvní účty jsou specifické tím, že obsahují kódy se smartkontrakty (druh aplikace), je s nimi spojené datové úložiště a nevztahuje se k nim žádný soukromý klíč. Místo soukromého klíče jsou tyto smluvní účty ovládány logikou svého smartkontraktu, což je aplikace vykonatelná prostřednictvím výpočetní funkcionality Etherea.

Oba typy účtů disponují adresami, na které mohou přijímat transakce, oba rovněž mohou přijímat a odesílat ether. Pokud je však cílem transakcí adresa smluvního účtu, tato transakce se vykoná prostřednictvím výpočetní funkcionality Etherea. Transakce u Etherea mohou kromě samotného kryptoaktiva ether obsahovat rovněž data, která fungují jako parametry pro funkce obsažené ve smartkontraktech u smluvních účtů, které se odesláním transakce vykonají.

Zahájit transakce mohou pouze externě vlastněné účty, smluvní účty mohou oproti tomu reagovat na ty transakce, které z externě vlastněných účtů směřují vůči nim

spuštěním dalších smluvních účtů, čímž se vytvoří pomyslný řetězec provedení smart-kontraktů.

2.2.2 Transakce

Transakce jsou zprávy podepsané digitálními klíči vzniklé v externě vlastněných účtech, které se posílají v Ethereu (konkrétně v jeho síti) a zaznamenávají se na jeho blockchainu. Jako klasický příklad transakce lze uvést převod etheru. Transakce jsou de facto hybnou silou měnící stavový automat Etherea, tzn. prostřednictvím transakcí se Ethereum „spouští, vykonává výpočetní úlohy a mění zápisy na blockchainu“. Nejvýznamnější částí jednotlivé transakce u Etherea je tzv. nonce, což je číselná hodnota, která udává počet odeslaných transakcí z adresy odesílatele transakce. Nonce slouží zároveň jako údaj o tom, kolikátá v pořadí těchto odeslaných transakcí je příslušná transakce. Nonce je významná ze dvou důvodů, chrání před duplicitou transakcí, neboť každá transakce z konkrétní adresy má jedinečnou nonci a zároveň udává pořadí vykonatelnosti transakcí, což je užitečné v případě, když chceme nějakou prioritizovat. Nonce je klíčovou funkcionalitou systému založeného na účtech Etherea, a proto tato funkcionalita není u Bitcoinu, který je, jak už bylo popsáno, založený na jednotlivých transakcích s UTXO.

Transakce dále obsahují adresu jejich příjemce či údaj o tom, kolik za ně bylo zaplaceno. Po provedení transakce se vytvoří tzv. účtenka (angl. receipt), kde jsou záznamy o jejím provedení, jež mohou dále sloužit jako informace například pro DApps.

2.2.3 Gas

Specifikou Etherea je gas, což je vedle etheru další nativní kryptoaktivum platformy Ethereum, sloužící k zaplacení poplatků za transakci. Gas je odlišen od etheru, aby se vyvaroval jeho potenciální volatilitě a rovněž aby s ním bylo možné lépe hradit náklady na výpočetní kapacity Etherea. Gas má vůči etheru vlastní kurz. V rámci transakce uživatel vyplní cenu, kterou je ochoten zaplatit etherem za gas, když platí, že čím vyšší cena, tím dříve se transakce zpracuje. Lze ovšem stanovit nulovou cenu za gas a i ta bude zpracována, a to typicky v období, kdy existuje málo transakcí če-

kajících na zpracování. Dále lze v transakci nastavit limit, kolik gasu je uživatel ochoten zaplatit za transakci. Pro některé jednoduché transakce je cena stanovená fixně. Skutečná částka, která se zaplatí za transakci, může být nižší nežli ta uživatelem vyplněná, protože bude vždy záležet na faktorech, jako jsou náklady na výpočetní kapacity Etherea. Skutečná částka etheru zaplacená za gas se odečte z příslušného účtu po realizaci transakce. Zajímavé je, že gas limituje i velikost jednotlivých bloků na požadovanou hodnotu 15 milionů gas na jeden blok s tím, že maximální velikost jednoho bloku může být dvojnásobná, tedy 30 milionů gas (Smith 2023).

2.2.4 Smartkontrakty

Smartkontrakty jsou aplikace (synonymně lze použít i termín počítačové programy) obsažené ve smluvních účtech a vykonávané prostřednictvím výpočetní funkcionality Etherea. Je to její klíčová funkcionalita, a proto je vhodné uvést klíčové znaky smartkontraktů dle Antonopoulose a Wooda (2019):

a) *Počítačové programy – smartkontrakty jsou počítačové programy.*
b) *Nezměnitelnost – jakmile je kód smartkontraktu jednou zadán do smluvního účtu, nelze ho změnit. A jedinou možností, jak ho upravit, je prostřednictvím zadání nové instance kódu.*
c) *Determinismus – výsledek provedení smartkontraktu je totožný pro každého, kdo ho provádí, a to s ohledem na souvislosti transakce, která iniciovala provedení, a stav blockchainu v okamžiku provedení.*
d) *Kontext virtuálního počítače Ethereum (angl. Ethereum virtual machine) – smartkontrakty fungují s velmi omezenými souvislostmi jejich provedení. Mají přístup ke svému vlastnímu stavu, souvislostem transakce, která je vyvolala, a k některým informacím o nejnovějších blocích blockchainu.*
e) *Decentralizovaný světový počítač – Ethereum jako virtuální počítač pracuje jako lokální instance na každém svém uzlu, ale protože všechny instance tohoto virtuálního počítače fungují na stejném počátečním stavu a vytvářejí stejný konečný stav, systém jako celek funguje jako jeden „světový počítač“.*

Smartkontrakty jsou vytvářeny prostřednictvím speciálních transakcí do smluvních účtů a jejich původce nemá k nim ani k jejich účtům po jejich vytvoření žádná práva. Smartkontrakty jsou následně zaevidovány ve smluvních účtech na blockchainu a čekají na své spuštění či vykonání. Výše bylo uvedeno, že smartkontrakty jsou spuštěny transakcemi z externě vlastněných účtů, nebo prostřednictvím jiného smartkontraktu ve smluvním účtu. Smartkontrakt sám sebe nikdy nespustí.

2.2.5 Tokeny

Tokeny jsou jednotky kryptoaktiv a na platformě Etherea mohou mít různorodou podobu, může se jednat o převodní token, jako je ether, token může rovněž představovat právo, jako je hlasovací právo, přístup k aplikaci apod. Jeden token může plnit rovněž několik funkcí. Přesto Antonopoulos a Wood upozorňují na významnou odlišnost mezi etherem a ostatními tokeny na Ethereu, neboť ether je nativním tokenem Etherea a Ethereum s ním explicitně počítá ve svém protokolu, například při platbách za transakce. Naproti tomu ostatní tokeny protokol Etherea explicitně nezná a neupravuje, jen je umožňuje naprogramovat do smartkontraktů. Proto dále i já budu v rámci Etherea rozlišovat mezi etherem a ostatními tokeny, které nadále nazývám „tokeny“.

V roce 2015 byl uveden standard tokenu ERC20 pro zastupitelné tokeny, který dodnes využívá většina tokenů na Ethereu. Tento standard popisuje společné rozhraní obsahující funkce (např. pro převod, autorizace, získání informací o tokenu) pro smartkontrakty implementující takové tokeny. Právě invence ERC20 tokenů stála za ohromným rozmachem kryptoaktiv prostřednictvím ICO, jak popisuji v kapitole 1.1.4, když mnoho projektů s kryptoaktivy si začalo vydávat své tokeny právě prostřednictvím tohoto standardu.
Dalším významných standardem tokenu na Ethereu je ERC721, na jehož základě vznikají nezastupitelné tokeny známé pod zkratkou NFT (angl. „non fungible tokens“).

2.2.6 Orákulum

Orákula jsou systémy či aplikace, které poskytují externí zdroje dat smartkontraktům Etherea. Mohou poskytovat informace o ceně stříbra, vývoji počasí či o výsledků fotbalového zápasu, které by se jinak neměly na Ethereum jak dostat. Orákula nejprve sesbírají data od svého zdroje, následně je prostřednictvím podepsané zprávy zašlou do úložiště příslušného smartkontraktu na Ethereu, odkud jsou data dostupná dalším smartkontraktům. Do smartkontraktu lze nahrát všechna potřebná data (například věk studentů) nebo lze vytvořit orákulum, které data průběžně aktualizuje (např. data o počasí). Jedním z nejznámějších poskytovatelů orákul je Chainlink, který se poskytovaná data snaží ověřovat z více zdrojů. Jako příklad využití orákula si můžeme představit sázku o vítězi fotbalového utkání uzavřenou prostřednictvím smartkontraktu. Informaci o vítězi daného zápasu získá smartkontrakt prostřednictvím orákula. Smartkontrakt po získání informace od orákula odešle výhru na daný účet výherce.

2.2.7 DApps

DApps jsou webové aplikace, které jsou vytvořené za účelem interakce s Ethereem a jsou typicky tvořené ze smartkontraktů, pokrývajících alespoň část backendového řešení aplikace (celé backendové řešení prostřednictvím smartkontraktů by bylo příliš nákladné) a frontendového uživatelského rozhraní, v jehož rámci lze použít standardní programovací jazyky a rozhraní, jako jsou JavaScript, CSS, HTML apod. Frontendové řešení je propojeno s Ethereem prostřednictvím javascriptové knihovny web3.js, která je poskytována prohlížeči webovým serverem. Jako příklady (Ethereum.org [b.r.]) DApps lze uvést například Uniswap, což je směnárna tokenů, hru Dark Forrest či tržiště s digitálním uměním a módou Foundation.

2.2.8 Mechanismus konsenzu

Termín konsensuální mechanismus se vztahuje na celý soubor protokolů, které umožňují síti uzlů dohodnout se na stavu blockchainu Etherea. Oproti Bitcoinu, který používá proof-of-work mechanismus, používá Ethereum mechanismus proof-of-stake,

na který přešlo z právě z proof-of-work mechanismu v roce 2022 z důvodů větší bezpečnosti kvůli implementaci pokut za porušení pravidel protokolu, menší energetické náročnosti, neboť v něm není třeba řešit složité matematické úlohy, a protože je vhodnější pro účely škálovatelnosti samotného Etherea. Ethereum využívá proof-of-stake prostřednictvím vložení aktiv validátora v podobě etheru do smartkontraktu (tento proces se nazývá stakingem, angl. *staking*). Tento vložený ether do smartkontraktu pak funguje jako zástava, která může být zničena, pokud se validátor chová nečestně či pasivně (neověřuje). Validátor je zodpovědný za ověřování, tzn. ověřuje, zda jsou nově distribuované bloky po síti platné, a sám rovněž může vytvářet a distribuovat nové bloky.

Aby uživatel mohl být validátorem, musí vložit 32 etherů do smartkontraktu a spustit příslušný software. Následně je uživatel zařazen do fronty validátorů, jejímž smyslem je omezovat vznik nových validátorů. Jakmile je uživatel potvrzen jako validátor, začne ověřovat nové bloky, tedy že mají příslušné náležitosti a jsou platné, což stvrdí svým hlasem ve prospěch tohoto bloku. Oproti mechanismu u Bitcoinu se u Etherea každý blok vytěží za 12 vteřin. Z hlediska času se těžení bloků dělí do slotů (každý má 12 vteřin) a epoch (každá má 32 slotů). Pro každý slot je validátor náhodně vybrán, aby vytvořil, navrhl a následně odeslal do sítě nový blok. Zároveň je pro každý slot vybrán výbor validátorů, kteří potvrzují nové bloky (Kashyap 2023). Obdobně jako u Bitcoinu dostávají validátoři za svou účast při validaci odměnu v podobě etherů, při vytváření bloků může rovněž vznikat forking, tzn. více větví bloků, který je vyřešen vždy ve prospěch většího počtu hlasů validátorů pro bloky v dané větvi.

2.3 Druhy DLT

V předchozích kapitolách jsem již uvedl základní popis DLT technologie, zejména jejího nejznámějšího druhu, blockchainu. V této kapitole se pokusím uvedené informace dále rozvést a rovněž popsat i další druhy DLT technologie.

DLT technologii lze rozdělit na několik typů a základním rozlišením je způsob, jak jsou dané záznamy v DLT technologii evidovány. Pokud architektura záznamů jdoucích

chronologicky za sebou tvoří řetězec bloků, potom hovoříme o tzv. blockchainu, což je nejznámější a nejčetněji zastoupená kategorie DLT. Dalšími důležitými druhy DLT jsou Directed Acyclic Graphs, Hashgraph, Holochain, Tempo.

2.3.1 Blockchain

V předchozích kapitolách jsem popisoval funkcionalitu blockchainu Bitcoinu a Etherea, v této kapitole popíšu několik hlavních druhů samotného blockchainu. Bashir (Bashir 2023) rozlišuje mezi následujícími blockchainy:

1. Soukromý blockchain – jedná se o druh blockchainu, který je přístupný pouze omezenému počtu osob, mezi známé příklady těchto blockchainů patří Hyperledger Fabric anebo Quorum. Samozřejmě je možné z nich udělat veřejné blockchainy.
2. Veřejný blockchain – veřejné blockchainy nikdo nevlastní a jejich uživatelem může být kdokoliv, například Bitcoin či Ethereum.
3. Polosoukromý blockchain – jedná se o hybridní modely využití charakteristik soukromého a veřejného blockchainu. Dle Bashira (2023) žádný takový blockchain doposud reálně neexistuje. Může jít například o příklad, kdy by jeho část byla soukromá a část veřejná, nebo by byl blockchain kontrolovaný jedinou autoritou, ale umožňoval by připojení ostatních. Podle mého názoru by jako takový příklad šlo uvést katastr nemovitostí pod kontrolou katastrálního úřadu, ale s možným napojením ostatních osob, jako jsou vkladatelé.
4. Povolovaný blockchain – jedná se o blockchain, jehož účastníci jsou ověření a důvěryhodní, proto zde není třeba mechanismu konsensu, jako je těžení, ale jen protokol založený na souhlasu těchto ověřených osob. Tento blockchain může být soukromý i veřejný.
5. Plně soukromý a vlastněný blockchain – takový blockchain by mohl existovat uvnitř soukromé či veřejné organizace, například pro sdílení informací mezi státními orgány, opět vzhledem k věrohodnosti účastníků takového blockchainu by bylo možné nahradit mechanismus konsenzu algoritmem založeném na prostém souhlasu či obdobném jednodušším procesu.

