FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Možnosti komerčního využití technologie blockchain
Student:	Vladislav Khomchenko
Vedoucí:	Ing. Pavel Šedek
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce zimního semestru 2020/21

Pokyny pro vypracování

Popište principy technologie blockchain. Analyzujte bezpečnost a dopady na ochranu soukromí uživatelů. Analyzujte možnosti využití technologie blockchain soukromými firmami, finančními a státními institucemi . Vyberte vhodnou možnost použití technologie blockchain a stanovte požadavky a případy užití pro zavedení ve firmě/instituci.
Po dohodě s vedoucím práce vyberte jednu netriviální konkrétní situaci/organizaci a případ užití a ten rozpracujte do formy návrhu implementace využití blockchain. Pro dokumentaci a návrh použijte vhodné nástroje a postupy softwarového inženýrství.

Seznam odborné literatury

Blockchain Enabled Applications: V. Dhillon, D. Metcalf, M. Hooper , 2017,Apress, Berkeley, CA
Blockchain Basics: D. Drescher, 2017,Apress, Berkeley, CA
Blockchain Technology in Finance: P. Treleaven, R. G. Brown, D. Yang, 2017, Computer, IEEE

Ing. Michal Valenta, Ph.D.
vedoucí katedry

doc. RNDr. Ing. Marcel Jiřina, Ph.D.
děkan

V Praze dne 20. února 2019

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Možnosti komerčního využití technologie blockchain

Vladislav Khomchenko

Katedra softwarového inženýrství
Vedoucí práce: Ing. Pavel Šedek

15. května 2019

Poděkování

Chtěl bych poděkovat Ing. Pavlu Šedekovi za vedení bakalářské práce, cenné rady a odborný dohled. Mé poděkování patří též Bc. Sofii Zhmakinové a Anastasii Sleptcové za jejich povzbuzování, trpělivé vysvětlování a učení cesty finanční gramotnosti. Na závěr bych chtěl poděkovat své rodině za podporu nejen během psaní této práce, ale i během celé doby mého dosavadního studia.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o etické přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 46 odst. 6 tohoto zákona tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou, a veškeré jejich dokumentace (dále souhrnně jen „Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla, a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu), licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 15. května 2019 ……

České vysoké učení technické v Praze
Fakulta informačních technologií
© 2019 Vladislav Khomchenko. Všechna práva vyhrazena.
Tato práce vznikla jako školní dílo na Českém vysokém učení technickém v Praze, Fakultě informačních technologií. Práce je chráněna právními předpisy a mezinárodními úmluvami o právu autorském a právech souvisejících s právem autorským. K jejímu užití, s výjimkou bezúplatných zákonných licencí a nad rámec oprávnění uvedených v Prohlášení na předchozí straně, je nezbytný souhlas autora.

Odkaz na tuto práci

Khomchenko, Vladislav. *Možnosti komerčního využití technologie blockchain.* Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2019.

Abstrakt

Bakalářská práce se zabývá principy technologie blockchain. V práci se provádí analýza mechanismů fungování blockchainu, analyzuje se bezpečnost a dopady na ochranu soukromí uživatelů, a možnosti využití technologie blockchain soukromými firmami, finančními a státními institucemi. V další části se práce zabývá analýzou existujících řešení a analýzou požadavků, na jejichž základě se navrhuje prototyp systému České spořitelny, a.s. s využitím blockchainu pro poskytnutí bankovního úvěru.

Klíčová slova technologie blockchain, smart kontrakt, Česká spořitelna, a.s., návrh systému, poskytnutí úvěru

Abstract

Bachelor thesis is devoted to the principles of blockchain technology. The thesis analyzes the mechanisms of functioning of the blockchain, analyzes the security and privacy protection of users, and assesses the possibility of using the blockchain technology by private companies, financial and public institutions. Part of the thesis is also an analysis of existing solutions and an analysis of requirements, on the basis of which a prototype of the Ceska sporitelna, a.s. system was developed using the blockchain to provide a bank loan.

Keywords blockchain technology, smart contract, Ceska sporitelna, a.s., system design, loan provision

Obsah

Seznam obrázků

Seznam tabulek

Úvod

Aktivní rozvoj naší společnosti pěstováním počítačových technologií a komunikačních sítí vstoupil do éry elektronických peněz. Mince a bankovky jsou postupně nahrazovány plastovými platebními kartami a na internetu je mnoho platebních systémů, původně vytvořených jen pro elektronické platby, jako PayPal, WebMoney apod.

Rozkvět informační infrastruktury přispěl ke vzniku takového pojmu jako „kryptoměna“ – typu digitální měny, nového platebního nástroje 21. století, který má řadu významných rozdílů od jiných druhů elektronických peněz, jehož tvorba a kontrola jsou založeny na kryptografických metodách. Takovým způsobem dnes velké množství lidí po celém světě používá kryptoměnu jako jednu z implementací technologie blockchain, což jen posiluje zájem o podrobnější posouzení a analýzu této sféry.

Práce se zaměřuje na návrh implementace systému České spořitelny, a.s. s využitím blockchainu pro poskytnutí bankovního úvěru. Teoretická část práce je rozdělena do několika částí. V první části se věnuje rozboru principů fungování technologie blockchainu z obecného hlediska. V další části práce jsou podrobně popsány mechanismy fungování technologie blockchain s technického pohledu. Na konci teoretické části jsou posouzeny výhody, nevýhody a možnosti využití technologie blockchain soukromými firmami, finančními a státními institucemi.

Praktická část práce stanoví uživatelské požadavky na systém a rozpracovává jeden z případů užití blockchainu v bankovnictví. Jako ilustrativní příklad je využitý systém poskytnutí bankovního úvěru v rámci České spořitelny, a.s. Hlavním cílem praktické části práce je návrh implementace celého systému tak, aby do sebe zapojoval blockchain.

Kapitola 1

Cíl práce

Cílem teoretické části práce je popsat principy technologie blockchain, analyzovat bezpečnost a dopady na ochranu soukromí uživatelů, ukázat možnosti využití technologie finančními a státními institucemi.

Cílem praktické části práce je vybrat vhodnou možnost použití technologie blockchain, stanovit požadavky a případy užití pro zavedení v instituci. Dílčím cílem práce je rozpracovat požadavky a případy užití do formy návrhu implementace pomocí vhodných nástrojů a postupů softwarového inženýrství.

Kapitola 2

Databáze

Na úvod je třeba provést rozbor analýzy základních mechanismů fungování technologie blockchain, posoudit jednotlivé typy databází a vymezit jejich hlavní rozdíly. S pomocí tohoto pak lze odpovědět na řadu otázek vylsovených v této práci.

2.1 Co je to databáze

Databáze – propracovaný systém pro ukládání dat organizovaných podle určitých pravidel s pevnou strukturou záznamů. Databáze tedy není nic jiného než úložiště dat [1]. Databázi si můžeme nejsnáze představit jako knihovnu, kde jsou knihy uloženy v určitém pořadí, což umožňuje zaměstnanci rychle najít požadovanou knihu.

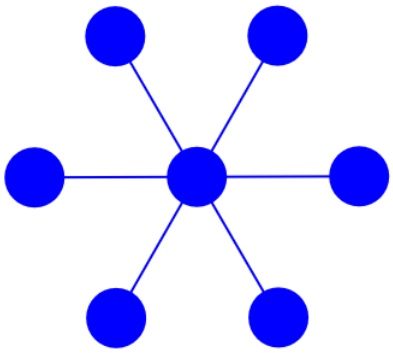
2.2 Typy databází

Z hlediska architektury se databáze dělí do následujících základních typů:

1. **centralizovaná**;
2. **decentralizovaná**;
3. **distribuovaná**.

2.2.1 Centralizovaná databáze

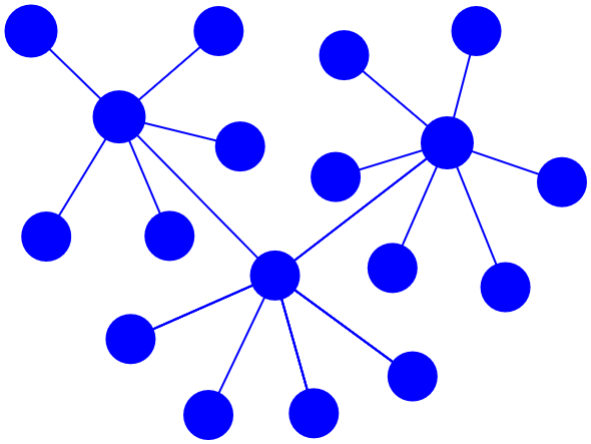
Centralizovaná databáze (obrázek 2.1) se vyznačuje tím, že je celá umístěná na centrálním počítači, kde uživatelé (klienti) přistupují k informacím prostřednictvím svých počítačů. Správa databáze se provádí centrálně. Počítač se zdroji se nazývá server, počítač, který přistupuje k serveru pro data, se nazývá klient [2].



Obrázek 2.1: Centralizovaná databáze

2.2.2 Decentralizovaná databáze

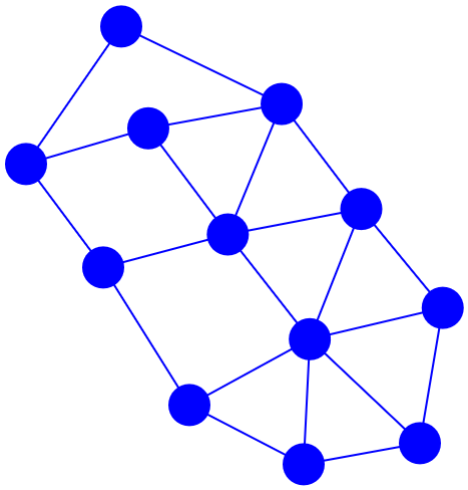
Decentralizovaná databáze (obrázek 2.2) znamená, že tato databáze nemá žádné hlavní centrální úložiště. Data nejsou přenášena z jednoho místa, ale existuje více hlavních serverů. Servery jsou navzájem propojeny. Výpadek jednoho serveru nemá jakýkoli vliv na další fungování sítě [2].



Obrázek 2.2: Decentralizovaná databáze

2.2.3 Distribuovaná databáze

Distribuovaná databáze (obrázek 2.3) je zcela soběstačná, stará se sama o sebe. Nikdo ji neřídí, její kopie jsou ukládány nezávisle na sobě ne na jednom místě, ale na několika místech, čímž vzniká databáze, která je řízena autonomně, bez jediného centra [2].



Obrázek 2.3: Distribuovaná databáze

2.3 Výhody distribuované databáze

Centralizovaná databáze má obrovskou nevýhodu před distribuovanou databází – zničení hlavního uzlu vede k nenávratné ztrátě dat, což zklame důvěru centrální autority.

„Na chodu a rozhodování decentralizované databáze se podílejí všichni její uživatelé za předem dohodnutých podmínek v podobě konsenzu. Blockchain je tedy decentralizovanou databází, která je jako celek dále rozdělována sítí na sobě navzájem nezávislých počítačích (tedy distribuována).“ [2]

Kapitola 3

Blockchain

3.1 Co je to technologie blockchain

Blockchain – velmi specifický druh databáze, ve které jsou uloženy všechny transakce, které jsou vedeny v takovém pořadí, ve kterém byly transakce uskutečněny, a všechna data ze všech existujících adres. Jde o neustále se rozšiřující chronologický řetězec záznamů, veřejných transakcí shlukovaných v blocích [3].

