FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Název:	Možnosti komerčního využití technologie blockchain - případová studie poskytnutí úvěru
Student:	Vladislav Khomchenko
Vedoucí:	Ing. Michal Valenta, Ph.D.
Studijní program:	Informatika
Studijní obor:	Webové a softwarové inženýrství
Katedra:	Katedra softwarového inženýrství
Platnost zadání:	Do konce zimního semestru 2020/21

Pokyny pro vypracování

1. Popište principy technologie blockchain, analyzujte bezpečnost a dopady na ochranu soukromí uživatelů.
2. Analyzujte možnosti využití technologie blockchain soukromými firmami, finančními a státními institucemi.
3. Pro zvolený případ užití - poskytnutí úvěru bankou - rozpracujte architekturu a aktéry.
4. Vypracujte rešerši technologií pro implementaci zvoleného případu užití.
5. Na zvolené technologii rozpracujte detailně návrh implementace včetně odhadu pracnosti a náročnosti řešení.

Pro dokumentaci a návrh použijte vhodné nástroje a postupy softwarového inženýrství. Očekávaným výstupem práce je návrh, který by následně mohl být implementován.

Seznam odborné literatury

Dodá vedoucí práce.

Ing. Michal Valenta, Ph.D.
vedoucí katedry

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

V Praze dne 1. července 2019

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Možnosti komerčního využití technologie blockchain - případová studie poskytnutí úvěru

Vladislav Khomchenko

Katedra softwarového inženýrství
Vedoucí práce: Ing. Michal Valenta, Ph.D.

9. srpna 2019

Poděkování

Chtěl bych poděkovat Ing. Michalu Valentovi, Ph.D. 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 9. srpna 2019 ……

Odkaz na tuto práci

Khomchenko, Vladislav. *Možnosti komerčního využití technologie blockchain - případová studie poskytnutí úvěru.* 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 banky s využitím blockchainu pro poskytnutí bankovního úvěru.

Klíčová slova technologie blockchain, smart kontrakt, banka, poskytnutí úvěru, návrh systému

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 a bank system was developed using the blockchain to provide a bank loan.

Keywords blockchain technology, smart contract, bank, loan provision, system design

Obsah

Seznam obrázků

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 banky 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. V závěru teoretické části jsou posouzeny výhody, nevýhody a možnosti využití technologie blockchain soukromými firmami, finančními a státními institucemi.

Praktická část práce analyzuje existující řešení, stanoví uživatelské požadavky na systém a rozpracovává jeden z případů užití blockchainu v bankovnictví. Jako ilustrativní příklad je využitý systém poskytnutí úvěru v rámci banky. Hlavním cílem praktické části práce je návrh implementace 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.

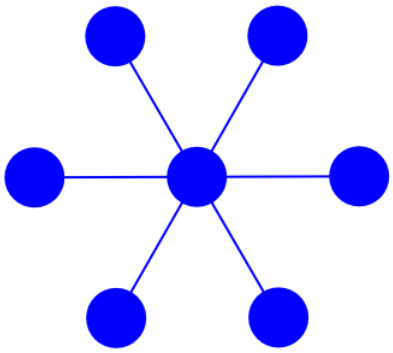
2.2 Typy databází

Podle zdroje [2], z hlediska architektury se databáze dělí do následujících základních typů:

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

2.2.1 Centralizovaná databáze

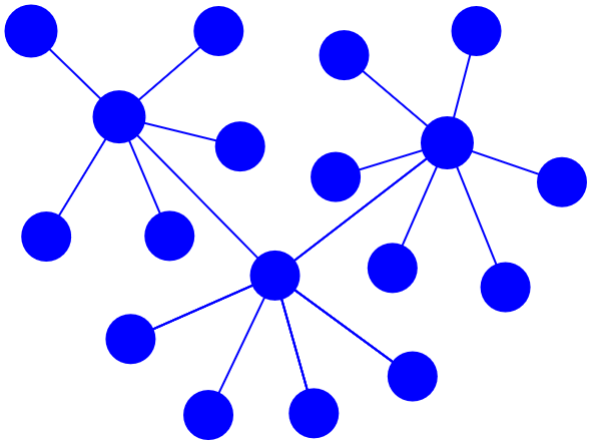
Centralizovaná databáze (obrázek 2.1) se vyznačuje tím, že je celá umístěná na centrálním počítači, kde uživatelé (klienti) přistupují k informacím prostřednictvím svých počítačů. Správa databáze se provádí centrálně. Počítač se zdroji se nazývá server, počítač, který přistupuje k serveru pro data, se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



Obrázek 2.1: Centralizovaná databáze

2.2.2 Decentralizovaná databáze

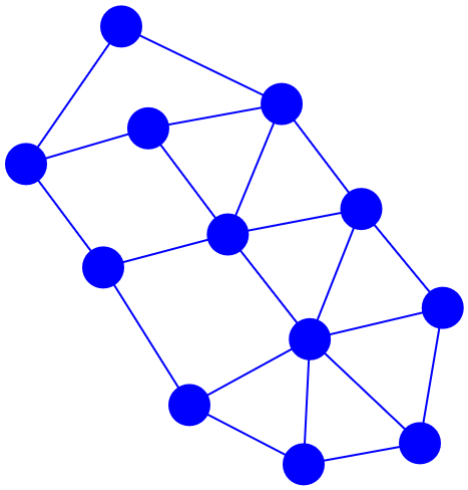
Decentralizovaná databáze (obrázek 2.2) znamená, že tato databáze nemá žádné hlavní centrální úložiště. Data nejsou přenášena z jednoho místa, ale existuje více hlavních serverů. Servery jsou navzájem propojeny. Výpadek jednoho serveru nemá jakýkoli vliv na další fungování sítě.



Obrázek 2.2: Decentralizovaná databáze

2.2.3 Distribuovaná databáze

Distribuovaná databáze (obrázek 2.3) je zcela soběstačná, nemá žádné centrální úložiště a 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.



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).“

Kapitola 3

Architektura blockchainu

3.1 Technologie blockchain

Podle informace ze zdrojů [3], [4] a [5] vychází, že 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 účtů. Jde o neustále se rozšiřující chronologický řetězec záznamů, veřejných transakcí shlukovaných v blocích.

„Každý blok v blockchainu je identifikován hashem, vytvořeným kryptografickým hashovacím 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 „hash předchozího bloku“ v hlavičce bloku. Jinými slovy, každý blok obsahuje hash svého rodiče uvnitř své hlavičky. Posloupnost hashů spojuje každý blok se svým rodičem vytváří řetěz jdoucí zpátky k prvnímu bloku, který byl kdy vytvořen, známému jako základní blok (genesis).“ [4]

„Položka „hash předchozího bloku“ je uvnitř hlavičky bloků a proto ovlivňuje hash aktuálního bloku. Vlastní identita dítěte se změní, pokud se změní identita rodiče. Pokud je rodič změněn v jakémkoliv směru, hash rodiče se změní. Změna hashe rodiče vyžaduje změnu v odkazu „hash předchozího bloku“ u dítěte. Tento krok způsobí změnu hashe 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.

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.

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.

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.

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.

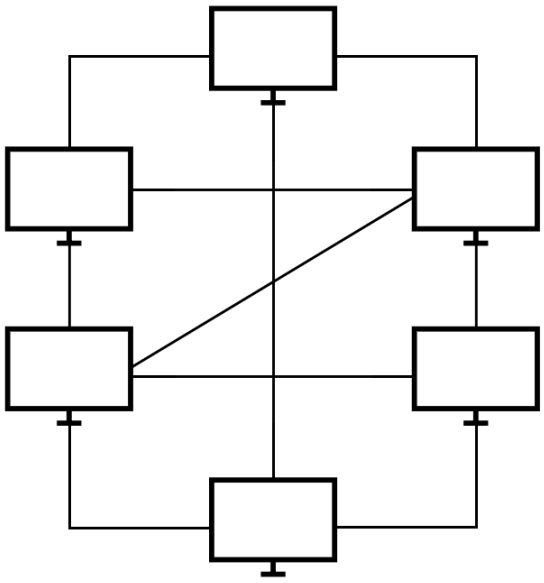
3.2 Síť Peer-to-Peer (P2P)

Ze zdroje [6] vychází informace, že 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.

