VYSOKÁ ŠKOLA EKONOMICKÁ V PRAZE

FAKULTA FINANCÍ A ÚČETNICTVÍ

Katedra finančního účetnictví a auditingu

studijní obor: Účetnictví a finanční řízení podniku

AUDIT BLOCKCHAINU

Autor diplomové práce:	Bc. Lukáš Dlask
Vedoucí diplomové práce:	Ing. Michal Šindelář, Ph.D.
Rok obhajoby:	2019

Čestné prohlášení

Prohlašuji, že diplomovou práci na téma Audit Blockchainu jsem vypracoval samostatně a veškerou použitou literaturu a další prameny jsem řádně označil a uvedl v přiloženém seznamu.

V Praze dne 13. ledna 2019

Abstrakt

Diplomová práce se zabývá vymezením technologie Blockchain a možnostmi jejího využití jak v podnikovém prostředí, tak při interním auditu i auditu účetní závěrky. Práce se v úvodu zaobírá vývojem auditu v kontextu využití informačních technologií a robotické automatizace auditu. Hlavní část práce popisuje vývoj, fungování a aplikaci v auditingu v současnosti často diskutované technologii Blockchain a s ní spojené Smart contracts, jejich výhody, ale i omezení a jejichž znalost je nejen pro auditory důležitá. Závěr práce je věnován teorii potrojného účtování s pomocí Blockchainu. Kapitoly jsou doplněny o tabulky, názorná schémata a výsledky aktuálních výzkumů.

Summary

The diploma thesis "Auditing the Blockchain" focuses on the definition of Blockchain technology and its possible applications in business practice, including in internal and financial statement audits. It describes the evolution of implementing and using information technologies in robotic process automation in audits. It additionally defines the development and application of Blockchain technology and smart contracts in audit practice, including the advantages and limitations of what knowledge is important not only to the auditors but others as well. Finally, the thesis proposes a triple-entry accounting scheme using the Blockchain. Its chapters are supplemented by figures, diagrams and current research results.

Klíčová slova | Keywords

Blockchain, Audit, Smart Contract, Smart Audit Procedure, Triple-entry Accounting, Potrojné účetnictví

Poděkování

Děkuji vedoucímu diplomové práce panu Ing. Michalu Šindelářovi, Ph.D. za jeho ochotu a čas, věcné připomínky a odborné rady, které mi poskytl při zpracování této práce. Zároveň děkuji rodině a přátelům za nekončící podporu při mém studiu.

Obsah

Úvod

Blockchain představuje druh digitální distribuované databáze s absencí centrální autority, např. centrální banky. Je primárně spojovaný s kryptoměnami, které od svého vzniku během světové finanční krize v roce 2008 používají tuto technologii jako transparentní, ověřitelnou a věrohodnou sdílenou databázi či „účetní knihu“ pro zaznamenávání uskutečněných transakcí. Každá transakce či změna je v databázi navždy zaznamenána a díky použitému šifrování nemůže být nikým zpětně upravena nebo smazána. Možnosti aplikace Blockchainu jsou mnohem širší. Kromě finančního sektoru již existují platformy i v mezinárodním obchodě, distribuci nebo zdravotnictví a podle odhadů bude jeho význam a využití v budoucnu nadále růst.

Blockchain s sebou nese velká očekávání i v oblasti účetnictví. Díky nemožnosti zpětně manipulovat vložená data získávají auditoři, ale i veřejnost, ujištění o jejich integritě a věrohodnosti. Dalším významným prvkem spojeným s Blockchainem jsou Smart contracts, které na bázi určitých předdefinovaných pravidel kontrolují podnikové procesy a v budoucnu by mohly samostatně provádět rozhodování a řídit tak celý business.

Cílem práce je vymezit vznik a fungování technologie Blockchain, jeho potenciální využití v účetnictví, v rámci něhož opět vyvstává myšlenka využití potrojného účetnictví a aplikaci v auditu účetní závěrky, a to se zaměřením na výhody, ale i úskalí, této technologie, které by měli mít na paměti nejen auditoři při auditu transakcí v Blockchainu. Práce obsahuje tři hlavní kapitoly a je doplněna o názorná schémata, aktuální data a výsledky celosvětových průzkumů.

První kapitola je věnována historickému vývoji auditingu, regulaci z národního i mezinárodního pohledu a vývoji používání informačních technologií v auditu, které je mapováno od používání tužky a kalkulačky až po dnešní dobu spojenou s big data, průmyslem 4.0, digitální ekonomikou a internetem věcí. Závěr kapitoly je věnován aktuálnímu tématu robotizace a automatizace procesů nejen v auditu a dále smart procedurám, tj. chytrým auditorským postupům.

Druhá kapitola popisuje nejznámější kryptoměny, okolnosti jejich vzniku, a především vývoj a technologické fungování Blockchainu. Zároveň se zabývá jednotlivými druhy této technologie použitelnými pro odlišné účely. Kapitola se podrobně zabývá i nevýhodami oproti jiným informačním systémům, srovnáním s ERP

(informačními systémy pro plánování podnikových procesů) a přibližuje současné aplikace Blockchainu v praxi.

Třetí kapitola vysvětluje pojem Smart contracts, jehož koncept byl popsán již v roce 1994. Následně je aplikován v prostředí Blockchainu ve spojení s chytrými auditorskými procedurami vedoucími ke zefektivnění auditu. Kapitola se také zabývá myšlenkou potrojného účtování s použitím Blockchainu. V závěru je pojednáno o procesu auditu transakcí uskutečněných v Blockchainu z pohledu auditora a s tím spojených rizicích při auditu účetní závěrky.

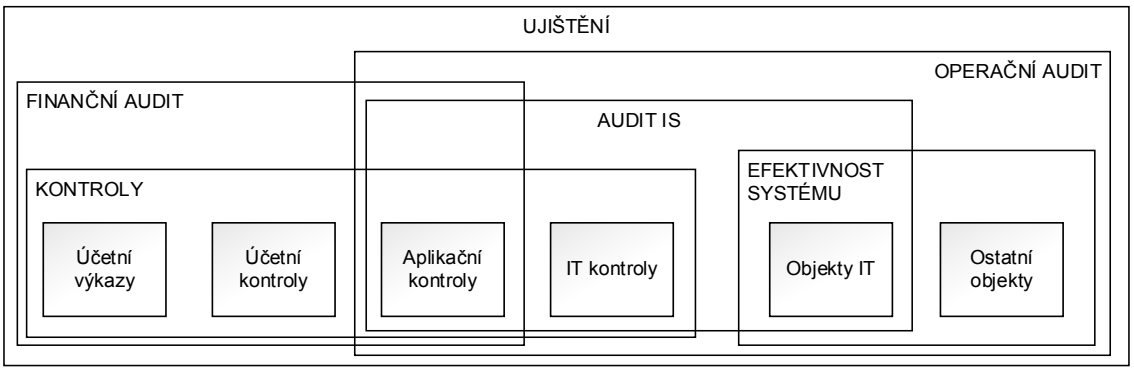
Všechny legislativní normy vychází ze stavu platného k 1. prosinci 2018.

1 Auditing – historie a budoucnost

Auditing je vědní disciplínou spadající do oboru ekonomie. Jedná se o systematický proces objektivního získávání informací a jejich vyhodnocování na základě tvrzení o ekonomickém působení a událostech, zjišťuje míru shody mezi těmito informacemi a ustanovenými kritérii a výsledky následně interpretuje zainteresovaným stranám (Silvoso, 1972).

Samotný proces auditu může být zaměřen na různé oblasti, tím se odlišují jeho cíle, legislativní úprava, uživatelé, požadavky, metody nebo postupy. Mezi nejznámější druhy auditu patří (Müllerová, Králíček a kol., 2017): audit účetní závěrky (nazývaný také jako externí audit, statutární audit či méně přesněji finanční audit jako překlad z angl. financial statement audit); interní audit či vnitřní audit; forenzní audit; energetický audit; ekologický audit; počítačový audit; personální audit nebo audit jakosti. Vazby mezi jednotlivými druhy auditu zobrazuje následující schéma.

Obrázek 1: Vazby mezi jednotlivými druhy auditu



zdroj: Svatá, 2012, vlastní zpracování

V některých případech bývá termín audit účetní závěrky zaměňován s běžnou kontrolou, která není prováděna podle zákonem stanovených norem, v České republice zákonem č. 93/2009 Sb., o auditorech ve znění pozdějších předpisů (dále jen zákon o auditorech). Takové kontroly, které nepodléhají uvedenému zákonu může provádět kdokoliv a výstupy tak nepodléhají dohledu. (Komora auditorů České republiky, 2013, s. 7-8).

Výsledkem auditu účetní závěrky je auditorská zpráva obsahující výrok auditora. Uživateli této zprávy jsou kromě společnosti a jejich vlastníků, akcionářů nebo společníků i angažované veřejnosti, tzv. steakholders (zaměstnanci, banky, obchodní partneři, finanční úřad atd.). Všechny tyto skupiny dostávají ujištění, že předložené účetní informace poskytují věrný a poctivý obraz a odpovídají skutečnosti.

1.1 Historický vývoj auditu

První číselné systémy, symboly a slova byly rozvinuty k zaznamenávání a sledování rozvíjejících se směnných obchodů zboží v obchodě. Historie auditu sahá až do starého Egypta, kde bylo požadováno, aby daňové příjmy potvrzovali dva na sobě nezávislí úředníci. Slovo auditor vychází z latinského *audire*, které znamená slyšet, poslouchat či naslouchat, protože se ve starých dobách účastnili ústních jednání úředníků s majetnými občany a potvrzovali správnost výsledných zpráv. Pozdějším vývojem začali auditoři ověřovat písemné dokumenty (Smieliauskas a kol., 2015). Celá podstata auditu jako kontroly nezávislou osobou, zda informace jsou odpovídající realitě, tak zůstala dodnes nezměněna.

Za dochované středověké zdroje z Anglie r. 1100 na dvoře Jindřicha I. Anglického považujeme ověřovatele správnosti zaúčtování státních příjmových a výdajových transakcí. Následně v roce 1285 bylo v Anglii již zákonem *Accountants Act 1285* definováno, kdo se může stát auditorem a zároveň cíl nezávislého posouzení účetních výkazů. Už tehdy byl kladen důraz na nezávislost auditora.

Audit byl poznamenán i vývojem účetnictví. V roce 1494 byl poprvé popsán a definován systém podvojného účetnictví františkánským mnichem a matematikem Lucou Pacioli ve spise *Soubor aritmetiky, geometrie, poměrů a úměr*.[1] Pacioli zároveň zdůrazňoval doporučení, aby účetní záznamy byly kontrolovány auditorem.

První provedený nezávislý audit je datován v roce 1720 (Chatfield a Vangermeersch, 2013). V závěrečné zprávě společnosti South Sea Company byly odhaleny podvody v účetních výkazech a podvodná jednání se členy Westminsterského paláce. Investoři najali účetního Charlese Snella ke kontrole výkazů a vyšetřování podvodu dceřiné společnosti Sawbridge and Company. Tento audit je považován za samotný vznik profese auditora ve Velké Británii, který se postupně od druhé poloviny 19. století významně rozvíjel. Vznikla organizace účetních Chartered Accountants in England a následně organizace Certified Public Accountants (zkr. CPA).

[1] Učebnice shrnuje matematické poznatky. Pojednání jedenácté, vyčleněné, o počtech a zápiscích. Česká verze vydána v roce 1940 překladem z němčiny. Pojednání začíná výkladem o sestavě účetních knih a pokračuje velmi podrobným návodem k vytvoření inventáře jako základu budoucího účtování obchodních případů (soupis majetku, sestavovaný zpravidla podle potřeby po delších obdobích, jinde každoročně či po dvou letech), knize pamětní (kniha pro evidenci všech skutečností, týkajících se koupě a prodeje se všemi podrobnostmi (počet kusů, splatnost atd.), každý zápis se nazýval položkou, jednotlivé položky se ve volném čase, nejlépe denně převáděly do deníku), deník sloužil pro zápis položek memoriálu načisto a dále se zapisovalo do hlavní knihy. (Janhuba, 2010)

Samotný začátek moderního auditingu je spojován s vydáním zákona Joint Stock Companies Act ve Velké Británii v roce 1844. Poprvé byly společnosti povinny zveřejňovat své finanční výsledky. Akcionáři získali právo kontrolovat účetní záznamy a výkazy a zároveň se vedení společnosti dotazovat na případné nesoulady nebo nejasnosti. Od roku 1900 bylo novelou zákona požadováno, aby auditor byl nezávislý na dané společnosti. (Müllerová, Králíček a kol., 2017).

Rostoucí výskyt zveřejňování zavádějících nebo nepravdivých účetních informací měl mimo jiné za následek pád newyorské burzy v roce 1929 a následně nástup hospodářské krize ve třicátých letech. V reakci na tyto události byl ve Spojených státech v roce 1933 vydán zákon U.S. Securitites Act, kterým zřídil Komisi pro cenné papíry (Securities and Exchange Commission; SEC), která přinesla významné změny pro společnosti, jejichž akcie jsou veřejně obchodované na burze. Vznikla jim povinnost nechat ověřit své účetní závěrky nezávislým auditorem. V reakci na významné účetní skandály společností Enron, WorldCom, Kmart nebo Xerox byl v roce 2002 schválen federální zákon Sarbanes-Oxley Act (SOX), který upravuje povinnosti společností, auditorů i dalších stran s důrazem na nezávislost auditora. V současné době je audit celosvětově regulovanou profesí.

Směrnice Evropské unie představují legislativní nástroj harmonizace předpisů jednotlivých členských států, tyto státy mají povinnost v určité stanovené lhůtě implementovat je do svých právních řádů. V roce 1984 tomu tak bylo i s osmou směrnicí Rady 84/253/EHS, o schvalování osob pověřených prováděním povinného auditu účetních dokumentů. Směrnice definovala požadavky potřebné k udělení auditorské licence. Především pro nedostatek harmonizovaného přístupu byla tato směrnice zrušena a od 29. června 2006 nahrazena směrnicí Evropského parlamentu a Rady 2006/43/ES, o povinném auditu ročních a konsolidovaných účetních závěrek. Tato úprava již detailně upravuje požadavky na povinný audit v Evropské unii. (Müllerová, Králíček a kol., 2017) Směrnice v úvodu definuje používané pojmy, definuje podmínky pro schvalování statuárních auditorů, vzdělávání a odbornou způsobilost, registrace auditorů a auditorských společností, profesní etiku, auditorské standardy i požadavky na zprávu auditora. Dále definuje i podmínky pro zajištění kvality, veřejného dohledu, požadavky na jmenování a odvolání statuárních auditorů a auditorských společností, stanovuje podmínky pro provedení povinného auditu subjektů veřejného zájmu a zabývá se i problematikou mezinárodního hlediska.

Nařízení Evropského parlamentu a Rady EU č. 537/2014 představuje poslední legislativní úpravu v oblasti regulace auditu. Na rozdíl od směrnice má nařízení obecnou působnost a je závazné v celém rozsahu, zatímco směrnice je závazná co do výsledku, jehož má být dosaženo, ale volba prostředků dosažení je ponechána vnitrostátním orgánům. Nařízení definuje mj. požadavky na provádění povinného auditu účetních závěrek veřejného zájmu s cílem zvýšení nezávislosti a zabránění případnému střetu zájmů. (Müllerová, Králíček a kol., 2017)

1.1.1 Vývoj auditingu v České republice

Auditorská profese prošla stagnací v Čechách i ve světě za dob světové války. Nástup socialismu značně ovlivnil jeho další směřování. V plném rozsahu byla auditorská profese obnovena po roce 1989. Původní Unie účetních ČSFR, která zastřešovala nejen auditory, ale i odborníky na účetnictví a finance, byla později přeměněna na Unii auditorů ČR, na kterou v únoru 1993 plynule navázala činnost nově založená Komora auditorů ČR (dále jen KAČR). Postupem času s rozvojem podnikání a vlivem privatizace docházelo k postupnému růstu poptávky po auditorských službách s čímž souviselo i zvyšování nároků na tuto profesi. Zákon o auditorech byl přijat 20. listopadu 1992.[2] (Komora auditorů České republiky, 2013, s. 9-12)

1.2 Regulace auditu

Protože práce auditora vyžaduje odbornost a pečlivou znalost teorie i praxe z oblasti auditu, účetnictví, podnikových financí, informačních a výpočetních technologií i daní, a na výstupy celého procesu se spoléhají kromě managementu i investoři, odborná veřejnost i široké okolí podniku, je celý proces provádění auditu regulován, aby byla zajištěna jeho objektivita.

Auditorskou profesi řadíme mezi tzv. svobodná povolání, mezi jejichž znaky patří mj. poskytování služeb veřejnosti, které jsou pro ni důležité a vyžadují speciální znalosti a činí tak objektivně, řádně a nestranně. Proto je důležité takové osoby označit, aby se odlišili od jiných osob, které danou kvalifikaci nemají. V průběhu let vznikaly profesní organizace pro daná svobodná povolání, u některých povolání je samotné členství pro výkon funkce povinné (např. lékaři – Česká lékařská komora, advokáti – Česká advokátní

[2] Podrobněji o Komoře auditorů pojednává subkapitola 1.2.2 Národní profesní organizace.

komora, daňoví poradci – Komora daňových poradců České republiky nebo právě auditoři – KAČR). (Müllerová, Králíček a kol., 2017, str. 38)

1.2.1 Mezinárodní profesní organizace

Mezinárodní federace účetních a auditorů

Mezinárodní federace účetních a auditorů (International Federation of Accountants) založena v roce 1977 se sídlem ve švýcarské Ženevě a výkonným sídlem v americkém New Yorku celosvětově sdružuje účetní a auditory ve více než 130 zemích s téměř třemi miliony členy. Cílem je sloužit veřejnému zájmu a posilovat účetní profesi vytvářením kvalitních mezinárodních standardů a podpora jejich implementace, podpora profesních organizací účetních a auditorů a vyjadřovat se k tématům a problematice veřejného zájmu. Federace zaštiťuje provoz následujících organizací, které vydávají mezinárodní standardy:

Rada pro mezinárodní auditorské a ověřovací standardy (International Auditing and Assurance Standards Board; IAASB) – organizace vydávající Mezinárodní standardy pro audit (International Standards on Auditing; ISA). Cílem je vytvořit ucelený soubor standardů, který bude všeobecně uznávaný po celém světě. V České republice byly přijaty tyto standardy jako národní předpisy a jejich používání je závazné.[3] Další standardy vydávané touto Radou jsou Mezinárodní standardy pro ověřovací zakázky (International Standards on Assurance Engagements; ISAE), Mezinárodní standardy pro související služby (International Standards on Related Services; ISRS), Mezinárodní standardy pro řízení kvality (International Standards on Quality Control; ISQC).

Dalšími orgány jsou **Rada pro mezinárodní etické standardy účetních** (International Ethics Standards Board for Accountants; IESBA), která se zabývá etickým kodexem a stanovuje tak základní požadavky pro odborníky působící v oboru. **Rada pro mezinárodní účetní standardy pro veřejný sektor** (International Public Sector Accounting Standards Board; IPSASB) sestavuje standardy pro veřejný sektor a **Rada pro mezinárodní standardy vzdělávání účetních** (International Accounting Education Standards Board; IAESB) stanovuje nároky na vzdělávání v oboru.

[3] „Auditor postupuje při provádění auditorské činnosti v souladu s auditorskými standardy upravenými právem Evropské unie.“ – ustanovení § 18 zákona o auditorech.

Organizace evropských účetních

Organizace evropských účetních (Accountancy Europe)[4] sídlí v Bruselu a byla založena v roce 1987 s cílem zlepšení harmonizace účetních postupů v Evropě a zvýšení informovanosti členů. Sdružuje 51 profesních organizací z 37 evropských zemí, což představuje přes jeden milion účetních a auditorů.

1.2.2 Národní profesní organizace

Americký institut certifikovaných účetních

Americký institut certifikovaných účetních (American Institute of Certified Public Accountants; AICPA) byl založen v roce 1887 a sídlí v New Yorku. V současnosti sdružuje přes 418 tisíc členů. Členové jsou certifikovaní účetní Certified Public Accountants (CPA) a kromě auditorů jsou členy i finanční odborníci nebo univerzitní pedagogové. Zkušební výbor této organizace připravuje jednotný systém zkoušek pro CPA, oprávnění pro výkon praxe pak udělují orgány v jednotlivých státech. V rámci vzdělávacího programu je vydáván měsíčník The Journal of Accountancy věnovaný současné problematice a trendům v oboru.

Ve Spojených státech je pro audit používáno několik odlišných standardů. Rada pro auditorské standardy (Auditing Standards Board; ASB), zřizovaná Americkým institutem certifikovaných účetních, sestavuje standardy pro společnosti, které nejsou veřejně obchodovány na burze. V reakci na pochybení při provádění auditu tehdy jedné z největších auditorských společností Arthur Andersen & Co. a v souvislosti s krachy společností, kde byly páchány finanční podvody a auditoři nebyli nezávislí na vedení společností, byl v roce 2002 vydán zákon Sarbanes-Oxley Act, kterým vznikla Rada pro veřejný dohled nad auditem (Public Company Accounting Oversight Board; PCAOB), která hájí zájmy investorů společností, jejichž akcie jsou veřejně obchodovány. PCAOB vytváří standardy pro audit těchto společností (Auditing Standard; AS). (Kleinman a Anandarajan, 2014, s. 11)

S používáním vlastních auditorských standardů ve Spojených státech souvisí i používání vlastních účetních standardů U.S. GAAP (United States Generally Accepted Accounting Principles), které musí používat pro vykazování svých finančních výsledků všechny společnosti kótované na burze.

[4] Původní název Federace evropských účetních (Federation of European Accountants; FEE) byl při třicátém výročí v roce 2016 přejmenován na současný název Organizace evropských účetních.