„Každý blok v blockchainu je identifikován hašem, vytvořeným kryptografickým hašovacím algoritmem aplikovaným na hlavičku bloků, obsahuje časové razítko a data o transakci (kdo posílá částku, jakou a komu). Každý blok také odkazuje na předchozí blok, známý jako rodičovský blok, pomocí pole „haš předchozího bloku“ v hlavičce bloku. Jinými slovy, každý blok obsahuje haš svého rodiče uvnitř své hlavičky. Posloupnost hašů spojuje každý blok se svým rodičem vytváří řetěz jdoucí zpátky k prvnímu bloku, který byl kdy vytvořen, známému jako základní blok (genesis).“ [4]

„Položka „haš předchozího bloku“ je uvnitř hlavičky bloků a proto ovlivňuje haš aktuálního bloku. Vlastní identita dítěte se změní, pokud se změní identita rodiče. Pokud je rodič změněn v jakémkoliv směru, haš rodiče se změní. Změna haše rodiče vyžaduje změnu v odkazu „haš předchozího bloku“ u dítěte. Tento krok způsobí změnu haše dítěte, což vyžaduje změnu v odkazu vnoučete, což způsobí změnu u pravnoučete, atd. Tento kaskádovitý efekt zajišťuje, že jakmile blok má mnoho generací následovníků, nemůže být změněn bez vynucení přepočítání všech následujících bloků. Protože takovéto přepočítání vyžaduje mnoho výpočtů, existence dlouhého řetězu bloků dělá blockchain v hluboké minulosti nezměnitelným, což je klíčovou vlastností blockchainové bezpečnosti.“ [4]

Jakmile se do řetězce přidá nový blok, je po ověření aktualizován na všech kopiích. To znamená, že každý klient má svou kopii blockchainu, kterou nezávisle kontroluje, a jakýkoli nesoulad okamžitě rozpoznán, v důsledku čeho takový blok bude odmítnut jinými uzly a nebude připojen k řetězci [5].

Blockchain lze přirovnat k Torrentu. Fungování torrentů probíhá v režimu P2P (*Peer-to-Peer* je počítačová síť, kde jsou všichni účastníci rovni). Když se stahuje nějaký soubor z trackeru, nepoužívá se centrální server ani úložiště. Soubor je přímo stažen od uzlu sítě. Pokud v peeringové síti nejsou žádní členové, nebude moci stahovat soubory. Stejně tak v blockchainu všechny operace jsou prováděny přímo mezi subjekty pomocí všech uzlů, které jsou připojeny ke stejné síti-blockchain [5].

Technologie blockchain, stejně jako internet, je odolná vůči chybám. Bitcoin, jako první implementace blockchainu, byl vynalezen v roce 2008. Od té doby funguje Bitcoin-blockchain bez významných narušení. Dnes problémy spojené s bitcoinem byly způsobeny hackingem služeb postavených na jeho vrcholu, nebo nedostatkem kontroly. Tyto problémy vznikají kvůli špatným záměrům a lidským chybám, a ne kvůli chybám v architektuře protokolu [5].

Internet již téměř 30 let prokazuje svou spolehlivost. Tento úspěch je dobrý pro technologii blockchain, která se neustále vyvíjí. Bez ohledu na to, jak to může být revoluční, je blockchain skutečně mechanismem, poskytující nejvyšší stupeň důvěryhodnosti. Žádné další zmeškané transakce, lidské nebo strojové chyby, ani změny provedené bez souhlasu zúčastněných stran nejsou známy [5].

Nejdůležitější je, že blockchain pomáhá zajistit legitimitu transakce tím, že ji zaznamenává nejen v hlavním registru, ale v distribuovaném systému registrů připojeném prostřednictvím bezpečného ověřovacího mechanismu [5].

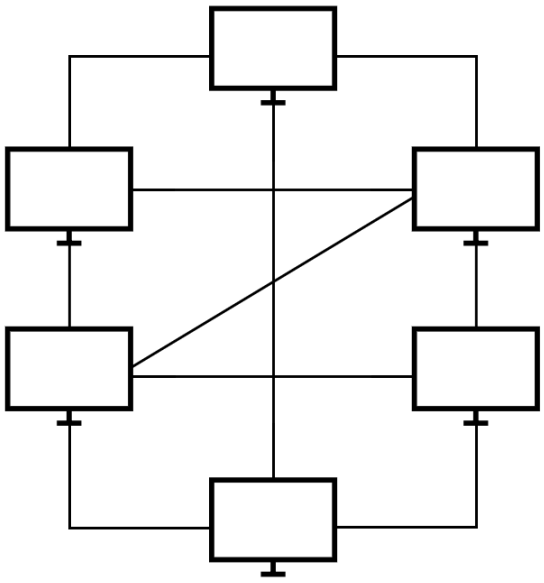
3.2 Síť Peer–to-Peer (P2P)

Síť Peer–to-Peer (obrázek 3.1) je založená na rovnosti účastníků. V takové síti často nejsou žádné centrální servery a každý uzel (*peer*) je klientem a funguje jako server, komunikující napřímo s ostatními klienty [6].

Na rozdíl od architektury *klient-server* taková struktura umožňuje udržovat síť na libovolném čísle a v libovolné kombinaci dostupných uzlů. Jednou ze základních výhod P2P sítí je i fakt, že výpadek jednoho z uzlů nemá žádný vliv na ostatní. Síť pokračuje, bez ohledu na to, ve fungování [6].

3.2.1 Řízení sítí

Při připojení nový klient kontaktuje tracker, který obsahuje seznam připojených uzlů. Může existovat spousta takových trackerů, které jsou potřebné pro optimální komunikaci mezi klienty. Optimalizací se rozumí, že stahovat řetězec bloků je lepší od uzlu, který se geograficky nachází v blízkosti, než od toho, který je daleko. To znamená, že propojovací centrum (*tracker*) umožňuje zjistit nového klienta, který je již v síti, a poskytuje mu seznam nejvhodnějších uzlů [6].



Obrázek 3.1: Síť Peer–to-Peer (P2P)

3.3 Typy blockchainu

V současné době existují jak decentralizované, tak i centralizované blockchainy a lze je rozdělit do dvou typů:

1. **veřejný blockchain**;
2. **privátní blockchain**.

3.3.1 Veřejný blockchain

Ve veřejném blockchainu neexistuje žádný řídící orgán. Veřejný blockchain (obrázek 3.2) může být viděn kýmkoliv a z kteréhokoli koutu světa. Každý má také možnost vytvořit v něm transakci. Tento systém navíc umožňuje každému uživateli účastnit se procesu konsensu a určit, které bloky budou přidány do sítě a které budou odmítnuty. Bezpečnost těchto systémů je zajištěna kryptografickými výpočty. Nejběžnější algoritmy jsou důkazem práce (*Proof-of-Work*) nebo důkazem sázky (*Proof-of-Stake*) [7].

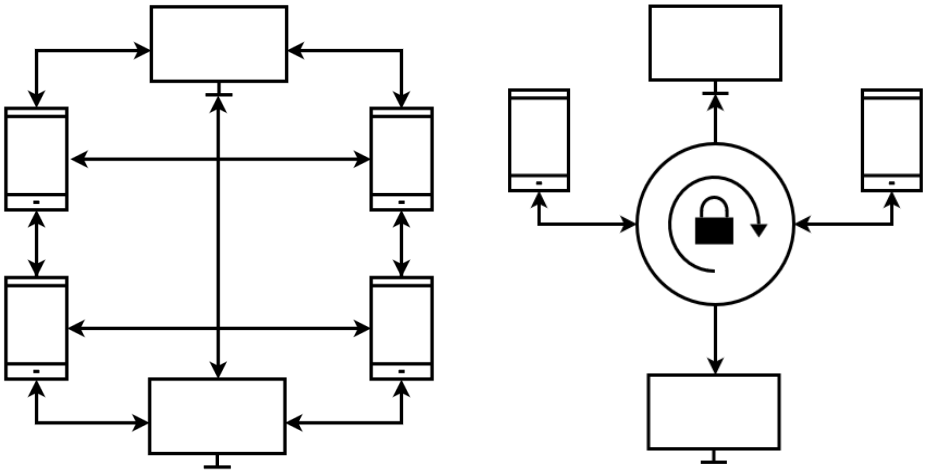
3.3.2 Privátní blockchain

Privátní blockchainy (obrázek 3.2) se vyznačují omezenou mírou přístupu. Potvrzení transakcí v těchto sítích, audit, správa databází jsou k dispozici přesně definovanému okruhu osob. Pokud mluvíme o čtení dat, pak takové právo může

být jak široce dostupné, tak přísně omezené. Jde tedy již o centralizovaný systém [7].

Kontrola sítě jedním centrem je výhodná v tom smyslu, že umožňuje rychle aktualizovat a zlepšovat funkčnost systému, což je obzvláště atraktivní pro organizace zabývající se účetnictvím [7].

Výjimka uzavřených systémů je to, že pro jejich efektivní fungování nevyžaduje algoritmus důkazů práce (*Proof-of-Work*). Může se připojit pouze podle potřeby, aby se usnadnil audit a zlepšilo se zabezpečení sítě. V tomto případě důvěra uživatelů již není založena pouze na důvěře k jedinému orgánu v podobě organizace a vychází z přísných matematických zákonů [7].



Obrázek 3.2: Veřejný a privátní blockchain

3.4 Mining (Těžba)

V závislosti na typu blockchainu (decentralizovaná varianta s použitím důkazů práce nebo centralizovaná s důvěryhodným centrem) mohou být transakční bloky (prázdné) vytvořené těžaři (*miners*) nebo hlavním uzlem (centrem). Těžaři – jsou uzly sítě, které vypočítají nový blok (což znamená blok transakce) [6].

Co znamená vypočítat nový blok a proč by měl být vypočítán? Jde o to, že v některých typech blockchainu vytvořit nový blok není tak jednoduché. Je třeba vyřešit obtížný úkol iterakce nad čísly, což je provedeno s cílem zabezpečení, aby ostatní účastníci nebyli schopni rychle nahradit řetězec bloku, protože výpočet takového haše může trvat hodiny, dny i týdny. V jiných typech blockchainu tyto lze haše vypočítat předem, proto cílem těžaře není extrakce bloků, ale poskytování svého pevného disku pro ukládání řetězců [6].

3.5 Konsensuální algoritmy blockchainu

Jakýkoliv systém fungující na základě distribuované databáze by měl poskytovat aktualizaci na všech zařízeních a maximalizovat správnost spojení bloků do řetězce. Konsensuální algoritmy dělají blockchain silnějším pokud jsou si účastníci navzájem neznámí [8].

K tomu existují různé metody. Nejznámější jsou:

- **Proof-of-Work** (PoW)
- **Proof-of-Stake** (PoS)

3.5.1 Proof-of-Work (PoW)

Důkaz práce (*Proof-of-Work*, PoW) – algoritmus pro dosažení konsensu v blockchainu. Slouží k potvrzení transakcí a vytvoření nových bloků. Pomocí PoW těžaři za odměnu navzájem soutěží o dokončení transakcí v síti [8].

Uživatelé sítě si navzájem posílají digitální žetony, po kterých jsou všechny transakce shromažďovány v blocích a zapsány do distribuovaného registru, tedy do blockchainu. Při potvrzení transakcí a uspořádání bloků je však třeba dbát zvýšené opatrnosti. Síť je založena na řešení složitých matematických problémů a schopností a lze snadno dokázat, že řešení bylo získáno [8].

3.5.1.1 Co je to matematický problém

Je to jeden z problémů, vyžadující značnou výpočetní sílu. Existuje mnoho takových problémů [8]:

1. hašovací funkce nebo pokus o nalezení vstupních dat, které znají výstup;
2. rozklad celého čísla na součin menších čísel;
3. problém výpočtu hodnot řetězce haš-funkcí někdy v určitém pořadí.

3.5.1.2 Jak funguje PoW

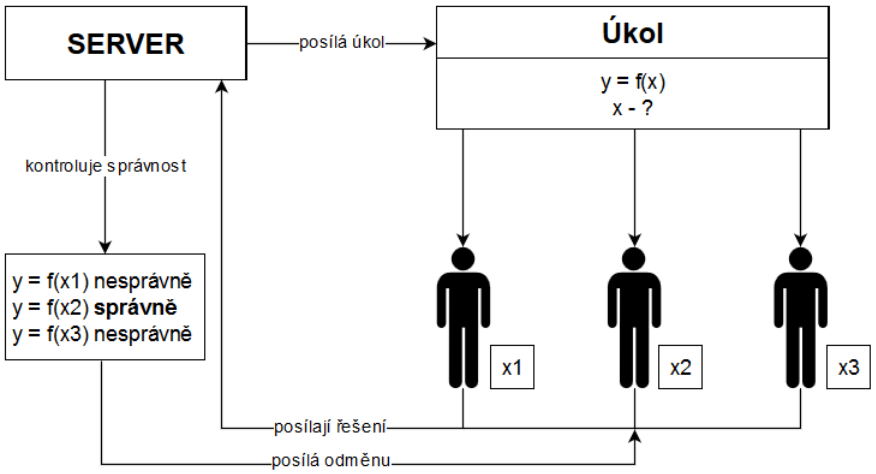
Přesnost a rychlost blockchainu závisí na tomto mechanismu. Problém by zároveň neměl být příliš komplikovaný – v tomto případě generování bloku bude trvat delší dobu, což znamená, že sada neúplných transakcí bude „viset“ na síti.

