UNIVERZITA PARDUBICE

FAKULTA CHEMICKO-TECHNOLOGICKÁ

BAKALÁŘSKÁ PRÁCE

2022 Martin Jiřinec

Univerzita Pardubice
Fakulta chemicko-technologická

Využití technologie blockchain a kryptoměn v podnikovém prostředí

Bakalářská práce

2022 Martin Jiřinec

Univerzita Pardubice
Fakulta chemicko-technologická
Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Martin Jiřinec**
Osobní číslo:	**C19141**
Studijní program:	**B0488A050003 Ekonomika a management podniků chemického průmyslu**
Téma práce:	**Využití technologie blockchain a kryptoměn v podnikovém prostředí**
Zadávající katedra:	**Katedra ekonomiky a managementu chemického a potravinářského průmyslu**

Zásady pro vypracování

1. Vymezit podstatu technologie blockchain a fungování technologie blockchain.
2. Charakterizovat kryptoměny postavené na technologii blockchain.
3. Vymezit využití technologie blockchain v podnikovém prostředí.
4. Posoudit různé formy využití technologie blockchain v různých odvětvích hospodářství.
5. Provést zhodnocení a závěr.

Rozsah pracovní zprávy: **30**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. Attaran, M., Gunasekaran, A. Applications of Blockchain technology in business: challenges and opportunities. 2019. Cham, Switzerland: Springer Nature. ISBN 978-3-030-27797-0.
2. Choi, P. M. S., Huang, S. H. ed., Fintech with artificial intelligence, big data, and blockchain. 2021. Singapore: Springer Nature. Blockchain technologies. ISBN 978-981-33-6136-2.
3. Mařík, V., a kol. Průmysl 4.0 výzva pro Českou republiku. 2016. Praha: Management Press. ISBN 978-80-7261-440-0.
4. Pritzker, Y. Vynález jménem bitcoin. 2020. Praha: Braiins Publishing. ISBN 978-80-907975-0-5.
5. Tomek, G., Vávrová, V. *Průmysl 4.0 aneb Nikdo sám nevyhraje*. Průhonice: Professional Publishing. 2017. ISBN 978-80-906594-4-5.
6. Ministerstvo průmyslu a obchodu ČR. *Iniciativa Průmysl 4.0*. 2016.
7. Stroukal, D., Skalický J., 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 3., rozšířené vydání. Praha: Grada Publishing. Finance pro každého. ISBN 978-80-271-4256-9.

Vedoucí bakalářské práce: **Ing. Jana Košťálová, Ph.D.**
Katedra ekonomiky a managementu chemického a potravinářského průmyslu

Datum zadání bakalářské práce: **28. února 2022**
Termín odevzdání bakalářské práce: **1. července 2022**

L.S.

prof. Ing. Petr Kalenda, CSc.
děkan

Ing. Jan Vávra, Ph.D.
vedoucí katedry

V Pardubicích dne 22. února 2022

Prohlašuji:
Práci s názvem Využití technologie blockchain a kryptoměn v podnikovém prostředí jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 27.06.2022

Martin Jiřinec v. r.

Poděkování

Rád bych touto cestou poděkoval vedoucí práce Ing. Janě Košťálové, Ph.D. za odborné vedení a cenné rady při zpracování bakalářské práce, dále bych též chtěl poděkovat všem respondentům, kteří si našli čas a zodpověděli mé otázky.

ANOTACE

Tato práce se zabývá technologií blockchain a jejím využitím v klíčových oblastech podnikové praxe. V teoretické části je technologie popsána do detailů, včetně asymetrického šifrování, digitálního podpisu a hashovacích funkcí, které technologie blockchain využívá. Dále je představena oblast, ve které má blockchain zatím největší uplatnění, a to oblast kryptoměn. Na závěr teoretické části je uveden přehled využití technologie blockchain v podniku dle odborné literatury. Na teoretickou část navazuje praktická část, ve které jsou uvedeny další oblasti využití technologie blockchain a kryptoměn v podniku, a to na základě strukturovaných rozhovorů s odborníky, kteří se v tomto prostředí aktivně pohybují.

KLÍČOVÁ SLOVA

technologie blockchain, asymetrická kryptografie, decentralizace, kryptoměny, Bitcoin, průmysl 4.0

TITLE

The Blockchain technology

ANNOTATION

This thesis deals with Blockchain technology and its use in key areas of business practice. In theoretical part the technology is described in detail, including asymmetric encryption, digital signature, and hash functions, used by blockchain technology. The following is the area in which the blockchain technology has the greatest application so far, and that is the area of cryptocurrencies. At the end of the theoretical part is an overview of the use of blockchain technology in the company according to the specialised literature. The theoretical part is followed by the practical part, in which are listed application areas of the blockchain technology and cryptocurrencies in the company, based on structured interviews with experts from particular fields, who are actively involved in this environment.

KEYWORDS

blockchain technology, asymmetric cryptography, decentralization, cryptocurrencies, Bitcoin, industry 4.0

Obsah

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK

BCH – Bitcoin Cash

BTC – Bitcoin

BTG – Bitcoin Gold

CBDC – Central bank digital currency (digitální měny centrálních bank)

ČR – Česká republika

Dapps – Decentralizované aplikace

DeFi – Decentralizované finance

DLT – Distributed ledger technology (distribuovaná účetní databáze)

DPoS – Delegované proof of Stake

EDI – Electronic Data Interchange (elektronická výměna dat)

ETH – Ethereum

GPS – Global Positioning System (globální polohový systém)

GPU – Graphics processing unit (grafický procesor)

IIoT – Industry Internet of Things (průmyslový internet věcí)

IoT – Internet of Things (Internet věcí)

LTC – Litecoin

MB – Megabyte

NFT – Non-fungible token (nezaměnitelný token)

PoA – Proof of Authority

PoB – Proof of Burn

PoS – Proof of Stake

PoW – Proof of Work (důkaz o provedení práce)

QR code – Quick Response code

R3 – Průmyslové konsorcium

RFID – Radio Frequency Identification (identifikace na rádiové frekvenci)

Sat – Satoshi (nejmenší jednotka Bitcoinu)

SegWit – Segregate Witness

TUSD – TrueUSD

USD – Americký dolar

USDT – Tether

ÚVOD

Moderní technologie mění způsob života a také podobu ekonomiky, právě moderní technologie stojí za 4. průmyslovou revolucí. Jako každá průmyslová revoluce, i ta čtvrtá přichází s novými technologiemi, promítá se nejen do průmyslu, služeb, ale i do každodenního života, stává se součástí vzdělávání, bezpečnosti a také právních norem. Fenoménem dneška je propojování internetu věcí, služeb, lidí a s ním spojené obrovské množství generovaných dat. Moderní technologie vytváří možnost nových obchodních modelů, vzniku chytrých továren, ale také větší nároky na kybernetickou bezpečnost. Jedním z prvků čtvrté průmyslové revoluce je i technologie blockchain.

Když lidé prvně slyší o blockchainu, mají sklon si vytvořit názor ještě dříve, než se vůbec pokusí pochopit o co jde. Problémem části lidí je to, že ani nechtějí pochopit základy moderních technologií a zajímá je jen to, co už má ve světě pevně dané své místo nebo to bez čeho se v každodenním životě zkrátka neobejdou, jako je například internet. Ale kolik z nás ví, jak internet funguje, a dokázal by to jednoduše vysvětlit? Pravděpodobně to nebude každý, kdo internet používá. To však u blockchainu tak úplně nejde, k jeho využívání je potřeba znát matematiku, statistiku, šifrování a mít základy z dalších vědních oborů. A to je právě problém blockchainu a kryptoměn, ve kterých je blockchain využíván zatím nejvíce, nejdou jednoduše vysvětlit. Je také potřeba si odpovědět na otázky, zda blockchain vůbec potřebujeme a co blockchain vlastně řeší.

Blockchain je pojem, který si veřejnost spojuje především s kryptoměnou Bitcoin. Veřejnost se však chybně domnívá, že pojmy blockchain a Bitcoin jsou synonyma. Není tomu tak, Bitcoin je pouze jedním z prvních převedení technologie blockchain do praxe. Technologie blockchain se neustále vyvíjí a zdokonaluje. Existují i technologie, které stojí nad blockchainem a již dávno přesáhly první myšlenku decentralizované měny v podobě Bitcoinu, a tak se blockchain postupně dostává do nových oblastí, kde může být využit.

Čím je toto téma zajímavé? Jedná se o jednu z nejmodernějších technologií s velkým potenciálem využití v budoucnu. Moderní technologie jsou fascinující, neboť představují perspektivu a přínos pro společnost.

Cílem práce je v teoretické části popsat technologii blockchain, přiblížit obecné principy kryptografie fungování technologie blockchain, včetně technických principů, popsání oblasti kryptoměn, ve kterých se blockchain hojně využívá, a také dalších oblastí jeho využití v praxi, a to zejména v podnikové praxi.

Cílem praktické části je analyzovat využití této technologie v jednotlivých odvětvích prostřednictvím strukturovaných rozhovorů s odborníky z praxe a vymezit charakteristiky technologie blockchain a kryptoměn spolu s doplněním o využití zejména v podnikové praxi.

Ačkoliv existuje pro blockchain český překlad bločenka, bude v této práci upřednostněn název originální, anglický, jelikož český překlad není příliš rozšířený a rovněž není mezi odborníky populární.

1 Kryptografie

Pro pochopení principů blockchainu a jiných technologií založených na důvěryhodné archivaci dat, je nutná základní orientace v oblasti kryptografie. Kryptografie je vědní obor zabývající se metodami utajovaní a šifrování zpráv do podoby, která je čitelná jen se speciální znalostí. Této znalosti se říká šifrovací klíč. Šifrování je proces, při němž se z obecně čitelné sekvence dat, například dokumentu, při použití šifrovacího klíče vytvoří šifrovaná sekvence dat, tedy zašifrovaný dokument, šifra (*Binance academy,* 2018a). Zašifrovaný dokument bez znalosti šifrovacího klíče je nečitelný. Šifry dělíme na šifry symetrické a asymetrické (*Earchivace.cz*, 2014b).

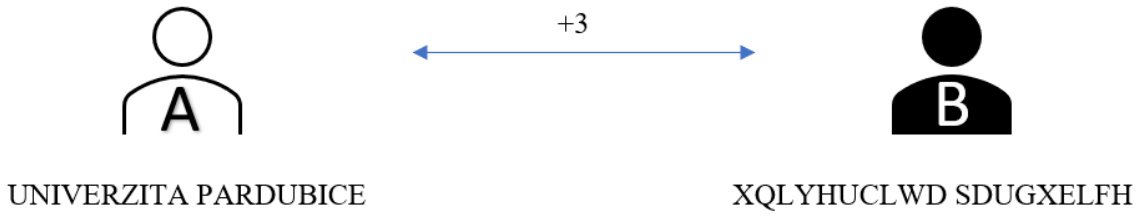
1.1 Symetrická kryptografie

Šifry symetrické využívají pro zašifrování i rozšifrování stejný klíč. Výhodou těchto šifer je rychlost a nízká výpočetní náročnost. Kvalita výsledného šifrovaného textu je dána použitým šifrovacím algoritmem a délkou šifrovacího klíče. Jeho nevýhodou je to, že šifrovací klíč musí být sdílen s každým účastníkem, který má zprávu zašifrovat či dešifrovat (*Earchivace*.cz, 2014b).

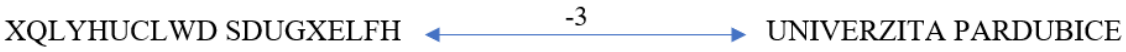
Obrázek 1- Symetrická kryptografie (vlastní zpracování)

Jednou z nejznámějších symetrických šifer je Caesarova šifra. Caesarova šifra sloužila pro vojenskou komunikaci a funguje na principu toho, že člověk A (dále Alice), který chce slovo zašifrovat, vezme dané slovo a posune každé písmeno o daný počet znaků v abecedě. Člověk B (dále Bob), který chce zprávu dešifrovat, zná šifrovací klíč, což je počet posunutí v abecedě, a zprávu tak dešifruje. Jako příklad Caesarovy šifry jsem zvolil slova UNIVERZITA PARDUBICE s šifrovacím klíčem +3, tj. posunutí o 3 písmena v abecedě dopředu čili Alice

chce Bobovi zašifrovat zprávu UNIVERZITA PARDUBICE s šifrovacím klíčem +3, který oba znají.



Obrázek 2 - Caesarova šifra, šifrování slova UNIVERZITA PARDUBICE (vlastní zpracování)



Obrázek 3 - Dešifrování slova UNIVERZITA PARDUBICE (vlastní zpracování)

Z výše uvedeného je zřejmé, že jde o jednoduché šifry s primitivními šifrovacími klíči, které při opakovaném použití lze prolomit. Blockchain symetrickou kryptografii nevyužívá, využívá složitější asymetrickou kryptografii.

1.2 Asymetrická kryptografie

Asymetrickou kryptografií se rozumí soubor kryptografických metod, u kterých šifrovací a dešifrovací klíč není stejný, používají se dva klíče, klíč soukromý a klíč veřejný. Tyto dva klíče tvoří klíčový pár. Klíčový pár je k sobě svázán na základě komplikovaného matematického algoritmu a tento pár patří neoddělitelně k sobě. Soukromý klíč (též privátní klíč) musí zůstat tajný a majitel ho používá k dešifrování jemu určené zprávy nebo k podepisování jím ověřované zprávy, případně odchozí transakce. Veřejný klíč může použít kdokoliv k zašifrování zprávy pro majitele soukromého klíče. Veřejný klíč může být vypočítán ze soukromého klíče, avšak nikoliv soukromý z toho veřejného. Asymetrie klíčů umožňuje adresátovi šifrované zprávy nesdílet s odesílatelem tajný dešifrovací klíč (soukromý klíč) a naopak druhý z páru klíčů zveřejnit (veřejný klíč) (Stroukal, Skalický, 2021).