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.

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.



Obrázek 3.1: Síť Peer-to-Peer (P2P)

3.3 Typy blockchainu

Podle zdroje [7] 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 vlastnictví (*Proof-of-Stake*).

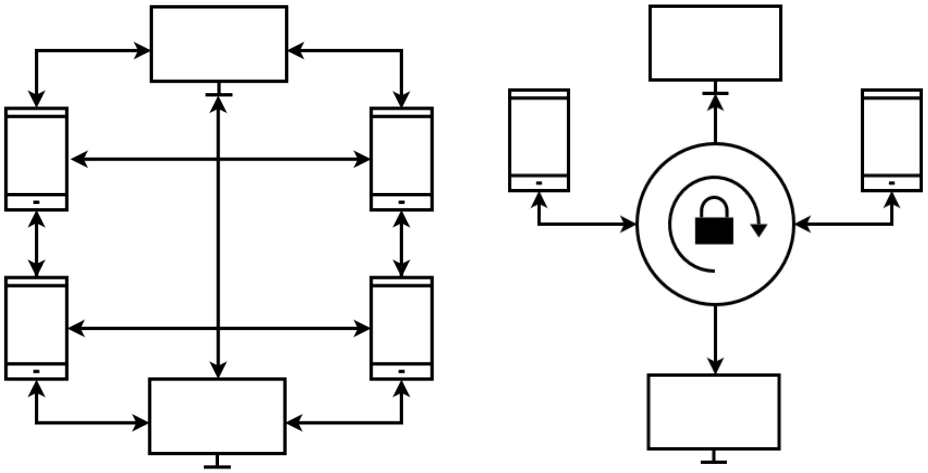
3.3.2 Privátní blockchain

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.

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.

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.



Obrázek 3.2: Veřejný (vlevo) a privátní (vpravo) blockchain

Kde na obrázku 3.2 zámek označuje omezení přístupových práv pro privátní blockchain informačním systémem organizace.

3.4 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 hashe může trvat hodiny, dny i týdny. V jiných

typech blockchainu tyto lze hashe vypočítat předem, proto cílem těžaře není extrakce bloků, ale poskytování svého pevného disku pro ukládání řetězců.

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.

K tomu existují různé metody. Podle zdrojů [8] a [9] 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.

Jeho hlavním účelem je chránit server před spamem a DDos útoky prostřednictvím přidání speciálního matematického úkolu, jehož řešení vyžaduje určité množství času a prostředků během vytváření nového bloku. Zároveň server stráví mnohem méně času kontrolou správnosti pořadí bloků a transakcí uvnitř. Mechanismus PoW je navržen speciálně pro výpočetní techniku.

3.5.1.1 Co je to matematický úkol

Je to jeden z úkolů, vyžadující značnou výpočetní sílu. Existuje mnoho takových úkolů:

1. hashovací funkce nebo pokus o nalezení vstupních dat;
2. výpočet hodnot hashovací funkce někdy v určitém pořadí;
3. rozklad celého čísla na součin menších čísel.

3.5.1.2 Jak funguje PoW

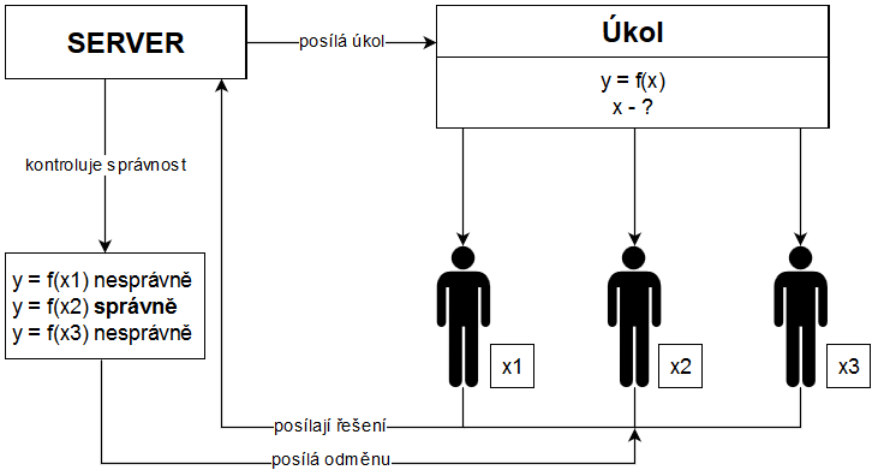
Přesnost a rychlost blockchainu závisí na tomto mechanismu. Problém by zároveň neměl být příliš komplikovaný – v tomto případě generování bloku bude trvat delší dobu, což znamená, že sada neúplných transakcí bude „viset“ na síti.

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 DDoS.

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.

3.5.1.3 Jak je implementován PoW v blockchainu

Těžaři řeší úkol, 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.



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 mnoha kryptoměnách podobných bitcoinu.

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.

3.5.1.5 PoW a problém zvaný „51% útok“

„51% útok“ neboli útok většiny je možný v situaci, kdy uživatel nebo skupina uživatelů kontrolují většinu kapacity výpočetního výkonu sítě – to jim dává možnost řídit události, ke kterým dochází v síti. Mohou tedy monopolizovat

vytváření nových bloků, rušit a přijímat všechny transakce, protože mají moc zabránit ostatním těžařům v dokončení bloků. Naštěstí „51% útok“ je spíše teoretický. Problém je v tom, že mít takové procento je v praxi nemožné a ani největší těžařské farmy nedosahují ani několika desítek procent výpočetního výkonu celé sítě. Je důležité si daný problém pamatovat proto, že výpočetní síla počítačů se neustále každý rok rychle zvyšuje. [10]

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 kryptoměny má těžař, tím vyšší je jeho těžební síla.

První kryptoměnou, která využila takový algoritmus, byl Peercoin, následovaný Nxt, BlackCoinem a ShadowCoinem. Tento algoritmus byl vyvinut jako alternativa k důkazu práce (PoW). Důkaz o vlastnictví (PoS) byl navržen tak, aby vyřešil problémy PoW. Těžař je nyní omezen svým podílem na celkové zásobě v síti. Například těžař, který vlastní 3 % dostupných kryptoměn, může teoreticky zkontrolovat pouze 3 % bloků.

Kapitola 4

Komponenty blockchainu

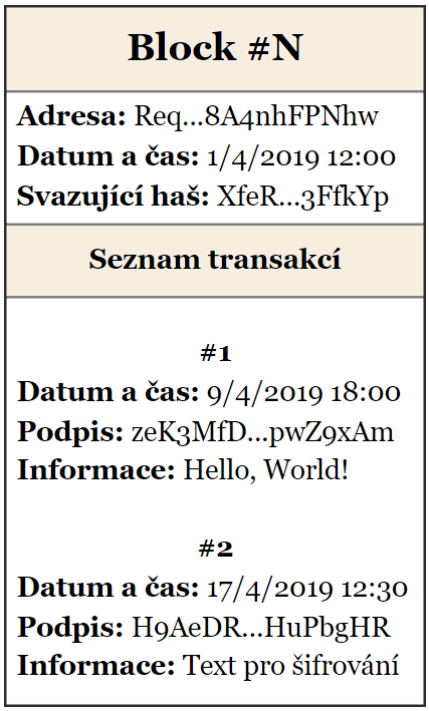
Následná informace v kapitole vychází ze zdrojů [6], [11] a [12].