Významné je dělení blockchainu z hlediska monolitické struktury, kde všechny funkcionality daného blockchainu jsou jeho součástí, jako je Bitcoin, a polylitické struktury, jako je Polkadot, Avalanche, které jsou typické existencí různých blockchainů provázaných s hlavním blockchainem a společně formující tzv. mnohořetězové sítě. Pokud jsou tyto řetězce stejné a podléhají stejným pravidlům, nazývají se homogenní, pokud naopak, pak se nazývají heterogenní.

Závěrem je třeba rovněž popsat blockchainy s druhou vrstvou, což jsou ty, jež používají některé funkcionality základního blockchainu, jako jsou vypořádání a evidence, ale jinak používají vlastní funkcionality. Typickým příkladem jsou tzv. sidechainy, které umožňují směny kryptoaktiv z různých blockchainů. Například sidechain Rootstock umožňuje vytváření smartkontraktů pro Bitcoin, což by na samotném blockchainu Bitcoinu nebylo možné.

V souvislosti s praktickou částí je třeba zmínit Hyperledger, což je projekt iniciovaný konsorciem Linux Foundation za účelem technologického rozvoje DLT, a to prostřednictvím knihoven, nástrojů, programovacích nástrojů a samotného DLT. V rámci Hyperledgeru se inovují všechny druhy DLT, a to včetně blockchainu, z nichž je nejznámější povolovaný blockchain Hyperledger fabric od společností IBM a Digital Asset Holdings založený na modulární a zásuvné architektuře spočívající v možnosti přidávání jednotlivých prvků do blockchainu dle požadavku uživatele či klienta. Mezi takové prvky patří identifikace, přístupová práva, druhy smartkontraktů, podoba transakcí, bezpečnost, způsob ukládání dat či mechanismu konsensu.

2.3.2 Directed Acyclic Graph

Directed acyclic graph nebo orientovaný acyklický graf (dále jen „DAG“) je významným, protože do této kategorie lze zařadit soukromé DLT Corda od společnosti R3, jenž používá mnoho subjektů na finančním trhu (více viz praktická část mé práce). DAG lze odlišit od blockchainu především v rámci návaznosti bloků a transakcí (Bybit Learn 2022). Zatímco blockchain je neměnný lineární řetězec ověřených bloků dat a těch dat a bloků, které stále čekají na ověření, v případě DAGu se jedná o řetězec

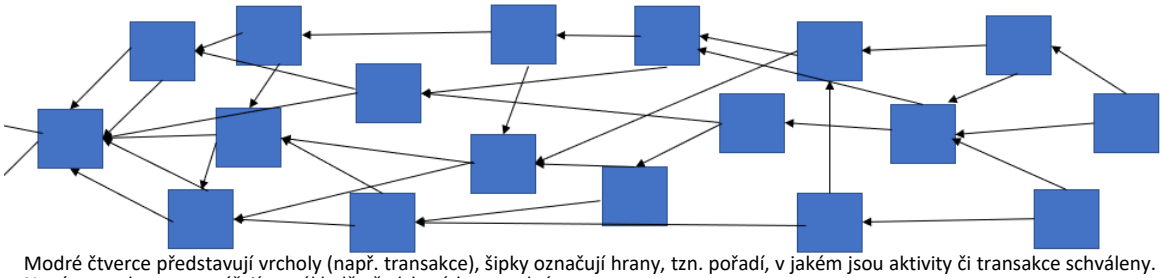
individuálně ověřených transakcí, které jsou navázané na mnoho předchozích transakcí (existují i studie využití bloků transakcí v rámci DLT DAG (Sompolinsky et al. 2018)). DAG se skládá z tzv. vrcholů, které mohou představovat aktivity jako například transakce a z hran představující pořadí, v jakém jsou aktivity či transakce schváleny. Nové transakce se vytvářejí na základě předchozích transakcí. Že je DAG orientovaný, znamená, že se hrany a vrcholy pohybují pouze jedním směrem, a acyklický znamená, že neobsahuje žádné cykly, tedy není zde možnost přesunu zpět na předchozí transakce z aktuální transakce.

Struktura DAGu umožňuje paralelní vytváření a potvrzování transakcí, což v důsledku umožňuje zpracování velkého počtu transakcí. Zároveň je pro DAG charakteristický velmi omezený mechanismus konsensu ve formě proof-of-work, což by mělo činit toto DLT méně nákladným.

Jako jednoduchý příklad DAGu lze uvést transakci v DAGu Tangle od společnosti Iota Foundation (Bhandary et al. 2020). Uživatel A vytvoří transakci. V rámci této transakce musí uživatel A ověřit dvě jiné předcházející transakce vybrané na základě algoritmu, čímž dojde k jejich zkontrolování, potvrzení a vepsání odkazu na ně do nové transakce uživatele A. Transakce uživatele A je následně potvrzena transakcí uživatele B, který ji ověří a také na ni odkáže. Problematika dvojí útraty je prostřednictvím DAGu řešená tak, že každá nová transakce je zkontrolovaná až do prvotní transakce jejího odesílatele. Četněji ověřené transakce mají rovněž vyšší váhu (uváděnou v procentech). Pokud při ověřování transakcí dojde určitý uživatel ke zjištění, že některá transakce byla chybná, nepotvrdí ji a nebude na ni jeho transakcí odkázáno. V rámci DAGu se neplatí žádné poplatky za transakce, neboť transakce je fakticky zaplacená náklady za výpočetní výkon při jejím ověřování. Tato skutečnost je vhodná zejména pro mikrotransakce.

Zajímavé je, že všechny nativní tokeny v DAGu Tangle sítě společnosti IOTA Foundation byly vydány úplně na začátku v rámci první transakce, tzv. „genesis transakce“. Vzhledem k riziku, že potenciální podvodník by mohl začít vytvářet velké množství

podvodných transakcí, což by mohlo významně narušit síť, byl zaveden speciální klient (uzel) sítě nazvaný koordinátor, jehož provozuje přímo IOTA Foundation, vytvářející každé dvě minuty tzv. milníkové transakce, které přímo i nepřímo potvrzují ostatní transakce a mají 100procentní váhu v síti. Existence koordinátora jako autority stvrzující transakce je určitým centralizovaným prvkem v distribuované architektuře, proto se v rámci projektu uvažuje o jeho odstranění (Beran 2019).



Modré čtverce představují vrcholy (např. transakce), šipky označují hrany, tzn. pořadí, v jakém jsou aktivity či transakce schváleny. Nové transakce se vytvářejí na základě předchozích transakcí.

Obrázek 5 – Schéma DLT DAG

Dalším významným zástupcem DAG je Hashraph od společnosti Swirlds, který vznikl už v roce 2016 (Baird 2016). Hashgraph je specifický tím, že používá tzv. „gossip about gossip“ protokol a algoritmus založený na konsensu pomocí virtuálního hlasování. Gossip about gossip protokol, který lze volně přeložit jako „klepy o klepech“, spočívá v tom, že uživatel si náhodně vybere jiného uživatele, kterému předá všechny informace, jimiž disponuje, respektive ty, které druhý uživatel nemá, což se následně opakuje. Uživatelé si neposílají pouze informace o tom, co vědí, ale i informace o tom, jakými informacemi disponují ostatní uživatelé sítě, kdy tyto informace obdrželi a od koho, tzv. klepy o klepech, odtud název samotného protokolu. Jedná se o soukromé DLT, takže je přístupné jen omezenému počtu autorizovaných uživatelů a každému uživateli je známa identita všech ostatních uživatelů (Akhtar 2023).

Transakce jsou v rámci sítě Hashraph součástí událostí, jež mají velikost několika bytů, a nemusí obsahovat pouze transakce. Každá transakce obsahuje časové označení svého vzniku, haš předchozí transakce tvůrce nové transakce a haš transakce,

která byla právě odeslána tvůrci nové transakce k ověření, dále příslušné nově vytvořené transakce a digitální podpis tvůrce transakce. Po vytvoření transakce gossip protokol náhodně předává informace o události ostatním uživatelům. Haše o transakcích předcházející nové transakci vytvářejí architekturu DAGu sítě Hashgraph a umožňují ostatním uživatelům poznat historii nové transakce. Například tvůrce transakce vytvoří transakci v čase t = 0, odešle ji dalšímu uživateli v čase t = 1, ten ji odešle s tvůrcem dál v čase t = 2 dvěma uživatelům, všichni, kdo transakci znají, ji odešlou dál v čase t = 3 čtyřem uživatelům, lze tedy vypočítat, že informace se rozdistribuuje exponenciálně mezi n uživatelů v celé v síti v čase vyjádřeném jako t = Log(n). Transakce, se kterými souhlasí prostřednictvím virtuálního hlasování více jak 2/3 uživatelů sítě, jsou pokládány za validní. Uživatelé se prostřednictvím hlasování konkrétně shodují na pořadí transakcí a dalších událostí v síti. Z toho lze vyvodit, že aby síť fungovala, může mít maximálně jednu třetinu nepřátelských uživatelů, a to ještě ověřených, což se jeví jako nevýhoda například v porovnání se sítí Bitcoin. Mezi výhody Hashgraphu patří, že je schopný zpracovat velké množství transakcí a není náročný na přenos velkého množství dat vzhledem k velké kompresi. Údaje o hlasování se nezasílají mezi uživateli, neboť jednotliví uživatelé si sami spočítají, jak hlasovali ostatní uživatelé vzhledem k tomu, že disponují všemi informacemi, jimiž disponují oni sami.

2.3.3 Holochain

Na úvod je nezbytné podotknout, že DLT typu Holochain od nadace Holochain Foundation je stále ve vývoji. V centru Holochainu jsou samotné uzly, tedy uživatelé, a nikoliv data obsažená například v distribuovaném blockchainu, jejichž stav vyžaduje konsenzus celé sítě. V rámci Holochainu má každý jeho účastník svůj registr, který autonomně spravuje, a bezpečnost na něm uložených dat je zajištěna kryptografií (Holochain Foundation [b.r.]). V Holochainu oproti jiným DLT neexistuje globální stav a účastníci nemají na svém registru data všech ostatních účastníků, jako je tomu například u blockchainu, ale každý uživatel má svůj registr a v rámci něj má svůj lokální datový stav, když může sdílet s ostatními účastníky jen jím zvolená data. Zároveň v rámci Holochainu neexistuje globální ověřovací proces, ale celá síť má soustavu

pravidel, která se nazývá „DNA“. Uživatelé mezi sebou používají aplikace prostřednictvím jednotlivých uzlů. Holochain je vyvíjen, aby na něm fungovaly například aplikace pro dodavatelské řetězce, nástroje pro týmovou produktivitu, cloudová úložiště pro osobní data, finanční aplikace apod.

2.3.4 Tempo

Dle příslušných webových stránek (Radix Publishing Ltd. 2023) je Radix názvem jak pro decentralizovaný projekt různorodých společností, vývojářů apod., tak i pro ekosystém této komunity, protokol, software, síť a DLT. Komunita Radix vytvořila zkušební protokol a druh DLT nazvaný Tempo. Tempo vzniklo v důsledku omezené škálovatelnosti blockchainu, ale i DAG. Cílem vývojářů tedy bylo navrhnout DLT, které by bylo škálovatelné a bylo schopno zpracovat miliony transakcí za vteřinu a zároveň by bylo decentralizované a programovatelné, aby v něm bylo možné vytvářet decentralizované aplikace. Škálovatelnost se snižuje s častější komunikací jednotlivých uzlů mezi sebou, typicky uzly mezi sebou komunikují při schvalování transakcí.

První část koncepce Tempa vychází z tzv. střihání (angl. sharding), když je DLT rozděleno na několik částí (fragmentů, angl. shards), ve kterých komunikují jen některé uzly, což snižuje celkový objem mezi-uzlové komunikace. Druhá část koncepce Tempa vychází ze skutečnosti, že uzly automaticky schvalují všechny transakce, které jim přijdou, a komunikují navzájem dále jen v případě, když je transakce zpochybněná. Jedná se o koncept tzv. líného konsensu.

Tempo je jak protokol, tak DLT, jehož klíčovou funkcionalitou jsou konsenzus prostřednictvím tzv. logických hodin. Každý uzel má své počítadlo (své logické hodiny), které se zvyšuje s každým novým požadavkem (událostí), který přijme. Hodnota na počitadle se nikdy nesnižuje. Při ukládání požadavku uzel k této události připojí svou aktuální hodnotu logických hodin a teprve poté ji odesílá a šíří dál sítí mezi další uzly. Hodnota logických hodin přiřazená každým uzlem tvoří důkaz o času. Důkaz o času se používá v případě, kdy uzel přijme požadavek, který je v konfliktu s požadavkem, který obdržel dříve. Aby uzel rozhodl, který požadavek zruší, shromažďuje související důkazy o času od ostatních uzlů, aby si potvrdil, který požadavek přišel do sítě dříve.

Významná je rovněž důvěryhodnost jednotlivých uzlů, která je zajištěna mechanismem nazvaným závazek (angl. commitment) ve formě kryptografického haše (Radix Publishing Ltd. 2023).

První testování Tempa proběhlo v roce 2019 za účasti 1000 uzlů a podařilo se zprocesovat 1 milion transakcí za vteřinu. Zároveň vyšlo najevo několik nevýhod. Například se ukázalo, že každý požadavek může být kdykoliv zpochybněn a přepsán jiným požadavkem, což znamená, že algoritmus Tempa nezaručuje konečnost zpracování požadavků. Na Tempo Radix navázal dalším prototypem Cerberus, který je v provozu, ovšem zatím ve zjednodušené verzi.

PRAKTICKÁ ČÁST

3 Metodologie

V této části uvádím vědecko-výzkumné metody, které jsem využil ve své diplomové práci, abych splnil její cíle.

Pro sběr dat používám metodu práce jak s primárními, tak se sekundárními daty. Primární data definuji jako data bezprostředně získaná za účelem řešení mého výzkumného problému. Naopak sekundární data byla již za účelem řešení mého problému shromážděna například v publikacích mezinárodních orgánů.

Následně získaná data zpracovávám pomocí jak metody dedukce, tak metody indukce, tzn. že z obecné teze dedukuji konkrétní závěry a naopak, z konkrétní teze indukuji obecné závěry. Tyto metody používám v praktické části, když na základě sebraných dat stanovím kritéria pro posouzení využití jednotlivých reálných případů užití na finančním trhu v ČR. Tyto metody rovněž používám při samotném posouzení variant i pro stanovení závěrů diplomové práce.