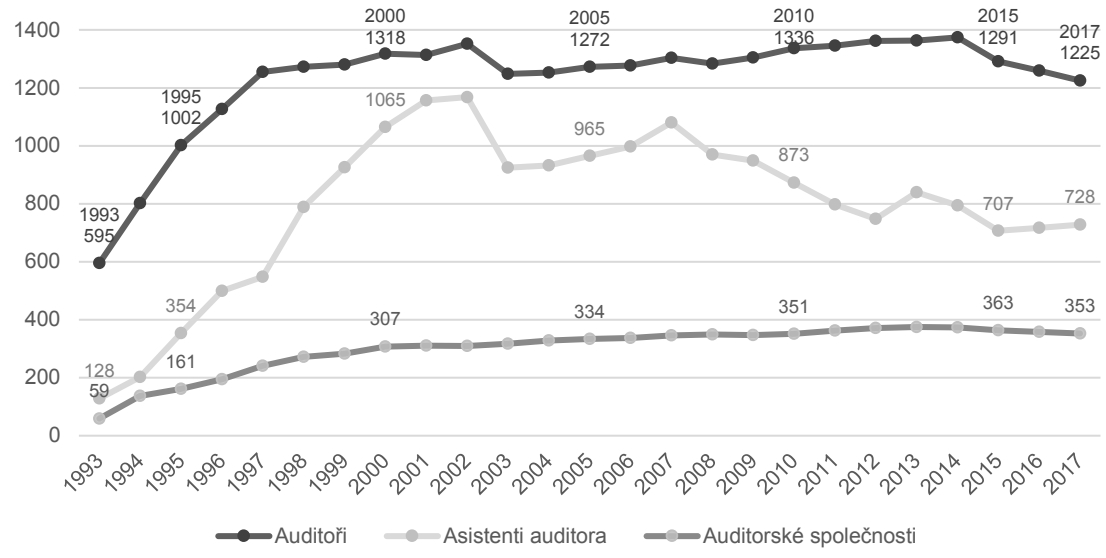
Komora auditorů České republiky

KAČR funguje od února 1993 uspořádáním ustanovujícího sněmu. Od dubna 2009 je působnost KAČR upravena zákonem o auditorech a povinné audity účetních závěrek podle tohoto zákona mohou provádět pouze auditoři zapsaní v Komoře. KAČR je členem Národní účetní rady a mezinárodních profesních organizací Mezinárodní federace účetních a auditorů (IFAC) a Organizace evropských účetních (AE). Od roku 1992 vydává odborný časopis Auditor.

KAČR mj. kontroluje dodržování ustanovení zákona o auditorech, stanovuje požadavky ke složení auditorské zkoušky a vydává auditorská oprávnění. Nejvyšším orgánem je Sněm, který se koná alespoň jednou za dva roky a mohou se ho účastnit všichni auditoři. Mezi sněmy komory ji řídí Výkonný výbor, kontrolním orgánem je Dozorčí komise a řízení o neplnění nebo porušení povinností provádí Kárná komise. (Komora auditorů České republiky, 2018)

Z původních 434 řádných členů datovaných k únoru 1993 se počet členů rozrostl k 31. prosinci 2017 na 1225 auditorů, 728 asistentů auditora a 353 auditorských společností. Podíl auditorů ve věku 51-70 let činil 665 auditorů, tj. 55 %, následován mladší generací ve věku 31-50 let s 38% podílem, tj. 463 auditorů. (Mikyna a Šnajdrová, 2018)

Graf 1: Vývoj počtu auditorů, asistentů auditorů a auditorských společností



zdroj: Auditor č. 2/2018, vlastní zpracování

1.3 Vývoj od Auditu 1.0 k Auditu 4.0

Průmysl 4.0, který byl představen na Hannoverském veletrhu v roce 2011, (Barreto, Amaral a Pereira, 2017) a je spojován s digitalizací, automatizací, internetem věcí a internetem služeb bývá považován za další průmyslovou revoluci. V tomto kontextu lze hovořit i o termínu či generaci Audit 4.0 představující ještě hlubší zapojení technologií do celého procesu provádění auditu. Podobně jako technologický vývoj v účetnictví, ale i v jiných oblastech, je v auditu hledán kompromis mezi kvalitou používaných technologií, vynaloženými náklady a zároveň spotřebovaným časem potřebným k provedení příslušných procedur.

1.3.1 Audit 1.0 a 2.0

Za audit 1.0 je považován audit, který existoval staletí a postupně se vyvíjel, jak již bylo popsáno v této kapitole. Za hlavní nástroje považujeme použití tužky a kalkulačky. Audit druhé generace je spojovaný se 70. léty 20. století a s využitím informačních technologií v podnicích a zároveň i pro potřeby auditu, v praxi často označované jako zkratky z anglických názvů Computer-assisted audit techniques (CAATs) či Computer-assisted audit tools and techniques (CAATTs). Zapojení informačních technologií výrazně zvýšilo efektivnost auditu a ulehčilo auditorům analytické testování. Tehdy používalo informační technologie kolem 15 % auditorů (Protiviti, 2015). Začátkem devadesátých let byly masivně zaváděny CAATTs (zprvu především pracovní papíry v elektronické podobě a používání tabulkových procesorů).

CAATs či CAATTs

Jedná se o anglické zkratky označující počítačově podporované auditorské techniky či nástroje, které jsou v dnešní době v podstatě nutností v této profesi. Představují použití výpočetní techniky v auditu. Mezi hlavní výhody patří efektivita práce, díky které auditoři šetří čas a snižují riziko, což má za následek lepší kvalitu provedených prací. Obecně můžeme takový software rozdělit na standartní a expertní.

Za dnes standardní aplikace lze považovat kancelářské balíčky jako např. Microsoft Office, který lze považovat za jeden z nejvíce používaných. Zahrnuje textový editor Word pro vedení auditorských dokumentů, tabulkový procesor Excel, prezentační program PowerPoint, nástroj Access pro práci s databázemi nebo emailový klient Outlook aj. Mezi alternativy patří kancelářský balíček Apps na cloudové platformě od společnosti Google (Docs, Sheets, Slide) či balíčky OpenOffice.org nebo LibreOffice. Při výběru vhodných aplikací je třeba zároveň uvažovat i povinnost archivace auditorských záznamů 10 let ode

dne vyhotovení zprávy auditora v souladu s ustanovením § 20a odst. 2 zákona o auditorech. S tím souvisí problematika kompatibility současných formátů jednotlivých souborů a jejich čitelnost za několik let.

Expertní systémy jsou vytvářeny speciálně přímo pro účely auditu. Provádí specifické operace pro auditory, jakými mohou být výběr vzorků pro testování, statistické funkce, provedení Benfordova zákona nebo tvorby a archivace spisů. Výhodou těchto systémů je nezávislost auditorů na informačních systémech auditovaného subjektu (Chartered Institute of Internal Auditors). Obvykle dochází k exportu dat ze systému klienta, následná kopie používaná auditorem zabraňuje poškození klientových dat a může případně sloužit i jako záloha při případné kritické ztrátě dat klienta. Specializovaný software zároveň obvykle poskytuje průkaznou dokumentaci o provedení konkrétních operací, takové výstupy bývají běžně součástí auditorského spisu. Mezi používané programy patří kontrolní a analytický program IDEA (Interactive Data Extraction and Analysis), který byl původně vyvinut ve veřejném sektoru v Kanadě a nyní ho vyvíjí společnost CaseWare International, která vyvíjí zároveň i aplikaci CaseWare Working Papers sloužící ke správě auditorského spisu, exportu finančních výkazů nebo doplňky používané pro konsolidaci účetních závěrek. V České republice je taktéž používán auditorský (účetní i daňový) software Datev vyvíjený v Německu. Velké mezinárodní auditorské společnosti si pak obvykle vyvíjí svůj vlastní software tzv. in-house, který je součástí jejich know-how.

1.3.2 Audit 3.0

Třetí generace auditu se vyvinula rychleji než předchozí etapy a je spojována s vývojem analytických nástrojů, aby byly schopny zpracovávat big data.

Big Data

Jak je z anglického překladu zřejmé, jedná se o soubory objemných dat, které je obtížné zpracovat v rozumném čase běžnými databázovými nástroji. Charakterizuje je velikost dat, rozmanitost typů dat (může se jednat o text, obrázky, zvuky apod.) a rychlost vzniku dat. Příkladem mohou být detailní analytická data z webových stránek či sociálních sítí, např. kdo v jaký čas a za jakých okolností klikl na určitou reklamu, záznamy z telefonních hovorů zákaznické podpory nebo historie nákupů jednotlivých zákazníků. Takové informace pomáhají lépe porozumět potřebám nebo zájmům daných cílových skupin a např. lépe cílit reklamu dle jednotlivých segmentů. Taková data mohou být zároveň velmi

cenná pro určitý okruh subjektů a při jejich úniku lze snadno dojít ke zneužití citlivých dat nejen konkurenty v odvětví.

Díky technologii radiofrekvenční identifikace (RFID) podniky mohou sledovat zásoby materiálu, výrobků nebo zboží individuálně např. po jednotlivých kusech, což umožňuje detailní okamžitý přehled o stavu a podporu pro efektivní řízení zásob. (Tang a Karim, 2018)

Auditoři při provádění auditu shromažďují důkazní materiály, mezi které mohou být zahrnuty i big data. Jejich použití může zvyšovat spolehlivost a relevantnost důkazních informací v souladu s ISA 500, odst. 26, což má vliv na celkovou kvalitu auditu. (Yoon, Hoogduin a Zhang, 2015).

1.3.3 Audit 4.0

Audit 4.0 významně změní auditorskou profesi automatizací současných procesů, zvětšením rozsahu auditu, zkrácením času potřebného k provedení auditu a ideálně i zvýšení úrovně celkového ujištění (Dai a Vasarhelyi, 2016). V tomto kontextu se jedná především o:

- digitální ekonomiku (Smart Factories),
- internet věcí (Internet of Things, zkr. IoT),
- internet služeb (Internet of Services, zkr. IoS) a
- kyber-fyzikální systémy (Cyber-Physical Systems).

Digitální ekonomika

Jedná se o digitalizaci výroby, tedy propojení internetu věcí, služeb a kyber-fyzikálních systémů. Anglický pojem Smart Factory lze chápat jako podnik reagující na požadavky trhu. V praxi při správné aplikaci dochází ke snižování výrobních nákladů, lepšímu využití zdrojů, zkracování běžných procesů, poskytování lepších služeb a tím i k vyšší produktivitě. Zákazník si může upravit požadovaný produkt podle svých potřeb.

Internet věcí

Internet věcí je označení pro samostatná zařízení (spotřebiče, auta, stroje), které jsou vybaveny softwarem, čipy nebo senzory a elektronikou s připojením k síti (např. internet nebo mobilní síť). Díky tomu si tato zařízení jsou schopna sbírat a vyměňovat data. Jejich využití je široké, od domácností (propojení s automobily, pračkami, ledničkami, osvětlením nebo nositelná elektronika jako např. hodinky), v podnikovém prostředí díky internetu věcí rozšiřují např. automatizaci strojů (označováno také jako Enterprise IoT).

Přístroje internetu věcí jsou používány i k řízení infrastruktury či ve zdravotnictví. (IoT Tech News)

Technologická a poradenská společnost Gartner v listopadu 2018 na konferenci v Barceloně[5] odhadla, že počet zařízení připojených k internetu věcí během příštích let bude rapidně růst, v roce 2019 odhaduje 14,2 miliard připojených přístrojů a později, v roce 2021, předpovídá až 25 miliard zařízení. Společnost zároveň předpověděla, že podniková přidaná hodnota z použití Blockchain technologie bude do roku 2025 kolem 176 miliard amerických dolarů a ro roku 2030 vzroste a překročí hranici 3,1 miliard dolarů[6].

Internet služeb

Cílem internetu služeb je poskytovat platformu, díky které mohou společnosti svým zákazníkům poskytovat své služby na dálku. Výhodou je, že se cílový uživatel s použitím webového prohlížeče může připojit kdekoliv, kde je dosah internetu. Je tak velkou výzvou pro aplikace či služby vyžívající cloudová úložiště. Typickým příkladem jsou online zálohování dat, online vedení účetnictví, webináře a videokonference či Customer-relationship management (zkr. CRM) systémy pro řízení vztahů se zákazníky.

Kyber-fyzikální systémy

Jedná se o systémy obsahující inteligentní objekty (snímače, senzory), které jsou připojeny k internetu a v reálném čase nezávisle na sobě na základě určitých spouštěcích podnětů analyzují data a mohou předpovídat případné poruchy či chyby, jsou nezávislé na uživateli. V praxi lze očekávat propojení strojů, skladů a IT systémů, a ještě výraznější usnadnění např. automatizací procesu zásobování materiálu. Digitalizace výroby bývá často spojována i s pojmem Digital factory (Spath a kol., 2013).

Mezi další techniky, které ovlivňují audit 4.0 patří RFID (radiofrekvenční systém identifikace objektů), který je rychlý a zároveň přesnější než čárové kódy. Informace jsou uchovávány v čipu a lze je tak zpětně přečíst či přepsat. Dále lze zařadit GPS pro sledování produktů nebo zaměstnanecké ID karty.

---

[5] Gartner Identifies Top 10 Strategic IoT Technologies and Trends, 7. listopadu 2018, Barcelona, Španělsko.

[6] Gartner Forecast: Blockchain Business Value, Worldwide, 2017-2030 online.

Tabulka 1: Jednotlivé generace auditu s běžně používanými prostředky

Generace	Používané prostředky
Audit 1.0	Ručně prováděný audit s použitím tužky a kalkulačky, využití přepisovací a následně propisovací formy zápisu
Audit 2.0	Použití informačních technologií s informačními technologiemi pro potřeby auditu, Microsoft Office Excel či jiné tabulkové editory a postupná elektronizace
Audit 3.0	Využití big data a rozvoj analytických nástrojů
Audit 4.0	Automatizace auditu, použití Smart contracts, internetu věcí a služeb, senzorů, GPS atd.

zdroj: Dai a Vasarhelyi, 2016, vlastní zpracování

1.4 Automatizace – budoucnost auditu

Odborníci zabývající se budoucím vývojem auditingu předpokládají významnou změnu v provádění auditu, a to především ve smyslu jeho automatizace a s ním spojené masivnější využití informačních technologií a zároveň snižování zapojení lidského kapitálu. Podle výzkumů je automatizace auditorských postupů iniciována samotnými auditorskými společnostmi.

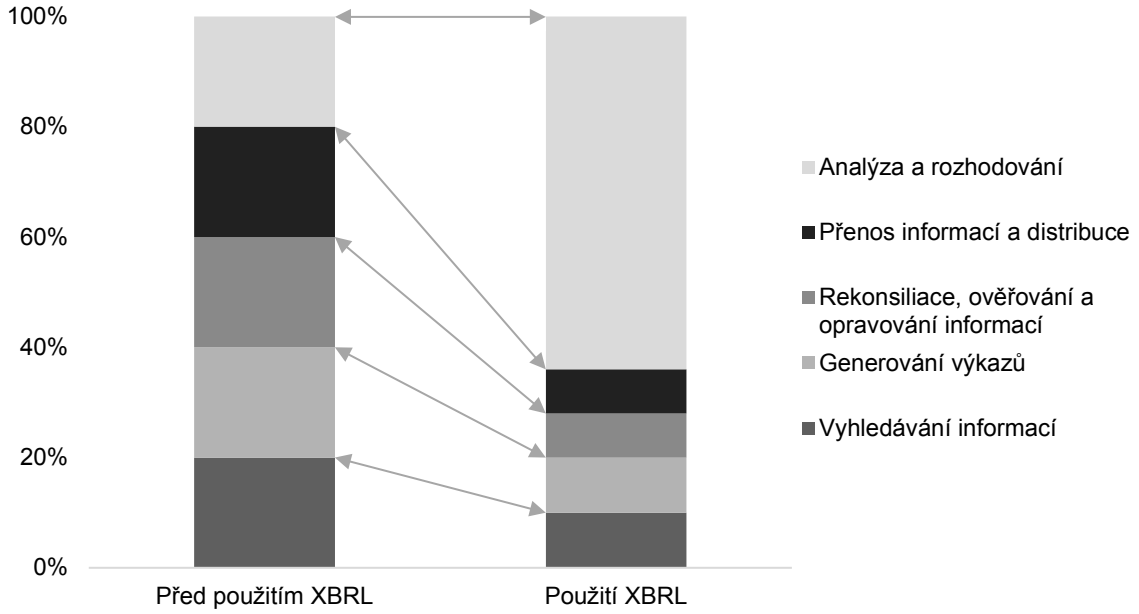
Zda auditoři používají manuální automatizované nástroje, datově analytický software nebo vylepšené auditní procedury, informační technologie dosud pouze pomáhají auditorům v jejich provádění auditu. Jsou používány algoritmy pro zjišťování zvláštností, nepravidelností či odchylek, které představují transakce, které nesplňují předpokládaná stanovená pravidla, nebo jsou odlišné vzhledem ke svým odlišnostem a jsou považovány za rizikové (ač mohou i nemusí být chybné či podvodné).

Na základě výzkumů se ukázalo, že takové analytické procedury prováděné na počítači jsou mylně považovány za automatizaci auditu, protože takové techniky ve skutečnosti nepředstavují automatizovaný audit. Analytické nástroje pouze vyhodnocují případné odchylky od stanovených pravidel a odchylky jsou následně manuálně zkoumány auditory, takový proces může výrazně ohrozit efektivitu auditora (Chan, Chiu a Vasarhelyi, 2018, s. 315). Současné nástroje nejsou schopny významně pomoci auditorům v samotné automatizaci auditu (Issa, Sun a Vaserhelyi, 2016).

Aby v budoucnu došlo ke skutečné automatizaci auditu, auditované společnosti musí zahájit digitální transformaci a eliminovat použití papírové dokumentace pro své interní i externí procesy, aby počítače mohly číst, porozumět a provádět auditorské postupy na základě dat ve strojově čitelné podobě. Takový audit může být realizován pouze v případě, pokud jsou implementovány určité obecně uznávané datové standardy (Vasarhelyi, Warren, Teeter a Titera, 2014).

Za samotný datový standard lze považovat např. XBRL – otevřený a volně dostupný standard a jazyk pro výměnu obchodních a finančních dat. Jeho využití se nabízí v účetním výkaznictví, pro sdílení informací s okolím podniku i sdílení nefinančních informací. Zavedením dochází k významnému snížení spotřeby lidských, časových i finančních zdrojů. Použitím standardu není požadováno po společnostech vykazovat další informace než před použitím jazyka, změní se pouze formát výkazu, který bude díky XBRL strojově čitelný. Jazyk tak pouze zprostředkovává požadavky jednotlivých účetních standardů.

Graf 2: Vliv použití XBRL na efektivnost v rámci organizace



zdroj: Hoffman a Watson, 2009, s. 51

V budoucnu lze očekávat, že auditoři budou klást mnohem větší důraz na prověřování spolehlivosti různých informačních systémů, senzorů a dalších nástrojů, které mají vliv na reporting účetních dat. Větší důraz na tuto problematiku by tak měl být kladen již při tvorbě studijních vzdělávacích plánů.

1.4.1 Smart Audit Procedures

S rozvojem nových technologií, a vzestupu vyžití big data, umělé inteligence, strojového učení a zpracování dat, internetu věcí a služeb dochází v auditingu k vývoji, který je také nazýván Smart Audit Procedures[7]. Proto neustále roste zapojení datových analýz prováděných během externího auditu. Mezi prvopočátky datové analýzy z osmdesátých let 20. století řadíme analýzu vývojových trendů a analýzu finančních ukazatelů.

[7] V angličtině jsou často používány také pojmy Continuous Audit a Audit Automation.

S vývojem softwarových auditorských aplikací, primárně určených pro interní auditu, jako např. IDEA, došlo k dalšímu sofistikovanějšímu rozvoji v oblasti testování populace dat, kterou lze označit za druhou generaci datové analýzy. Dnes už se postupně rodí třetí generace datové analýzy (Appelbaum a kol., 2017).

Především díky Blockchainu a použití Smart contracts se schyluje k reportingu v téměř reálném čase. Použití Smart contracts mají potenciál zlepšit kvalitu auditu a zmírnit rozdíly v očekávání mezi auditory a steakholdery. Zároveň ale tvoří nová rizika a vyvolává otázku spolehlivosti (Rozario a Vasarhelyi, 2018). Spolehlivost nově vytvořených testů by měla být ověřována podle IAASB ex-ante i ex-post.

1.4.2 Robotická automatizace procesů

Americký Institut pro elektrotechnické a elektronické inženýrství (Institute of Electrical and Electronics Engineers, zkr. IEEE) definuje robotickou automatizaci procesů (angl. Robotic Process Automation, zkr. RPA) jako „Předem nakonfigurovaný příslušný software, který používá pravidla a předdefinované chování k provádění kombinace procesů, činností, transakcí a úkolů za použití jednoho nebo více softwarových systémů, aby poskytl výstupy s použitím řízení pomocí výjimek[8].“ (Moffitt, Rozario a Vasarhelyi, 2018).

Zjednodušeně můžeme definovat RPA jako automatizované úkoly, které za lidi provádí roboti. Na konkrétním příkladu robot může být přirovnán k vytvořenému makru v Microsoft Excel, které automatizuje specifické úkoly. RPA může být nakonfigurovaný na jakýkoli software a může tak za uživatele posílat emaily nebo vkládat data do podnikových systémů. Manuální a často se opakující auditorské úlohy jako jsou sesouhlasení účtů, inventury, nebo procesy konfirmací účetních zůstatků, testování vnitřního kontrolního systému a detailní testy mohou být automatizovány. Takovéto procesy jsou v praxi často prováděny ve zmiňovaném Microsoft Excel s použitím makra nebo s pomocí analytického software CaseWare IDEA, který již ve výchozím balíku obsahuje předdefinované procesy usnadňující auditorské úlohy. Větší uzpůsobení nabízí programovací jazyky Python nebo R, k jejich používání je ale třeba zkušené vývojáře.

[8] Anglický pojem Management by Exception je technikou managementu, kdy se výstupy procesů či úkolů dělí na běžné a výjimečné či nestandartní., pouze takovým je následně věnována pozornost.

Obrázek 2: Využití RPA napříč obory

zdroj: PwC Robotic Process Automation, 2018, vlastní zpracování

Za nejvýznamnější přínos robotické automatizace procesů v podmínkách auditu je považována úspora času věnovaného často opakovaným procesům. Díky tomu řeší pouze odchylky ve výstupech automatizovaných procesů a mohou se zaměřit na náročnější a komplexnější problémy (např. odhady a oceňování) či důležitá rozhodnutí. Mezi další výhody patří i spolehlivost a doložitelná auditní stopa, tedy důkazní materiál o provedení operací.

Automatizací dochází v podnicích ke zkracování času mezi vystavením faktury a platbou nebo mezi objednávkou a dodáním. Vývojáři stále vylepšují tento systém implementací vč. umělé inteligence. Argumentem proti zavádění automatizovaných procesů je nahrazování zaměstnanců roboty. Případové studie předpovídají, že podniky budou v budoucnu schopny rozšiřování bez nutnosti přijímání nových zaměstnanců (Chappell, 2007). Naopak vzroste poptávka po odbornících, kteří budou spravovat a implementovat takový software.

