Univerzita Hradec Králové

Fakulta informatiky a managementu

katedra ekonomie

TOKENIZACE CENNÝCH PAPÍRŮ

diplomová práce

Autor: Bc. Radek Wildmann

Studijní obor: Informační management

Vedoucí práce: Ing. Jan Mačí, Ph.D.

Hradec Králové duben 2022

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracoval samostatně a uvedl jsem všechny použité prameny a literaturu.

V Hradci Králové dne 27. dubna 2022 Radek Wildmann

Poděkování

Děkuji Ing. Janu Mačímu, PhD. za trpělivost, podnětné rady a pomoc při kontrole této práce.

Anotace

Práce shrnuje dosavadní poznatky ohledně cenných papírů (akcie a dluhopisu) a technologie blockchain v souvislosti s procesem jejich potenciální tokenizace, jak z České republiky, tak ze světa. Výstup práce přináší ucelený návod, jak cenné papíry v České republice tokenizovat. Tento návod zpracovává celý proces od počátečních fází příprav přes právní a technické principy procesu (včetně programovací části) až po vlastní úpis security tokenů (tokenizovaných cenných papírů).

Annotation

The Diploma Thesis is focused on summarization of current knowledge about assets (stocks and bonds) and blockchain technology relating tokenization process in The Czech Republic and also the rest of the world and presenting complete instructions to perform tokenization in The Czech Republic. Manual goes through the whole process from early preparation phases follow by legal and technical perspective (including programming phase) and with emission of security token (tokenized assets) ends.

Obsah

Úvod

Rychlý technologický vývoj. Spojení, které v dnešní době rezonuje napříč odvětvími a světadíly. Nelze přehlédnout, jak rychle se dnes jednotlivá odvětví mění, ať už ta méně či více konzervativní. Není tomu tak dávno, kdy neexistovaly mobilní technologie, robotická výroba byla v začátcích a virtuální realita prakticky neexistovala . Dnes tu jsou telefony, které mají větší výkon než 3 roky staré počítače, a blíží se období, kdy bude zboží dováženo drony a pracovní meetingy svolávané s brýlemi na očích přes celý svět. Vývoj se dotýká nás všech, a proto není divu, že ani konzervativní odvětí, jakým je finanční sektor, se mu nevyhne. Zejména odvětví bankovnictví patří va adaptaci nových technologií k těm pomalejším.[28] Vždyť teprve až nedávná COVID krize donutila mnohé instituce přejít do online formy uzavírání smluvních vztahů a řízení komunikace se zákazníky. I přes tato úskalí, zejména pak v souvislosti s právním rámcem, k vývoji levnějších a efektivnějších nástrojů ve finančním sektoru dochází.

Již je to pár let, co technologie blockchain vznikla. Technologie, která je dnes většině známá zejména díky kryptoměnám, jež ji využívají. Kryptoměny v čele s bitcoinem jsou dnes používány zejména k investičním a spekulativním účelům, i přestože mnozí věří, že by mohly nahradit tzv. fiat měny, tedy peníze, kterými jsme dnes zvyklí platit. Tyto virtuální měny však nejsou jediný způsob využití této virtuální účetní knihy, kterou blockchain představuje.

Pokud chce dnes společnost získat kapitál pro svou činnost, má hned několik možností. Kromě standardních neveřejných nástrojů financování jako bankovní úvěry existují i další cesty, jak oslovit veřejnost, a to pomocí emise cenných papírů, zejména pak dluhopisů a akcií. A právě k emisi, resp. tokenizaci, těchto cenných papírů lze techno-

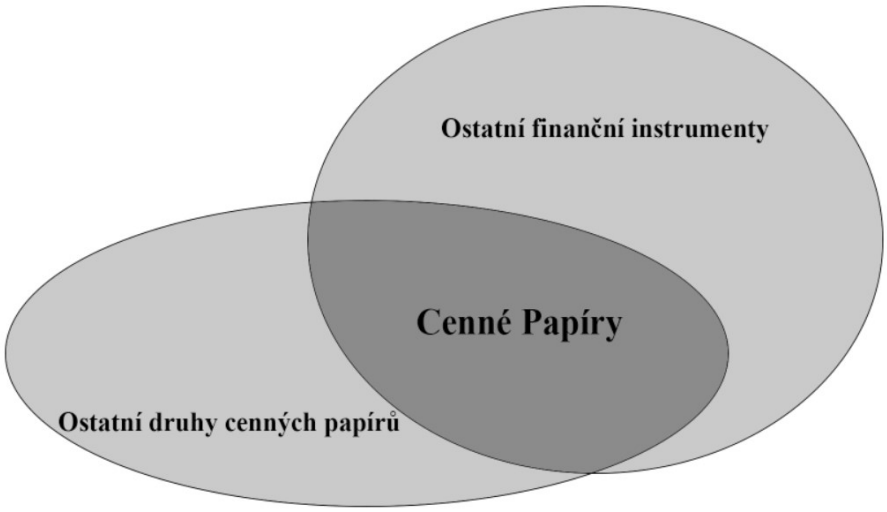
logie blockchain použít.

Tokenizací se zabývá i tato práce. Jejím cílem je čtenářovi přiblížit technologii, která za ní stojí. Vysvětlit zejména technologické, procesní, regulatorní i ekonomické výhody a nevýhody takového přístupu k vydání cenného papíru oproti standardní cestě emise. A neposlední řadě pak poskytnout ucelený návod, jak takovou tokenizaci akcie či dluhopisu provést v České republice.

Práce je rozdělena do několika kapitol. Kapitola 1. se zabývá fungováním akcií, dluhopisů a krátce se dotýká i jiných cenných papírů. O historii a fungování blockchain technologie pojednává 2. kapitola. Ve 3. kapitole je vysvětlena samotná tokenizace. Zpracovává se zde způsob jejího provedení, dále je ukázáno porovnání tokenizace se standardní emisí. V závěrečné kapitole jsou shrnuty výsledky práce.

1 Cenné papíry

Pod termínem cenný papír je mnohdy chybně označováno vše, co člověk považuje za investici, ke které je vydán nějaký dokument říkající, že někdo je majitelem něčeho. V praxi se však pojmem cenný papír označují pouze některé finanční investiční instrumenty. Z právního hlediska jsou cennými papíry pouze právně vymezené dokumenty, které za cenný papír prohlásil daný stát[1]. Cenným papírem pak nemusí být jen finanční investiční instrument, ale ani se nemusí jednat o nástroj finančního charakteru. Toto je znázorněno na obrázku 1.2.



Obrázek 1.1: Právní vymezení cenných papírů [25]

[1] V ČR toto do roku 2014 upravoval zákon o cenných papírech, který byl po roce 2014 v základu nahrazen občanským zákoníkem. Specificky pak jednotlivé cenné papíry upravují příslušné zákony (např. zákon o dluhopisech)[16]

Vedle cenných papírů finančního charakteru totiž existují i druhy, které s finančním systémem či trhy nesouvisejí. Jedná se zejména o cenné papíry ve vztahu s komoditami, mezi které patří například zemědělské skladní listy či konosamenty [2]. Takto vymezená množina cenných papírů však neobsahuje pouze investiční cenné papíry, ale i neinvestiční jako například šeky (tedy platební instrumenty). Je tedy zřejmé, že finanční instrumenty, ani pokud jsou to obchodovatelné nástroje investiční povahy, nelze obecně zaměňovat s cennými papíry. [25] [2]

Klasické [3] cenné papíry jsou nejvýznamnější investiční instrumenty finančního trhu. Představují totiž základní konstrukce investičních cenných papírů a také jejich standardní vlastnosti. Zároveň bývají emitovány a uváděny do oběhu prostřednictvím primárního trhu. Cenné papíry se dají rozdělit do následujících kategorií:

1. Z hlediska délky jejich životnosti
    - **Cenné papíry peněžního trhu** mají zpravidla dobu životnosti do jednoho roku
    - **Cenné papíry kapitálového trhu** mají zpravidla dobu životnosti větší než jeden rok
2. Podle majetkové podstaty
    - **Majetkové cenné papíry** zpravidla akcie
    - **Dluhové cenné papíry** zpravidla dluhopisy

Tato práce se zabývá právě akciemi a dluhopisy. Řeší jejich vlastnosti a zejména pak způsob, jak tyto cenné papíry vydat s použitím technologie blockchain. [25] [2]

[2] Konosament, neboli náložní list, je dokumentem používaným v lodní přepravě. Potvrzuje, že přepravce převzal zboží, které předá majiteli konosamentu. [25]

[3] Označení *klasické* je použito z toho důvodu, že jako cenné papíry jsou označovány rovněž některé druhy strukturovaných produktů, jejichž vlastnosti jsou úplně odlišné. [25]

1.1 Akcie

Akcie jsou považovány za klasické cenné papíry [4]. Jejich zakoupením nabývá akcionář práv společníka tím, že majetkově vstupuje do dané akciové společnosti. Význam těchto akcií spočívá za prvé v tom, že jejich prodejem na primárním trhu si firma opatřuje peněžní prostředky, které na rozdíl od dluhových cenných papírů nemusí později vracet. Za druhé přitahují tyto cenné papíry díky svým vlastnostem celou řadu investorů. Ti se snaží vedle běžných výnosů (dividend) koupí akcie dosáhnout i výnosů kapitálových, vyplývajících z růstu, nebo poklesu ceny akcie. Akciové trhy tedy krom umisťování dlouhodobých peněžních prostředků slouží také ke spekulačním účelům. Skutečnost, zda a jakou bude vlastník akcie dostávat dividendu, či jak bude růst, nebo klesat hodnota akcie, pak záleží zejména na hospodářských výsledcích dané frmy.[25] [2]

Obrázek 1.2: Příklad fyzické podoby podnikové akcie.[20]

Existuje velké množství různých druhů akcií. Vzájemně se liší mnohými vlastnostmi, včetně druhu práv, která jsou s jejich vlastnictvím spojena. Tyto rozdíly jsou způsobeny různými legislativními rámci, dle kterých k emitování dochází. Záleží tedy na míře vol-

[4] Mluvíme o podnikových akciích.

nosti, co legislativa odsouhlasí a jakou volnost společnosti udělí. V této kapitole jsou v rychlosti vysvětleny dva typy akcií, neboť ty jsou pro práci stěžejní a pravděpodobně to budou právě tyto druhy, jež budou emitovány přes blockchain. [25] [2]

Kmenové akcie

Kmenové akcie, anglicky nazývané *common stocks*, s sebou nesou tři základní práva akcionářů, přičemž platí, že životnost akcie ani s ní spojená práva nejsou časově ohraničená [5]:

- Právo účastnit se valných hromad společnosti a hlasovat s hlasovací silou odpovídající počtu držených akcií.
- Právo na odpovídající podíl na zisku společnosti vypláceném formou dividend.
- Právo na odpovídající podíl na likvidačním zůstatku společnosti.

S kmenovými jsou tedy spojená výše uvedená práva. Tato práva jsou označována jako standardní, další druhy akcií tato práva rozšiřují či jinak upravují. Vlastník kmenové akcie se však plně vystavuje i všem rizikům s nimi spojenými. Zisky společnosti mohou klesat nebo firma může zkrachovat. V případě likvidace jsou pak z dostupných aktiv zaplaceny nejdříve dluhy, poté majitelé prioritní akciií, o nich bude řeč později, a až poté se zbývající majetek rozdělí mezi majitele kmenových akcií. Proto mají tito majitelé právo hlasovat o všech záležitostech společnosti, a to ve věcech procesních i personálních. Aby mohli udržet svůj poměrný podíl ve společnost, disponují předkupním právem, pokud by firma vydávala akcie nové. [25] [2]

Prioritní akcie

Prioritní akcie, anglicky *preferred stock*, je podkategorií tzv. akcií se zvláštními právy. Kombinují v sobě standardní vlastnosti kmenových akcií s některými vlastnostmi obligací. Důvodem jejich emise je zvýšení kapitálu společnosti bez toho, aby se měnil

[5] Vyjma úpadku firmy, či snižování základního kapitálu firmy.

stávající poměr hlasovacích práv a aniž by se takto získané prostředky musely později vracet. S těmito akciemi tak často nebývá spojeno hlasovací právo jako u kmenových akcií. Držitelům však přináší některé výhody. Mezi tyto výhody může patřit dopředné určení výše dividendy. Tato výše pak nezávisí na hospodářském výsledku společnosti, ani na tom jak vysokou dividendu si odhlasují vlastníci kmenových akcií na valné hromadě. Další výhodou pak může být přednostní právo na likvidačním zůstatku společnosti. Držitelé prioritních akcií se tak k případnému zbylému majetku dostanou dříve než majitelé akcií kmenových. [25] [2]

Všechny emise prioritních akcií musí být vždy v souladu jak se zákony příslušných zemí, tak se stanovami akciové společnosti, která tyto cenné papíry vydává. Všeobecnou zásadou je, že podíl prioritních akcií nesmí překročit legislativně stanovený maximální podíl na základním kapitálu akciové společnosti [6].[25]

1.2 Dluhopisy

Dluhopisy jsou dalším způsobem, jakým může firma získat kapitál. Na rozdíl od akcií s nimi však není spojeno vlastnictví podílu na majetku společnosti, ale na jejím dluhu. Zároveň firma, která získala peníze prostřednictvím emise dluhopuisů, musí tyto peníze později vrátit zpravidla s připočtením úroků. Na světovém trhu potom existuje velká řada různých typů dluhopisů. Vzhledem k volnějším možnostem než u akcií se pak jedná o typy ohraničené pouze zákony daného státu. [25]

Zvažujeme-li členění z hlediska délky splatnosti jako základní členění, lze je rozdělit na krátkodobé dluhopisy peněžního trhu s délkou splatnosti zpravidla do jednoho roku a na dlouhodobé dluhopisy kapitálového trhu, které se také označují jako obligace, a jejich doba splatnosti je zpravidla delší než jeden rok. [25]

[6] v ČR je tento limit 100% (stav v roce 2022)

Obrázek 1.3: Příklad fyzické podoby dluhopisu.[26]

Krátkodobé dluhopisy peněžního trhu

Nejvýznamnějšími druhy krátkodobých dluhopisů jsou:

- **Státní pokladniční poukázky**
  - Jde o krátké státní dluhopisy, anglicky *teasury bills*, používané na vyrovnání nesouladu ve státním rozpočtu. Emitentem je ministerstvo financí skrze centrální banku. Na trh bývají uváděny formou uzavřených aukcí pro určitý sektor finančních institucí. Jejich životnost se pohybuje od 3 do 12 měsíců.[25]
- **Pokladniční poukázky**
  - Tyto krátkodobé dluhové cenné papíry emituje centrální banka z měnových důvodů.[25]

- **Depozitní certifikáty**
  - Jedná se o dluhopisy, které potvrzují investorovi vklad jeho prostředků, obdoba termínovaných vkladů. Mohou být diskontované, či nést předem stanovený úrok. [25]
  - Doba těchto dluhopisů opět nepřesahuje 12 měsíců a vydávají je především komerční banky.[25]
- **Směnky**
  - Z hlediska jejich vlastností se jedná o krátkodobé, individuálně vydávané dluhopisy. Představují jednostranný slib výplaty peněz bez právních výhrad a podléhají směnečnému právu [7].[25]

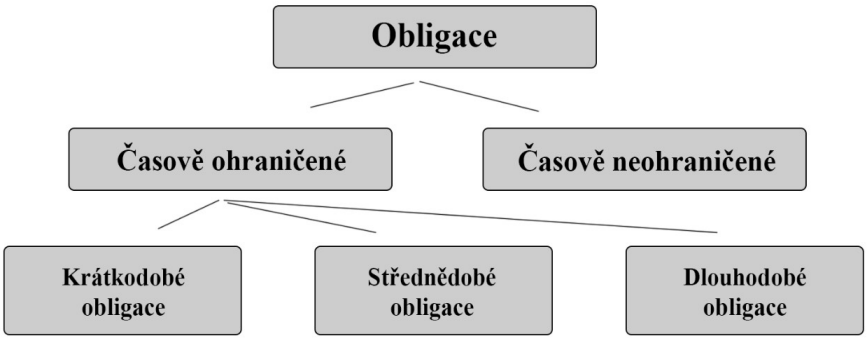
Dlouhodobé dluhopisy

Jednou z charakteristických vlastností dlouhodobých dluhových cenných papírů je mezinárodní označení anglickým slovem *obligace*. Délka jejich splatnosti je obecně delší než jeden rok, díky tomu bývají veřejně obchodovatelné. Existuje celá řada práv, která jsou spojená s těmito obligacemi. Podle těchto práv se obligace člení. Pro účely práce postačí vysvětlit členění dle délky splatnosti a dle výnosů plynoucích z jejich držby. [25]

Členění z hlediska délky splatnosti

Délku splatnosti obligace lze považovat za jedno z nejdůležitějších kritérií pro systematizaci vůbec. Dlouhodobé dluhopisy tak můžeme rozdělit do tří kategorií, a to krátkodobé (splatnost 1-5 let), střednědobé (splatnost 5-10 let) a dlouhodobé (splatnost 10 a více let). Přestože je fakt, že dluhopis má nějakou dobu splatnosti, považován za implicitní, nemusí tomu tak ve skutečnosti vždy být. Některé státy totiž umožňují existenci dluhopisů, které nemají v emisních podmínkách žádné datum splatnosti. Tyto dluhopisy

[7] V ČR jsou řešeny zákonem směnečným a šekovým.



Obrázek 1.4: Členění obligací z hlediska délky splatnosti [25]

se nazývají dluhopisy věčné. Populární jsou zejména v zahraničí (Velká Británie, USA). Jistinu z takové obligace je možné obdržet pouze jejím prodejem. Graficky znázorněné členění lze vidět na obrázku 1.4. [25] [17]

Členění z hlediska výnosů plynoucích z držby

S obligacemi mohou být spojeny různé druhy běžných výnosů i různé způsoby jejich výpočtů a nároků na jejich vyplácení. [25]

- **Kuponové obligace**
  - Jedná se v praxi o nejčastěji emitovaný a zároveň nejrozšířenější druh obligace. Držitelé mají nárok na běžné výnosy v předem určených termínech na základě tzv. kuponů. [25]
- **Diskontované (bezkuponové) obligace**
  - Anglicky *zero-coupon bonds* jsou emitovány s tzv. diskontem. Jsou tedy na primárním trhu prodávány s nižší hodnotou, než je jejich nominální hodnota. Tento rozdíl pak nahrazuje kuponové platby a zmenšuje se s přibližujícím se datem splatnosti. [25]
- **Obligace s kombinací vlastností kuponových a diskontovaných**

– Většinou se jedná o dluhopisy, které jsou emitovány jako bezkuponové a v emisních podmínkách je informace, že po určité době držení začne vyplácení kupónů.[25]

1.3 Ostatní cenné papíry

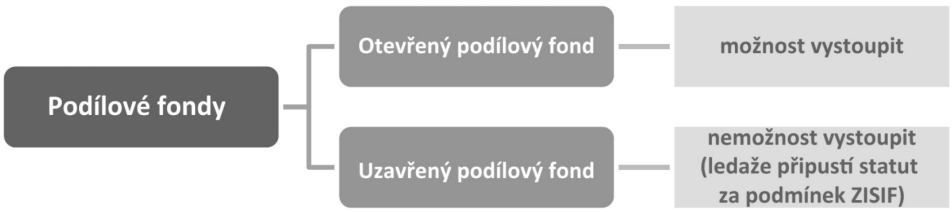
Vedle klasických cenných papírů, o kterých byla zmínka v předchozích odstavcích, existuje celá řada dalších cenných papírů. I když jejich fungování není pro práci stěžejní, pro ucelenější obrázek o tématu cenných papírů je nutné je zmínit, neboť s akciemi a dluhopisy velmi často úzce souvisí. V této kapitole je krátce vysvětlen zástupce termínových derivátových instrumentů **Opce**, zástupce strukturovaných produktů **Investiční certifikáty** a cenné papíry podílových fondů **Podílové listy**.