4.1 Struktura bloku

Existuje spousta množství implementace technologii blockchain jako Bitcoin, Ethereum, EOS, Monero apod. Obecně se každý blok v blockchainu (obrázek 4.1) skládá z jednotlivých částí:

- **Adresa bloku**
  Je generována během vytváření nového bloku.
- **Datum a čas**
  Okamžik vytvoření bloku (transakce má také datum a čas vytvoření).
- **Svazující hash**
  Vypočítá se pomocí hashovacího algoritmu z adresy předchozího bloku a součtu hashe 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.



Obrázek 4.1: Možná struktura bloku

4.2 Digitální podpis

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

Digitální podpis – jedná se o 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 hashovacích funkcí. Jedním z takových algoritmů může být RSA.

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!

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.

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.

Obrázek 4.2: Digitální podpis

4.2.2 Algoritmus podepisování informací

Vytvoření podpisu vyžaduje:

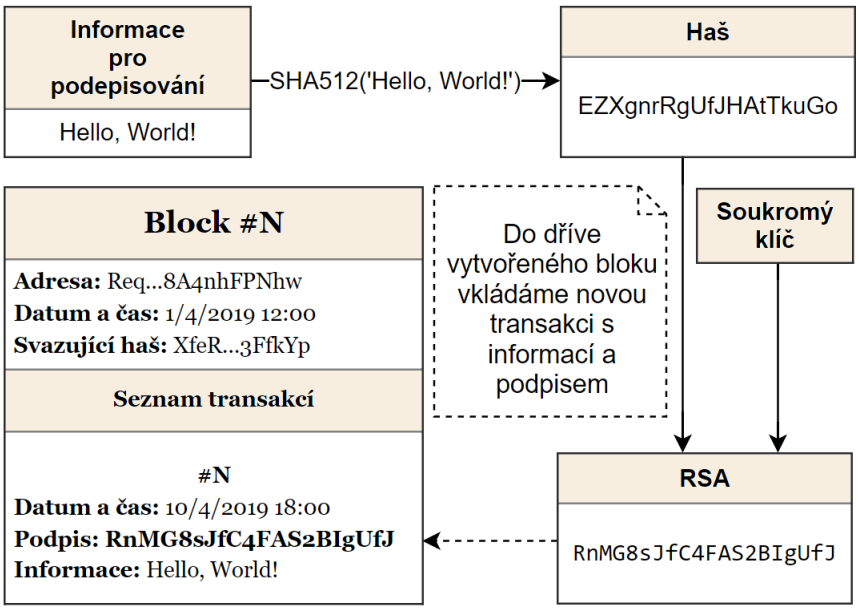
- asymetrický šifrovací algoritmus (například RSA);
- hashovací funkce (například SHA512);
- informace pro podepisování.

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 hash podepsaných dat místo originálních dat. Hash se získává pomocí hashovací funkcí, které přijímají určité informace jako vstup a vracejí hash určité délky. Hashování 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.

Tedy se digitální podpis neaplikuje přímo na samotný dokument, ale na jeho hash. Hashovací funkce není součástí algoritmu digitálního podpisu, takže v systému lze použít jakoukoli spolehlivou hashovací funkci.

Algoritmus (obrázek 4.3) lze rozdělit na fáze:

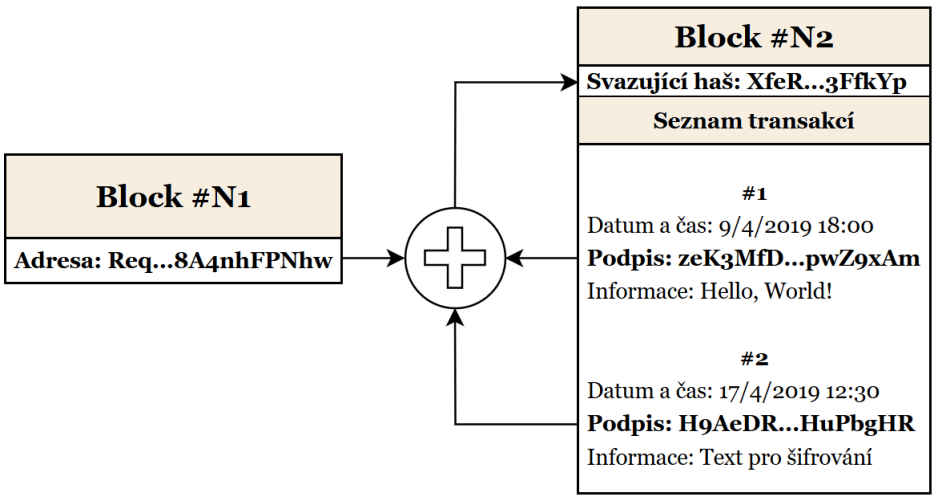
1. generování veřejného a soukromého klíče;
2. hashování informací pomocí SHA512;
3. pomocí RSA se dostává na výstupu podpis.



Obrázek 4.3: Algoritmus podepisování informací

4.3 Svazující hash

Svazující hash bloku (obrázek 4.4) se přepočítá při každém přidání nové transakce. Uvažuje se sčítáním všech transakčních hashů aktuálního bloku a adresy předchozího bloku. Navíc pro svazující hash **1. bloku** se používá hash **0. bloku** (*genesis*), který je generován náhodně nebo ručně.



Obrázek 4.4: Příklad svazujícího hashe

Jedná se o hash, 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 hash byl založen na adrese, kterou vetřelec chce nahradit nebo odstranit.

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

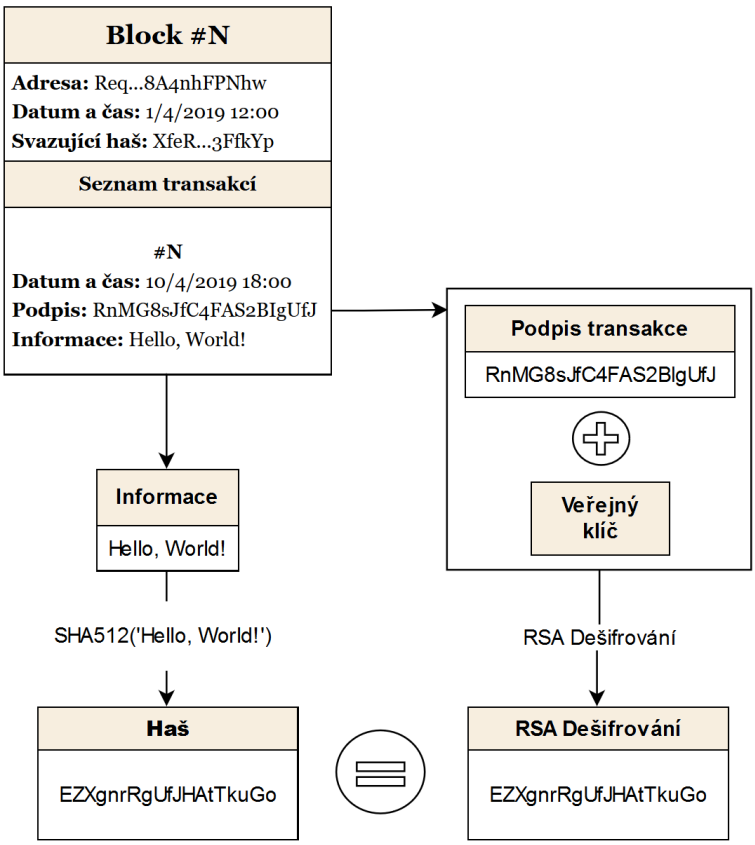
4.4 Ověřování dat blockchainu

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.

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 hashe z informace;
3. dešifrování podpisů pomocí veřejného klíče;
4. porovnání hashe získaného v 2. kroku s hashem, získaným z dekódovaného podpisu v 3. kroku;
5. při neshodě hashů jsou data falešná a transakce je odmítnuta a není přidána do bloku.