Tabulka 2: Srovnání tradičního a budoucího přístupu v auditu

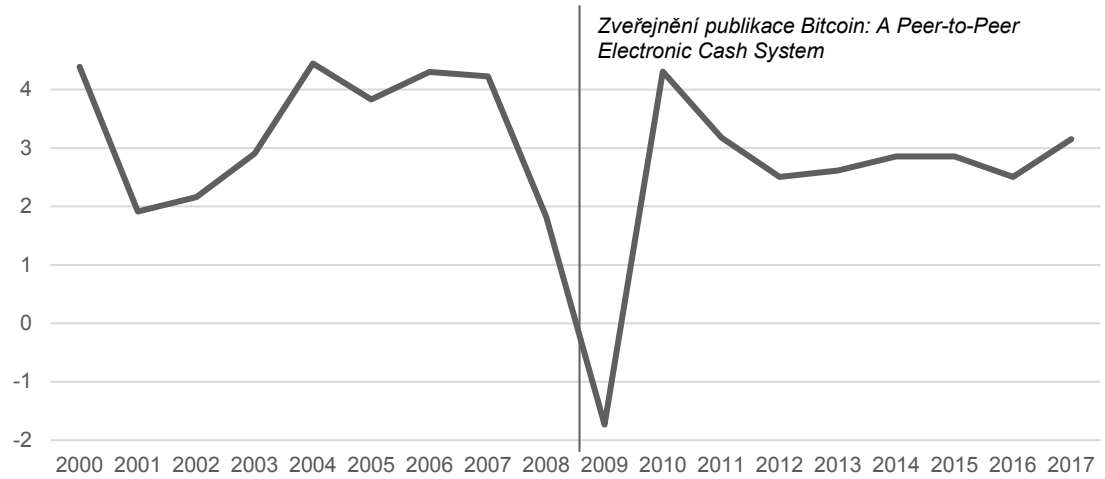
	Tradiční audit	Budoucí audit
Frekvence provádění auditu	Periodicky	Průběžně, téměř nepřetržitě
Přístup	Reaktivní	Proaktivní
Procedury	Manuální	Automatizované
Práce a role auditora	Velké množství práce vyžaduje intenzivní vynaložení úsilí na samotné provedení auditních procedur	Práce se zaměřuje na řešení výjimek zjištěných automatizovanými procedurami a procedurami vyžadující lidské posouzení
Charakter, načasování a rozsah	Testování spočívá v analytických testech a testech věcné správnosti, testy kontrol jsou prováděny nezávisle a k testování jsou vybírány vzorky	Testování spočívá v nepřetržitých kontrolách a kontrole zabezpečení dat, testy kontrol jsou prováděny souběžně a celá populace je testována
Testování	Testování provádí primárně lidé	Významné zapojení informačních technologií a datových analýz pro monitorování a testování
Vykazování	Periodicky	Průběžně nebo častěji

zdroj: Chan a Vaserhelyi, 2018, vlastní zpracování

2 Vymezení kryptoměn a Blockchain

Historie Bitcoinu se datuje od doby světové finanční krize v roce 2008. V první polovině téhož roku došlo ve Spojených státech k převzetí akcií banky Bear Stearns gigantem JPMorgan Chase v hodnotě 2 dolary za akcii, rok před touto transakcí se jedna taková akcie obchodovala za 170 dolarů. Druhá největší banka dle tržní kapitalizace – Bank of America převzala největší investiční banku Merrill Lynch za 50 mld. dolarů. Americká vláda spustila program na pomoc bankám od krachu, a to nákupem toxických aktiv (Burniske a Tatar, 2018), což představovalo rizikové půjčky zákazníkům se špatnou platební morálkou a neodpovídajícími zárukami, kteří nebyli schopni dostát svým závazkům. Tato toxická aktiva byla následně prodávána bankám a investorům po celém světě formou obligací krytých zástavou, tzv. collateralized mortgage obligation. Postupem času se dlužníci dostávali do neschopnosti hradit své dluhy, to vyvolalo další zadlužování, které označujeme jako dluhovou spirálu vedoucí k osobnímu bankrotu. Protože hodnota úvěrových zástav byla nízká, zapříčinilo to postupně krach bankovních institucí a vznik světové finanční krize. Ve druhé polovině roku došlo k bankrotu Lehman Brothers, jedné z největších investičních bank ve Spojených státech. Celkem vláda Spojených států vynaložila na záchranu bank 2 500 mld. dolarů. Jen v roce 2008 v USA ztratilo práci 2,6 milionu lidí (Uchitelle, 2009), za celou dobu trvání krize o práci přišlo téměř 9 milionů lidí podle americké Bureau of Labor Statistics. To vedlo v růst nedůvěry veřejnosti v bankovní systém a etiku jejich managementu.

Graf 3: Dopad světové finanční krize na vývoj světového HDP v %



data: Světová banka, Worldbank.org, 2018, vlastní zpracování

2.1 Kryptoměny

Kryptoměny jsou definovány jako virtuální elektronická měna či digitální aktivum, jejíž transakce jsou kryptograficky[9] zabezpečeny (Technopedia). Kryptoměny jsou alternativní digitální měnou s decentralizovanou[10] kontrolou jako protiklad k tzv. fiat měnám (tzn. měnám s nuceným oběhem) v systému centrálního bankovnictví. Kryptoměny tedy nejsou regulovány žádnou institucí či zemí. (Tapscott a Tapscott, 2016, s. 5)

2.1.1 Bitcoin, bitcoin

Bitcoin představuje virtuální měnu a zároveň platební systém. V říjnu 2008 byla zveřejněna devítistránková publikace Bitcoin: A Peer-to-Peer Electronic Cash System pod pseudonymem Satoshi Nakamoto, světu dosud neznámou osobou nebo uskupením. Doména Bitcoin.org byla zaregistrována 18. srpna 2008. Je důležité rozlišovat odlišnost velkého a malého písmene počátečního písmene:

- Bitcoin: peer-to-peer platební systém, kterým jsou prostředky převáděny bez účasti centrální autority, která by se zaručovala za kryptoměnu nebo měla možnost „tisknout“ nové peníze; software s otevřeným zdrojovým kódem (open-source),
- bitcoin: jednotka virtuální měny.

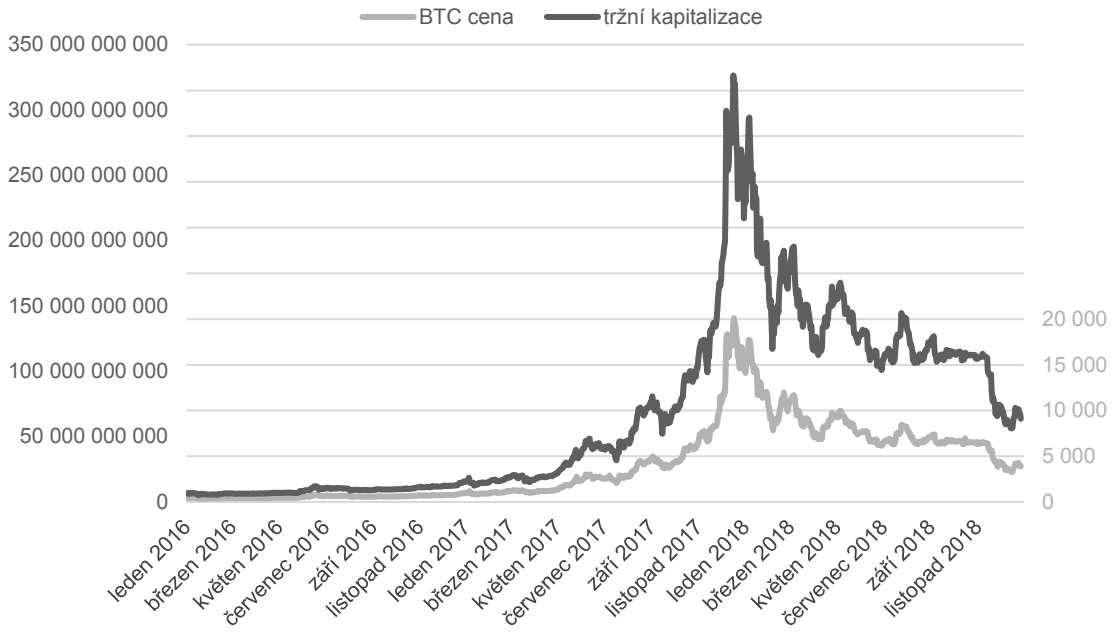
Bitcoin funguje na technologii Blockchain („řetězec bloků“), což je digitální sdílená účetní kniha fungující na bázi distribuované databáze zaznamenaných informací, tedy soubor souvislého záznamu na sobě vázaných či řetězených transakcí (bloků) s ověřitelnou neporušitelností, kterou si může ověřit každý vyhledáním jakékoliv již uskutečněné transakce. Každý jednotlivý blok obsahuje časové razítko a provázanost použitím „otisku“, není tudíž možné transakce zpětně upravovat nebo vymazat.[11]

[9] Kryptografie je disciplína, která se zabývá šifrováním, tzn. převodem zpráv do/z utajené podoby, která je čitelná pouze se znalostí šifrovacího klíče. Pokud klíč k zašifrování není stejný jako klíč k dešifrování, jedná se o asymetrickou kryptografii. (Stroukal a Skalický, 2015, s. 21)

[10] Architektura peer-to-peer, P2P či klient-klient je označení typu počítačové sítě, kde spolu komunikují klienti napřímo tzn. jedná se o decentralizovanou komunikaci. Protikladem je architektura klient-server (tak fungují např. webové stránky).

[11] V případě finanční krize v r. 2008 by blockchain pomohl svou provázaností identifikovat investorům a bankám rizika spojená s nákupem obligací krytých zástavou. Jednoduše by účastníci měli možnost zobrazení detailních informací o skladbě jednotlivých instrumentů.

Obrázek 3: Vývoj tržní kapitalizace a ceny Bitcoinu (v USD)



zdroj: CoinMarketCap.com, k prosinci 2018, vlastní zpracování

2.1.2 Další kryptoměny

Vzhledem k úspěšnosti Bitcoinu došlo k významnému rozšíření kryptoměn. Některé přišly s novými alternativními technologiemi a mají tak šanci uspět, jiné pouze kopírují zdrojový kód bitcoinu. Databáze CoinMarketCap.com eviduje již více než dva tisíce kryptoměn. Následující tabulka shrnuje deset nejvýznamnějších kryptoměn řazených dle jejich tržní kapitalizace.

Tabulka 3: Kryptoměny dle tržní kapitalizace

#	Vlastnost	Symbol	Tržní kapitalizace v USD	Cena v USD
1.	Bitcoin	BTC	66 798 675 136	3 829,63
2.	XRP	XRP	15 651 342 127	0,38
3.	Ethereum	ETH	13 514 375 132	129,95
4.	Bitcoin Cash	BCH	3 032 356 936	172,99
5.	Stellar	XLM	2 372 049 162	0,12
6.	EOS	EOS	2 363 862 056	2,61
7.	Tether	USDT	1 886 717 928	1,02
8.	Litecoin	LTC	1 875 272 577	31,40
9.	Bitcoin SV	BSV	1 639 759 454	93,55
10.	TRON	TRX	1 337 511 594	0,02

data: CoinMarketCap.com k 25. prosinci 2018

Ethereum

Ethereum je kryptoměna spuštěná v roce 2015[12] fungující taktéž na Blockchainu, tzn. že uchovává neustále se zvyšující počet záznamů. Jedná se o decentralizovaný virtuální stroj (angl. Ethereum Virtual Machine) fungující na tisících zařízení. Pro ověřování transakcí je používán výpočetní výkon těžařů metodou Proof of Work (stejně jako Bitcoin).

Primární cíl Etherea nebyla tvorba nové kryptoměny k provádění platebního styku, ale jeho využití k ukládání zdrojových kódů a aplikací na něm postavených a jejich zavedení do praxe. Takové aplikace mají podobu chytrých kontraktů, tzv. Smart contracts[13]. Tím se liší od Bitcoinu, jehož Blockchain sleduje transakce s měnou bitcoin. Dalším významným rozdílem je průměrný čas potřebný k vytěžení jednoho bloku – v případě Bitcoinu se jedná přibližně o deset minut, ale ethereum těží nový blok každých 12 sekund, čímž je potvrzování transakcí značně rychlejší.

2.1.3 Regulace kryptoměn

Kryptoměnové transakce vzhledem k jejich povaze digitálních peněz probíhají po celém světě. Zástupci centrálních bank a ministři financí G20 na summitu v argentinském Buenos Aires v březnu 2018 doporučili regulaci odvětví s cílem omezit anonymitu spojovanou s financováním terorismu, daňovými úniky a praním špinavých peněz a regulací tak lépe tak chránit investory a jejich uživatele. Usnesli se také, že z důvodu absence atributů měny nepovažují kryptoaktiva za suverénní měnu. (G20, 2018).

Největším regulátorem kryptoměn je Čínská lidová republika, těžba na jejím území je ilegální. V roce 2016, rok před zákazem těžby, tvořil výpočetní výkon těžařů z Číny více než poloviční podíl všech těžařů Bitcoinu na světě s podílem 58 % (Hileman a Rauchs, 2017). Ve Spojených státech amerických regulace dovoluje vydávat finanční deriváty – futures kontrakty na Bitcoin, což umožňuje nepřímo ovlivňovat ceny kryptoměn bez toho, abychom je vlastnili. To způsobilo příliv nového kapitálu. Společnosti obchodující s kryptoaktivy (burzy, ale i softwarové peněženky) se na základě rozhodnutí Komise pro cenné papíry a burzy v březnu 2018 musí registrovat a získat povolení od Komise (U.S. Securities and Exchange Commission, 2018). Evropský parlament v roce 2018 zpřísnil pravidla proti praní špinavých peněz, což ovlivní všechny burzy a směnárny, které musí zamezit provádění anonymních transakcí a ověřovat totožnost svých klientů.

[12] Koncem roku 2013 byl zveřejněný white paper rusko-kanadského programátora a autora Vitalika Buterina. Někdy bývá tato Ethereum označováno za kryptoměnu druhé generace nebo za Bitcoin 2.0.

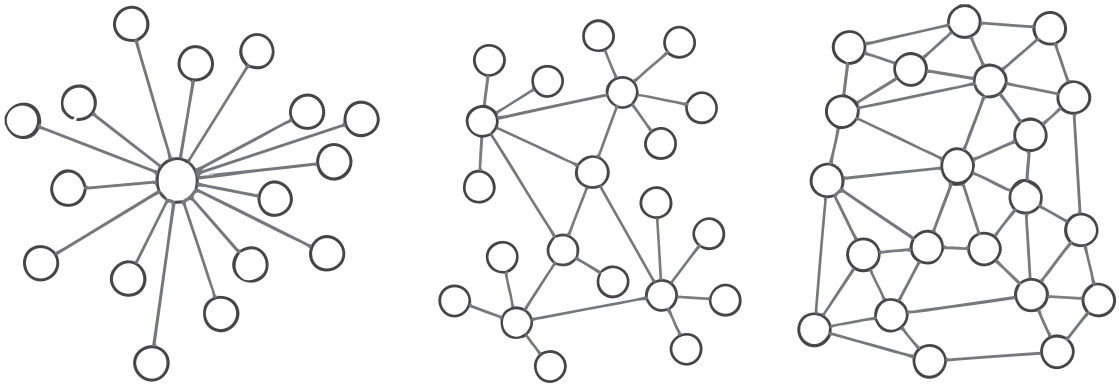
[13] Podrobně o tzv. chytrých kontraktech pojednává kap. 3.1 Smart contract.

V legislativním prostředí České republiky nelze kryptoměny považovat podle ustanovení zákona č. 284/2009 Sb., o platebním styku za elektronické peníze, protože peníze podle ustanovení tohoto zákona představují pohledávku vůči tomu, kdo je vydal. V případě kryptoměn jsou kryptoměny evidovány v Blockchainu s absencí centrální autority. Kryptoměny tak považujeme za nehmotné věci movité zaměnitelné podle ustanovení zákona č. 89/2012 Sb., občanský zákoník. Samotná těžba, tedy ověřování transakcí v síti, je považována za poskytování služeb, činnost vykazující znaky podnikání, a tudíž je k jejímu výkonu třeba živnostenské oprávnění (Hanych a kol., 2018).

2.2 Databáze

Databáze je definována jako soubor či množina strukturovaných záznamů (dat), které jsou organizovány za určitým účelem. Mezi její přínosy podle Kalčeva obecně řadíme rychlost, spolehlivost, přesnost a bezpečnost. Za předchůdce databází jsou považovány papírové kartotéky. Podle způsobu přístupu k databázi je dělíme na centralizované, decentralizované a distribuované.

Obrázek 4: Přístupové metody v sítích



zdroj: Kokina, Mancha a Pachamanova, 2017

Centralizovaná databáze představuje závislost na jednom datovém centru, přes které protékají veškeré informace. Jedná se o nejjednodušší řešení s použitím architektury klient-server. Problém tohoto typu přístupu v síti je zřejmý, při výpadku sítě (angl. single point of failure) přestane fungovat celá síť. Tento systém obvykle spravuje pouze malá skupina lidí, kteří mají velkou moc. Za předpokladu, že by Bitcoin fungoval na centralizované síti, nelišil by se od peněz a jeho hodnota by byla nulová (Matuszyński, 2018).

Decentralizovaná databáze nemá centrální bod a data tak nejsou umístěna na jednom místě, ale pracují s nimi všichni uživatelé sítě. Aby došlo k ohrožení sítě, muselo by dojít

k výpadku na všech počítačích v síti ve stejný čas. Pokud někdo znehodnotí obsah na jednom počítači, data jsou na všech ostatních. Distribuovaná síť ukládá veškerá data na všechny počítače. Komunikace mezi počítači probíhá na základě stanoveného protokolu a ke změně dojde až po shodě všech nebo většiny počítačů. Decentralizované sítě jsou současně i distribuované.

Tabulka 4: Rozdíly mezi centralizovanou a distribuovanou databází

Vlastnost	Centralizovaná databáze	Distribuovaná databáze
Náklady na provoz a údržbu *Náklady na ověřování transakcí a jejich přidání do databáze.*	$	$$$
Zprostředkovatelské náklady *Náklady spojené s přítomností důvěryhodné třetí strany.*	$$$	$
Transparentnost *Schopnost jednotlivých účastníků zobrazit data.*	✓	✓✓
Bezpečnost *Jak je obtížně vytvořit podvodné transakce (např. zneužitím).*	✓	✓✓

zdroj: The Future of Blockchain, Chartered Accountants Australia & New Zealand, vlastní zpracování

2.3 Blockchain

Blockchain je v informatice označení pro druh distribuované databáze[14] s neustále se rozšiřujícím počtem záznamů chráněných proti neoprávněnému zásahu. Použití kryptografie zajišťuje anonymitu a neoprávněné operace. Dosud je Blockchain spojován především s použitím v oblasti kryptoměn, tj. jako jejich účetní kniha, zároveň dochází k postupnému rozšiřování jeho použití pro tzv. Smart Contracts(3.1). Don Tapscott v jeho knize Blockchain definuje jako „*nezničitelnou síť ekonomických transakcí, která v budoucnu může sloužit nejen finančnictví, ale v podstatě všemu, co má hodnotu“*.

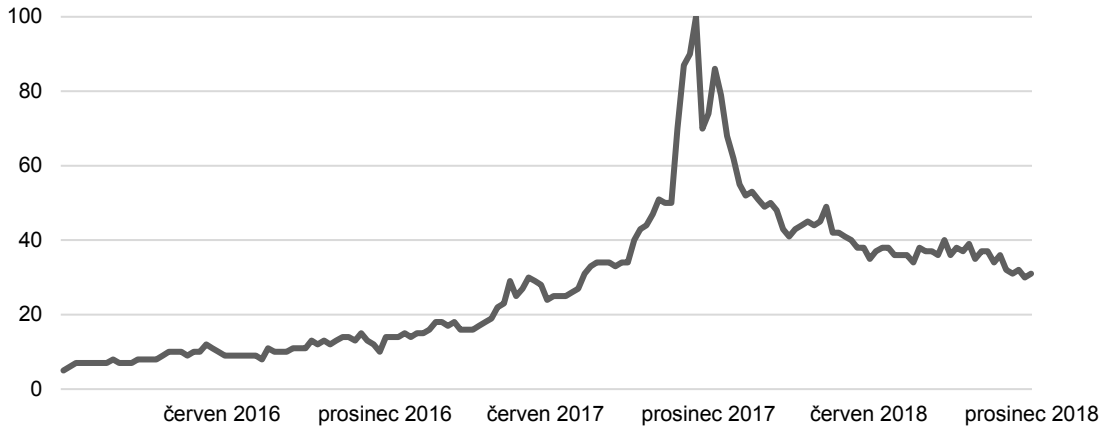
Decentralizace, tedy schopnost provádět transakce bez nutnosti schválení či asistence třetí strany (např. centrální banky) a odstraňování zprostředkovatelských mezičlánků v takovém procesu, vedoucí ke snižování provozních nákladů, je považována za klíčovou odlišnost Blockchainu. Další důležité charakteristiky definované na Světovém ekonomickém fóru v roce 2017 jsou transparentnost, tzn. že veškeré veřejné záznamy jsou dostupné všem tržním subjektům, a věrohodnost, protože každá transakce

[14] V angl. Mutual Distributed Ledger, chápáno jako společná distribuovaná „kniha“ transakcí sdílených v distribuované databázi řazené v chronologickém pořadí, které jsou postupně přidávány, ale nemohou být dodatečně zpětně změněny či odstraněny, k jejich vymazání či změně by byla potřeba další „účetní operace“.

v Blockchainu je ověřována a zaznamenána s časovým razítkem, uživatelé mohou jednoduše ověřit a zpětně vystopovat předchozí záznamy.

V roce 2017 proběhl v České republice projekt blockchain.cz, jehož cílem bylo vybrat vhodný český ekvivalent pojmu Blockchain. Nejdříve byl pojem překládán jako „řetězec bloků“, pro jeho těžkopádnost od něj ale bylo upuštěno. Hlasováním veřejnosti zvítězil pojem bločenka.

Graf 4: Četnost vyhledávání pojmu „Blockchain“ celosvětově v letech 2016-2018



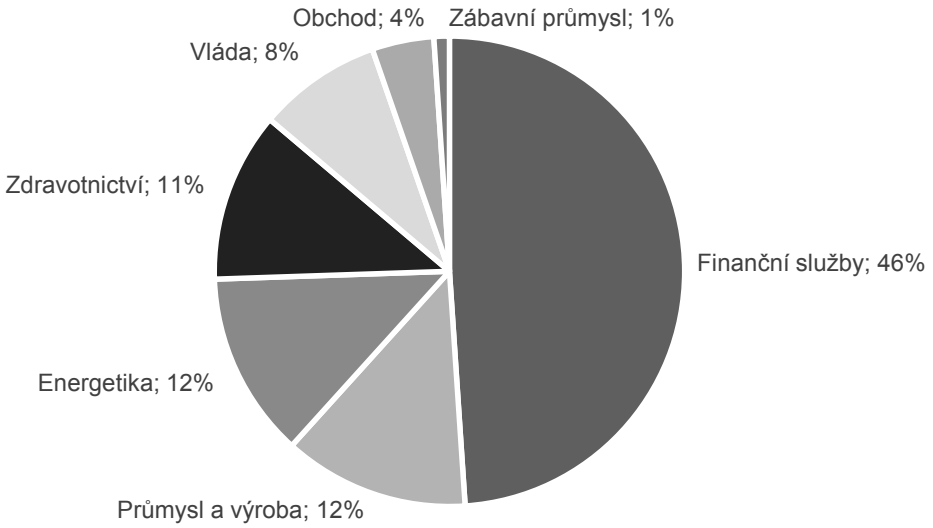
zdroj: Google Trends k prosinci 2018, vlastní zpracování

Aktuální průzkumy o Blockchainu

Podle celosvětového průzkumu poradenské společnosti PwC, provedeném v roce 2018, bylo dotazováno šest set vedoucích pracovníků[15], podle kterých se největší využití Blockchainu očekává ve finančnictví.