Podílové listy

Podílové listy jsou cenné papíry podílových fondů. Podílové fondy jsou instrumentem spočívajícím na principu kolektivního investování, kdy velká skupina drobných investorů shromažďuje majetek v takovém fondu, který jej následně investuje dle předem dohodnuté investiční strategie. Podílové fondy nemají právní subjektivitu. Jejich majetek náleží přímo podílníkům v poměru podle počtu vlastněných podílových listů. Podílové fondy jsou spravovány zpravidla investiční společností s tím, žpřejímajíaaaaaaaaae vložené prostředky investorů zůstávají jejich majetkem a investiční společnost jim je pouze spravuje v souladu se statutem daného fondu. [25] [2]

Investování do podílových fondů pak probíhá tak, že investoři nakupují od investiční společnosti nikoli akcie, ale podílové listy. Tímto se stávají podílníky fondu. Investiční společnost jim pak majetek za úplatu spravuje. Podílové fondy existují ve dvou základních variantách, a to jako otevřené, či uzavřené. Od otevřeného podílového fondu si může investor podílové listy kdykoliv nakoupit a zároveň má takový fond povinnost odkoupit tyto podílové listy za předem stanovenou cenu zpět. Uzavřený podílový fond

pak umožňuje zakoupení si jeho podílových listů po omezenou dobu. Nárok na vyplacení investovaných prostředků vzniká až po uplynutí určité doby. Grafické znázornění členění podílových fondů je znázorněno na obrázku 1.5. [25] [2]

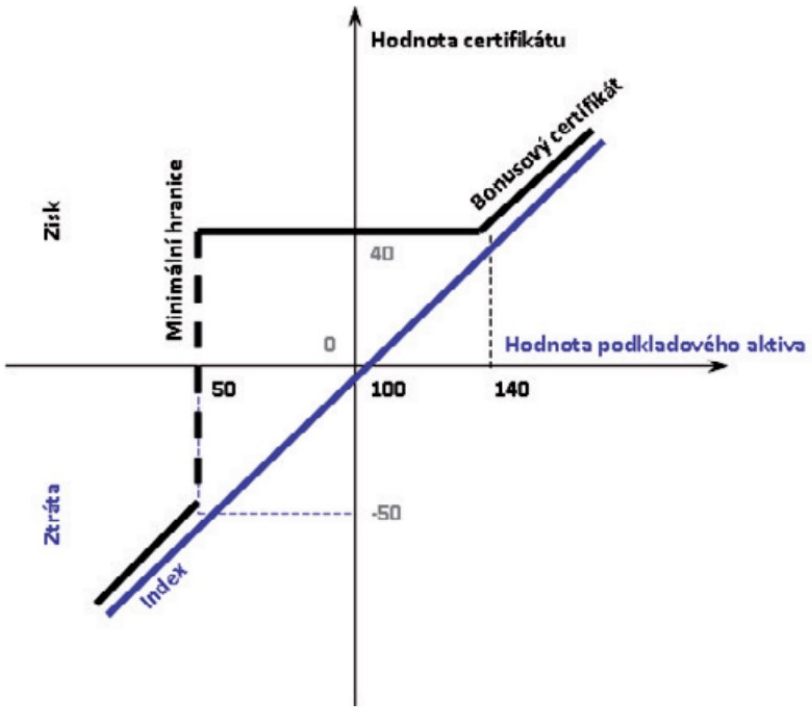


Obrázek 1.5: Základní členění podílových fondů [2]

Investiční certifikáty

Investiční certifikáty jsou zkráceným názvem pro Investiční strukturované certifikáty. Jsou to dluhové cenné papíry emitované finančními institucemi, které jejich prostřednictvím získávají finanční prostředky. Bývají časově neohraničené, či ohraničené. Podkladovým aktivem bývají zpravidla akciové indexy nebo individuálně konstruované akciové koše.[25]

Investiční certifikáty kombinují základní vlastnosti dluhopisů a některých finančních derivátů. Od dluhopisů přejímají jasně ohraničený, či naopak časově neohraničený termín splatnosti a také to, že jsou obchodovány na veřejných trzích. Od finančních derivátů přejímají skutečnost, že odvozují svou tržní cenu od vývoje cen podkladových aktiv. V případě časově ohraničených investičních certifikátů mají jejich držitelé právo na vyplacení v době splatnosti. Výše výplaty se odvíjí od hodnoty podkladového aktiva způsobem stanoveným v emisních podmínkách. Příklad certifikátu je uveden na obrázku 1.6. [25]



Obrázek 1.6: Příklad odvození hodnoty certifikátu[8]od hodnoty podkladového indexu. [1]

Opce

Opce je vydávána na základě opční smlouvy, která říká, že má držitel opce právo na nákup nebo prodej podkladového aktiva v předem dohodnutém období za předem dohodnutou cenu. Jedná se o tzv. podmíněný termínový kontrakt. Obchodují se buď smluvně, či na opčních burzách. Opce jsou tak v praxi velmi častým nástrojem používaným k zajištění *(hedgingu)* nebo spekulaci. Postavení účastníků opčních obchodů je pak následující: [25]

- **Zakoupením** opce má držitel právo volby podkladové aktivum koupit nebo prodat. Za toto právo platí kupní cenu opce *(opční prémii)*. Tato prémie je však pouze

[8]Jedná se o tzv. bonusový certifikát. Pokud se hodnota podkladového aktiva (v tomto případě nějakého indexu) pohybuje v určeném rozmezí, investor dostává bonusový výnos nad úroveň výnosu tohoto podkladového aktiva. Jakmile hodnota klesne, či stoupne nad stanovenou hranici, kopíruje certifikát výkonnost podkladového aktiva 1:1.

zlomkem ceny podkladového aktiva, k jehož nákupu či prodeji daná opce opravňuje. [25]

- **Vypsáním** opce se člověk dostává do opačné pozice. Obdrží opční prémii za výpis opce, je však následně povinen na vyzvání držitele opce mu buď prodat, nebo od něho koupit dané podkladové aktivum za domluvenou (strike) cenu. [25]

2 Blockchain technologie

V roce 2008 svět zasáhla velká finanční krize, někdy také označovaná jako Velká recese[1]. Mnoho podniků krachovalo a lidé ztráceli víru ve finanční a bankovní systém. Ve stejný čas, a možná právě kvůli probíhající krizi, vznikl Bitcoin. Kryptoměna, která ke svému fungování nepotřebuje vládu, banku ani jinou instituci. Je rozšířená po celém světě, decentralizovaná a rezistentní vůči útokům. Vznikla nová blockchain síť řízená myšlenkou *kód je zákon ve vlastnictví lidí*. [15]

Technologie blockchain umožnila vznik bitcoinu a dalším kryptoměnám. Co však vzniklo jako základ pro digitální měnu, dnes umožňuje lidem digitalizovat cenné papíry a to bez bank či jiných institucí. Místo toho, abychom cenné papíry, jako akcie a dluhopisy pouze převedli do digitální podoby pod taktovkou banky, je využito distribuované databáze, zabezpečené matematickým algoritmem a použitelné po celém světě. Žádné centralizované místo, které by šlo vypnout, žádný diktát ze strany finančního regulátora. [15] [6]

Pojmenování blockchain technologie nebo častěji jednoduše blockchain je dnes používáno v mnoha kontextech, a může tak být zavádějící, co tím chtěl autor říci. Hodně lidí totiž používá tato označení pro různé věci. Přesnější pojem je spíše databáze, nebo lépe distribuovaná účetní kniha [2]. Proč je tedy potřeba nové paradigma, když již existuje

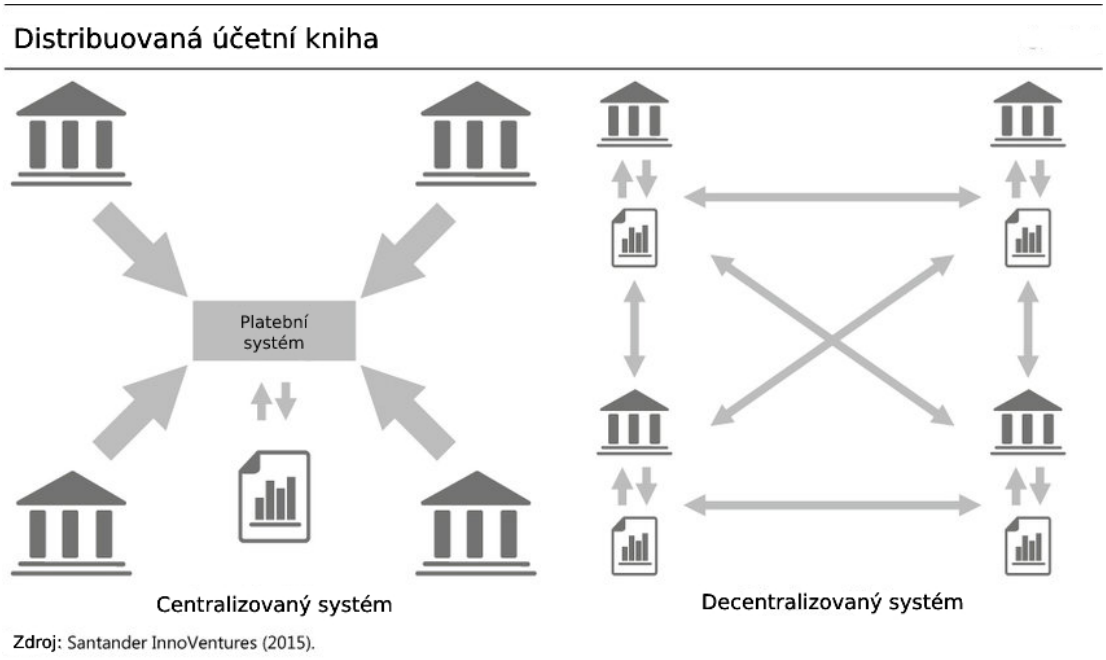
[1] Tato krize byla způsobena splasknutím bubliny na americkém hypotečním trhu a díky nedostatečně rychlé intervenci ze strany americké vlády zasáhla krize celý svět. [22]

[2] Distribuovaná účetní kniha je nadmnožinou blockchainů, kterých může být mnoho. Proto, pokud chceme mluvit o technologii jako takové a ne o konkrétní síti, je lepší použít označení distribuovaná účetní kniha [19]

způsob, jak ukládat informace, tedy databáze? Každý počin, který se dnes na internetových platformách jako jsou například sociální sítě uskuteční, vygeneruje nějaká data. Tato data jsou pak zaznamenána a uchována v databázi, již vlastní firma provozující danou sociální síť. Stejně tak to funguje i v případě bankovní platby. Jednoduše je zadán příkaz, že z jednoho účtu má být převedena nějaká suma peněz na jiný bankovní účet. Banka má někde databázi bankovních účtů se jmény a zůstatky svých zákazníků. Pokud se takový příkaz objeví, instituce jednoduše aktualizuje údaje zůstatku na účtech těch, mezi kterými převod proběhl. Protože existuje důvěra v banku, vypořádávání probíhá na její straně v její databázi. Je zadán příkaz a banka jej provede. Blockchain, resp. distribuovaná účetní kniha, se zvažuje ve chvíli, kdy je uvažováno o transakci bez banky či jakékoliv jiné instituce jako prostředníka, který by databázi vlastnil. Schématické porovnání centralizovaného a blockchainového potvrzování dat je znázorněno na obrázku 2.1.Jak je zaručeno, že mají všichni přístup ke svým penězům, když neexistuje žádná banka? Co když daný člověk bude tvrdit, že má více peněz, než reálně má a není tu žádná třetí strana, která by takovou skutečnost ověřila? [15][19] [6]

Bitcoin byl první, kdo blockchain použil a dal odpověď přesně na tyto otázky. Dodal lidem monetární systém, který řídí sami uživatelé bez banky či jiné třetí strany. **Decentralizace** je prvním základním principem této nové technologie. Databáze není vlastněna nebo poháněna jednou entitou, nýbrž velkým množstvím jejich různých uživatelů. Banka, která doteď transakce potvrzovala, byla nahrazena neznámými lidmi, kteří se o potvrzování zůstatků účtů a transakcí starají. Abychom měli jistotu, že se těmto neznámým validátorům dá věřit, blockchain implementuje jistá opatření k zajištění takové důvěryhodnosti viz 2.3. Bez těchto opatření by síť nemohla fungovat. [6] [19]

Druhým základním principem této sítě je **distribuovanost**. Nejenom, že jsou data v blockchainu potvrzována více lidmi, jsou také duplikována na mnoha místech. Je tak velmi těžké takovou síť napadnout, neboť jsou jednotlivé uzly sítě a potvrzovatelé transakcí rozmístěni po celém světě. Představte si banku se zaměstnanci a fyzickými pobočkami. Zrušit takovou instituci není nic těžkého. Pokud se však síť skládá z milionů uživatelů, kteří řídí její chod, je bezpečné tvrdit, že taková síť je vůči zásahům zvenku



Obrázek 2.1: Schématické porovnání potvrzování dat centralizovaného systému a decentralizovaného systému

imunní. Je třeba si říci, že tento popis blockchainu se vztahuje k blockchainu vytvořeném v roce 2008. Dnes existují různé další varianty takové sítě, například sem patří privátní varianta blockchainu, přístupná pouze určitým identifikovaným uživatelům atd. [19] [6]

Třetím elementem blockchainu je **transparentnost**. Ať už se jedná o soukromou nebo veřejnou variantu sítě, je možné zajistit, aby každá transakce byla viditelná každému uživateli v síti. Privátní blockchain tyto informace nezveřejňuje každému, ale pouze vybrané skupině lidí. I v tomto případě je proces transparentní, neboť každá akce na síti je zaznamenána. Pokud někdo podvádí, o jeho podvodu se ostatní (byť pouze určená skupina) dozví. Příkladem tohoto typu může být konsorcium pěti různých bank, které sdílejí privátní blockchain, protože nechtějí, aby někdo mimo toto shromáždění viděl, jaké transakce si vyměňují. Uvnitř konsorcia jsou však transakce viditelné a banka 1 může například vidět, že banka 2 provádí nepovolenou transakci, aby poškodila banku

3. [19] [6] [15]

Bezpečnost je v případě blockchainu zajištěna matematickými funkcemi (hashovací funkce). Kdyby se někdo pokoušel podvádět, všichni by to okamžitě zjistili. To samé platí pro úpravu či mazání již zapsaných dat. Tím, že každý má kopii poslední verze této účetní knihy, blockchainu, jsou všichni schopni okamžitě zaznamenat jakékoliv změny v datech, které jsou podvodné. Co je na blockchainu zapsáno a schváleno, z blockchainu nejde smazat ani změnit. [15] [19]

Blockchain je užitečný ve chvíli, kdy nelze, nebo nechceme věřit konkrétnímu subjektu nebo subjektům. Pokud by například banka A kooperovala s bankou B a banka B by měla na starosti správu databáze dat, pak by banka A musela věřit, že banka B dělá vše poctivě a správně. Toto není bezpečné a efektivní řešení. Databáze nepatří ani bance A ani bance B. Obě mohou navrhnout změny v této distribuované účetní knize, avšak pouze pokud se obě shodnou a vytvoří konsensus, je transakce provedena. Nikdo tak nemusí na nikoho spoléhat a vše je provedeno pouze, pokud se dojde ke shodě. Blockchain je tedy distribuovanou účetní knihou, která je sdílená určitou skupinou lidí (uzavřenou - private či otevřenou - public) a vytváří tak chráněné důvěryhodné prostředí bez nutnosti spoléhat na jakoukoliv třetí stranu. [15] [19]

Obrázek 2.2: Grafické znázornění blockchainu [15]

Blockchain, v češtině *řetězec bloků*, je název odvozený od stylu, jakým jsou data v této distribuované účetní knize zapsána. V klasické databázi, která je známá po staletí, jsou data zapsána v řadách, kde jedna informace následuje za druhou. Blockchain, jak již název vypovídá, zapisuje data do bloků. Tento blok pak připomíná standardní databázi,

tedy informace psané v řádcích. Důležité však je, že jednotlivé bloky dat jsou spojeny jeden za druhým tak, že tvoří řetězec. Odtud tedy název *řetězec bloků*, Blockchain. Grafické znázornění je zobrazeno na obrázku 2.2. Tato struktura v jednoduchosti zaručuje právě onu bezpečnost. Bloky jsou svázány jeden s druhým a pokud by někdo chtěl změnit data v konkrétním bloku, toto propojení by bylo přerušeno. Takovéto rozpojení by pak bylo zaznamenáno uživateli, kteří by viděli, že je řetěz porušen a došlo k manipulaci s daty. Veškeré tyto věci jsou zajištěny matematickými algoritmy. [15] [19]

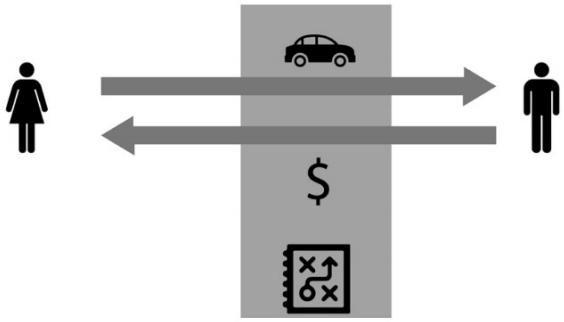
2.1 Jaké problémy pomáhá blockchain řešit

Jak již bylo řečeno na začátku této kapitoly, blockchain jako technologie má různé způsoby využití. Bitcoin je používán jako platidlo nebo investiční aktivum, zatímco další významná kryptoměna Ethereum je používaná k něčemu, co se nazývá *Smart Contracts* (tento pojem je vysvětlen na příkladu dále v této kapitole) a stovky dalších blockchainů mají zase jiná využití. [15] [19]

Pokud prvně slyšíte o blockchainu, o distribuované účetní knize, mnoho lidí si klade otázku, proč je potřeba takto komplexní decentralizované infrastruktury, když zde již staletí máme klasické databázové systémy pro uchování dat. Tato otázka je více než na místě, když vezmeme v potaz fakt, že tato technologie je často používána na místech, kde nemá žádné reálné výhody oproti klasickým centralizovaným systémům. V mnoha případech může mít Blockchain technologie přínos, umožňuje procesy, které by jinak kvůli své decentralizované povaze nešly uskutečnit. [15] [19]

V následujícím příkladu vystupují dva aktéři Kateřina a Tomáš, kteří chtějí uskutečnit prodej auta. Kateřina chce prodat své auto na internetovém bazaru a Tomáš by jej rád koupil. Bydlí daleko od sebe, Tomáš je však ochoten zaplatit za dovoz auta do jeho města. Nicméně musí zaplatit Kateřině peníze dopředu, aniž by si mohl fyzicky ověřit, že auto opravdu vlastní. Mohl by teoreticky poslat peníze přes kurýra, který k němu auto odveze. Kurýr však nemůže zkontrolovat, že vyzvedl opravdu správné auto. Tomáš tak může být Kateřinou podveden. Opačně Kateřina nechce být podvedena, a proto

požaduje peníze předem. Nikdo se nepohne dál, dokud jedna strana na sebe nevezme riziko a nepošle peníze nebo auto předem. Tento problém může Blockchain odstranit.