Obrázek 4.5: Algoritmus ověřování transakcí

4.4.2 Algoritmus kontroly bloku

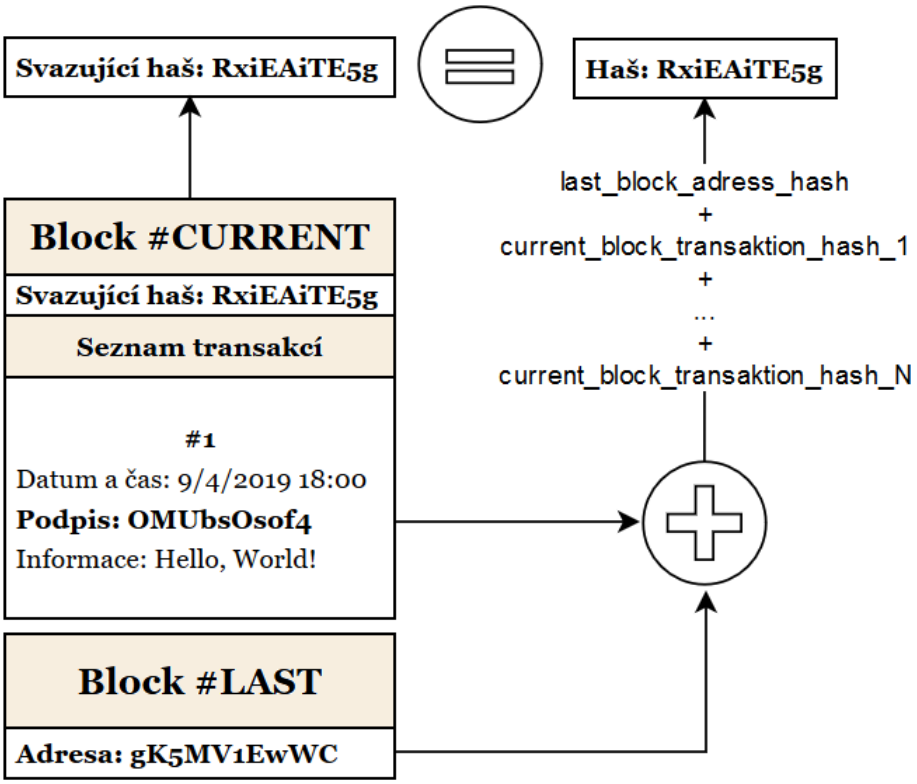
Algoritmus kontroly nového bloku (obrázek 4.6) lze rozdělit do kroků:

1. přijetí adresy posledního přijatého bloku (aktuální blok ještě nebyl přijat a není poslední) a seznam transakcí aktuálního bloku;

2. výpočet hashe SHA512;

3. porovnání výsledného hashe s hashem (spojovacím hashem) 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

4.5 Smart kontrakt

Smart kontrakt – elektronický protokol napsaný pomocí počítačového kódu. Jeho účelem je předávat informace a zajišťovat plnění smluvních podmínek oběma stranami.

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.

4.5.1 Vlastnosti smart kontraktu

Smart kontrakty umožňují bezpečně vyměňovat peníze, akcie, majetek a další aktiva přímo bez účasti zprostředkovatelů. Aby bylo možné uzavřít jakoukoli smlouvu, 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 smlouvy v reálném životě se lidé musí obrátit na soud, znovu utrácet peníze na proces a dokázat nevinu. Při uzavírání těchto smluv nelze mluvit o důvěře účastníků smlouvy.

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).

4.5.2 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/výstupů smart kontraktu a vést k jakýmkoli činnostem mimo blockchain, v reálném nebo digitálním světě.

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.

Kapitola 5

Výhody a nevýhody blockchainu

Navzdory univerzálnosti blockchainu ve všech oblastech má každá technologie řadu výhod, ale i nevýhod. Podle informace, která vychází ze zdrojů [13], [14] a [15], jsou v dané kapitole popsány některé z nich.

5.1 Výhody technologie

5.1.1 Decentralizace

Jedním z hlavních důvodů přitažlivosti blockchainu je to, že technologie nezahrnuje centrální uzel sběru dat. Namísto spouštění datového centra a provádění všech transakcí přes tento uzel, blockchain skutečně umožňuje, aby jednotlivé transakce měly vlastní ověřování a autorizaci, aby se zajistilo, že jsou vzájemně propojeny. Informace o konkrétních blocích řetězce jsou rozptýleny 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.

5.1.2 Bezpečnost dat

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

5.1.3 Transparentnost

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.

5.2 Nevýhody technologie

5.2.1 Nadměrné 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 Škálovatelnost

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 3 až 5 hodin a maximálně 2 dny. Stojí za zmínku, že při zavedení tento čas nepřesáhl 10 minut.

5.2.3 Obrovské výdaje

Většina implementací blockchainu (Bitcoin, Ethereum, EOS, Monero apod.) využívá konsensuální algoritmus s důkazem práce neboli „Proof-of-Work“. Tento algoritmus má však z dlouhodobého hlediska poměrně velký problém. Komplexní výpočty vyžadují velký výpočetní výkon, z čehož vyplývá neustále rostoucí spotřeba elektřiny. V poslední době těžba bitcoinu a etherea spotřebuje 27krát a 8krát více energie, než kolik se spotřebuje celá síť VISA.

Kapitola 6

Existující využití blockchainu

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.

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.

Podle informace uvedené ze zdrojů [16] a [17] jsou v dané kapitole 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.

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.

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.

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.

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.

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.

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).

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Kapitola 7

Blockchain v bankovnictví

Bankovní služby jsou oblast, která zřejmě nejvíce využívá technologii blockchain. Co je to banka? Ze zdroj [18] je to organizace, která by měla plnit čtyři základní funkce: provádět převody, ukládat prostředky zákazníků, poskytovat úvěry a nabídnout klientům možnosti investování.

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.

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.

7.1 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.

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.

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.

7.2 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.

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.

7.3 Klasifikace smart kontraktů

V závislosti na stupni automatizace smart kontrakty mohou být:

1. plně automatizované;
2. s kopií na papíře;
3. většinou na papírových/elektronických nosičích, s některými částmi přenesenými do programového kódu.

Řešení založená na blockchainu jsou teprve v počátečním stadiu vývoje, takže v praxi dosud neexistují opravdu složité smart kontrakty. K dnešnímu dni drtivá většina smart kontraktů je 3. typu, kde jsou automatizovány pouze některé aspekty, včetně automatizace plateb.

Kapitola 8

Specifikace zadání práce

Po zkoumání základních principů a mechanismů fungování technologie blockchain se od dané kapitoly začíná rozpracovávat jeden z případů užití blockchainu v bankovnictví. Podle zadání práce jako ilustrativní příklad poslouží systém poskytnutí úvěru v rámci banky.

8.1 Všeobecný popis

Budoucí bankovní úvěrový systém by měl uživateli poskytnout funkcionalitu, pomocí které by uživatel mohl zahájit proces poskytnutí úvěru.

Zahájení tohoto procesu zavazuje k vyplnění povinných atributů vztahujících se k osobním údajům uživatele, jakož i k připojování nutných dokladů nezbytných pro rozhodnutí banky ohledně této žádosti.

V případě kladného rozhodnutí by systém měl mít možnost zaznamenat tuto skutečnost v blockchainu. Všechny postupy týkající se plateb a zpoždění v rámci jednoho úvěru musí být rovněž zaznamenány v blockchainu.

Tato funkcionalita by měla být použita pro sledování historie úvěrů poskytnutých uživateli, jakož i možnosti získání nezbytných informací úvěrů bez účasti třetí strany.

8.2 Analýza požadavků

Rozbor požadavků je důležitá část analýzy upřesňující fungování systému dle očekávání. V rámci analýzy se uvádí především přehled funkčních a nefunkčních požadavků.