Pokud problém nelze vyřešit v předvídatelném čase, vytváření bloků se stane šťastnou náhodou. Pokud je problém vyřešen příliš jednoduše, je systém zranitelný vůči zneužití, spamu a útokům DoS.

Řešení by mělo být snadno ověřitelné, jinak ne všechny uzly budou schopny pochopit, zda byl výpočet proveden správně, což znamená, že budou muset důvěřovat ostatním uzlům, což je v rozporu s jedním z nejdůležitějších principů blockchainu – kompletní transparentnosti [8].

3.5.1.3 Jak je implementován PoW v blockchainu

Těžaři řeší problém, tvoří nový blok a potvrzují transakce. Složitost úkolů závisí na počtu uživatelů, aktuální síle a zatížení sítě. Pokud se těžařovi podařilo tento úkol vyřešit, vytvoří se nový blok – do něho se umístí další soubor transakcí, které se považují za potvrzené [8].



Obrázek 3.3: Důkaz práce v blockchainu

3.5.1.4 Kde se používá PoW

Důkaz práce se používá v mnoha kryptoměnách. Nejznámější z nich je Bitcoin, používající algoritmus, který umožňuje měnit složitost úkolu v závislosti na celkovém výpočetním výkonu sítě. Podobný systém je implementován v kryptoměnách podobných bitcoinu, například v litecoinu [8].

Dalším velkým projektem, který využívá PoW, je Ethereum. Vzhledem k tomu, že téměř 3/4 všech projektů blockchainu jsou implementovány na této platformě, lze s jistotou říct, že většina aplikací používá konsensuální model s důkazem práce [8].

3.5.1.5 Proč právě PoW

Jeho hlavními výhodami jsou ochrana proti DoS-útokům a nízký dopad podílu kryptoměny ve vlastnictví těžaře na možnosti výroby.

PoW ukládá určitá omezení na jednání účastníků, protože řešení problémů vyžaduje značné úsilí. Účinný útok také vyžaduje velký výpočetní výkon a zdlouhavé výpočty. Nezáleží na tom, kolik peněz máte ve své peněžence, je důležité mít velké výpočetní schopnosti pro řešení problémů a vytváření nových bloků, což znamená, že držitelé velkého kapitálu nemohou rozhodovat o celé síti [8].

3.5.1.6 Nevýhody PoW

Hlavní problémy: obrovské výdaje, „zbytečnost“ výpočtů a „51% útok“. Komplexní výpočty vyžadují specializované a drahé počítačové vybavení. Náklady nekontrolovatelně rostou a těžba je možná pouze pro velké skupiny těžařů. Specializované počítače navíc spotřebovávají velké množství energie, což zvyšuje náklady. V důsledku toho se postupně zvyšuje centralizace systémů, protože je to výhodné, je to přesně to, co se děje v případě bitcoinu [8].

3.5.1.7 Co je to 51% útok

„51% útok“ neboli útok většiny je možný v situaci, kdy uživatel nebo skupina uživatelů kontrolují většinu kapacity sítě – to jim dává možnost řídit události, ke kterým dochází v síti. Mohou tedy monopolizovat vytváření nových bloků a přijímat všechny odměny, protože mají moc zabránit ostatním těžařům v dokončení bloků. Navíc mohou zrušit transakce. Priklad: předpokládá se, že Alice poslala Bobovi „peníze“ přes blockchain. Alice se podílí na „51% útoku“, Bob ne. Jejich transakce je umístěna v bloku, ale útočníci nedovolí, aby se převod uskutečnil. Tím pádem Bob nedostane své peníze [8].

V dalším kroku se útočící připojí k jedné z větví, a protože mají větší výpočetní výkon, jejich řetězec obsahuje více bloků. Síť je navržená tak, aby byl přijat delší řetězec, a ten krátký odmítnut, což znamená, že transakce mezi Alicí a Bobem se neuskutečnila a Bob nedostal peníze. Tímto způsobem mohou útočníci zrušit transakce. „51% útok“ pravděpodobně nebude rentabilní. To vyžaduje obrovské výpočetní zdroje, a jakmile se to stane známým, síť je považována za kompromitovanou a uživatelé ji začínají opouštět, což nevyhnutelně vede ke snížení ceny kryptoměny [8].

3.5.2 Proof-of-Stake (PoS)

Důkaz o vlastnictví (Proof-of-Stake, PoS) předpokládá, že právo osoby na těžbu a kontrolu bloků s transakcemi určuje počet mincí, které vlastní. To znamená, že čím více bitcoinů nebo altcoinů má těžař, tím vyšší je jeho těžební síla [9].

První kryptoměnou, která využila takový algoritmus, byl Peercoin, následovaný Nxt, Blackcoinem a ShadowCoinem. Tento algoritmus byl vyvinut jako alternativa k důkazu práce (PoW), který má velké nevýhody. Když je transakce zahájena, její transakční data jsou umístěna v bloku s maximální kapacitou 1 MB a poté jsou duplikována na několika počítačích (síťové uzly). Uzel je administrativní jednotka blockchainu, která kontroluje správnost transakcí v bloku. Za účelem provedení takové kontroly těžaři musejí řešit speciální výpočetní problém a první z nich, kdo najde řešení, dostane právo dokončit blok a získat odměnu. Po kontrole bloku se transakce přidává do blockchainu [9].

Řešení takových problémů vyžaduje velký výpočetní výkon, což znamená spoustu elektřiny. Kromě toho, za účelem splacení těchto účtů, musí těžaři obvykle prodávat mince, které obdrželi jako odměnu [9].

Důkaz o vlastnictví (PoS) byl navržen tak, aby vyřešil tento problém. Těžař je nyní omezen svým podílem na celkové peněžní zásobě. Například těžař, který vlastní 3 % dostupných bitcoinů, může teoreticky zkontrolovat pouze 3 % bloků. Bitcoin používá důkaz o výkonu práce (PoW) a kvůli tomu je síť potenciálně náchylná k problému, který se obvykle nazývá *tragédie komunit*. V budoucnu se počet těžařů bitcoinu sníží, protože odměna za těžbu v průběhu času klesá. Jedinými poplatky jsou poplatky za zpracování transakcí, které se také snižují. Čím méně těžařů, tím zranitelnější je síť pro „51% útok“ [9].

Kapitola 4

Mechanismy fungování blockchainu

4.1 Struktura bloku

Každý blok (obrázek 4.1) se skládá z jednotlivých částí:

- **Adresa**
  Veřejný klíč generovaný asymetrickým šifrovacím algoritmem, založený na základě soukromého klíče, vytvořeného uživatelem.

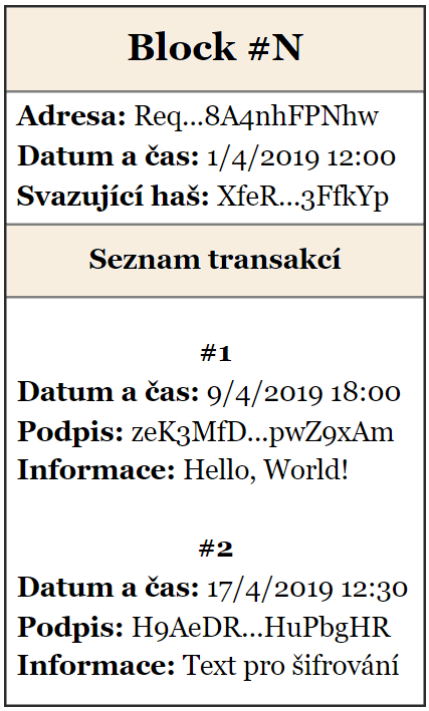
- **Datum a čas**
  Okamžik vytvoření bloku (transakce má také datum a čas vytvoření).

- **Haš (svazující)**
  Vypočten pomocí hašovacího algoritmu z adresy předchozího bloku a součtu haše všech transakcí aktuálního bloku. Proč je svazující? Protože při výpočtu je požadována adresa předchozího bloku.

- **Podpis**
  Umožňuje ostatním, aby věděli, že účet odesílatele uvedený v transakci je skutečně účtem, ze kterého byla transakce odeslána.

- **Informace**
  Zpráva, množství peněz, dokumenty, historie nemocí, programový kód apod.

Pro jednoduché pochopení, co je to blok, stačí prezentovat jej jako truhlík se zámkem, do kterého je potřeba něco dát. Pak je potřeba odemknout zámek klíčem, tento klíč je vytvořen při vytváření bloků a nazývá se soukromý klíč [10].



Obrázek 4.1: Struktura bloku

4.2 Digitální podpis

Aby nedošlo k padělání informací uvnitř transakcí, je každá transakce uvnitř bloku podepsána elektronickým digitálním podpisem (obrázek 4.2).

Digitální podpis – jedná se posloupnost bajtů, které jsou vytvořeny převedením podepsané informace pomocí kryptografického algoritmu, a je určen k ověření autorství elektronického dokumentu. Digitální podpis je založen na použití algoritmu asymetrického šifrování a hašovacích funkcí. Jedním z takových algoritmů může být RSA [10].

Na rozdíl od asymetrického šifrování v symetrických šifrovacích algoritmech digitálního podpisu se šifrování i dešifrování provádí pomocí stejného klíče, zatímco v asymetrických šifrovacích algoritmech digitálního podpisu se podepisování provádí pomocí privátního (*private key*) klíče a ověření podpisu se provádí pomocí veřejného klíče (*public key*). Je třeba poznamenat, že „**ověření**“ a „**dešifrování**“ není to samé [10]!

Volba asymetrického šifrování je odůvodněna tím, že ostatní členové sítě se musí ujistit, že změny provedl vlastník bloku a podepsal právě svým podpisem.

4.2.1 Soukromý a veřejný klíč

Soukromý klíč (*private key*) je generován uživatelem a používá se k podpisu transakcí. Klíč je držen v tajnosti, ten kdo vlastní soukromý klíč má přístup k bloku v blockchainu [10].

Veřejný klíč (*public key*) musí být generován na základě soukromého klíče, tj. existuje mezi nimi matematický vztah. Může být zveřejněn, navíc je používán v blockchainu jako adresa bloku a také se používá k ověření podpisu v jiných blocích. Znalost veřejného klíče znemožňuje určení soukromého klíče [10].

Obrázek 4.2: Digitální podpis

4.2.2 Algoritmus podepisování informací

Vytvoření podpisu vyžaduje:

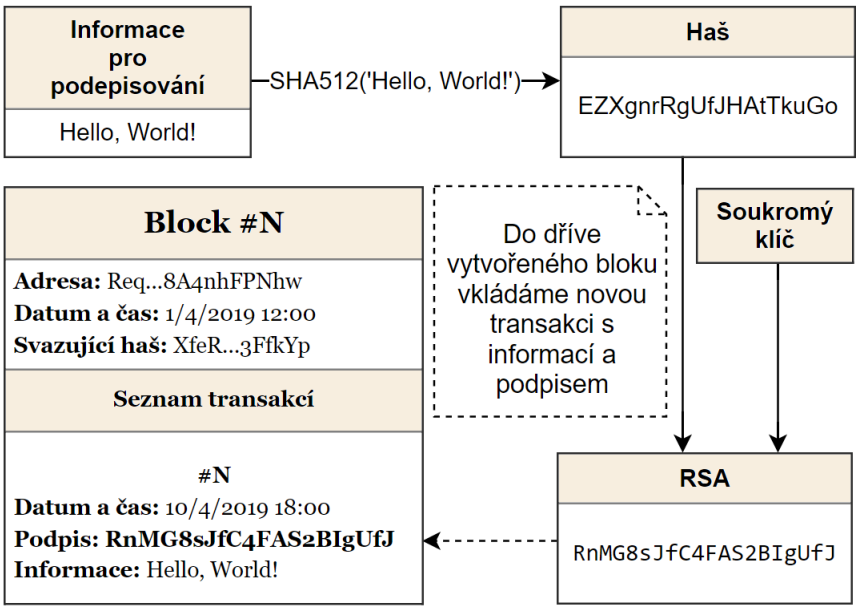
- asymetrický šifrovací algoritmus (například RSA);
- haš funkce (například SHA512);
- informace pro podepisování.