Asymetrickou kryptografii používáme všichni častěji, než si vůbec uvědomujeme, běží nám v pozadí na počítači kdykoliv se pohybujeme na internetových stránkách využívající protokol https. Kombinace asymetrického šifrování a digitálních podpisů se využívá v internetovém bankovnictví. S asymetrickým šifrováním se můžeme též setkat v komunikačních aplikacích zprostředkovávajících výměnu zpráv, jako například aplikace Signal, která je open source čili má veřejný zdrojový kód a veřejný protokol a kdokoliv jej může

ověřit. Šifrování využívá též populární aplikace WhatsApp, ačkoli není open source, a tím pádem není nikdo schopen ověřit kvalitu jejího zabezpečení. V blockchainu se využívá asymetrická kryptografie v digitálních podpisech, které fungují na podobných principech. Jedním z největších prakticky nasazených projektů je Bitcoin (Vejmola, 2020b).

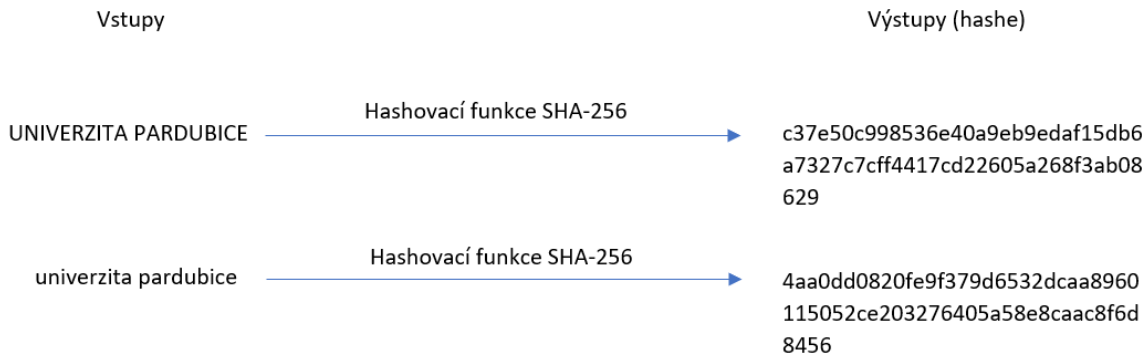
Obrázek 4 - Asymetrická kryptografie (vlastní zpracování)

1.3 Hashovací funkce

Hashovací funkce je speciální funkce, do které vložíme-li jakýkoliv řetězec písmen, čísel nebo jiných údajů, dostaneme otisk – výstup, který je pro daný vstup jedinečný. Otisk neboli hash, má podle použité funkce jednoznačnou délku v bitech, např. 160 bitů, 256 bitů a podobně. Hashovací funkce mají několik klíčových vlastností (Pritzker, 2020):

- **jednosměrnost** – z výstupu (hashe) dané funkce, nelze zjistit vstup;
- **jednoznačnost** – výstup je pevně daný, stejný vstup vždy vyprodukuje stejný výstup**;**
- **vysoká nelinearita** – změna jen jednoho písmena, přidání mezery nebo doplnění tečky radikálně změní výstup, a to tak, že nelze vypozorovat jakoukoliv korelaci;
- **nezaměnitelnost** – není možné najít dva vstupy, které by vyprodukovali stejný výstup.

V současné době je nejpoužívanější hashovací funkcí SHA, bitcoinový protokol využívá hashovací funkci SHA-256. Pro příklad si zvolím dvě hesla, na které aplikuji hashovací funkci SHA-256, UNIVERZITA PARDUBICE a univerzita pardubice. Jediný rozdíl je v tom, že první heslo je napsané velkými písmeny a druhé malými, přesto dostaneme rozdílný výstup, hash (Pritzker, 2020).



Obrázek 5 - Příklad hashovací funkce (vlastní zpracování)

Hashovací funkce jsou běžně používané datové struktury ve výpočetních systémech pro úkoly, jako je kontrola integrity zpráv a ověřování informací. Používají se všude tam, kde není žádoucí, aby třetí strana odhalila námi napsanou zprávu. V rámci internetové bezpečnosti se tento způsob šifrování uplatňuje například při zadávání hesel nebo elektronických podpisů. Pokud si zvolíte heslo do e-mailu nebo na webovou stránku, projde hashovacím procesem a do cílové databáze se uloží jako pouhý otisk, který má podobu shluku písmen a čísel. *(Digitální pevnost*, 2018). Hashovací funkce hrají taktéž důležitou roli při těžbě kryptoměn, což je vysvětleno v následujících kapitolách.

1.4 Digitální podpisy

Digitální podpis jednoznačně zajišťuje, že podepsaný dokument, soubor nebo transakce byl podepsán určitou osobou nebo systémem. Vytvoření a platnost digitálního podpisu je založeno na asymetrické kryptografii a hashovacích funkcích. Pro digitální podpis jsou důležité tyto dvě vlastnosti (*Earchivace.cz*, 2014a):

- **nezfalšovatelnost** – digitální podpis nelze vytvořit bez znalosti soukromého klíče podepisované osoby;
- **nepopíratelnost** – digitální podpis dokládá s právní vymahatelností, že byl použit pro podepsání dokumentu.

Obrázek 6 - Vytvoření digitálního podpisu (vlastní zpracování)

Jak digitální podpis vytvořit? Digitální podpis probíhá ve dvou krocích. V prvním kroku se vytvoří hash podepisovaného souboru a v druhém kroku se získaný hash zašifruje soukromým klíčem podepisovaného. Takto vytvořený digitální podpis se připojí k podepisovanému souboru, jehož je součástí. Ověřování platnosti digitálního podpisu probíhá také ve dvou paralelních krocích. Vytvoří se hash originálního dokumentu stejnou hashovací funkcí, jaká byla použita při podepisování. Zároveň s tím se dešifruje hash pomocí veřejného klíče uživatele, jenž dokument podepsal. Následně se oba hashe porovnají. Pokud jsou stejné, je ověřena platnost podpisu, v opačném případě je podpis neplatný (*Earchivace.cz*, 2014a).

2 Blockchain

Základem blockchainu je technologie distribuované účetní databáze (Distributed ledger technology – DLT), ve které jsou navždy uloženy veškeré záznamy, které jsme do ní vložili. DTL nabízí konsenzus mechanismus ověřování prostřednictvím sítě počítačů, které umožňují transakce typu peer-to-peer bez potřeby centrální autority. Každá transakce je ověřována a po úspěšném ověření je přidán nový blok do řetězce již existujících bloků, z toho je také odvozen název blockchain čili řetězec bloků (Reennok, Cohn, Butcher, 2018).

Technologie blockchain byla poprvé představena v roce 1991 Stuartem Haberem a W. Scottem Stornettou, dvěma výzkumníky, kteří chtěli implementovat systém, kde by nebylo možné falšovat časová razítka dokumentů. Ale teprve téměř o dvě desetiletí později, byla v roce 2008 zaregistrována doména bitcoin.org a publikován vědecký článek s názvem Bitcoin: A Peer-to-Peer Electronic Cash System. Článek popisuje koncept technologie blockchainu a představení kryptoměny Bitcoin. Se spuštěním Bitcoinu v lednu 2009 měl blockchain svou první reálnou aplikaci (Conway, 2021).

Blockchain není tak úplně novou revoluční technologií. Všechny prvky, které využívá, tedy internet, kryptografii a přenosový protokol, jsou známy již několik desítek let a kryptografie dokonce stovky let. Revoluční na něm tedy nejsou technologie samotné, ale způsob, jakým stávající technologie využívá (Wolf, 2019).

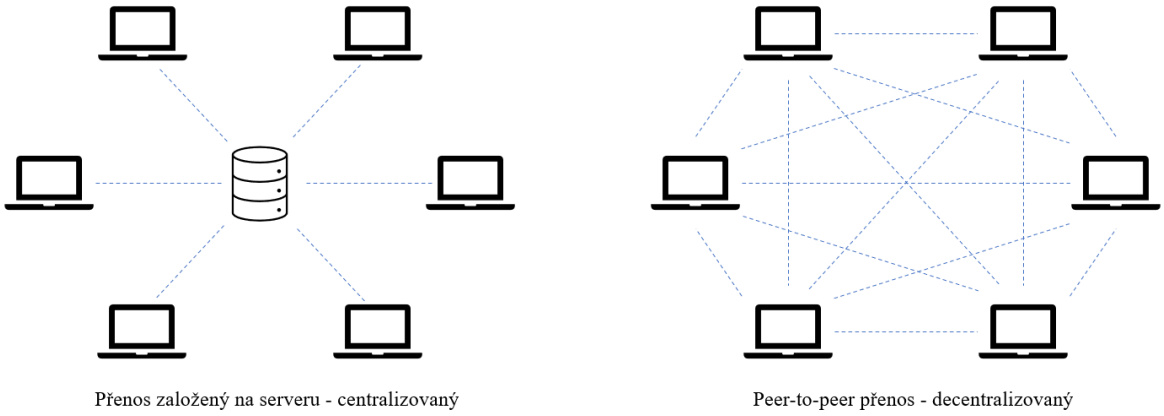
2.1 Principy fungování blockchainu

Blockchain se skládá ze dvou typů záznamů, a to z transakcí a bloků. Jako transakce označujeme data, která do databáze vkládají samotní uživatelé blockchainu (například převod kryptoměn). Transakce, které uživatelé vytvoří, se předávají od uzlu k uzlu v závislosti na tom, kdo s kým má v tu danou dobu navázané spojení. Za validní transakci se považuje taková transakce, která obsahuje správný elektronický podpis uživatele, v případě kryptoměn je patrný finanční pohyb v peněžence a splňuje další podmínky, jako je například odměna pro uživatele, zatímco bloky tyto transakce díky úsilí těžařů shromažďují a potvrzují. Potvrzují, kdy a jak byly transakce do databáze blockchainu přidány a jestli je vše podle pravidel (*Finex*, 2018).

Blockchain funguje na několika základních principech (Lansiti, Lakhani, 2017):

- **distribuovaná databáze** – kniha je sdílena ve velkém počtu identických databází. Každý účastník má přístup k celé databázi a žádný jednotlivý účastník nekontroluje data ani informace. Záznamy o transakcích lze ověřit přímo, aniž by bylo potřeba zprostředkovatelů třetích stran;

- **peer-to-peer přenos** – komunikace mezi uzly probíhá přímo bez nutnosti centrální koordinace. Uzly simultánně fungují jako „klienti“ a „servery“ k ostatním uzlům v sítí;
- **transparentnost s pseudonymitou** – každou transakci a její hodnotu vidí každý, kdo má přístup do systému. Každý uzel nebo uživatel na blockchainu má jedinečnou alfanumerickou adresu s několika znaky, která jej identifikuje. Uživatelé se mohou rozhodnout zůstat v anonymitě nebo poskytnou důkaz o své identitě ostatním;
- **nevratnost záznamů** – jakmile je transakce zadána do databáze a účty jsou aktualizovány, záznamy nelze měnit, protože jsou propojeny se všemi záznamy o transakcích, které byly před nimi. Jsou zavedeny různé výpočetní algoritmy a přístupy, které zajišťují, že záznam v databázi je trvalý, chronologicky seřazený a dostupný pro všechny ostatní v síti;
- **výpočetní logika** – digitální povaha účetní knihy znamená, že transakce blockchainu mohou být svázány s výpočetní logikou a v podstatě naprogramovány. Uživatelé tak mohou nastavit algoritmy a pravidla, která automaticky spouští transakce mezi uzly.



Obrázek 7 – Peer-to-peer přenos (vlastní zpracování)

Attaran a Gunasekaran (2019) pak těchto pět základních principů doplňují o další neméně podstatný, a to **rychlost transakce,** neboť transakce v systému založeném na blockchainu jsou dokončené a ověřitelné během několika sekund bez zásahu člověka.

Známy jsou tři typy blockchainů. **Veřejné blockchainy** jsou určeny k odstranění požadavku na prostředníka a jsou navrženy tak, aby byly přístupné každému, kdo má přístup k počítači a k internetu. Veřejné blockchainy se nejvíce uplatňují tam, kde je potřeba čistě decentralizovaná transakce. Příkladem je bitcoinový blockchain a další kryptoměny jako Ethereum a další. Tyto veřejné blockchainy jsou pomalé a náročné na zdroje kvůli vysokým nárokům na výpočetní kapacitu a výkon, který je k provádění transakcí nutný. Výhodou je, že jsou velmi bezpečné (Pinto, 2019).

Soukromý blockchain funguje na principu, kdy společnost zřizuje síť oprávnění, kde jsou všichni účastníci známí a důvěryhodní. Přístup k síťovému systému je omezen. Aby se účastníci mohli připojit, je třeba získat pozvánku nebo povolení. Ověřování může být povoleno pouze některým uzlům prostřednictvím správce (Pinto, 2019). To je užitečné, když je blockchain používán mezi společnostmi, které patří stejnému majiteli. Soukromý blockchain nabízí několik výhod, včetně vyšší rychlosti transakcí, dostupnosti dat a centralizované kontroly nad poskytováním přístupu k blockchainu. Své uplatnění soukromý blockchain najde v obchodních a vládních modelech. Vlády by například mohly využívat blockchain pro hlasování a současně ušetřit miliardy, protože hlasování se stane plně odolným proti korupci a skutečně bezpečné (Thompson, 2016). Velká část aplikace soukromého blockchainu probíhá ve finančních službách. NASDAQ, Bank of America, JPMorgan, New York Stock Exchange a Fidelity Investments testují soukromou technologii blockchain jako náhradu za papírové a manuální transakce (Lansiti, Lakhani, 2017).