Obrázek 2.3: Grafické znázornění obchodu mezi Kateřinou a Tomem s použitím chytrého kontraktu jako notáře [15]

Konkrétně onen tzv. chytrý kontrakt (Smart Contract). Není to nic jiného než tzv. *if-else* konstrukce. Když nastane určitá podmínka, poté se něco stane. Chytrý kontrakt si lze představit jako digitální formu notáře, který se stará o to, aby se všichni zúčastnění chovali tak, jak jim nařizuje dohoda. V tomto případě by to fungovalo následovně:

1. Kateřina i Tomáš odešlou předměty dohody (peníze a auto) do tohoto chytrého kontraktu.

2. Chytrý kontrakt neustále kontroluje, jestli obě strany dostály dohody. Pokud ano, pak vydá peníze Kateřině a auto Tomášovi.

V tomto případě chytrý kontrakt zastává funkci úschovy. Drží peníze a auto do doby, než obě strany splní svoji část dohody. Díky použití Blockchainu tak nebylo zapotřebí lidského notáře, který by úschovu zprostředkoval. Vše automaticky zařídil chytrý kontrakt. Bude ještě chvíli trvat, než síť automaticky vypořádá i hmotné statky. Dnes se Blockchain používá zejména pro věci v digitální podobě. [15] [6]

Úschova je pouze jeden jednoduchý příklad z možných využití takového chytrého kontraktu. Může být použit na mnohem složitější věci naprogramováním digitálních

smluvních kontraktů, které požadují konsensus, aby byly naplněny. Další konkrétní příklady využití mohou být:

- **Zpoždění letu**: Chytrý kontrakt neustále kontroluje, jestli byl let zpožděn, pokud ano, automaticky vrátí peníze.
- **Dividendy**: Kdykoliv se na valné hromadě schválí rozdělení zisků, dividendy jsou automaticky odeslány akcionářům.
- **Dědictví**: Chytrý kontrakt kontroluje, jestli je někdo naživu. Pokud zemře, vyřídí dědictví s pozůstalými.

Blockchain, distribuovaná účetní kniha, databáze ve formě zřetězených bloků řízená mnoha uživateli, kteří spolu mohou interagovat i v situacích, kdy nemohou, nebo nechtějí někomu věřit (ať už se jedná o protistranu, či nějakou třetí stranu). Spoléhají na konsensus, a tím pádem nemůžou jeden druhého podvádět. Informace jsou v síti zapsané v blocích, které jsou jeden s druhým propojené. Díky matematickým funkcím je zajištěno, že jakákoliv snaha o manipulaci dat je ihned odhalena. Data jsou tak dokonale chráněna. [15] [6]

2.2 Historie

První implementace moderního Blockchainu pochází od Satoshi Nakamota z roku 2008. Osoba nebo skupina osob pod pseudonymem Nakamoto publikovala článek, „Bitcoin: A Peer-to-Peer Electronic Cash System," v němž vysvětluje koncept online platby jednoho subjektu druhému bez nutnosti zásahu třetí strany. Článek popsal elektronický platební systém založený na důkazu správnosti založeném na kryptografii místo na víře. [23]

Blockchain technologie, na které byl bitcoin postaven, jako mnoho vynálezů však nevznikla ve vakuu. Již dříve vznikaly pokusy o vytvoření decentralizovaného platebního systému, jejichž postupným zdokonalování vznikl dnešní Blockchain. Níže jsou stručně

popsány technologie, které byly přímou, či nepřímou inspirací, z nichž nejvýznamnější jsou rozepsány dále. [19]

Digicash

Digicash byla nizozemská firma Davida Chauma, která v roce 1983 popsala koncept anonymních virtuálních peněz. Dle tohoto konceptu by banky vytvářely digitální hotovost pro své zákazníky, kteří by s ní mohli platit v obchodech, jež by pak tuto digitální hotovost vyměnily v bance zpětně na peníze. Banka by byla schopná ověřit, že tato digitální hotovost je pravá a obchodníkovi vydat reálné peníze, nicméně by již nevěděla, kdo těmito penězi platil. Transakce by tak byly anonymní. Některé banky s tímto konceptem údajně experimentovaly, avšak firma roku 1998 oznámila krach. [19]

B-money

Listopadu 1998 kryptografik Wei Dai publikoval krátký článek ohledně digitálních peněz, které budou fungovat na netrasovatelné síti, kde odesílatel i příjemce budou indentifikovatelní pouze na základě digitálních pseudonymů (dnešních veřejných klíčů). Každá transakce bude podepsána odesílatelem a zašifrována pro příjemce. Transakce by byly rozposílány na síť serverů, kde by se vedly záznamy o zůstatcích na účtech. Tvorba peněz by byla schvalována uživateli v pravidelných aukcích. [19]

Hashcash

Roku 1992 Cynthia Dwork a Moni Naor popsali techniku boje s emailovým spamem. Odesílatel emailu by musel připojit nějaký důkaz, potvrzenku k odesílané zprávě říkající, že za odeslání zaplatil nějakou velmi malou cenu. Emaily bez takového důkazu by byly odmítnuty. Cena pro odesílatele by byla velmi malá při normálním objemu posílaných zpráv, ale zvedala by se s přibývajícím objemem tak, aby spammery odradila. Cena však neměla být platba nějaké třetí straně, ale byla popsána jako práce ve formě

opakujících se kalkulací, které byly nezbytné pro přijetí zprávy. Takže potvrzenka přiložená k emailu by byla důkazem o provedení těchto kalkulací (práce). Vzniklo spojení *proof-of-work*. Adam Back představil podobnou myšlenku s pomocí hashovacích funkcí a popsal Hashcash v roce 1997. Bitcoin tento koncept převzal. [19]

BitTorrent

BitTorrent je úspěšný peer-to-peer protokol ke sdílení souborů, který je dodnes velmi používaný. Spoluzakladatelem firmy, která za tímto protokolem stojí, je Bram Cohen. Jedná se o decentralizovaný systém, kdy je každý požadavek prováděn ve smyslu uživatel-uživatel místo využití nějakého centrálního serveru. Není zde také žádné centrální místo, které by protokol řídilo, je tak těžké jej cenzurovat či vypnout. [19]

2.2.1 Důležité milníky vývoje Blockchainu

Roku 2008 vznikl článek popisující bitcoin. Reálně však tento blockchain začal operovat až na začátku roku 2009, kdy došlo k potvrzení prvního bloku transakcí a vytvořilo se prvních 50 bitcoinů [3]. Pár dní na to byl zveřejněn také zdrojový kód. Roku 2010, konkrétně pak 15. srpna, byla nalezena chyba v kódu blockchainu, která zapříčinila, že bylo neoprávněně vytvořeno 184 milionů bitcoinů. Díky principům fungování distribuované účetní knihy byla tato chyba uživateli velmi rychle odhalena, opravena a síť prošla tzv. forkem [4]. V roce 2013 pak přišla zatím největší změna v podobě kryptoměny Ethereum, která předvedla blockchain jako decentralizovanou platformu pro chytré kontrakty 2.1. Na této síti můžou vývojáři vytvářet tržiště s půjčkami, spravovat registry dlužníků, obchodovat zdroje formou totožnou s opcemi a mnoho dalších věcí. Zatímco bitcoin je jednoduše platidlem, Ethereum je blockchain, na kterém běží nejrůznější aplikace. Dnes hojně využíván pro tzv. DeFi [5].

[3] Transakce, mimo oněch 50 bitcoinů, obsahovala text *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks* [30]

[4] Jedná se o radikální změnu sítě, která prakticky vytvoří novou verzi blockchainu [8]

[5] Pojem označující decentralizované finance. Tedy burzy, směnárny, atd...

Dnes existují již desítky různých blockchain sítí, které začaly vznikat po roce 2017 a z nichž každá se snaží překonat ty předchozí [6]. Většinou se však jedná o změny, které s sebou nesou negativa zpravidla ve formě nižší bezpečnosti. V popředí tedy stále stojí sítě Bitcoin a Ethereum. [13]

2.3 Kryptografie

K jasnému pochopení konceptu blockchain, zejména pak toho, proč je tato technologie bezpečná, je třeba znát pár základních konceptů z kryptografie. Kryptografie se mimo jiné vyznačuje především posíláním zabezpečených zpráv, které mohou přečíst pouze ti, jimž náleží. Díky kryptografii mohou data bezpečně kolovat po internetu. Například dnes hojně používané zabezpečení webových stránek (např. internetového bankovnictví) pomocí https [7]. Díky tomu má uživatel jistotu, že se nejedná o podvrženou stránku. Zároveň data, která jsou mezi uživatelem a stránkou přenášena, jsou šifrována a nelze je snadno odposlouchávat. V této kapitole jsou rozebrány základy šifrování a dešifrování zpráv v druhé řadě pak hashing či digitální podpis. Porozumění těchto konceptů je nutné pro porozumění toho, jak bezpečný je blockchain. [19]

Šifrování a dešifrování

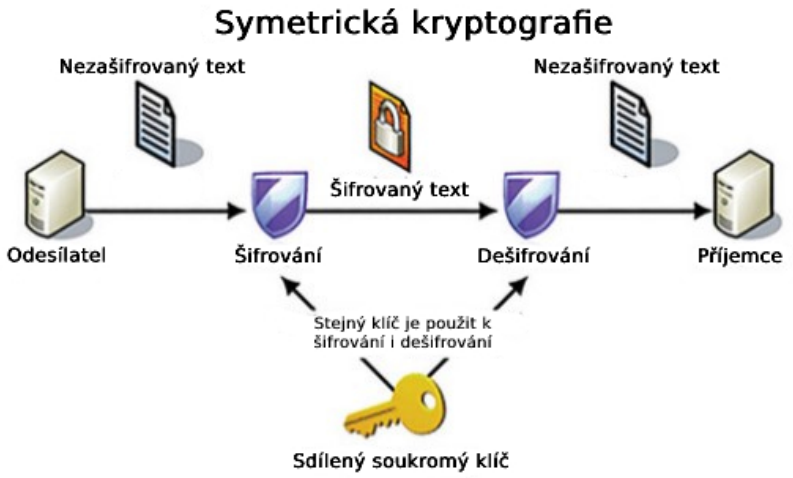
Šifrování a dešifrování jsou jedny z nejpoužívanějších a zároveň nejzákladnějších pojmů v kryptografii. Blockchainy zpravidla šifrované nebývají, avšak k pochopení kryptografických pojmů, které již tyto sítě využívají, je nezbytné vysvětlit, jak šifrování a dešifrování funguje. [19] [24]

Šifrování je v jednoduchosti proces, kdy je třeba převést klasický text, který může kdokoliv přečíst (tzv. plaintext) na šifrovaný text (tzv. cyphertext), jenž již sám o sobě

[6] Za zmínku stojí například síť PolkaDot, která se snaží být vylepšenou verzí sítě Etherea. https://polkadot.network

[7] Zkratka pro *hypertext transfer protocol secure*. Jedná se o protokol pro bezpečné prohlížení webových stránek.

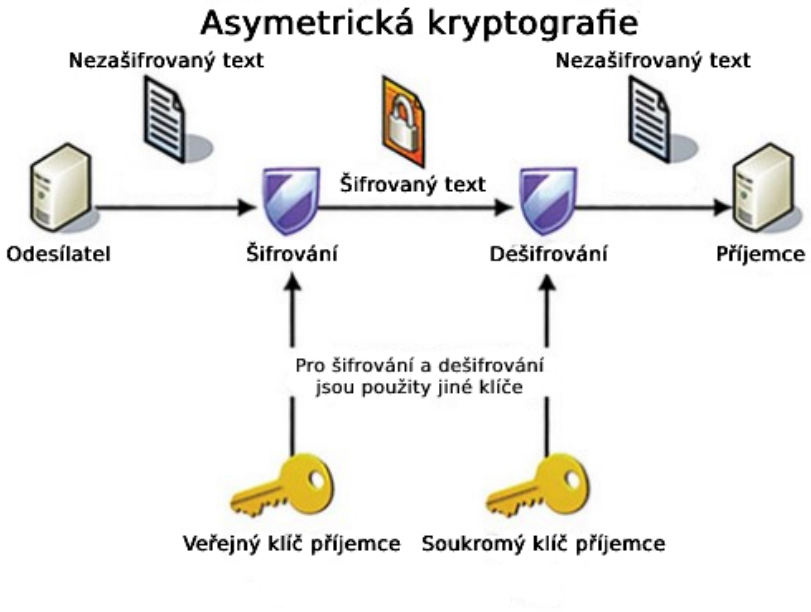
přečíst nejde, neboť nedává smysl. Dešifrování je pak na druhou stranu proces, který převádí šifrovaný text zpátky na klasický text. K tomuto procesu je třeba znát šifrovací klíč. Takovým klíčem může být například to, že každé písmeno ve zprávě je nahrazeno písmenem o jedno místo za ním v abecedě. Slovo *ahoj* by pak bylo *bipk*. Pokud se na takovém klíči domluví obě strany, tedy jak strana odesílající zprávu, tak příjemce, jedná se o symetrické šifrování. Tedy varianta, kde se používá stejný klíč k šifrování i dešifrování. Tento způsob se dnes však nevyužívá, neboť je jednoduše napadnutelný kvůli faktu, že existuje pouze jeden klíč, na kterém se účastníci musí domluvit a při tomto domlouvání může někdo jiný klíč zachytit. Schéma symetrického šifrování je zobrazeno na obrázku 2.4.



Obrázek 2.4: Schéma symetrického šifrování [19]

Protože tento způsob není příliš bezpečný, používá se v dnešním světě asymetrického šifrování. Princip spočívá ve vygenerování dvou matematicky propojených klíčů. Tzv. *veřejný klíč* a *soukromý klíč*. Veřejný klíč je možné sdílet a kdokoliv jej může použít k zašifrování zprávy. Avšak pouze vlastník soukromého klíče může takto zašifrovanou zprávu pomocí něj přečíst. Tímto odpadá bezpečnostní problém se sdíleným klíčem, neboť klíč pro šifrování a klíč pro dešifrování je jiný. Schéma asymetrického šifrování je zobrazeno na obrázku 2.5. [19] [24]

Na tomto principu je pak postaveno právě fungování blockchainu. Adresy, resp. účty účastníků jsou vytvořeny z veřejných klíčů, a tudíž všem veřejně viditelné. K provedení transakce je však zapotřebí potvrzení soukromým klíčem, tedy prokázání, že jsem vlastníkem dané adresy. [19] [24]



Obrázek 2.5: Schéma asymetrického šifrování [19]

Hashovací funkce

Hashovací funkce je sérií matematických operací, které jsou provedeny nad vstupními daty a jejichž výsledkem je digitální otisk prstu, nezpochybnitelný podpis, jednoduše hash. Existují základní hashovací funkce (nepoužívají se v blockchainu) a kryptografické hashovací funkce (používají se v blockchainu). [19] [24]

Základní hashovací funkce může například fungovat tak, že vezme první písmeno vstupu. Tedy *Hash(Kolik je hodin?)* dá výsledek *K*. Vstupem je zpráva *Kolik je hodin?* a výstupem, tedy hashem, je písmeno *K*. Hashovací funkce, jakožto všechny matematické funkce, je deterministická. Výsledek takové funkce je pak vždy stejný, tedy první písmeno vstupní zprávy.[19] [24]

Kryptografická hashovací funkce je pak speciální základní hashovací funkcí, která musí splňovat několik znaků, díky nimž je ideální pro použití v blockchainu:

- Je deterministická
- Pro jakoukoliv zprávu vytvoří příslušný hash rychle
- Není možné vygenerovat původní zprávu z příslušného hashe. Tedy nejde jít obráceně a z K vytvořit zprávu *Kolik je hodin?* jinak než pouhým hádáním.
- Malá změna ve vstupní zprávě způsobí velké změny ve výsledném hashi. Tedy není možné najít podobnosti mezi jednotlivými výsledky.
- Je téměř nemožné najít dvě zprávy se stejným hashem.

Kombinace těchto vlastností znamená, že je lehké vytvořit hash ze vstupní zprávy, avšak není možné vytvořit původní zprávu z vytvořeného hashe. Zároveň není možné uhádnout danou zprávu z toho, jak hash vypadá. Jedinou možností, jak zjistit původní zprávu, je hádáním a porovnáváním hashů vytvořených vkládáním hádaných zpráv s hashem, jenž byl vytvořený originální zprávou. Hashovací funkce může být prakticky použita v případech, kdy je třeba prokázat, že dvě věci jsou to samé, aniž bychom je museli odhalit. Pro příklad je možné vzít vytvoření předpovědi počasí na následující den, která však nemá být zveřejněna dříve než následující den. Taková predikce je zahashována a daný hash pak zveřejněný. Všichni vidí hash, avšak neznají onu predikci. Jakmile přijde druhý den a již víme, jaké bylo počasí, může být predikce zveřejněna a lidé si mohou ověřit (po vložení zprávy do hashovací funkce), jestli hash souhlasí s tím, který byl zveřejněn. [19] [24]

Kryptografické hashe, tedy výstup z kryptografických hashovacích funkcí, se v blockchainu používá hned k několika účelům:

- V procesu těžení [8].

[8] Proces potvrzování transakcí v síti

- Jako identifikátor transakcí.
- Jako identifikátor bloků pro účely propojení v řetezci bloků [9].
- Zajišťující, že jakákoliv neoprávněná manipulace s daty je hned evidentní.

Nejznámější hashovací funkcí z prostředí blockchainu je pak SHA-256, která se používá u Bitcoinu. Příklad je pak zobrazen na obrázku 2.6.