Vzhledem k tomu, že asymetrické algoritmy jsou ve srovnání se symetrickými algoritmy poměrně pomalé, objem podepsaných dat hraje významnou roli. V případě velkého objemu se bere haš podepsaných dat místo originálních dat. Haš se získává pomocí haš funkcí, které přijímají určité informace jako vstup a vracejí haš určité délky. Hašování lze přirovnat k fungování mlýnku na maso, kdy je možné mlít celé maso a získat mleté maso, ale není možné dostat celé maso zpět z mletého masa [10].

Tedy se digitální podpis neaplikuje přímo na samotný dokument, ale na jeho haš. Haš funkce není součástí algoritmu digitálního podpisu, takže v systému lze použít jakoukoli spolehlivou hašovací funkci [10].

Algoritmus (obrázek 4.3) lze rozdělit na fáze:

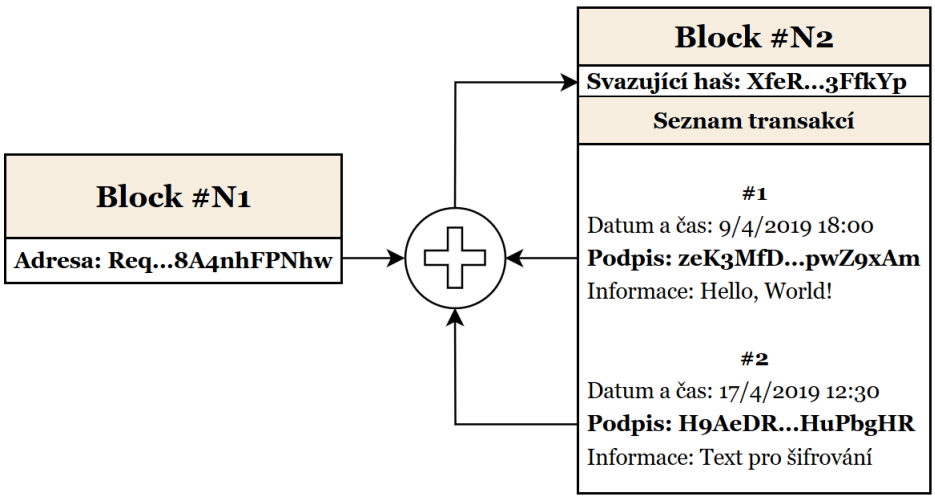
1. generování veřejného a soukromého klíče;
2. hašování informací pomocí SHA512;
3. pomocí RSA se dostává na výstupu podpis.



Obrázek 4.3: Algoritmus podepisování informací

4.3 Svazující haš

Svazující haš bloku (obrázek 4.4) se přepočítá při každém přidání nové transakce. Uvažuje se sčítáním všech transakčních hašů aktuálního bloku a adresy předchozího bloku [10]:



Obrázek 4.4: Svazující haš

Jedná se o haš, který kombinuje bloky do jediného řetězce, a co je nejdůležitější, chrání blockchain před padělaním vetřelci. Předpokládá se, že pokud někdo „bude chtít vyhodit“, nebo vložit svou jednotku do středu řetězce, pak následující bloky za ním již nebudou schválené, protože jejich haš byl založen na adrese, kterou vetřelec chce nahradit nebo odstranit [10].

Ve skutečnosti neexistují žádná definovaná pravidla pro generování haše předchozího bloku. Důležité je, aby se jeho pomocí vytvořila upřesněná posloupnost bloků.

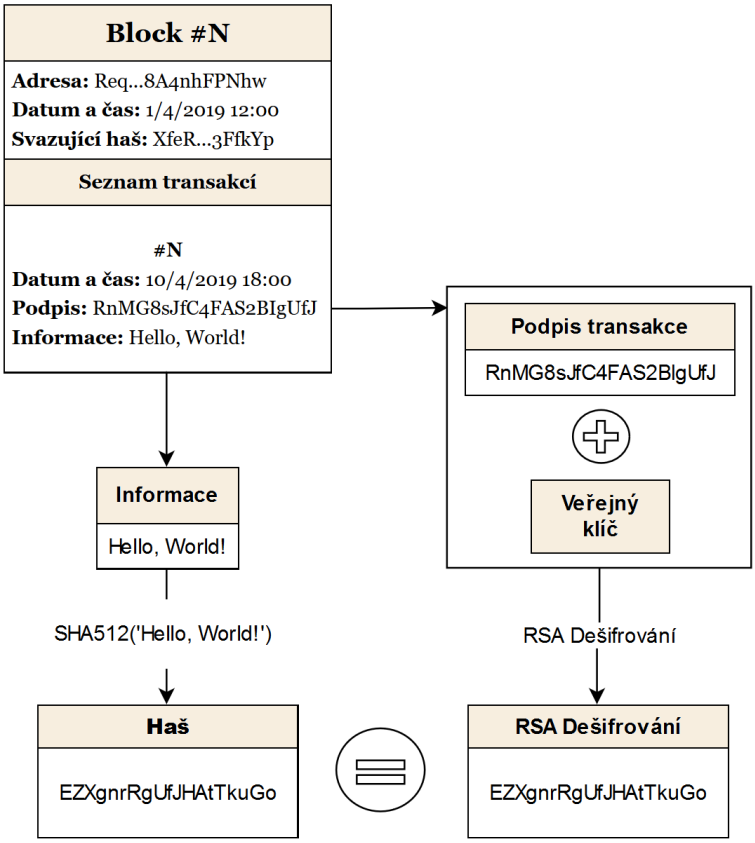
4.4 Ověřování dat blokchainu

Konsenzusový algoritmus může být definován jako mechanismus, kterým síť blockchain dosahuje konsenzu. Veřejné (decentralizované) blockchainy jsou postaveny jako distribuované systémy, a protože se nespoléhají na ústřední orgány, distribuované uzly se musí dohodnout na ověření transakce. Toto je místo, kde se projeví konsenzusový algoritmus, který zajišťuje dodržování pravidel protokolu a zajišťuje to, aby všechny transakce probíhaly důvěryhodným způsobem, takže žádná transakce nemůže být zaevidována několikrát [6].

4.4.1 Algoritmus kontroly transakcí

Algoritmus ověření transakcí (obrázek 4.5) ostatními účastníky sítě lze rozdělit do kroků:

1. získávání informace a podpisů z nové transakce;
2. získávání SHA512 haše z informace;
3. dešifrování podpisů pomocí veřejného klíče;
4. porovnání haše získaného v 2. kroku s hašem, získaným z dekódovaného podpisu v 3. kroku;
5. při neshodě hašů jsou data falešná a transakce je odmítnuta a není přidána do bloku.

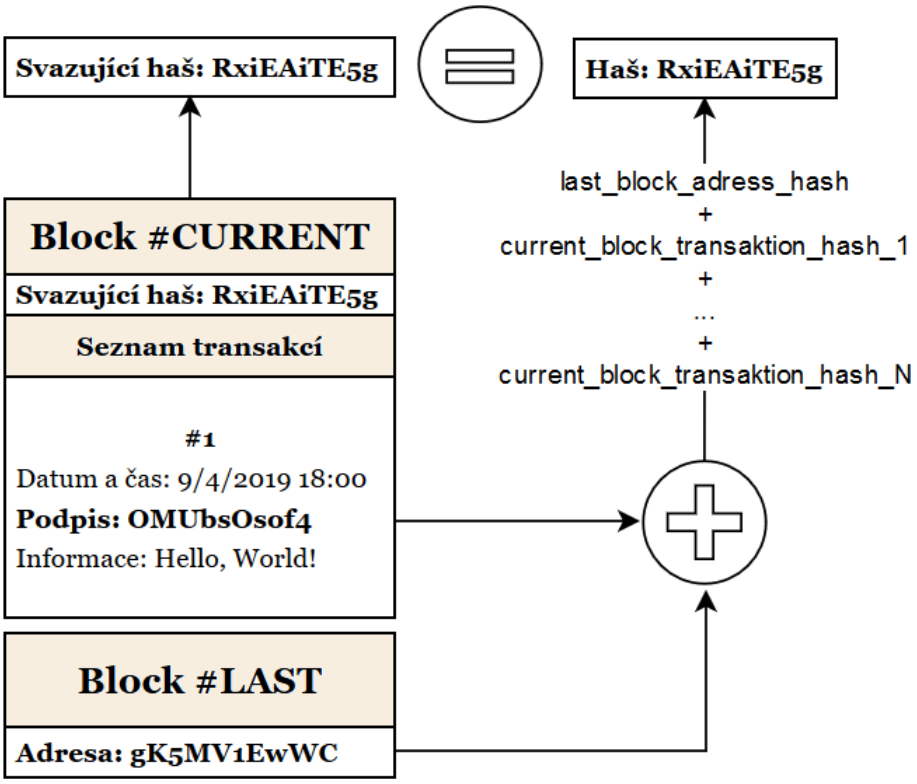


Obrázek 4.5: Algoritmus ověřování transakcí

4.4.2 Algoritmus kontroly bloku

Algoritmus kontroly nového bloku (obrázek 4.6) lze rozdělit do kroků:

1. přijetí adresy posledního přijatého bloku (aktuální blok ještě nebyl přijat a není poslední) a seznam transakcí aktuálního bloku;
2. výpočet haše SHA512;
3. porovnání výsledného haše s hašem (spojovacím hašem) z dosud nepřijatého bloku;
4. při shodě je blok správný a přidává se do řetězce. Jinak jsou data nesprávná a blok není akceptován.



Obrázek 4.6: Algoritmus kontroly bloku

Kapitola 5

Výhody a nevýhody blockchainu

Navzdory univerzálnosti blockchainu ve všech oblastech má každá technologie řadu výhod, ale i nevýhod. Oba pohledy jsou v této sekci podrobněji popsány.

5.1 Výhody technologie

5.1.1 Decentralizace

Jedním z hlavních důvodů přitažlivosti blockchainu je to, že technologie nezahrnuje centrální bod sběru dat. Namísto spouštění rozsáhlého datového centra a provádění všech transakcí přes tento bod, blockchain skutečně umožňuje, aby jednotlivé transakce měly vlastní ověřování a autorizaci, aby se zajistilo, že jsou vzájemně propojeny. Informace o konkrétních blocích řetězce jsou roztýleny na různých serverech po celém světě, což zajišťuje, že i když se tyto informace dostanou k nečlenům, jako jsou hackeři, bude ohroženo pouze malé množství dat a ne celá síť [11].

5.1.2 Bezpečnost dat

Mnohonásobná duplikace dat mezi účastníky zajišťuje bezpečnost a neměnnost informací uložených v bloku. Kvůli specifičnosti blokového zařízení nelze tyto informace nahradit, upravit nebo odstranit. Použití konsenzuálních algoritmů naznačuje, že všechny transakce obsažené v blockchainu jsou potvrzeny [11].

5.1.3 Transparentnost transakcí

Každý účastník sítě má přístup k celé historii transakcí až po první transakci. Proto, aby bylo možné ověřit, zda transakce mezi těmito dvěma adresami prošla, stačí se obrátit na jejich historii, která je uložena v bloku [11].

5.1.4 Vysoká rychlost transakcí

Běžné banky někdy potřebují k dokončení transakce několik dní. Taková období jsou způsobena protokolem v bankovním softwaru a také tím, že banky fungují pouze během pracovní doby, tedy pěti dnů v týdnu. Kromě toho mohou být finanční instituce umístěny v různých časových pásmech, což může také zpozdit zpracování transakce. Technologie blockchain zároveň funguje 24 hodin denně, sedm dní v týdnu, což znamená, že transakce na jeho základě je výrazně rychlejší [11].

5.1.5 Snížení transakčních nákladů

Vzhledem k tomu, že sítě blockchain jsou peer-to-peer, není nutné pro provedení transakce není nutné využívat služeb zprostředkovatelů. Díky blockchainu tak mohou uživatelé zjednodušit ověřování transakcí, zkrátit dobu platnosti transakcí, zvýšit likviditu a minimalizovat riziko podvodu. Uživatelé sítě blockchain navíc platí poplatky za potvrzení transakcí, které jsou ve srovnání s tradičními finančními institucemi, jako jsou banky, mnohem nižší [11].