Hybridní blockchain kombinuje veřejný a soukromý blockchain a bere si z obou typů to nejlepší. Hybridní blockchain se skládá z veřejného blockchainu, jehož jsou všichni účastníci součástí, a soukromé sítě, která omezuje účast jen na základě pozvání, či oprávnění. Tato technologie umožňuje flexibilitu a kontrolu nad tím, jaká data jsou uchována a jaká jsou sdílena s veřejností. Existuje několik reálných příkladů využití hybridního blockchainu (Freuden, 2018). Například XinFin je hybridní blockchain postavený jak na Ethereu (veřejný blockchain), tak na Quoru (soukromý blockchain). XinFin dokončil několik pilotních projektů napříč logistikou dodavatelského řetězce (supply chain logistics), letectvím, mezinárodním obchodem a finančním vypořádáním. Ramco Systems, globální společnost zabývající se vývojem podnikového softwaru, poskytuje svým klientům hybridní řešení blockchainu XinFin k implementaci logistických řešení dodavatelského řetězce na bázi blockchainu (Freuden, 2018).

2.2 Blockchain a kryptoměny

Jako první přišel s využitím blockchainu Satoshi Nakamoto, což je jeden člověk nebo skupina lidí, kteří stojí za vznikem prvních decentralizovaných peněz, za Bitcoinem, který je prvním využitím technologie blockchain na světě (*Finex,* 2018).

O validaci transakcí se stará samotná síť. Uživatelé, kteří se na validaci transakcí podílejí, jsou za svou aktivitu odměňování v podobě síťových tokenů daného blockchainu. Tyto uživatelé jsou označováni jako těžaři a jejich činností je těžba. Odměnou jim jsou kryptoměny, například Bitcoin, Litecoin, Ethereum atd., podle toho, na jaké síti fungují. Tyto tokeny jsou

snadno směnitelné do dnešních státem vydávaných peněz s nuceným oběhem, označovaných jako fiat money (Wolf, 2019).

Jak se do blockchainu přidávají bloky, když neexistuje jeden nadřazený uzel, který by všem říkal, co je třeba dělat? Všechny uzly si jsou rovnocenné, takže musí existovat mechanismus, který bude spravedlivě rozhodovat o tom, kdo může přidávat bloky do blockchainu. Potřebujeme systém, který zajistí, že podvádění bude pro uživatele nákladné, a naopak jednání čestné bude odměněno. V souvislosti s kryptoměnami se používá veřejný blockchain, síť funguje bez nutnosti povolení, vytváření bloků musí tedy být přístupné všem (*Binance academy*, 2019). Protokoly to zajistí tím, že vyžadují, aby uživatel musel vystavit riziku své vlastní peníze čili vložit podíl, kterým může být například nákup hardwaru, či využitá energie. Vložení určitého podílu mu umožní podílet se na vytváření bloků, a pokud vygeneruje platný blok, bude mu vyplacena odměna. Pokud se však pokusí podvádět, zbytek sítě se o tom dozví a vložený podíl bude ztracen. Těmto mechanismům říkáme konsensuální algoritmy, protože účastníkům umožňují dosáhnout konsensu o tom, jaký blok se má přidat (*Binance academy, 2019)*.

2.3 Proof of Work

Proof of Work (PoW) se dá do češtiny přeložit jako důkaz o vykonané práci a je typickým příkladem těžby. Jedná se o nejčastěji používaný konsensuální algoritmus. Představit si to lze jako soutěž o vyřešení složitého matematického problému. Ten, kdo problém vyřeší jako první, získá odměnu. Blok transakce se dle předem daných pravidel naplní, těmito pravidly může být například určitý objem bloku nebo čas. Zatím neověřené transakce se dostanou k těžařům. Ti blok vezmou a pomocí hashovací funkce převedou velké množství dat na hash. U systému PoW se do bloku přidá ještě nonce. Nonce označuje v kryptografii číslo, které se používá jako jednorázová hodnota přinášející náhodný element (Vencl, 2021). Takové hodnotě není přisuzován žádný specifický význam, její role spočívá pouze v její libovolnosti a nemožnosti ji odhadnout. Program změní nonce, software vyřeší hash a kontroluje, zda splňuje všechny požadavky, pokud ne celý proces se opakuje. K validaci transakcí je zapotřebí vysokého výpočetního výkonu a zároveň je potřeba i štěstí, jelikož těžaři generují hashe a kontrolují, zda jejich vygenerovaný hash je ten pravý. K řešení se používá buď speciální hardware tzv. ASIC miner, anebo grafické karty (Vencl, 2021).

Podílem při těžbě jsou náklady na hardware a elektrická energie potřebná na jeho provoz. ASIC minery jsou postaveny za jediným účelem a nemají využití v aplikacích mimo těžbu kryptoměn. Jediným způsobem, jak získat zpět počáteční investici, je těžba, která přináší

značnou odměnu, pokud úspěšně přidáte nový blok do blockchainu. Aby těžaři mohli co nejvíce zvýšit svojí šanci na odměnu, začali se spojovat a vytvářet těžební pooly. Prvním takový poolem byl Slush Pool, který vznikl v České republice (ČR) (*Binance academy*, 2018c).

PoW využívá mnoho kryptoměn, například Bitcoin, Litecoin, Monero a Dash. Mezi výhody tohoto algoritmu patří (*Binance academy*, 2019):

- **osvědčenost** – PoW je nejrozšířenější konsensuální algoritmus;
- **otevřenost** – zapojit se do těžební soutěže může kdokoliv;
- **decentralizace** – těžaři při vytváření bloků soutěží s sebou navzájem, což znamená, že kontrola nad hashovacím výkonem nikdy nespočívá v rukou jediného účastníka.

Naopak nevýhodou algoritmu PoW jsou (*Binance academy*, 2019):

- **vysoké náklady** – těžba spotřebovává obrovské množství elektrické energie;
- **postupně se zvyšující bariéry vstupu** – protokoly se zvyšujícím se počtem těžařů zvyšují obtížnost těžební hádanky. Aby uživatelé zůstali konkurenceschopní, musí investovat do lepšího vybavení;
- **hrozba 51% útoku** – ačkoliv těžba podporuje decentralizaci, existuje možnost, že jeden těžař získá většinu hashovacího výkonu. Pokud k tomu dojde, může teoreticky vrátit transakce a ohrozit bezpečnost blockchainu.

2.4 Proof of Stake

Protokol Proof of Stake (PoS) je mechanismus konsensu, podle kterého účastníci sítě mohou těžit (též validovat nebo ověřovat) záznamy v závislosti na počtu žetonů, které drží. (Dapp, Helbing, Klauser, 2021). PoS je konsensus o úspoře energie, který má nahradit PoW. Místo toho, aby PoS spotřebovával velké množství výpočetního výkonu jako PoW, vybere jeden uzel k vytvoření dalšího bloku na základě výše vsazené částky. Algoritmus PoS namísto používání hashovacích funkcí využívá digitální podpisy, které prokazují vlastnictví dané kryptoměny. PoS je protokol konsensu o pravděpodobnosti a konečnosti, kde šance na vytvoření bloku závisí na „bohatství“. Vzhledem k tomu, že nejbohatší uzel musí dominovat síti, je výběr tvůrce na základě výše podílu dosti nespravedlivý. Mnoho výzkumníků proto navrhlo nová schémata, která by rozhodovala o uzlu k vytvoření dalšího bloku (Zhang, 2022).

PoS využívá řada kryptoměn, mezi nejznámější patří Cardano a VeChain, a přechod z PoW na PoS chystá také druhá největší kryptoměna Ethereum. Mezi výhody PoS patří (*Binance academy*, 2019):

- **šetrnost k životnímu prostředí** – stakování odstraňuje potřebu operací hashování, které jsou náročné na zdroje a tím pádem je snížena uhlíková stopa**;**

- **rychlejší transakce** – jelikož není třeba vynakládat další výpočetní výkon, PoS by mohla zvýšit propustnost transakcí;
- **odměny za stykování a úroky** – namísto těžařům se odměny vyplácejí přímo držitelům tokenů, kteří si mohou tímto vytvořit pasivní příjem.

K nevýhodám konsensu PoS patří:

- **relativně neotestované, nové** – protokoly PoS se zatím netestují ve velkém měřítku, dle kritiků má PoS řadu slabých míst;
- **plutokracie** – protokol PoS zvýhodňuje ty validátory, kteří drží více tokenů.

2.5 Další konsensuální algoritmy

Delegované PoS (DPoS) jsou postaveny na principu zastupitelské demokracie na rozdíl od PoS, které stojí na principu přímé demokracie. V DPoS hlasují zúčastněné strany o volbě delegátů. Volení delegáti zodpovídají za vytváření a ověřování bloků. Hlasování v DPoS je důležité, protože umožňuje zúčastněným stranám dát delegátům právo vytvářet bloky místo vytváření samotných bloků; DPoS tak může snížit výpočetní spotřebu energie zúčastněných stran na nulu (Zhang, 2022).

Proof of Authority (PoA) je algoritmus konsensu založený na pověsti, který zavádí praktické a efektivní řešení pro blockchainové sítě (zejména ty soukromé). Algoritmus shody PoA využívá hodnotu identit, což znamená, že validátoři bloků nevkládají mince, ale vlastní pověst. Model PoA spoléhá na omezený počet validátorů bloků, a proto se jedná o vysoce škálovatelný systém. Bloky a transakce jsou ověřovány předem schválenými účastníky, kteří působí jako moderátoři systému. Algoritmus konsensu PoA lze použít v různých scénářích a je považován za vysoce hodnotnou volbu pro logistické aplikace. Pokud jde například o dodavatelské řetězce, je PoA považováno za efektivní a rozumné řešení. (*Binance academy*, 2018a).

Proof of Burn (PoB) v zásadě vypadá jako algoritmus PoW, ale se sníženou spotřebou energie. Proces ověřování bloků v sítích založených na PoB nevyžaduje použití výkonných výpočetních prostředků a nezávisí na výkonném těžebním hardwaru (jako jsou ASIC). Místo toho jsou kryptoměny záměrně spalovány jako způsob jak „investovat“ zdroje do blockchainu, takže těžaři nemusí investovat fyzické zdroje. Funguje na principu, který umožňuje těžařům „spálit“ tokeny virtuální měny. Poté jim bude uděleno právo psát bloky v poměru k spáleným mincím. V systémech PoB těžaři investují do virtuálních těžebních souprav (nebo virtuální těžební síly). Jinými slovy, pomocí vypalování mincí jsou uživatelé schopni prokázat svůj závazek vůči síti, získat tak právo „těžit“ a ověřovat transakce. (*Binance academy*, 2018b).

3 Kryptoměny

Definovat nějakým způsobem kryptoměny je poměrně obtížné, jelikož není jasné, kdo a jakým způsobem může kryptoměny definovat, ne každá kryptoměna má stejné využití a zákony týkající se kryptoměn se omezují jen na daňovou problematiku. Kryptoměny tak bývají označovány jako podmnožina krypto-aktiv, či jako virtuální aktiva.

Definice Evropského orgánu pro bankovnictví definuje krypto-aktiva jako aktivum (majetek), který (Uhlířová, 2020):

- závisí primárně na kryptografii a DLT nebo obdobných technologiích jako součásti jejich domnělé či inherentní hodnoty;
- není vydávaný ani garantovaný centrální bankou či jinou veřejnoprávní institucí;
- může být použit jako prostředek směny anebo pro investiční účely anebo k přístupu ke zboží či službám.

Frankenfield (2021) tvrdí, že kryptoměny jsou digitální nebo virtuální měny, které jsou zabezpečeny kryptografií, což téměř znemožňuje padělání nebo dvojí útratu, tzv. double spend. Mnoho kryptoměn jsou decentralizované sítě založené na technologii blockchain – Charakteristickým rysem kryptoměn je to, že je obecně nevydává žádný centrální orgán, což je činí teoreticky imunními vůči vládním zásahům nebo manipulaci (Frankenfield, 2021b).

První kryptoměnou založenou na blockchainu byl Bitcoin, který stále zůstává nejpopulárnější a nejcennější. V současné době existují tisíce alternativních kryptoměn s různými funkcemi a specifikacemi, k 30. 10. 2021 jich je dle webu coinmarketcap 6903, přičemž každý den další vznikají a neúspěšné zanikají. Některé z nich jsou klony nebo forky Bitcoinu (blíže viz kapitola 3.3 Softfork a hardfork), zatímco jiné jsou nové měny, které byly vytvořeny od nuly. K 30. 10. 2021 bylo v oběhu více než 18,8 milionu bitcoinů s celkovou tržní kapitalizací kolem 1,115 bilionu USD, přičemž tento údaj se v závislosti na vývoji kurzu Bitcoinu k dolaru v čase mění. Některé z konkurenčních kryptoměn vzniklých díky úspěchu Bitcoinu, známe jako „altcoiny“, například Litecoin, Peercoin a Namecoin, stejně jako Ethereum, Cardano a EOS. Na konci října 2021 byla souhrnná hodnota (tržní kapitalizace) všech existujících kryptoměn přes 2,5 bilionu USD – bitcoin v současnosti představuje přibližně 44,5 % celkové hodnoty všech kryptoměn (*CoinMarketCap*, 2021).

S kryptoměnami lze provádět transakce, tedy přesouvat je z jednoho počítače, telefonu či hardwarové peněženky do druhé, a to nehledě na to, ve které části světa se nacházejí. Pomocí kryptoměn tedy lze s prakticky nulovými poplatky platit komukoli za cokoli, aniž by o tom

někdo jiný věděl nebo to mohl zastavit. Nástrojem pro bezpečné uchování kryptoměn jsou kryptoměnové peněženky (*Finex*, 2016).