8.2.1 Funkční požadavky

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

F1: Podání žádosti
Systém umožňuje uživateli podat žádost 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: Rozhodnutí o žádosti
Systém automatické analýzy rozhoduje o poskytnutí úvěru na základě údajů a dokumentů vyplněných uživatelem.

F5: Příprava elektronického dokumentu se smlouvou
Systém připravuje elektronický dokument se smlouvou pro podepisování mezi uživatelem a bankou.

F7: Podepisování elektronického dokumentu se smlouvou
Systém umožňuje uživateli a bance podepsat elektronický dokument se smlouvou zaručeným digitálním podpisem.

F8: Příprava smart kontraktu
Systém připravuje smart kontrakt pro podepisování mezi uživatelem a bankou.

F9: Podepisování smart kontraktu
Systém umožňuje uživateli a bance podepsat smart kontrakt podpisem.

8.2.2 Nefunkční požadavky

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

NF1: Blockchain
Systém by měl zaznamenávat historii úvěrů poskytnutých uživateli v blockchainu.

NF2: Poplatky
Systém by měl fungovat s minimálními poplatky pro uživatele, v nejlepším případě by poplatky měly být nulové.

NF3: Přístupnost
Systém musí být přístupný minimálně přes webové prohlížeče: Google Chrome, Mozilla Firefox, Safari a Opera.

NF4: Intuitivita
Systém musí být intuitivní a mít jednoduché prostředí na používání.

NF5: Zabezpečení
Systém musí zajistit, aby komunikace se serverovou částí byla šifrována a přenášena pomocí zabezpečených protokolů, protokol HTTP je striktně zakázán.

NF6: Stabilita
Systém by měl fungovat bez pádů, které by omezovaly možnosti jejího využití.

NF7: Přenosová schopnost
Systém by měl schopen poskytovat služby v jednom okamžiku co nejvíce uživatelům.

Kapitola 9

Návrh architektury systému

Následující kapitola se věnuje návrhu architektury budoucího systému poskytnutí úvěru. V úvodu se stanoví počáteční informace, které jsou nutné před podáním žádosti a zahájením procesu poskytnutí úvěru. V dalším kroku se je představeno samotné schéma architektury, která se skládá z několika komponent popisujících jejich úkol, komunikaci mezi komponentami, z pohledu funkčních částí systému, a hlavní toky dat mezi nimi. V závěru kapitoly je popsán tok procesů poskytnutí úvěru bankou od doby podání žádosti do momentu zaznamenávání transakce ve veřejném blockchainu.

9.1 Počáteční informace

Pro korektní zpracování procedury poskytnutí úvěru je potřeba, aby se každému uživateli v systému od začátku přiřazovala následující informace:

- Unikátní identifikátor uživatele v systému banky;
- Adresa uživatele v blockchainu;
- Adresa smart kontraktu používaného k vedení záznamu smluv spojených s uživatelem;
- Certifikát zaručeného digitálního podpisu uživatele.

9.2 Komponenty architektury

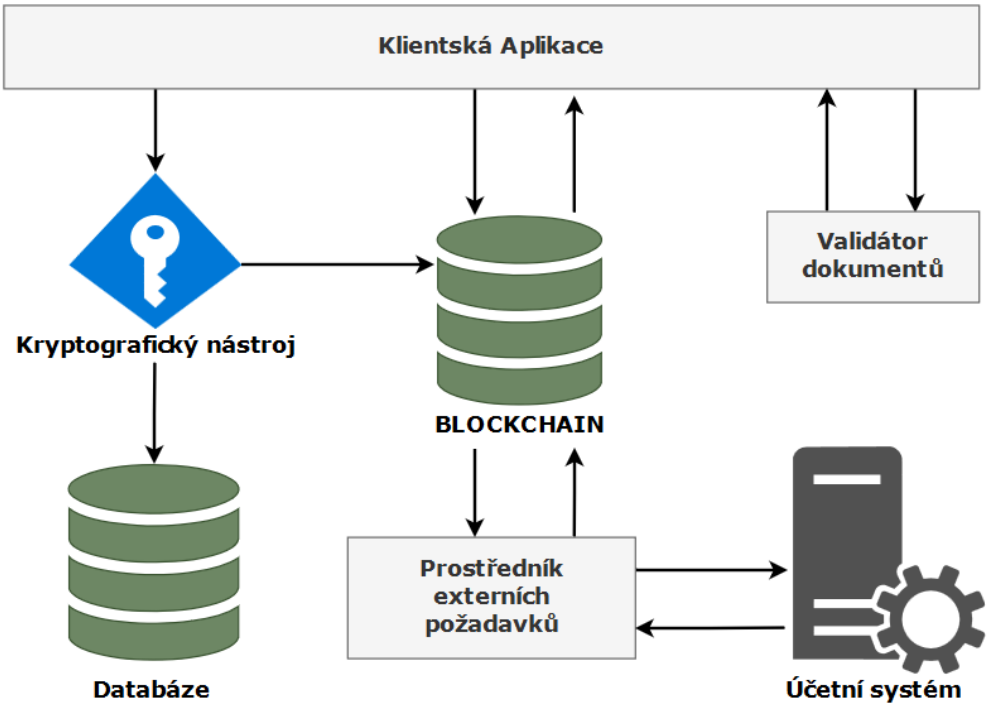
Z koncepce architektury systému vyplývá potřeba použití následujících funkčních složek:

- **Klientská aplikace** – hlavní nástroj uživatele během procedury poskytnutí úvěru;

- **Validátor dokumentů** – nástroj automatické kontroly vyplněných uživatelem dokumentů za účelem žádosti o poskytnutí úvěru;
- **Kryptografický nástroj** – prostředek zajištění šifrování dokumentů, zaručeného digitálního podpisu a časových razítek;
- **Databáze** – místo ukládání šifrovaných a podepsaných dokumentů;
- **Blockchain** – registr poskytující nejvyšší stupeň důvěryhodnosti transakcí a taktéž inteligentní prostředí provádění smart kontraktů;
- **Prostředník externích požadavků** – jednotka přístupu k účetním systémům banky a zpracování externích událostí;
- **Účetní systém** – sada standardních komponentů systému banky spojených se zpracováním plateb, převodů, splátek apod.

9.3 Koncepce architektury

Na obrázku (9.1) uvedeném níže je zobrazeno obecné schéma systému a hlavní toky dat mezi jeho komponenty.



Obrázek 9.1: Koncepce architektury systému

Během procedury poskytnutí úvěru fungují komponenty systému následujícím způsobem:

- Klientská aplikace slouží k zadání nutných informací týkajících se uživatele a procedury poskytnutí úvěru, vytvoření potřebných smart kontraktů a správě stavu smart kontraktů v manuálních krocích obchodního procesu. Manuální kroky obchodního procesu lze chápat jako kroky, při kterých se mění stav smart kontraktů z vnější strany bez použití jeho vnitřní logiky.
- Dokument se smlouvou o poskytnutí úvěru se podepisují pomocí kryptografického nástroje zaručeným digitálním podpisem uživatele a banky. Dokument se dále šifruje, ukládá se do interní databáze banky a je k dispozici pro dešifrování pouze účastníkům smlouvy. Nakonec se hash výchozího dokumentu přiřazuje ke smart kontraktu.
- Při zpracování transakcí může smart kontrakt použít informace od prostředníků externích požadavků. Pomocí čeho je možné kontrolovat datum přijetí transakce, uplynutí doby sjednání smlouvy, včasném splácení apod.
- Při přechodu do určitého stavu může smart kontrakt zaslat transakce prostředníkovi externích požadavků na očekávanou externí událost nebo příkaz k provedení externí akce. Jakmile dojde k externí události, prostředník zašle transakce s informacemi o události příslušnému smart kontraktu. Podle výsledků zpracování této transakce může smart kontrakt přejít do nového stavu nebo zůstat ve stejném až do doby další události.