SHA256(`**Kolik je hodin?**`) ->
9FC97FC63D43AF0A7361F2A882C886B25E2E368766CF56FA5A6FCD537C39C2CB

Obrázek 2.6: Příklad vygenerovaného hashe pomocí hashovací funkce SHA-256 používané u Bitcoinu

Digitální podpis

Digitální podpisy jsou hojně používány v blockchainových sítích pro určování validních transakcí. Jsou podtřídou elektronických podpisů a mají formu hashe, viz obrázek 2.7. Vytváří se ze *soukromého klíče*. Každý, kdo zná příslušný *veřejný klíč* k tomuto primárnímu, může jednoduše ověřit, že transakci doopravdy podepsal držitel onoho soukromého klíče (avšak bez odhalení tohoto klíče). Proces je možné popsat jednoduchým schématem: [19] [24]

- zpráva + soukromý klíč -> digitální podpis
- zpráva + digitální podpis + veřejný klíč -> validní/nevalidní

Dititální podpisy mají oproti standardním podpisům (tužka a papír) dvě zásadní výhody, a proto má jejich využití smysl. Těmito výhodami jsou:

[9] Viz 2.2

Obrázek 2.7: Příklad digitálního podpisu navázaného na soukromý klíč [19]

- V případě klasického podpisu, který je na konci dokumentu, nemá nikdo jistotu, že dokument nebyl po podpisu upraven. V případě digitálního podpisu toto není možné, neboť zpráva jde upravit pouze při vlastnictví soukromého klíče.
- Klasický podpis lze lehce falšovat, či znovu použít pro podpis jiného dokumentu. V případě digitálního podpisu toto možné není, protože k vytvoření podpisu je třeba soukromý klíč.

Digitální podpis, narozdíl od klasického, zkrátka vždy patří k danému kusu dat a je vytvořen soukromým klíčem. Není tak možné jej znovupoužít pro jiný dokument. Jakákoliv změna dat by pak vedla k zneplatnění podpisu. Digitální podpis je unikátním důkazem, že daná osoba se soukromým klíčem opravdu data (dokument, transakci, atd...) podepsala. Nikdo jiný takový podpis nedokáže vytvořit, aniž by onen soukromý klíč vlastnil. [19] [24]

Digitální podpisy se používají v blockchainových transakcích, protože prokazují vlastnictví daného účtu, daných prostředků, Tento důkaz je proveden matematicky bez nutnosti zásahu nějaké třetí strany. V případě transakce v běžném bankovním systému je nejprve nutné se ověřit přihlášením do internetového bankovnictví, či prokázáním se občanským průkazem na pobočce banky. Pokud banka ověří, že jste vlastníkem daného účtu, transakci provede. V síti blockchain, kde neexistuje žádná autorita, která by účty spravovala, je digitální podpis kritický důkaz o tom, že prováděnou transakci dělá oprávněný majitel účtu. [19] [24]

2.4 Kryptoměny

Dnes existuje spousta kryptoměn fungujících na velké množství blockchainů. Není tak úplně snadné shrnout všechny jako jeden ekosystém. Není cílem zde popisovat všechny kryptoměny a blockchainy, existují však zástupci, kteří stojí za zmínku, ať už z technologického nebo finančního hlediska. Co se technologického hlediska týče, lze uvést například již zmiňovaný Bitcoin fungující na mechanismu zvaném *proof-of-work* či Ethereum používající *chytré kontrakty*. [19]

Bitcoin

Bitcoiny jsou digitální aktiva, jejichž vlastnictví je zapsáno v distrubuované účetní knize (Bitcoinovém blockchainu), která je řízena více než 14 000 nezávislými počítači, jež spolu navzájem komunikují [10]. Transakce Bitcoinů se řídí protokolem, kde jsou definována pravidla pro řízení sítě. Tento protokol je implementován v aplikaci, která na těchto počítačích běží. Počítače jsou zvány *nodes*. Každý tento node nezávisle potvrzuje transakce v celé síti a aktualizuje si svou účetní knihu transakcí. Specializované počítače (nodes), zvaní těžaři, pak sbírají validní transakce z těchto účetních knih do bloků a distribuují je dalším počítačům v síti. [19]

Každý může Bitcoin nakoupit, vlastnit jej, poslat jinému člověku. Každá transakce je zapsána v blockchainu ve formě *plaintext*. Blockchain Bitcoinu není zašifrován, resp. každý může vidět kolik a kam se mince poslaly. Každý se může podílet na procesu *těžení*, hlídat správnost transakcí a vytvářet tím nové Bitcoiny. [19]

Bitcoin byl první kryptoměnou, která dala světu technologii blockchain. Od ostatních kryptoměn se liší kromě svého prvenství i v dalších věcech:

- Existuje omezené množství mincí (konkrétně 21 milionů). Mince se získávají jako odměna za potvrzování správnosti transakcí v síti každých cca 10 minut a tato odměna stále klesá [11].

[10] Dle stránky https://bitnodes.io k 25.12.2021

[11] Aktuálně je tato odměna 6,25BTC a k vytěžení všech mincí dojde někdy v roce 2140

- Chod sítě je zajistěn systémem *proof-of-work* [12]
- Díky svým vlastnostem je Bitcoin svými příznivci označován jako digitální zlato (uchovatel hodnoty) či ochrana proti inflaci. Vznikl jako alternativa k dnešním penězům.

Ethereum

Vizí Etherea je vytvoření necenzurovatelného, soběstačného, decentralizovaného světového počítače. To se liší od vize Bitcoinu, jež je alternativou k dnešním tradičním měnám. K dosažení těchto cílů staví tato kryptoměna na konceptu Bitcoinu a rozšiřuje jej. Pokud se o Bitcoinu mluví jako o nezávislém distribuovaném úložišti dat, pak Ethereum je nezávislým distribuovaným úložištěm a zpracováním dat a operací nad nimi. Blockchain Etherea je řízen více než 5 000 počítači [13]. Stejně jako Bitcoin se transakce na Ethereu řídí protokolem, který je implementován v aplikaci bežící na daných počítačích. Avšak na rozdíl od nejznámějsí kryptoměny mohou transakce obsahovat nejen data o platbách, ale i celé kusy kódu. Tomu se říká chytrý kontrakt. [19]

Tento chytrý kontrakt obsahuje kód k provedení nějakého úkonu a může být spuštěn tím, že do něho jsou vloženy mince Etherea (v podstatě jako jukebox, do kterého je třeba vhodit minci, aby přehrál vybranou skladbu). Když je tento chytrý kontrakt takto zaplacen, všechny počítače v síti (nodes) spustí příslušný kód a výsledek zapíší do účetní knihy (blockchainu). Tomuto systému se někdy přezdívá *Ethereum Virtual Machine*. [19]

[12] Systém, který vyžaduje provedení nějaké práce jako prokázání pravosti. Více popsáno v kapitole 2.2 (Hashcash) v této práci.

[13] Dle stránky https://www.ethernodes.org k 25.12.2021

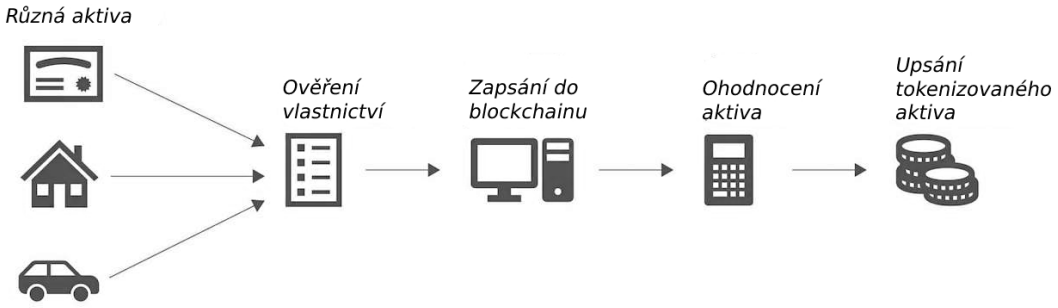
Další kryptoměny

Jak již bylo zmíněno, kryptoměn a blockchainů, které jsou jimi využívány, dnes existuje celá řada[14] a každou chvíli vznikají nové. Těmto kryptoměnám se souhrnně říká altcoiny (zkratka pro alternativní kryptomince) a většina z nich se snaží o totéž, být rychlejší, levnější, flexibilnější blockchain technologií, která umožní lidem fungovat bez nutnosti intervence banky či jiné třetí strany, a bude tak levnější a bezpečnější. [21] [19]

[14] Dle serveru https://www.coingecko.com/en skoro 12 000 k 16.12.2021

3 Tokenizace

Jádrem tokenizace, jak již samotný název tohoto procesu napovídá, je token. Token je v podstatě jakákoliv jednotka zapsaná v blockchainu. Může sloužit jako reprezentant měny, pak lze hovořit o kryptoměně, tedy například bitcoinu. Může však reprezentovat i jakýkoliv jiný objekt, v tomto případě podíl na firmě (akcii) nebo podíl na dluhu firmy (dluhopis). Termín tokenizace je pak proces, kdy jsou vytvářeny takovéto tokeny na blockchainu, které reprezentují již existující objekty (cenný papír, nemovitosti, atd...). Jinými slovy jsou transformována aktiva ze standardní podoby do podoby tokenu zapsaného na blockchainu. Token pak slouží pouze jako reference originálního podkladového objektu a implicitně v sobě nenese žádnou "cenovku". Ta je přiřazena až trhem. [15] [33]



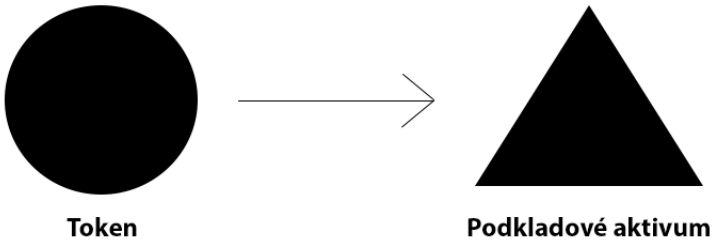
Obrázek 3.1: Grafické znázornění procesu tokenizace aktiva [9]

Tokenizace přináší oproti standardním metodám emise mnohé výhody. Kupříkladu odstraňuje většinu finančních a regulatorních požadavků, a tudíž razantně snižuje cenu i časovou náročnost například emise cenného papíru. Tokenizace je tak díky těmto vý-

hodám v poslední době velmi skloňovaný pojem[1], avšak díky své mladosti čelí velkým překážkám. Mezi největší patří praktická absence regulatorního rámce, která fakticky brání její širší implementaci, například z důvodu s tím související nejistoty a technický rámec, kdy je aktuálně nemožné důvěryhodně zajistit konzistenci mezi tokenem a aktivem, které reprezentuje. [15] [33]

3.1 Token

Jak již bylo řečeno v předchozí kapitole, základním prvkem tokenizace je token, tedy jednotka zapsaná v síti blockchain nesoucí určitou informaci například o vlastnictví něčeho (nemovitosti, atd...), či práva na něco (vyplácení dividend, atd...). Ať již však nese jakoukoliv informaci, je striktně navázán na podkladové aktivum, a měl by tak reprezentovat jeho hodnotu.



Obrázek 3.2: Obrázek ilustruje fakt, že token vždy reprezentuje podkladové aktivum[2].

To znamená, že pokud dojde k přesunu tokenu k jinému vlastníkovi, vlastník podkladového aktiva se změní taktéž. Jinými slovy, kdokoliv je držitelem tokenů, je i držitelem podkladového aktiva, které reprezentuje. Tento krok je celkem obtížné právně zabezpečit. Pokud se totiž stane, že dojde k přesunu tokenů k jinému majiteli, avšak legálně se nezmění vlastnictví podkladového aktiva, token je fakticky k ničemu. Je tedy nutné,

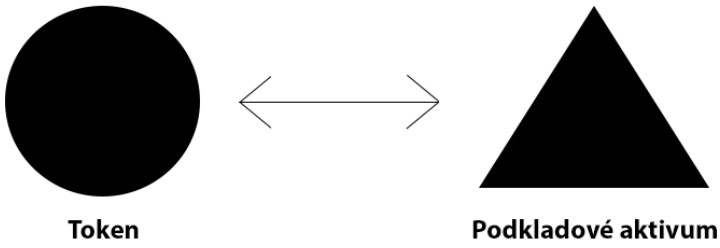
[1] V Čechách poslední dobou vzbuzuje velké kontroverze firma XIXOIO, která nabízí zprostředkování tokenizace komerčním subjektům.[34]

[2] Šipka pak naznačuje, že daný token vždy reprezentuje stejné podkladové aktivum, nebo jeho část.

aby každá akce, která se stane na blockchainu s tokeny, byla i dle práva vynutitelná v reálném světě. [15]

Ve skutečnosti je však třeba zabezpečit oboustrannou závislost mezi tokenem a podkladovým aktivem. Platí tedy, že pokud token změní vlastníka, změní se vlastník podkladového aktiva a naopak. [15] Ke správnému znázornění je tedy třeba upravit šipku na obrázku 3.2. Musí tedy být zajištěno:

- Když se změní vlastník tokenů, legální vlastnictví podkladového aktiva je také změněno.
- Když se změní vlastnictví podkladového aktiva, změní se i vlastník tokenů.



Obrázek 3.3: Obrázek ilustruje oboustrannou provázanost tokenu a podkladového aktiva, které reprezentuje.

V podstatě se tak token stává podkladovým aktivem, ať již jde o akcii, dluhopis či jiné tradiční aktivum. [15]

Jakékoliv finanční aktivum může být tokenizováno, resp. může být reprezentováno formou tokenu, ať již přímo, tedy token je finančním aktivem, nebo formou dokladu, kdy token reprezentuje některé právo vyplývající z držby finančního aktiva. Akcie či dluhopis se může jevit jako fyzický objekt, avšak finanční aktiva nejsou nic jiného, než dohody mezi jednotlivými stranami, zpravidla upisovatele a vlastníka. Akcie představuje například dohodu, či smlouvu nebo kontrakt mezi emitentem, tedy firmou, a vlastníkem akcie. Všechny tyto dohody mohou být reprezentovány ve formě tokenu (díky

chytrým kontraktům[3] zapsaným v blockchainu.)[19] [15]

3.1.1 Výhody tokenů

Některé výhody a překážky, kterými tokeny, a tím i proces tokenizace jako takové čelí, již byly zmíněny výše. Ve zbytku kapitoly jsou jak pozitivní, tak negativní aspekty probrány více do detailu.

Důvěra

To, že byl token vydán a je stále aktivní i další den, je zajištěno využitím distribuované účetní knihy, tedy blockchainu. Jakmile je na něm informace zapsána, nejde ji odstranit ani změnit. [15] [19]

Verifikace

Díky použití technologie blockchain je věškeré zacházení s tokeny transparentní. Vlastník podkladového aktiva tak může jednoduše prokázat, že aktivum opravdu vlastní, či drží určitá práva k němu tím, že jednoduše ukáže aktiva na svém "účtu"[4]. [15] [19]

Vlastnictví podílů podkladového aktiva

U mnohých typů aktiv je vlastnictví podílu do této šíře umožněno poprvé v historii právě díky tokenizaci. Například vlastnictví jedné nemovitosti 50 osobami je v dnešní době velmi obtížné právně zpracovat. Dalším příkladem pak může být vlastnictví firmy desítkami tisíc akcionářů, nebo vlastnictví jednoho dluhopisu s velkou nominální hodnotou více investory. Token je možné teoreticky rozdělit na neomezený počet dílků, a tím výše zmíněné velmi snadno umožnit. [15] [31]

[3] Více o chytrých kontraktech v kapitole 2

[4] Jak je možné tento proces provést bezpečně je vysvětleno v kapitole 2.3

Přístup ke globálnímu trhu

Na rozdíl od tradičních aktiv nejsou tokeny implementovány rozdílně pro rozdílné státní jurisdikce. Jakmile je token vydán, může být lehce adopdován po celém světě a integrován do různých distribučních platforem. Je však třeba v daném státě zajistit potřebné právní compliance. [15] [19]

Snadné, rychlé a levné vypořádání transakcí

Vypořádání obchodu, tedy převodu aktiva (nakoupení, prodej, a další...), je zajištěno blockchainem. Není zde žádné konsorcium bank či burz pro zajištění chodu celé infrastruktury, která by vypořádání měla na starosti. [15] [19]

Globální škálovatelnost

Díky snadné škálovatelnosti primárního a sekundárního trhu je možné s tokeny obchodovat globálně napříč časovými pásmy a na různých místech světa. [15] [19]

Nižší nároky na investice

Díky větší efektivitě vypořádání obchodu je možné přijmout a zprocesovat daleko menší transakce od retailových investorů. V dnešní době se ke sběru malých objemů peněz od investorů využívá crowdfundingových platforem, avšak ty si zpravidla berou velké poplatky [5] v porovnání s úpisem na burze. [15] [31]

Nižší nároky pro samotnou tokenizaci (emisi) aktiv z pohledu firmy

Díky faktu, že vydání tokenizovaných aktiv vyžaduje méně stakeholderů, je technicky zprocesovatelné rychleji a díky tomu levněji, výrazně tak snižuje zejména tyto bariéry, se kterými se emitenti potýkají:

[5] https://maxkops.de/comparing-crowdfunding-and-ico-fees-commissions

- **Standardní emise je příliš náročná**. Díky tomu, že jsou peněžní i časové náklady na vydání například tokenizovaného cenného papíru daleko nižší než standardní úpis akcií, stává se z tokenizace cesta, jakou můžou firmy, které by jinak cestou využití standardního finanční systému nešly, získat kapitál. IPO je pro ně buď příliž drahé, nebo procesně příliš náročné.[15] [31]

- **Cena**, díky které si standardní úpis mohou často dovolit pouze velké firmy, je další bariérou pro spoustu firem. Efektivita tokenizace dělá prostředí díky zapojení menších podniků do procesu více konkurenčním, jelikož snižuje cenu úpisu díky odstranění prostředníků, tedy banek či burz. [15] [31]

- **Časová náročnost** je při procesu tokenizace nižší kvůli tomu, že je třeba menší množství stakeholderů, kteří se musí domluvit. Dále pak technické zpracování celého procesu umožňuje velké množství automatizací, což snižuje časové zatížení celé operace. [15] [31]

Svoboda trhu

Banky a finanční instituce, které existují po staletí, mají oligopol na poli zprostředkování finančních služeb a produktů. V případě tokenů je proces technicky řízen blockchainem a může být uskutečněn různými firmami. Noví účastníci na trhu, kteří nabízejí tokenizaci, tak mohou značně otřást oligopolem bank a finančních institucí. [15] [31]

Lehčí správa po úpisu

Tokeny mohou být po tokenizaci daleko snadněji administrovány než standardní aktiva. Chytré kontrakty mohou zautomatizovat věci, které dříve vyžadovaly opakovaný administrativní zásah, či notářské potvrzení jako například výplata dividend. [15] [31]

3.1.2 Nevýhody tokenů

I přesto že tokenizace má mnohé výhody, čelí také velkým překážkám. Některé z nich jsou dány aktuálním stavem vývoje technologie blockchain, a tudíž jsou řešitelná v čase a některé jsou koncepčního rázu.