3.1 Kryptoměnové klíče a peněženky

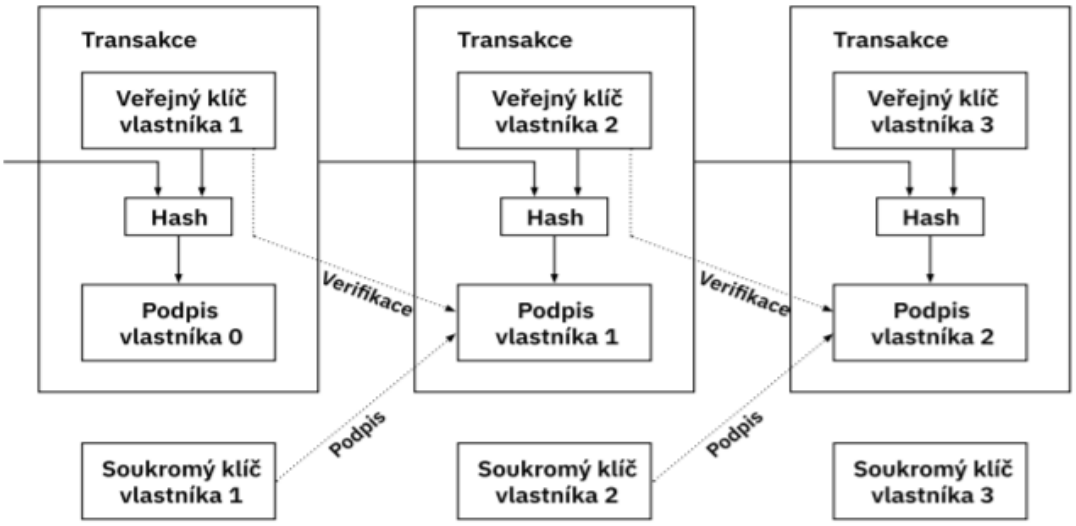
Kryptoměnové klíče souvisejí s asymetrickou kryptografií, jsou známy dva: veřejný klíč a soukromý klíč. Veřejný klíč umožňuje v rámci kryptoměn přijímat transakce, hashem veřejného klíče jsme totiž schopni získat veřejnou adresu, která slouží k přijímání bitcoinů. Veřejný klíč je kryptografický kód, který je spárován se soukromým klíčem. Zatímco kdokoli může posílat transakce na veřejnou adresu, která je odvozena z veřejného klíče, potřebujeme soukromý klíč, abychom prokázali, že jsme vlastníkem kryptoměny přijaté v transakci. Svůj veřejný klíč tedy můžete bez obav volně sdílet. K odemknutí a přístupu k darovaným prostředkům budeme potřebovat soukromý klíč (Cryptopedia Staff, 2021).

Soukromý klíč dává možnost prokázat vlastnictví kryptoměny nebo utratit finanční prostředky spojené s veřejnou adresou. Svůj soukromý klíč nikdy s nikým nesdílíme. Soukromý klíč má 3 základní podoby (Cryptopedia Staff, 2021):

- **256 znaků dlouhý binární kód** – binární soustava 1 a 0;
- **QR kód –** grafické zobrazení;
- **64místný hexadecimální kód** – šestnáctková soustava.

Bez ohledu na jeho formu, je soukromý klíč astronomicky velký a je velký z dobrého důvodu. Zatímco veřejný klíč může být vygenerován pomocí soukromého klíče, opak je prakticky nemožný. K soukromému klíči může být připojen libovolný počet veřejných klíčů. Aby byla transakce na blockchainu dokončena, musí být podepsána (Cryptopedia Staff, 2021). Kroky, jak vypadá samotná transakce, vypadají následovně (Mikulášek, 2021):

- Uživatel 2 sdělí uživateli 1 svou veřejnou adresu, kterou vygeneroval ze svého veřejného klíče;
- uživatel 1 vytvoří pomocí hashe předchozí transakce a veřejného klíče uživatele 2 svůj podpis;
- podpis ověří svým veřejným klíčem, aby bylo jasné, z jaké adresy bude danou kryptoměnu posílat;
- nakonec uživatel 1 tuto transakci podepíše svým soukromým klíčem, tato transakce opět slouží jako vstupní data další transakce (viz obr. 8)



Obrázek 8 - Schéma transakce (převzato z (Nakamoto, 2008b))

Transakce musí být digitálně podepsána, aby bylo prokázáno vlastnictví finančních prostředků. Uzly automaticky kontrolují a ověřují transakce. Všechny neověřené transakce jsou sítí odmítnuty. Vytěžená transakce na blockchainu je nevratná. Soukromé klíče jsou v kryptoměnové peněžence, což je obvykle mobilní či počítačový software nebo specializované hardwarové zařízení. Soukromé klíče nejsou v kryptoměnové blockchainové síti. Pokud je kryptoměna držena na burze, pak je burza správcem soukromých klíčů; uživatel jí svěřuje své klíče podobně, jako by bance svěřil své zlato, s tím rozdílem, že svěřit bance zlato je mnohem bezpečnější (Cryptopedia Staff, 2021). V souvislosti s tím se v kryptoměnové komunitě vžilo heslo "not your keys, not your coins", které značí, že pokud nemáte pod kontrolou své soukromé klíče, nemáte pod kontrolou ani své kryptoměny, proto se nedoporučuje nechávat kryptoměny na burzách, nýbrž je mít uložené v peněženkách. Kvůli konfiguraci a funkčnosti kryptoměnových peněženek pravděpodobně nikdy nebude uživatel manipulovat se soukromými klíči přímo, protože peněženky je obvykle spravují za něj automaticky. Obvykle dostane počáteční frázi, které se říká recovery seed, jenž zakóduje vaše soukromé klíče jako zálohu (Cryptopedia Staff, 2021).

Veřejné a soukromé klíče ovládají vaše kryptoměny. Jak veřejné a soukromé klíče spolupracují, je zásadní pro pochopení toho, jak transakce kryptoměn fungují. Když říkáte, že máte kryptoměnu, ve skutečnosti tím říkáte, že máte soukromý klíč, který dokazuje vlastnictví této kryptoměny. Protože je uložena na blockchainu, může vás kdokoli ověřit jako vlastníka pomocí vašeho veřejného klíče.

3.2 Bezpečnost soukromého klíče

V souvislosti se soukromým klíčem se nabízí otázka, zda je bezpečný a či lze nějakým výkonným počítačem uhodnout. Celý proces při zakládání peněženky funguje tak, že peněženka vygeneruje náhodné 256bitové číslo a z něj pak odvozuje všechno ostatní.

Možnost uhádnutí 256bitového čísla je prakticky rovna nula, musíme si uvědomit kolik těch možností je a jak si takové číslo vůbec představit. Nejlépe si takové číslo, které se skládá z jedniček a z nul, připodobnit s hodem mincí, padne buď pana nebo orel. Pokud padne orel napíšeme jedničku, pokud padne pana napíšeme nulu, a tak se to provede 256krát a máme 256bitové číslo, a to je právě to číslo, které musí útočník uhodnout. Celkový počet možností našeho čísla je 2^{256}. To je to samé jako 2^{32}, které mezi sebou vynásobíme 8krát. Toto rozdělení je z důvodu toho, že 2^{32} je 4 294 967 296, pro výpočet bude zjednodušeno na 4 miliardy. Takže si nyní musíme představit, jak velké číslo je, když mezi s sebou 8krát musíme vynásobit 4 miliardy (viz obr. 9) (Vejmola, 2020a).

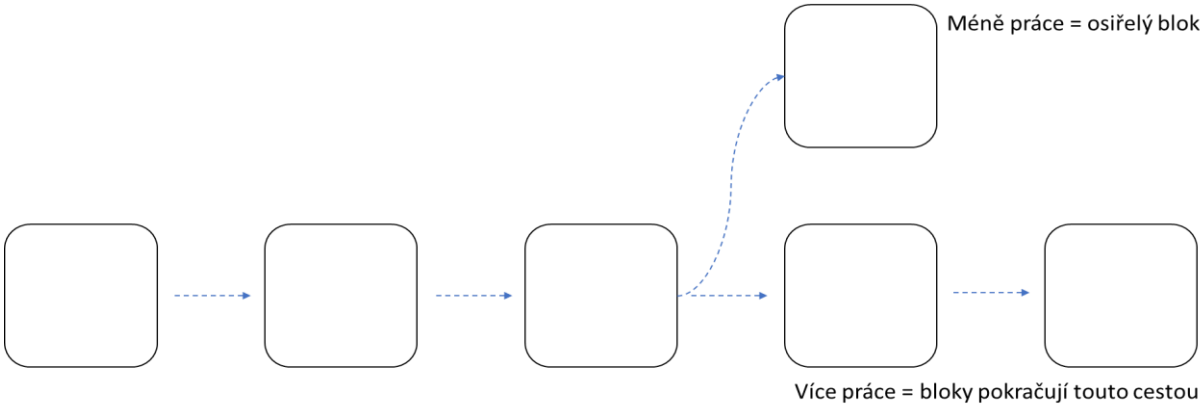
Obrázek 9 - Bezpečnost 256bitového čísla (vlastní zpracování)

Řekněme, že ono tajné číslo budeme hádat pomocí výkonného počítače s více grafickými kartami, které zvládnou vyzkoušet 4 miliardy možností za sekundu. Tím jsme pokryli první 4 miliardy, které reprezentují počet výpočtů (Hashů) na jeden počítač za 1 sekundu. Pro pokrytí druhých 4 miliard budeme potřebovat 4 miliardy takových počítačů, pro srovnání ani Google nedisponuje takovým počtem serverů, ale vezměme hypotetickou situaci a řekněme, že by Google měl takové servery, říkejme tomu např. Kilogoogle. Kilogoogle nám pokryje tedy druhé 4 miliardy. Na zemi žije cca 7, 75 miliard lidí, takže si představme, že každý druhý člověk dostane výkon Kilogooglu, tím máme pokryté třetí 4 miliardy. A teď si představte 4 miliardy kopií téhle naší planety Země, kde každý druhý obyvatel má doma jeden Kilogoogle výkonu čili takovou „malou“, ale super výkonnou galaxii. Takových galaxií budeme mít 4 miliardy a v každé té galaxii bude 4 miliardy planet, kde každý druhý člověk bude mít výkon jednoho Kilogooglu. Tím jsme pokryli páté 4 miliardy a nyní dosahujeme teoretického výkonu 2^{160} Hashů/sekundu. Dále nám zbývá pokrýt ještě 3krát 4 miliardy. 4 miliardy sekund, to je přibližně 126,8 let, krát 4 miliardy, to je cca 507 miliard let, což je asi 37krát věk celého vesmíru (Sanderson, 2017).

Čili i když budeme mít server plný grafických karet, budeme disponovat 4 miliardy těchto serverů v podobě Kilogooglu, tenhle Kilogoogle dáme každému druhému člověku na 4 miliardách planet, které navíc existují zároveň v každé ze 4 miliard galaxií, a budeme to s tímhle výkonem hádat 37krát déle než existuje vesmír, pak pořád máme šanci jen 1 ku 4 miliardám, že se trefíme (Sanderson, 2017). Existuje tedy šance, že by někdo trefil mé 256bitové číslo? Jednoduše řečeno ne, ta šance se sice nerovná nule, ale ta pravděpodobnost je tak strašně malá, že to riziko prakticky neexistuje.

3.3 Softfork a hardfork

Už víme, že data o transakcích se ukládají do bloků a ty se řetězí za sebou do blockchainu. Pokud se nalezne (vytěží) nový blok, je zapojen za předchozí a těžaři začínají těžit další blok, který bude zapojen za tento nový. Jestliže se ale vytěží dva či více bloků ve stejný okamžik, potom je více bloků zapojeno za stejný předchozí blok. To už není řetěz, kdy jsou všechny bloky uspořádány za sebou. Této situaci se říká **fork** (podle tvaru, který dva takto zapojené bloky připomíná, fork = vidlička). Jak se ale rozhodne, který řetězec platí, který je tím pravým? Například v bitcoinovém protokolu se používá pravidlo, které považuje, za platný blockchain vždy ten nejdelší, který máme k dispozici, a pokud máme dva řetězce stejně dlouhé jako v našem případě (viz obr. 10), pak je platný ten, na jehož nalezení bylo vykonáno více práce. Bloky forku, které nejsou použity pro rozvoj blockchainu, se označují jako orphan (osiřelé) bloky. Fork může být také důsledkem změny protokolu, tuto změnu dělíme na validní – softfork a nevalidní – hardfork (Stroukal, Sklaciký, 2021; Pritzker, 2020).

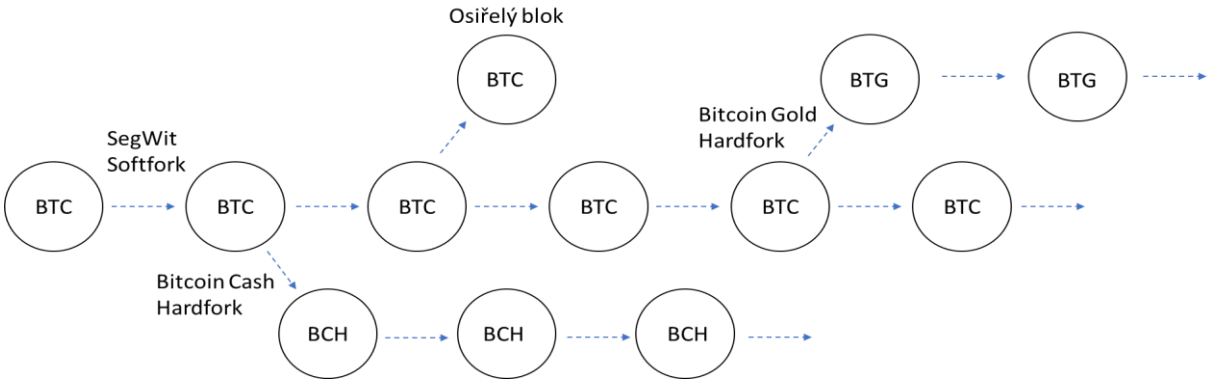


Obrázek 10 - Osiřelý blok (vlastní zpracování)

Softfork je zpětně kompatibilní změna všeobecně sdílených pravidel, jenž pravidla zpřísňuje. To znamená, že pokud uživatel provozuje starý uzel, který nepřešel na nová pravidla, bloky vytvářené podle nových pravidel pro něj budou přesto platné. Příkladem softforku je změna v bitcoinovém protokolu z roku 2010, kdy se určilo, že bloky mohou být nanejvýš 1 MB

velké. Cílem této změny bylo zabránit spamování v řetězci bloků. Dalším významným softforkem u Bitcoinu je Segregate Witness (SegWit), který šetří místo v blocích a tím pádem se do bloku vejde více transakcí. Softfork je tedy způsob, jak nenásilným způsobem upgradovat systém, protože umožňuje provozovatelům uzlů upgradovat postupně a dobrovolně v průběhu času (Pritzker, 2020).