5.2 Nevýhody technologie

5.2.1 Problém nadměrného využívání

„Velkou nevýhodou blockchainu představuje problém jeho nadměrného využívání. Vytvoření jednoho bloku trvá nějaký čas, přičemž při globálním využití by mohl být tento systém snadno přetížen a neúnosně by se zpomalil. Lze však předpokládat, že dokud tento problém nebude vyřešen, k všeobecné aplikaci blockchainové technologie nedojde.“ [3]

5.2.2 Problém měřítka

Další nevýhodou blockchainu by mohla být jeho neustále se zvyšující velikost, protože každý blok v sobě uchovává informace, které navždy na blockchainu zůstanou. Když je databáze příliš velká, kontrola informací trvá dlouho. Platby jsou tedy mnohem pomalejší. V současné době je v bitcoinu průměrná doba převodu plateb 4 až 5 hodin a maximálně 2 dny. Stojí za zmínku, že při zavedení tento čas nepřesáhl 10 minut [12].

5.2.3 Problém ochrany

Velké množství držitelů kryptoměn udržuje své úspory na burzách. To může být problém, protože burzy jsou cílem pro hacking. Mt Gox – největší kryptoměnová burza, byla v raných letech kryptoměny „hacknuta“ a všechny bitcoiny uživatelů uložených v ní byly odcizeny. V důsledku hackingu byly ztraceny

miliony dolarů. Perfektní bezpečné uložení bitcoinů a dalších krychtoměn založených na blockchainu je v současné době složitý úkol [12].

5.2.4 Problém kriminality

Kvůli anonymní povaze decentralizace technologie a kryptoměn, používajících tento systém, se stal blockchain klíčovým finančním nástrojem pro podvodníky. Jedním z příkladů je nelegální černý trh *Silk Road*, používající bitcoin k provádění transakcí. Na této stránce si lidé mohli kupovat takové věci, jako jsou nelegální drogy, pomocí kryptoměny založené na blockchainu. Nicméně, tento trh byl uzavřen několik let po zveřejnění, jakmile se FBI dozvěděla o jeho existenci [13].

Uzavření *Silk Road* bylo důležitým krokem prevence trestných činů. Někteří lidé stále považují tuto technologii za příliš atraktivní pro zločince a financování nelegálních aktivit bez detekce. V budoucnosti mohou být zavedena přísnější pravidla, aby se zabránilo používání technologie blockchain pro nelegální účely [12].

Kapitola 6

Využití blockchainu v praxi

Obecná povaha a potenciální šířka použití technologie blockchain jsou hlavními důvody, proč jí téměř všechna průmyslová odvětví věnují takovou pozornost. Poprvé v historii je možné získat transparentní, neměnný a distribuovaný registr, který poskytuje bezchybný reporting a eliminuje lidskou chybu [14].

Důsledky vzniku technologie blockchain tedy jdou mnohem dál, než je pouhé odesílání kryptoměny od jedné osoby ke druhé. Všechny výše uvedené vlastnosti blockchainu jako databáze znamenají, že každý průmysl, který vyžaduje jakékoliv zvážení, může být touto technologií radikálně transformován [14].

V dané kapitole jsou rozebrány některé příklady praktického využití technologie blockchain, mimo rozsah finančních služeb.

6.1 Sledování zásilek po celém světě

Podle generálního ředitele společnosti Smart Containers, Richarda Ettla, odeslání zásilky po celém světě vyžaduje několik set případů komunikace mezi různými stranami v dodavatelském řetězci. Je zřejmě jasné, jak je to neúčinné. Čím více lidí se podílí na jakékoli činnosti, tím více existuje příležitostí pro lidské chyby, jejichž výsledkem může být zpoždění, nedorozumění a nevyhnutelný nárůst nákladů [14].

Přidává se další úroveň složitosti, jakými jsou různé zákony, jazyky, měny a kultury. Jen v překladu z jednoho jazyka do druhého existuje velké množství míst pro úplnou nebo částečnou ztrátu informací. S technologií blockchain má každý zájemce jedno místo k vyhledávání informací, které již byly ověřeny, jsou přesné a neustále dostupné [14].

Je možné položit logickou otázku: může být obecná dostupnost a transparentnost technologie blockchain problémem pro podnik? Odpověď je rozhodně kladná. Některé informace by měly být k dispozici pouze určitým osobám. Pro takové případy, jako u společnosti Smart Containers, se používají bloká-

tory s omezeným přístupem veřejnosti, aby zajistily, že pouze ti lidé, kteří to skutečně potřebují, mohou získat přístup k informacím, které vyžadují [14].

Co je pak důsledkem? Rychlejší a levnější logistika s větší kontrolou celého dodavatelského řetězce. To je obzvláště důležité v zemědělství, protože zpoždění může vést k poškození nebo zhoršení kvality výrobků [14].

Velké společnosti, jako je Walmart a Kroger, také vidí význam použití technologie blockchain ve sledování potravin a zvýšení jejich bezpečnosti. Společnosti se podílely na iniciativě blockchainu společnosti IBM a úspěšně sledovaly určité potraviny, jako například čínské vepřové maso a mexické mango, po celém světě, a získaly vynikající výsledky [14].

6.2 Kontrola původu zboží

Poměrně málo lidí, zejména ve vyspělých zemích, se stará o původ potravin. Obrovské množství různých diet a nutričních schémat vyžaduje vyloučení standardních produktů a jejich výběr pouze podle určitých kritérií. Často to způsobuje, že lidé nakupují potraviny přímo na místě výroby, aby si byli jisti původem, což v závislosti na místě bydliště a stravovacím režimu může výrazně omezit výběr [14].

V současné době je těžké zjistit, zda se naše káva pěstuje například s využitím dětské práce, v souladu s normami vegetariánství, nebo podle určitých náboženských norem. To může být problém nejen pro lidi, kteří preferují určitý životní styl, ale i pro ty, kteří mají závažné alergické reakce nebo nesnášenlivost některých složek potravin (např. lepku) [14].

Společnosti jako VeganCoin, Ripe.io a Origintrail pracují na úpravě technologie blockchain pro použití v zemědělství. S ním lze nejen kontrolovat původ a přísady, ale také sledovat celou cestu dodávání potravin. To znamená, že lidé s určitou stravou již nemusejí být omezeni na místní nákup. Mohou si být jisti kvalitou a autentičností svého jídla, i když jsou vyráběny tisíce kilometrů daleko. Zvláště pečlivé mohou dokonce sledovat všechny fáze cesty svých výrobků od místa určení do svého talíře [14].

6.3 Správa identit

Služby správy identit umožňují uživatelům přenášet osobní údaje do blockchainu, čímž vytvářejí digitální identitu (*digital identity*). Uživatelé tak mají k dispozici širokou škálu nástrojů pro ukládání informací, jako jsou údaje o pasech, rodné listy a sňatky, řidičské průkazy, průkazy totožnosti, přihlašovací údaje, hesla a další osobní údaje. Pomocí blockchainu si uživatel může vybrat, které informace se budou sdílet a kdo k nim bude mít přístup. Kromě toho, po jedinečném absolvování procesu identifikace osoby, se uživatel může přihlásit do sítě a dalších služeb bez opětovného zadávání informací [15].

V roce 2017 se konzultační gigant Accenture a největší IT korporace Microsoft Corporation spojili pro vývoj a implementaci blockchain platformy, s jejíž pomocí více než 1 miliarda lidí po celém světě dostane platné digitální průkazy totožnosti [15].

Mimo to na kryptografickém trhu existuje již 20 společností, které poskytují různé služby v oblasti správy osobních údajů, identifikace a potvrzení přístupových práv. Takové startupy zahrnují HYRP, BlockVerify, OneName a mnoho dalších [15].

6.4 Digitální aktiva

Za digitální aktivum považujeme cokoliv, co je reprezentováno v digitálním formátu. Taková aktiva jsou uložena na libovolném médiu: bud' je to počítač nebo multimediální přehrávač. Na druhé straně tokenizace je proces převodu práv na aktivum do tokenu, jehož digitální „dvojče“ je uloženo v bloku [15].

Vzhledem k tomu, že tokenizace probíhá pomocí blockchainu, společnosti mohou zavést nový systém správy aktiv, který zvýší likviditu, zajistí správu aktiv všem účastníkům a dokonce úplatní scénáře kolektivního použití. Navíc je efektivnější integrovat takové komponenty tradičního trhu s cennými papíry jako depozitář, burza, clearingové centrum a software [15].

Startupy Vaultoro, OneGram a Orebits se zabývají tokenizací zlata, kde si uživatelé mohou koupit digitální aktiva pro tento drahý kov pomocí kryptoměny. Společnost LAToken provádí tokenizaci cenných papírů a akcií prostřednictvím protokolu LAT Protokol, který umožňuje tokenizaci práv na aktiva a obchodování s nimi za kryptoměny. Navíc mezinárodní blockchain platforma Atlant umožňuje tokenizovat nemovitosti s následným umístěním ATL právního tokenu na decentralizovaných burzách [15].

6.5 Ochrana autorských práv

Porušení autorských práv je považováno za jeden z největších problémů v takových oblastech, jako je umění, hudba, kino a literatura. Použití blockchain technologie umožňuje autorům potvrdit a chránit autorská práva a práva k duševnímu vlastnictví. Navíc technologie umožňuje bezpečné ukládání a rychlou aktualizaci informací o všech objektech [15].

Tímto způsobem společnost Ascribe, prostřednictvím použití blockchainu, pomáhá umělcům potvrdit svá autorská práva k vytvořeným objektům umění pomocí unikátních identifikátorů a digitálních certifikátů. K dispozici je také převod vlastnického práva od umělce nebo autora na kupujícího nebo sběratele [15].

6.6 Elektronické hlasování

Follow My Vote vyvíjí bezpečné a transparentní platformy pro anonymní online hlasování pomocí technologie blockchain a eliptické kryptografie pro zajištění přesných a spolehlivých výsledků. Zdrojový kód projektu je zcela veřejný [15].

V únoru 2016 Nasdaq a estonská vláda oznámily, že státní digitální platforma e-Residency bude použita pro zjednodušení procesu hlasování ve státě. Platforma e-Residency je elektronický identifikační systém, který široce používají jak estonští obyvatelé, tak lidé, kteří mají obchodní zájmy v zemi. Platforma umožňuje všem majitelům příslušných identifikačních karet a digitálních klíčů přístup k široké škále vládních, bankovních a dalších služeb [15].

Kapitola 7

Blockchain v bankovnictví

Bankovní služby jsou oblast, která zřejmě nejvíce využívá technologii blockchain. Co je to banka? Je to organizace, která by měla plnit čtyři základní funkce: provádět převody, ukládat prostředky zákazníků, poskytovat úvěry a nabídnout klientům možnosti investování [16].

Aktivní účastníci kryptoměnového trhu poukazují na to, že infrastruktura blockchainu prakticky umožňuje takovou funkcionalitu. Mnoho kryptonadšenců se domnívá, že blockchain zničí existující bankovní systém. Podle názoru autor práce bude vše naopak: banky budou schopny přizpůsobit blockchain tak, aby vyřešily své problémy, a budou se vyvíjet cestou evoluce, snižováním nákladů a poskytováním pokročilejších služeb uživatelům [16].

Bankovní převod lze porovnat s blockchain-transakcí, například v bitcoinu, ale s jednou důležitou výjimkou: transakce v rámci blockchainu jsou nevratné. Pokud uživatel udělá chybu při zadávání adresy nebo částky převodu, nebude možné vrátit peníze bez souhlasu druhé strany. Kvůli této vlastnosti jsou transakce blockchainu mnohem komplikovanější než tradiční bankovní převody a spíše omezují možný okruh klientů pro banky [16].

7.1 Smart contract (Chytrý kontrakt)

Smart contract (Chytrý kontrakt) – elektronický protokol napsaný pomocí počítačového kódu. Jeho účelem je předávat informace a zajišťovat plnění smluvních podmínek oběma stranami [17].

Smart kontrakty jsou v podstatě programy, které jsou vytvořeny na základě počítačové logiky a jsou přenášeny ve formě kódu. To je důvod, proč účastníci transakce nebo smlouvy si mohou být jisti, že všechny podmínky smlouvy budou dodrženy, a nikdo z účastníků nebude moci změnit podmínky nebo interpretovat je pro sebe. Kód – zákon inteligentních smluv [17].