Praktická absence právního rámce

Upsáním tokenu, který pouze reprezentuje určité aktivum, není možné se nezodpovídat regulacím příslušné země. Z logiky věci by tokenizované firmy měly podléhat stejným podmínkám jako firmy netokenizované. Z dnešního pohledu je v mnohých zemích obtížné tokenizovaná aktiva vůbec vydat z toho důvodu, že jurisdikce v těchto zemích nepočítají s tokeny jako s validním nástrojem pro určování vlastnictví daného aktiva. Právním pohledem na tokenizaci v České republice se práce v základních parametrech podrobněji zabývá v kapitole 3.3.1. [15] [3]

Specifické použití

I přestože tokenizace může znít velmi moderně, mnoho investorů není dostatečně obeznámeno s technologií blockchain, na které celý proces běží. Kvůli tomu se mnozí neumí v tomto prostředí pohybovat a s tokeny správně a bezpečně zacházet. [15] [14]

Absence promyšlené infrastruktury

Infrastruktura pro možnosti obchodu s tokeny tokenizovaných firem je v současné době stále budována. Mnohé deentralizované burzy se potýkají s nízkou likviditou [6] a centralizované burzy pak s nedostatečně jasným právním rámcem čekají na schválení možnosti takové tokeny upisovat. [15] [31]

[6] https://maxkops.de/comparing-crowdfunding-and-ico-fees-commissions

Špatné aspekty odstranění prostředníka

Odstraněním prostředníků, kterými jsou banky a finanční instituce, se sice ušetří nemalé náklady, avšak zmizí dohled expertů nad prováděnými úpisy a firmami, jež se tokeny snaží upsat. [15]

Pověst kryptoměn

I přestože tokeny reprezentující aktiva nelze příliš porovnávat s kryptoměnami, o kterých dnes ví celý svět, mnoho lidí vnímá oba zástupce ze světa blockchainu totožně. Tokenizace se tak musí potýkat se špatnou reputací některých kryptoměn či faktem, že některé státy kryptoměny dokonce zakazují používat. [15] [19]

Utility token

Pojem utility token označuje tokeny, které se využívají k určitým službám. Objevují se v sítích, které jsou vytvořeny pro specifické použití. Jedná se například o decentralizovaná úložiště, decentralizované burzy. Utility tokeny pak v takové síti reprezentují právo či jakousi vstupenku pro použití dané sítě. Tedy v případě decentralizovaného úložiště by se mohlo jednat o právo využívat dané úložiště. V případě decentralizované burzy by pak mohlo jít o snížení transakčních poplatků v případě vlastnictví tokenů. [15] [19] [14]

Dalším specifikem utility tokenů je jejich investiční status. Na rozdíl od security tokenů, viz níže, je mnozí nepovažují za investiční nástroj a to právě proto, že jsou určeny pro využití v určité službě a pokud jsou správně nastaveny, nevztahují se na ně zákony o cenných papírech dané země. Firmy, které tokeny vydávají, je nevytváří pro investiční účely. Jejich smyslem je použití pro specifický účel v dané síti. [14]

Utility tokeny jsou upisovány formou ICO (Initial coin offering). Původní ICOs byly vytvářeny z důvodu výběru kapitálu do nových blockchainových stratupů s revolučními myšlenkami bez nutnosti spoléhat na tradiční stakeholdery zapojené do fundraisingového procesu. Důvodem, proč se ICO nedostaly do křížku s regulátory, byl fakt, že uti-

lity token nepředstavuje investiční instrument, nýbrž klíč k určitému produktu či službě. Sběr peněz od investorů byl v případě ICO založen na jednoduché myšlence, a sice nabídnout tokeny za relativně nízkou cenu a za vybrané peníze dotvořit daný produkt či službu, kterou budou moci držitelé tokenů díky jejich vlastnictví využívat. Za první ICO je pak považován úpis tokenů Etherea, které jsou používány jako palivo pro chytré kontrakty. Reálně první ICO se však uskutečnilo již v roce 2013 pod taktovkou projektu Mastercoin. [14]

Security token

Na rozdíl od utility tokenů security tokeny reprezentují určitá práva jejich držitele podobně jako například akcie či dluhopisy emitované firmou. Vlastnictví tokenů pak jejich držitelům přináší hlasovací práva v síti, nebo mohou být kryty nějakým podkladovým aktivem, například komoditou či právě akcií nebo dluhopisem. [19]

Security tokeny jsou konstruovány pro investiční účely, jejich smyslem je tedy být koupen investorem, kterému mají v budoucnu přínést výnos, ať se již jedná o výnos kapitálový, kupónový či dividendový. Cílem security tokenů je nahradit klasické investiční aktivum, jakým může být akcie, dluhopis a jiné. Úpis security tokenů pak probíhá formou tzv. STO (security token offering). Tento proces bude popsán podrobněji v následujících kapitolách. [14]

3.2 Příklady tokenizace

Proces tokenizace je již několik let na světě, a tudíž existuje pár příkladů jeho úspěšného provedení (zejména ze zahraničí). Jsou k vidění příklady tokenizace akcií firmy, dluhopisů i nemovitostí. Základní překážkou tokenizace zůstává právní rámec, resp. jeho praktická absence. Celý proces se tak velmi protahuje a činí složitějším. Výhodou je, že je možné se rozhodnout, pod jakou jurisdikcí bude tokenizace, resp. úpis security tokeny (STO) proveden. Pomalu začínají existovat i firmy zabývající se přímo procesem

tokenizace, v Česku se pak jedná o již zmíněnou firmu XIXOIO. [15]

V této kapitole je uvedeno několik příkladů úspěšných tokenizací dluhopisů a akcií větších firem.

World bank dluhopisy

World bank je jednou z největší fundraisingových institucí světa se zaměřením na rozvojové země. Jako první tokenizovala dluhopis nesoucí název bond-i. Dluhopis byl vytvořen, upsán a řízen do doby splatnosti za použití technologie blockchain. Tento dvouletý dluhopis byl upsán celkem za 110 milionů australských dolarů. Aranžérem úpisu byla Bank of Australia (CBA) a celý proces trval dva týdny, kdy probíhaly konzultace na trhu s investory. Samotná CBA pak byla jedním z investorů, kteří si dluhopis pořídili. [11]

bond-i shrnutí úpisu	
Emitent	World Bank
Rating emitenta	Aaa/AAA
Výše úpisu	110 milionů AUD
Datum úpisu	28.08.2018
Splatnost dluhopisu	28.08.2020
Kupón	2.20% p.a. vyplácen pololetně
Splatnost kupónu	28.02 a 28.08.
Měna a minimální velikost investice	AUD. Minimální výše investice 500 000
ISIN	AU0000020612
Aranžér emise	Commonwealth Bank of Australia (CBA)

Tabulka 3.1: Tabulka ukazuje parametry tokenizovaného dluhopisu.[11]

Daimler AG a LBBW

Daimler AG a Landesbank Banden-Württemberg (LBBW) společnými silami využily technologii blockchain pro provedení finanční transakce. Vydaly dluhopisy v Německu nazývané Schuldschein se splatností jeden rok v celkové hodnotě 100 milionů eur. Investory byly banky Esslingen-Nürtingen, Ludwigsburg, Ostalb i samotná Landesbank Baden-Würtenberg (LBBW). Celá transakce od počátku přes distribuci, alokaci peněz a spuštění dluhopisového kontraktu až po vyplácení kupónu byla provedena přes blockchain v kooperaci s dceřinými společnostmi TSS (dceřiná společnost Daimler) a Targens (dceřiná společnost LBBW). [5]

Kurt Schäfer, viceprezident Daimler pokladny*(Daimler and LBBW successfully utilize blockchain technology for launch of corporate Schuldschein, strana 2, 2017)*, řekl: *„Blockchain může mít vliv na téměř celý hodnotový řetězec. Z tohoto důvodu, jakožto přední výrobce automobilů, chceme hrát aktivní roli v globální blockchainové komunitě a pomoci formovat mezisektorové blockchainové standardy. Toto chceme udělat ve všech oblastech, které jsou pro nás důležité (Vztahy se zákazníky, prodej a marketing, řízení zásob, elektronický a finanční servis.).“*

„Blockchain technologie změní roli bank jakožto prostředníků v ekonomických procesech. Nechceme pouze přihlížet tomuto vývoji, ale chceme proaktivně formovat toto odvětví. Schuldschein je ideálním projektem pro náš vstup do používání technologie blockchain. Zároveň v rámci tohoto odvětví jsme chopni generovat podstatnou přidanou hodnotu pro naše firemní zákazníky a pro investory, protože proces vydání dluhopisů je více efektivní a časová náročnost výrazně nižší,“ Joachim Erdle, Finanční řiditel LBBW *(Daimler and LBBW successfully utilize blockchain technology for launch of corporate Schuldschein, strana 2, 2017).*

Telegram

V roce 2018 vybrala populární platforma rekordní sumu 1,7 miliard amerických dolarů na posílání zpráv Telegram skrz prodej svého tokenu (tokenizované akcie) GRAM.

Tyto peníze byly vybrány pouze od soukromých investorů. Úpis byl celosvětový, tedy účastnili se jej investoři z celého světa. V roce 2019 šel pak token do veřejné nabídky. Parametr tokenu byly následující:

- **Označení tokenu**: GRAM
- **Cena tokenu**: 1 GRAM = 4 USDT [7]
- **Minimální možná investice:** 1 GRAM

Protože však nebyly splněny všechny státem nařízené regulace, byl úpis v roce 2019 pozastaven americkou kontrolní organizací SEC (The Securities and Exchange Commission), která vykonává dohled nad finančními trhy v Americe. Dle tohoto regulátora firma Telegram Group Inc. jí vlastněnou firmou TON Issuer Inc. začala sbírat kapitál v roce 2018 k financování podnikání firmy včetně vývoje vlastního blockchainu TON blockchain a vývoje mobilní aplikace Telegram Messenger. Celkem bylo prodáno přibližně 2,9 miliard digitálních tokenů 171 investorům a více než jedna miliarda z toho byla prodána investorům v USA. Telegram slíbil doručení tokenů GRAM těmto investorům při spuštění svého blockchainu TON. SEC obvinila Telegram z toho, že nezaregistroval svůj token GRAM jako cenný papír, a tím pádem porušil zákon o cenných papírech v Americe. [32] [27]

Erste Group

Erste Group a ASFINAG vydaly první tokenizovanou obligaci v Evropě skrze blockchain technologii. Celkový úpis této obligace byl ve výši 20 milionů EUR. Mezi prvními investory byly rakouské pojišťovací společnosti Wiene Städtische Versicherung a DONAU Versicherung a rakouská regionální banka Hypo Vorarlberg. Využitím technologie blockchain byl úpis efektivnější, více transparentní a zároveň bylo dosaženo menšího

[7] USDT je označení pro tzv. stable coin, tedy kryptoměnu, která nemění svoji hodnotu v čase a odpovídá hodnotě jednoho dolaru, tedy platí že 1 USDT = 1 USD.

provozního rizika. Úpis se odehrál prostřednictvím platformy, kterou vytvořila Erste Group použitím Hyperledger fabric [8]. Workflow celé emise dluhopisu proběhlo na této blockchainové platformě vyvinuté společností Erste Group bez nutnosti použití tradičních metod. [10]

Použitím technologie blockchain věci zahrnuté do procesu tvorby a spuštění takového projektu, kdy standardní papírový proces trvá několik dní, mohou být hotové v řádech sekund. Zároveň bylo umožněno masivně zredukovat administrativní náročnost spojenou s takovouto transakcí. Platforma byla vyvinuta tak, že je možné integrovat do procesu i další banky a platformy. [10]

3.3 Tokenizace cenného papíru v ČR

V této kapitole se práce zaměřuje již na tokenizaci cenného papíru v České republice. Detalněji je proces rozebrán u dvou cenných papírů, a tím je akcie a dluhopis. Ve zbytku práce je rozebrán celý proces a co mu předchází tak, aby čtenář dostal jasnou představu a návod, co musí pro tokenizaci udělat, aby byla úspěšná. V neposlední řadě by měla práce odpovědět na otázku, zda-li je tokenizace pro čtenáře správnou volbou a proč je výhodnější než standardní úpis. Práce se lehce dotýká i právního rámce celé operace. Zde je nutno podotknout, že z pohledu právních úprav v České republice není tokenizace nijak zaběhlým jevem (viz následující podkapitola 3.3.1). Spíše by se dalo říci, že jde o velmi novou metodu, jak získávat kapitál na českém trhu. Je tak velmi pravděpodobné, že bude v průběhu času docházet k úpravám právního rámce vzhledem k faktu, že tokenizované akcie a dluhopisy budou vznikat čím dál častěji a tyto okolnosti s sebou budou přinášet nové výzvy. Dále díky skutečnosti, že i aktuální technologická vyspělost blockchainu je na počátku, je taktéž možné, že se budou upravovat v průběhu času i procesní věci, a tedy i celý postup tokenizace jako takové. Čtenář by tak měl mít na paměti, že v práci uvedené informace je třeba konfrontovat s aktuálním stavem, neboť

[8] Jedná se o blockchain framework, který se používá jako základ pro blockchainové produkty, využívá plug-and-play komponenty a je určena pro firemní klientelu.

mohou být (v době čtení) již neaktuální.

3.3.1 Právní rámec v České republice

Jak již bylo v práci zmíněno, právní rámec zdaleka není dotažen do podoby, kdy by bylo jasně dáno, jak má proces z regulatorního pohledu vypadat tak, aby u regulátora finančního trhu, tedy ČNB, prošel. V případě konzultování procesu s právní kanceláří se tak mohou názory jednotlivých právníků na jednotlivé aspekty tokenizace lišit. Určitě je však třeba si uvědomit, že proces vydání security tokenů, které mají nahradit klasické akcie či dluhopisy, je proces, na nějž se vztahují regulace stejné jako v případě klasické emise cenných papírů. Je tak třeba tyto regulace vzít v potaz.

Vzhledem ke členství České republiky v EU se na celý proces vztahují mnohá regulatorní opatření společná pro všechny členské země. Tím se úpis tokenizovaných aktiv zjednodušuje, neboť lze v rámci tokenizace cílit na investory rovnou z několika států bez nutnosti procházet různými schvalovacími procesy napříč jurisdikcemi. Malé rozdíly však mezi státy jsou a některé tak mají proces snažší než jiné. V České republice pak právní rámec (jiný než ten evropský) prakticky neexistuje [3], nicméně podrobněji se této problematice věnuje následující podkapitola. V rámci EU tak existují tyto regulace, které je třeba brát v zřetel.

MiFID II

MiFID II je upravenou verzí zákona Evropské unie MiFID I neboli *Markets in Financial Instruments Directive (2004/39/EC)*. Tento zákon se dotýká všeho, co je spojeno s finančními trhy a finančními instrumenty a je aplikovatelný napříč státy Evropské unie již od roku 2007. MiFID upravuje především tyto věci: [15] [29]

- Podobu nutných požadavků, které musí splňovat investiční firmy.
- Požadavky pro povolení činnosti na regulovaných trzích.
- Požadavky na kontrolu trhů pro zabránění podvodnému jednání.

- Povinnost transparentnosti pro obchod s akciemi.
- Pravidla pro přijímání investičních pokynů.

MiFID II vešel v platnost roku 2018 a měl za cíl vytvořit na trzích férovější prostředí, větší bezpečí a efektivitu. Úpravy se dotkly zejména investičních firem a transparentnosti v případě dokumentací a reportingu. V jednoduchosti tak MiFID II měl vést k větší ochraně investorů. [29]

KYC a AML

KYC (know your customer) a AML (anti money laundering) jsou regulatorní opatření. KYC je zkratka anglického názvu, který by se dal do češtiny přeložit jako *poznej svého zákazníka*. Jedná se o opatření k ochraně proti praní špinavých peněz, financování terorismu či nelegálního chování. Aby mohl investor (ať se již jedná o fyzickou, či právnickou osobu) tokeny nakoupit, musí předložit data o své osobě. To se standardně naplňuje předložením identifikačního dokumentu, v České republice občanského průkazu, výpisu z účtu (pro ověření, že má subjekt účet na své jméno) a doklad prokazující adresu bydliště. [15] [4]

AML je zkratka anglického názvu, který by se dal přeložit jako *opatření proti praní špinavých peněz*. Narozdíl od KYC se zaměřuje více na získání informací o původu peněz investora, než o investorovi jako takovém. Standardně se získávají informace o zaměstnání, výše mzdy a dalších věcí. Investor zároveň prohlašuje, že se nepodílí na financování terorismu ani dalších nezákoných aktivitách, že jedná s vlastními penězi na vlastní účet. AML také rozlišuje, zdali je osoba politicky exponovaná [9], či nikoliv. [15] [4]

[9] Jedná se o osobu vykonávající vyšší veřejnou funkci, zjednodušeně by se dalo říci, že se jedná o politika, avšak politicky exponovanou osobou může být i důstojník v armádě či jeho nejbližší rodina. Tyto osoby pak podstupují speciální proces ověření https://www.mesec.cz/clanky/chodite-s-namestkem-ministra-mozna-budete-mit-problem-zalozit-si-ucet-nebo-dostat-hypoteku/

Prospekt

Otázka nutnosti tvorby proskeptu je jednou z klíčových při veřejné nabídce cenných papírů. Úkolem prospektu je informovat investory ohledně podmínek a pravidel emise. Za tímto účelem Evropská unie specifikuje, jaké přesně náležitosti musí takový dokument obsahovat, aby mohl být považován za prospekt.

[15] V rámci světa blockchain existuje termín tzv. *Whitepaper*, což je dokument, který popisuje token a jeho vlastnosti a je primárním dokumentem sloužícím pro potenciální kupce. Tento dokument však nenahrazuje prospekt z právního hlediska, neboť neobsahuje všechna regulátorem nařízená sdělení. Zároveň lze však říci, že prospekt nahrazuje *whitepaper*, protože taktéž obsahuje důležité informace o tokenu pro investory. [15]

Existují však výjimky, při kterých není nutné prospekt tvořit:

- Pokud jsou kupující pouze tzv. kvalifikovanými investory.
- Pokud se jedná o tzv. omezenou nabídku. Tedy velikost celkového úpisu nesmí přesáhnout 1 000 000 EUR.
- Pokud jsou tokeny nabízeny méně než 150 investorům.
- Minimální investice je vyšší než 100 000 EUR.