Naopak **Hardfork** není zpětně kompatibilní změna. Jedná se o rozšíření souboru pravidel, podle kterého se původně platné bloky nově považují za neplatné. Staré uzly jsou nuceny upgradovat na nová pravidla. Uzly, které na nová pravidla nepřistoupí, nebudou moci zpracovávat bloky, jelikož budou brát bloky za neplatné. Teoreticky by hardforky prošly lehce, kdyby se na nich shodly všechny uzly v síti, takové hardforky by nezpůsobily žádné potíže. V praxi ale hard forky neprojdou hladce. Jako příklad lze vzít hardfork na bitcoinovém protokolu z roku 2017, kdy někteří lidé nebyli spokojeni s vývojem bitcoinového řetězce ve vztahu k malým platbám, a tak se rozhodli, že vytvoří řetězec s většími bloky než 1 MB. Tenhle hardfork vstoupil do dějin pod názvem Bitcoin Cash (BCH). Hardfork bez všeobecné shody, jako je Bitcoin Cash, na který nepřistoupí všichni těžaři a všechny uzly, vytvoří nový řetězec bloků. Řetězec sdílí historii s původním až do vzniku forku a mince, které na této větvi vznikly, se již nepovažují za bitcoiny, protože je nepřijímají žádné uzly bitcoinové sítě. Takových hardforků se na bitcoinovém protokolu událo mnoho a dnes existuje několik odnoží Bitcoinu, jako jsou například Bitcoin Gold (BTG), Bitcoin SV nebo Bitcoin Diamond, pravý Bitcoin je ovšem jen jeden. Forky Bitcoinu mají jiná pravidla, například jinou velikost bloku, o čemž se uzly navzájem informují a následně se rozhodnou, jaký blockchain budou přijímat a ve které síti budou aktivní (Pritzker, 2020).



Obrázek 11 - Příklady rozvětvení bitcoinového blockchainu (vlastní zpracování)

Jak můžeme vidět na obrázku výše, blockchain se může rozvětvit, uživatelé a těžaři si ale musí vybrat, který budou akceptovat, většina z nich jich logicky zůstane u Bitcoinu a k žádným jiným nepřechází, jelikož často nemají žádné vývojáře, jsou náchylné k útokům, a navíc u

některých kryptoměn, které vznikly jako hardfork Bitcoinu, se hodnota blíží k nule a spoustu jich už také zaniklo.

3.4 Bitcoin

Vznik Bitcoinu (označovaného též zkratkou BTC) jako první kryptoměny se datuje k 31. 10. 2008, kdy dosud neznámá osoba nebo skupina osob vystupující pod pseudonymem Satoshi Nakamoto (2008), publikovala vědecký článek Bitcoin: A Peer-to-Peer Electronic Cash System, kde je představen Bitcoin jako kryptograficky zabezpečený systém založený na algoritmu PoW. První vytěžené bitcoiny pak datujeme k 3. 1. 2009, kdy byl vytěžen první blok, tzv. Genesis blok. Technologie tedy byla popsána v roce 2008 a převedení technologie do praxe proběhlo na začátku roku 2009 (Huillet, 2019).

Abstrakt článku tuto novou měnu představuje a charakterizuje. Konkrétně Satoshi tvrdí, že čistě peer-to-peer verze elektronických peněz by umožnila přímé provádění online plateb mezi dvěma stranami, a to bez zprostředkování finanční institucí. Dále navrhuje řešení problému dvojí útraty pomocí peer-to-peer sítě, která přidělí každé provedené transakci časové razítko a pomocí hashovacích funkcí ji přidá do neustále se aktualizujícího řetězce důkazů o vykonané práci (PoW). Vznikne tak záznam, který nelze změnit bez opětovného provedení důkazů o této již vykonané práci. Dodává, že Síť jako taková přitom nevyžaduje speciální strukturu. Zprávy se šíří na principu nevynucování spolehlivosti všech uzlů (princip best-effort), proto se mohou jednotlivé uzly kdykoliv odpojit nebo připojit, přičemž po opětovném připojení akceptují nejdelší řetězec důkazů o vykonané práci jako záznam událostí, ke kterým došlo v jejich nepřítomnosti (Nakamoto, 2008a).

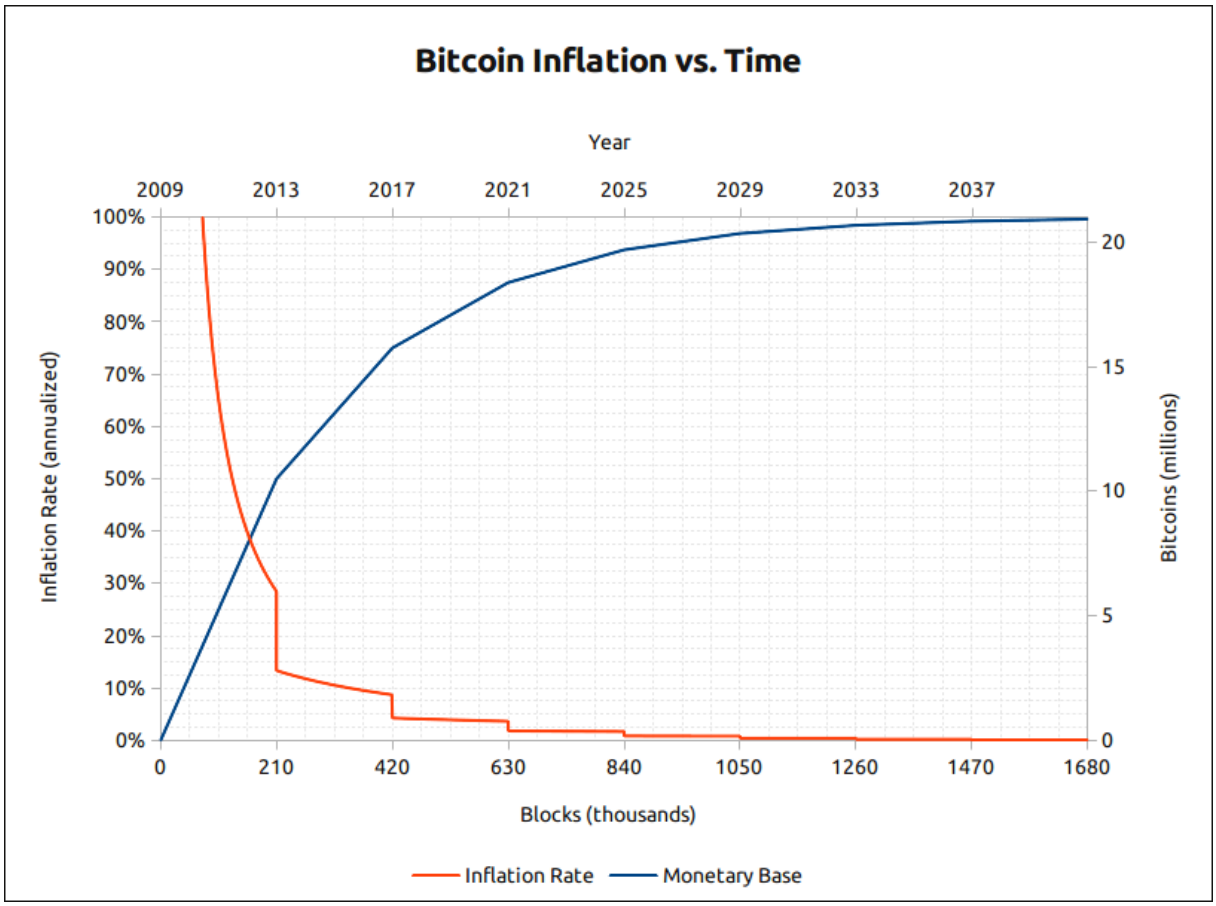
Proč vlastně Bitcoin vznikl? Za hlavní důvod je považována odluka peněz od státu a od centrálních institucí, které představují banky. Ale Bitcoin má mnohem větší přesah, než si většina lidí uvědomuje. Dříve byl vnímán jen jako platební prostředek, ale dnes je také uživateli hodlován (dlouhodobě držen). Termín hodl se objevil na diskusním fóru v roce 2013, kdy jeden z členů, který byl pod vlivem alkoholu, napsal „I am Hodling“ místo I am Holding. Jeho termín se používá dodnes, hodl tedy znamená dlouhodobě držet a nebrat ohledy na cenové výkyvy (Engelmannová, 2019). Jelikož fiat peníze téměř ztratily funkci uchovatele hodnoty, je to právě Bitcoin, který tuto funkci zastává. Kromě navrácení funkce úspor má Bitcoin potenciál zásadně proměnit i globální ekonomiku. Ta je totiž v posledních padesáti letech značně poznamenána existencí fiat peněz. Peněz, které nemají jakoukoliv návaznost na zlato či jiné vzácné a drahé aktivum, které by krotilo státní monetární politiku. Papírové peníze s těmito parametry mají poměrně drtivé následky: silné hospodářské cykly, obohacování finančního sektoru na úkor

jiných sektorů, znehodnocování úspor prostřednictvím inflace, zadlužování států, firem a domácností (Tětek, 2021). Bitcoin představuje unikátní kombinaci vlastností: decentralizaci, dlouhodobě udržitelnou motivaci těžařů, předvídatelnou a nezměnitelnou monetární politiku s přesně definovaným množstvím bitcoinů, které nemůže být překročeno. Historie lidstva je poznamenána neustálým zneužíváním peněžního monopolu ze strany vladařů a států. V případě Bitcoinu ale takovým monopolem nikdo nedisponuje. Suverénem je zde každý provozovatel bitcoinového uzlu (Tětek, 2021).

Je Bitcoin deflační nebo inflační měna? Překvapivě může být oboje správně, záleží, z jakého úhlu se na Bitcoin podíváme. Celkový počet bitcoinů bude 21 milionů, jedná se o limit, který je implementován přímo do bitcoinového protokolu a nikdy ho nebude více, což z něj dělá vzácné aktivum.

Deflační měna? Ačkoli celkový počet bitcoinů nikdy nepřesáhne 21 milionů, počet bitcoinů v oběhu je ve skutečnosti nižší a dost pravděpodobně bude stále klesat. Již nyní víme, že zhruba 3,8 milionu bitcoinů se nepohnulo déle než 5 let (Tětek, 2021). Pravděpodobně se jedná o bitcoiny, k nimž majitelé ztratili svou neopatrností privátní klíče a o své bitcoiny tak nadobro přišli. Toto číslo bude vlivem neopatrného zacházení s privátními klíči pravděpodobně růst. To v praxi bude znamenat, že s pravděpodobným růstem hodnoty bitcoinů se bude potřebné množství mincí pro nákup zmenšovat, průměrná transakce se sníží a namísto v celých bitcoinech budeme uvažovat spíše v jeho jednotkách, v satoshi. Satoshi (sat) je nejnižší jednotka bitcoinu, nazvána podle tvůrce Satoshiho Nakamota (1 BTC = 100 000 000 sat). Bitcoin tak představuje deflační měnu – měnu, ve které počet jednotek v oběhu s časem klesá, a kupní síla bitcoinu se v průběhu času zvyšuje (Tětek, 2021).

Inflační měna? Inflace je běžně definována jako všeobecné zvýšení cen a pokles kupní hodnoty peněz. Při použití tradiční definice je Bitcoin inflační, protože nabídka bitcoinů se časem zvyšuje. Ačkoli Bitcoin a zlato jsou v současné době považovány za inflační, jejich míry inflace jsou předvídatelné a neustále klesající. Satoshi Nakamoto zcela záměrně navrhl Bitcoin tak, aby bylo tempo uvolňování nových jednotek do oběhu zcela transparentní a dlouhodobě předvídatelné, jak ukazuje obrázek níže (Hays, 2018). Bitcoinový protokol stanovuje, kolik nových bitcoinů se s každým vytěženým blokem dostává do oběhu. Na rozdíl od nepředvídatelné peněžní expanze, jejímu utahování a míry inflace je aktuálně roční míra inflace bitcoinu pouze 1,77 %, a v roce 2030 bude pouhá 0,4 %. Roční míra inflace bitcoinu tak nakonec dosáhne nula procent, při vytěžení posledního bitcoinu v roce 2140. Bitcoin tedy spíše začíná plnit roli zajištění proti inflaci (Hays, 2018).