9.4 Proces poskytnutí úvěru

Účastníci procesu:

- **Uživatel**
- **Systém**

Popis procesu:

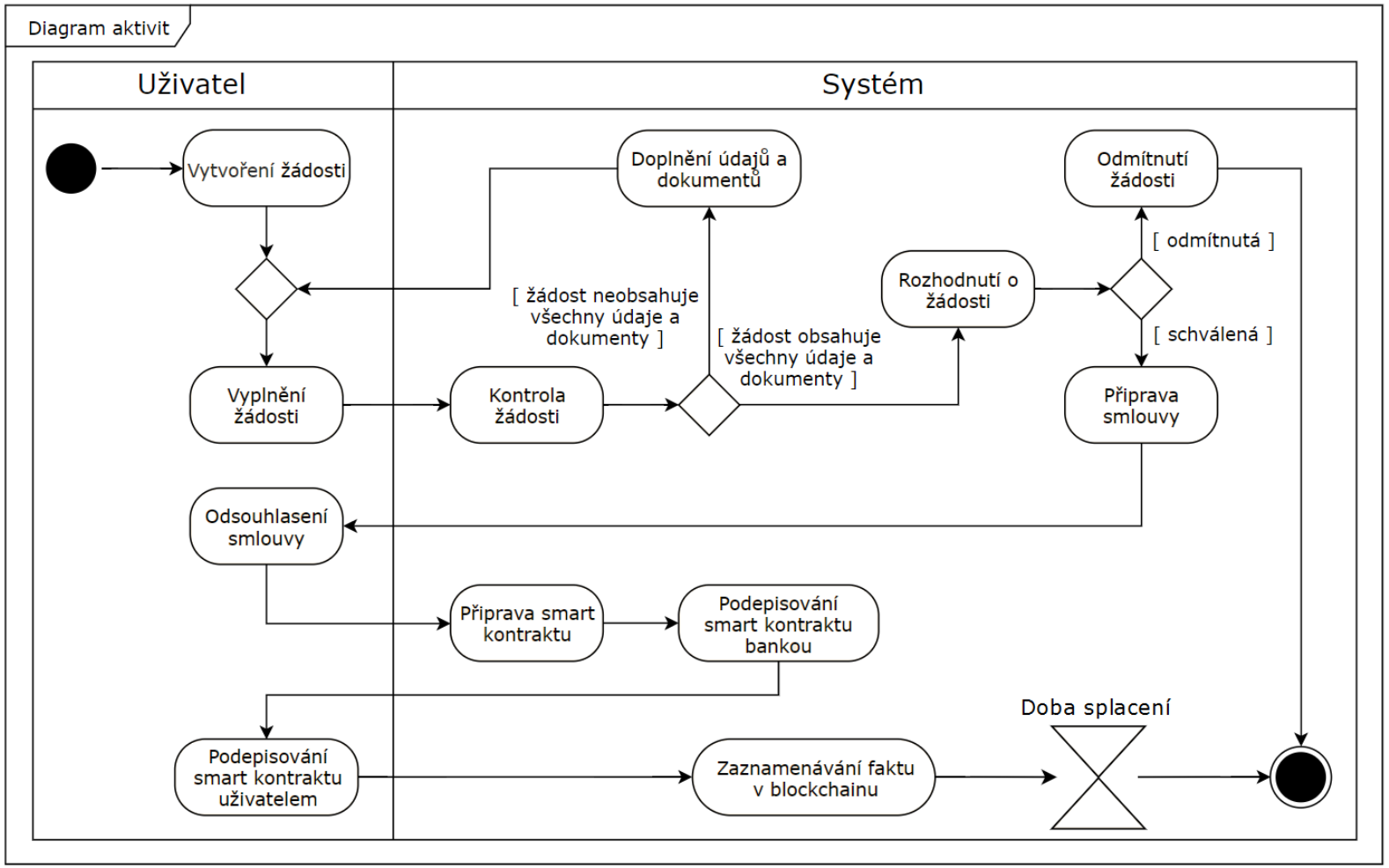
1. Uživatel podává žádost o poskytnutí úvěru, vyplní povinné atributy vztahující se k osobním údajům uživatele a připojuje nutné doklady. Následně žádost obdrží status „**New**“.
2. V případě rozhodnutí uživatele o zrušení žádosti status žádosti se nastaví na „**Cancelled**“.
3. Systém automaticky kontroluje žádost a informace poskytnuté uživatelem. V případě nejasností je žádost kontrolovaná pomocí odborníků.

- Pokud má systém jakékoli výhrady ohledně obsahu přiložených dokumentů, odmítá žádost a nastavuje jí stav „**Rejected**“.
- Pokud systém souhlasí s přijetím žádosti, nastavuje status žádosti na „**Confirmed**“.

4. Při nastavení žádosti na status „**Confirmed**“ systém připravuje elektronický dokument se smlouvou a nastavuje status žádosti na „**Released**“.
5. Při nastavení žádosti na status „**Released**“ systém automaticky umístí do fronty prostředníka externích požadavků dva požadavky:
   - Požadavek kontroly vypršení doby odsouhlasení smlouvy,
   - Požadavek čekání na odsouhlasení smlouvy.
6. Uživatel může, po prostudování elektronického dokumentu se smlouvou, smlouvu odmítnout. V takovém případě uživatel manuálně nastavuje stav související žádosti na „**Invalid**“, žádost je zrušena a další manipulace jsou nemožné.
7. Pokud dojde nejprve k vypršení doby odsouhlasení smlouvy, nastaví se status příslušné žádostí na „**Overdue**“ a další manipulace jsou nemožné.
8. Pokud dojde nejprve k odsouhlasení smlouvy, systém připravuje smart kontrakt a přikládá k němu hash elektronického dokumentu se smlouvou. Následně se status smart kontraktu a příslušné žádosti nastaví na „**Repayment**“.
   - Systém na základě elektronického dokumentu se smlouvou provádí platbu finančních prostředků na účet uživatele. Informace o skutečném provedení platby se zaznamenává v příslušném smart kontraktu.
9. Veškeré činnosti související s platbami v rámci daného úvěru, včetně splátek a sankcí za porušení, se zaznamenávají do smart kontraktu.
10. Po splacení celého úvěru se status smart kontraktu a žádosti nastaví na „**Closed**“.
11. Úvěr je splacen.

9.5 Diagram aktivit

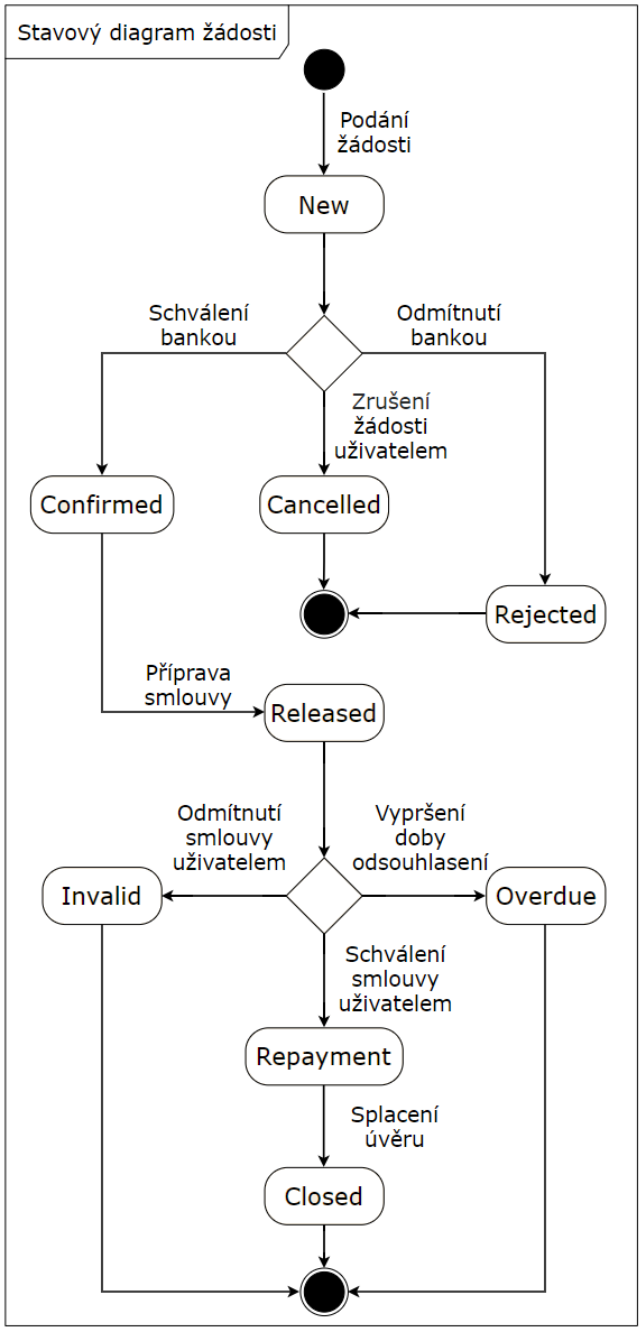
Na základě specifikace zadání práce je sestaven diagram aktivit popisující tok procesů poskytnutí úvěru bankou od doby podání žádosti do momentu zaznamenávání transakce ve veřejném bankovním blockchainu. Diagram aktivit je znázorněn na obrázku 9.2.