[15] V angličtině jsou často používány pojmy VPs, tj. Vice Presidents, kteří mají v podnikové struktuře nižší postavení, než hierarchicky výše postavení C-Suite či C-Level, tzv. výkonní pracovníci: CEO - Chief Executive Officer, tj. výkonný ředitel, CFO - Chief Financial Officer (finanční ředitel), mezi další patří např. Chief Accounting Officer, Chief Marketing Officer nebo Chief Information Officer.

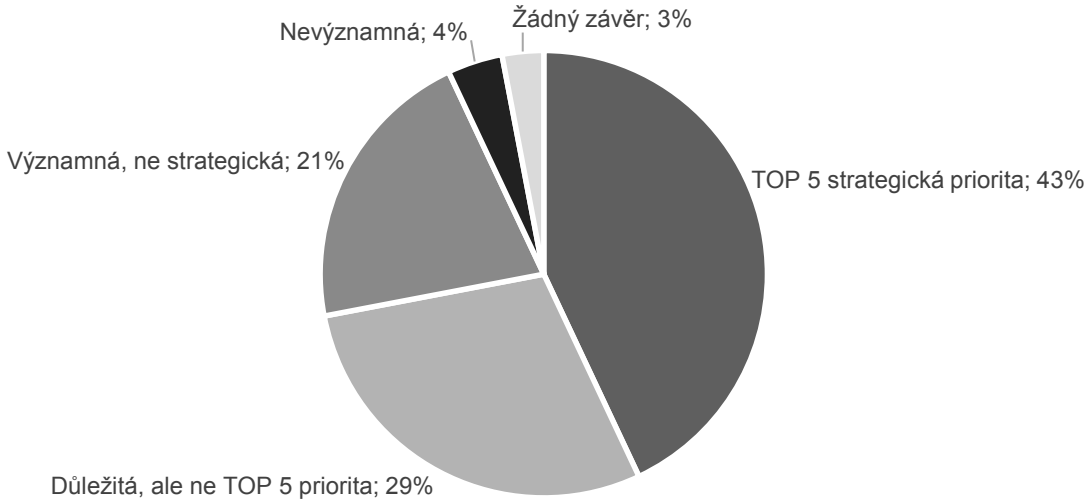
Graf 5: Očekávané využití Blockchainu v jednotlivých segmentech



zdroj: PwC's Global Blockchain Survey 2018, vlastní zpracování

Průzkum poradenské společnosti Deloitte dotazoval v roce 2018 přes tisíc vedoucích pracovníků primárně finančního, technologického, zpracovatelského průmyslu a zdravotnictví napříč největšími ekonomikami světa.

Graf 6: Význam Blockchainu pro danou společnost



zdroj: Breaking Blockchain open: Deloitte's 2018 Global Blockchain Survey, vlastní zpracování

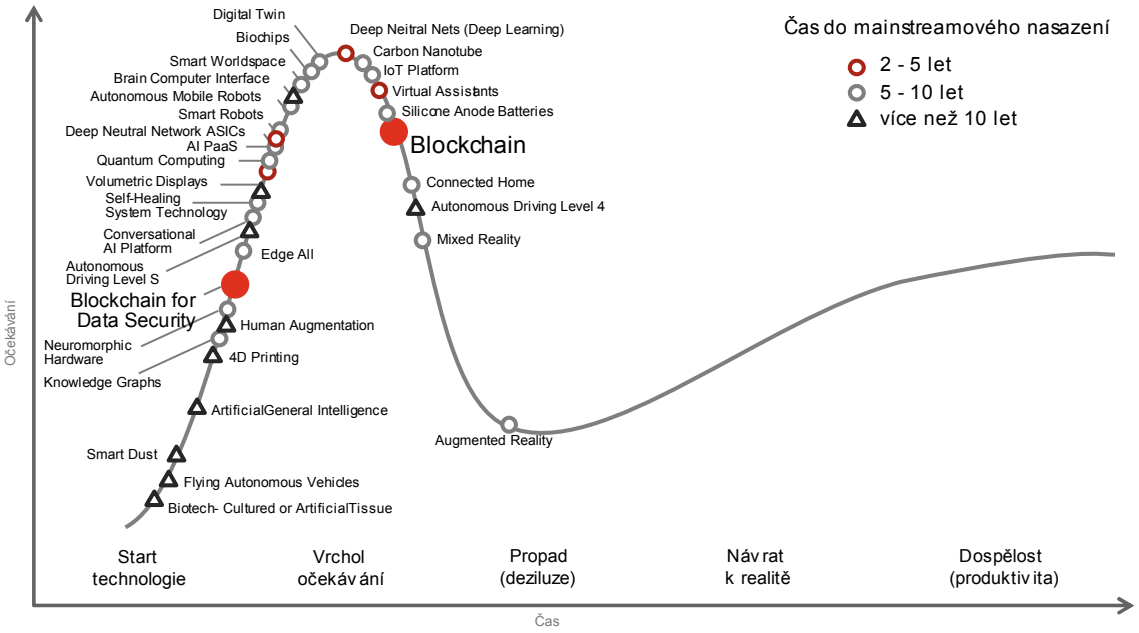
Hype křivka

Hype křivku či cyklus poprvé definoval americký vědec Roy Amara, podle jehož zákona ze sedmdesátých let „máme sklon přeceňovat význam nových technologií v krátkodobém horizontu a podceňovat jejich dopad v dlouhodobém horizontu". Několikrát ročně aktualizovaný výzkum publikovaný poradenskou společností Gartner popisuje životní cestu a vývoj jednotlivých rodících se technologií a trendů až po jejich ustálení na trhu. Vertikální křivku lze rozčlenit podle časového určení na pět fází: start technologie, vrchol

očekávání, deziluze, návrat k realitě a dospělost (produktivita). Vertikální křivka představuje očekávání. Křivka má uživatelům v praxi sloužit jako nástroj k pochopení a uvažování o nových rodících se technologiích a také pro rozhodování, zda do nich investovat v souladu s jejich firemní strategií, ta může být trojího typu: technologičtí inovátoři, hlavní proud a konzervativci.

Je třeba zmínit i kritiku křivky vycházející z neexistujícího měřítka determinace očekávání vyjádřeném na vertikální ose. Zároveň je nutné brát v úvahu odlišné fáze technologií v závislosti na geografické lokaci, tzn. různé trhy a odvětví. Jedná se tak o dobře strukturovaný a vhodný doplněk k rozhodování o strategii organizací (Fenn a kol., 2017, s. 25-26).

Graf 7: Hype křivka – Blockchain



zdroj: Gartner Inc., srpen 2018, vlastní zpracování

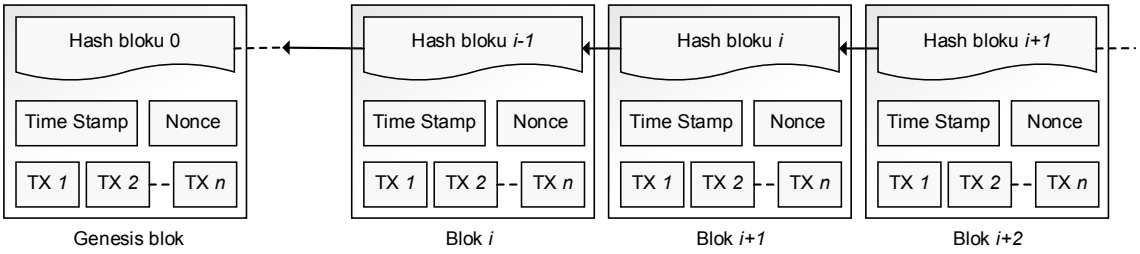
Podle Gartner Hype křivky se Blockchain nachází v raném stádiu a v současnosti prozatím disponuje omezenou distribucí. Společnost odhaduje implementaci chytrých kontraktů a masivní využití vlastností Blockchainu kolem roku 2020, později následně nástup tzv. decentralizovaných autonomních společností (angl. Decentralized Autonomous Organization/Corporation, zkr. DAO či DAC). Jedná se o nový druh společnosti, které s pomocí předdefinovaných chytrých kontraktů provádí rozhodování a řídí tak celý business (Dai a Vasarhelyi, 2017).

2.3.1 Struktura bloků

Transakce jsou realizovány po celém světě v různý čas a jejich záznam je přístupný ve stejný okamžik, proto jsou transakce zapisovány do Blockchainu v blocích. Protože se

jedná o distribuovaný systém, na validitě každého nového bloku se musí shodnout všichni těžaři, ti poskytují sítí výpočetní výkon a za nalezení každého nového bloku jsou odměněni. Tento proces kontroly a potvrzování transakcí je nazýván těžba (angl. mining).

Obrázek 5: Struktura bloků v Blockchainu



zdroj: Zheng a kol., 2018, vlastní zpracování

Previous Hash

Previous Hash představuje unikátní odkaz či referenci na předcházející blok. Každý nový blok je k bloku předchozímu přiřazen pomocí hashe obsaženého v předchozím bloku. U každého bloku je následně možné identifikovat předchozí blok. Jedinou výjimkou je první blok, zvaný Genesis block, v takovém případě je místo hashe předchozího bloku uvedena 0 (nula).

Time Stamp

Časové razítko určující přesný čas vytvoření bloku. Termín *block time* je doba mezi dvěma vydanými bloky. Např. Bitcoin vydává blok přibližně každých 10 minut, Ethereum každých cca 15 sekund. Některé systémy považují transakci za platnou až po vydání několika dalších bloků, kde je transakce již včleněna.

TX Root

Jedná se o souhrn všech uskutečněných transakcí obsažených v daném bloku. Alespoň jedna transakce je potřebná k vytvoření bloku.

Difficulty

Hodnota vyjadřující obtížnost, s jakou byl daný blok vytvořen. Pomocí algoritmu na automatizované bázi je hodnota pravidelně upravována tak, aby byl každý blok vytvořen po deseti minutách (v případě Bitcoinu) nezávisle na výkonnosti sítě. Výkonnost tedy roste, když roste výpočetní síla sítě a naopak.

Nonce

Náhodné číslo sloužící k ověření hashe, které může být využito pouze jednou.

Data Hash

Soubor všech výše uvedených dat, které jsou za pomocí hashovací funkce[16] převedeny na hash aktuálního bloku. Bitcoin používá algoritmus SHA-256, který je z libovolně dlouhého textu schopný vyprodukovat hash o 32 znacích. Jakákoliv změna původního vstupu vede k významné změně výsledného hashe. Neexistuje žádný způsob, jak z hashe začínající nulou zpětně získat původní zašifrovanou zprávu. Jedinou možností je zkusit původní zprávu uhodnout metodou pokus-omyl, což vyžaduje vynaložit určité úsilí[17]. Těžaři věnují síti výpočetní výkon, kterým daný kryptografický problém řeší. Kdo vyšle do sítě řešení jako první a jeho správnost je ověřena, může na konec Blockchainu přidat nový záznam, který je považován za platný.

2.4 Druhy Blockchainu

Blockchain může být podle přístupu do takové databáze kategorizován na veřejný (angl. permissionless) a neveřejný (angl. permissioned), ten ještě dále můžeme rozčlenit na soukromý a konsorcium (částečně soukromý)[18]. Veřejný Blockchain je přístupný bez potřebného povolení, tzn. každý může přidat nový blok do takového řetězce, může se zúčastnit i tzv. konsensus procesu, který určuje bloky, které budou přidány do Blockchainu[19]. Příkladem je Blockchain používaný jako účetní kniha Bitcoinu.

Soukromý Blockchain přidává oproti veřejnému navíc prvky kontroly, které jej mohou činit více atraktivní pro použití ve firemním prostředí, protože firmy střeží velké množství citlivých údajů a soukromí dat je klíčová výhoda soukromého Blockchainu. Přístup do takového Blockchainu má pouze firma a pouze uživatelé s přiděleným přístupem mohou přidávat nové transakce do Blockchainu.

Konsorcium představuje sdružení několika definovaných subjektů. Konsensus proces obsahuje předem stanovené uzly a aby byly platné, tak každý z nich musí jednotlivé bloky podepsat. Právo na čtení obsahu může být veřejné i omezené.

---

[16] Hashovací funkce (angl. Secure Hash Algorithm, zkr. SHA) je matematický algoritmus, který z prakticky neomezeně dlouhých vstupních dat vytvoří výstup předem stanovené délky – hash či otisk. Zásadní výhodou je, že i malá změna vstupu vede k velké změně výstupu – odlišného otisku, čímž zajišťuješ integritu dat.

[17] Více viz. Subkapitola 2.6 Konsensus algoritmu.

[18] Takto je poprvé rozdělil tvůrce kryptoměny Ethereum Vitalik Buterin.

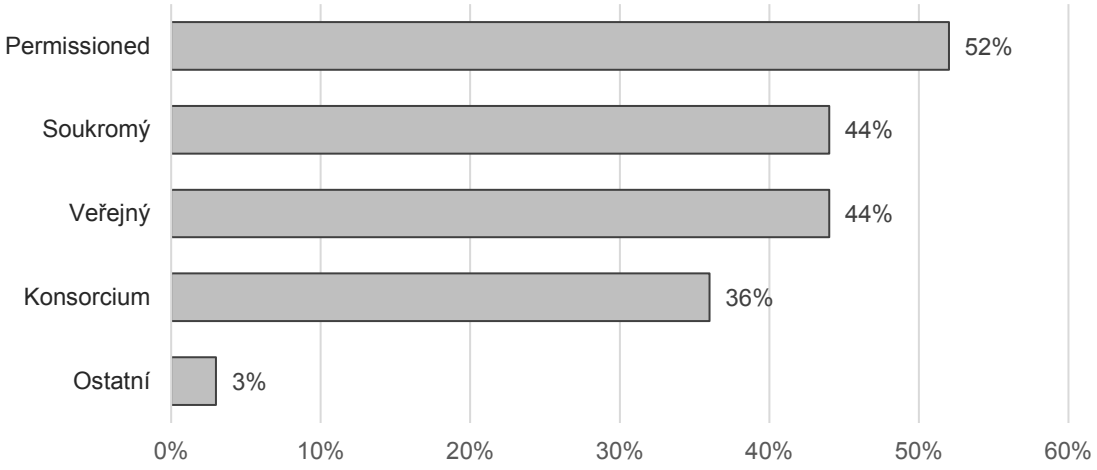
[19] Podrobněji o tomto problému pojednává subkapitola 2.6 Konsensus algoritmu.

Tabulka 5: Srovnání veřejného, soukromého a konsorcium Blockchainu

Vlastnost	Blockchain		
	Veřejný Public (Permissionless)	**Soukromý** Private (Permissioned)	**Konsorcium** Consorcium (Permissioned)
Ověřování transakcí	Všichni uživatelé	Definovaná (malá) skupina uživatelů	Uživatelé uvnitř organizace
Čtení obsahu	Veřejně dostupný	Veřejný nebo omezený	Veřejný nebo omezený
Neměnnost *(stálost dat)*	Téměř nemožné zfalšovat	Může být zmanipulováno	Může být zmanipulováno
Efektivita	Nízká	Vysoká	Vysoká
Centralizace	Decentralizovaný	Plně centralizovaný	Částečně centralizovaný
Konsensus proces	Kdokoliv bez potřebného povolení	Pouze uživatelé s přiděleným právem	Pouze uživatelé s přiděleným právem

zdroj: Zheng a kol., 2018, vlastní zpracování

Graf 8: Na jaký druh Blockchainu zaměřují pozornost firmy v roce 2018



Respondenti měli možnost vybírat více možností k odpovědi, proto součet přesahuje 100 %.

zdroj: Breaking blockchain open: Deloitte's 2018 Global Blockchain Survey, vlastní zpracování

2.5 Blockchain 1.0 – 3.0

Od představení Blockchainu v roce 2008 můžeme jeho vývoj rozdělit na tři zásadní etapy (Swan, 2015). V první fázi byl Blockchain používán do roku 2014 primárně k obchodování s kryptoměnami. Funkce jako zasílání a přijímání plateb utvořily nový systém tzv. „Internetu peněz". Blockchain druhé generace zahrnuje taktéž obchodování s kryptoměnami, ale v mnohem širším měřítku ve spojení s aplikacemi v oblasti

vlastnictví digitálního obsahu nebo Smart property[20]. Pozornost je věnována tzv. Smart contracts[21]. Blockchain 3.0 posouvá tento systém za hranice aplikace ve financích. Blockchain je v současnosti implementován jako volební systém, jako systémy v cloudových úložištích, jako atestační služby či v leasingu. Ve spojení s internetem věcí tak umožňuje kontrolu fyzických objektů a provádění služeb pomocí zmíněných chytrých kontraktů, což vede k automatizaci, flexibilitě a efektivního životního stylu. (Swan, 2016)

2.6 Konsensus algoritmu

Bez účasti centrální autority v Blockchainu je nutné zajistit, aby záznamy v jednotlivých uzlech v síti byly konzistentní. K zajištění konsensu jsou používány protokoly, které zároveň určují odměnu těžaři za vytvoření a ověření bloků (Castor, 2017). Jedná se o soubor pravidel specifikující, jak těžaři zužitkují jejich počítače ke tvorbě bloků, dosažení konsensu (ověření bloků) a odměnu, kterou za tuto činnost dostanou. Dva hlavní protokoly jsou Proof-of-work (dále také PoW) a Proof-of-stake (PoS).

2.6.1 Proof-of-work

Jedná se o první algoritmus použitý v oblasti kryptoměn. Těžaři je řešen složitý matematický problém zahrnující ověření provedených transakcí k ověření následné ukládání do řady bloků v Blockchainu. Tuto metodu používá kryptoměna Bitcoin a za výhodu je považována její ověření v čase. Nevýhodou jsou vysoké nároky na spotřebu elektrické energie k provádění náročných výpočtů, což představuje časově zdlouhavý proces.

Odhaduje se, že roční spotřeby elektrické energie na těžbu bitcoinu představuje 68,81 terawatthodiny, což je hodnota srovnatelná s roční spotřebou České republiky. (ČTK, 2018)

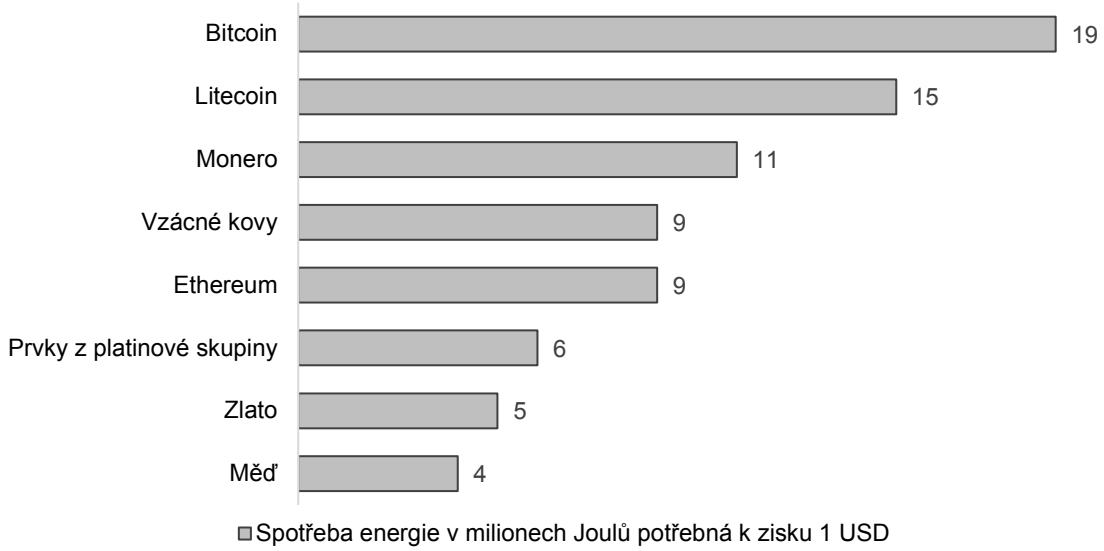
Podle studie Oak Ridge Institute publikované v Nature Sustainability množství energie k získání jednoho amerického dolaru z těžby kryptoměn je více než dvojnásobné v porovnání se získáním stejné hodnoty v těžbě zlata nebo jiných vzácných kovů, čímž se virtuální těžba přibližuje k té skutečné. Studie dále uvádí, že spotřebovaná energie

[20] Smart Property (česky chytrý majetek) je majetek, jehož vlastnictví je evidováno v blockchainu. Majetek může mít hmotnou podstatu, např. domy či auta, ale i nehmotnou podstatu, např. akcie. Digitální stopa může mapovat historii vlastnictví majetku, jeho umístění i další detaily.

[21] Smart Contracts (tzv. chytré kontrakty) představují protokol či software, který nezávisle ověřuje, zajišťuje nebo vynucuje provedení určitého kontraktu (např. smlouvy nebo dohody). Podrobně je tento termín popsán ve třetí kapitole.

k těžbě bitcoinu za jediný rok je větší, než spotřeba celého Irska a vyprodukované emise uhlíku odpovídají jednomu milionu transatlantických letů. (Krause a Tolaymat, 2018)

Tabulka 6: Energetické náklady na těžbu kryptoměn



zdroj: Krause a Tolaymat – Quantification of energy and carbon costs for mining cryptocurrencies, 2018

2.6.2 Proof-of-stake

Algoritmus byl představen, stejně jako další algoritmy, s cílem nahradit původní proof-of-work. Proof-of-stake představuje alternativu k Proof-of-work s nižší energetickou náročností. Nové bloky se vytvářejí díky mincím (angl. coins), které jsou jako důkaz „vsazeny“ jejich vlastníky o platnosti nově vzniklých bloků. Čím více a déle coins kryptoměny účastník drží, tím je větší pravděpodobnost získání úkolu ověření transakce. Tato metoda vybízí uživatelskou základnu kryptoměny k vlastní ochraně sítě (Coyne a McMickle, 2017). Tento algoritmus využívá např. kryptoměna Ethereum.

2.6.3 Další algoritmy

V poslední době se spolu se vznikem nových kryptoměn objevila celá řada algoritmů pro schvalování transakcí, výčet některých z nich: Proof-of-Burn, Proof-of-Importance, Proof-of-Stake-Velocity, Proof-of-Capacity, Proof-of-Authority.