Obrázek 12- Inflace Bitcoinu v čase (převzato z bitcointalk.org)

Kde se berou nové bitcoiny? Nové bitcoiny vznikají pomocí procesu těžby, dle algoritmu PoW. Těžba vychází z teorie her a lze ji popsat jako hraní matematické loterie důkazu práce, takové soutěže a získávání přístupových práv k účetní knize. Právo na zařazení transakcí do bloku a připojení tohoto bloku na konec blockchainu vyhrává ten, kdo podá důkaz o vynaložení dostatečného množství výpočetního výkonu jako první. Důkaz je podáván v podobě hashe začínajícího na určitý počet nul. Ale proč vlastně musí těžaři vynakládat tak vysoký výpočetní výkon a spotřebovat obrovské množství energie, za což je Bitcoin často kritiky označován jako neekologický? Je to kvůli tomu, aby systém mohl fungovat bez centrálního správce, byl bezpečný, odolal útokům hackerů a zároveň aby jeho účastníci byly odrazeni od podvádění (Tětek, 2021). Odměna za vytěžení bloků je dvousložková, jednak těžař obdrží nové bitcoiny, a jednak mu náleží i odměna v podobě transakčních poplatků. Každý nový blok se přidá do řetězce bloků v průměru každých 10 minut. Zpočátku byla odměna za nalezení nového bloku 50 bitcoinů, přičemž se tato odměna každé 4 roky snižuje na polovinu (tzv. halving), v letech 2012–2016 byla odměna 25 bitcoinů, aktuální odměna za vytěžení nového bloku činí 6,25 bitcoinů (Tětek, 2021). Okolo roku 2140 bloková odměna klesne na nulu a těžaři budou motivování jen transakčními poplatky. Proto je mylné označovat Bitcoin za měnu s nízkými

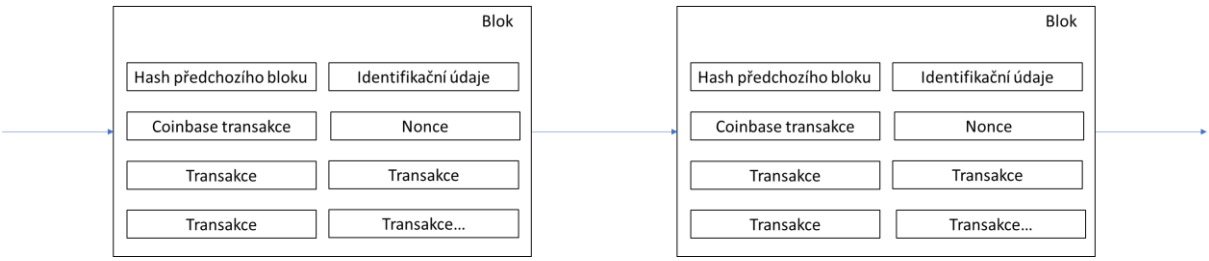
transakčními poplatky, ty budou v průběhu času spíše růst a měla by tím pádem růst i ekonomická hodnota každé jednotlivé transakce (Tětek, 2021).

Co když je těžařů málo anebo naopak hodně? Celkové množství hashů za vteřinu, provedených všemi těžaři v síti Bitcoin, se nazývá hash rate. Pokud bude těžit méně lidí a bude hash rate nízký, mohou vzniknout dva problémy. Bitcoiny budou vydávány příliš pomalu, což narušuje Satoshiho časový plán, druhým problémem může být to, že se systém stane nepoužitelným, protože lidé čekají hodiny, dny nebo ještě déle na zápis transakcí do blockchainu (Pritzker, 2020). Opačně, když je těžařů naopak více a hash rate je vysoký, může to vést k opačnému problému, a to že bitcoiny budou vydávány příliš rychle, a také by mohlo dojít k nedohodě těžařů na lineární historii. Počet těžařů se s každým okamžikem mění. Aby nedocházelo k výše uvedeným situacím, potřebujeme zajistit, aby rychlost vytváření nového bloku byla stabilní a nedocházelo k zpomalování nebo k zrychlování pokaždé, když se připojí nový těžař, nebo se naopak současný těžař odpojí. Bitcoin tento problém řeší elegantně regulací obtížnosti těžby. Pokaždé, když je vyprodukováno 2016 bloků, což odpovídá přibližně 14 dnům, se zjistí, jak dlouho v průměru trvalo vytěžení těchto bloků (Pritzker, 2020). Výpočet je jednoduchý, 2016/čas na jejich vytvoření, tím se získá průměrný čas na vytěžení jednoho bloku. Jeli to více než 10 minut, značí to méně těžařů. Číslo hledané těžaři se zvýší, s tím se zvětší interval platných hashů a zvětší se pravděpodobnost nalezení vítězného hashe. Tomu říkáme snížení obtížnosti těžby, opačným způsobem může být složitost těžby také zvýšena. Při nižším hash ratu se složitost nalezení bloku snižuje, zatímco při vyšším hash ratu se složitost nalezení bloku zvyšuje (Pritzker, 2020).

Co vlastně Bitcoin řeší po technické stránce? Hlavním přínosem Satoshiho Nakamota po technické stránce je vyřešení double-spendu (dvojitého utrácení) aplikováním blockchainu. Ve fiat penězích tento problém je vyřešen tím, že hotovost nelze naklonovat a u bankovních převodů tento problém řeší banka, centrální autorita, kterou však u Bitcoinu z mnoha důvodů nemáme. Satoshi vyřešil problém blockchainem, do kterého se dostane pouze ta transakce, která je platná (Janda, 2021). Pokud bychom chtěli podvádět a stejné bitcoiny poslat na dvě adresy najednou, těžaři zkrátka tyto transakce nepotvrdí, jelikož ví, že nedisponujeme tolika bitcoiny, respektive potvrdí jen jednu z nich. V blockchainu nemohou být dvě konfliktní transakce, jinak je celá část počínající konfliktní transakcí neplatná. V případě dvojího utracení blockchain nezaručuje, která z transakcí bude nakonec ta správná, ale zaručuje, že to bude vždy jen jedna z nich a všichni budou vědět, která to je (Janda, 2021).

3.4.1 Životní cyklus bitcoinové transakce

Jak přesně probíhá taková bitcoinová transakce od okamžiku, kdy je zadaná v peněžence, do okamžiku, kdy se objeví v peněžence protistrany jako platná a ověřená? Prvním krokem je zkonstruování transakce peněženkou. Peněženka vezme bitcoiny, které jsou uložené na dané adrese, a k ní je pak přiřazena adresa příjemce. Dále vybereme poplatek těžařům a následně je transakce podepsána soukromým klíčem. Tato transakce je odeslaná 1 až 8 uzlům, ke kterým je peněženka připojená. Těmito uzly mohou být peněženky, těžaři, mohou patřit burzám či směnárnám nebo někomu, kdo provozuje uzel jen tak, bez vidiny zisku. V okamžiku, kdy transakce dorazí na některý uzel, tak první, co uzel udělá, je ověření transakce, jestli je skutečně podepsaná vlastníkem, což lze ověřit pomocí veřejného klíče, dále také zkontroluje částky a zda je nastaven poplatek (Vejmola, 2020c). Pouze pokud je transakce platná = validní, tak uzel transakci vezme a pošle dalším uzlům, na které je on sám připojen, a ten ji zase rozesílá dál. Nakonec je rozšířena celou sítí a ví o ní úplně každý uzel. Co s transakcí dále? Každý uzel si udržuje tzv. mempool nepotvrzených transakcí, lze si to představit jako „zásobník“, ve kterém si uzel uchovává platné, ale dosud neověřené transakce. Čili neexistuje jen jeden mempool, ale existuje tolik mempoolů, kolik je aktuálně uzlů. Pro těžaře plní mempool klíčovou roli, protože z něj konstruují každý nový blok (Vejmola, 2020c). Jako první musí těžař uvést hash předchozího bloku, tím vytvoří odkaz na blok předchozí. Dále musí těžař uvést časové razítko a další identifikační informace, a jako první transakci do bloku vloží tzv. coinbase transakci, která v případě úspěšného vytěžení připisuje na adresu, kterou si určí nově emitované bitcoiny. Těžební uzel se podívá do mempoolu a do bloku přidá transakce až do úplného zaplnění, tím vznikne tzv. kandidátní blok. Dělá to tak, aby maximalizoval zisk čili transakce s větším transakčním poplatkem mají přednost. Poté už je to „jen“ o tom, aby těžař našel zlatou nonci, kterou blok uzavře, a všem uzlům okolo nahlásí, že blok byl nalezen a začne ho opět propagovat sítí všem ostatním uzlům. Uzly blok ověří a pokud je vše v pořádku, je ukončeno toto soutěžní kolo o nalezení bloku a celá série se znovu a znovu opakuje. Pokud byl nastaven odpovídající poplatek a blok byl vytěžen, protistrana uvidí na své adrese, že transakce je vyřízená (Vejmola, 2020c). Příklad bloků a jejich obsah je znázorněn na obrázku č. 13.



Obrázek 13 - Schématické znázornění bloků (vlastní zpracování)

3.4.2 Lightning network

Lightning network je technologické řešení určené k vyřešení problému rychlosti transakcí na bitcoinovém blockchainu zavedením transakcí mimo knihu. Transakce prováděné na lightning network (tj. off-chain) jsou rychlejší, méně nákladné a snadněji potvrzené než transakce prováděné přímo na bitcoinovém blockchainu (tj. on-chain). Odstraněním transakcí z hlavního blockchainu a jejich převedením mimo řetězec byla lightning network navržena tak, aby odblokovala bitcoinový blockchain a snížila související transakční poplatky. Lightning network byl poprvé navržen Josephem Poonem a Thaddeusem Dryjou v roce 2016 a od té doby se vyvíjí (Frankenfield, 2021a). Tato síť navrhla vyřešit problém škálování vytvořením druhé vrstvy na hlavním blockchainu Bitcoinu. Druhá vrstva se skládá z několika platebních kanálů mezi stranami nebo uživateli Bitcoinů. Kanál lightning networku je transakční mechanismus mezi dvěma stranami. Pomocí kanálů mohou strany vzájemně provádět nebo přijímat platby. Tyto transakce jsou zpracovávány odlišně ve srovnání se standardními transakcemi probíhajícími na bitcoinovém blockchainu. Aktualizují se pouze na hlavním blockchainu, když dvě strany otevřou a zavřou kanál. Tyto strany mohou donekonečna přesouvat finanční prostředky mezi sebou, aniž by o svých aktivitách informovaly hlavní blockchain. Tento přístup dramaticky zrychluje rychlost transakce, protože všechny transakce nemusí být schváleny všemi uzly v rámci blockchainu. Jednotlivé platební kanály mezi různými stranami se spojují a vytvářejí síť lightning uzlů, které mohou mezi sebou provádět transakce. Výsledkem propojení mezi různými platebními kanály je Lightning Network. Lightning network je tedy řešení, jak efektivně platit Bitcoinem, a tím se stává jedním z nejdůležitějších vylepšení Bitcoinu (Frankenfield, 2021a).

3.5 Litecoin

Litecoin (označovaný též zkratkou LTC) je alternativní kryptoměna (altcoin) vytvořená v říjnu 2011 bývalým inženýrem Googlu Charlie Leem. Litecoin vychází z open source zdrojového kódu Bitcoinu, ale s několika úpravami. Stejně jako Bitcoin je i Litecoin založen na globální platební síti s otevřeným zdrojovým kódem, kterou nekontroluje žádný centrální orgán. Litecoin se od Bitcoinu liší v aspektech, jako je rychlejší generování bloků a použití Scryptu jako schématu důkazu práce. Scrypt vyvinul Lee speciálně pro ztížení rozsáhlých hardwarových útoků na měnu, které byly vytvořeny na zakázku (Frankenfield, 2021c). Algoritmus Bitcoinu SHA-256 nevyžaduje mnoho paměti s náhodným přístupem jako překážku paralelního zpracování, zatímco Scrypt ano. Litecoinu se přezdívá digitální stříbro, je jakýmsi mladším bratrem k digitálnímu zlatu, Bitcoinu, a na svém vrcholu byla 3. největší kryptoměnou

podle tržní kapitalizace. Vzhledem k tomu, že jeho struktura je podobná struktuře Bitcoinu, byla použita jako testovací síť nebo testovací základna pro vylepšení, která byla později aplikována na Bitcoinu například pro SegWit či pro lightning network (Frankenfield, 2021c)

Čím se liší Litecoin od Bitcoinu? Litecoin je navržen tak, aby produkoval čtyřikrát více bloků než Bitcoin a také umožňuje čtyřnásobek limitu coinů, takže jeho hlavní přitažlivost oproti Bitcoinu spočívá v rychlosti a snadné akvizici. Protože však Litecoin používá Scrypt (na rozdíl od Bitcoinového SHA-256) jako algoritmus PoW, použití těžebního hardwaru, jako jsou ASIC minery nebo těžební zařízení GPU, vyžaduje výrazně větší výpočetní výkon (Frankenfield, 2021c).

	Bitcoin	**Litecoin**
Vznik	**2008/2009**	**2011**
Tvůrce	**Satoshi Nakamoto**	**Charlie Lee**
Jednotka	**BTC**	**LTC**
Celkový počet	**21 milionů**	**84 milionů**
Tvorba bloku	**≈ 10 minut**	**≈ 2,5 minuty**
Algoritmus	**SHA-256**	**Scrypt**
Aktuální odměna	**6,25 BTC**	**12,5 LTC**
Půlení	**Každý 210 000. bloků**	**Každý 840 000. blok**

Tabulka 1 - Porovnání Bitcoinu a Litecoinu (vlastní zpracování)

3.6 Ethereum

Ethereum již není „jen“ měnou, ale stává se kryptoplatformou. V souvislosti s tím se o Ethereu mluví jako o blockchainu 2. generace, za blockchainy 1. generace jsou pak považovány měny jako Bitcoin. Ethereum vynalezl Vitalik Buterin v roce v 2013, samotný projekt byl pak spuštěn v roce 2015, jednotkou projektu je 1 ether (1 ETH). Jedná se o tržiště finančních služeb, her a aplikací, které nemohou ukrást uživatelská data ani uživatele cenzurovat. Záměrem Etherea je vytvořit alternativní protokol pro budování decentralizovaných aplikací. Ethereum stojí stejně jako Bitcoin na algoritmu PoW, v příštích letech však plánuje přechod na ekologičtější PoS (Buterin, 2013).