Jako další jsem zvolil metodu komparace, a to i v obecné části, když například porovnávám jednotlivé druhy DLT, klady a zápory této technologie či srovnávám technickou stránku Bitcoinu a Etherea. V praktické části tvoří komparace rovněž stěžejní metodu, když porovnávám jednotlivé varianty reálných případů užití DLT dle daných kritérií či významnost samotných kritérií.

Při hodnocení variant reálných případů užití DLT dle daných kritérií používám rovněž metodu syntézy, tzn. že z několika údajů o dané variantě se snažím popsat a ohodnotit variantu komplexně jako celek. Syntézu využívám i v samotném závěru své práce.

Pro stanovení vah kritérií používám metodu, kterou vymyslel americký matematik L. H. Saaty, tzv. Saatyho metodu(Fotr a Švecová 2022), která se skládá ze dvou kroků. V rámci prvního kroku se nejprve zjistí preferenční vztahy pro každou dvojici kritérií, když se určí kromě směru preference jednoho kritéria i její velikost počtem bodů ze

zvolené bodové stupnice (např. 1–9). Ve druhé fázi Saatyho metody se stanoví váhy kritérií pomocí geometrického průměru jednotlivých preferenčních vztahů každého kritéria. K výsledným vahám dojdeme tak, že geometrické průměry znormujeme, tedy vydělíme součtem všech geometrických průměrů. Váhy normujeme proto, aby součet vah byl roven jedné a váhy byly lépe srovnatelné.

Pro samotný výběr nejvhodnější varianty reálných případů užití DLT dle daných kritérií pro finanční trh v ČR jsem rovněž vybral metodu L. H. Saatyho, kterou nazval analytický hierarchický proces, protože je dle odborné literatury (Fotr a Švecová 2022) *vhodná pro hodnocení variant při souboru kvalitativních kritérií, resp. v situacích se smíšeným souborem kritérií, kde kvalitativní kritéria převažují*. To je přesně případ i mého souboru kritérií v kapitole V. Předností této metody je rovněž jednoduchost a srozumitelnost pro uživatele.

Specifikem této metody je stanovení dílčích ohodnocení variant vzhledem k jednotlivým kritériím, které je analogické k výše popsané metodě pro stanovení vah kritérií s tím rozdílem, že srovnávané objekty nejsou kritéria, nýbrž varianty rozhodování.

Pro každé kritérium se vytvoří Saatyho matice na základě párového srovnání variant, při němž dojde k určení velikosti preference všech dvojic variant. Následně se určí pomocí Saatyho matice pro jednotlivá kritéria dílčí ohodnocení variant vzhledem k těmto kritériím, k čemuž se dospěje tak, že se 1) stanoví váhy variant pomocí geometrického průměru jednotlivých preferenčních vztahů každé varianty, 2) geometrické průměry znormujeme, tedy vydělíme součtem všech geometrických průměrů dané matice, čímž dostane preferenci dané varianty k danému kritériu, 3) preferenci následně vynásobíme vahou příslušného kritéria. Tímto třetím krokem dostaneme konečnou preferenci varianty k danému kritériu, tedy dílčí ohodnocení varianty. Všechna dílčí ohodnocení variant následně sečteme, čímž dostaneme celkové ohodnocení dané varianty.

4 Přehled významného využití DLT technologie v sektorech finančního trhu ve světě

V naprosté většině není DLT technologie na finančním trhu po celém světě zavedena do praxe, ale zůstává ve fázi studií, konceptů a prototypů. V této kapitole popisuje nejvýznamnější realizace a návrhy využití DLT technologie pro jednotlivé sektory finančního trhu. Pro sběr informací jsem použil veřejně dostupné informace publikované na webových stránkách světových a evropských mezinárodních organizací jako jsou Banka pro mezinárodní vypořádání či evropské orgány dohledu, univerzit a sdělovacích prostředků zabývajících se problematikou DLT ve finančnictví. Dle dostupných informací, mých předpokladů a zkušeností více reálných příkladů DLT technologie v praxi nebude.

4.1 Využití DLT technologie na kapitálovém trhu

Na kapitálovém trhu se DLT prosazuje velmi pomalu, když stále existuje jen několik reálných příkladů využití DLT. Tato skutečnost se ovšem může změnit v příštích letech v souvislosti s přijetím evropského nařízení MiCA a dalších regulací v ostatních státech, což by kromě právní jistoty mohlo přinést i větší důvěru zákazníků v tuto technologii.

4.1.1 Societe Generale-Forge

V roce 2023 oznámila společnost Societe Generale-FORGE (dále jen „SG Forge“) vydání vlastního stablecoinu navázaného na euro nazvanéEUR CoinVertible (Blemus 2023). SG-Forge je dceřinou společností francouzské finanční skupiny Societe Generale, jejímž klientům má být stablecoin nabízen. Do této skupiny patří i česká dceřiná společnost Societe Generale Komerční banka a. s., tudíž je možné, že i ta tento stablecoin bude nabízet i svým zákazníkům v ČR. Stablecoin bude vydaný na veřejném blockchainu Ethereum a má být určen pro institucionální zákazníky, jako jsou fondy či obchodníci s cennými papíry, kteří poskytují finanční služby pro své zákazníky. Prostřednictvím tohoto stablecoinu bude možné vypořádávat velké obchody s aktivy, inovativně řídit firemní finance (cash management, cash pooling apod.), poskytování

likvidity (například margin call u obchodníků s cennými papíry) a možnosti refinancování. SG-Forge má ve Francii licenci obchodníka s cennými papíry a poskytovatele služeb souvisejících s digitálními aktivy, což jí umožňuje vykonávat úschovu, obchodovat na účet zákazníka s těmito aktivy. Rezervu stablecoinů bude SG-Forge mít na účtech třetí strany (pravděpodobně samotné banky Societe Generale) ve fiat měnách a ve vysoce kvalitních a likvidních cenných papírech a bude dosahovat 100 procent vydaných stablecoinů, což zajistí cenovou stabilitu stablecoinu. Dle dostupných informací (Forge Societe Generale Group 2023) je zřejmé, že nový stablecoin je přímou reakcí na novou evropskou regulaci MiCA.

4.1.2 Agora

Agora je britská finančně technologická společnost zabývající se obchodováním na dluhopisovém trhu, jejíž softwarové aplikace běží na DLT Corda od společnosti R3 (R3 2021). Agora hledala řešení, jak modernizovat komunikační prostředí na dluhopisovém trhu, které stále používá komunikační prostředky, jako jsou telefonní hovory, chatování či e-mailová komunikace, což může mít za následek časovou prodlevu, manuální přepis dat či chybovost, přinášející v důsledku náklady. Agora původně chtěla používat řešení prostřednictvím centralizovaných databází, ale toto řešení nebylo vhodné pro potřeby synchronizovat data mezi stranami, které si vzájemně nedůvěřují a chtějí mít zároveň kontrolu při nakládání se svými daty. Následně chtěla Agora využít veřejné DLT jako například Ethereum, ale nelíbilo se jim nedostatečné nakládání s osobními údaji, správa identit uživatelů těchto systémů či nedostatečná míra stability jejich řízení. Nakonec řešení na výše uvedené požadavky našla u povolovaného (přístup k DLT mohou mít jen povolené subjekty) DLT Corda.

Agora prostřednictvím svých aplikací mj. umožňuje emitentům rychle strukturovat a emitovat své dluhopisy, prostřednictvím DLT Corda umožňuje synchronizovat transakce mezi dvěma stranami a digitálně je podepisovat, přičemž dochází k zabezpečení přístupu k jejich informacím a obecně k nakládání s těmito dluhopisy, využití technologie Corda rovněž pomáhá zabraňovat nákladným chybám při vypořádání (Agora Digital Capital markets 2022). Italská investiční banka Mediobanca digitalizovala své

emise investičních certifikátů, kterých ročně provede přibližně 300 prostřednictvím aplikací Agora včetně jejího DLT řešení, jež využívají jednotlivá oddělení banky. Díky tomu bylo dosaženo velké míry automatizace, když manuální vstupy přípravy dokumentace jsou nezbytné jen na začátku emise.

4.1.3 GS DAP od Goldman Sachs

Globální finanční skupina, která se zabývá především investiční činností, Goldman Sachs provozuje od roku 2022 platformu pro digitální aktiva nazvanou GS DAP (Businesswire 2023). GS DAP funguje jako další aplikační vrstva, která je postavená na povolovaném blockchainu Canton používajícím smartkontrakty napsané v programovacím jazyce Daml (Digital Asset [b.r.]). Smartkontrakty napsané v jazyce Daml jsou určené pro širokou škálu funkcionalit, jako jsou zápis práv a povinností, zachycení digitálních hodnot, jako jsou převodní tokeny, akcie či dluhopisy, a jejich životních cyklů za účelem jejich distribuce a kooperace mezi ekosystémy (databáze, systémy, ale i jiné DLT) různých subjektů finančního trhu prostřednictvím API. Významnou funkcionalitou platformy GS DAP je zajištění ochrany údajů striktním rozlišováním a zabezpečováním, kdo má ke kterým údajům přístup. Na GS DAP emitovala své dvouleté dluhopisy v digitální podobě v hodnotě 100 milionů Euro v listopadu roku 2022 Evropská investiční banka, když se jí na GS DAP podařilo snížit dobu vypořádání o 5 dnů z T+5 na vypořádání během jediného dne (T+0). Další velkou emisí byla emise tzv. „zelených dluhopisů“ (dluhopisy s ekologickými charakteristikami) hongkongské vlády ve výši 800 milionů hongkongských dolarů, což má být první tokenizovaná emise vládních zelených dluhopisů na světě (Hong Kong Monetary Authority 2023). Ohledně této emise se neuvádí žádné významné benefity oproti předchozím emisím hongkongské vlády.

K projektu Goldman Sachs je tedy závěrem nutné dle mého názoru podotknout, že teprve časem se ukáže, zda se jejich projekt platformy pro obchodování s digitálními aktivy osvědčí i v budoucnu.

4.1.4 Progmat

Od roku 2019 japonská finanční skupina Mitsubishi UFJ Trust and Banking Corporation (dále jen „MUFG“) provozuje platformu založenou na DLT nazvanou Progmat umožňující vydávat cenné papíry na DLT včetně jejich správy a transakcí s nimi (Kawai et al. 2021). V Japonsku bylo v tu dobu založeno několik obdobných projektů, které vznikly i v důsledku přijetí zákona o digitalizaci cenných papírů. V budoucnu má platforma rovněž v úmyslu umožnit vydávání, transakce a správu stablecoinů různých společností (Ledger Insights 2022). V porovnání s ostatními využitími na finančním trhu je ovšem nejzajímavější vydávání uživatelských tokenů na této platformě. V Japonsku více než polovina společností, jejichž akcie jsou veřejně nabízeny, poskytují svým držitelům odměny, vlastní-li například více než 100 akcií. Například japonské aerolinky některým držitelům akcií poskytují 50procentní slevy na tuzemské lety a čím více akcií takový jejich vlastník disponuje, tím více slev dostane. Mezi další odměny patří dárkové poukazy, členství apod. Tyto odměny v listinné podobě jsou nahrazeny uživatelskými tokeny ve formě nezastupitelných tokenů, které může jejich uživatel dále převádět na DLT. MUFG má v plánu tyto uživatelské tokeny rozšířit nejenom na odměny za držení cenných papírů, ale i na další služby. MUFG používá DLT Corda od společnosti R3.

4.1.5 Burza SDX

Švýcarská burza SIX Digital Exchange (dále jen „SDX“) je první digitální burza a zároveň centrální depozitář na světě s příslušnými licencemi od orgánu dohledu nad finančním trhem ve Švýcarsku, kde je možné vydávat, obchodovat a deponovat tokenizované cenné papíry (např. akcie či dluhopisy) na povolovaném DLT od R3 Corda, která zároveň podléhá právním předpisům o obchodování s cennými papíry (SIX Digital Exchange [b.r.]). Obchodování na SDX je již od roku 2021 umožněno jenom omezenému počtu investorů, jako jsou například banky. Emise cenných papírů probíhá prostřednictvím zástupce emitenta, který distribuuje cenné papíry na DLT mezi příslušné banky a další investory. Jako největší výhoda této burzy je uváděno okamžité vypořádání obchodu, což zpravidla u burz s cennými papíry trvá i několik dnů. V současnosti se na burze obchodují dle oficiálních webových stránek tři dluhopisové tituly. Dále SDX nabízí svým institucionálním partnerům služby a infrastrukturu týkající

se stakování etheru při jeho těžbě a ověřování (ke stakování etheru blíže kapitola 2.2.8), což jim umožní mj. vytvářet nové validátory etherů z řad svých klientů (SIX Digital Exchange [b.r.]).

4.2 Využití DLT technologie v pojišťovnictví

V pojišťovnictví se DLT zatím moc neprosazuje, řada projektů byla dokonce zrušena jako projekt Blochchain Insurance Industry Initiative (tzv. „B3i“), jehož prostřednictvím kterého zkoumalo přes 20 převážně evropských pojišťoven a zajišťoven možnosti DLT v pojišťovnictví. Projekt byl zrušen v roce 2020 z důvodu nedostatečného zájmu ze strany pojišťoven vytvořit společnou platformu pro pojišťovny a zajišťovny na DLT (Howard 2022). Obdobně již v roce 2020 zrušila svou platformu pro smartkontrakty na Ethereu nazvanou Fizzy pojišťovna AXA. Fizzy Axa nabízela od roku 2017 a vyplácela na ní pojistná plnění za zpoždění letů. Fizzy byla zrušená, protože nenaplňovala své komerční cíle a nebyla po ní dostatečná poptávka (Artificial Lawyer 2020). Z těchto důvodů tedy uvádím pouze 2 významné případy reálného používání DLT v pojišťovnictví a dále popisuje další způsoby jejího testování v pojišťovnictví.

4.2.1 Blockchain skupiny Allianz

V roce 2021 zavedla nadnárodní skupina Allianz řešení pro zefektivnění mezinárodních pojistných událostí motorových vozidel, které bývají pro pojišťovny administrativně a časově náročné, neboť se jedná o zdlouhavé procesy mezi pobočkami – právnickými osobami z různých zemí, jež trvají někdy i týdny (Ledger Insights 2021). Skupinová blockchainová platforma byla zavedena ve 23 evropských pobočkách. Během prvních šesti týdnů po jejím nasazení bylo zpracováno více než 145 tisíc transakcí ke zhruba 10 tisícům pojistných událostí. Blockchain Hyperledger Fabric umožňuje sjednotit záznamy o pojistné události, díky čemuž procesy trvající doposud týdny trvají nyní minuty. Proces funguje tak, že po oznámení pojistné události pobočka v příslušné zemi zadá předem určené informace o pojistné události do blockchainu a pomocí smartkontraktů se rozdělí náklady pojistné události mezi dotčené pobočky příslušných zemí. V blockchainu je rovněž snáze dohledatelný rozhodovací proces.