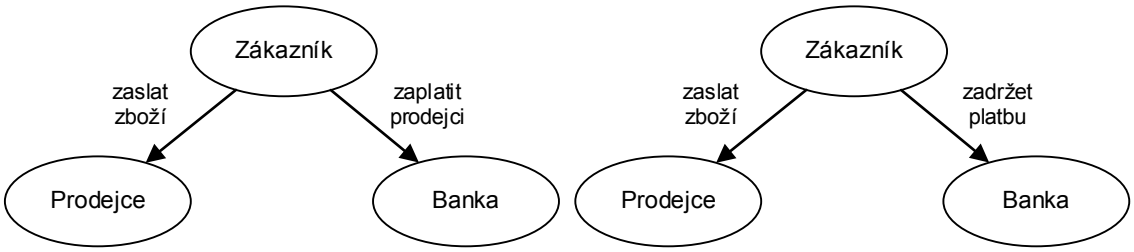
2.7 Omezení a výzvy Blockchain technologie

2.7.1 Problém dvou generálů

V souvislosti s kryptoměnami či elektronickými penězi vyvstává řada otázek. Jak synchronizovat platnou aktuální databázi („účetní knihu“)? Jak v případě konfliktních záznamů dosáhnout distribuované shody s absencí centrální autority (např. centrální banky), která by učinila rozhodnutí? A především jak v síti včas odhalit podvodníka?

Problém byzantských generálů, problém dvou armád či problém dvou generálů (angl. Byzantine Generals Problem) je teoretický experiment z roku 1982, který objasňuje, jak narušená komunikace ohrožuje jistotu dvou subjektů domluvit se (Lamport a kol., 1982). V následující situaci generál musí komunikovat svůj rozkaz několika poručíkům, kteří následně musí uposlechnout generálův rozkaz a řídit se jim. Problém nastává v situaci, kdy generál nebo některý z jeho poručíků představuje zrádce. Generál může vyslat poručíkům rozdílné rozkazy nebo některým nevyslat žádný. Za předpokladu, že poručíci spolu nemohou komunikovat navzájem, není možné garantovat, že se všichni budou řídit stejným rozkazem. Tento problém se vztahuje jednak k pochybení komunikace počítačových systémů, ale stejně tak i k lidskému selhání a Coyne a McMickle (2017) ho v účetním kontextu popsali následovně: Předpokládejme situaci, kdy je *v roli generála zákazník* a *dva poručíky představují prodejce a banka*, takový případ znázorňuje následující schéma.

Obrázek 6: Chování věrného zákazníka (vlevo) a zrádce



zdroj: Coyne a McMickle, 2017, vlastní zpracování

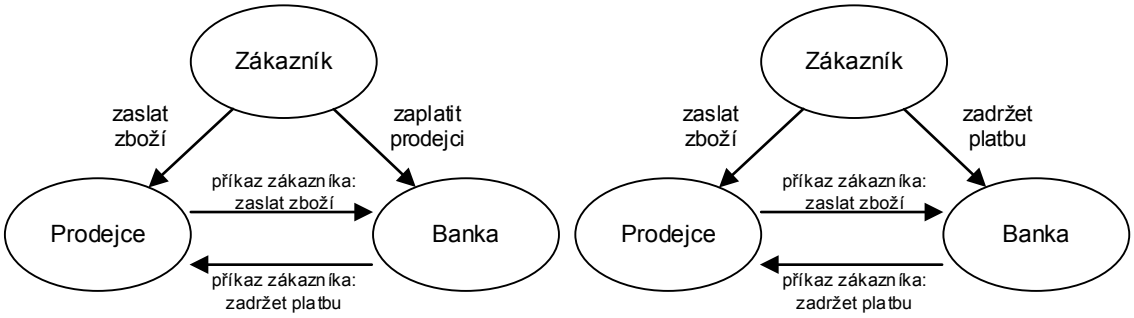
V prvním případě decentralizované komunikace si věrný zákazník objedná zboží od prodejce a zároveň bance zadá příkaz k úhradě[22]. Ve druhém případě nepoctivý zákazník objednává u prodejce a zároveň bance nedá příkaz zaplatit. Jelikož prodejce nemůže komunikovat s bankou, není tak schopen rozpoznat, zda se jedná o věrného či zrádného zákazníka. Obchod by nemohl proběhnout, protože jinak by prodejce vždy zaslal zboží, ale nedostal zaplaceno.

Prvním požadavkem k vyřešení výše popsaného problému je **vzájemná komunikace a ověřování příkazů** (transakcí), které poručíci obdrželi.[23] Věrný poručík bude poctivě komunikovat generálův rozkaz, ale poručík zrádce může změnit příkaz nebo část rozkazu zatajit, když ho sděluje ostatním poručíkům. Zrádcem může být generál i poručík.

[22] Rozkaz generála poručíkům by měl být identický, jednotný příkaz by mohl znít „výměna aktiv".

[23] Požadavek na dodatečnou komunikaci či ověření pouze mezi dvěma subjekty (generál a poručík) je nemožná, protože poručík nemá možnost určit, zda je generál zrádce. (Akkoyunlu, Ekanadham a Huber, 1975)

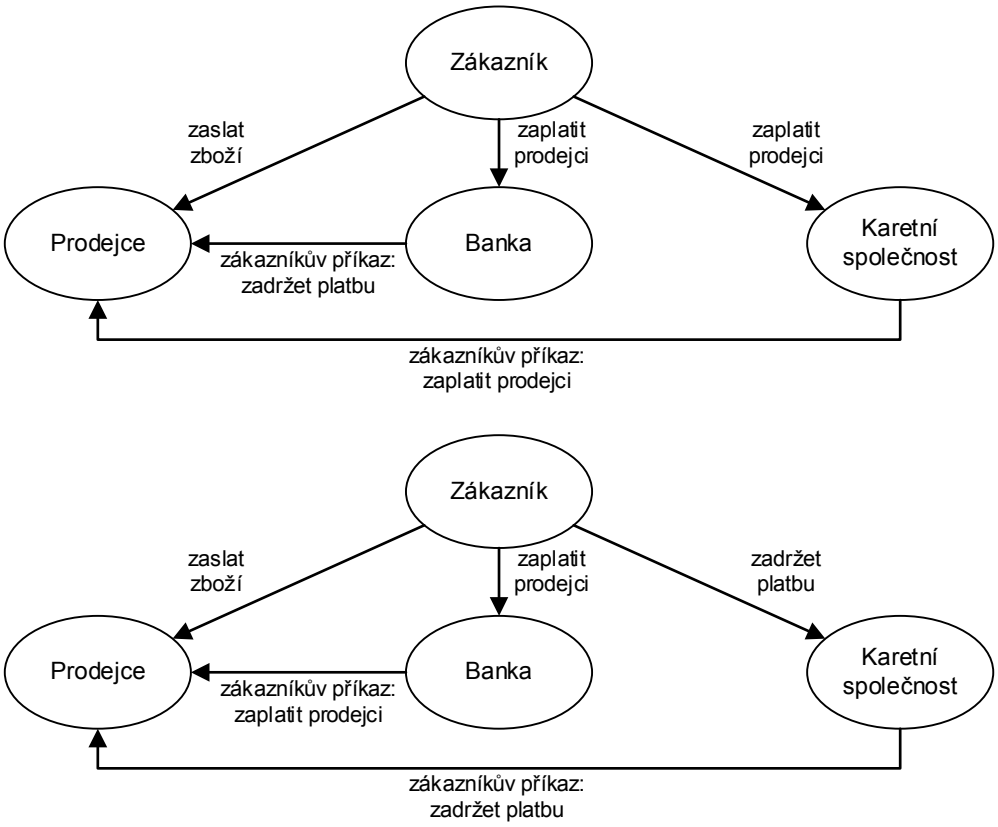
Obrázek 7: Chování věrného zákazníka a banky v role zrádce (vlevo) a naopak



zdroj: Coyne a McMickle, 2017, vlastní zpracování

V prvním případě nepoctivý zákazník objedná zboží u prodejce, ale bance nedá příkaz k úhradě. Ve druhém případě loajální zákazník objedná zboží od prodejce a dá bance příkaz zaplatit prodejci, ale banka zrádce sdělí prodejci, že od zákazníka nedostala příkaz k provedení platby. Prodejce tak nemůže určit, zda je zrádce zákazník nebo banka, ale prodejce v roli poručíka bude nucen odeslat zboží v obou případech. Problém lze řešit přidáním dalšího subjektu tak, aby počet věrných (loajálních) subjektů byl alespoň třikrát větší než počet zrádců.

Obrázek 8: Chování věrného zákazník a banky v role zrádce (nahoře) a naopak (dole)



zdroj: Coyne a McMickle, 2017, vlastní zpracování

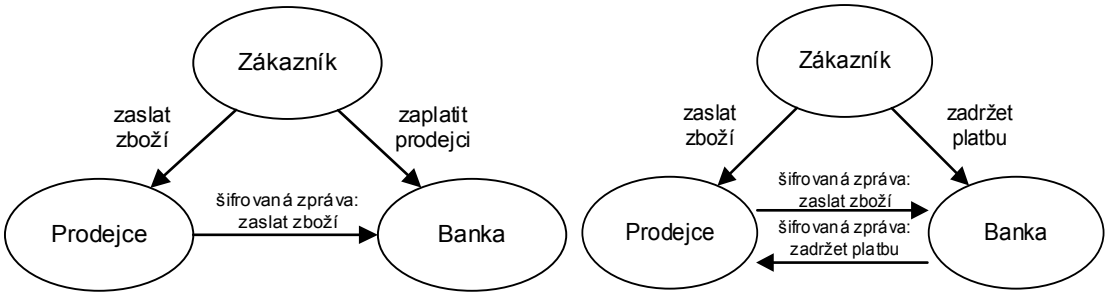
V pořadí třetí schéma zobrazuje, jak přidání jednoho věrného člena umožní dosažení konsensu v decentralizované síti. První, výše zobrazené schéma zobrazuje vztah čtyř

subjektů s jedním zrádcem. V prvním případě věrný zákazník s bankou-zrádcem a věrnou karetní institucí objednává u prodejce a zároveň přikazuje oběma subjektům zaplatit. Následně, ačkoliv banka-zrádce předává prodejci nepravdivou informaci, že od klienta nedostala příkaz k platbě, ale karetní instituce potvrzuje prodejci příkaz zaplatit. V distribuované síti bez existence centrální autority, která by rozhodla o pravdivém tvrzení, zvítězí většinové tvrzení, tzn. že by nastala výměna aktiv a došlo by k obchodu.[24]

Spodní schéma zobrazuje podvodného zákazníka, který karetní instituci nedá příkaz k platbě. I v tomto případě by na základě většinového tvrzení došlo k obchodu. Pokud by zákazník dal příkaz nezaplatit bance i karetní instituci, na základě většiny by k obchodu či „výměně aktiv" nedošlo.

V případě, že více než třetina členů v distribuované síti jsou podvodníci, síť nemůže fungovat. (Pease, Shostak a Lamport, 1980). Proto je dodatečná kontrola nezbytná k překonání tohoto problému tak, aby decentralizovaná síť o třech účastnících mohla fungovat i za přítomnosti podvodníka. Řešením je, aby každá modifikace rozkazu loajálního generála podvodným poručíkem mohla být odhalena, pokud generál příkaz podepíše nezfalšovatelným způsobem (tzv. **ověřením identity**). Pokud by zrádcem byl generál, každý poručík by dostal odlišný rozkaz, po následné vzájemné komunikaci mezi sebou by rozpoznali, že generál představuje zrádce. Jelikož poručík-zrádce nemá možnost modifikovat generálův rozkaz, jediný platný rozkaz, který může věrný poručík dostat je od věrného generála a poručík-zrádce by byl odhalen.

Obrázek 9:Věrný zákazník a banka v roli zrádce (vlevo) a naopak



zdroj: Coyne a McMickle, 2017, vlastní zpracování

Schéma zobrazuje, jak šifrované zprávy řeší problém spolupráce v decentralizované síti tří členů, kteří mohou komunikovat mezi sebou. V prvním případě banka-zrádce nemůže zmanipulovat zákazníkův příkaz a prodejce tak uposlechne zákazníkův příkaz. Ve

[24] Schémata pro zjednodušení zobrazují pouze komunikaci směrem k prodejci. Ve skutečnosti všichni členové dostanou kopii rozkazu, kterou dostali a komunikují ji navzájem.

druhém případě podvodného zákazníka banka předává zašifrovaný příkaz (nezaplatit) od zákazníka k prodejci, který následně identifikuje rozdílné rozkazy od zákazníka a ví tak, že zákazník je podvodník. Blockchain tak splňuje oba prvky řešení Problému byzantských generálů – vzájemnou komunikaci a ověřování identity v distribuované síti.

Problém byzantských generálů je tak vyřešen. Na základě použitého příkladu výše si zákazník objednává u prodejce zboží a do banky zasílá nezfalšovatelný kryptograficky podepsaný příkaz k platbě. Banka představuje síť, kde je spravována digitální kniha záznamů. Členové následně mezi sebou ověří transakci a přidají ji do řetězce záznamů. Následně je vysláno potvrzení prodejci o provedené platbě za zboží. Prodejce tak může zaslat zboží s jistotou, že zákazník není podvodník.

2.7.2 Problém dvojité útraty

Kopírování a problematika tzv. dvojité úhrady představuje velkou hrozbu pro svět digitálních měn. Fyzické peníze, na rozdíl od digitálních, existují v určitý okamžik na jednom místě a není možné je tak díky existenci centrální autority poslat dvěma subjektům najednou. V digitálním světě hrozí, že stejné peníze budou použity vícekrát. Digitální měna sama o sobě není schopna takovým problémům předcházet. Řešením je použití účetní knihy (jako je Blockchain) na základě řešení Problému dvou generálů. Vzhledem k absenci centrální autority Blockchain problém řeší problém tzv. hlasováním, které určí další soubor transakcí v řetězci. Jednotlivé metody byly popsány v subkapitole 2.6 Konsensus algoritmu.

2.7.3 51% útok

Situace, kdy dojde k ovládnutí více než poloviny výkonu sítě fungující na algoritmu Proof-of-work je nazývána 51% útok. V minulosti byla takováto forma útoku provedena na kryptoměnu Bitcoin Gold. Vzhledem k obrovské výpočetní síle sítě Bitcoin je v současnosti útok na tuto kryptoměnu nepravděpodobný. Ani použití veřejného Blockchainu firmami automaticky neznamená zajištění ochrany před zpětně proveditelnými změnami. Pokud by společnost použila veřejný Blockchain, neustále by byla vystavena tomuto riziku. Použitím soukromého Blockchainu by to ale znamenalo 100% kontrolu nad ověřováním transakcí, tzn. že hrozí riziko schopnosti zpětně přepsat jakoukoliv část Blockchainu (Rückeshäuser, 2017, s. 26).

Jedna z metod vedoucí k omezení výpočetní síly v síti by mohla představovat přizvání auditora k aktivní účasti v ověřovacím procesu, což by mohlo přesunout 50 % nebo více kontroly pryč z firmy (Coyne a McMickle, 2017).

2.7.4 Problém neoprávněných plateb

Jedná se o jeden z problémů spojených s kryptoměnami. Obecně tento problém postihuje každý platební systém. Držba hotovosti opravňuje držitele s nimi nakládat, ale hotovost může být odcizena nebo padělána. O to těžší je oprávnění v digitálním světě, protože se nabízí mnoho možností k podvodům.

Blockchain řeší problém neoprávněných plateb použitím kryptografického ověření pro každou transakci. Blockchain může představovat list platebních transakcí, které mají svého odesílatele a příjemce. Odesílatel musí digitálně podepsat transakci, čímž nezvratně stvrzuje jeho identitu[25].

2.7.5 Krádeže při provádění plateb

Blockchain nezabraňuje krádeži kryptoměn při jeho použití k platbám. Bezpečnost kolem kryptoměn je věnována soukromému klíči. Ten je jako jediný potřeba k nakládání s účtem a při jeho úniku lze převést veškeré kryptoměny. Soukromé klíče jsou ukládány v elektronických peněženkách, ačkoliv i data z těchto peněženek již byla napadena prolomením nedostatečného hesla nebo pomocí phising útoků[26].

2.7.6 Nevýhody či nedostatky

Blockchain je v současnosti pomalejší než jiné databáze, (Peck, 2017) proto jeho použití prozatím není vhodné v prostředí, kde je preferovaná rychlost informačního systému. Při použití konsensus algoritmu proof-of-work je zároveň náročný na spotřebu elektrické energie. Jedná se zároveň o novou technologii, která není v praxi hojně otestována a problematická může být tak i jeho implementace.

2.8 Porovnání ERP a Blockchainu

Srovnání Blockchainu s ERP systémy v praxi běžně používanými zvýrazní rozdíly a případné výhody této nově vznikající technologie. ERP sytém (z angl. Enterprise Resource Planning) je informační systém, pomocí kterého podnik řídí většinu oblastí své činnosti – plánování, zásoby, nákup, prodej, marketing, finance nebo personalistiku. Aplikace jednotlivých modulů dokáží komunikovat mezi sebou. Příkladem ERP systémů jsou SAP nebo Oracle či Helios.

---

[25] Rozkaz generála je potvrzen a zrádce tak nemůže modifikovat rozkaz bez toho, aby byl zjištěn. Viz. Problém dvou generálů.

[26] Phising je podvodná technika získávání přístupových údajů, čísel platebních karet a jiných citlivých údajů používaná na internetu. Pachatelé předstírají komunikaci důvěryhodné instituce (banka, sociální síť, IT oddělení uvnitř společnosti či úřad státní správy) směrem k důvěřivé veřejnosti.

ERP systém je považován za jednu z nejdůležitějších inovací v podnikovém použití databází (Davenport, 1998). Použitím ERP systému dochází k automatizaci procesů mnoha podnikových transakcí, systém zároveň poskytuje přesná data pro podporu manažerského rozhodování.

Tabulka 7: Rozdíl mezi ERP a Blockchain

ERP	Blockchain
Centralizovaná databáze	Decentralizovaná a distribuovaná databáze
Vysoké riziko neoprávněného zásahu	Nízké riziko neoprávněného zásahu
Mnoho datových operací	Pouze přidávání operací
Relační databáze	Transakční zpracování
Vysoká míra vynaložení lidského úsilí	Nízká míra vynaložení lidského úsilí
Dosud nepodporuje automatizované kontrakty	Jednoduchá tvorba tzv. chytrých kontraktů
Kontroly jsou specificky navrhované	Možnost kontroly skrz chytré kontrakty a kontroly
Specifické moduly pro účetnictví	Dosud žádný modul zaměřený na účetnictví

zdroj: Dai a Vasarhelyi, 2017, vlastní zpracování

Blockchain je považován za nový typ distribuované databáze, na rozdíl od ERP systémů, které pracují na bázi centralizované databáze. Blockchain tak může výrazně eliminovat riziko selhání jedince a zároveň silněji čelit případnému tlaku managementu na obcházení systému, také je schopný zabránit veškerým neautorizovaným změnám, čímž chrání firmy od kybernetických útoků.

Blockchain relativně jednoduše organizuje data a skupina operací je chápána jako transakce – používá tzv. transakční zpracování. ERP systém je obvykle založen na relačních databázích[27], tzn. používá propojené tabulky s předem nadefinovanými vztahy, kde řádky představují záznamy a sloupce představující atributy. ERP tak umožňuje mnoho operací s daty, jako vkládání, následné úpravy nebo jejich smazání, což ale vyžaduje značné vynaložení lidského úsilí.

Možnost vytvořit chytré kontrakty v rámci Blockchainu umožňuje navrhovat a aplikovat nejrůznější kontroly a díky decentralizaci dochází k zabránění manipulace kontrolních mechanismů. V současnosti Blockchain není implementován do ERP systémů (Dai a Vasarhelyi, 2017). Další kapitola bude mj. také věnovat myšlenkám

[27] Obvykle jsou tyto databáze stavěny na základu Relational Database Management Systems (RDBMS).

vedoucím k zapojení Blockchain technologie do ERP systémů a použití této technologie pro potřeby účetnictví.

2.9 Praktické aplikace Blockchainu

V současnosti v praxi již existuje mnoho aplikací Blockchianu. Řešení společnosti IBM pro přepravní společnost Maersk nazvané TradeLens Blockchain Shipping Solution bylo představeno srpnu 2018 a v celém projektu je aktivně zapojeno 94 společností. Cílem bylo vytvořit efektivnější a bezpečnější systém pro mezinárodní obchod propojením mnoha subjektů, kteří navzájem sdílí transparentní informace.

Americká nadnárodní maloobchodní společnost Walmart, která provozuje hypermarkety a obchody s potravinami vyvinula ve spolupráci s IBM blockchainové řešení Food Trust, kontrolující bezpečnost potravin. Vysledování konkrétních dodavatelů potravin je nyní jednodušší a rychlejší např. při zjištění kontaminovaných potravin.

We.trade je konsorcium devíti bank (Deutsche Bank, HSBC, KBC, Natixis, Nordea, Rabobank, Santander, Societe Generale and UniCredit), které v roce 2018 představilo platformu pro Trade Finance. Jedná se o služby v zahraničním obchodě (záruky, dokumentární inkasa, akreditivy, směnečná inkasa apod.) Kromě IBM se vývoji věnuje také Microsoft Azure ve spojení s velkými poradenskými společnostmi.

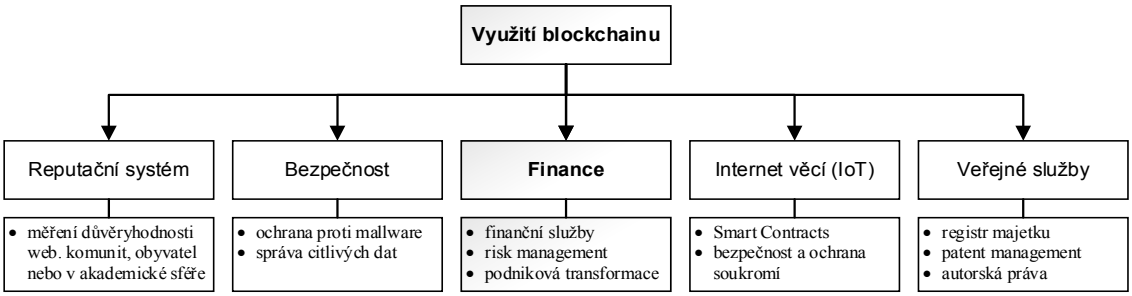
Budoucí využití této technologie je diskutováno i v souvislosti s připravovaným Systémem sociálního kreditu[28], jehož spuštění je vládou Čínské lidové republiky plánováno v roce 2020. Systém bude hodnotit obyvatele a firmy na základě různých kritérií společenského a ekonomického chování, na jehož základě (ne)budou mít přístup k veřejným službám. Dohledový systém bude využívat masivního dohledu s využitím Big data a umělé inteligence. Podle odborníků je pravděpodobné právě využití určité formy decentralizované databáze (Caldwell, 2018).

[28] Anglicky Social Credit System.