Obrázek 9.2: Diagram aktivit

9.6 Stavový diagram

Pomocí stavového diagramu (obrázek 9.3) jsou znázorněny stavy žádostí o poskytnutí úvěru a přechody mezi těmito stavy.



Obrázek 9.3: Stavový diagram žádosti

Kapitola 10

Návrh implementace systému

Následující kapitola se věnuje návrhu implementace budoucího systému poskytnutí úvěru. V úvodu jsou zvoleny vhodné technologie umožňující v plné míře splnit požadavky kladené na systém. V dalším kroku je představena architektura webové aplikace a na základě toho je v závěru kapitoly zobrazeno rozložení jednotlivých softwarových komponent na hardwarových zdrojích a jejich spolupráce.

10.1 Zvolení technologií

Výslednou architekturu webové aplikace je možné rozdělit do několika částí:

1. **blockchain**
2. **frontend**
3. **backend**

10.1.1 Blockchain

10.1.1.1 Bitcoin

Bitcoin je první implementací blockchainu, která umožnila uživatelům lépe se seznámit s touto technologií. Bitcoin by mohl být považován za základ pro budoucí zavedení systému poskytnutí bankovního úvěru, ale postrádá jeden důležitý aspekt, který by do značné míry zajistil bezpečnost pro obě strany smlouvy. Jedná se o turingovsky úplné smart kontrakty. Bez ohledu na existenci smart kontraktů v blockchainu Bitcoin, smart kontrakty v dané síti nejsou turingovsky úplné, což znamená omezení realizace potřebné funkcionality.

10.1.1.2 Ethereum

Ethereum patří k další generaci blockchainů, což přináší vlastnosti a možnosti, které chybí v blockchainu Bitcoin. Hlavním cílem blockchainu Ethereum je stát se platformou pro vytváření a provoz decentralizovaných aplikací (DApps) založených na blockchainu pomocí inteligentních smluv, jinými slovy smart kontraktů.

Ethereum je optimalizován několikrát lépe než Bitcoin. V souvislosti s tím v dnešní době v blockchainu Ethereum čas vytváření bloku je 15 sekund a čas zpracování transakce je průměrně 5 minut. Na rozdíl od toho v blockchainu Bitcoin čas vytváření bloku je průměrně 10 minut a čas zpracování transakce je v rozpětí od 3 do 5 hodin.

Na závěr stojí za zmínku skutečnost, že odesílatel transakcí v blockchainu Ethereum musí zaplatit poplatky těžařům, kteří ji potvrzují a zapisují do blockchainu. Tato platba se provádí v jednotkách nazývaných „Gas“. „Kdo uhradí transakční poplatky?“ Jedná se o otázku, kterou si musí položit ty společnosti, které poskytují služby s využitím technologie blockchain i v případě poskytnutí bankovního úvěru.

10.1.1.3 EOS

Pokud jde o rychlost transakcí a poplatků, je možné posoudit ještě jednoho kandidáta pro základ budoucího systému – EOS.

Mezi ostatními kryptoměnami vyniká EOS nulovými poplatky za převod a schopností během sekundy vyřídit až 4 000 transakcí, což v průměru 190krát více než konkurenční Ethereum. Rychlé zpracování transakcí je jedním z klíčových faktorů, na který se musí zaměřit společnosti, jejichž systém je postavený na blockchainu. Každý systém, který potenciálně plánuje poskytovat své služby velkému počtu uživatelů, musí zpracovat transakce co nejrychleji a tím si zachovat konkurenceschopnost na trhu.

10.1.1.4 Shrnutí zvolení blockchainu

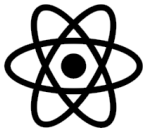
Po analýze některých potenciálních kandidátů blockchainu pro základ budoucího systému padá volba na blockchain Ethereum.

Důvodem je, že ekosystém Ethereum se neustále rozvíjí a získává v posledních několika letech velkou popularitu, a proto v současné době existuje množství projektů, které jsou postaveny na blockchainu Ethereum.

Dalším důvodem je to, že již existuje mnoho knihoven, které jsou napsané pro různé programovací jazyky pro práci s blockchainem Ethereum a psaní smart kontraktů v jazyce Solidity, z čehož vyplývá vysoká pravděpodobnost toho, že již existují odpovědi na otázky, které vzniknou během práce a díky kterým se ušetří čas vývoje systému.

10.1.2 Frontend

10.1.2.1 React

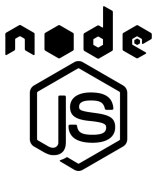


Použití Reactu je dobrým řešením pro frontendovou část webové aplikace. React je na leaderboardu již dlouhou dobu díky své jednoduchosti a vysokému výkonu vyvinutých aplikací. Komponenty, které byly vytvořeny při práci na projektu, nemají v podstatě závislosti. Nic tedy nebrání jejich opětovnému použití v projektech různých typů. Všechny předchozí zkušenosti lze snadno použít při práci na novém webu nebo při vytváření mobilní aplikace. Schopnost snadno znovu použít stávající kód zvyšuje rychlost vývoje, zjednodušuje proces testování a v důsledku toho snižuje náklady.

10.1.3 Backend

10.1.3.1 NodeJS

Pro backendovou část webové aplikace je možné použít NodeJS. NodeJS – prostředí JavaScript, které se používá k vytváření výkonných, rychlých a škálovatelných serverových aplikací. S předchozím bodem souvisí i fakt, že značná část knihoven používaných pro klientský JavaScript je díky NodeJS možné používat i na serveru.



NodeJS je skvělý pro aplikace, které pracují současně s velkým počtem paralelních připojení. Pomocí asynchronní povahy zpracování dat v JavaScriptu je možné vytvořit vysoce škálovatelný serverový kód, který umožní maximalizovat využití výkonu a paměti jednoho procesoru a nakonec umožní zpracovávat více paralelních požadavků.

10.1.3.2 Solidity

Důležitým prvkem v systému Ethereum jsou tzv. smart kontrakty. Pro vytvoření smart kontraktů s požadovanou funkcionalitou je vhodný programovací jazyk Solidity.

Sám o sobě Solidity je poměrně jednoduchý jazyk a ve své struktuře je podobný mnoha jiným klasickým programovacím jazykům. Je třeba poznamenat, že při používání Solidity (stejně jako jiné podobné nástroje Ethereum) existuje vysoké riziko a vysoké náklady na chyby, takže při testování vytvořených aplikací je třeba opatrnosti.