Pokud by se tak projekt, resp. tokenizace cenného papíru, pohybovala v rámci těchto výjimek, nemusel by se prospekt vydávat, a bylo by o jednu regulatorní záležitost méně. [15]

Výše zmíněné regulace jsou zajišťovány z pozice Evropské unie a měly by platit ve všech členských státech. Co se změn a dodatečných regulací přímo v rámci České republiky týká, dalo by se říci, že prakticky žádné neexistují. Naše země se řadí mezi ty, kde security tokeny a i vlastní tokenizace (STO) jsou prakticky bez regulace, a dokonce i evropská regulace zde neplatí v plném kontextu. V Čechách neexistuje žádný právní dokument, který by nějak upravoval kryptoaktiva jako celek. Dle soukromého práva tokeny nespadají do definice cenných papírů, spadají však pod definici nehmotného

movitého majetku. Aby se mohlo jednat o cenný papír, pak dle občanského zákoníku musí být právo v něm obsažené spojeno s listinou (resp. jakýkoliv hmotný podklad). Token tak nesplňuje základní premisi, aby mohl být v České republice považován za cenný papír. [15] [7]

V roce 2018 ministryně financí konzultovala změnu občanského zákona, který by zapříčinil, že by na security tokeny mohlo být pohlíženo jako na investiční aktivum (cenný papír), a tudíž by se na něj vztahoval zákon ZPKT[10], a tím pádem i regulace MiFID II (Ta totiž nedefinuje, co je to cenný papír, ale jak se s ním má pracovat. Definici cenného papíru pak přejímá z jurisdikce daného státu). Avšak aktuální stanovisko Ministerstva financí České republiky je, že security tokeny nesplňují definici pro cenné papíry, a tudíž jimi nejsou. [7]

Mnozí s postojem ministerstva financí nesouhlasí a volají po zahrnutí tokenů pod ZPKT [7]. I přes to, že dnes není tokenizace v ČR prakticky nijak regulována, a je zde tak možnost tokenizovat akcii i dluhopis bez jakéhokoliv svazujícího právního rámce, dělá z tokenizace v ČR na jednu stranu zajímavou příležitost, jak obejít regulace při klasické formě úpisu cenných papírů, avšak na druhou stranu vytváří velký prostor pro podvodné jednání. Pokud však člověk uvažuje o seriózní tokenizaci, je na místě přistupovat k procesu, jako by se jednalo o standardní emisi cenného papíru. Pravděpodobnost, že při rozšiřující se popularitě security tokenů regulace dříve, nebo později přijde, je velmi vysoká. Tokenizovaná akcie či dluhopis tak mohou do regulace za několik let spadnout a nepřipravenému emitentovi (a v konečném důsledku i investorovi) to může způsobit nepříjemnost navíc.

3.3.2 Postup provedení tokenizace

V této kapitole je sepsán návod na provedení procesu tokenizace. Čtenáři by měl dát konkrétnější představu o tom, co je pro proces třeba udělat. Vzhledem k absenci právního rámce v ČR je čtenáři prezentován návod, který (dle mála zdrojů, které jsou k

[10] Zákon o podnikání na kapitálovém trhu

dispozici, v Česku prakticky žádné) povede k vytvoření security tokenu, avšak faktické kompliance s budoucí regulací, technická příprava tokenu, tokenomika [11] je pak třeba konzultovat s příslušnými odborníky (právníci, programátoři, a další). Zároveň použité nástroje pro tvorbu tokenu, služby třetích stran a další jsou ukázkou a možným využitím.

Dříve než bude vysvětlen vlastní postup tokenizace, je nutné si říci, jaké entity vstupují či mohou do procesu vstupovat:

- **Emitent**, tedy firma, která tokeny vydává. [15]
- **Platforma**, na které bude STO, tedy úpis tokenů proveden. Platforma by měla splňovat možnost registrace investorů, ověření jejich identity a samozřejmě by měla umožnit vlastní investici do tokenu. Zde jsou dva možné přístupy, buď si takovou platformu vytvořit, nebo využít již existující platformu třetí strany. [15]
- **Tým zabezpečující STO a poradci** by pak měli být nedílnou součástí projektu. Je třeba vytvořit tým lidí, kteří budou mít na starosti přímo emisi tokenů jako takovou. Jedná se o lidi, kteří mají na starosti jak procesní věci související s úpisem, tak i zákaznickou podporu v průběhu úpisu. Je dobré pamatovat i na poradenství od lidí, kteří si procesem již prošli či jsou znalí v oboru technologie blockchain a mohou poskytnout cenné rady, jak proces co nejlépe zvládnout. [15]
- **Prvotní investoři**, tedy ti, kteří investovali kapitál do firmy ještě před samotným STO. Stejně jako u klasické emise formou IPO vznikají ještě před samotným úpisem náklady firmě, které je třeba krýt počátečním kapitálem ať od vlastníků firmy, či od externích investorů. [15]
- **Advokáti** z důvodu konzultace nad splněním regulatorního rámce tokenizace. [15]
- **Banka** do procesu vstupuje také a to z toho důvodu, že je třeba někde shromažďovat vybrané peníze od investorů. Zároveň může banka poskytnout vlastní due

[11] Popsaný proces distribuce tokenů mezi investory https://coinmarketcap.com/alexandria/glossary/tokenomics

diligence firmy a pro investory to pak může být záruka kvality projektu, a tudíž bude větší zájem do projektu investovat. [15]

- **Burza**, na které bude moci se security tokeny po úpisu obchodovat. Mít sekundární trh pro následné obchodování je stejně důležité jako primární úpis tokenů. Pokud totiž neexistuje sekundární trh, kde by investoři mohli své tokeny prodat, není zde žádná přidaná motivace tokeny v primární nabídce kupovat. Toto však neplatí, pokud se jedná o private equity.[12] [15]

Jednotlivé kroky provedení tokenizace

Následující kroky tokenizace, které jsou v práci prezentovány, jsou zaměřeny zejména na práci se security tokenem, resp. jeho vytvořením až po způsoby nabídky investorům. Z pohledu úspěšného úpisu tokenů (jakož i jakéhokoliv cenného papíru) jsou však důležité i další kroky, jako například kvalitní business model či vztah s investory a PR firmy, které nejsou v návodu zmíněny, jelikož se práce zabývá pouze vlastním procesem převodu klasického cenného papíru na security token. Pro celkový úspěch jsou však důležité.

1. Definice struktury tokenu

Před započetím vlastní tvorby tokenu je třeba si definovat jeho strukturu, resp. to, co vlastně daný token reprezentuje a jakým způsobem bude nabízen investorům. Toto je nutné udělat nejen kvůli investorům, tedy aby přesně věděli, co kupují, ale i pro případného regulátora. I když aktuálně v ČR regulace není, neznamená to, že nemůže v brzké době přijít a v takovém případě je potřeba mít vše připraveno. Odpovědi na tyto tři otázky mohou pomoci při definici struktury: [15]

- **Proč** je token vydáván, resp. k čemu budou použity vybrané peníze?

[12] Tedy formu neveřejného úpisu cenného papíru.

- **Jak** bude s vybranými penězi zacházeno, reps. jak bude vytvořena přidaná hodnota pomocí těchto peněz.

- **Co** dostanou na oplátku investoři za nákup tokenu?

Odpovědi na tyto otázky dávají jasný obraz toho, co by měl token reprezentovat. Jedná se o tokenizovanou akcii, která vyplácí dividendu, nebo se jedná o diskontovaný tokenizovaný dluhopis či dluhopis s kupónem? Je token určen pouze pro institucionální, či kvalifikované investory, nebo pro retailové investory, v tomto případě je to otázka hlavně z pohledu regulace, neboť v případě nabídky tokenů pouze kvalifikovaným investorům není třeba podstupovat tolik regulatorních opatření, jako když je investice otevřena i retailovým zákazníkům. Dále mohou dát tyto odpovědi jasný pohled na to, zda-li bude, či nebude třeba vytvářet prospekt a další. Tyto otázky nesouvisejí pouze s tokenizací, i v případě standardní emise by měly být zodpovězeny, jsou však obecně velmi důležitým krokem před samotným začátkem.

Tato struktura tokenu by se pak měla jasně popsat a přeložit do srozumitelné řeči investorům při vlastním prodeji tokenů. Tomuto se říká ekonomika tokenu, zkráceně tokenomika, která byla v této kapitole zmíněna již dříve. Jedná se o popis podmínek distribuce tokenu:

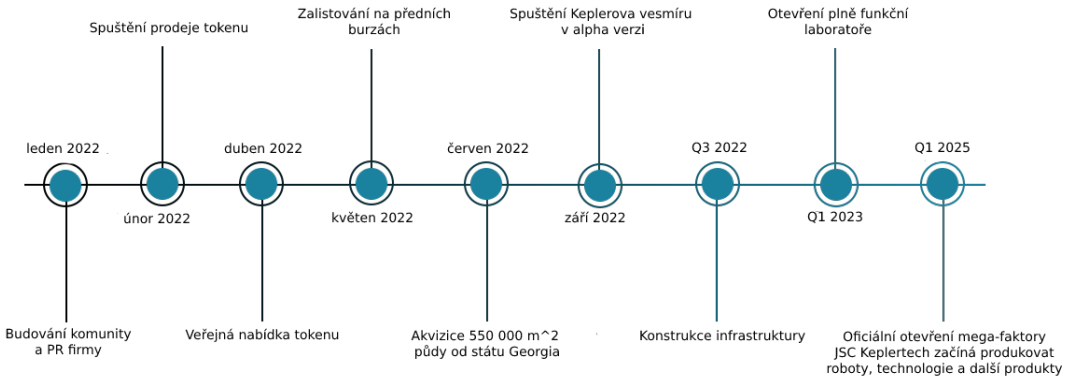
- **Minimální hranice** definuje minimální množství peněz, které je třeba v rámci úpisu vybrat. Pokud úpis skončí a není vybráno dostatečné množství peněz, firma peníze investorům vrací. Protože však i samotný úpis tokenů a přípravy na něj něco stály, nevrací se investorům celá původně vložená částka, avšak o něco méně. [15]

- **Maximální hranice** definuje maximální množství peněz, které může být vybráno, tedy maximální množství emitovaných tokenů. Může být, i nemusí být nastaveno. I přesto, že nenastavování takového limitu může vést k většímu výběru peněz, není to většinou ta správná cesta. Mnozí totiž tvrdí, že pokud firma obdrží

větší množství peněz, než které je schopna efektivně alokovat v rámci svého podnikání a vytvořit s nimi nějakou přidanou hodnotu, je ve výsledku horší jak pro investory, tak firmu samotnou [15]. Z tohoto důvodu by maximální hranice emise měla být nastavena.

- **Distribuce tokenů** pak říká, jak bude nastavena alokace tokenů mezi jednotlivé stakeholdery. Povětšinou platí, že záleží méně na tom, jaké množství tokenů celkem existuje, resp. bude emitováno, než na skutečnosti, jak jsou rozděleny mezi jednotlivé skupiny. Transakce na blockchainu jsou téměr neomezeně dělitelné, a tudíž je možné dát někomu i například tisícinu tokenu, je tedy důležité pouze relativní rozložení podílu. [15]

- **Distribuce vybraných peněz** je pak neméně důležitou součástí tokenomiky. Říká investorům, na co budou jejich prostředky použity a díky tomu si mohou udělat obrázek o tom, zdali se jim jejich investice vyplatí. [15]



Obrázek 3.4: Příklad grafického znázornění distribuce vybraných prostředků

Předposledním krokem při definici struktury tokenu je je zvážení nabídkové ceny tokenu, tedy startovací cenu, za kterou bude token v prvopočátku nabídnut investorům. Zde se proces od standardního IPO liší jen málo. Startovací cenu určí management firmy, případně za pomoci underwriterů[13], dle toho, kolik se chystají vydat tokenů a

[13] Jedná se o skupinu posuzující rizikovost firmy, často pomáhají stanovit férovou cenu za úpis aktiva.

kolik je třeba vybrat peněz za jejich prodej. Toto vychází právě z nastavení tokenomie. Na rozdíl od IPO však do procesu často nevstupuje banka (která u standardního úpisu ohodnocuje firmu a podává svůj pohled na férovou cenu po úpisu za účelem přilákání investorů). Je zde tak kladen daleko větší důraz na marketingovou složku celého procesu, aby token přilákal dostatečně množství investorů. [12]

Správné stanovení tzv. *offering price* je tak v případě procesu tokenizace trochu složitě. Obecně však platí, že by měla zahrnovat marže třetích stran, které s úpisem tokenů měly co dočinění.

Posledním krokem v první části je zamyšlení se nad právy (z legálního hlediska) investorů, kteří token dostanou. Jak již bylo napsáno v předchozích kapitolách, v případě security tokenů je nutné zajistit právní vymahatelnost toho, co představují. Díky tomu, že v ČR regulace prakticky není a díky tomu, že je tento krok po technické stránce velmi obtížný, je tato část problematická. V konečném důsledku záleží na advokátech, kteří budou emisi spolupřipravovat. Emitentovi však můžou pomoci k definování struktury práv spojených s tokenem následující otázky: [15]

- Z čeho se skládá podkladové aktivum?
- Jaký druh práv držitel tokenu dostává?
  - Jedná se o právo na podíl na zisku společnosti?
  - Jedná se o hlasovací právo na chod společnosti?
- Kdy jsou držiteli tokenu vypláceny výnosy?
  - Dividendy (kupóny)
    - Pravidelné dividendy
    - Dividendy na základě rozhodnutí managementu
    - Dividendy na základě rozhodnutí valné hromady
  - Výnos při prodeji tokenu

- Jaká je splatnost tokenu?

Definici struktury tokenu je dobré nepodceňovat, neboť veškeré další kroky na tento navazují a případná špatná, či nepromyšlená rozhodnutí by se tak propsala do celého procesu a mohla by znamenat rozdíl mezi úspěšným a neúspěšným úpisem. Ve zkratce je dobré strukturu konzultovat s poradenským týmem složeným ať již z lidí, kteří jsou odborníky na STO a svět blockchain, tak i například s advokáty.

2. Výroba tokenu

K výrobě tokenu lze použít v zásadě tři přístupy [15] [33]. Každý má své plusy a mínusy, které jsou v tomto kroku vysvětleny. Na jednom z těchto přístupů je pak vytvoření tokenu ukázáno.

1. Prvním přístupem je vytvoření vlastní blockchain sítě s vlastním tokenem, vlastním přístupem dosahování konsensu atd. Tento přístup je velmi náročný na technickou odbornost a velmi pravděpodobně bude vyžadovat najmutí externích programátorů a lidí, kteří jsou v problematice vývoje blockchainové sítě znalí. Zároveň bude třeba po vytvoření síť udržet bezpečnou a funkční, což bude vyžadovat rozšíření sítě mezi velké množství uživatelů, kteří budou transakce na ní ověřovat a zároveň jich bude dostatek na to, aby síť nebyla napadnutelná. Podrobnější výklad k bezpečnosti takové sítě je v kapitole 2.

   Pokud by byl zvolen tento přístup, pak základním prvkem, který je třeba určit před samotnou stavbou vlastního blockchainu, je mechanismus dosahování konsensu. Tedy vybrat jeden ze široké škály možností (proof of work, proof of stake, a další). Dále by bylo třeba určit, zdali bude blockchain veřejný, či soukromý a jak bude vůbec celý architektonicky postavený vzhledem k potřebám security tokenu. Dalším krokem, který by bylo třeba podstoupit, by byl audit kódu vytvořeného blockchainu. Tento audit provádí specializované firmy, které pomáhají odhalit chyby v kódu. Pokud by se toto neudělalo, investoři by mohli mít v ruce

token, za který někomu dali své peníze, ale který je k ničemu, protože nefunguje, jak má. V poslední řadě je pak dobré, aby na proces dohlížel i právní expert, s nímž je možné konzultovat technické vymoženosti sítě tak, aby v budoucnu mohly podléhat právním regulacím. Z textu by mělo být patrné, že tento přístup zvolí jen málo který emitent, většinou na to musí mít dostatečnou kapitálovou i lidskou kapacitu. Proces samotný je velmi náročný jak časově, tak i peněžně [14]. Výhodou tohoto přístupu je naprostá svoboda v řešení tokenizace. Security token běžící na vlastním blockchainu může mít jakoukoliv podobu. Tento přístup se tak hodí pro velké korporace, které mají velmi specifickou představu, jak by token i samotný proces tokenizace měl vypadat.

2. Druhým přístupem je využít již vytvořený blockchain, resp. jeho kód a modifikovat jej tak, aby splňoval představy emitenta. Tento přístup je velice podobný tomu předchozímu, stále je vyžadována velká technická znalost a je třeba zařídit prakticky totožné věci jako v případě prvního přístupu včetně následného zabezpečení sítě potom, co je vytvořena. Vypadává nicméně nutnost programovat síť od základů, a tudíž je práce o něco snazší. Ruku v ruce s tím jde však omezenější možnost upravit si síť do nejmenších detailů.

3. Třetí a nejjednodušší varianta je vytvoření tokenu na již existujícím blockchainu. Díky této variantě odpadá veškerá starost spojená s vývojem vlastního blockchainu, ať už je řeč o technické náročnosti či o bezpečnosti sítě (pokud je tedy zvolena již dostatečně bezpečná, velká síť, na které bude token vytvořen). Sítí, na nichž lze takto token vytvořit, dnes existuje několik. Každá přináší některé výhody a nevýhody:

    - **ETH** síť je největší, nejstarší a nejetablovanější sítí pro tvorbu tokenu. Mezi její výhody patří právě bezpečnost, podpora chytrých kontraktů a velké množství již vytvořených tokenů, tudíž existuje velké množství informací a in-

[14] Dle některých se cena tohoto přístupu (a to pouze implementace samotné) může vyšplhat až k 5 milionům Kč. https://azati.ai/how-much-does-it-cost-to-blockchain/

spirace pro to, jak cenný papír tokenizovat. Nevýhodou této sítě jsou pak poplatky, které jsou s transakcemi na ní spojené [15]. [18]

- **Hyperledger Fabric** [16] je privátní blockchain zaměřující se na řešení pro firmy. Funguje na modulárním principu. Taktéž podporuje chytré kontrakty. Mezi nevýhody patří nižší bezpečnost, neboť se jedná o centralizované privátní řešení. Mezi výhody pak patří jednoduchost a profesionální podpora.[18]
- **Tezos** je jeden ze starších blockchainů, který je taktéž hojně využívaný pro tvorbu tokenů. Oproti ETH má nižší zabezpečení vzhledem k jeho velikosti, avšak umožňuje velmi dobrou adaptaci a modifikaci na něm vzniklých tokenů s nižšími transakčními náklady.[18]

Smyslem práce není porovnávat mezi sebou desítky různých platforem za účelem odhalení, která je nejlepší. Pro shrnutí stačí říci, že každá se liší v určitém ohledu hlavně mírou bezpečnosti, poplatky a technickou přívětivostí. V konečném důsledku pak však všechny vedou k jednomu cíli, a tím je vytvoření security tokenu. Vzhledem k tomu, že je přístup vytvoření tokenu na již existující síti díky své nízké peněžní, časové i odborné náročnosti nejčastější, v práci je prodrobněji rozebrán právě ten.