3 Využití Blockchainu v účetnictví a auditu

Distribuované databáze, jako je Blockchain, představují potenciální řešení pro řadu problémů. Firmy v současné době mohou retrospektivně manipulovat transakcemi, např. s úmyslem úpravy výše obratu nebo hospodářského výsledku (Coyne a McMickle, 2017). Naděje k zabránění takového jednání jsou místo tradičních účetních systémů směřovány k vedení účetní knihy v Blockchainu. Ve spojení s internetem věcí takový systém může nabídnout sledování aktivit a objektů v reálném čase, automatizaci v účtování a měření výkonnosti podniků a v určitém stupni agregace i následný reporting spolehlivých informací oprávněným stranám (manažerům, auditorům nebo věřitelům). Kromě finančního sektoru existuje široká možnost využití Blockchainu také v jiných odvětvích.

Obrázek 10: Reprezentativní využití Blockchainu napříč obory

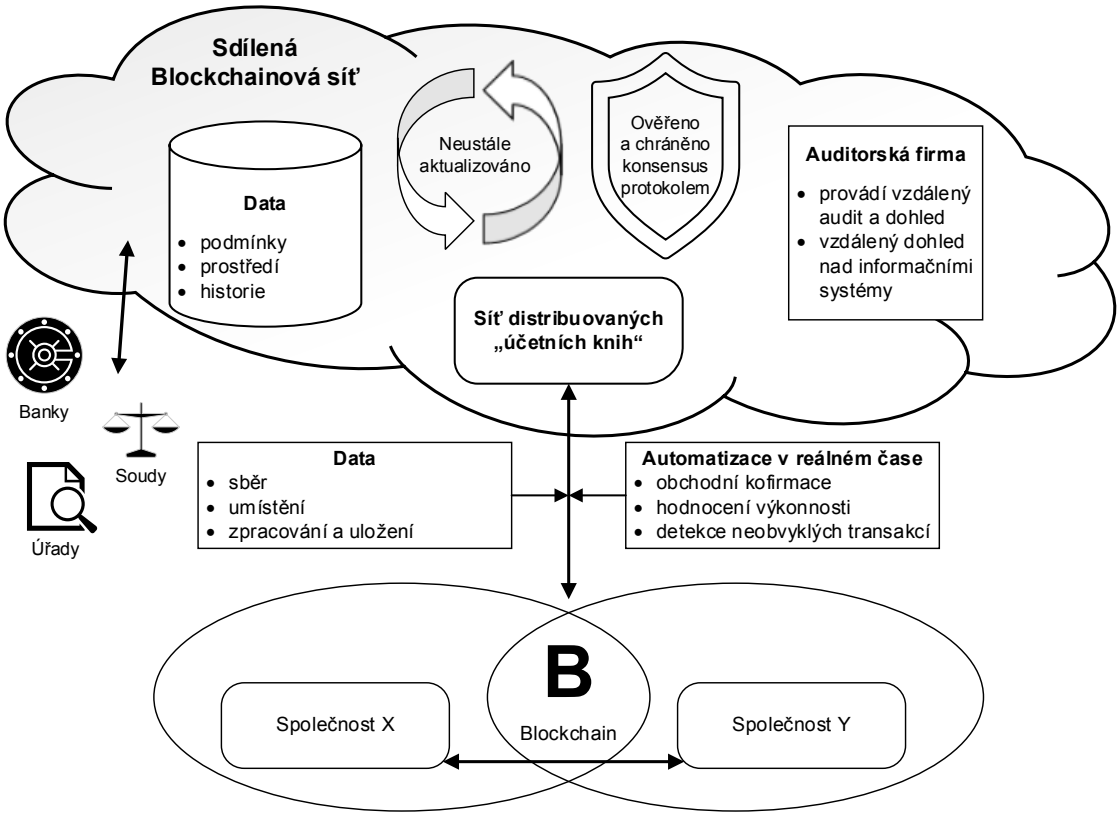


vlastní zpracování

Postupná implementace Blockchainu ovlivňuje vývoj tradičních finančních a podnikových služeb. V oblasti finančnictví je uváděna možná aplikace v bankovním clearingu a provádění platebních transakcí a poskytování úvěrů. Účetnictví a audit z této technologie bude taktéž profitovat. Protože Blockchain zbraňuje zpětné úpravě dat, auditoři získávají formu automatického ujištění o integritě dat. Použitím Blockchainu by mohl vzniknout nový účetní informační systém, který zaznamenává a ověřuje jednotlivé transakce nesmazatelným způsobem. Nemusí se jednat pouze o peněžní transakce mezi dvěma subjekty, ale o kompletní tok účetních transakcí uvnitř podniku nebo s jeho okolím. Takový systém by díky okamžitému sdílení účetních transakcí manažerům, obchodním partnerům nebo auditorům umožnil reporting v téměř reálném čase. Automatické ujištění je zajištěno i při použití Smart contracts, tj. program fungující v Blockchainu, který kontroluje podnikové procesy na bázi určitých předdefinovaných pravidel, (Dai a Vasarhelyi, 2017) jeho použití je vhodné samotnou společností, ale i externím auditorem, který by díky implementaci ušetřil čas věnovaný provádění opakovaných úkonů a mohl tento čas věnovat rizikovým oblastem. Další potenciální výhoda pro auditory je přístup k účetním datům v téměř reálném čase, čímž je

eliminována sezónnost auditu a kontroly lze provádět průběžně, nikoliv až po poskytnutí dat klientem.

Obrázek 11: Základní struktura a funkce Blockchainu

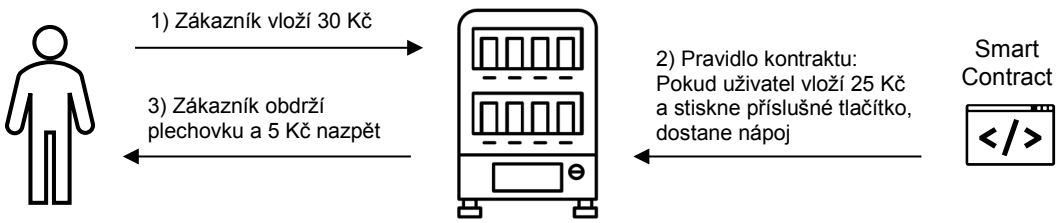


zdroj: Kostić a Tang, 2017, vlastní zpracování

3.1 Smart contract

Smart Contract je spojován s Blockchainem od jeho druhé generace a více než o chytrý kontrakt nebo chytrou smlouvu se jedná se o označení pro počítačový protokol či algoritmus, který nezávisle ověřuje, vykonává či vynucuje smluvní podmínky v kontraktech, smlouvách nebo dohodách. Koncept chytrého kontraktu poprvé použil americký počítačový vědec Nick Szabo v roce 1994, který ho přiblížil na praktickém příkladu nápojového automatu (v tomto případě hardwaru), ve kterém po vložení mincí dojde buď k vydání nápoje nebo vrácení mincí.

Obrázek 12: Původní koncept Smart Contract z roku 1994



vlastní zpracování

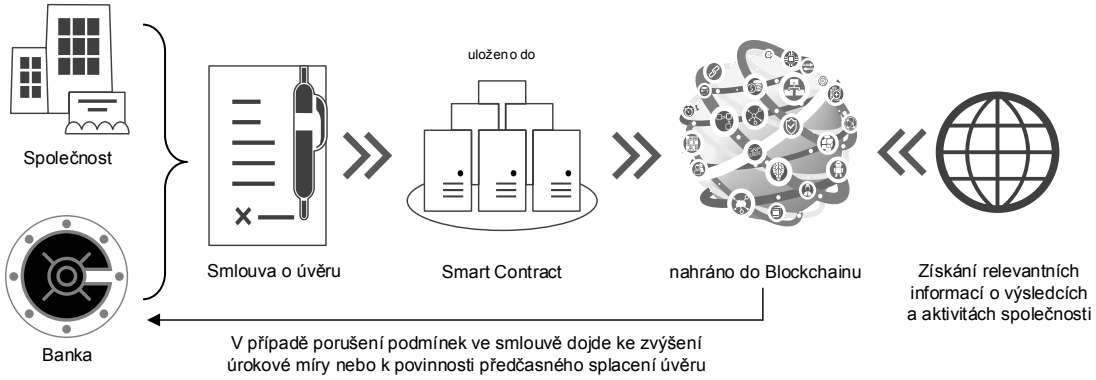
Bez asistence člověka tento elektronický systém kontroluje platnost mincí, velikost sumy pro případné vrácení přeplatku či zrušení objednávky zákazníkem. Automat tak bez přítomnosti člověka na jedné straně uzavírá kupní smlouvu s protistranou za předem specifikovaných podmínek, v tomto případě musí mít zákazník pro uskutečnění transakce dostatečný počet mincí.

Zatímco původní návrh předpokládal existenci dohledu určitou centrální autoritou (zprostředkovatelem), technologie založená na Blockchainu uzavírá obchodní vztahy napřímo bez účasti třetí strany. Předdefinovaná pravidla smluvních stran mohou být uložena v Blockchainu s definicí jejich účastníků. Kontrakt je následně aktivován poskytnutím potřebných dat, data jsou ověřena a zpracována chytrým kontraktem (např. při splnění požadavků je provedena platba za zboží). V případě nesplnění podmínek by bylo vygenerována chybové hlášení o neuskutečněné transakci.

Hlavní myšlenkou je tedy automaticky skrze algoritmy provést plnění smlouvy bez vůle smluvních stran, jakmile jsou splněny stanovené podmínky (Alharby a Moorsel, 2017), které jsou nezměnitelně zapsány v Blockchainu. Tím zvyšují transparentnost a zamezí neshodám či odchylkám od smluvních podmínek při plnění kontraktů. Chytré kontrakty absencí zprostředkovatele snižují transakční náklady (např. provizi) v porovnání s tradičním systémem. Účastníci mají jistotu, že smlouva díky kryptografii funguje podle algoritmu, jehož zdrojový kód je veřejný smluvním stranám, čímž se zamezí ovlivnitelnosti smluvních podmínek a zároveň se snižuje riziko selhání protistrany.

V praxi Smart kontrakty fungující v síti Ethereum na bázi technologie Blockchain a ve spojení s kryptografií tvoří platformu, na které lze zajistit transparentní vykonání zdrojového kódu, který si mohou uživatelé kdykoli zobrazit a sledovat jeho průběh, protože je veřejně přístupný (v případě veřejného Blockchainu). Protože Blockchain neumožňuje zpětné úpravy jednotlivých bloků a v případě Etherea je každý blok vytěžen v řádu několika sekund, zvyšuje to důvěryhodnost a nezměnitelnost uzavřených smluv.

Obrázek 13: Smart Contract v praxi



zdroj: Dai a Vasarhelyi, 2017, vlastní zpracování

Praktický příklad ilustruje Smart contract fungující v blockchainové síti, který je používán k automatickému monitorování úvěrového kovenantu. Jedná se o smluvní ujednání smlouvy o úvěru spojené s informačními povinnostmi dlužníka vůči věřiteli. Bankovní úvěr se může stát splatným na vyžádání, pokud účetní jednotka nesplní omezující podmínky – kovenanty[29]. V takovém případě je třeba během auditu věnovat pozornost správnému ocenění a klasifikaci (dlouhodobý vs. krátkodobý úvěr). Jakmile se banka s dlužníkem dohodnou na podmínkách kovenantu, jsou tyto podmínky zakódovány do chytrého kontraktu a následně uloženy do Blockchainu. Blockchain bude následně neustále monitorovat aktivity dlužníka oproti požadavkům ve smlouvě. Jakmile bude zjištěno porušení kovenantu, Blockchain automaticky aktivuje ujednání ve smlouvě vztahující se k porušení smluvních podmínek. To může představovat předčasnou splatnost úvěru nebo např. zvýšení úrokové míry. Auditoři i management banky se také mohou účastnit dohledu, zda mechanismus funguje na základě smluvně definovaných pravidel.

[29] V praxi se v současnosti obvykle zasílá zpráva o plnění ve smlouvě přesně specifikovaných ukazatelů čtvrtletně. Z pohledu auditu se jedná o test kontrol.

Obrázek 14: Ukázka zdrojového kódu Smart Contract

```
pragma solidity ^0.4.6;

contract TrackPayments {

    struct PaymentStruct {
        address sender;
        uint amount;
    }

    // look up the struct with payment details using the unique key for each payment
    mapping(bytes32 => PaymentStruct) public paymentStructs;

    // payment keys in order received
    bytes32[] public paymentKeyList;

    event LogPaymentReceived(address sender, uint amount);

    function payMe() public payable returns(bool success) {
        if(msg.value==0) throw;
        // make a unique key ...
        bytes32 newKey = sha3(msg.sender, paymentKeyList.length);
        paymentStructs[newKey].sender = msg.sender;
        paymentStructs[newKey].amount = msg.value;
        paymentKeyList.push(newKey);
        LogPaymentReceived(msg.sender, msg.value);
        return true;
    }

    function getPaymentCount() public constant returns(uint paymentCount) { return
paymentKeyList.length; }

}
```

zdroj: Stack Overflow

Další oblastí, kde je vhodná implementace chytrých kontraktů, je výrobní a dodavatelský sektor. Dodavatel a odběratel opět dohodnou pravidla kontraktu včetně detailních vlastní dodávaných produktů, množství, ceny a dodacích a platebních podmínek, které jsou naprogramovány do chytrého kontraktu a vloženy do Blockchainu. Odběratel následně má možnost zpětně dohledat detailní podmínky uzavřeného kontraktu a kontrolovat její status. V případě porušení smluvních podmínek je opět generováno chybové hlášení a transakce není dokončena. Následným chybovým hlášením by se zabývali odpovědní zaměstnanci (pravděpodobně interní audit). V případě splnění podmínek je kontrakt proveden, jakmile odběratel obdrží zboží a proběhne platba dodavateli.

3.1.1 Aplikace v auditingu

V praxi najdeme aplikaci chytrých kontraktů na bázi Blockchain technologie, jedná se ale o automatizované vypořádávání derivátových transakcí a transakce dokládající převod vlastnictví. Avšak aplikace v oblasti auditingu zatím zůstává neprozkoumaná.

Podle některých autorů (Rozario a Vasarhelyi, 2018) je nyní třeba, aby IT odborníci auditorských firem vyvinuli tzv. chytré auditní procedury (z angl. Smart audit procedures), jejichž funkčnost by následně byla důkladně prověřena a otestována.

Potenciál je především v oblasti analytických testů věcné správnosti[30] a testů kontrol[31]. Následně by došlo k nahrání takového kódu do Blockchainu a poskytnutím potřebných dat proběhne celý proces podle naprogramovaného scénáře. Výstupy z tohoto kontraktu jsou následné viditelné auditorem jako vlastníkem Blockchainu a případně dalším uživatelům s přidělenými právy (přístup by dával smysl v jisté agregaci dat pro auditorského regulátora, jako např. v ČR Rada pro veřejný dohled nad auditem v případě auditů subjektů veřejného zájmu nebo v USA pro Komisi pro cenné papíry a burzu – SEC či klíčovým investorům).

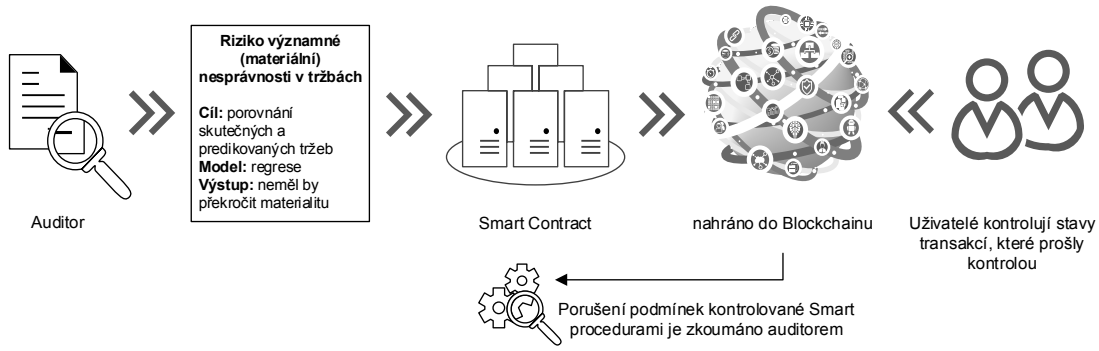
Předdefinované analytické procedury by mohly být postaveny na podmínce „když-tak“ a dalších filtrech identifikující případná rizika nakonfigurovaná auditorskou firmou a zakódované do Smart kontraktu uloženém v Blockchainu. (Rozario, 2017). Praktickým příkladem takového kontraktu je analytický test věcné správnosti, který by se mohl skládat z podmínky predikce aktuálních tržeb modelem regresní analýzy, který zahrnuje finanční i nefinanční parametry jako týdenní tržby, geolokační umístění, teplotu a data z předchozích týdnů. Postupným sběrem dat budou výstupy z modelu přesnější. Predikované tržby mohou být srovnávány se skutečností (Yoon, 2016) a nabízí se využití funkce „když-tak“ k rozhodnutí, zda aktuální tržby odpovídají predikci nebo jsou vyšší čí menší anebo překračují určitou hranici významnosti (materiality)[32]. V takovém případě není potřeba žádné dodatečné testování a auditor je schopen kvantifikovat riziko významné (materiální) nesprávnosti pro tržby. Jestliže se kontrolovaná aktuální data neshodují s naprogramovanými pravidly, chybové či upozorňující hlášení informuje auditora o nezbytné potřebě další pozornosti a auditor může navrhnout alternativy k testování jednotlivých záznamů.

[30] Test věcné správnosti jsou auditorské postupy navržené k odhalení významných (materiálních) nesprávností na úrovni tvrzení a zahrnují testy detailních údajů a analytické testy věcné správnosti. Analytické testy věcné správnosti jsou obecně vhodnější pro velké objemy transakcí, které mají většinou předvídatelný vývoj. (ISA 330)

[31] Auditorské postupy navržené k posouzení provozní účinnosti kontrol při prevenci nebo odhalování a opravách významných (materiálních) nesprávností na úrovni tvrzení. (ISA 330) V oblasti IT se zaměřují např. na nastavení přístupových práv k různým informačním systémům jednotlivých uživatelů v organizaci.

[32] Materialita (významnost) představuje hodnotu nesprávností, kterou auditor bude považovat za významnou ve vztahu k účetní závěrce. Podle ISA 320 jsou nesprávnosti považovány za významné (materiální), jestliže je možné přiměřeně očekávat, že jednotlivě nebo v součtu ovlivní ekonomická rozhodnutí uživatelů přijatá na základě účetní závěrky.

Obrázek 15: Návrh aplikace Smart contract při auditu účetní závěrky



zdroj: Rozario, 2017, vlastní zpracování

Vzhledem k tomu, že Blockchain dokáže ve spolupráci s internetem věcí monitorovat lokaci chytrých zařízení, dalším vhodným testem, který auditoři mohou navrhnout je test kontrol k ověření aktuálního umístění zboží v porovnání s očekávanou lokací podle posloupnosti vnitropodnikových procesů (Dai a Vasarhelyi, 2017).

Při opakovaném používání Smart kontraktů tak dochází efektivnímu provádění auditů, zlepšení celkové kvality auditu, a pro auditora zároveň i jako důkazní prostředek o provedení daných procedur.

3.2 Potrojné účetnictví [33]

Jednoduché či kamerální účetnictví funguje na základě jediného účetního zápisu o uskutečněné události, u nás je také spojováno s pojmem daňová evidence. Ačkoli se jedná o jednoduchý a účinný mechanismus, je vystaven vysokému riziku chyb a podvodů, neboť je obtížné tyto problémy sledovat. Ke zvýšení přesnosti účetního systému je používán podvojný systém, který poprvé definoval Luca Pacioli[34] v roce 1514. Současně nejrozšířenější podvojné účetnictví je založeno na dvoustranném zápisu každé hospodářské operace z hlediska vlivu na finančně-majetkovou strukturu podniku (Hradecký a kol., 2008, s. 250). Podvojné účetnictví může snížit riziko lidské chyby jako např. neúmyslné smazání transakcí, čímž neposkytuje záruku správnosti. Aby zveřejněné údaje měli důvěru uživatelů účetní závěrky, jsou ověřovány auditory, to znamená, že důvěra je vkládána třetí nezávislé osobě.

Systém potrojného účetnictví byl navržen k zajištění nezávislé kontrole a zabezpečení účetních dat a tím i zvýšení vypovídací schopnosti účetních výkazů. Protože auditoři

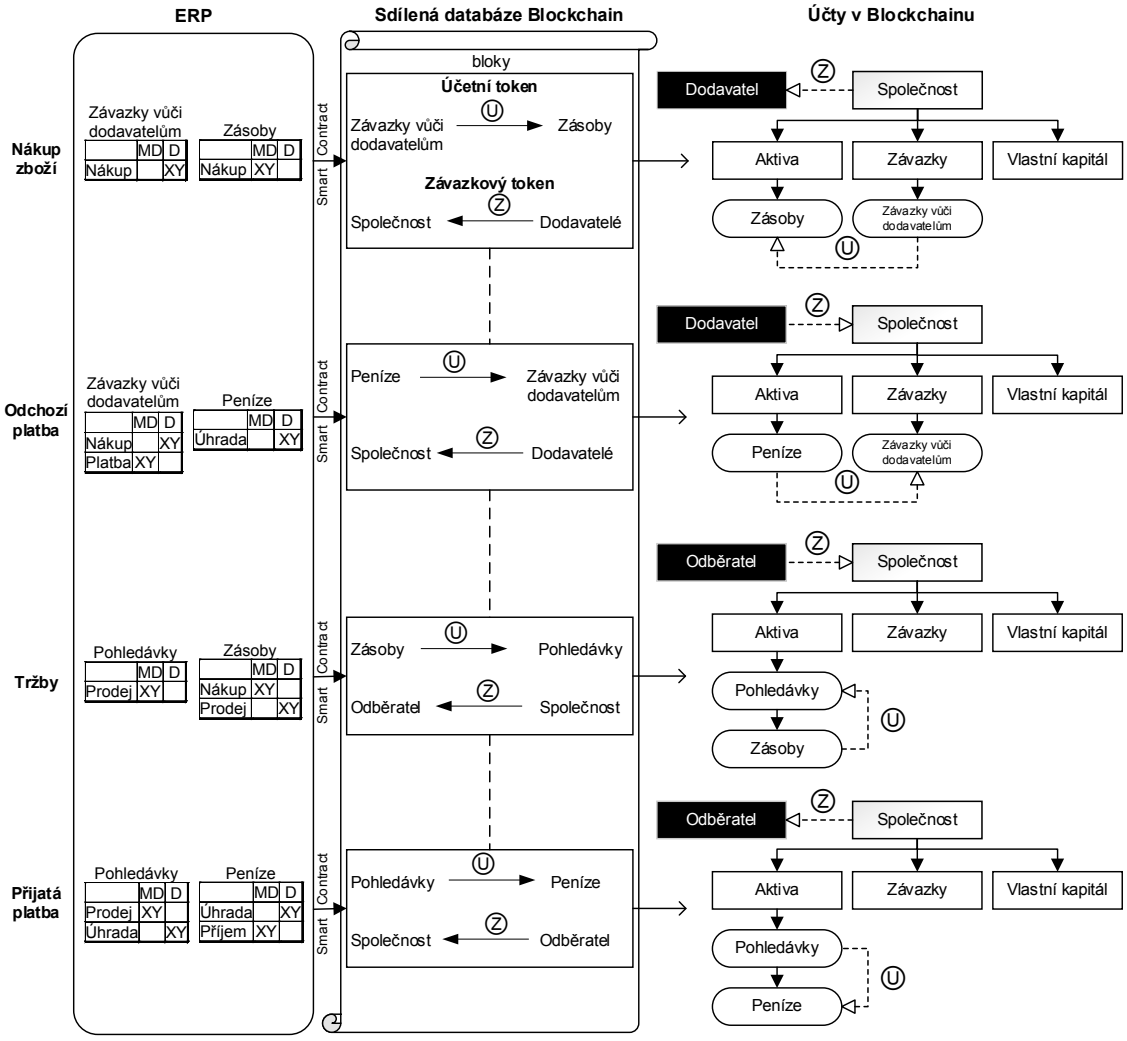
[33] Anglicky Triple-entry Accounting.