10.1.3.3 Truffle

Před zahájením nasazení smart kontraktů je nutné několikrát zkontrolovat kód, najít možné chyby a nekonzistence. Pro tyto potřeby je dalším pomocným nástrojem Truffle, který by se mohl využít během vývoje aplikace a smart kontraktů.

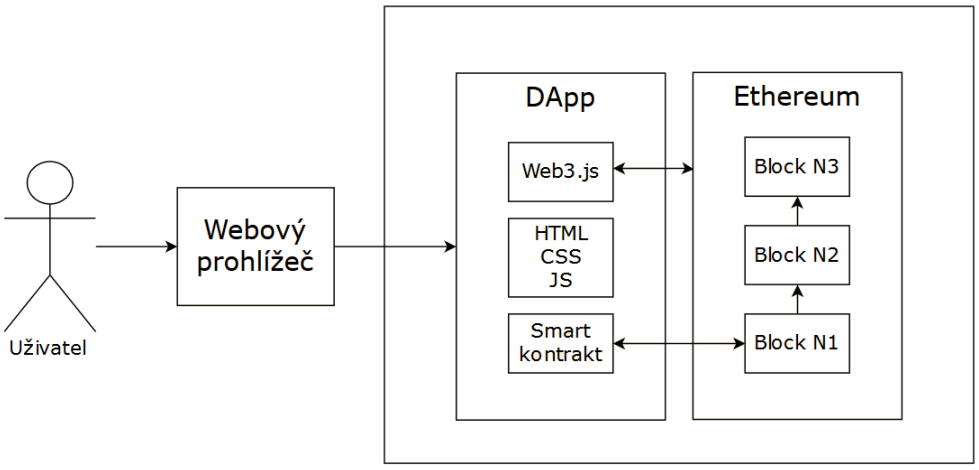
Truffle – vývojové prostředí a rámec pro testování produktů pro Ethereum, jehož cílem je usnadnit život vývojářům Ethereum.

10.1.3.4 Web3.js

Pro usnadnění práce s blockchainem Ethereum je vhodné použití kolekce knihoven Web3.js. Uvedená kolekce umožňuje interakci s lokálním nebo vzdáleným uzlem Ethereum pomocí HTTP nebo Remote Proceduře Call (RPC), načítat uživatelské účty, posílat transakce a komunikovat se smart kontrakty.

10.2 Architektura webové aplikace

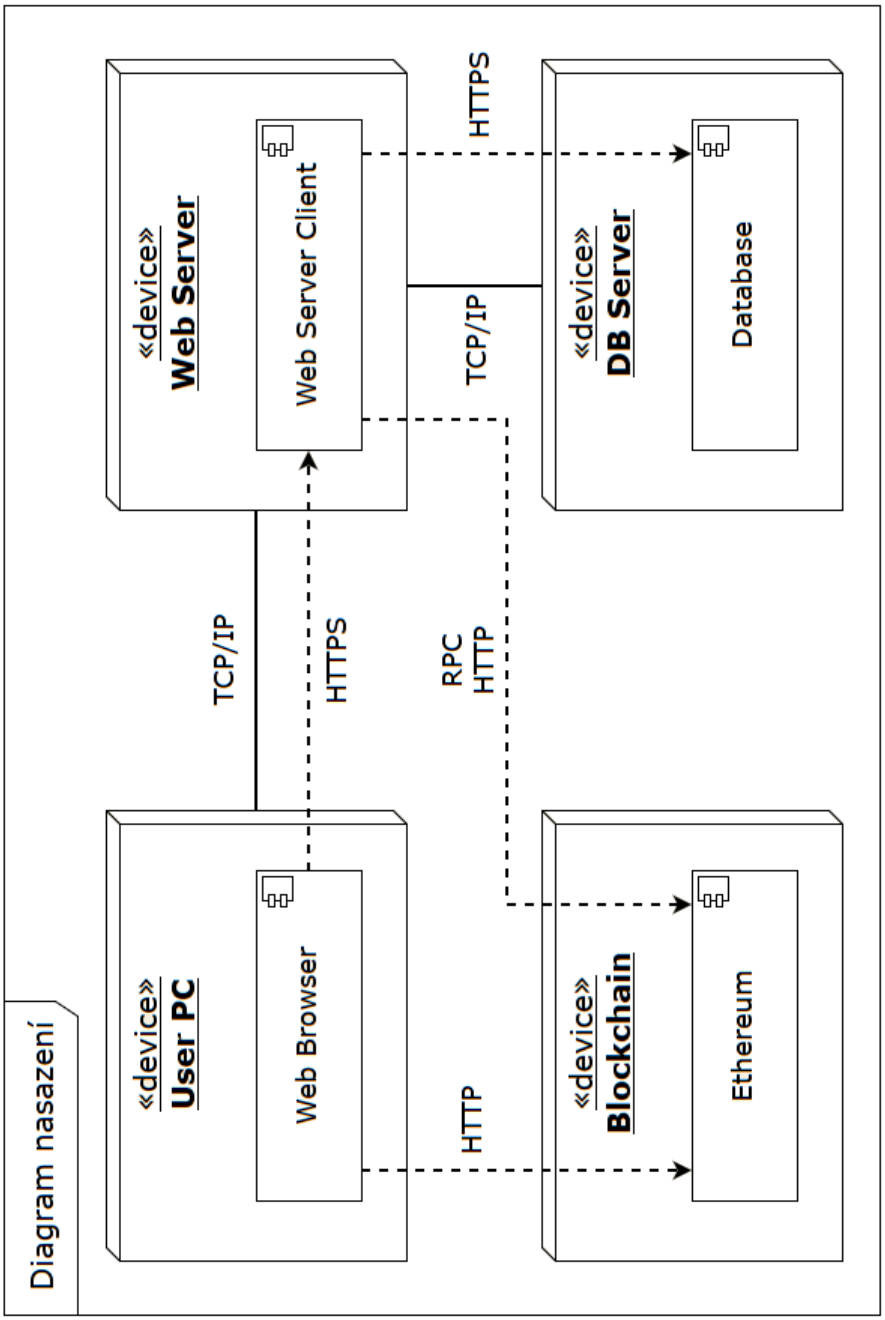
Schéma architektury webové aplikace na obrázku 10.1 znázorňuje interakci s blockchainem přes webový prohlížeč.



Obrázek 10.1: Architektura webové aplikace

10.3 Diagram nasazení

Diagram nasazení na obrázku 10.2 zobrazuje specifikaci fyzické architektury systému.



Obrázek 10.2: Diagram nasazení

Závěr

V rámci této práce byla provedena analýza principů a mechanismů fungování technologie blockchain z 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, na jejímž základě pomocí postupů softwarového inženýrství byl 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] TradeArena: *Co je a jak funguje 51% útok ©2019* [online]. [cit. 2019-07-16]. Dostupné z: https://www.tradearena.cz/rubriky/bitcoin/co-je-a-jak-funguje-51-utok-u-bitcoinu_383.html

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

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

[13] 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/

[14] 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

[15] CNewsCz: *Jak velká je dnes těžba kryptoměn? ©2019* [online]. [cit. 2019-07-16]. Dostupné z: https://www.cnews.cz/jak-velka-je-dnes-tezba-kryptomen-spotrebuje-vic-elektriny-nez-stredne-velke-staty/

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

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

[18] 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/

Příloha A

Seznam použitých zkratek

P2P Peer-to-Peer

DoS Denial of service

DDos Distributed denial of service

DApps Decentralized applications

PoW Proof-of-Work

PoS Proof-of-Stake

SHA512 Secure Hash Algorithm 512

HTTP Hypertext Transfer Protocol

HTTPS Hypertext Transfer Protocol Secure

RPC Remote Procedure Call

API Application Programming Interface

VISA Visa International Service Association