4.2.2 Krypto-klimatická koalice vedená Lemonade

Americká pojišťovací společnost společně s koalicí dalších společností vytvořila dobročinnou iniciativu spočívající v projektu založeném na blockchainu, který slouží drobným zemědělcům v Keni za účelem pojištění jejich budoucí úrody před poškozením v důsledku nepříznivých povětrnostních vlivů nebo jiných živelních událostí (Wininger [b.r.]). V Africe je problém, že neexistuje dostatečné množství stanic monitorujících počasí, což má za následek nepřesné předpovědi počasí a zanedbatelné množství varovných systémů před blížícími se cyklony, povodněmi či jinými živelními katastrofami, což odrazuje pojišťovny i zajišťovny od pojišťování v rozvojových zemích. Krypto-klimatická koalice vedená Lemonade si stanovila za svůj cíl tento problém vyřešit prostřednictvím přesné kvantifikace rizik výskytu živelních katastrof (realizovanou novým matematickým modelem), automatizace posuzování pojistných nároků a poskytování dostatečného financování a zajištění, když mohou do společného fondu určeného pro výplatu pojištění investovat i investoři prostřednictvím kryptoaktiv.

Zemědělci mají možnost se přihlásit do aplikace ve svém mobilním telefonu, kde provádějí a přijímají platby související s pojištěním, které jsou následně umístěny do smartkontraktů na blockchainu (Business Wire 2023). Jednotlivé pojistné události jsou automaticky, tedy bez nutnosti podat žádost ze strany pojištěné osoby, vyřizovány prostřednictvím smartkontraktů, čímž dochází k významnému snížení nákladů na vyřízení. V první fázi projektu od října 2022 do ledna 2023 bylo pojištěno 7000 keňských farmářů. Blockchain byl dodán společností Avalanche.

4.2.3 Ostatní projekty

Z řady případů užití a prototypů DLT v pojišťovnictví, které by mohly být relevantní i pro pojistný trh v ČR, lze zmínit projekty popsané v dokumentu z roku 2021 o využití blockchainu a smartkontraktů v pojišťovnictví publikovaném Evropským orgánem pro pojišťovnictví a zaměstnanecké penzijní pojištění za účelem konzultace s účastníky pojistného trhu (dále jen „EIOPA“) (European Insurance and Occupational Pensions Authority. 2021, s. 12–15). Například v Itálii proběhlo testování možného využití DLT pro ověřování a získávání nových zákazníků (např. v souvislosti s legislativou

proti praní špinavých peněz), v Itálii a v Litvě subjekty na pojistném trhu testovaly platformu založenou na DLT pro sjednání P2P pojištění (person-to-person, dle EIOPA je způsobem pojištění, kde se sdružují osoby, které se vzájemně pojišťují za účelem společného sdílení rizika), v Maďarsku jedna pojišťovna testovala využití DLT v případě řešení pojistného plnění v důsledku špatného počasí či vad lanovek při rekreaci na horách. Na Maltě jeden subjekt testoval DLT, kde na jednotlivých uzlech byly banky, pojišťovny i zástupci orgánu dohledu, přičemž cílem bylo poskytovat orgánu dohledu informace, které mají povinnosti mu reportovat. V Irsku jeden subjekt zabývající se pojištěním testoval DLT pro účely sdílení dat o pojištění napříč celým svým hodnotovým řetězcem.

4.3 Využití DLT technologie v bankovním sektoru

4.3.1 Abra

Americká společnost Abra, která provozuje stejnojmennou obchodní platformu s kryptoaktivy, žádá v současné době o bankovní licenci v USA pod názvem Abra Bank a zároveň má v plánu vytvořit obdobnou banku i mimo USA pod názvem Abra International (Abra Global 2022). Abra klade důraz na to, aby podléhala v příslušných státech veškeré regulaci. Právě tato informace je klíčová i pro trend, který je patrný v rámci společností podnikajících s kryptoaktivy. Je to snaha o to být maximálně začleněný pod příslušnou regulaci a nebýt nadále společností „mimo regulatorní systém“.

Abra má v plánu své dosavadní klienty zahrnout pod novou banku a poskytovat jim v rámci ní i nadále služby, jako jsou přijímání vkladů a jejich úročení v kryptoaktivech, půjčování stablecoinů se zajištěním v kryptoaktivech, a to i s nulovým úrokem při vysoké hodnotě zajištění, poskytování kryptopeněženky a obchodování s kryptoaktivy. Abra rovněž ve spolupráci se společností American Express plánuje vydávat první kreditní kartu, která by poskytovala odměny s kryptoměnami.

4.3.2 BitPesa

Společnost BitPesa se sídlem v Keni provozuje směnárnu a platební platformu využívající DLT ke snížení nákladů a zrychlení obchodních platebních transakcí se zeměmi, jejichž trhy jsou méně rozvinuté, a to především v Africe. BitPesa byla založena již v roce 2013 a na svých webových stránkách (BitPesa 2021)o sobě uvádí, že má licenci platební instituce od britského orgánu dohledu nad finančním trhem Financial Conduct Authority. Původním záměrem této společnosti bylo zjednodušit remitence zasílané keňskými pracovníky ve Velké Británii do Keni. Od té doby se obchodní činnosti nezměnily, když převážilo využívání BitPesy pro transakce související s obchodními činnostmi. Dle veřejně dostupných informací z roku 2018 (Reed 2018) fungují globální transakce v rámci BitPesa v Tanzanii či v Keni okamžitě s poplatkem 3 procent z posílané částky, zatímco u konkurenčních společností, jako jsou banky, takové převody trvaly 2–10 dnů s 5–10procentními poplatky. BitPesa provádí globální převody konkrétně tak (Yen 2017), že například eura v Německu nejprve vymění online u obchodníka za bitcoin, který následně vymění za příslušnou africkou měnu, tu následně poukáže na účet svého klienta v Africe, čímž se vyhne korespondenčním bankám či jiným institucím, které celý systém prodražují mj. i tím, že nemění africké měny za jiné měny zpravidla přímo, ale prostřednictvím směny amerického dolaru.

4.3.3 Kate Coin

Pro finanční instituce v ČR je důležité sledovat inovační aktivity skupiny belgické finanční skupiny KBC, kam patří i Československá obchodní banka a. s. (dále jen „ČSOB“) (KBC Group 2022). Právě vedle virtuální asistentky Kate, která využívá i prvky strojového učení, chce zavést KBC stablecoin Kate Coin, který má být evidován na blockchainu vyvinutém KBC, navázáním 1 : 1 k euru a bude s ním možné nakládat pomocí speciální peněženky vyvinuté rovněž KBC v bankovní mobilní aplikaci. Kate Coin půjde převádět pouze v uzavřeném okruhu subjektů, nelze je převádět mezi klienty KBC. Kate Coin nebude možné vyměnit za eura. KBC uvádí, že s Kate Coin bude spjatá programovatelnost, když ovšem nepopisuje technickou specifikaci. Například není jasné, zda Kate Coin budou fungovat obdobně jako smartkontrakty Etherea. Mezi příklady programovatelnosti je v tiskové zprávě uvedeno, že lze např. díky programovatelnosti omezit lhůtu, do kdy lze Kate Coin uplatnit. V první fázi se počítá

s využitím Kate Coin v rámci stávajících produktů KBC, jako jsou bankovní či pojistné produkty, když je uveden příklad odměňování klientů prostřednictvím Kate Coinů. KBC má ambice v budoucnu Kate Coin použít i v širším měřítku v rámci své partnerské sítě a jako příklad uvádí slevové poukázky na zboží partnerů apod.

4.3.4 Onyx od J. P. Morgan

Americká finanční skupina J. P. Morgan se DLT technologií zabývá již 7 let a provedla přes 60 ověření konceptů souvisejících s DLT. Nejvýznamnějším z nich je tzv. projekt Onyx, což je obchodní jednotka zabývající se hned několika projekty s DLT. Prvním takovým projektem je platforma založená na DLT pod názvem ONYX Digital Assets, která zpracovala více než 300 miliard dolarů vnitrodenních repo transakcí (jde o transakce s vysoce likvidními aktivy, zejm. dluhopisy centrálních bank) (Eva Szalay 2022). Pro banky je zde výhoda, že tokenizací těchto vysoce likvidních aktiv mohou tato aktiva využívat na několik hodin jako zajištění pro jejich derivátové pozice, aniž by porušily požadavky na minimální rezervu likvidních aktiv, která se počítá na konci obchodního dne. Tato platforma používá pro transakce smartkontrakty, které řídí detaily transakcí pro stanovení lhůt či vypořádání transakcí. Dle webových stránek projektu (JPMorgan Chase & Co. [b.r.]) používá Onyx Digital Assets blockchain založený na principu virtuálního počítače Etherea s API (aplikační programovací rozhraní), s funkcionalitou „flexibilních pravidel konsenzu“, když transakce jsou na něm vypořádány v reálném čase, tedy bez zpoždění. V rámci DLT se nepoužívají poplatky, jako je gas u Etherea.

Součástí projektu Onyx je rovněž komunikační síť Liink založená na blockchainu. První aplikací, která využívala Liink byla aplikace Resolve, jež se zabývá usnadňováním zasílání doprovodných informací k přeshraničním platbám vyžadovaných právem, jako jsou informace o plátci, příjemci apod., jejichž komplikovaná výměna mezi bankami zpomalovala přeshraniční platební styk. Resolve používá kolem 100 bank. Další aplikace Liinku nazvaná Confirm umožňuje bankovním obchodním klientům určit, zda účet jejich dodavatele je platný a není například uzavřený. Zbylé aplikace Liinku se zabývají přenosem informací k usnadnění rozhodnutí o převodu měn, a to téměř v reálném čase, nebo digitalizací platebních šeků, které se v USA stále hojně používají, prostřednictvím blockchainu. Jako výhoda Liinku je uvedeno sdílení velkého

množství mezibankovních dat zároveň s velkým důrazem na jejich bezpečnost a důvěrnost. V ideálním případě by se Liink mohl stát peer-to-peer prostředkem pro zasílání informací mezi bankami.

Třetí významnou součástí projektu Onyx je tzv. JPM Coin, což je povolovaný blockchain sloužící jako platební infrastruktura a k evidenci bankovních vkladů, umožňující v současnosti korporátním klientům banky provádět okamžité platební transakce neomezeně, tzn. i o víkendech a svátcích. Cílem tohoto blockchainu je zkvalitnit a zrychlit pokročilé platební služby jako dodání proti zaplacení, platba proti platbě, platby mezi dvěma automaty a rovněž zlepšit nedostatky nejenom v rámci domácího, ale i přeshraničního platebního styku. V rámci tohoto systému se mají zkoumat jak možnosti programovatelnosti transakcí, tak transakce s více měnami.

4.3.5 Spunta ABI Lab DLT

Spunta Banca DLT je projekt založený na soukromém povolovaném DLT postaveném na technologii Corda od společnosti R3, což je cloudová DLT platforma sloužící pro mezibankovní vypořádání v Itálii (R3 2020a). Projekt vznikl na základě iniciativy Italské bankovní asociace v roce 2020, kdy na něj povinně přešly banky v Itálii, tzn. více než 100 bank z původních systémů. Původní mezibankovní vypořádací systém v Itálii byl velmi složitý, nedostatečně standardizovaný, což mělo za následek častý nesoulad v transakčním vypořádání. Během prvních 6 měsíců zpracovala Spunta Banca DLT 204 milionů transakcí, přičemž cílem má být zpracování téměř 9 miliard transakcí za rok. Klíčovými vlastnostmi využité technologie je omezení, kdo má přístup k transakcím, což je relevantní zejména k ochraně osobních údajů, standardizace komunikačních a procesních protokolů a možnost pro banky řídit vypořádání v reálném čase. Průměrná doba mezibankovního vypořádání transakcí se zrychlila ze 30–50 dnů na méně než jeden den (R3 2020b).

5 Vytipování vhodných adeptů k implementaci pro velkou finanční skupinu v ČR

V této kapitole vytipuji na základě rozhodovací analýzy vhodné adepty pro implementaci pro velkou finanční skupinu v ČR v každém ze sektorů finančního trhu z vybraných příkladů v předchozí kapitole. Není-li stanoveno jinak, teoretické předpoklady čerpám z publikace (Fotr a Švecová 2022).

5.1 Předpoklady rozhodovacího procesu

5.1.1 Rozhodovací problém a varianty rozhodování

Formulace rozhodovacího problému je klíčovou otázkou celého rozhodovacího procesu, ale především analýzy rozhodovacího procesu. Může se stát, že je nesprávně formulován, například příliš široce, či příliš úzce, což v důsledku může vést k chybnému rozhodnutí. Můj rozhodovací problém byl již předem nadefinován v zadání diplomové práce jako „vytipování vhodných adeptů k implementaci pro velkou finanční skupinu v ČR“. Jako varianty pro rozhodování mi bude sloužit všech 12 reálných příkladů užití, které jsem identifikoval v předchozí kapitole.

5.1.2 Cíle, kritéria, objekty a subjekty rozhodování

Pro stanovení vhodných kritérií rozhodování je třeba nejprve určit cíle, neboť kritéria se od nich zpravidla odvozují. *Cílem rozhodování chápeme určitý stav firmy, resp. jejího okolí, kterého se má řešením rozhodovacího problému dosáhnout. Cíle mohou mít zpravidla podobu jako maximalizace např. zisku, minimalizace např. ztráty nebo dosažení určitých hodnot veličin* (Fotr a Švecová 2022).

Jako cíle velké finanční skupiny v ČR pro daný rozhodovací problém jsem zvolil:

a) Zvýšit inovativnost skupiny – zavádění inovací na finančním trhu je cílem všech subjektů a je trendem doby.
b) Zvýšit tvorbu zisku – každá finanční instituce jako svůj cíl sleduje ziskovost.
c) Podpora marketingu a reputace skupiny – inovace mají velký dopad na marketing a potenciál ho podpořit.

d) Konkurenceschopnost – pro velkou finanční skupinu v ČR je klíčové, aby nezůstala pozadu v rámci nabídek DLT řešení pro své zákazníky.
e) Budování vnitřních kapacit – DLT řešení pomáhá budování know-how dovnitř společnosti, které může být následně využité i v rámci jiných projektů.