7.1.1 Smart kontrakt v bankovnictví

Jednoduchý příklad: Chcete-li otevřít klientský vklad, je nutné zapojit provozovatele a kontrolního manažera. Dále s klientem je nutné podepsat smlouvu, která podle pravidel musí být zaslána pro potvrzení různým službám (minimálně právnímu oddělení). Banka by měla také zohlednit hotovost v rozvaze, přepočítat účetní závěrku a různé finanční údaje (kapitálová přiměřenost, požadovaná výše jistoty vkladů). Takové řetězce má každá banka jiné a v praxi jsou mnohem složitější [17].

Zavedení smart kontraktů umožní automaticky uzavřít smlouvu, odeslat ji klientovi k podpisu, zkontrolovat správnost, zaslat ji příslušným oddělením, zadat informace do bankovních výpisů a přepočítat ukazatele, a to i v reálném čase. Není těžké si představit, kolik prostředků tato automatizace ušetří [17].

7.1.2 Vlastnosti smart kontraktu

Smart kontrakty umožňují bezpečně vyměňovat peníze, akcie, majetek a další aktiva přímo bez účasti zprostředkovatelů. Aby bylo možné uzavřít jakoukoli transakci, je třeba kontaktovat notáře nebo advokáta, zaplatit za dokumenty a počkat na jejich provedení. Často položky těchto dokumentů obsahují odkazy na právní články, které lze interpretovat pro sebe, takže lze obejít zákon. V případě nesplnění podmínek transakce v reálném životě se lidé musí obrátit na soud, znovu utrácet peníze na proces a dokázat nevinu. Při uzavírání těchto transakcí nelze mluvit o důvěře účastníků smlouvy [17].

Za tímto účelem byl vytvořen program, který sleduje plnění závazků obou stran stanovených ve smlouvě a také automaticky ukládá sankce za porušení nebo nedodržení podmínek transakce. Smart kontrakty zajišťují bezpečnost transakcí a zbaví nejednoznačného výkladu podmínek, a to díky tomu, že jsou založeny na kryptografii. Jedná se o výhodnější transakce z materiálního hlediska, protože osoba nemusí platit právníky, zprostředkovatele nebo žalovat někoho při nedodržení smlouvy. Navíc plnění podmínek transakce probíhá automaticky s minimálními náklady na jejich podporu, bez účasti třetích stran (zprostředkovatelů) [17].

7.1.3 Jak funguje smart kontrakt

Smart kontrakt je obvykle zapsán do bloku, kde je veškerá logika umístěna v softwarovém kontejneru. Tento kontejner kombinuje všechny zprávy týkající se konkrétní inteligentní smlouvy. Zprávy mohou hrát roli vstupů a mohou výstupů inteligentního smluvního programového kódu a vést k jakýmkoli činnostem mimo blockchain, v reálném nebo digitálním světě [17].

Povinné atributy smart kontraktu:

1. využití metod elektronického podpisu na základě veřejných a soukromých klíčů, které mají dvě nebo více stran dohody;

2. přítomnost soukromého decentralizovaného prostředí, do kterého se zapisují chytře kontrakty;
3. předmět smlouvy a existence nástrojů potřebných k jeho provedení (kryptoměnové účty, atd.);
4. přesně popsané podmínky jeho provedení, které účastníci smlouvy potvrzují podpisem.

7.2 Výhody blockchainu v bankovnictví

První výhoda – absolutní transparentnost transakcí, o což každá banka usiluje. Každý řetězec operací lze sledovat od začátku až do konce a pochopit původ finančních prostředků na účtu. V současné době je vše poněkud komplikovanější: nelze vidět informace o majiteli účtu, pokud je majitel v jiné bance. Pro to je potřeba zaslat do banky žádost o informace, čekat na výsledky a opakovat postup pro každou novou banku v řetězci [17].

Blockchain umožní bankám vytvořit velké společné registry, pomocí kterých lze sledovat jakýkoli peněžní tok. To znamená efektivnější boj proti praní špinavých peněz a daňovým únikům [17].

Druhá výhoda – automatické zúčtování. Pod tímto pojmem se rozumí provádění dohod mezi bankami na konci určitého období. Pokud například během dne dvě banky provedly spoustu vzájemných převodů, na konci jedna banka převede druhé „finální čistou“ částku. Zúčtování je nyní často vedeno třetí stranou – zúčtovacími středisky, které jsou povinny spravovat je spravedlivě. V blockchainu garantem spravedlnosti je síť a automatizované procesy provádění transakcí. Při použití blockchainu mohou banky snížit své náklady odstraněním zprostředkovatelů a realizací všech vzájemných zúčtování v reálném čase[17].

Třetí výhoda – schopnost automatizovat platby, včetně mezinárodních převodů a plateb. Nejživějším příkladem je protokol Ripple, který umožňuje nejen rychle provádět převody bez ohledu na umístění odesílatele a příjemce, ale také rychlý převod měn (například na dolary, eura, jeny atd.). Nyní musí banky držet zásoby měny pro převod a shromažďovat informace o směnných kurzech od protistran [17].

Zvláštností Ripple je to, že řetězy mohou být libovolně dlouhé, mohou obsahovat téměř všechna aktiva a zahrnovat všechny možné protistrany. A co je nejdůležitější – nejziskovější řetěz je postaven automaticky během několika sekund. To může výrazně zjednodušit život nejen bankám, ale i běžným uživatelům. Univerzálnost transakcí a automatizace blockchainu může významně snížit dopad lidského faktoru na výsledek a zároveň snížit náklady eliminováním manuální práce [16].

7.3 Úvěry a investice

Pokud jde o půjčování a investování peněz, je situace ještě zajímavější. V obou případech je nejdůležitějším problémem pro banku bodování příjemce finančních prostředků (hodnocení rizik). K tomu je třeba znát příslušné informace o dlužníkovi: jeho úvěrovou historii, finanční situaci, míru finanční stability organizací atd [17].

Dnes jsou banky nuceny sdílet tyto údaje buď ve dvojicích, nebo přes úvěrový registr – samostatnou organizaci, která ukládá a zpracovává informace o úvěrové historii občanů. Blockchain je schopen eliminovat zprostředkovatele a šetřit náklady díky společné automatizované databázi kvality dlužníků [17].

V ideálním případě banky budou vidět klíčové informace o kvalitě dlužníka a jeho prostředcích ve všech finančních strukturách, dluhové zatížení, množství a frekvenci delikvencí a další vlastnosti. To vše vytvoří rozsáhlou databázi s informacemi o chování zákazníků, kterou lze použít k vytvoření přesnějších bodovacích modelů [16].

Kapitola 8

Návrh implementace

Po zkoumání základních principů a mechanismů fungování technologie blockchain se v dané kapitole rozpracovává jeden z případů užití blockchainu v bankovnictví. Jako ilustrativní příklad poslouží systém poskytnutí bankovního úvěru v rámci České spořitelny, a.s.

8.1 Analýza požadavků

V úvodu této kapitoly jsou popsány požadavky na systém. Rozbor požadavků je důležitá část analýzy, upřesňující fungování systému dle očekávání. V rámci analýzy se uvádí především přehled funkčních a nefunkčních požadavků.

8.1.1 Funkční požadavky

Funkční požadavky udávají požadavky na funkcionalitu systému, které by měl splňovat. Abstraktně popisují procesy pro dosažení určitého výsledku [18].

F1: Vytvoření žádosti
Systém umožňuje uživateli vytvořit žádost o poskytnutí úvěru. Proces vytvoření v sobě zahrnuje vyplnění povinných položek s údaji, na základě kterých banka rozhoduje o poskytnutí úvěru.

F2: Zrušení žádosti
Systém umožňuje uživateli zrušit žádost o poskytnutí úvěru.

F3: Kontrola stavu žádosti
Systém umožňuje uživateli sledovat aktuální stav žádosti.

F4: Schválení a odmítnutí žádosti
Systém na základě analýzy vyplněných dokumentů a údajů uživatele rozhoduje o poskytnutí úvěru.

F5: Vytvoření smart kontraktu
Systém v případě schválení žádosti o poskytnutí úvěru připravuje smart kontrakt pro podepisování mezi uživatelem a bankou.

F6: Podepisování smart kontraktu
Systém po vytvoření smart kontraktu umožňuje uživateli a bance podepsat kontrakt digitálním podpisem.

F7: Zápis do privátního blockchainu
Systém po podepsání smart kontraktu mezi uživatelem a bankou přidává transakce do privátního blockchainu banky. Z takového blockchainu lze jasně poznat, kterému klientovi byl jaký úvěr poskytován.

F8: Zápis do veřejného blockchainu
Systém po podepsání smart kontraktu mezi uživatelem a bankou přidává transakce do veřejného blockchainu mezi všemi bankami. Z takového blockchainu lze jasně poznat jaká banka poskytla jaký úvěr, ale nelze poznat komu.

8.1.2 Nefunkční požadavky

Nefunkční požadavky popisují další nezbytné vlastnosti systému vzhledem k prostředí a kontextu. K takovým požadavkům patří spolehlivost, bezpečnost, výkonost, atp. [19]

NF1: Bezpečnost
Pro libovolný systém je nejvyšší prioritou bezpečnost. Systém musí poskytovat vyšší důvěryhodnost.

NF2: Výkon
Aktualizace informací a provedení transakce musí být co nejrychlejší. Musí být zajištěny kvalitní algoritmy zpracování transakcí.

8.2 Diagram případů užití

Na základě stanovených funkčních požadavků je znázorněn diagram případů užití tak, aby se pokrývala funkcionalita systému. Diagram případů užití je znázorněn na obrázku 8.1.

Aktéři: Uživatel
Klient mající registraci v rámci bankovního systému. Podává žádost o poskytnutí úvěru.

Aktéři: Česká spořitelna, a.s.
Přezkoumá žádost o poskytnutí úvěru a na základě schválení/odmítnutí žádosti poskytuje/neposkytuje úvěr.

UC1: Vytvořit žádost
Uživatel vytvoří žádost, vyplní povinné položky s údaji a přidá potřebné dokumenty pro rozhodnutí banky.

UC2: Zrušit žádost
Uživatel zruší žádost, když on o tom rozhodne. Na to je stanoven časový interval, během kterého systém schvaluje/odmítá žádost. V případě schválení systém připravuje nutné dokumenty a čeká na konečné řešení uživatele.

UC3: Zkontrolovat stav žádosti
Uživatel zkontroluje aktuální stav žádosti.

UC4: Schválit žádost
Systém na základě analýzy vyplněných dokumentů a údajů uživatele schvaluje žádost a mění stav žádosti na „odmítnutá“.