Co Ethereum dělá? Ethereum může pohánět řadu aplikací, které nabízejí širokou škálu funkcí (Roayl, 2021):

- **měna** – s kryptoměnovou peněženkou můžete odesílat a přijímat Ethereum nebo platit za zboží a služby, podobně jako tomu je u Bitcoinu;

- **chytré kontrakty** (smart contracts) – často označované jako chytré, či inteligentní smlouvy jsou samočinné smlouvy, přičemž podmínky dohody mezi kupujícím a prodávajícím jsou přímo zapsány do řádků kódu;
- **digitální decentralizované aplikace** (dapps) – Ethereum pohání digitální aplikace, které uživatelům umožňují hrát hry, investovat, posílat peníze, sledovat investiční portfolio, sledovat sociální média a mnoho dalšího;
- **nezaměnitelné tokeny** (NFTs) – tyto tokeny mohou být poháněny Ethereem a umožňují umělcům nebo jiným osobám prodávat umění nebo jiné předměty přímo kupujícím pomocí chytrých smluv;
- **decentralizované finance** (DeFi) – používáním Etherea se někteří lidé mohou vyhnout centralizované (vládní) kontrole nad pohybem peněz nebo jiných aktiv.

Je tedy přesnější myslet na Ethereum jako na token, který pohání různé aplikace, spíše než jako na pouhou kryptoměnu, která uživatelům umožňuje posílat si peníze. Navíc open source koncept Etherea umožňuje vývojářům stavět na něm zcela nové kryptoměny, jako je Chainlink nebo Uniswap, tyto kryptoměny jsou vybudovány na blockchainu Etherea a nemají vlastní blockchain, obecně jsou označovány jako ERC-20 tokeny. Za zmínku stojí ještě kryptoměna BAT, která je používaná prohlížečem Brave, který blokuje reklamy a cookies (Haar, 2021).

Jak se liší Ethereum a Bitcoin? Bitcoin se primárně používá jako virtuální měna a uchovatel hodnoty. Ether funguje také jako virtuální měna a uchovatel hodnoty, ale decentralizovaná síť Etherea umožňuje vytvářet a provozovat aplikace, chytré smlouvy a další transakce v síti. Bitcoin tyto funkce nenabízí. Používá se pouze jako měna a uchovatel hodnoty. Ethereum také zpracovává transakce rychleji. Nové bloky jsou ověřovány v bitcoinové síti jednou za 10 minut, zatímco nové bloky jsou ověřovány v síti Ethereum každých 12 sekund (Rodeck, 2021). Budoucí vývoj by mohl transakce Etherea ještě více urychlit. U Etherea neexistuje žádný limit na počet potenciálních etherových tokenů, zatímco Bitcoinu nebude více než 21 milionů (Rodeck, 2021). Ethereum je tedy mnohem komplexnější, umí toho mnohem více, je otázkou, jak velké reálné využití budou mít funkce, které Ethereum přináší. Mezi komunitou se pak často objevuje názor, že Vitalik Buterin přišel s řešení problému, který zatím neexistuje.

3.6.1 Non-fungible token

Non-fungible token (NFT) je záznam na blockchainu – krátký kód v blockchainu, který reprezentuje vlastnictví určitého souboru dat. NFT jsou nezastupitelné tokeny, na rozdíl od

Bitcoinů, které jsou zastupitelné, což znamená, že jedna mince je v podstatě nerozeznatelná od druhé a má ekvivalentní hodnotu, to u NFT neplatí. To znamená, že jsou jedinečné, takže mohou představovat jedinečné věci. A protože jsou jedinečné a uložené na blockchainu, jsou nepochybně autentické. To je zvláště důležité, když aktivum, které představují, je digitální (Brown, 2021). Protože digitální soubory lze kopírovat donekonečna a dokonale, je těžké vlastnit (nebo prodat) vzácnou digitální fotografii. NFT řeší tento problém tím, že prokáží, že jeden digitální soubor je jediný „originál“. Při nákupu NFT získáte jak nevymazatelný záznam o vlastnictví aktiva, tak přístup ke skutečnému aktivu. Těmito aktivy může být cokoliv. V současné době jsou to většinou díla digitálního umění nebo sběratelské karty. Některé jsou virtuálním zbožím, které existuje pouze na trhu, kde se prodává, a některé jsou zabalené ve známých formátech, jako je JPEG nebo PDF. Malá menšina NFT jsou digitální záznamy o vlastnictví skutečného fyzického předmětu (Brown, 2021).

Fenomén NTF začal kolem roku 2017. Dvěma oblíbenými ranými NFT byly CryptoPunks, digitální obrázky 10 000 lidských a zvířecích postav v roztomilé, 8bitové animaci, a CryptoKitties, sbírka fantasticky nakreslených kočkovitých šelem. Původně byly rozdávány zdarma. Nejcennější CryptoKitties se nyní prodávají za více než 100 000 dolarů, CryptoPunks za více než 1 milion dolarů (Brown, 2021).

Když tedy někdo vytvoří – nebo „vyrazí“ – NFT, píše základní kód smart kontraktu, který řídí kvality NFT, a přidává tyto vlastnosti do příslušného blockchainu, na kterém je NFT spravováno. Samotná tvorba kontraktu vyžaduje pokročilé znalosti programování. Ke správě NFT lze použít mnoho blockchainů, včetně Etherea. Pro obchodování NFT existují speciální trhy „marketplaces“, kde se obchodují všechny možné položky. Podobá se to burze s cennými papíry nebo například platformě Binance pro obchody s kryptoměnami, i samotná burza Binance má své NFT tržiště, které stojí na jejich vlastní síti BSC (Mahmood, 2021). Jak takové dílo může vypadat je uvedeno v příloze 1.

3.7 Stablecoins

Stablecoins jsou třídou kryptoměn, které se pokoušejí nabídnout cenovou stabilitu a zároveň jsou kryty rezervním aktivem, nejčastěji dolarem, na jehož cenu jsou navázané. Stablecoiny získaly na síle, protože se pokoušejí nabídnout to nejlepší z obou světů – okamžité zpracování, zabezpečení nebo soukromí plateb kryptoměn a stabilní zhodnocení fiat měn bez vysoké volatility kryptoměn (Hayes, 2021). Ačkoli Bitcoin zůstává nejoblíbenější kryptoměnou, má tendenci trpět vysokou volatilitou. Ta například stoupla z úrovně kolem 5 000 USD na vrcholu výprodeje na začátku pandemie Covid-19 v březnu 2020 až na téměř 65 000

USD v dubnu 2021, než se propadla o více než 50 % na přibližně 30 000 USD v červnu 2021 a následně se vrátila zpět na hodnoty kolem 65 000 USD v listopadu 2021. Dokonce i jeho cenové výkyvy v rámci dne mohou pohybovat v obou směrech až o 10 % během několika hodin (Hayes, 2021). Tento druh krátkodobé volatility činí Bitcoin a další kryptoměny nevhodnými pro každodenní použití veřejností. Měna by měla fungovat jako prostředek peněžní směny a způsob uchovávání peněžní hodnoty, její hodnota by měla zůstat v delších časových horizontech relativně stabilní. Stablecoiny poskytují řešení pro utrácení měn namísto jejich dlouhodobého držení. Existuje několik kategorií stablecoinů, všechny založené na jejich pracovních mechanismech (Hayes, 2021).

Stablecoiny zajištěné fiatem udržují rezervu nekryté měny, jako je americký dolar, jako kolaterál pro vydání vhodného počtu kryptoměn. Jiné formy kolaterálu mohou zahrnovat drahé kovy, jako je zlato nebo stříbro, stejně tak komodity, jako je ropa, ale většina současných stablecoinů zajištěných fiatem využívá dolarové rezervy. Tyto rezervy jsou udržovány nezávislými správci a jsou pravidelně kontrolovány z hlediska dodržování nezbytného souladu. Tether (USDT) a TrueUSD (TUSD) jsou oblíbené kryptoměny, které mají hodnotu ekvivalentní hodnotě jednoho amerického dolaru a jsou kryty dolarovými vklady. V listopadu 2021 byl USDT čtvrtou největší kryptoměnou podle tržní kapitalizace s hodnotou více než 73 miliard USD (Hayes, 2021; Mikulášek, 2018).

Stablecoiny zajištěné komoditami udržují rezervu v podobě vzácné komodity. Jsou navázané právě na cenu dané komodity, a to z důvodu toho, že v případě krize mohou i fiat měny podléhat veliké volatilitě, o čemž se nedávno přesvědčili obyvatelé Venezuely, Turecka či Ruska. Ze stablecoinů zajištěných komoditami stojí za zmínku například PAX Gold, jehož cena je navázána na 1 trojskou unci zlata (Mikulášek, 2018).

Stablecoiny zajištěné kryptoměnami jsou kryty jinými kryptoměnami. Vzhledem k tomu, že rezervní kryptoměna může být také náchylná k vysoké volatilitě, jsou takové stablecoiny nadměrně zajištěny – to znamená, že větší počet tokenů kryptoměny je udržován jako rezerva pro vydání nižšího počtu stablecoinů. Například Ethereum v hodnotě 4 000 USD může být držen jako rezerva pro vydávání stablecoinů krytých kryptoměnami v hodnotě 2 000 USD, které pokrývají až 50 % výkyvů v rezervní měně (ether) (Hayes, 2021). Výhodou je, že tento systém je zcela decentralizovaný, využívá výhod blockchainu a je velmi transparentní naopak od stablecoinů zajištěnými fiatem, které jsou absolutně centralizované navázáním na státní měnu. Nevýhodou je však určitá náchylnost na změny hodnot podkladových kryptoměn. Nejznámějším stablecoinem zajištěným kryptoměnami je Dai, který funguje na blockchainu Etherea (Hayes, 2021).

Nezajištěné stablecoiny (algoritmické) nevyužívají žádnou rezervu, ale obsahují fungující mechanismus, jako je mechanismus centrální banky, k udržení stabilní ceny. Například basecoin vázaný na dolar používá mechanismus konsensu ke zvýšení nebo snížení nabídky tokenů na základě potřeby. Toho lze dosáhnout implementací chytré smlouvy na decentralizované platformě, která může běžet autonomně (Hayes, 2021).

3.8 Využití Bitcoinu v podniku

Bitcoin mohou využívat stejně jako běžní občané i podniky. Společnosti mohou Bitcoin přijímat jako platidlo od svých zákazníků, platit svým dodavatelům, dlouhodobě jej držet, či využít volné budovy a energii k jeho těžbě. Při platebním styku se svým dodavatelem, či se zákazníkem, může firma využívat klasické bitcoinové transakce, platební síť lightning network pro minimalizování transakčních poplatků, či používat prostředníka, který nabízí bitcoinovou platební bránu, která funguje na podobném principu jako platební brána klasická, platební operaci si tak zajistí jako službu od externího dodavatele. Firma, která prostředníka využije poté, neobdrží Bitcoiny, kterými bylo zaplaceno, nýbrž České koruny. Bitcoiny si v tomto případě ponechá prostředník a firmě pošle klasické peníze (Tětek, 2020). Tuto službu využívá řada firem u nás, například Alza, a jedná se o zajímavou konkurenční výhodu oproti ostatním firmám, která může přilákat nové zákazníky, především z řad kryptoměnových nadšenců. Společnosti také mohou Bitcoin koupit a dlouhodobě jej držet, čímž ochrání své volné prostředky před inflací, jelikož cena Bitcoinu dlouhodobě roste. Prozíraví představitelé firem, správci aktiv a velcí investoři se snaží zajistit vůči propadu hodnoty fiat měn dříve než ostatní. Žebříčku veřejně obchodovaných firem kraluje MicroStrategy, americká firma zaměřená na vývoj business intelligence software (Tětek, 2020). Její zakladatel a dlouholetý ředitel Michael Saylor se v posledních letech intenzivně vzdělával ve světové ekonomice, povaze peněz a Bitcoinu. MicroStrategy za sebou měla několik úspěšných let a měla k dispozici stovky milionů dolarů, o jejichž schopnosti dlouhodobě udržovat hodnotu začínal Saylor stále více pochybovat. Během léta 2020 se proto vedení firmy rozhodlo většinu svých volných prostředků převést do Bitcoinu. Celkem šlo o 425 milionů dolarů, za něž firma na trhu získala 38 250 BTC. Firma to vysvětluje jako jediný smysluplný krok pro dlouhodobé uchování hodnoty pro své akcionáře (Tětek, 2020).

V roce 2021 MicroStrategy od svých plánů neustoupila a k 13. září 2021 drží již 114 042 BTC. MicroStrategy utratila za nákup Bitcoinu 3,16 miliard USD, k 13. září 2021 má veškerý Bitcoin v jejich držení hodnotu přes 5,1 miliard USD, což odpovídá nárůstu 42 % (Copeland, 2021).

4 Další využití technologie blockchain

S blockchainem se do budoucna musí počítat, jelikož potenciál, který přináší, je obrovský. Blockchain však nejsou jen kryptoměny, i když je s nimi nejčastěji spojován a také je v nich nejčastěji využíván. Mnoho blockchainových technologií a projektů jde ve vývoji kupředu, projekty založené na blockchainových technologiích buduje například Microsoft či IBM. Těchto společností bude bezesporu v budoucnu přibývat. Blockchain bývá označován za druhou generaci internetu, a tak se dá předpokládat, že i on, podobně jako internet, ovlivní životy nás všech (*Finex*, 2018).

Ne nadarmo bývá blockchain považován za jeden z prvků Průmyslu 4.0, který rozšiřuje možnosti současného internetu o elektronickou monetární komponentu a o decentralizovaný způsob validace elektronických transakcí. Využití blockchainu ve vazbě na kyber-fyzikální produkční systémy a umělou inteligenci je další možností plnohodnotného rozvoje digitální ekonomiky Průmyslu 4.0 (*Iniciativa průmyslu 4.0*, 2017).