Dalšími důležitými pojmy týkajícími se rozhodování jsou objekt rozhodování, což je organizační jednotka nebo její část, které se rozhodování týká, od objektu je vhodné odlišovat subjekt rozhodování, což je ten, kdo činí rozhodování.

Kritéria rozhodování představují hlediska zvolená rozhodovatelem (na základě jeho hodnotové soustavy, resp. hodnotové soustavy jeho firmy), která slouží k posouzení výhodnosti jednotlivých variant rozhodování z hlediska dosažení, resp. stupně plnění dílčích cílů řešeného rozhodovacího problému (Fotr a Švecová 2022). Kritéria mohou být vyjádřena číselně, tzv. kvantitativní kritéria, nebo slovně, tzv. kvalitativní kritéria. Dále lze dle povahy rozlišovat kritéria maximalizační a minimalizační. U maximalizačních kritérií je vyšší hodnota lepší či výhodnější. U minimalizačních kritérií je pro nás naopak nižší hodnota lepší či výhodnější.

Soubor kritérií by měl být úplný, tedy nemělo by žádné chybět, neměla by se překrývat, neměly by být mezi nimi přílišné provazby, počet kritérií by měl být co nejmenší, čímž se zjednodušuje závěrečné hodnocení a výběr variant. A nakonec by každé kritérium mělo mít jasný a jednoznačný smysl a mělo by být pro rozhodovatele plně srozumitelné.

Na základě cílů jsem stanovil následující kritéria:

Kritérium číslo 1 – Inovativnost řešení dle Valenty
Kritérium vychází z cíle zvýšit inovativnost finanční skupiny. Jedná se o kvantitativní a maximalizační kritérium. Míru inovativnosti řešení lze měřit dle inovativní řady dle prof. Valenty (Český statistický úřad 2014), který inovace dělí do deseti řádů dle toho, co se u nich mění a co se zachovává, zda například proces, nebo jen rychlost operací.

Kritérium číslo 2 – Konkurenceschopnost
Kritérium vychází z cílů zvýšit inovativnost a konkurenceschopnost finanční skupiny. Jedná se o kvalitativní a maximalizační kritérium, o subjektivní hodnocení inovativnosti z hlediska finanční skupiny s ohledem i na konkurenci jiných finančních institucí na českém trhu a realizovatelnost.

Kritérium číslo 3 – Potenciální výnosnost inovace
Kritérium vychází z cíle zvýšit tvorbu zisku finanční skupiny, je to kvalitativní a maximalizační kritérium. Jedná se o kvalitativní kritérium, protože nemám k dispozici přesná čísla, nýbrž velmi hrubé odhady. Z hlediska tohoto kritéria se budou analyzovat náklady na zavedení daného řešení a potenciální výnosy z jeho zavedení v horizontu příštích deseti let.

Kritérium číslo 4 – Marketingový potenciál daného řešení
Kritérium vychází z cíle podpory marketingu a reputace skupiny. Jedná se o kvalitativní a maximalizační kritérium.

Kritérium číslo 5 – Dopad na budování interních kapacit finanční skupiny.
Kritérium vychází z cíle podpory marketingu a reputace skupiny. Jedná se o kvalitativní a maximalizační kritérium.

Kvalitativní kritéria jsou kvantifikována a maximalizována na škále od 1–10, kdy 1 představuje nejhorší hodnocení a 10 nejlepší hodnocení.

5.1.3 Stanovení vah kritérií

Pro stanovení vah kritérií byla použita Saatyho metoda, kterou popisuji v kapitole 3. Pro bodování vzájemného srovnávání kritérií jsem použil bodování dle Saatyho: 1 – kritéria jsou stejně významná, 3 – první kritérium je slabě významnější než druhé, 5 – první kritérium je dosti významnější než druhé, 7 – první kritérium je prokazatelně významnější než druhé, 9 – první kritérium je absolutně významnější než druhé. Například v prvním řádku Tabulky 1 jsem porovnával preferenční vztah inovativnosti dle

Valenty vůči inovativnosti dle Valenty, kde mi logicky muselo vyjít 1/1 = 1, preferenční vztah inovativnosti dle Valenty a konkurenceschopnosti jsem vzhledem k tomu, že kritérium konkurenceschopnosti je slabě významnější než kritérium inovativnosti, vydělil 1 číslem 3, tzn. 1/3 = 0,33.

Ve druhé fázi Saatyho metody se stanoví váhy kritérií pomocí geometrického průměru (označeno jako Geomean v tabulce níže) jednotlivých preferenčních vztahů každého kritéria tak, jak je to vypočítáno v Tabulce 1.

K výsledným vahám (označeno jako váhy v tabulce níže) dojdeme tak, že geometrické průměry znormujeme, tedy vydělíme součtem všech geometrických průměrů. Největší váha mi vyšla u kritéria konkurenceschopnosti, které se týká zařazení varianty do reálií českého finančního trhu, což považuji za adekvátní, a je bezpochyby nejdůležitějším kritériem, protože sebelepší varianta bez možnosti realizovatelnosti na českém finančním trhu je neakceptovatelná. Na druhém místě mi vyšla shodně kritéria inovativnost dle Valenty a marketingový potenciál a jako nejméně významná vyšla kritéria výnosnosti a budování interních kapacit.

Tabulka 1 – Přiřazení vah kritériím dle Saatyho metody

Saatyho metoda	Inovativnost dle Valenty	Konkurence-schopnost	Výnosnost	Marketingový Potenciál	Int. kapacity	Geomean	Váhy
Inovativnost dle Valenty	1	0,33	5	1	5	1,53	0,213787
Konkurence-schopnost	3	1	7	3	7	3,38	0,47283
Výnosnost	0,2	0,14	1	0,2	1	0,36	0,049798
Marketingový potenciál	1	0,33	5	1	5	1,53	0,213787
Int. kapacity	0,2	0,14	1	0,2	1	0,36	0,049798

5.2 Rozhodovací proces

Pro rozhodovací proces používám metodu analytického hierarchického procesu, kterou blíže popisuji v kapitole 3.

Pro větší přehlednost a porozumění tedy stručně zopakuji, že pro každé kritérium se vytvoří Saatyho matice na základě párového srovnání variant, při němž dojde k určení velikosti preference všech dvojic variant (stejně jako když jsme stanovili váhy kritérií v Tabulce 1). Následně se určí pomocí Saatyho matice pro jednotlivá kritéria dílčí ohodnocení variant vzhledem k těmto kritériím, k čemuž se dospěje tak, že se 1) stanoví váhy variant pomocí geometrického průměru jednotlivých preferenčních vztahů každé varianty (např. v tabulkách 2 – 6 označené jako Geomean), 2) geometrické průměry znormujeme, tedy vydělíme součtem všech geometrických průměrů dané matice, čímž dostane preferenci dané varianty k danému kritériu (např. v tabulkách 2 – 6 označené jako Preference), 3) preferenci následně vynásobíme vahou příslušného kritéria (např. v tabulkách 2 – 6 označené jako Dílčí ohodnocení varianty). Tímto třetím krokem dostaneme konečnou preferenci varianty k danému kritériu, tedy dílčí ohodnocení varianty. Všechna dílčí ohodnocení variant následně sečteme (viz tabulky 7, 13 a 19), čímž dostaneme celkové ohodnocení dané varianty.

Data v tabulkách níže jsem zaokrouhlil na dvě desetinná místa, při samotných výpočtech, pro které jsem použil MS Excel, jsem žádná čísla nezaokrouhloval.

U projektu Progmat hodnotím část platformy vydávající uživatelské tokeny, protože o jejich burze není dostatek informací a řešení burzy se týká rovněž projekt SDX.

5.2.1 Hodnocení variant na kapitálovém trhu

Inovativnost dle Valenty je jediné kvantitativní kritérium. Jako nejinovativnější jsem ohodnotil SDX, jak je patrné z Tabulky 2, protože se jedná o technologickou změnu celého systému, tedy burzy, což odpovídá inovačnímu stupni 8 dle Valenty. Agora, GS DAP a Progmat odpovídají inovačnímu stupni číslo 7, tedy změně druhu, kdy se mění konstrukční koncepce systému, ale k výrazným technologickým změnám systému nedochází. SG Forge odpovídá inovačnímu stupni číslo 6, tedy změně generace, kdy konstrukční koncepce systému zůstává (používá se Ethereum), ale mění se konstrukční řešení systému (finanční instituce vydávající stablecoiny na Ethereu).

Tabulka 2 – Hodnocení variant na kapitálovém trhu z hlediska inovativnosti dle Valenty

Inovativnost dle V.	SG Forge	Agora	GS DAP	Progmat	SDX	Geomean	Preference	Dílčí ohodnocení varianty
SG Forge	1	0,33	0,33	0,33	0,2	0,38	0,06	0,01
Agora	3	1	1	1	0,33	1	0,17	0,04
GS DAP	3	1	1	1	0,33	1	0,17	0,04
Progmat	3	1	1	1	0,33	1	0,17	0,04
SDX	5	3	3	3	1	2,67	0,44	0,09

Z pohledu konkurenceschopnosti na finančním trhu v ČR se zdá jako nejlepší řešení SG Forge (viz Tabulka 3), protože vytváří stablecoiny na Ethereu, k čemuž vytváří další infrastrukturu. To se může setkat s velkým zájmem nejenom velkoobchodních, ale potenciálně i maloobchodních zákazníků v ČR, kteří by určitě uvítali podobnou infrastrukturu od velké renomované finanční skupiny v ČR. Rovněž řešení Progmatu spočívající v platformě pro uživatelské tokeny by se mohlo v ČR ujmout, například pro vyplácení různých dividend a bonusů na kapitálovém trhu. Takové DLT by mohlo fungovat i jako společná platforma pro ostatní uživatelské tokeny společností mimo kapitálový trh. Pro řešení společnosti Agora vidím spíše malý potenciál v ČR, protože by potenciálně poskytlo jen malou konkurenční výhodu tím, že by se částečně inovoval proces. Nejmenší potenciál z hlediska konkurenceschopnosti je ovšem u SDX a GS DAP, protože se jedná o robustní projekty s potenciálně malou poptávkou v ČR.

Tabulka 3 – Hodnocení variant na kapitálovém trhu z hlediska konkurenceschopnosti

Konkurence-schopnost	SG Forge	Agora	GS DAP	Progmat	SDX	Geomean	Preference	Dílčí ohodnocení varianty
SG Forge	1	5	7	3	5	3,5	0,50	0,24
Agora	0,2	1	3	0,33	1	0,72	0,10	0,05
GS DAP	0,14	0,33	1	0,2	0,33	0,32	0,05	0,02
Progmat	0,33	3	5	1	3	1,72	0,25	0,12
SDX	0,2	1	3	0,33	1	0,73	0,10	0,05

Jako nejvýnosnější řešení vychází SG Forge (viz tabulka 4), protože samotné DLT – Ethereum, na kterém mají tokeny být emitovány, je připravené, tudíž náklady budou spočívat pouze ve vybudování související infrastruktury a obsluhy, jako jsou marketing, úschova rezervy, právní služby apod. O služby SG Forge by mohl být největší zájem v ČR, což se promítne do příjmů. U řešení Progmat by se muselo vytvořit DLT

řešení a související infrastruktura, zároveň zde je ovšem potenciál získat klienty pro řešení spočívající v inovativních uživatelských tokenech. Vybudování obdoby burzy SDX by bylo velmi nákladné a nepochybně v nejbližších letech ztrátové. Pro řešení společnosti Agora vidím v ČR malý potenciál ČR, protože by se inovoval proces, což by přineslo velké náklady na přechod na toto řešení, a velikost úspor pravděpodobně nebude velká a projeví se spíše v dlouhodobém horizontu. Řešení GS DAP a SDX jsou velmi robustní a nákladná a je otázka jejich aktuální vhodnosti pro malý kapitálový trh v ČR, resp. je zde významné riziko, že by nepřinášela dostatečné výnosy.

Tabulka 4 – Hodnocení variant na kapitálovém trhu z hlediska výnosnosti

Výnosnost	SG Forge	Agora	GS DAP	Progmat	SDX	Geomean	Preference	Dílčí ohodnocení varianty
SG Forge	1	5	5	3	5	3,28	0,5	0,03
Agora	0,2	1	1	0,33	1	0,58	0,09	0,004
GS DAP	0,2	1	1	0,33	1	0,58	0,09	0,004
Progmat	0,33	3	3	1	3	1,56	0,24	0,01
SDX	0,2	1	1	0,33	1	0,58	0,09	0,004

Pro marketing celé finanční skupiny má největší potenciál řešení DLT pro uživatelské tokeny společnosti Progmat, protože na něj mj. může snadno navázat i marketing ostatních společností vydávajících tokeny na DLT (viz Tabulka 5). SDX jako burza na DLT je rovněž významná z marketingového hlediska, GS DAP a SG Forge jsou spíše velkoobchodní řešení, která směřují k uzavřenému okruhu zákazníků. Agora vzhledem ke svému úzkému a velmi technickému zaměření představuje řešení s vůbec nejmenším marketingovým potenciálem.

Tabulka 5 – Hodnocení variant na kapitálovém trhu z hlediska marketingového potenciálu

Marketingový pot.	SG Forge	Agora	GS DAP	Progmat	SDX	Geomean	Preference	Dílčí ohodnocení varianty
SG Forge	1	5	1	0,33	1	1,11	0,18	0,04
Agora	0,2	1	0,2	0,2	0,2	0,28	0,04	0,01
GS DAP	1	5	1	0,33	0,33	0,89	0,14	0,03
Progmat	3	5	3	1	3	2,67	0,42	0,09
SDX	1	5	3	0,33	1	1,38	0,22	0,05

Na interní kapacity, tzn. na zaměstnance bude nejnáročnější SDX (viz Tabulka 6), protože se jedná o projekt celé burzy na DLT, následně druhým nejvíce náročným řešením je GS DAP, které má mnoho funkcionalit. Agora, Progmat a SG Forge naopak mnoho lidských kapacit potřebovat nebudou, protože se oproti SDX a GS DAP jedná o mnohem menší projekty.