[34] Podrobněji o historickém vývoji účetnictví a auditu pojednává kap. 1 Auditing – historie a budoucnost.

nezávisle ověřují účetní závěrku, koncept potrojného účetnictví s využitím Blockchainu by mohl pomoci zlepšit vypovídací schopnost, důvěru a ujištění, které auditoři poskytují.

S cílem zlepšit důvěru a posílit nezávislost ve vykazování finančních výsledků společností byla myšlenka o potrojném systému účtování publikována již v roce 2005. Původní návrh předpokládal autorizaci každé transakce od nezávislého zprostředkovatele, která vyústí ve tři účetní zápisy (Grigg, 2005). Vzhledem k tomu, že tento mechanismus vyžaduje vstup třetí nezávislé strany, společnosti by se vystavovaly riziku neoprávněných změn v účetních záznamech při případném kybernetickém útoku. Využitím Blockchainu vyvstává potenciál zlepšit takový mechanismus a zároveň snížit zmíněná rizika. Blockchain by mohl být onou třetí stranou a distribuovat a automatizovat tak celý proces a zároveň zabránit neoprávněným změnám v účtování, protože s jeho použitím není možné zpětně upravovat účetní záznamy. Využití Smart contracts by umožnilo rychlé, transparentní a šifrované ověřování záznamů podle naprogramovaných účetních standardů nebo vnitropodnikových směrnic a zároveň by mohlo sdílet data napříč subjekty v okolí podniku. (Dai a Vasarhelyi, 2017) Protože se jedná o citlivá data, ke kterým mají obvykle přístup pouze účetní, management a auditoři, v praxi bude třeba využít soukromého nebo konsorcium Blockchainu. Transakce by navíc mohly být před nahráním do Blockchainu zašifrovány a pouze autorizovaní uživatelé s dešifrovacím klíčem by je mohli zobrazit.

Obrázek 16: Potrojné účtování v Blockchainu

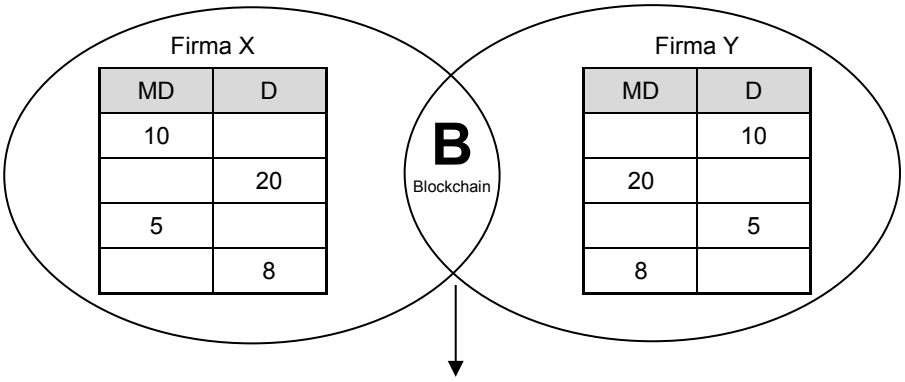


zdroj: Dai a Vasarhelyi, 2017, přepracováno

Výše vyobrazené schéma znázorňuje teoretický návrh potrojného účetního systému, který zaznamenává jednotlivé transakce, které nastaly. Každá transakce je kromě tradičního podvojného zápisu zaznamenána zároveň do Blockchainu a tvoří tak zápis třetí. Ke zohlednění transakčních důsledků do Blockchainu Společnosti jsou transakce zaznamenávány ve formě tokenových převodů mezi jednotlivými účty. Tokeny slouží mezi obchodními partnery jako důkaz o vlastnictví aktiv nebo o závazku. Účetní token představuje symbol pro účely zaznamenávání a sledování transakcí. Každý účet v podvojném účetním systému by měl příslušný účet v Blockchainu, který by představoval ekvivalent k Bitcoinové peněžence. Účty by v Blockchainu mohly být členěny hierarchicky do tří úrovní: nejnižší na úrovni účtů, v další úrovní v rozdělení na aktiva a pasiva a následně samotná Společnost jako nejvýše postavená. S použitím Smart Contracts následně lze zajistit bilanční rovnost. (Dai a Vasarhelyi, 2017)

Na příkladu nákupu a prodeje zboží se v prvním kroku při nákupu zboží od dodavatelů v ERP a účetnictví Společnosti promítne jako zvýšení aktivního účtu Zboží na skladě[35] a zároveň zvýšení Závazků vůči dodavatelům na pasivní straně bilance. Současně je tato událost zaznamenána do Blockchainu ve formě „účetního tokenu". Závazek společnosti bude vyjádřen ve formě „závazkového tokenu", jehož výše se okamžikem vydání stává nesmazatelná a nepopiratelná. Zakotvením ve Smart contracts s obchodním partnerem může být ujednána platba při splnění specifikovaných podmínek (např. blížící se datum splatnosti), podobně lze naprogramovat i slevy za včasné platby nebo automatické konfirmace. Odesláním tokenů do Blockchainu následuje ověření zaznamenání v ERP systému, zaúčtování v účetním systému (částky a účty) nebo převod aktiv. „Účetní tokeny" budou následně provedením platby přesunuty z Peněžního účtu na Závazky vůči dodavatelům. Jakmile dodavatel platbu zpracuje, pošle společnosti zpět „závazkový token" jako uznání platby a závazek společnosti zaniká. V případě prodeje zboží společnost naopak obdrží „závazkový token", který zašle po zpracování platby zpět.

Obrázek 17: Zobrazení účetních transakcí v Blockchainu



Sdílená úč. kniha

Firma X	Firma Y
-10	10
20	-20
-5	5
8	-8

zdroj: Tang a Karim, 2018, přepracováno

[35] Abstrahujeme od použití technického účtu Pořízení zboží, který je v praxi používán jako kalkulační účet pro snadnější evidenci vedlejších pořizovacích nákladů (pojištění, přepravné, balné apod.).

3.3 Audit transakcí v Blockchainu

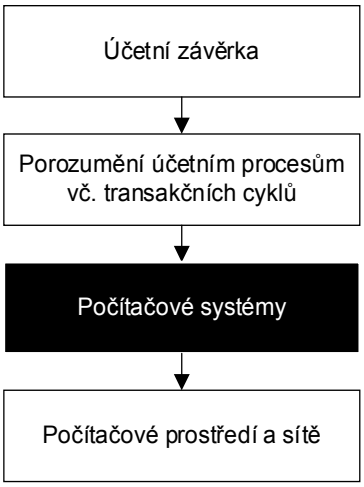
Externí audit účetní závěrky má tendenci se orientovat spíše na finanční stránku podniku, ale zaměřuje se i na používané informační technologie, a to v rámci porozumění struktury transakčních cyklů a jejich obsahů, vzniku zůstatků na účtech a účetnímu systému. Auditor má dle standardu ISA 315 povinnost identifikovat rizika významné (materiální) nesprávnosti[36] v účetní závěrce na základě znalosti účetní jednotky a jejího prostředí, a to včetně vnitřního kontrolního systému[37]. Standard věnující se seznámení se s používanými informačními technologiemi klienta klade vysoký důraz. Auditor se musí seznámit s informačními systémy, které se týkají účetního výkaznictví a slouží k inicializaci, zaznamenávání a zpracovávání transakcí a jejich přenosu do hlavní knihy a vykázání v účetní závěrce. Zjištění následně slouží při plánování auditu k návrhům reakcí na vyhodnocená rizika.

Distribuované databáze jsou zkoumány v souvislosti s informační podporou pro účtování v transakčních cyklech zároveň i jako podpora reportingu, tedy vykazování výsledků společnosti. Takové informace poslouží auditorům lépe porozumět výměně informací v podniku a vyhodnotit faktory ovlivňující auditorské riziko. Na nejvyšší úrovni je ověřováno, zda účetní závěrka a informace v ní obsažené souhlasí s účetními záznamy. V rámci jednotlivých cyklů je následně kontrolováno, zda jsou jednotlivé hodnoty, časové údaje či smluvní strany v souladu s realitou.

[36] Riziko identifikované a vyhodnocené auditorem jako riziko s povahou významné (materiální) nesprávnosti, kterému je třeba věnovat zvláštní pozornost. Mezi rizika významné (materiální) nesprávnosti řadíme i změny v prostředí IT systémů, které mají vliv na účetní výkaznictví.

[37] Jedná se o navržený, zavedený a vykonávaný proces osobami pověřenými správou a řízením účetní jednotky za účelem poskytnutí určitého ujištění o dosažení cílů účetní jednotky s ohledem na spolehlivost účetního výkaznictví, účelnost a hospodárnost operací a soulad s příslušnými právními předpisy. (ISA 315, odst. 4, písm. c).

Obrázek 18: Vztah informačních systémů k transakčním cyklům a reportingu



zdroj: Mainelli a Leitch, 2017

Blockchain jako distribuovaná databáze či „kniha záznamů" snižuje auditorské riziko díky použití kryptografických funkcí, které zabraňují provádění změn či vymazání transakcí zpětně po vložení takové transakce do Blockchainu. Tím snižuje riziko záměrně podvodného jednání a zároveň předchází nechtěným chybám. Auditoři se touto problematikou zabývají a testují i v současnosti, a to v rámci testů věcné správnosti[30] a testů kontrol[31].

Problém, kterému bude v budoucnu třeba věnovat pozornost je možné zpoždění mezi proběhlou transakcí a jejím zařazením do Blockchainu. Takové transakce představují zvýšené riziko především v době před a po rozvahovém dni nebo např. při kvartálních uzávěrkách. V tyto okamžiky je důležité se zaměřit na správné zachycení výnosů a nákladů, aby jejich vykazování nebylo v rozporu s účetními standardy, se správným okamžikem uznání výnosů nebo s principem přiřazování nákladů jednotlivým výnosům. Zároveň je na místě, že některé transakce nebudou do bloku zařazeny vůbec nebo se budou vyskytovat dvakrát.

3.3.1 Ověřování transakcí v Blockchainu

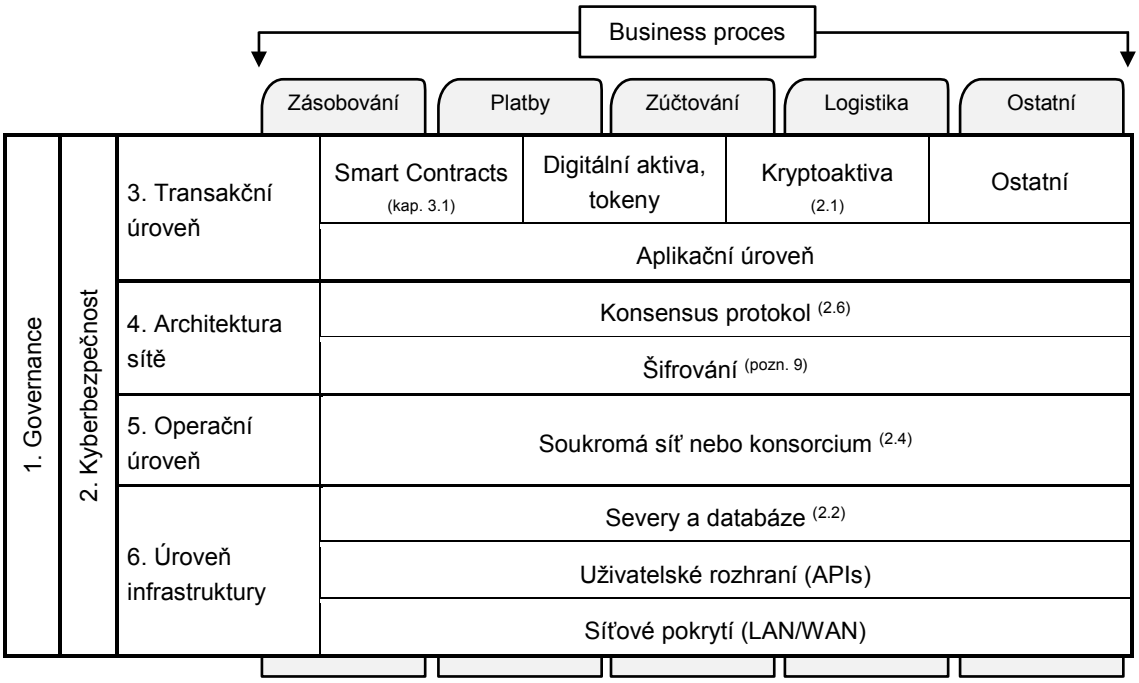
Zatímco jednotlivé individuální transakce v každém bloku Blockchainu jsou ověřovány v samostatně, podniky potřebují testovat transakce, které vznikají např. automaticky během různých procesů. S unikátní architekturou Blockchainu a zároveň nízkou znalostí technologií navíc v současnosti neexistuje žádný právně závazný standard pro ověřování transakcí v Blockchainu. V tomto ohledu vyvíjejí svá řešení především největší auditorské společnosti. Řešení společnosti PwC Blockchain Validation umožňuje, aby externí auditoři, interní auditoři, případně i výkonní pracovníci měli přístup a kontrolu

nad testováním transakcí. Každému klientovi musí přizpůsobit kontrolní prostředí specifického businessu. Řešení spočívá ve dvou komponentech: vlastní auditorský software pracující na bázi Smart audit procedur a zároveň rizikový a kontrolní rámec vytvořeným speciálně pro tyto účely.

Rizikový a kontrolní rámec pro Blockchain

Tento rámec byl vytvořen k identifikaci a řešení rizikových očekávání ve třech liniích: na operační linii, risk management a interní audit. Rámec obsahuje šest rizikových bodů s podkategoriemi, které blíže přibližují jednotlivé části a definují případné kybernetické hrozby. Informace získané v tomto rámci mohou být následně použity v auditorském softwaru.

Obrázek 19: Rizikový a kontrolní rámec navržený pro audit transakcí v Blockchainu



zdroj: PwC: Governance in the Age of Blockchain Distributed Ledger Technology, 2018, upraveno

Proces ověřování transakcí

- Samotný proces ověřování začíná u výše zmíněného rámce identifikujícího šest klíčových oblastí. Prověřuje se např. v jaké úrovni infrastruktury Blockchain funguje, jaká práva jsou udělena uživatelům sítě nebo jaký druh šifrování je používán. Odpovědi na jednotlivé oblasti slouží ke stanovení případných rizik a oblastí k testování.
- Dalším krokem je zapojení speciálně vyvinutého softwaru přizpůsobeného na míru a pro potřeby společnosti (odlišné pro vedoucí pracovníky a interní audit).

Společnost si může zvolit, zda chce monitorovat všechny transakce nebo pouze takové, které překročí určitou hodnotu.

- V dalším kroku je do Blockchainu instalován uzel určený pouze pro čtení transakcí téměř v reálném čase tak, jak vznikají.
- Software postupně zaznamenává a testuje transakce podle stanovených kritérií. Ty transakce, které splňují (nebo naopak nesplňují) určitá kritéria, jsou označeny jako výjimky a určeny k detailnější kontrole.
- Uživatelé následně mají možnost zobrazit si přehledné výstupy a reporty.
- Vzhledem k technologickému vývoji je možné upravit softwarové nastavení požadavkům společnosti.

3.3.2 Reakce na auditorská rizika

Auditor k posouzení auditorského rizika používá mj. i v první kapitole zmíněné Smart audit procedures. Následující tabulka popisuje existující rizika týkající se výnosů a jsou členěny na existující rizika, které existují v tržbách bez ohledu na používaný systém k zaznamenávání transakcí, a nová či postupně vznikající rizika, která vznikají s vývojem a postupnou implementací Blockchainu a Smart contracts jednotlivými klienty.

Tabulka 8: Reakce na auditorská rizika

	Auditorské riziko	Smart Audit přístup	Tradiční přístup
Existující	(1) Neautorizované, fiktivní nebo chybné smlouvy jsou vkládány do systému.	Automatické srovnávání klíčových ujednání v původním Smart contract kódu s klíčovými ujednáními kódu v auditovaném období.	Auditor testuje klíčová ustanovení ve smlouvě na základě vybraného vzorku smluv např. v PDF. Alternativně lze k analýze textových informací použít software tzv. „hlubokého učení“ k automatizované kontrole podmínek smluv.
		Automatická kontrola spárování klientova Smart contractu k aktivní blockchainové peněžence.	
		Test kontrol je nakonfigurován tak, aby samostatně odesílal transakce do Blockchainu.	
	Odeslané zboží není zaúčtováno přesně nebo úplně.	Analytické testy jsou nastaveny k automatizovaným predikcím tržeb za použití finančních i nefinančních dat a srovnání s realitou.	Auditor provádí analytické procedury ke kalkulaci předpokládaných tržeb na základě prodaného množství a prodejní ceny, následně jsou srovnávány s vykazovanými hodnotami.
		Výše uvedené analytické testy jsou nakonfigurovány tak, aby autonomně zpracovávaly chybová upozornění.	
	Peněžní příjmy nejsou správně zaúčtovány nebo zařazeny ve správném období.	Nevztahuje se k testování, Blockchain rekonciliuje (sesouhlasuje) každou výnosovou transakci.	Auditor na základě vybraného vzorku peněžních příjmů ověřuje jejich správnost na základě potvrzení od externího subjektu (např. bankovní výpis).
Nové	Blockchain nemusí mít mechanismus k zajištění integrity dat.	Test kontrol je konfigurován k automatickému ověřování konsensus mechanismu (kap. 2.6 Konsensus algoritmu).	
		Test kontrol je nakonfigurován k automatickému ověřování, že žádný účastník v Blockchainu neovládá více než 51 % výpočetní síly (kap. 2.7.3 51% útok).	
	Klientův Blockchain může zadávat neautorizované transakce.	Test kontrol je nakonfigurován k automatickému ověřování aktivních uživatelů, zda mají autorizovaný přístup.	

	Smart contracts mohou být vytvářeny svévolně bez autorizace.	Test kontrol je konfigurován k automatickému párování celkového počtu Smart contracts v testovaném období a je srovnáván s předchozím obdobím. U kontraktů, které nebyly napárovány, je kontrolována oprávněná autorizace k tvorbě kontraktu a zároveň i odůvodnitelnost samotného vzniku.	
	Smart contracts, které jsou zastaralé, mohou být nahrazeny novými kontrakty.	Test kontrol je konfigurován k automatickému párování kontraktů, které by měly být neaktivní se skutečně neaktivními Smart contracts.	

zdroj: Rozario a Vasarhelyi, 2018, vlastní zpracování

Auditor může k testování prvního existujícího rizika, uvedeného v tabulce výše, použít Smart procedury. Test kontrol srovnávající smluvní podmínky zakódované ve Smart contract v auditovaném období s původními hodnotami při uzavření kontraktu. Výsledky by mohly být přístupné v Blockchainu auditora např. i subjektům v okolí auditovaného podniku. Klíčoví dodavatelé klienta by měli prospěch z ověření, že se podmínky smlouvy nijak nezměnily. Dalšími uživateli by mohli být inspektoři kontroly kvality provedeného auditu, v tomto případě by provedené procedury sloužily jako důkazní prostředek o provedení příslušných postupů. Zároveň se jedná o dvouúčelový test, protože shromažďuje informace o existenci a zároveň o hodnotách těchto kontraktů.

Nově identifikovaná rizika spojená s Blockchain technologií vytváří poptávku po novém typu IT auditu. Nezměnitelnost zápisu a decentralizace významně pomáhají omezit riziko spojené s nepřesnostmi peněžních příjmů. Pokud auditor potvrdí správnost konsensus mechanismu a fakt, že žádný uživatel nemá výpočetní výkon přesahující 51 % sítě, pak použití externích konfirmací není třeba, protože Blockchain sesouhlasuje každou platbu, která je obdržena a auditoři mohou získat hash každé individuální transakce a mohou tak ověřit existenci, výskyt a ocenění. Rizika a příslušné procedury uvedené v tabulce výše představují model evoluce auditu, který přichází spolu s Blockchain a Smart contracts. Je důležité zároveň zdůraznit, že ne všechny součásti auditu mohou být přesunuty do blockchainových chytrých auditních procedur. Příkladem jsou oblasti jako oceňování investic reálnou hodnotou nebo daňová oblast. Celkový audit by tak tvořila část prováděna pomocí chytrých auditorských procedur s pomocí Blockchainu a další část procedur prováděných mimo Blockchain (Rozario, 2017).

Závěr

Přínosem této práce je definice a popis fungování technologie Blockchain se zaměřením na jeho využití v účetnictví a při auditu účetní závěrky. Práce ve svém úvodu popisuje historický vývoj auditingu s důrazem na regulaci nejen v České republice, ale i ve světě. Následně se první kapitola věnovala zapojení výpočetní techniky do procesu auditu včetně počítačového zpracování dat až po současné trendy velkokapacitního zpracování dat, internetu věcí a služeb, robotizace a automatizace a zároveň nástinu budoucího potenciálního vývoje auditu.

Kryptoměny, tedy digitální aktiva, které nejsou regulovány žádnou institucí či zemí, a jejichž transakce jsou kryptograficky zabezpečené, zažily masivní rozšíření od představení Bitcoinu až po vypuknutí Světové finanční krize v roce 2008. Jejich fungování je spojeno s databázemi, konkrétně s Blockchainem, typem distribuované databáze s neustále se rozšiřujícím počtem záznamů chráněných proti neoprávněnému zásahu. Popsaná Hype křivka odhaduje masivní využití této technologie okolo roku 2020. Až 72 % dotázaných vedoucích pracovníků v celosvětových průzkumech uvedlo Blockchain jako jejich strategickou či důležitou firemní prioritu a téměř polovina dotázaných očekává největší využití ve finančním sektoru. Po důkladném vysvětlení fungování celé technologie jsou zmíněny nejen omezení, výzvy a srovnání s podnikovými informačními ERP systémy, ale i úspěšné realizované projekty společnosti Walmart nebo konsorcia We.trade. Velká očekávání v oblasti vládního využití decentralizovaných databází přinese i připravovaný Systém sociálního kreditu v Čínské lidové republice, který bude firmy a obyvatele od roku 2020 hodnotit za dodržování jak zákonů, tak ekonomické nebo společenské chování včetně chování na internetu.