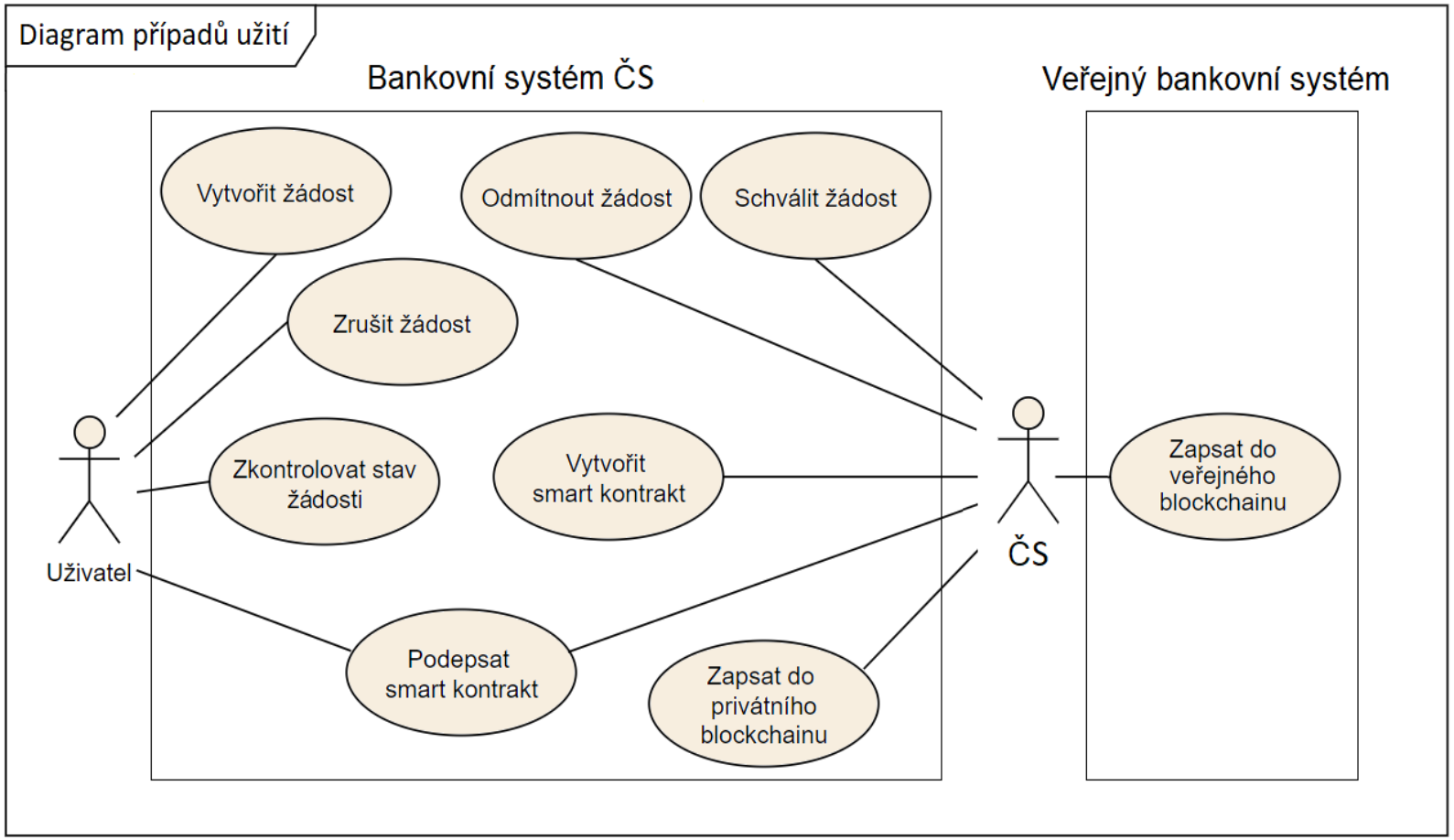
UC5: Odmítnout žádost
Systém na základě analýzy vyplněných dokumentů a údajů uživatele schvaluje žádost a mění stav žádosti na „schválená“.

UC6: Vytvořit smart kontrakt
Systém připravuje smart kontrakt pro podepisování mezi uživatelem a bankou. Takový smart kontrakt zahrnuje v sobě nutné údaje: jméno a příjmení uživatele, datum splatnosti úvěru, sankce za porušení, atd.

UC7: Podepsat smart kontrakt
Uživatel a banka podpisují smart kontrakt digitálním podpisem.

UC8: Zapsat do privátního blockchainu
Systém vytváří nový blok s transakcí a přidává do privátního blockchainu banky.

UC9: Zapsat do veřejného blockchainu
Systém vytváří nový blok s transakcí a přidává do veřejného blockchainu mezi všemi bankami.



Obrázek 8.1: Diagram případů užití

Tabulka 8.1 znázorňuje přehledně mapování případů užití na funkční požadavky. Z tabulky je jasně vidět, že každý z případů užití pokrývá minimálně jeden funkční požadavek.

	Případy užití								
Požadavky	UC1	UC2	UC3	UC4	UC5	UC6	UC7	UC8	UC9
F1	+								
F2		+							
F3			+						
F4				+	+				
F5						+			
F6							+		
F7								+	
F8									+

Tabulka 8.1: Pokrytí funkčních požadavků případy užití

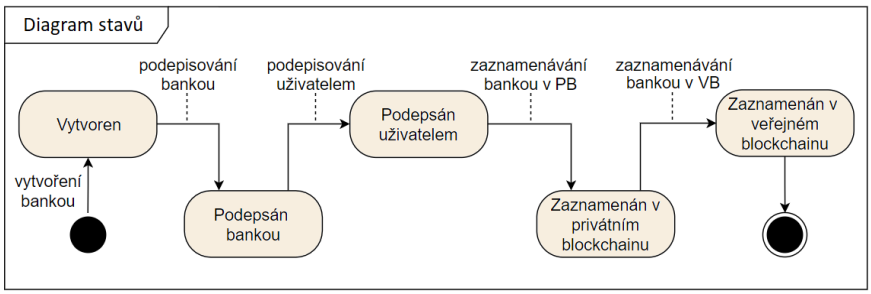
8.3 Diagram aktivit

Diagram aktivit je typem diagramu, který přesně popisuje chování celého systému nebo části systému. Takový diagram znázorňuje tok procesů dosažení určitých výsledků.

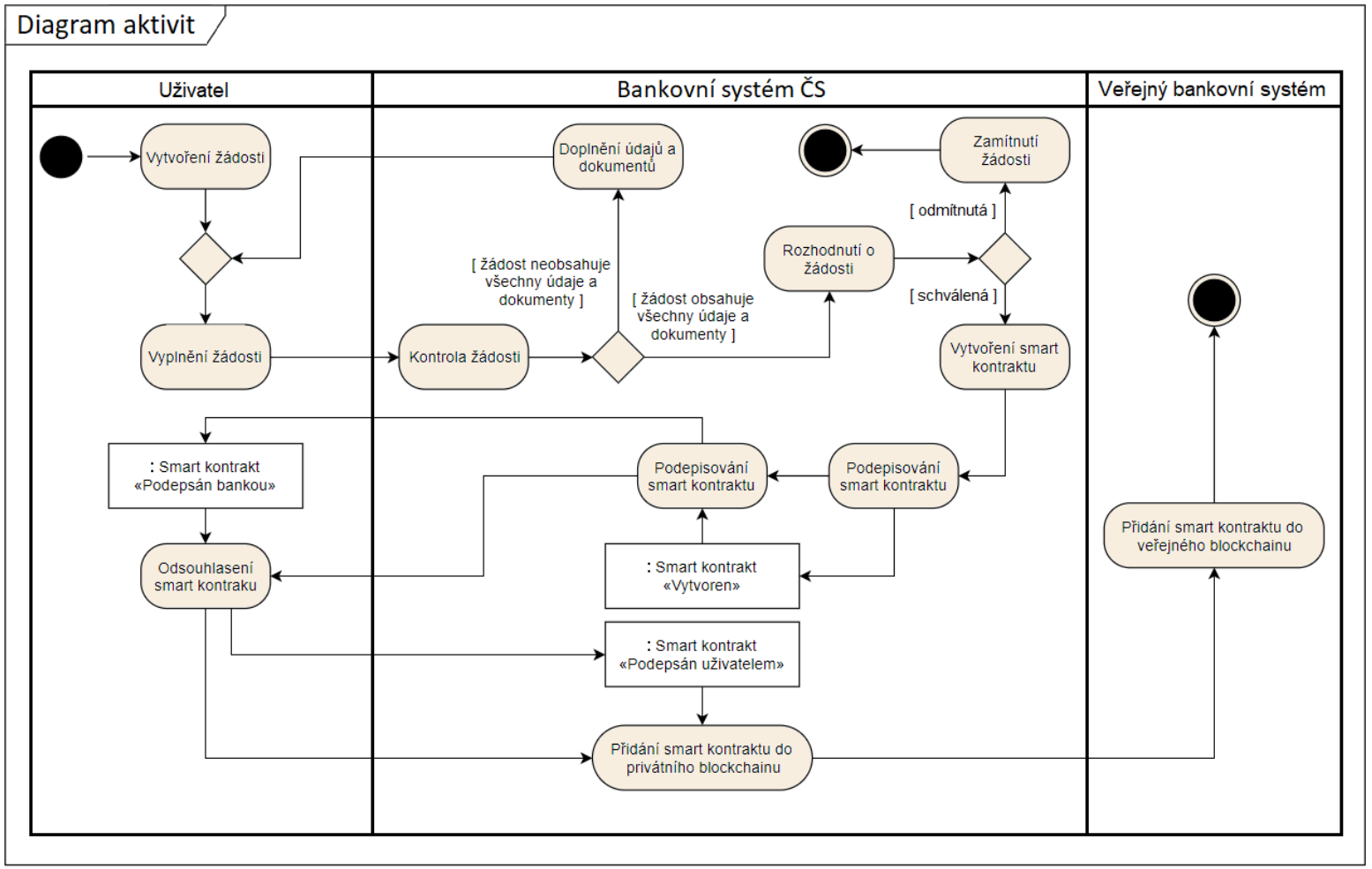
Na základě stanovených funkčních požadavků a diagramů případů užití je sestaven diagram aktivit, popisující tok procesů poskytnutí úvěru bankou od doby podání žádosti do momentu zaznamenávání transakcí ve veřejném bankovním blockchainu. Diagram aktivit je znázorněn na obrázku 8.3.

8.4 Diagram stavů

Stavový diagram, znázorněný na obrázku 8.2, vyjadřuje stavy smart kontraktu a přechody mezi těmito stavy.



Obrázek 8.2: Diagram stavů smart kontraktu



Obrázek 8.3: Diagram aktivit

8.5 Diagram nasazení

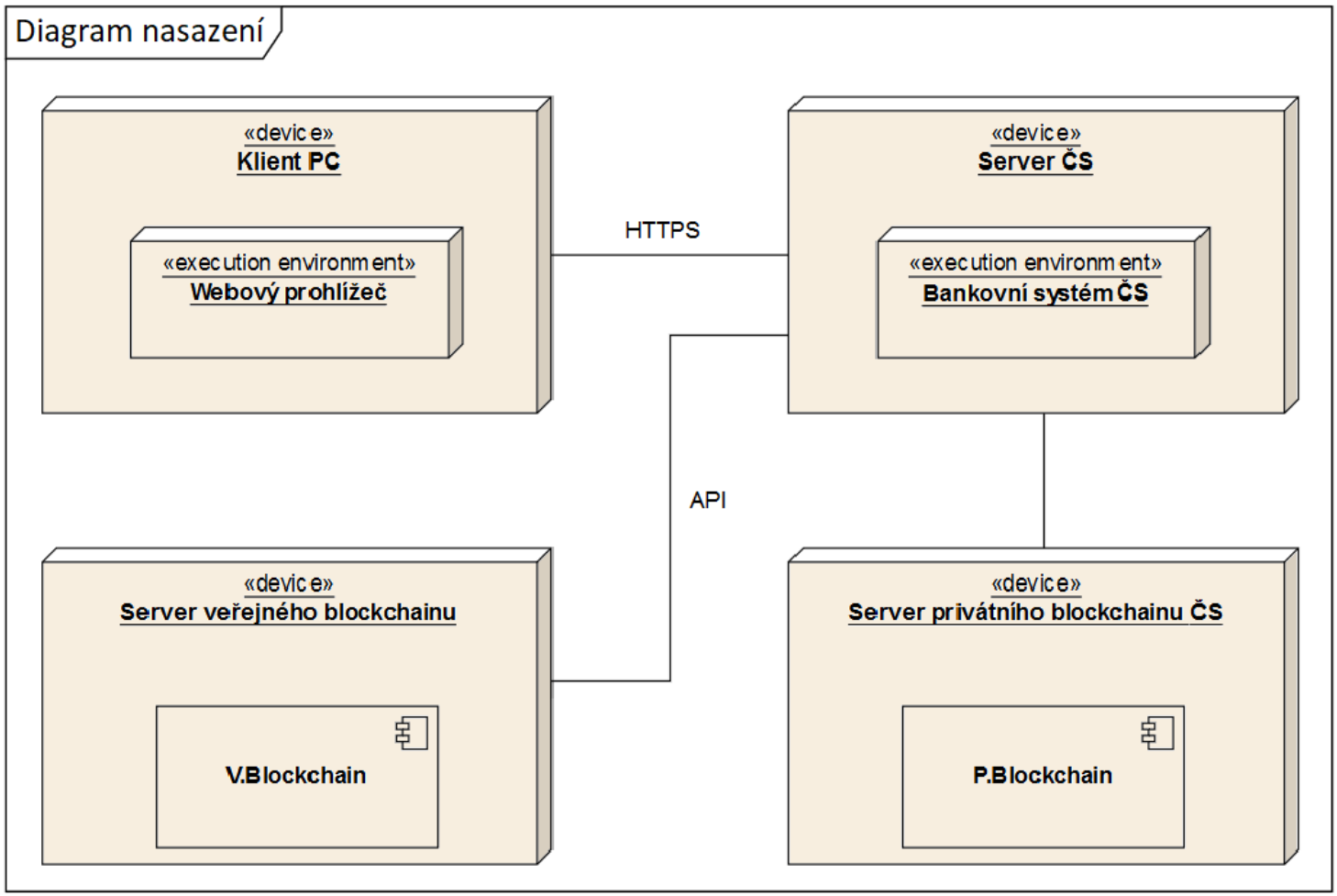
Diagram nasazení (znázorněným na obrázku 8.4) ukazuje specifikaci fyzické architektury systému, která je rozdělena na čtyři části:

KlientPC
: Pomocí daného zařízení a na něm instalovaného webového prohlížeče uživatel pracuje na vyplnění žádosti. Dané zařízení komunikuje se serverovou částí bankovního systému České spořitelny, a.s. přes zabezpečený protokol HTTPS zajišťující autentizaci, důvěrnost přenášených dat a jejich integritu.