Tabulka 6 – Hodnocení variant na kapitálovém trhu z hlediska interních kapacit

Int. kapacity	SG Forge	Agora	GS DAP	Progmat	SDX	Geo-mean	Preference	Dílčí ohodnocení varianty
SG Forge	1	3	0,2	1	0,14	0,61	0,09	0,005
Agora	0,33	1	0,2	0,33	0,14	0,32	0,05	0,002
GS DAP	5	5	1	3	0,33	1,90	0,29	0,0145
Progmat	1	3	0,33	1	1	1	0,15	0,01
SDX	7	7	3	1	1	2,71	0,41	0,02

Pokud sečteme dílčí ohodnocení jednotlivých variant, dostaneme celkové výsledky rozhodovacího procesu (viz Tabulka 7), ve kterém se nejlépe umístil SG Forge, jako druhá se umístila varianta Progmat a třetí SDX. Na posledních místech s velkým odstupem se umístily projekty Agora a GS DAP. Vzhledem k tomu, že cílem mé práce je vytipovat několik vhodných adeptů k implementaci pro velkou finanční skupinu v ČR, z této skupiny se mi jeví jako vhodní adepti první tři varianty.

Mezi silné stránky SG Forge patří vysoká konkurenceschopnost na českém trhu, nízké náklady na implementaci a s tím související vysoká potenciální výnosnost. Naopak SG Forge má omezený marketingový potenciál, je ze všech zkoumaných řešení nejméně inovativní a nevybuduje moc interních kapacit, protože se jedná o relativně jednoduché řešení na implementaci a správu.

Nejsilnější stránkou Progmatu je marketingový potenciál, dalšími silnými stránkami jsou konkurenceschopnost v českém prostředí a výnosnost. Progmat je průměrně inovativní řešení a rovněž průměrně náročné na budování interních kapacit.

SDX je ze všech řešení nejnáročnější hned ve dvou aspektech, jedná se o nejinovativnější řešení, ale také nejnáročnější na budování vnitřních kapacit. SDX je rovněž silný

v marketingovém potenciálu. Naopak velmi slabé hodnocení získalo vzhledem ke konkurenceschopnosti v českém prostředí a v otázce výnosnosti.

Tabulka 7 – Celkové vyhodnocení variant na kapitálovém trhu

Varianta	Celkové preference
SG Forge	0,32
Agora	0,10
GS DAP	0,11
Progmat	0,26
SDX	0,22

5.2.2 Hodnocení variant v pojišťovnictví

Inovativnost dle Valenty je jediné kvantitativní kritérium. Jako nejinovativnější jsem ohodnotil Lemonade (viz Tabulka 8), jehož řešení odpovídá inovačnímu stupni číslo 7, tedy změně druhu, kdy se mění konstrukční koncepce systému (pojištění prostřednictvím DLT, rychlejší vypořádání), ale k výrazným technologickým změnám systému nedochází. Řešení Allianz odpovídá inovačnímu stupni číslo 6, tedy změně generace, kdy konstrukční koncepce systému zůstává, ale mění konstrukční řešení systému, tedy zakomponování DLT do stávajících procesů a řešení.

Tabulka 8 – Hodnocení variant v pojišťovnictví z hlediska inovativnosti dle Valenty

Inovativnost dle Valenty	Allianz	Lemonade	Geomean	Preference	Dílčí ohodnocení varianty
Allianz	1	0,33	0,58	0,25	0,05
Lemonade	3	1	1,73	0,75	0,16

Projekt Lemonade se jeví nerealisticky pro zavedení ze strany české pojišťovny, protože cílí na specifické případy v zemích „3. světa“ (viz Tabulka 9). Oproti tomu řešení Allianz je mnohem menší než projekt Lemonade a zdá se být vhodným řešením využívajícím přínosy DLT oproti tradičním databázím, tedy systém pro entity na totožné úrovni, v případě Allianz společnosti ze skupiny pro práci s daty v reálném čase.

Tabulka 9 – Hodnocení variant v pojišťovnictví z hlediska konkurenceschopnosti

Konkurence-schopnost	Allianz	Lemonade	Geomean	Preference	Dílčí ohodnocení varianty
Allianz	1	7	2,65	0,88	0,41
Lemonade	0,14	1	0,38	0,13	0,06

Obě řešení potřebují náklady na vytvoření DLT, když související náklady jsou u Lemonade nepochybně mnohem vyšší, když jejich DLT bude používat i související aplikace, jako jsou orákula, a bude zahrnovat významné náklady na marketing, které u Allianz budou žádné či minimální (viz Tabulka 10). Zároveň řešení Allianz přináší zřejmé úspory pro skupinu jako celek, když naopak řešení Lemonade se jeví jako velmi rizikové a spíše jako charitativní řešení, kde zisk není primárním cílem.

Tabulka 10 – Hodnocení variant v pojišťovnictví z hlediska výnosnosti

Výnosnost	Allianz	Lemonade	Geomean	Preference	Dílčí ohodnocení varianty
Allianz	1	3	1,73	0,75	0,04
Lemonade	0,33	1	0,58	0,25	0,01

Pokud jde o marketingový potenciál, pak řešení společnosti Lemonade vzhledem ke svému charitativnímu charakteru s globálním významem je mnohem významnější a vhodnější nežli velmi technické řešení Allianz (viz Tabulka 11).

Tabulka 11 – Hodnocení variant v pojišťovnictví z hlediska marketingového potenciálu

Marketingový potenciál	Allianz	Lemonade	Geomean	Preference	Dílčí ohodnocení varianty
Allianz	1	0,2	0,45	0,17	0,04
Lemonade	5	1	2,24	0,83	0,18

Allianz potřebuje obsluhu základního DLT, oproti tomu Lemonade je mnohem robustnější řešení, které vyžaduje několikanásobně více odborníků na jeho obsluhu (viz Tabulka 12).

Tabulka 12 – Hodnocení variant v pojišťovnictví z hlediska interní kapacity

Int. kapacity	Allianz	Lemonade	Geomean	Preference	Dílčí ohodnocení varianty
Allianz	1	0,2	0,45	0,17	0,01
Lemonade	5	1	2,24	0,83	0,04

Přestože se dalo předpokládat, že řešení společnosti Allianz bude z hlediska uplatnění na českém finančním trhu vhodnější než řešení společnosti Lemonade, rozdíl mezi nimi, jak ukazuje Tabulka 13, nebyl nakonec tak markantní, jak by se na první pohled mohlo zdát. Přesto z těchto dvou řešení nakonec vytipovávám jako vhodného adepta k implementaci pro český finanční trh řešení společnosti Allianz.

Výhody Allianz oproti řešení společnosti Lemonade spočívají v jeho větší konkurenceschopnosti a výnosnosti, oproti tomu řešení společnosti Lemonade má lepší ohodnocení oproti Allianz z hlediska marketingového potenciálu, interních kapacit a inovativnosti.

Tabulka 13 – Celkové vyhodnocení variant v pojišťovnictví

Varianta	Celkové preference
Allianz	0,55
Lemonade	0,45

5.2.3 Hodnocení variant v bankovnictví

Inovativnost dle Valenty je jediné kvantitativní kritérium. Jako nejinovativnější jsem ohodnotil řešení Abra a Spunta (viz Tabulka 14), protože se jedná o technologickou změnu celého systému, tedy systému vypořádání v případě Spunty a banky s kryptoaktivy v případě Abry, což odpovídá inovačnímu stupni 8 dle Valenty. Onyx odpovídá inovačnímu stupni číslo 7, tedy změně druhu, kdy se mění konstrukční koncepce systému, ale k výrazným technologickým změnám nedochází. Kate Coin odpovídá inovačnímu stupni číslo 6, tedy změně generace, kdy konstrukční koncepce systému zůstává, ale mění konstrukční řešení systému (slevy na DLT). BitPesa odpovídá inovačnímu stupni číslo 5, když inovace spočívá ve změně varianty, tedy pro převody měn se používají kryptoaktiva na stávajících DLT.

Tabulka 14 – Hodnocení variant v bankovnictví z hlediska inovativnosti dle Valenty

Inovativnost dle Valenty	Abra	BitPesa	Kate Coin	Onyx	Spunta	Geomean	Preference	Dílčí ohodnocení varianty
Abra	1	5	5	3	1	2,37	0,36	0,08
BitPesa	0,2	1	0,33	0,2	0,2	0,31	0,05	0,01
Kate Coin	0,2	3	1	0,33	0,20	0,53	0,08	0,02
Onyx	0,33	5	3	1	0,33	1,11	0,17	0,04
Spunta	1	5	5	3	1	2,37	0,36	0,08

Z hlediska konkurenceschopnosti vychází v bankovnictví v ČR nejlépe Kate Coin a Abra (viz Tabulka 15). Kate Coin je minimalistické řešení, které se může rozrůst v ekosystém banky. Oproti Kate Coin je Abra velké a radikální řešení, které by vedle jeho nepochybných přínosů mohlo narazit na získání příslušné licence centrální banky či na reputační riziko v případu propadu trhu s kryptoaktivy. Onyx nabízí několik zajímavých řešení, která by se ovšem musela buď více přizpůsobit pro český trh, nebo dále otestovat jako projekty pro obchodování s vysoce likvidními aktivy. Spunta je hodnocena nízko vzhledem ke kvalitnímu mezibankovnímu systému v ČR, pro který oproti Itálii není v ČR důvod ho nahrazovat. Je otázka, zda převody měn prostřednictvím kryptoaktiv, jako je bitcoin, by byly tak výhodné jako v době vzniku projektu BitPesa před několika lety, a to vzhledem k růstu poplatků za transakce s nimi. Zároveň by řešení BitPesa mohlo ohrozit reputaci bank a krátit jim zisky, které mají z převodu měn.

Tabulka 15 – Hodnocení variant v bankovnictví z hlediska konkurenceschopnosti

Konkurence-schopnost	Abra	BitPesa	Kate Coin	Onyx	Spunta	Geomean	Preference	Dílčí ohodnocení varianty
Abra	1	9	1	3	7	2,85	0,37	0,18
BitPesa	0,11	1	0,11	0,14	0,33	0,23	0,03	0,01
Kate Coin	1	9	1	3	7	2,85	0,37	0,18
Onyx	0,33	7	0,33	1	5	1,31	0,17	0,08
Spunta	0,14	3	0,14	0,2	1	0,42	0,05	0,03

Kate Coin vyžaduje vytvoření poměrně jednoduchého DLT, které už v takto zjednodušené podobě je možné komercionalizovat a dále vyvíjet (viz Tabulka 16). Abra přináší potenciálně velmi výnosný projekt, pro který je ovšem nutné vytvořit infrastrukturu, jež nemá ve světě z hlediska bankovního sektoru obdobu, proto jeho realizace může být velmi nákladná a trvat i delší období. Proto oba projekty hodnotím jako

rovnocené z hlediska výnosnosti. Onyx předpokládá vytvoření specifického DLT řešení a obsahuje velmi inovativní nápady, jejichž komercializace na českém trhu je ale těžko odhadnutelná, ovšem není vyloučena. Zavedení řešení BitPesa do procesu banky by s sebou neslo jisté provozní náklady, zejména na lidské zdroje, ale i na vytvoření příslušné infrastruktury. Přitom odhad výnosnosti BitPesa v ČR lze stanovit jako minimální i vzhledem k rostoucím poplatkům za transakce s kryptoaktivy, přesto nelze vyloučit některé možné dílčí úspory při převodech měn. Spunta jako mezibankovní platební systém s sebou nese velké náklady na zavedení takového systému (mj. náklady na zabezpečení, náklady na právní poradenství apod.). Úspory tohoto řešení vzhledem k tomu, že v ČR dlouhodobě úspěšně (oproti italskému systému, který nahradila Spunta) existuje mezibankovní zúčtovací platební systém České národní banky Certis, lze očekávat minimální.

Tabulka 16 – Hodnocení variant v bankovnictví z hlediska výnosnosti

Výnosnost	Abra	BitPesa	Kate Coin	Onyx	Spunta	Geomean	Preference	Dílčí ohodnocení varianty
Abra	1	7	3	5	7	3,74	0,51	0,03
BitPesa	0,14	1	0,2	0,33	1	0,39	0,05	0,003
Kate Coin	0,33	5	1	3	5	1,90	0,26	0,01
Onyx	0,2	3	0,33	1	3	0,90	0,12	0,006
Spunta	0,14	1	0,2	0,33	1	0,39	0,05	0,003

Marketingový potenciál je největší u Kate Coin a Spunta (viz Tabulka 17). Spunta jako mezibankovní systém pro vypořádání na DLT může zvýšit renomé celému odvětví. Oproti tomu Kate Coin lze použít a nabízet i ve spolupráci s ostatními partnery společnosti. Onyx a Abra mají marketingový potenciál obdobný, když u Abry je třeba brát v úvahu kromě vysokého marketingového potenciálu banky s kryptoaktivy i negativní marketingový potenciál v případě negativní publicity některých kryptoaktiv, které lze u ní ukládat. U Onyxu lze hodnotit pozitivně vlastní JPM Coin. Marketingový potenciál BitPesa je v prostředí ČR velmi slabý, když v rámci možných obchodů s valutami je na trhu mnoho.

Tabulka 17 – Hodnocení variant v bankovnictví z hlediska marketingového potenciálu

Marketingový potenciál	Abra	BitPesa	Kate Coin	Onyx	Spunta	Geomean	Preference	Dílčí ohodnocení varianty
Abra	1	3	0,2	1	0,2	0,65	0,09	0,02
BitPesa	0,33	1	0,2	0,33	0,2	0,34	0,05	0,01
Kate Coin	5	5	1	5	1	2,63	0,38	0,08
Onyx	1	3	0,2	1	0,2	0,65	0,1	0,02
Spunta	5	5	1	5	1	2,63	0,37	0,08

Nejnáročnější z hlediska interních kapacit jsou projekty Abra a Onyx, přičemž Abra je náročná infrastrukturu kolem DLT a Onyx je naopak náročný na vytvoření a obsluhu samotného DLT řešení (viz Tabulka 18). Spunta je rovněž náročné řešení, ale vzhledem k tomu, že jde o mezibankovní zúčtovací systém, lze předpokládat, že se kapacity na vývoj rozdělí mezi participující subjekty. Kate Coin vyžaduje obsluhu jednoduchého DLT a BitPesa je na technologické znalosti DLT téměř nenáročné řešení.