Pro ukázku byla vybrána síť ETH. Na této síti se tvoří tzv. ERC-20 tokeny. Díky tomuto označení je zřejmé, že pocházejí právě ze sítě Etherea. Opět existuje několik možností, jak token na platformě vytvořit, v této práci je ukázán postup vytvoření tokenu na testovací síti ETH s využitím nástroje Remix [17] (pro hlavní síť je proces stejný, pouze jsou tokeny umístěny tam).

Jako první krok je třeba mít nainstalovanou aplikaci Metamask [18]. Jedná se o kryp-

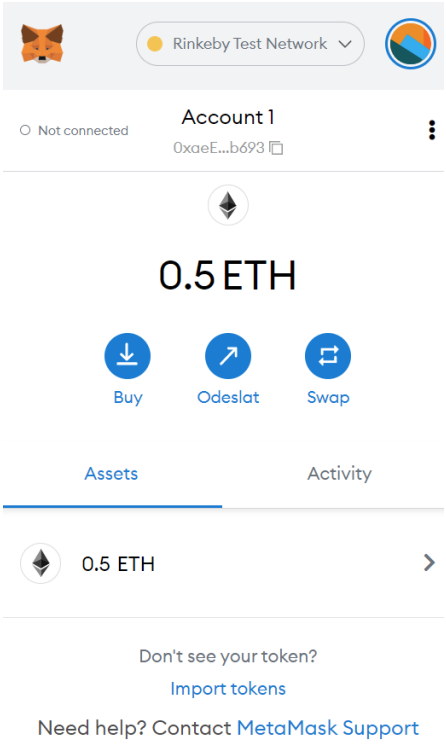
[15] Cena transakce je proměnlivá a někdy může dosahovat až stovky dolarů za jednu transakci. https://coingeek.com/the-ridiculously-high-cost-of-gas-on-ethereum/

[16] https://www.hyperledger.org/use/fabric

[17] Nástroj pro vytvoření a umístění tokenu na síť ETH. Token je totiž třeba nejen vytvořit, ale také na blockchain umístit, k tomu slouží právě takovéto platformy. https://remix-project.org

[18] https://metamask.io

toměnovou peněženku, díky které lze přesouvat tokeny, a zároveň je třeba mít v této peněžence nahrané tokeny ETH, ty slouží právě jako platidlo pro transakce a jsou počátečním nákladem, jenž je s procesem tvorby tokenu spojen. To, jaké množství tokenů ETH bude potřeba, se různí dle velikosti poplatků v síti, která je nestálá. Pro potřeby práce bude stačit 0,5 ETH viz obrázek 3.5.



Obrázek 3.5: Příklad peněženky Metamask[19]

Následně je třeba token naprogramovat. Cílem práce není token programovat, avšak pouze čtenáři přiblížit, jak celý proces vypadá. V práci je tak pouze na ukázku vytvořena základní podoba tokenu. Vzhledem k tomu jaké aktivum má token reprezentovat, se pak jeho parametry mění. Základními parametry tokenu jsou jeho název (*tokenName*), symbol, pod kterým je označován (*tokenSymbol*), na kolik částí je možno token rozdělit (*decimalUnits*) a počáteční množství (*initialAmount*).

```
function DPtoken(
```

[19]Na obrázku je vidět otevřený účet na peněžence Metamask připravený pro vytvoření vlastního tokenu.

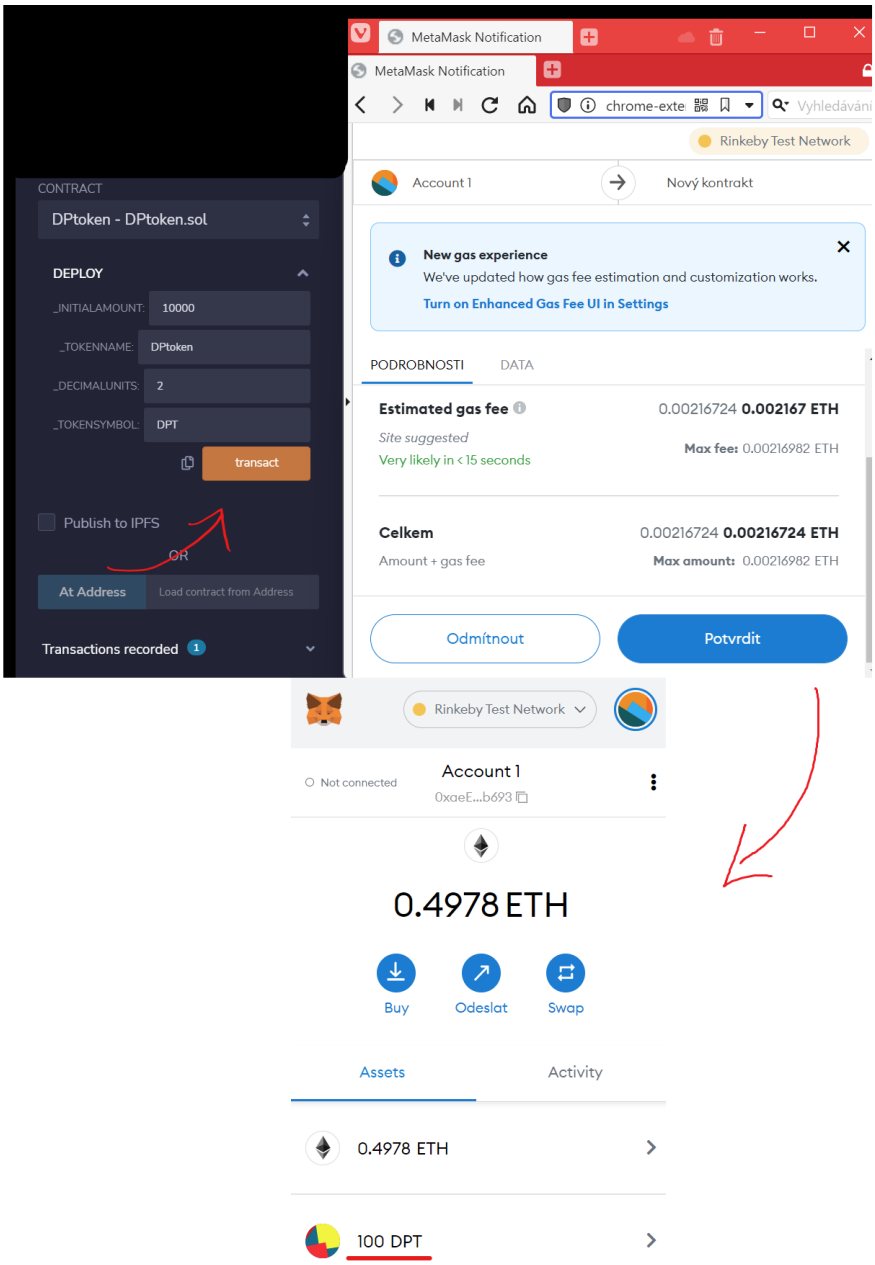
```
        uint256 _initialAmount,
        string _tokenName,
        uint8 _decimalUnits,
        string _tokenSymbol
    ) public {
        balances[msg.sender] = _initialAmount;
        totalSupply = _initialAmount;
        name = _tokenName;
        decimals = _decimalUnits;
        symbol = _tokenSymbol;
    }
```

Pokud je definován token, je třeba ještě definovat jeho chování. Zde velmi záleží na tom, co má token reprezentovat, pokud akcii, která vyplácí dividendu, je třeba tuto skutečnost zanést do kódu. Stejně tak by to bylo v případě dluhopisu, který vyplácí pravidelný kupón. Token umožňuje velkou míru automatizace těchto procesů, což je jednou z výhod tokenizace. Aby byl token funkční, měl by umět následující funkce:

- Zobrazení množství tokenů daného uživatele
- Transfer tokenu mezi vlastníky
- Transfer tokenu mezi vlastníky při splnění určité podmínky (například rozhodnutí valné hromady o vyplacení dividend, atd...)

Po naprogramování základní funkčnosti je určeno, kolik tokenů má být vytvořeno. Tyto tokeny se vytvoří na adresu peněženky Metamask, tedy na účet majitele tokenizované firmy či tokenizovaných dluhopisů. Z této adresy pak budou tyto tokeny při úpisu rozdělovány jednotlivým investorům.

Na obrázku 3.6 je pak ukázáno vytvoření 100 tokenů DPT, které byly přesunuty na testovací blockchain sítě ETH pomocí Metamask.



Obrázek 3.6: Vytvoření 100 tokenů na testovací síti blockchainu ETH.

Takto vytvořené tokeny jsou připraveny k úpisu a je možno přejít k dalšímu kroku. Je třeba mít na paměti, že prezentovaný příklad slouží jako ilustrace. V reálném případě bude třeba programováním tokenu a jeho vlastností (dle typu tokenizovaného aktiva) strávit více času. Nicméně vytvoření tokenu na již existující blockchainové síti není tak

moc náročné.

3. Úprava dokumentů pro investory

Příprava informačních dokumentů pro investory je zásadním krokem pro úspěšný úpis tokenů. Zde je třeba si dopředu promyslet, jaké skupiny investorů budou token kupovat a podle nich dokumenty připravit. Je dobré, připravené dokumenty nejdříve prezentovat vybrané skupině investorů a sesbírat od nich zpětnou vazbu. [15]

Důležité je také nezapomínat na právní stránku věci, pokud tedy parametry tokenizace cenného papíru zapříčíní nutnost vydat prospekt, je třeba to učinit.

4. Zřízení sekundárního trhu

Jak již bylo zmíněno v kapitole výše, jedna z předních výhod reprezentace podkladového aktiva tokenem je jeho jednoduchá převoditelnost a obchodovatelnost v globálním měřítku. Nicméně zalistování takového tokenu po úpisu na přední burzy není zdaleka automatická věc a je třeba k tomu učinit přípravné kroky. [15]

Mít k dispozici sekundární tržiště, na kterém je možné token prodat co nejdříve po úpisu, snižuje v očích investorů riziko, že token nebude likvidní. Burzy, na nichž se obchoduje s cennými papíry a security tokeny, jsou zpravidla velmi regulovaným prostředím a je tak pravděpodobné, že bude burza po firmě, která na ní chce své tokeny zalistovat, vyžadovat, aby taktéž tyto regulatorní opatření splňovala. [15] Je tedy třeba si určit, na jaké burze bude token zalistován a dle toho připravovat podklady. V podstatě existují dva typy burz:

1. **Centralizované burzy** řídí jedna entita (zpravidla firma), jsou většinou přísně regulovány, je na nich větší likvidita a jsou bezpečnější. Mají daleko přívětivější rozhraní na ovládání. Mezi nejznámější zástupce patří burzy: *Binance, Coinbase, Bitfinex, a další.*

2. **Decentralizované burzy** jsou pak burzy přímo na blockchain síti. Nejsou řízeny jednou entitou, likviditu zajišťují přímo uživatelé a záleží, o jakou burzu se jedná.

Pro nové tokeny je zpravidla likvidita výrazně nižší než u centralizovaných burz [20]. S velikostí burz se pak pojí i jejich bezpečnost, která je v porovnání s centralizovanými burzami menší. Mezi nejznámější zástupce patří: *Uniswap, Pancakeswap, 1inch, a další.*

Je samozřejmě možné vydat se cestou private equity, tedy cestou, kdy nebude řesen sekundární trh přes veřejnou burzu a security tokeny budou obchodovatelné například jenom formou P2P[21] po schválení prodeje volnou hromadou. Tento přístup pak snižuje požadavky na splnění regulatorního rámce.

Ať už je zvolený přístup jakýkoliv, vždy je dobré jej mít dopředu promyšlený a mít přichystány veškeré nutné věci s tím spojené.

5. Příprava bankovní infrastruktury

Na konci celého procesu chce firma vybrat peníze za prodej tokenů pro financování svého vývoje a zároveň svá tokenizovaná aktiva předat investorům. Infrasktruktura, která toto zabezpečí, se pak může skládat z:

- **Bankovního účtu**, na který budou peníze za tokeny vybírány.
- **Přístup na burzu** pro případ, že by byla platba za token prováděná formou kryptoměny, pak by měla být tato kryptoměna převedena na standardní FIAT[22] měnu.

6. Výběr platformy pro úpis

Platforma pro úpis poskytuje technické zázemí, kde se střetávají investoři s nabízeným tokenem. Opět zde existují dva přístupy:

1. První cestou je tvorba vlastní platformy. Je to cesta, která vyžaduje relativně velkou technickou a právní znalost aby bylo vše správně nastaveno. Výhodou je individualizace řešení.

[20] Někdy až stonásobně https://finex.cz/rubrika/kryptomeny/decentralizovane-burzy/
[21] Tedy z člověka na člověka.
[22] FIAT měny je označení pro klasické měny jako je koruna, dolar, euro a další.

2. Druhou cestou je výběr jedné ze stovek platforem, kde lze STO provést. Protože výběr platformy závisí na konkrétních specifikách tokenu, není předmětem práce je zde porovnávat. Je však důležité říci, že vybraná platforma by měla splňovat veškeré náležitosti, které s sebou daný token nese. Tedy musí splňovat všechny právní náležitosti (KYC,AML) a zároveň musí splňovat věci z hlediska ochrany soukromý dat investorů a dalších. Nezáleží však pouze na technických specifikách platformy, ale zejména pak na likviditě, kterou zvládne zabezpečit. Velké množství aktuálně existujících platforem totiž technické i právní zázemí splňuje, avšak postrádají likviditu již registrovaných investorů. [15]

7. STO a post-STO

V této fázi je již vše připraveno a je možné vlastní STO spustit. Již příchozí investoři se mohou zaregistrovat a pro přilákání nových se spouští marketingové kampaně. Zároveň se tým podpory stará o vyřizování případných dotazů od investorů. I když je většina procesů automatizovaných, je dobré jednotlivé transakce kontrolovat a před vydáním tokenů vše projet kontrolou.

Po proběhlém STO jsou přiděleny tokeny investorům. Transakce je dobré zdokumentovat, i když jsou zapsány na blockchainu. Následuje vyúčtování nákladů za celý proces tokenizace a zbylých peněz vybraných od investorů. Zároveň dochází k zaktivnění práv plynoucích z držby tokenů.

Po provedení všech výše zmíněných kroků je výsledný stav takový, že investoři mají v rukou tokenizované aktivum v podobě tokenu, z jehož vlastnictví jim plynou určitá práva a firma, jež tokeny upisovala, má na svém účtu prostředky pro další rozvoj.

Rozdíli v přípravě akcie a dluhopisu

Smyslem práce bylo zaměřit se na tokenizování z pohledu dvou typů cenných papírů, a sice akcie a dluhopisu. Rozdíl mezi těmito cennými papíry vychází z jejich podstaty, která je popsána v kapitole 1.1 a 1.2 této práce. Vlastnosti těchto cenných papírů je

pak třeba promítnout v rámci programování tokenu. Tedy zda se jedná o kupónovou tokenizovanou obligaci s periodou vyplácení kupónu 1x ročně. Je třeba tuto skutečnost promítnout v kódu tokenu.

V případě akcie je pak třeba ošetřit, aby vlastnictví její tokenizované podoby opravdu dávalo právo účasti na valných hromadách či na výplatu dividendy. První skutečnost je třeba ošetřit ve skutečném světě, druhou lze naprogramovat do kódu tokenu.

Rozdíly mezi tokenizováním těchto cenných papírů jsou tak spíše právního či procesního rázu, tedy jak zajistit, aby token reprezentoval vlastnosti právě tohoto cenného papíru. Co se rozdílů v tokenizaci jako takové týká, prakticky žádné neexistují, tedy až na část přípravy tokenu, kde se programovací část bude lišit dle toho, jaké vlastnosti se budou tokenizovanému aktivu přisuzovat.

3.3.3 Kdy je tokenizace vhodná

I když má tokenizace aktiv značné výhody, nevyplatí se vždy, resp. je nutná provádět. Je mylné se domnívat, že tokenizace vyřeší veškeré náklady spojené se standardními formami emise. Zejména pokud je na tokenizaci nahlíženo z dnešního pohledu, kdy je mnoho nedotaženého jak na poli technologie samotné, tak zejména pak na poli regulatroním, kdy mnohé jurisdikce nemají dokonce regulace vyřešeny nijak (případ například České republiky). Technická, právní i ekonomická infrastruktura pro ekosystém security tokenů je ve své rané fázi. Díky tomu je třeba vyvinout mnohdy větší úsilí, než bude třeba, až bude technologie dotaženější, což je pro mnohé, hlavně menší entity, zásadní problém. Zároveň je zde fakt, že pro většinu entit, které jsou v procesu tokenizace zapojeny, je tokenizace jako taková nová a pro mnoho z nich je tak lepší držet se zaběhlých konvencí. Zejména pak již několikrát skloňovaní právníci, kteří mnohdy pracují právě s nejasným výkladem práva, a musí tak investovat spoustu času do projektu, aby jej správně regulatorně nastavili.

Určitě je tedy třeba si podrobně promýšlet, zdali cenný papír ztokenizovat, či nikoliv. Případ, v němž je to chytré řešení, se odvíjí od několika faktorů. Nejzásadnějším

je otázka finanční, tedy kolik peněz je třeba vybrat, za jaký čas a od jaké skupiny investorů a zda-li má tokenizace v budoucnu i nějaké jiné, nepeněžní benefity. Pokud je třeba vybrat malou sumu peněz, nemusí být tokenizace vhodná a naopak. Pokud je kapitál získáván od několika různých drobných skupin investorů místo malé skupiny velkých investorů, pak je naopak tokenizace velmi vhodným nástrojem. Další věcí, co je třeba mít na paměti, je doba, kterou příprava samotné tokenizace a následný úpis tokenů zabere. Vzhledem k tomu, že v současné době velké množství burz shání potřebné licence pro možnost úpisu security tokenů, může proces trvat několik měsíců (pokud by byl zvolen více technicky náročný přístup, jako například tvorba vlastního blockchainu, mohl by proces zabrat mnohem více času). [15]

Je tedy zřejmé, že odpovědi na otázku, jestli tokenizovat, či netokenizovat cenný papír, není prosté ano, či ne a je třeba si věc více promyslet. Dřívější kapitoly této práce by však měly poskytnout již poměrně jasný obraz o tom, zdali je to proces, do kterého se chce firma pustit, či nikoliv. Poslední část, kterou zbývá osvětlit, je tak porovnání s běžnou emisí cenného papíru.