Server ČS
: Serverová část bankovního systému České spořitelny, a.s. je zodpovědná za zpracování podaných žádostí. Kontroluje, schvaluje a odmítá žádosti. Hlavním cílem tento serverové části je generování smart kontraktů pro další podepsání bankou a uživatelem.

Server privátního bankovního blockchainu
: Tento server pracuje na přidávání podepsaných smart kontraktů do interního privátního blockchainu bankovního systému České spořitelny, a.s. Server je odolný proti poruchám a má co nejnovější zabezpečení.

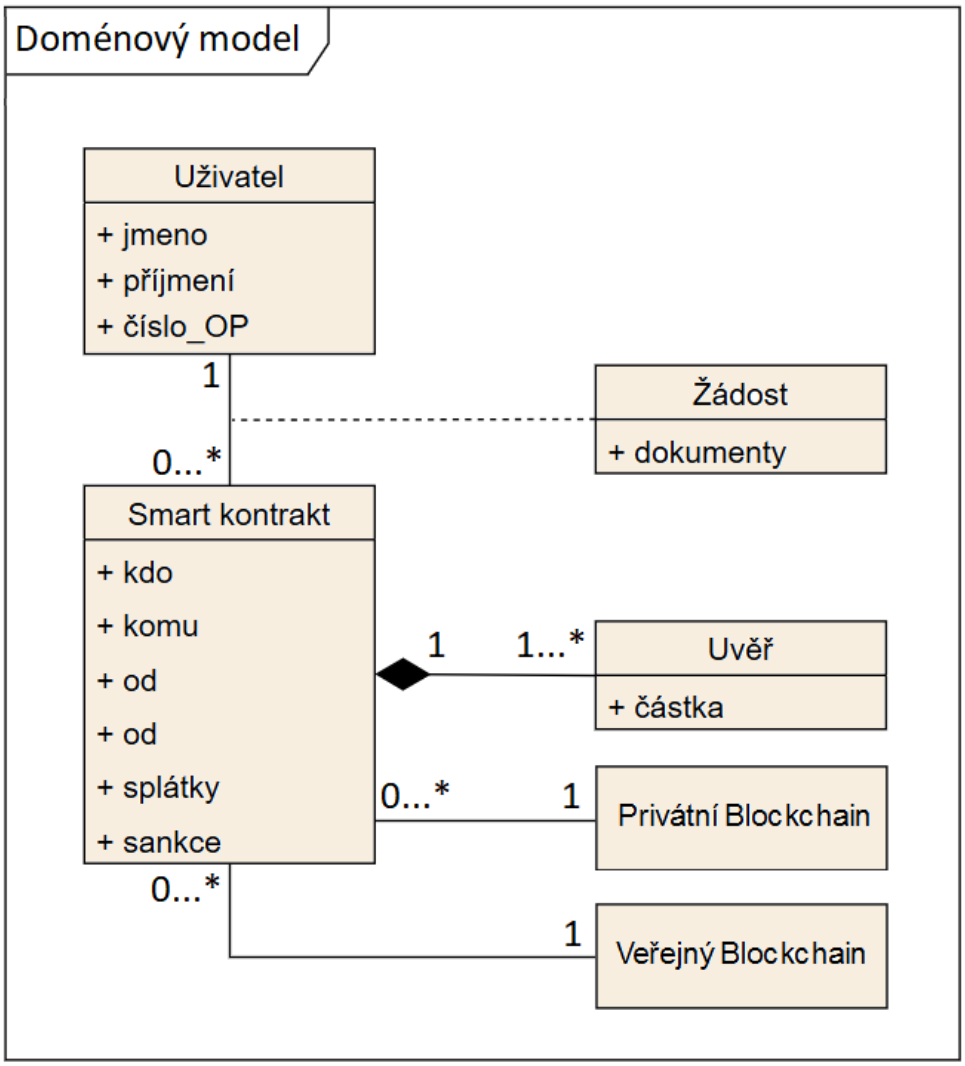
Server veřejného bankovního blockchainu
: Tento server pracuje na přidávání podepsaných smart kontraktů jakékoli banky do veřejného blockchainu. Vzhledem k tomu, že takový server je zcela veřejný, nikdo nemůže mít k němu přístup napřímo a server České spořitelny, a.s. se s ním musí kontaktovat přes API.



Obrázek 8.4: Diagram nasazení

8.6 Doménový model

Doménový model (obrázek 8.5) představuje pohled na modelovaný systém. Na základě stanovených funkčních požadavků a diagramů případů užití je sestaven doménový model, úkolem kterého je znázornit typy objektů v systému a jejich vztahy [20].



Obrázek 8.5: Doménový model

8.7 Volba implementačního jazyka

Pro takový velký systém je potřeba zajistit rychlost, výkonnost a co nejdůležitější – bezpečnost práce systému. Podle toho je vybrán vhodný implementační jazyk.

C++ – jeden z nejstarších jazyků, kterému se podařilo zachovat svůj význam až do dneška. Je to vysoce kvalitní multiparadigmatický programovací jazyk, který může být použit k vytváření složitých aplikací bez nadměrného zatížení paměti nebo výkonu zařízení. Díky efektivnímu řízení paměti a výkonu C++ umožňuje současně komunikaci více uzlům. Z hlediska maximální bezpečnostní politiky, vytváření a podepsání smart kontraktů v takovém systému je důvěryhodné, což je hlavní myšlenkou technologie blockchain, podle které by uživatelé v síti měli možnost rychlé simultánní interakce.

Závěr

V rámci této práce byla provedena analýza principů a mechanismů fungování technologie blockchain s obecného a technického hlediska. Byla analyzována bezpečnost a dopady na ochranu soukromí uživatelů, a posouzeny možnosti využití technologie blockchain soukromými firmami, finančními a státními institucemi. Dále v práci byla provedena analýza existujících řešení a analýza požadavků na bankovní systém České spořitelny, a.s., na jejichž základě pomocí postupů softwarového inženýrství byly stanoveny případy užití a navržen prototyp systému s využitím blockchainu pro poskytnutí bankovního úvěru.

Na základě analýzy bylo zjištěno, že technologie blockchain již není nová, ale pro většinu lidí je prakticky neznámá. Vzhledem k tomu, že mechanismus fungování je univerzální a potenciál dané technologie je zcela neomezený, blockchain může být použit nejen pro práci s kryptoměnami, ale také v jakékoli oblasti života společnosti.

Z dlouhodobého hlediska taková technologie poskytne ještě více možností a rozšíří hranice v oblasti obchodu, služeb, automatizace a zároveň přenese kontrolu na lidi, nikoli na centrální orgány. Ve skutečnosti se jedná o nový krok v ekonomickém rozvoji lidstva a lze s jistotou říct, že technologie blockchain radikálně mění téměř všechna odvětví a má velkou budoucnost.

Literatura

[1] Adaptic: *Databáze ©2005-2019* [online]. November 2018, [cit. 2019-04-22]. Dostupné z: https://www.adaptic.cz/znalosti/slovnicek/databaze/

[2] Finex: *Co je blockchain a jak on funguje? ©2014-2019* [online]. November 2018, [cit. 2019-04-22]. Dostupné z: https://finex.cz/blockchain/

[3] Coindesk: *What is Blockchain Technology? ©2019* [online]. April 2019, [cit. 2019-04-22]. Dostupné z: https://www.coindesk.com/information/what-is-blockchain-technology

[4] Antonopoulos, A. M.: *Mastering Bitcoin: Programming the open blockchain ©2019* [online]. 2017, [cit. 2019-04-22]. Dostupné z: https://bitcoinbook.info/wp-content/translations/cs/book.pdf

[5] Mining-Cryptocurrency: *Co je to Blockchain?©2017 – 2019* [online]. January 2018, [cit. 2019-05-11]. Dostupné z: https://mining-cryptocurrency.ru/blockchain/

[6] HybridTech: *Blockchain: řízení sítí, ověření podpisu ©2006 – 2019* [online]. January 2018, [cit. 2019-04-22]. Dostupné z: https://habr.com/ru/post/348020/

[7] ProfitGid: *Privátní a veřejný blockchain ©2019* [online]. [cit. 2019-05-11]. Dostupné z: https://profitgid.ru/raznica-mezhdu-publichnymi-i-privatnymi-blokchejnami.html

[8] Ihodl: *Proof-of-Work: jak to funguje? ©2019* [online]. [cit. 2019-04-26]. Dostupné z: https://ru.ihodl.com/tutorials/2018-01-23/proof-work-kak-eto-rabotaet/

[9] Ihodl: *Proof-of-Stake: jak to funguje? ©2019* [online]. [cit. 2019-04-26]. Dostupné z: https://ru.ihodl.com/tutorials/2018-07-06/proof-stake-kak-eto-rabotaet/

[10] HybridTech: *Blockchain: vlastnosti, struktura, digitální podpis ©2006 – 2019* [online]. January 2018, [cit. 2019-04-22]. Dostupné z: https://habr.com/ru/post/348014/

[11] Ihodl: *5 výhod blockchainu ©2019* [online]. [cit. 2019-05-11]. Dostupné z: https://ru.ihodl.com/investment/2017-12-13/5-preimushestv-blokchejna-i-odna-lovushka-dlya-investora/

[12] Cryptor: *Hlavní problémy implementace technologie blockchain ©2019* [online]. [cit. 2019-04-23]. Dostupné z: https://cryptor.net/bitkoin-dlya-chaynikov/osnovnye-problemy-povsednevnogo-vnedreniya-blokcheyn-tehnologii

[13] Xakep: *Silk Road fail story ©2019* [online]. [cit. 2019-05-11]. Dostupné z: https://xakep.ru/2014/08/13/silkroad-fail-story/

[14] Crypto-Obzor: *Příklady využití technologie Blockchain v zemědělství ©2019* [online]. [cit. 2019-04-24]. Dostupné z: http://crypto-obzor.ru

[15] Decenter: *Oblasti využití blockchain ©2019* [online]. [cit. 2019-04-24]. Dostupné z: https://decenter.org/ru/primenenie-blokcheina

[16] Coinspot: *Oblasti využití smart kontraktu ©2013-2019* [online]. [cit. 2019-05-15]. Dostupné z: https://coinspot.io/beginners/chto-takoe-smart-kontrakt-prostymi-slovami-kak-rabotaet-i-gde-primenyaetsya/

[17] Prostocoin: *Co je to Smart Contract ©2019* [online]. [cit. 2019-05-15]. Dostupné z: https://prostocoin.com/blog/smart-contract

[18] PMConsulting: *Funkční požadavky ©2019* [online]. [cit. 2019-05-05]. Dostupné z: https://www.pmconsulting.cz/slovnikovy-pojem/funkcni-pozadavky/

[19] PMConsulting: *Nefunkční požadavky ©2019* [online]. [cit. 2019-05-05]. Dostupné z: https://www.pmconsulting.cz/slovnikovy-pojem/nefunkcni-pozadavky/

[20] Rejnková, P.: *Diagram tříd ©2009* [online]. [cit. 2019-05-08]. Dostupné z: http://uml.czweb.org/diagram_trid.htm

Příloha A

Seznam použitých zkratek

P2P Peer-to-Peer

DoS Denial-of-Service

PoW Proof-of-Work

PoS Proof-of-Stake

SHA512 Secure Hash Algorithm 512

HTTPS Hypertext Transfer Protocol Secure

API Application Programming Interface