Tabulka 18 – Hodnocení variant v bankovnictví z hlediska interní kapacity

Int. kapacity	Abra	BitPesa	Kate Coin	Onyx	Spunta	Geomean	Preference	Dílčí ohodnocení varianty
Abra	1	5	5	1	3	2,37	0,36	0,02
BitPesa	0,2	1	0,33	0,2	0,2	0,31	0,05	0,002
Kate Coin	0,2	3	1	0,33	0,33	0,58	0,09	0,005
Onyx	1	5	3	1	3	2,14	0,33	0,02
Spunta	0,33	5	3	0,33	1	1,11	0,17	0,009

Pokud sečteme dílčí ohodnocení jednotlivých variant, dostaneme celkové výsledky rozhodovacího procesu (viz Tabulka 19), ve kterém se jasně nejlépe umístilo řešení Abra těsně před Kate Coin. Spunta a Onyx jsou s odstupem na 3., respektive 4. místě. Zdaleka nejméně vhodnou variantou je řešení BitPesa. Na základě tohoto hodnocení vytipovávám jako vhodné adepty pro implementaci na český finanční trh řešení Abra a Kate Coin.

Řešení Abra bylo vůbec nejlepší v konkurenceschopnosti, (společně s Kate Coin), výnosnosti a požadavcích na budování interních kapacit. Abra byla průměrná v inovativnosti, marketingovém potenciálu.

Kate Coin byla nejlepší v marketingovém potenciálu (společně s řešením Spunta) a zároveň měla nejlepší výsledek v rámci konkurenceschopnosti (společně s řešením Abra). Kate Coin je druhá z hlediska výnosnosti a spíše podprůměrná v nárocích na interní kapacity a v inovativnosti.

Tabulka 19 – Celkové vyhodnocení variant v bankovnictví

Varianta	Celkové preference
Abra	0,32
BitPesa	0,04
Kate Coin	0,29
Onyx	0,16
Spunta	0,19

Závěr

Na finančním trhu nejenom v ČR, ale v celé EU dojde v souvislosti s přijetím nařízení MiCA k velkým změnám pro zavedené finanční instituce, neboť těm toto nařízení explicitně povolí vydávání kryptoaktiv na DLT a poskytování souvisejících služeb. Z tohoto důvodu je třeba světový finanční trh soustavně mapovat, analyzovat a monitorovat existující DLT řešení, která by byla vhodná i pro implementaci v ČR.

V současnosti na finančních trzích ve světě neexistuje velké množství DLT projektů, které by byly funkční a reálně zapojené do poskytování finančních služeb. Mnoho DLT projektů naopak v průběhu času skončilo. Například v rámci pojišťovnictví se mi podařilo najít pouze 2 existující řešení.

Celkem se mi podařilo vytipovat 12 řešení DLT na finančních trzích, které jsem rozdělil dle sektoru finančního trhu na DLT řešení pro bankovnictví, DLT řešení pro kapitálový trhu a DLT řešení pro pojišťovnictví. Následně jsem tato řešení hodnotil pomocí metody analytického hierarchického procesu v rámci sektorů, který je vhodný, pokud rozhodovací proces obsahuje větší množství kvalitativních kritérií, což je i případ mého rozhodovacího problému. Jako hodnoticí kritéria jsem stanovil inovativnost dle metodologie profesora Valenty, konkurenceschopnost na finančním trhu v ČR, výnosnost, marketingový potenciál a dopad na budování interních kapacit finanční skupiny. Pro kritéria jsem následně stanovil váhy dle Saatyho metody.

Následně jsem na základě hodnocení vybral vhodné adepty k implementaci, když jsem nutně nevybíral pouze nejlépe hodnocené řešení v daném sektoru, ale rovněž jsem bral v úvahu nízký bodový odstup ostatních variant od tohoto nejlepšího řešení. Proto jsem vytipoval 3 adepty k implementaci pro kapitálový trh, dva pro bankovnictví a 1 pro pojišťovnictví.

K implementaci pro kapitálový trh jsem vytipoval řešení společnosti SG Forge, protože se jedná o stablecoin na Ethereu od velké finanční skupiny, což je velmi jednoduché řešení (oproti ostatním), které by mohlo být v ČR vysoce konkurenceschopné

a výnosné. Dále jako druhé se umístilo japonské řešení DLT s užitnými tokeny Progmat, které by mohlo mít výrazný marketingový potenciál a zároveň být konkurenceschopné i výnosné. DLT burza SDX je vysoce inovativní, velmi náročná na budování vnitřních kapacit a má silný i marketingový potenciál.

K implementaci pro pojišťovnictví jsem vytipoval skupinovou blockchainovou platformu Allianz pro pojistné události s motorovými vozidly, jejíž výhody spočívají v konkurenceschopnosti a potenciálním vytváření úspor.

K implementaci pro bankovnictví jsem zvolil kryptobanku Abra, protože by mohla být potenciálně vysoce konkurenceschopná v ČR, výnosná, zároveň se jedná o řešení náročné na budování interních kapacit. Kate Coin na DLT skupiny KBC sloužící v první fázi pro odměňování stávajících klientů je menší řešení, které by ovšem mohlo být vysoce konkurenceschopné v ČR s významným marketingovým potenciálem.

Bibliografie

ABRA GLOBAL, 2022. Abra Announces Abra Bank and Abra Boost. *Abra* [online]. [vid. 2023-04-08]. Dostupné z: https://www.abra.com/blog/abra-bank-and-abra-boost/

AGORA DIGITAL CAPITAL MARKETS, 2022. Mediobanca SpA: launches innovative agoraPlatform for automated issuance and lifecycle management of investment certificates. *agoradcm.com* [online] [vid. 2023-04-21]. Dostupné z: https://agoradcm.com/updates/mediobanca-spa-launches-innovative-agoraplatform-for-automated-issuance-and-lifecycle-management-of-investment-certificates/

AKHTAR, Zuhaib, 2023. *From Blockchain to Hashgraph: Distributed Ledger Technologies in the Wild* [online]. 2023. [vid. 2023-05-06]. Dostupné z: https://arxiv.org/abs/2303.14848v1

ANTONOPOULOS, Andreas, 2017. *Mastering Bitcoin: Programming the Open Blockchain*. 2nd edition. Sebastopol, CA: O'Reilly Media. ISBN 978-1-4919-5438-6.

ANTONOPOULOS, Andreas M. a Gavin WOOD, 2019. *Mastering Ethereum: building smart contracts and DApps*. First edition. Sebastopol, CA: O'Reilly. ISBN 978-1-4919-7194-9.

ARTIFICIAL LAWYER, 2020. AXA Scraps Fizzy Insurance Smart Contract…But Still Interested in the Tech. *Artificial Lawyer* [online]. [vid. 2023-05-01]. Dostupné z: https://www.artificiallawyer.com/2020/10/08/axa-scraps-fizzy-insurance-smart-contract-but-still-interested-in-the-tech/

BACK, Adam, 1997. Hashcash – A Denial of Service Counter-Measure. 10.

BAIRD, Leemon, 2016. *THE SWIRLDS HASHGRAPH CONSENSUS ALGORITHM: FAIR, FAST, BYZANTINE FAULT TOLERANCE* [online]. 31. květen 2016. Dostupné z: https://www.swirlds.com/downloads/SWIRLDS-TR-2016-01.pdf

BASHIR, Imran, 2023. *Mastering Blockchain*. 4. Birmingham, Velká Británie: Packt Publishing Ltd. ISBN 978-1-80324-106-7.

BERAN, Pavel, 2019. Představení a analýza IOTA protokolu – 5. část – proof of work a koordinátor. *Medium.com* [online] [vid. 2023-05-05]. Dostupné z: https://medium.com/@pavelberan/ p%C5%99edstaven%C3%AD-a-anal%C3%BDza-iota-protokolu-5-%C4%8D%C3%A1st-proof-of-work-a-koordin%C3%A1tor-77848be564bc

BHANDARY, Mohan, Manish PARMAR a Dayanand AMBAWADE, 2020. *A Blockchain Solution based on Directed Acyclic Graph for IoT Data Security using IoTA Tangle* [online]. 2020. B.m.: 2020 5th International Conference on Communication and Electronics Systems (ICCES), Coimbatore, India, 2020, pp. 827-832. [vid. 2023-05-05]. Dostupné z: doi:10.1109/ICCES48766.2020.9137858.

BINANCE, 2020. Vysvětlení decentralizovaných autonomních organizací (DAO). *Binance Academy* [online] [vid. 2022-10-21]. Dostupné z: https://academy.binance.com/cs/articles/decentralized-autonomous-organizations-daos-explained

BITPESA, 2021. About BitPesa. *Bitpesa.com* [online] [vid. 2023-04-08]. Dostupné z: https://www.bitpesa.co/about/

BLANDIN, APOLLINE AND CLOOTS, ANN SOFIE AND HUSSAIN, HATIM AND RAUCHS, MICHEL AND SALEUDDIN, RASHEED AND ALLEN, JASON GRANT AND CLOUD, KATHERINE AND ZHANG, BRYAN ZHENG, 2019. *Global Cryptoasset Regulatory Landscape Study*. B.m.: {Cambridge Centre for Alternative Finance, Cambridge Judge Business School, University of Cambridge.

BLEMUS, Stéphane, 2023. Societe Generale - Forge launches „Convertible": The first institutional stablecoin deployed on a public blockchain. *SG FORGE* [online] [vid. 2023-04-21]. Dostupné z: https://www.sgforge.com/societe-generale-forge-launches-coinvertible-the-first-institutional-stablecoin-deployed-on-a-public-blockchain/

BUSINESS WIRE, 2023. *Nearly 7,000 Kenyan Farmers Protected by the Lemonade Crypto Climate Coalition* [online] [vid. 2023-04-29]. Dostupné z: https://www.businesswire.com/news/home/20230328005342/en/Nearly-7000-Kenyan-Farmers-Protected-by-the-Lemonade-Crypto-Climate-Coalition

BUSINESSWIRE, 2023. Goldman Sachs' Tokenization Platform GS DAP™, Leveraging Daml, Goes Live. *Businesswire.com* [online] [vid. 2023-04-26]. Dostupné z: https://www.businesswire.com/news/home/20230110005308/en/Goldman-Sachs%E2%80% 99 - Tokenization-Platform-GS-DAP%E2%84%A2-Leveraging-Daml-Goes-Live

BYBIT LEARN, 2022. What Is a Directed Acyclic Graph (DAG)? *Bybitlearn.com* [online] [vid. 2023-05-05]. Dostupné z: https://learn.bybit.com/crypto/what-is-a-directed-acyclic-graph-dag/

ČESKÁ NÁRODNÍ BANKA, 2018. Stanovisko: Je k obchodování s tzv. převodními tokeny nebo k jejich směně vyžadováno oprávnění ČNB? *cnb.cz* [online] [vid. 2023-02-23]. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/stanoviska-k-regulaci-financniho-trhu/RS2018-13/

ČESKÁ REPUBLIKA, 2004. *Zákon č. 256/2004 Sb., zákon o podnikání na kapitálovém trhu*. 2004.

ČESKÁ REPUBLIKA, 2008. *Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu*. 2008.

ČESKÝ STATISTICKÝ ÚŘAD, 2014. Metodické vysvětlivky. *Czso.cz* [online] [vid. 2023-05-27]. Dostupné z: https://www.czso.cz/csu/czso/9605-06-v_roce_2005-metodicke_vysvetlivky

DAI, W., 1998. *B-Money* [online] [vid. 2022-10-19]. Dostupné z: http://www.weidai.com/bmoney.txt

DEMATTEO, Megan, 2022. Bitcoin Price History 2009-2022. *Time.com* [online] [vid. 2022-10-09]. Dostupné z: https://time.com/nextadvisor/investing/cryptocurrency/bitcoin-price-history/

DIEM ASSOCIATION, 2022. *Statement by Diem CEO Stuart Levey on the Sale of the Diem Group's Assets to Silvergate* [online] [vid. 2022-11-11]. Dostupné z: https://www.diem.com/en-us/updates/stuart-levey-statement-diem-asset-sale/

DIGITAL ASSET, [b.r.]. Customer story: Goldman Sachs. *Digitalasset.com* [online] [vid. 2023-04-26]. Dostupné z: https://www.digitalasset.com/customer-story/goldman-sachs

ETHEREUM.ORG, [b.r.]. Decentralized applications (dapps). *ethereum.org* [online] [vid. 2023-04-10]. Dostupné z: https://ethereum.org/en/dapps/

EUROPEAN BANKING AUTHORITY, 2019. *EBA reports on crypto-assets* [online]. 9. leden 2019. [vid. 2022-11-10]. Dostupné z: https://www.eba.europa.eu/eba-reports-on-crypto-assets

EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS AUTHORITY., 2021. *Discussion paper on blockchain and smart contracts in insurance.* [online]. LU: Publications Office [vid. 2023-05-02]. Dostupné z: https://data.europa.eu/doi/10.2854/136043

EVA SZALAY, 2022. Banks turn to blockchain in search for high-quality trading assets | Financial Times. *The Financial Times* [online]. [vid. 2023-04-11]. Dostupné z: https://www.ft.com/content/f23c990a-913d-4613-8014-f61d35b6e09d

EVROPSKÁ KOMISE, 2020. *Návrh Nařízení Evropského parlamentu a Rady o trzích s kryptoaktivy a o změně směrnice (EU) 2019/1937* [online]. 2020. [vid. 2023-05-22]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:52020PC0593

EVROPSKÁ UNIE, 2022. *Nařízení Evropského parlamentu a Rady (EU) 2022/858 ze dne 30. května 2022 o pilotním režimu pro tržní infrastruktury založené na technologii sdíleného registru a o změně nařízení (EU) č. 600/2014 a (EU) č. 909/2014 a směrnice 2014/65/EU* [online]. 2022. [vid. 2023-04-17]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32022 R08 58 &from=EN#d1e725-1-1

EVROPSKÁ UNIE, 2023. *Nařízení Evropského parlamentu a Rady (EU) 2023/1114 ze dne 31. května 2023 o trzích kryptoaktiv a o změně nařízení (EU) č. 1093/2010 a (EU) č. 1095/2010 a směrnic 2013/36/EU a (EU) 2019/1937 (Text s významem pro EHP)* [online] [vid. 2023-06-14]. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32023R1114

EVROPSKÝ PARLAMENT, 2023. Crypto-assets: green light to new rules for tracing transfers in the EU | Zpravodajství | Evropský parlament. *europarl.europa.eu/* [online] [vid. 2023-05-23]. Dostupné z: https://www.europarl.europa.eu/news/cs/press-room/20230414IPR80133/crypto-assets-green-light-to-new-rules-for-tracing-transfers-in-the-eu

FORGE SOCIETE GENERALE GROUP, 2023. *EUR CoinVertible (EURCV), White Paper Version 1.0* [online]. 2023. Dostupné z: https://www.sgforge.com/wp-content/uploads/2023/04/SGF_Coinvertible_White-Paper-v1.0.pdf

FOTR, Jiří a Lenka ŠVECOVÁ, 2022. *Manažerské rozhodování: postupy, metody a nástroje rozhodování v dynamickém a nejistém prostředí*. Čtvrté vydání. Jesenice: Ekopress. ISBN 978-80-87865-76-7.