3.3.4 Běžná emise versus tokenizace

Porovnání z hlediska vlastností běžné emise s tokenizací je v práci probráno již v kapitole 3.1.1 a 3.1.2, kde se pojednává o výhodách a nevýhodách tokenů. Vzhledem k tomu, o čem pojednává zbytek práce, je jasné, že ani vydání tokenizovaných cenných papírů ani jejich běžná emise se neobejdou bez účasti třetích stran, alespoň ne nyní. U tokenizace existuje vidina doby v budoucnu, kdy budou doladěna technická a právní úskalí, v tu dobu odpadne nutnost mít některé prostředníky. I tak však může být proces tokenizace oproti běžné emisi mnohdy levnější záležitostí a to dle některých zdrojů až o 40%[23], a to zejména díky digitální povaze tokenu a faktu, že většina procesů lze díky chytrým kontraktům a technologii blockchain jako takové zautomatizovat (například vypořádání transakcí, či vyplácení kupónů). Při porovnání nákladovosti běžné emise **100**

[23] https://edsx.ch/blog-news/the-key-distinctions-between-an-ipo-and-sto

	Akcie	Dluhopis (bez prospektu)
Běžná emise	3 050 000 Kč [24]	3 800 000 - 6 150 000 Kč [25]
Tokenizace	1 830 000 Kč	2 280 000 - 3 690 000 Kč

Tabulka 3.2: Tabulka rozdílů nákladů emise[26]

milonů Kč akcií a dluhopisů oproti jejich tokenizaci je možno se dostat až na několika milionovou úsporu viz výše. Je zde však nutné ještě jednou říci, že při nízkých objemech může být tokenizace nákladnější, a to zejména kvůli tomu, že je zde málo výdajů, které se škálují dle velikosti emise. Většina výdajových položek je fixních.

Tokenizace, pokud je zvolena vhodně, může přinést značné výhody oproti běžné emisi, ať je již řeč o lepších vlastnostech tokenů, jakými jsou zejména možnost vlastnictví podílů podkladového aktiva, nižší nároky pro emitenta i investora na samotný proces emise, globální škálovatelnost a další či je řeč o nižší nákladovosti celého procesu díky automatizovaným procesům.

3.3.5 Diskuse a shrnutí výstupů práce

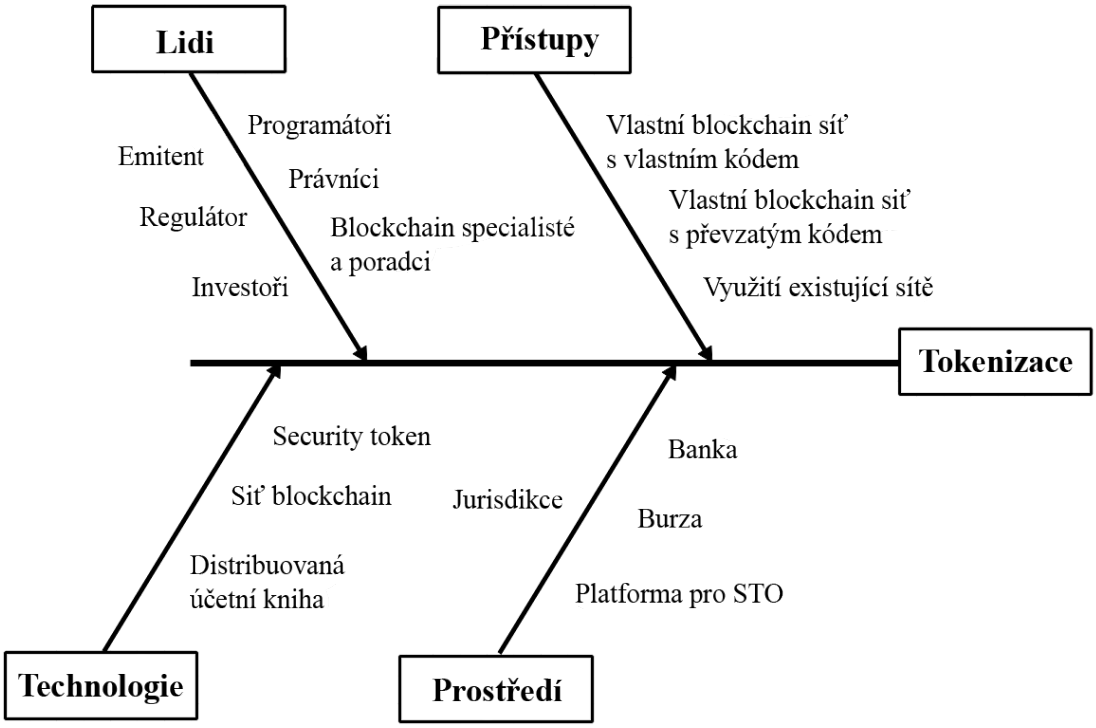
Přístup k vytvoření návodu na tokenizaci v práci byl přímý. Cílem bylo z neuceleného množství zahraničních a několika málo českých zdrojů s použitím vlastních znalostí dané problematiky poskládat a alespoň po technické stránce otestovat ucelené a hlavně praktické řešení provedení tokenizace v ČR. Mnoho autorů (viz někteří výše v textu) se ve svých publikacích zabývá obecným vysvětlováním dílčích problémů tokenizace, avšak čtenář je nucen si závěry poskládat sám. Ucelená literatura dnes prakticky neexistuje, a to z pochopitelných důvodů. Technický proces je specifický pro každou tokenizaci (vzhledem k tomu, jaké aktivum je tokenizováno a jaké vlastnosti mu chce emitent dát). Vytvořit jednotný návod technické části je tak kontraproduktivní. Zároveň je zde

[25] https://www.kapitalovypruvodce.cz/kapitalove-nastroje/akciove-trhy

[26] https://www.kapitalovypruvodce.cz/dluhove-nastroje/trh-s-dluhopisy

[26] Tabulka ukazuje možné rozdíly v nákladech na emisi mezi běžnou emisí a tokenizací cenných papírů v objemu 100 milionů korun.

stále ona absence právního rámce v ČR, a je tak obtížné být být i v této oblasti velmi konkrétní. Většina autorů (např. [14], [33]) se tak pouští pouze do rozebírání dílčích věcí, které jsou více ukotveny. Tyto problémy vyvstávaly i v průběhu tvorby této práce a tyto problémy jsou obsahem níže uvedeného Ishikawova diagramu (viz Obrázek 3.7).



Obrázek 3.7: Diagram procesů, které do problému tokenizace vstupují.

Při zkoumání této problematiky bylo překvapivým zjištěním, jak snadné je vytvoření základní podoby tokenu založeného na již existujících sítích jako je například Ethereum a jak složité je vytvoření vlastního na míru šitého řešení. Zároveň bylo překvapivým i zjištění, že se proces tokenizace pro jednotlivé druhy cenných papírů (akcie a dluhopisy) liší pouze v tom, jak je token naprogramován, avšak zbylý proces je prakticky totožný.

Tokenizace jako taková může být v budoucnu velmi zajímavou alternativou ke standardním formám emise, a dokonce se může stát i hlavní formou, jak si firmy budou na kapitálové trhy chodit pro kapitál. Vše záleží na tom, jak moc a jak rychle pokročí technologie blockchain a jak rychle budou zpracovány chybějící právní rámce.

Závěr

Cílem práce bylo přiblížit technologii blockchain, na které proces tokenizace stojí, probrat, jaké výhody a nevýhody skýtá a zejména poskytnout ucelený návod, jak takovou tokenizaci provést právě v České republice. Vzhledem k tomu, jak je technologie i celý přístup tokenizace mladý je těžké získat relevantní zdroje, které se problematikou očima českého prostředí zabývají. Zahraniční literatury pak existuje o mnoho více, avšak i zde jsou zdroje neucelené a zároveň mnohdy nepoužitelné pro české prostředí, a to zejména kvůli rozdílným jurisdikcím, kdy většina literatury nahlíží na security tokeny optikou amerického regulátora SEC, který přistupuje k výkladu práva velmi odlišným způsobem, než tomu je v Evropě, natož v České republice. Díky neexistenci právního rámce v ČR bylo sestavení takového návodu lehké i těžké zároveň. V konečném důsledku je totiž z pohledu českého práva velmi jednoduché cokoliv tokenizovat, protože se nebude jednat o cenný papír. Pokud však uvažujeme do budoucna a chceme být v souladu s možnými budoucími regulacemi, aby například naše tokenizované akcie mohly fungovat i za 5 let, je velmi těžké takový návod vytvořit.

Z pohledu technického je pak překvapivým zjištěním, jak lehké je takový token vytvořit, pokud bude použita již vytvořená technologie, na které bude programován. Tvorba tokenu pro příklad, který je v práci uveden, zabral několik málo hodin i se studiem dané problematiky. I samotná technologie je však nedokonalá, a to zejména v případě propojení tokenu s reálným světem. Tedy otázka, jak zajistit vymahatelnost práv spojených s držbou security tokenu, zůstává zatím nezodpovězena.

Tato práce vytváří základní kostru přístupu k tokenizaci a dává tak základ pro další výzkum v této oblasti. Zejména co se rozvinutí technické či právní stránky týká. Zároveň

je možné poznatky z této práce využít i při zkoumání možností tokenizace reálných aktiv (nemovitostí), kde je proces tokenizace velmi specifický a složitější, co se technického provedení týká, nicméně může být efektivnější.

Literatura

[1] Česká spořitelna a.s.: Bonusové certifikáty. [online], 2017, naposledy navštíveno 19.1.2021.
URL https://cz.products.erstegroup.com/Retail/cs/Produkty/Certifikaty/Bonus_certifikaty/Factsheety/Bonus_Certificate/LetuC3uA1k_-_BonusovuC3uA9_certifikuC3uA1ty/index.phtml

[2] Chalupa, I.; Reiterman, D.: *Cenne papiry: Zaklady Soukromeho Prava IV*. Praha, CZ: C.H. Beck, 2014, ISBN 9788074005428.

[3] Chance, C.: SECURITY TOKEN OFFERINGS – a European perspective on regulation. *Clifford Chance*, 2020.
URL https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/10/security-token-offerings-a-european-perspective-on-regulation.pdf

[4] Cruz-Cunha, M. M.; Mateus-Coelho, N. R.: *Handbook of Research on Cyber Crime and Information Privacy*. Hershey, PA: IGI Global, 2021, ISBN 9781799857280.

[5] Daimler; LBBW: Daimler and LBBW successfully utilize Blockchain technology for launch of Corporate Schuldschein. [online], 2017, naposledy navštíveno 27. 03. 2022.
URL https://group-media.mercedes-benz.com/marsMediaSit

e/en/instance/ko/Daimler-and-LBBW-successfully-utilize-blockchain-technology-for-launch-of-corporate-Schuldschein.xhtml?oid=22744703

[6] Di Pierro, M.: What is the blockchain? *Computing in Science amp; Engineering*, ročník 19, č. 5, 2017: str. 92–95, doi:10.1109/mcse.2017.3421554.

[7] Dědič, J.; Šovar, J.; Mikula, O.: Proč podle českého soukromého práva nelze uvažovat o (ICO) tokenech jako o cenných papírech. *PR 15-16*, 2018.
URL https://www.finregpartners.cz/wp-content/uploads/2018/09/ICO_Article_2018.pdf

[8] Frankenfield, J.: Hard fork (blockchain) definition. [online], 2021, naposledy navštíveno 16.02.2021.
URL https://www.investopedia.com/terms/h/hard-fork.asp

[9] Glasban: Asset Tokenization Services. [online], 2020, naposledy navštíveno 19.04.2022.
URL https://glasbans.com/asset-tokenization.php

[10] Group, E.: Erste Group and ASFINAG successfully launch Europe's first entirely blockchain-based capital markets issuance. [online], 2018, naposledy navštíveno 27. 03. 2022.
URL https://www.erstegroup.com/en/news-media/press-releases/2018/10/23/paperless-ssd-blockchain-alias

[11] Group, W. B.: World Bank prices first global blockchain bond, raising A$110 million. [online], 2018, naposledy navštíveno 27. 03. 2022.
URL https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million

[12] Hayes, A.: What is an offering price? [online], 2021, naposledy navštíveno 19.04.2022.
URL https://www.investopedia.com/terms/o/offeringprice.asp

[13] Jiang, S.; Li, Y.; Wang, S.; aj.: Blockchain competition: The tradeoff between platform stability and efficiency. *European Journal of Operational Research*, ročník 296, č. 3, 2022: str. 1084–1097, doi:10.1016/j.ejor.2021.05.031.

[14] Kaal, W. A.: Securities versus utility tokens. *SSRN Electronic Journal*, 2022: str. 22–15, doi:10.2139/ssrn.4021599.

[15] Kops, M.: *Assets on Blockchain: Security token offerings and the tokenization of securities*. Wroclaw, PL: Amazon Fulfíllment, 2019, ISBN 9789949012442.

[16] Kurzy.cz: Zkon o cennch paprech . 591/1992 sb. - seznam paragraf. [online], 2014, naposledy navštíveno 19.3.2022.
URL https://www.kurzy.cz/zakony/591-1992-zakon-o-cennych-papirech/seznam/

[17] Kučera, D.: *Dluhopisy a jejich druhy*. Diplomová práce, Právnická fakutla Univerzity Karlovy v Praze, 2010.

[18] Lawton, G.: Top 9 blockchain platforms to consider in 2022. [online], 2022, naposledy navštíveno 27. 03. 2022.
URL https://www.techtarget.com/searchcio/feature/Top-9-blockchain-platforms-to-consider

[19] Lewis, A.: *The Basics of Bitcoins and blockchains: An introduction to cryptocurrencies and the technology that Powers Them*. Bristol, UK: Mango Media / Open Road Integrated Media, 2018, ISBN 9781633538009.

[20] LUKRATIV, A.: Informace pro akcionáře. [online], 2010, naposledy navštíveno 19.3.2022.
URL http://www.lukrativ-as.cz/informaceproakcionare/

[21] Mikhaylov, A.: Cryptocurrency market analysis from the Open Innovation Perspective. *Journal of Open Innovation: Technology, Market, and Complexity*, ročník 6, č. 4, 2020: str. 197, doi:10.3390/joitmc6040197.

[22] Musílek, P.: Causes of global financial crises and Regulation-Failure. *Český finanční a účetní časopis*, ročník 2008, č. 4, 2008: str. 6–20, doi:10.18267/j.cfuc.285.

[23] Popovski, L.; Soussou, G.; Webb, P.: A brief history of blockchain. *Legaltech News*, 2018.
URL https://www.pbwt.com/content/uploads/2018/05/01005 1804-Patterson2.pdf

[24] Raikwar, M.; Gligoroski, D.; Kralevska, K.: Sok of used cryptography in Blockchain. *IEEE Access*, ročník 7, 2019: str. 148550–148575, doi:10.1109/access.2019.2946983.

[25] Rejnuš, O.: *Financni Trhy*. Praha, CZ: Grada, 2014, ISBN 9788024736716.

[26] Česká republika: Státní dluhopis České republiky. [online], 2000, naposledy navštíveno 19.3.2022.
URL http://www.akcie-dluhopisy.eu/cp1993/dluhopisy/stat/js0004-statni-dluhopis-ceske-republiky.htm

[27] SEC: Press release. [online], 2019, naposledy navštíveno 27. 03. 2022.
URL https://www.sec.gov/news/press-release/2019-212

[28] Shaughnessy: Innovation in Financial Services: The Elastic Innovation Index Report. *Inno Tribe*, 2015.

URL https://www.swift.com/resource/innovation-financial-services-elastic-innovation-index-report

[29] Sheridan, I.: MiFID II in the context of financial technology and Regulatory Technology. *Capital Markets Law Journal*, ročník 12, č. 4, 2017: str. 417–427, doi: 10.1093/cmlj/kmx036.

[30] Sherry, B.: What is the Genesis Block in bitcoin terms? [online], 2022, naposledy navštíveno 16.02.2021.
URL https://www.investopedia.com/news/what-genesis-block-bitcoin-terms

[31] Tian, Y.; Adriaens, P.; Minchin, R. E.; aj.: Asset tokenization: A blockchain solution to financing infrastructure in emerging markets and developing economies. *SSRN Electronic Journal*, 2021, doi:10.2139/ssrn.3837703.

[32] Tokenomy: Telegram (GRAM) token sale on tokenomy launchpad! [online], 2019, naposledy navštíveno 27. 03. 2022.
URL https://tokenomy.medium.com/telegram-gram-token-sale-on-tokenomy-launchpad-100b830173bc

[33] Wang, G.; Nixon, M.: SOK. *Proceedings of the 14th IEEE/ACM International Conference on Utility and Cloud Computing Companion*, 2021, doi:10.1145/3492323.3495577.

[34] Záruba, N. O.: Xixoio Dostává Naloženo PRÁVEM, Není Však Jediná. [online], 2021, naposledy navštíveno 15.12.2021.
URL https://finsider.cz/investovani/xixoio-dostava-nalozeno-pravem-neni-vsak-jedina/

Univerzita Hradec Králové
Fakulta informatiky a managementu

Zadání diplomové práce

Autor: **Radek Wildmann**

Studium: I1900321

Studijní program: N0688A140001 Informační management

Studijní obor: Informační management

Název diplomové práce: **Tokenizace cenných papírů v České republice**

Název diplomové práce AJ: Tokenization of securities in the Czech Republic

Cíl, metody, literatura, předpoklady:

Práce má za cíl poskytnou přehledný návod k emisi cenných papírů (akcií a dluhopisů) prostřednictvím technologie blockchain, tedy formou tzv. tokenizace a vysvětlit, jak se tento způsob liší od standardních způsobů emisí, jaké výhody a nevýhody přináší. Student v rámci práce připraví optimalizovaný návod jak tokenizaci provést v prostředí České republiky.

Osnova práce:

1. Úvod
2. Cenné papíry
3. Blockchain technologie
4. Běžná emise vs tokenizace
5. Jak na tokenizaci v ČR
6. Závěr

1. DĚDIČ, Jan, Jan ŠOVAR a Ondřej MIKULA. Proč podle českého soukromého práva nelze uvažovat o (ICO) tokenech jako o cenných papírech. *Právní rozhledy . Praha, 2018, 2018(15-16), 554-556.*
2. *AU, Sean a Thomas POWER. Tokenomics: The Crypto Shift of Blockchains, ICOs, and Tokens . Packt Publishing, 2018. ISBN 978-1789136326.*
3. *KOPS, Max. Assets on Blockchain: Security Token Offerings and the Tokenization of Securities . Tallinn: Blockerix OÜ, 2019. ISBN 978-9949012442.*
4. *HALE, Vincent. Launch an ICO. Successful Initial Coin Offering {\& Token Crowdsale: The Complete Guide to Prepare your Startup for Launching Successful Initial Coin Offering, raising Venture {\& Cryptocurrency Capital. Smashwords, 2018. ISBN 9781980218722.*
5. *LEWIS, Antony. The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them . Mango Media, 2018. ISBN 9781633538016.*

Garantující pracoviště: Katedra ekonomie,
Fakulta informatiky a managementu

Vedoucí práce: Ing. Jan Mačí, Ph.D.

Datum zadání závěrečné práce: 15.3.2020