Třetí kapitola zaměřující se na využití Blockchainu v účetnictví vysvětluje termín Smart contracts, který spíše než „chytrou smlouvu“ představuje algoritmus nezávisle ověřující, vykonávající či vynucující smluvní podmínky v kontraktech, smlouvách nebo dohodách. Jeho využití v auditu přispěje k ještě větší a skutečné automatizaci procesu. Již nyní dochází k implementaci ve výrobním a dodavatelském sektoru. V kapitole je následně popsáno schéma potrojného účetnictví, které bylo navrženo s cílem zlepšit důvěru, nezávislost a vypovídací schopnost finančního výkaznictví. Jeho aplikace se může stát brzy realitou, anebo zapadne v současném rychle se vyvíjejícím světě. V závěru kapitoly jsou zmíněny existující a vznikající potenciální rizika z pohledu auditora při auditu transakcí uskutečněných v Blockchainu. Lze očekávat, že v budoucnu významně

poroste poptávka po auditorech informačních systémů v souvislosti s testováním vnitřního kontrolního systému v rámci auditu účetní závěrky, který ověřuje systémy sloužící k inicializaci, zaznamenávání a zpracovávání transakcí, jejich přenosu do hlavní knihy a následně používané k účetnímu výkaznictví.

Samotné vedení účetnictví a provedení auditu účetní závěrky představuje pro firmy vynakládání značných finančních prostředků. Velká část zabezpečení průkaznosti samotného účetnictví se s vývojem nových technologií stále více přesouvá k ověřování spolehlivosti a správnosti a kvality algoritmů zpracovávajících takové účetní záznamy a zároveň též ověření identifikovaných kontrolních systémů. V případě použití Blockchainu by se jednotlivé transakce transparentně zaznamenávaly do sdílených účetních knih, ke kterým by v reálném čase a s příslušným oprávněním měli přístup obchodní partneři, auditoři, banky nebo státní správa. Docílilo by se mnohem efektivnější vzájemné výměny informací a významně by se snížilo riziko neoprávněných zásahů do účetních dat. Nestandartní transakce by použitím Smart contracts a chytrých auditorských procedur mohly být identifkovány v reálném čase před samotným „zaúčtováním“ do Blockchainu a určeny tak ke kontrole pověřenou osobou nebo auditorem společnosti, čímž by byla částečně eliminována chybovost a zároveň oprava takových záznamů. Protože záznamy v Blockchainu díky použitému šifrování nelze zpětně upravit nebo vymazat, opravy v účetních záznamech tudíž splňují požadavky příslušného ustanovení zákona o účetnictví o provádění oprav v účetnictví, podle kterého opravy nesmějí vést k neúplnosti, neprůkaznosti, nesprávnosti, nesrozumitelnosti nebo nepřehlednosti účetnictví. Implementace Blockchainu by tak napomohla zvýšit důvěru a transparentnost vykazovaných informací a zároveň snížit chybovost a manipulaci s daty a podvody.

Auditoři s přicházející robotizací a automatizací tak budou moci aplikovat chytré postupy při provádění auditu. Podniky s využitím Smart contracts budou mít jistotu ve stálosti dodržování smluvních podmínek, přičemž jim technologie umožní snadnější vzájemnou fakturaci. Dosud se tématu Blockchainu věnovaly především poradenské a technologické společnosti a univerzitní výzkumy. Otazníky prozatím zůstávají u chybějící právní úpravy a nad přístupem firem k rozvíjející se technologii.

Má společnost opravdu zájem, aby výměna těchto informací byla takto transparentní a úplná? Jak se účetnictví, audit a nejen finanční sektor vyrovná s nástupem této technologie v budoucích měsících a letech, ukáže teprve čas.

Seznam literatury

Odborné publikace

Auditorská profese v České republice: Komora auditorů 1993-2013: 20 let. Praha: Komora auditorů České republiky, 2013. ISBN 978-80-86679-25-9.

BURNISKE, Chris a Jack TATAR. *Cryptoassets: the innovative investor's guide to bitcoin and beyond*. New York: McGraw-Hill, 2018. ISBN 978-1-260-02667-2.

HRADECKÝ, Mojmír, Jiří LANČA a Ladislav ŠIŠKA. *Manažerské účetnictví*. Praha: Grada, 2008. Účetnictví a daně. ISBN 978-80-247-2471-3.

HOFFMAN, Charles a Liv WATSON. *XBRL For Dummies.* Wiley Pub., 2009, 432 s. ISBN 978-0-470-49979-5.

CHAN, David Y., Victoria CHIU a Miklos A. VASARHELYI. *Continuous Auditing: A Book of Theory and Application*. Emerald Publishing Limited, 2018, 359 s. ISBN 9781787434141. Dostupné z: https://www.emeraldinsight.com/doi/book/10.1108/9781787434134

CHATFIELD, Michael a Richard VANGERMEERSCH. *The History of Accounting (RLE Accounting): An International Encylopedia.* Routledge Library Editions: Accounting, 2013, 678 s. ISBN 978-0415713122.

JANHUBA, Miloslav. *Teorie účetnictví: (výběr z problematiky)*. Praha: Oeconomica, 2010. ISBN 978-80-245-1662-2.

KLEINMAN, Gary a Asokan ANANDARAJAN. *International Auditing Standards in the United States.* Business Expert Press, 2014. ISBN 9781606496138.

MÜLLEROVÁ, Libuše, Vladimír KRÁLÍČEK a kol. *Auditing.* Vydání 2. přepracované. Praha: Oeconomica, nakladatelství VŠE, 2017. ISBN 978-80-245-2233-3.

SMIELIAUSKAS, Waldemar John, Wally SMIELIAUSKAS a Kathryn KATHRYN BEWLEY. *Auditing: an International Approach.* McGraw-Hill Education, 2015, 700 s., 7. edice. ISBN 9781259087462.

SPATH, Dieter, Olivier GANSCHAR, Stefan GERLACH, Moritz HÄMMERLE, Tobias KRAUSE a Sebastian SCHLUND. *Studie Produktionsarbeit der zukunft – Industrie 4.0.* Stuttgart: Fraunhofer Verlag, 2013. ISBN 978-3-8396-0570-7. Dostupné z: http://www.mechatronik-bw.de/attachments/article/272/Fraunhofer-IAO-Studie_Produktionsarbeit_der_Zukunft_-_Industrie_4.0.pdf

STROUKAL, Dominik a Jan SKALICKÝ. *Bitcoin: peníze budoucnosti*. Praha: Ludwig von Mises Institut, 2015. ISBN 978-80-87733-26-4.

SVATÁ, Vlasta. *Audit informačního systému*. 2. vyd. Praha: Professional Publishing, 2012. ISBN 978-80-7431-106-2.

SWAN, Melanie. *Blockchain: blueprint for a new economy.* Sebastopol, CA: O'Reilly, 2015. ISBN 978-1491920497.

TAPSCOTT, Don a Alex TAPSCOTT. *Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World.* USA: Penguin Books, 2016. ISBN 978-0-241-23785-4.

Odborné články

AKKOYUNLU, E. A., K. EKANADHAM a R. V. HUBER. *Some constraints and tradeoffs in the design of network communications*. ACM SIGOPS Operating Systems Review. 1975, 9 (5), 67-74. DOI: 10.1145/1067629.806523. ISSN 01635980. Dostupné z: https://doi.org/10.1145/1067629.806523

ALHARBY, Maher a Aad van MOORSEL. *Blockchain Based Smart Contracts: A Systematic Mapping Study*. 2017, 125-140. DOI: 10.5121/csit.2017.71011. ISBN 9781921987700. Dostupné z: https://doi.org/10.5121/csit.2017.71011

APPELBAUM, Deniz, Alexander KOGAN a Miklos A. VASARHELYI. *Big Data and Analytics in the Modern Audit Engagement: Research Needs*. 2017, 36 (4), 1-27. DOI: 10.2308/ajpt-51684. ISSN 0278-0380. Dostupné z: https://doi.org/10.2308/ajpt-51684

BARRETO, L., A. AMARAL a T. PEREIRA. *Industry 4.0 implications in logistics: an overview.* Procedia Manufacturing. 2017, 13, 1245-1252. DOI: 10.1016/j.promfg.2017.09.045. ISSN 23519789. Dostupné z: https://doi.org/10.1016/j.promfg.2017.09.045

CASTOR, Amy. *A (Short) Guide to Blockchain Consensus Protocols.* Coindesk. 4th March 2017. Dostupné z: https://www.coindesk.com/short-guide-blockchain-consensus-protocols/

CALDWELL, Malachy. *China's "Big Brother" Social Credit System "Will Be a Boost to Bitcoin.* ICOExaminer, 2018. Dostupné z: https://icoexaminer.com/ico-news/chinas-big-brother-social-credit-system-will-be-a-boost-to-bitcoin/

Cryptocurrency. Technopedia. Dostupné z: https://www.techopedia.com/definition/27531/cryptocurrency

Computer-aided audit tools. Chartered Institute of Internal Auditors. Dostupné z: https://www.iia.org.uk/resources/delivering-internal-audit/computer-assisted-audit-techniques-caats/

COYNE, Joshua G. a Peter L. MCMICKLE. *Can Blockchains Serve an Accounting Purpose? Journal of Emerging Technologies in Accounting.* 2017, 14 (2), 101-111. DOI: 10.2308/jeta-51910. ISSN 1554-1908. Dostupné z: https://doi.org/10.2308/jeta-51910

ČTK. *Analytici: Bitcoiny se kvůli nákladům nevyplatí těžit samostatně.* České noviny. 10. června 2018. Dostupné z: https://www.ceskenoviny.cz/zpravy/analytici-bitcoiny-se-kvuli-nakladum-nevyplati-tezit-samostatne/1630833

DAI, Jun a Miklos A. VASARHELYI. *Imagineering Audit 4.0.* Journal of Emerging Technologies in Accounting. 2016, 13 (1), 1-15. DOI: 10.2308/jeta-10494. ISSN 1554-1908. Dostupné z: https://doi.org/10.2308/jeta-10494

DAI, Jun a Miklos A. VASARHELYI. *Toward Blockchain-Based Accounting and Assurance.* Journal of Information Systems. 2017, 31 (3), 5-21. DOI: 10.2308/isys-51804. ISSN 0888-7985. Dostupné z: https://doi.org/10.2308/isys-51804

DAVENPORT, Thomas H. *Putting the Enterprise into the Enterprise System*. Harvard Business Review 76 July-August. 1998. Dostupné z: https://hbr.org/1998/07/putting-the-enterprise-into-the-enterprise-system

Deloitte's 2018 global blockchain survey: Breaking blockchain open. Deloitte [online]. 2018. Dostupné z: https://www2.deloitte.com/us/en/pages/consulting/articles/innovation-blockchain-survey.html

Employment Situation Summary. Bureau of Labor Statistics: United States Department of Labor. Dostupné z: http://www.bls.gov/news.release/empsit.nr0.htm

FENN, Jackie, Mark RASKINO, a Betsy BURTON. *Understanding Gartner's Hype Cycles*. Gartner, 2017. Dostupné z: https://www.gartner.com/doc/2538815/understanding-gartners-hype-cycles

Gartner Identifies Top 10 Strategic IoT Technologies and Trends. Dostupné z: https://www.gartner.com/en/newsroom/press-releases/2018-11-07-gartner-identifies-top-10-strategic-iot-technologies-and-trends

GRIGG, Ian. *Triple Entry Accounting.* 2005. DOI: 10.13140/RG.2.2.12032.43524. Dostupné z: https://doi.org/10.13140/RG.2.2.12032.43524

HABEEB, Ahmed. *Introduction to Secure Hash Algorithms*. University of Mansoura, 2018. DOI: 10.13140/RG.2.2.11090.25288. Dostupné z: https://doi.org/10.13140/RG.2.2.11090.25288

HANYCH, Michal, Anna DRGOVÁ a Michal GREMLICA. *Zdanění kryptoměn.* SimpleTax, 2018. Dostupné z: http://zdanenikryptomen.cz/zdanenikryptomen.pdf

HILEMAN, Garrick a Michel RAUCHS. *2017 Global Cryptocurrency Benchmarking Study.* SSRN Electronic Journal. University of Cambridge, 2017. DOI: 10.2139/ssrn.2965436. ISSN 1556-5068. Dostupné z: https://doi.org/10.2139/ssrn.2965436

Hype křivka vám pomůže pochopit technologické cykly. KPC Group. Dostupné z: https://kpc-group.cz/blog/metodika/hype-krivka

CHAN, David Y. a Miklos A. VASARHELYI. *Innovation and Practice of Continuous Auditing. Continuous Auditing*. Emerald Publishing Limited, 2018, 271-283. DOI: 10.1108/978-1-78743-413-420181013. ISBN 978-1-78743-414-1. Dostupné z: https://www.doi.org/10.1108/978-1-78743-413-420181013

CHAPPELL, David. I*ntroducing Blue Prism: Robotic Process Automation for the Enterprise*. 2017. Dostupné z: http://www.davidchappell.com/writing/white_papers/Introducing_Blue_Prism_v2--Chappell.pdf

CHEN, Hsueh-Ju, Shaio YAN HUANG, An-An CHIU a Fu-Chuan PAI. *The ERP system impact on the role of accountants*. 2012, 112 (1), 83-101. DOI: 10.1108/02635571211193653. ISSN 0263-5577. Dostupné z: https://www.doi.org/10.1108/02635571211193653

IBM Blockchain. IBM [online]. Dostupné z: https://www.ibm.com/blockchain

Internet of things. IoT Tech News: Internet of Things news and strategy [online]. Dostupné z: https://www.iottechnews.com/

ISSA, Hussein, Ting SUN a Miklos A. VASARHELYI. *Research Ideas for Artificial Intelligence in Auditing: The Formalization of Audit and Workforce Supplementation.* Journal of Emerging Technologies in Accounting. 2016, 13 (2), 1-20. DOI: 10.2308/jeta-10511. ISSN 1554-1908. Dostupné z: https://doi.org/10.2308/jeta-10511

KALČEV, Petr. *Úvod do databází: Modelování v řízení*. Dostupné z: http://people.fsv.cvut.cz/~dlaskpet/Help/UvodDoDatabazi.pdf

KOKINA, Julia, Ruben MANCHA a Dessislava PACHAMANOVA. *Blockchain: Emergent Industry Adoption and Implications for Accounting.* Journal of Emerging Technologies in Accounting. 2017, 14 (2), 91-100. DOI: 10.2308/jeta-51911. ISSN 1554-1908. Dostupné z: https://doi.org/10.2308/jeta-51911

KRAUSE, Max J. a Thabet TOLAYMAT. *Quantification of energy and carbon costs for mining cryptocurrencies.* Nature Sustainability, 2018. DOI: 10.1038/s41893-018-0152-7. ISSN 2398-9629. Dostupné z: https://www.nature.com/articles/s41893-018-0152-7

KOSTIĆ, Nikola a Xiao TANG. *The future of audit: Examining the opportunities and challenges stemming from the use of Big Data Analytics and Blockchain technology in audit practice.* 2017. Diplomová práce. Lund University. Vedoucí práce Rolf Larsson. Dostupné z: http://lup.lub.lu.se/student-papers/record/8916727

LAMPORT, Leslie, Robert SHOSTAK a Marshall PEASE. *The Byzantine Generals Problem.* ACM Transactions on Programming Languages and Systems. 1982, 4 (3), 382-401. DOI: 10.1145/357172.357176. ISSN 01640925. Dostupné z: https://doi.org/10.1145/357172.357176

MAINELLI, Michael a Matthew LEITCH. *Auditing Mutual Distributed Ledgers (aka Blockchains): A Foray Into Distributed Governance & Forensics*. Long Finance, 2017. Dostupné z: https://www.zyen.com/media/documents/Audting_Mutual_Distributed_Ledgers_aka_Blockchains_2017.pdf

MATUSZYŃSKI, Dariusz. *Co je Blockchain a jak funguje.* Kryptomagazín. 22. dubna 2018. Dostupné z: https://kryptomagazin.cz/co-je-blockchain/

MIKYNA, Jiří a Libuše ŠNAJDROVÁ. *Auditorská obec v číslech.* Auditor. č. 2/2018 Komora auditorů ČR, 2018, XXV. ročník, s. 13-16. ISSN 1210-9096.

MOFFITT, Kevin C., Andrea M. ROZARIO a Miklos A. VASARHELYI. *Robotic Process Automation for Auditing.* Journal of Emerging Technologies in Accounting. 2018, 15 (1), 1-10. DOI: 10.2308/jeta-10589. ISSN 1554-1908. Dostupné z: http://doi.org/10.2308/jeta-10589

NAKAMOTO, Satoshi. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Dostupné z: https://bitcoin.org/bitcoin.pdf

Nařízení, směrnice a další právní akty. Evropská unie. Dostupné z: https://europa.eu/european-union/eu-law/legal-acts_cs

O Komoře auditorů. Komora auditorů České republiky. Dostupné z: https://www.kacr.cz/o-komore-auditoru/

PEASE, M., R. SHOSTAK a L. LAMPORT. *Reaching Agreement in the Presence of Faults.* Journal of the ACM. 1980, 27 (2), 228-234. DOI: 10.1145/322186.322188. ISSN 00045411. Dostupné z: https://doi.org/10.1145/322186.322188

PECK, Morgen E. *Blockchain world - Do you need a blockchain? This chart will tell you if the technology can solve your problem.* IEEE Spectrum. 2017, 54. ročník (10. vyd.), 38-60. DOI: 10.1109/MSPEC.2017.8048838. ISSN 0018-9235. Dostupné z: https://doi.org/10.1109/MSPEC.2017.8048838

Phishing. In: Phising.org. Dostupné z: http://www.phishing.org/what-is-phishing

PwC Blockchain Executive Summary. PwC. 2018. Dostupné z: https://www.pwc.com/jg/en/publications/blockchain-is-here-next-move.html

Realizing the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies. The World Economic Forum. 28. června 2017. Dostupné z: https://www.weforum.org/whitepapers/realizing-the-potential-of-blockchain

ROZARIO, Andrea M. *Reshaping the Audit with Blockchain and Artificial Intelligence: An External Auditor Blockchain for Close to Real-Time Audit Reporting.* Rutgers Accounting Web, 2017. Dostupné z: http://raw.rutgers.edu/docs/wcars/41wcars2/Andrea_Rozario.pdf

ROZARIO, Andrea M. a Miklos A. VASARHELYI. *Auditing with Smart Contracts.* The International Journal of Digital Accounting Research. 2018, 1-27. DOI: 10.4192/1577-8517-v18_1. Dostupné z: https://www.doi.org/10.4192/1577-8517-v18_1

RÜCKESHÄUSER, Nadine. *Do We Really Want Blockchain-Based Accounting? Decentralized Consensus as Enabler of Management Override of Internal Controls*. 13th International Conference on Wirtschaftsinformatik. St. Gallen, Švýcarsko, 2017, s. 16-30.

Smart Property. Bitcoin Wiki. Dostupné z: https://en.bitcoin.it/wiki/Smart_Property

SILVOSO, J. A. *Report of the Committee on Basic Auditing Concepts*. The Accounting Review. American Accounting Association, 1972, (Vol. 47), 15-74. Dostupné z: https://www.jstor.org/stable/244879

Statement on Potentially Unlawful Online Platforms for Trading Digital Assets: Public Statement. U.S. Securities and Exchange Commission. 7. března 2018. Dostupné z: https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading

SWAN, Melanie. *Blockchain Temporality: Smart Contract Time Specifiability with Blocktime. Rule Technologies. Research, Tools, and Applications.* Cham: Springer International Publishing, 2016, 184-196. Lecture Notes in Computer Science. DOI: 10.1007/978-3-319-42019-6_12. ISBN 978-3-319-42018-9. Dostupné z: https://doi.org/10.1007/978-3-319-42019-6_12

SZABO, Nick. *Smart Contracts*. 1994. Dostupné z: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

TANG, Jiali Jenna a Khondkar E. KARIM. *Big Data in Business Analytics: Implications for the Audit Profession.* The CPA Journal: The Voice of the Profession, červen 2018. Dostupné z: https://www.cpajournal.com/2017/06/26/big-data-business-analytics-implications-audit-profession/

UCHITELLE, Louis. *U.S. lost 2.6 million jobs in 2008*. The New York Times. New York, 2009. Dostupné z: https://nyti.ms/2kv08Xo

VASARHELYI, Miklos A., J. Donald WARREN Jr., Ryan A. TEETER a William R. TITERA. *Embracing the automated audit: How the Audit Data Standards and audit tools can enhance auditor judgment and assurance.* Journal of Accountancy. April, 2014, s. 34-37. ISSN 1945-0729. Dostupné z: https://www.journalofaccountancy.com/issues/2014/apr/automated-audits-20127039.html

XBRL: The Business Reporting Standard. Dostupné z: https://www.xbrl.org/

YERMACK, David. *Corporate Governance and Blockchains*. Review of Finance. Oxford University Press, 2017, 21 (1). DOI: 10.1093/rof/rfw074. ISSN 1572-3097. Dostupné z: https://doi.org/10.1093/rof/rfw074

YOON, Kyunghee. *Three Essays on Unorthodox Audit Evidence.* Newark, New Jersey, 2016. Disertační práce. Rutgers, The State University of New Jersey. Vedoucí práce Dr. Miklos A. Vasarhelyi. Dostupné z: https://doi.org/10.7282/T3DJ5HVN

YOON, Kyunghee, Lucas HOOGDUIN a Li ZHANG. *Big Data as Complementary Audit Evidence.* Accounting Horizons. 2015, 29 (2), 431-438. DOI: 10.2308/acch-51076. ISSN 0888-7993. Dostupné z: http://doi.org/10.2308/acch-51076

ZHENG, Zibin, Shaoan XIE, Hong Ning DAI, Xiangping CHEN a Huaimin WANG. *Blockchain challenges and opportunities: a survey.* International Journal of Web and Grid Services. 2018, 14 (4). DOI: 10.1504/IJWGS.2018.095647. ISSN 1741-1106. Dostupné z: http://doi.org/10.1504/IJWGS.2018.095647

ØLNES, Svein, Jolien UBACHT a Marijn JANSSEN. *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing.* Government Information Quarterly. 2017, 34 (3), 355-364. DOI: 10.1016/j.giq.2017.09.007. ISSN 0740624X. Dostupné z: https://doi.org/10.1016/j.giq.2017.09.007

České zákonné normy

Zákon č. 89/2012 Sb., občanský zákoník

Zákon č. 93/2009 Sb., o auditorech ve znění pozdějších předpisů

Zákon č. 284/2009 Sb., o platebním styku ve znění pozdějších předpisů

Zákon č. 563/1991 Sb., o účetnictví ve znění pozdějších předpisů

.

Seznam tabulek, grafů a obrázků