FRANKENFIELD, Jake, 2021. DigiCash Definition. *Investopedia.com* [online] [vid. 2022-10-19]. Dostupné z: https://www.investopedia.com/terms/d/digicash.asp

FRANKENFIELD, Jake, 2022a. 51% Attack: Definition, Who Is At Risk, Example, and Cost. *Investopedia.com* [online] [vid. 2023-04-13]. Dostupné z: https://www.investopedia.com/terms/1/51-attack.asp

FRANKENFIELD, Jake, 2022b. Initial Coin Offering (ICO): Coin Launch Defined, with Examples. *Investopedia.com* [online] [vid. 2022-10-21]. Dostupné z: https://www.investopedia.com/ terms/ i/ initial-coin-offering-ico.asp

GENÇ, Ekin, 2023. Algorithmic Stablecoins: What They Are and How They Can Go Terribly Wrong. *Coindesk.com* [online] [vid. 2023-05-23]. Dostupné z: https://www.coindesk.com/learn/algorithmic-stablecoins-what-they-are-and-how-they-can-go-terribly-wrong/

HAFFKE, Lars a Mathias FROMBERGER, 2020. ICO Market Report 2019/2020 – Performance Analysis of 2019's Initial Coin Offerings. *SSRN Electronic Journal* [online]. [vid. 2022-10-21]. ISSN 1556-5068. Dostupné z: doi:10.2139/ssrn.3770793

HOLOCHAIN FOUNDATION, [b.r.]. App framework with P2P networking. *Holochain.com* [online] [vid. 2023-05-09]. Dostupné z: https://holochain.org

HONG KONG MONETARY AUTHORITY, 2023. Hong Kong Monetary Authority - HKSAR Government's Inaugural Tokenised Green Bond Offering. *Hong Kong Monetary Authority* [online] [vid. 2023-04-26]. Dostupné z: //www.hkma.gov.hk/eng/news-and-media/press-releases/2023/02/20230216-3/

HOWARD, L. S., 2022. Industry's Blockchain Project, B3i, Ceases to Trade After Filing for Insolvency. *Insurance Journal* [online] [vid. 2023-05-01]. Dostupné z: https://www.insurancejournal. com/ news/international/2022/07/29/677926.htm

JAVŮREK, Karel, 2018. Bitcoin vznikl v roce 2008: Co se vlastně tenkrát stalo? *Connect.cz* [online] [vid. 2022-10-09]. Dostupné z: https://connect.zive.cz/clanky/bitcoin-vznikl-v-roce-2008/sc-320-a-194622/default.aspx

JONES, Evans, 2023. A Brief History of Cryptocurrency - CryptoVantage. *Cryptovantage.com* [online] [vid. 2023-05-20]. Dostupné z: https://www.cryptovantage.com/guides/a-brief-history-of-crypto-currency/

JPMORGAN CHASE & CO., [b.r.]. *Onyx by J.P. Morgan: Transforming the future of banking.* [online] [vid. 2023-04-11]. Dostupné z: https://www.jpmorgan.com/onyx/about.htm

KASHYAP, Bhaskar, 2023. Proof-of-stake (PoS). *ethereum.org* [online] [vid. 2023-04-13]. Dostupné z: https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/

KAWAI, Ken, Kei SASAKI, Aoki SHUNSUKE a Takeshi NAGASE, 2021. Fintech: Japan. *Chambers Global Practise Guides* [online]. Dostupné z: https://www.amt-law.com/asset/res/news_2021_pdf/publication_0022808_ja_001.pdf

KBC GROUP, 2022. *KBC creates a first in Europe with the Kate Coin, its own digital coin based on blockchain* [online] [vid. 2023-04-10]. Dostupné z: https://newsroom.kbc.com/kbc-creates-a-first-in-europe-with-the-kate-coin-its-own-digital-coin-based-on-blockchain

LEDGER INSIGHTS, 2021. Allianz launches blockchain claims solution in 23 countries. *Ledger Insights - blockchain for enterprise* [online] [vid. 2023-04-29]. Dostupné z: https://www.ledgerinsights.com/allianz-launches-blockchain-claims-solution-in-23-countries/

LEDGER INSIGHTS, 2022. Japan's largest bank MUFG provides blockchain utility token issuance platform. *Ledger Insights – blockchain for enterprise* [online] [vid. 2023-04-26]. Dostupné z: https://www.ledgerinsights.com/mufg-provides-blockchain-utility-token-issuance-platform/

LESSNER, Dan, Martin LÁNA, Michala PODRÁZKÁ TOMKOVÁ a Jiří HAUT, 2020. *Základy informatiky pro střední školy* [online]. B.m.: Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta [vid. 2022-10-19]. Dostupné z: https://popelka.ms.mff.cuni.cz/~lessner/mw/index.php/U%C4%8Debnice/Algoritmus/Co_je_to_algoritmus

LEWIS, Antony, 2018. *The basics of bitcoins and blockchains: an introduction to cryptocurrencies and the technology that powers them*. Coral Gables: Mango Publishing. ISBN 978-1-63353-800-9.

LOCKE, Taylor, 2021. From bitcoin hitting $1 trillion in market value to Elon Musk's dogecoin tweets: 12 key crypto moments from 2021. *CNBC* [online] [vid. 2022-10-21]. Dostupné z: https://www.cnbc.com/2021/12/27/12-key-moments-that-fueled-cryptos-record-growth-in-2021.html

MERRE, Ruben, 2021. ICO 101 — History of Initial Coin Offerings (ICOs). *HackerNoon.com* [online]. [vid. 2022-10-21]. Dostupné z: https://medium.com/hackernoon/ico-101-history-of-initial-coin-offerings-icos-part-1-from-mastercoin-to-ethereum-4689b7c2326b

MINISTERSTVO FINANCÍ ČR, ODDĚLENÍ 3502 – PLATEBNÍ SLUŽBY A TRŽNÍ INFRASTRUKTURA a Dič:, 2022. Nařízení o pilotním režimu DLT. *Mfcr.cz* [online] [vid. 2023-02-25]. Dostupné z: https://www.mfcr.cz/cs/soukromy-sektor/platebni-sluzby-a-vyporadani-obchodu/aktuality/2022/narizeni-o-pilotnim-rezimu-dlt-47746

MURPHY, Hannah, Miles KRUPPA a James FONTANELLA-KHAN, 2022. *Facebook gives up on crypto ambitions with Diem asset sale* [online] [vid. 2022-11-11]. Dostupné z: https://www.ft.com/content/e237df96-7cc1-44e5-a92f-96170d34a9bb

NAKAMOTO, Satoshi, 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008, 9.

NATARAJAN, Harish, Solvej KRAUSE a Helen GRADSTEIN, 2017. *Distributed Ledger Technology and Blockchain* [online]. B.m.: World Bank, Washington, DC [vid. 2023-03-13]. Dostupné z: doi:10.1596/29053

R3, 2020a. *Spunta Case Study: Fast and Transparent Interbank Reconciliation Powered by Distributed Ledger Technology* [online]. 2020. Dostupné z: https://r3.com/wp-content/uploads/2022/09/Corda_Spunta_Case_Study_R3_Nov2020.pdf

R3, 2020b. Spunta. *corda.net* [online] [vid. 2023-04-19]. Dostupné z: https://corda.net/modal/spunta/

R3, 2021. Case study: The future of fixed income markets. *R3.com* [online] [vid. 2023-04-21]. Dostupné z: https://r3.com/case-studies/agora/

RADIX PUBLISHING LTD., 2023. *What is the Radix roadmap?* [online] [vid. 2023-05-14]. Dostupné z: https://learn.radixdlt.com/article/what-is-the-radix-roadmap?_gl=1*17 gnw4q*_ ga*MTEyMzQxMz l0OS4xNjg0MDY5NDk5*_ga_MZBXX3HP5Q*MTY4NDA3NDcyOC4yLjEuMTY 4NDA3N TM1NC41 NC4wLjA.

RAPHAEL AUER & MARC FARAG & ULF LEWRICK & LOVRENC ORAZEM & MARKUS ZOSS, 2022. *Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies*. B.m.: Bank for International Settlements. BIS Working Papers 1013.

REED, Andy, 2018. A Look at BitPesa: Powering African Business with Bitcoin. *Wolverine Blockchain* [online]. [vid. 2023-04-08]. Dostupné z: https://medium.com/wolverineblockchain/a-look-at-bitpesa-powering-african-business-with-bitcoin-8b84f2140106

RODRIGUES, Francisco, 2022. Bitcoin Lightning Network vs Visa and Mastercard: How do they stack up? *Cointelegraph.com* [online] [vid. 2023-03-13]. Dostupné z: https://cointelegraph. com/news/bitcoin-lightning-network-vs-visa-and-mastercard-how-do-they-stack-up

SHARMA, Rakesh, 2021. Bitgold: Meaning, Overview, Differences From Bitcoin. *Investopedia.com* [online] [vid. 2022-10-19]. Dostupné z: https://www.investopedia.com/terms/b/bit-gold.asp#citation-2

SHERMAN, Alan T., Farid JAVANI, Haibin ZHANG a Enis GOLASZEWSKI, 2019. On the Origins and Variations of Blockchain Technologies. *IEEE Security & Privacy* [online]. **17**(1), 72–77. ISSN 1540-7993, 1558-4046. Dostupné z: doi:10.1109/MSEC.2019.2893730

SIX DIGITAL EXCHANGE, [b.r.]. SIX Digital Exchange - Home. *Sdx.com* [online] [vid. 2023a-04-29]. Dostupné z: https://www.sdx.com/

SIX DIGITAL EXCHANGE, [b.r.]. Staking. *Web3 Sdx* [online]. [vid. 2023b-04-29]. Dostupné z: https://web3.sdx.com/staking/

SMITH, Corwin, 2023. Blocks. *ethereum.org* [online] [vid. 2023-04-13]. Dostupné z: https://ethereum.org/en/developers/docs/blocks/

SOBOL, Michal, 2022. Co je problém byzantských generálů a jak jej řeší Bitcoin? » Finex.cz. *Finex.cz* [online] [vid. 2022-10-19]. Dostupné z: https://finex.cz/co-je-problem-byzantskych-generalu-a-jak-jej-resi-bitcoin/

SOMPOLINSKY, Yonatan, Shai WYBORSKI a Aviv ZOHAR, 2018. PHANTOM and GHOSTDAG: A Scalable Generalization of Nakamoto Consensus. *Cryptology ePrint Archive* [online]. [vid. 2023-05-05]. Dostupné z: https://eprint.iacr.org/2018/104

STATISTA, 2022. Overall cryptocurrency market capitalization per week from July 2010 to September 2022. *Statista.com* [online] [vid. 2022-10-09]. Dostupné z: https://www.statista.com/statistics/730876/cryptocurrency-maket-value/

VASWANI, Karishma, 2017. China bans initial coin offerings calling them „illegal fundraising". *BBC News* [online] [vid. 2022-10-21]. Dostupné z: https://www.bbc.com/news/business-41157249

WININGER, Shai, [b.r.]. Introducing the Lemonade Crypto Climate Coalition. *Lemonade Blog* [online]. [vid. 2023-04-29]. Dostupné z: https://www.lemonade.com/blog/crypto-climate-coalition/

YEN, David, 2017. Blockchain-based FX/Treasury Solution in Africa. In: [online]. B.m. Dostupné z: http://www.gtreview.com/wp-content/uploads/2017/03/Classroom-style-breakout_How-is-technology-enabling-African-trade.pdf

Seznam obrázků

Obrázek 1 – Agregovaná tržní kapitalizace kryptoaktiv a objem transakcí 12
Obrázek 2 – Centralizovaný, decentralizovaný a distribuovaný systém 15
Obrázek 3 – Schéma blockchainu 28
Obrázek 4 – Schéma Merkleova stromu 30
Obrázek 5 – Schéma DLT DAG 40

Seznam tabulek

Tabulka 1 – Přiřazení vah kritériím dle Saatyho metody 60
Tabulka 2 – Hodnocení variant na kapitálovém trhu z hlediska inovativnosti dle Valenty 62
Tabulka 3 – Hodnocení variant na kapitálovém trhu z hlediska konkurenceschopnosti..... 62
Tabulka 4 – Hodnocení variant na kapitálovém trhu z hlediska výnosnosti 63
Tabulka 5 – Hodnocení variant na kapitálovém trhu z hlediska marketingového potenciálu..... 63
Tabulka 6 – Hodnocení variant na kapitálovém trhu z hlediska interních kapacit 64
Tabulka 7 – Celkové vyhodnocení variant na kapitálovém trhu 65
Tabulka 8 – Hodnocení variant v pojišťovnictví z hlediska inovativnosti dle Valenty..... 65
Tabulka 9 – Hodnocení variant v pojišťovnictví z hlediska konkurenceschopnosti 66
Tabulka 10 – Hodnocení variant v pojišťovnictví z hlediska výnosnosti 66
Tabulka 11 – Hodnocení variant v pojišťovnictví z hlediska marketingového potenciálu 66
Tabulka 12 – Hodnocení variant v pojišťovnictví z hlediska interní kapacity 66
Tabulka 13 – Celkové vyhodnocení variant v pojišťovnictví 67
Tabulka 14 – Hodnocení variant v bankovnictví z hlediska inovativnosti dle Valenty..... 68
Tabulka 15 – Hodnocení variant v bankovnictví z hlediska konkurenceschopnosti 68
Tabulka 16 – Hodnocení variant v bankovnictví z hlediska výnosnosti 69
Tabulka 17 – Hodnocení variant v bankovnictví z hlediska marketingového potenciálu 70
Tabulka 18 – Hodnocení variant v bankovnictví z hlediska interní kapacity..... 70
Tabulka 19 – Celkové vyhodnocení variant v bankovnictví 71

Evidence výpůjček

Prohlášení:
Dávám svolení k půjčování této diplomové práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

Jméno a příjmení: Tomáš Bízek
V Praze dne: Klikněte nebo klepněte sem a za-dejte datum. Podpis:

Jméno	Oddělení/ Pracoviště	Datum	Podpis