4.1 Blockchain ve finančním sektoru

Zvyšování výkonu proti riziku je konečným cílem pro každého, kdo pracuje ve finančním odvětví. Blockchain tímto způsobem zlepšil výkon snížením nákladů a zlepšením efektivity. Distribuovaný charakter záznamů v blockchainu snižuje operační riziko. Protože nepodléhá zásahům ze strany zprostředkovatelů, je mezi subjekty méně manuální práce. PoW usnadňuje automatizaci v technologii blockchain. Blockchain snižuje náklady na důvěru. Současný finanční systém klade na zákazníky v obchodě vysoké náklady na zajištění důvěry mezi institucemi a uživateli. Centralizovaní zprostředkovatelé s sebou nesou koncentrovaná rizika. Decentralizovaný blockchain zlepšuje administraci finančních služeb v oblasti plateb, digitální identity, cenných papírů, zpracování derivátů a podobně (Choi, Huang, 2021).

Technologie blockchain by mohla být použita v oblasti pojištění, plateb a finančních služeb k ukládání záznamů o majetku, zúčtování a vypořádání účtů, zajištění platnosti a provádění smluvních ujednání. Blockchain umožňuje realizaci smluv, když jsou splněny zvláštní podmínky. Blockchain zlepšuje autentizaci a shodu ohledně integrity dat. Schopnost blockchainu provádět vypořádání akcií peer-to-peer téměř okamžitě činí technologii přitažlivou pro obchodování s akciemi, což by mohlo vést ke snížení poplatků ze strany clearingových středisek a odstranit potřebu auditorů. Průmyslové konsorcium (R3) více než čtyřiceti bank bylo založeno za účelem výzkumu a vývoje blockchainové technologie pro finanční aplikace a investování do slibných iniciativ v rané fázi. Do R3 se zapojili banky jako například JP Morgan, Citigroup, Commerzbank, National Australia Bank, Deutsche Bank, Morgan Stanley, ING

Bank, UniCredit a další. R3 identifikovala případy použití, kdy blockchainová řešení mohou snížit náklady na infrastrukturu a dodržování předpisů a poskytnout hodnotu tím, že usnadňují interoperabilitu mezi interními systémy. Burzy cenných papírů a komodit, včetně Australian Securities Exchange, Frankfurtské burzy cenných papírů a Japan Exchange Group, experimentují s blockchainovými aplikacemi pro služby, které nabízejí (Attaran, Gunasekaran, 2019).

4.1.1 Digitální měny centrálních bank

Technologie blockchainu by mohla ovlivnit celý finanční průmysl, včetně bankovního sektoru. Velká pozornost věnovaná blockchainu v bankovním kontextu vede k otázce, jakou roli mohou hrát centrální banky při používání blockchainu. Měla by centrální banka vydávat digitální měnu? Potřeba dostatečné likvidity upoutala pozornost centrálních bank, které uvažují o emisi digitálních měn centrálních bank (Central bank digital currency – CBDC) (Choi, Huang, 2021).

CBDC, o jejichž emisi centrální banky začínají uvažovat, jsou sice inspirovány Bitcoinem, ale ve skutečnosti představují něco úplně jiného. CBDC jsou centralizovaný systém s vratnými a cenzurovanými transakcemi, kde musíme plně důvěřovat bance, jakožto centrální instituci. Pointa CBDC je taková, že vedle současných peněz vzniknou ještě jedny peníze, tedy CBDC, avšak ty budou plně pod kontrolou centrální banky, na rozdíl od dnešních elektronických peněz, které uživatelům spravují banky komerční (Stroukal, Skalický, 2021). CBDC budou fungovat tak, že uživatel si otevře účet u centrální banky, kam si převede peníze, a centrální banka oproti těmto vkladům nakoupí státní dluhopisy, kterými budou CBDC kryté, ne však zpětně směnitelné. Na tyto vklady uživatelům, na rozdíl od jejich banky, poskytne centrální banka úrok, aby uživatele motivovala peníze k sobě převádět. Vše je zatím ve fázi vývoje a hledání možností do budoucna, jedná se především o příležitost pro centrální banky, jak získat větší kontrolu nad penězi a konkurovat komerčním bankám u běžných uživatelů (Stroukal, Skalický, 2021).

4.2 Výroba a průmysl

Zatímco většina aplikací blockchainu je ve finančním průmyslu, zájem o využití blockchainu ve zpracovatelském průmyslu je menší, ale postupně roste. Technologie blockchain má velký potenciál pro řadu činností ve zpracovatelském průmyslu a má schopnost radikálně změnit tvář výroby. Distribuované účetní knihy lze použít při řešení výrobních problémů, zejména při řízení dodavatelského řetězce, včetně sledování kontejnerů během přepravního procesu a zaznamenávání důležitých informací o produktech v celém

dodavatelském řetězci (Attaran, Gunasekaran 2019). Spotřebitelské požadavky na lepší úroveň služeb rostou, což znamená mít k dispozici správný produkt. Nekonečný cyklus rostoucích nákladů dodavatelského řetězce má dopad na konečný výsledek všech zúčastněných stran. Výrobci, maloobchodníci a distributoři označili snižování nákladů dodavatelského řetězce za zásadní problém, který je třeba řešit. Vynikající výkon dodavatelského řetězce má navíc strategickou hodnotu, která by mohla vést k (Attaran, Gunasekaran 2019):

- rychlé finanční návratnosti, často během měsíců;
- zlepšení produktivity a zisků;
- zlepšení pozice zákazníků a kvality produktů;
- zlepšení dlouhodobých vztahů s dodavateli.

V průběhu let technologie jako GPS sledování, radiofrekvenční identifikace (RFID), čárové kódy, chytré štítky, data založená na poloze, bezdrátové senzorové sítě a cloudové technologie sehrály roli v digitálním dodavatelském řetězci s cílem sjednotit informace, procesy a monitorování úrovní zásob v reálném čase a interakce zákazníků s produktem. Následující části poskytují přehled možného využití technologie využívající blockchain ve výrobním sektoru ekonomiky (Attaran, Gunasekaran 2019).

4.2.1 Blockchain pro dodavatelský řetězec a logistiku

Současná koncepce dodavatelských řetězců přestává vyhovovat jednotlivým firmám a zejména pak finálním spotřebitelům. Dnešní doba vyžaduje řešení, která jsou transparentní. Zákazník potřebuje znát co nejvíce informací o produktu, který kupuje, a to nejlépe online, jednoduše a ve správném čase. Těmito informacemi může být např. původ suroviny, seznam dodavatelů, cesta suroviny k zákazníkovi nebo kontrola uhlíkové stopy (Formánek, 2017). Blockchain je vhodným řešením pro velice složité a komplexní uskupení, jakým bezpochyby dodavatelský řetězec je. Průměrný dodavatelský řetězec má stovky až tisíce článků, mezi kterými denně proudí ohromné množství produktů, a ještě více informací. V blockchainu dojde k uvolnění peněz v případě, že dojde k řádnému předání zboží, nebo naopak dojde k převodu peněz zpět při vadné dodávce zboží. To vše lze jednoduše dohledat, což činí transakce transparentní (Formánek, 2017).

Firmy, jenž chtějí mít větší kontrolu nad svým dodavatelským řetězcem, dnes často používají technologii elektronické výměny dat (Electronic Data Interchange – EDI). Jedná se o krok správným směrem, mezi dodavateli a zákazníky existuje protokol, ve kterém všichni účastníci chápou jednotlivé operace. Nicméně v porovnání s blockchainem se jedná o poměrně zastaralou technologii, kde každý ze subjektů musí mít vlastní řešení, které EDI podporuje.

Navíc se jedná o technologii postavenou na centralizovaném modelu. V dodavatelských řetězcích se dříve používala běžná papírová dokumentace, která s postupným rozšířením dodavatelských řetězců přestala být dostačující, což vedlo k využívání EDI. Nyní přestává stačit využívání EDI a objevuje se nová výzva v podobě využívání blockchainu (Formánek, 2017). Dle Formánka (2017) je Blockchain ideální řešení pro řízení dodavatelských řetězců, protože je transparentní, decentralizovaný, online, bezpečný, může být i levný a v neposlední řadě podporuje smart contracts.

V současnosti existují společnosti, které využívají technologie ke zlepšení efektivity dodavatelských řetězců. Například německá kosmetická společnost Beiersdorf experimentovala s blockchainem, aby vytvořila otevřenou výměnu palet. Informace o paletách obsahujících kosmetické produkty osobní péče jsou denně digitalizovány. Naskenováním QR-kódu je možné odeslat, přijmout a zpracovat zásilku palet. Všechny ručně zpracované informace jsou nyní zaznamenávány v důvěryhodné distribuované blockchainové síti. Sdílení dat důvěryhodným způsobem šetří čas a vede k lepší spolupráci (Saxena, 2018).

Také farmaceutická společnost Bayer vyvinula sledování materiálů pomocí blockchainu. Cílem bylo vyvinout snadný tok materiálů a informací pro produkt spolu se sítí partnerů. Bayer úzce spolupracuje s dodavateli, aby přímo informoval průmyslové partnery o potenciálních problémech s produkty. Když dojde k potenciálnímu problému, je možné, že místo pobytu produktu zjistí rychleji než obvykle. Další oblastí, na kterou se plánuje společnost Bayer zaměřit, je prozkoumání potenciálu blockchainu pro rozvoj personalizované zdravotní péče ve spolupráci s průmyslovými partnery a Evropskou unií. Cílem je vyvinout snadný tok materiálů a informací pro produkt a úzce spolupracovat s dodavateli a distributory na přímém informování průmyslových partnerů o potenciálních problémech s produkty. Řešení identifikuje místo, kde se produkt nachází, rychleji než obvykle, což pomůže dosáhnout větší efektivity a bezpečnosti v rámci dodání léčiv (Saxena, 2018).

V roce 2017 vyvinula EZ Lab blockchainovou platformu pro vinařský průmysl s názvem Carto. Farmáři, vinaři a maloobchodníci se mohou zaregistrovat pomocí šifrovaného digitálního podpisu, aby si spotřebitelé mohli ověřit, co kupují. Tato platforma pomáhá vinařskému průmyslu zabránit šíření padělaných produktů. Platforma byla dobře přijata vinařským průmyslem a od roku 2017 zpracovala prodeje vína v hodnotě přes 200 000 USD (Meisner, 2019). Dalším příkladem je Carrefour, nadnárodní společnost, která používá blockchainovou platformu založenou na Ethereu ke sledování stavu produktů – kuřat z volného výběhu a také nabízí možnost ověření pravdivých informací o původu a chovu. Zákazníci naskenují pomocí svého chytrého telefonu QR kód na obalu a získají přístup k informacím o

narození kuřete až do okamžiku, kdy bylo umístěno do chladícího pultu. Carrefour plánuje rozšířit svou platformu na osm dalších živočišných a rostlinných produktových řad, včetně vajec, sýra, mléka, pomerančů, rajčat, lososa a mletého hovězího steaku, ve snaze zaručit to, co popisuje jako úplnou sledovatelnost produktu (Meisner, 2019). V ještě širším a perspektivnějším příkladu potenciální role blockchainu se ukazuje Tesseract, blockchain zaměřený na dopravní průmysl vyvinutý společností EY. V rámci Tesseract mohou uživatelé sledovat vlastnictví, používání a příslušné platby v jakékoli kombinaci jednotlivých vozidel nebo vozových parků. Vozidla a cesty jsou digitálně přihlášeny na blockchain a transakce jsou automaticky vypořádávány mezi vlastníky, operátory a poskytovateli služeb třetích stran prostřednictvím jednotného platebního systému. Protože dopravní prostředky jsou kritickým prvkem v jakémkoli fyzickém dodavatelském řetězci, blockchain může pomoci zahájit novou éru mobility (Meisner, 2019).

Zajímavým projekt pro zlepšení řízení dodavatelského řetězce a obchodních procesů dodavatelského řetězce přináší blockchainová platforma VeChain. Její cílem je zefektivnit tyto procesy a tok informací pro komplexní dodavatelské řetězce pomocí DLT. VeChain se také plánuje stát přední platformou pro provádění transakcí mezi zařízeními připojenými k internetu věcí (IoT). Platformu lze například použít ke sledování kvality, autenticity, skladovací teploty, přepravního média a doručení balení léků nebo lahve na alkohol přímo z výrobního závodu až po konečnou dodávku koncovému zákazníkovi. K dosažení tohoto cíle využívá VeChain chytré čipy nebo RFID štítky a senzory, které vysílají klíčové informace do blockchainové sítě, ke které mají oprávněné zúčastněné strany přístup v reálném čase (Frankenfield, 2021d). Použití senzorů znamená, že všechny parametry související s produktem mohou být neustále monitorovány a případné problémy mohou být sděleny příslušným zainteresovaným stranám. Výrobci a zákazníci jsou informováni, pokud je balíček léku skladován mimo předepsaný teplotní rozsah, což umožňuje zlepšení služeb a lepší kontrolu kvality. Kromě případných problémů jde platforma naproti i lidem s určitým životním postojem, například ekologicky smýšlející jedinci si budou moct koupit takové výrobky, které při cestě neurazily tisíce kilometrů a mají nízkou uhlíkovou stopu (Frankenfield, 2021d).

Technologie blockchain může být také použita v logistice k převedení papírové dokumentace do elektronické, rychlejšímu poskytování důležitých informací, prevenci podvodů při přepravě a dramatickému snížení nákladů na přepravu. Nemálo společností v poslední době testovalo aplikace blockchainu v logistice. IBM a přepravní společnost Maersk dospěly k závěru, že blockchain efektivně sleduje kontejnery během přepravního procesu a tím snižuje náročnost řízení přepravy (Sandner, 2017).

Groopman (2017) poskytuje souhrn aplikací technologie blockchain při řízení dodavatelského řetězce:

- efektivní sledování kontejnerů a produktů po celou jejich cestu;
- přesné zaznamenávání důležitých informací o produktu;
- podporování zabezpečení a dodržování předpisů;
- zajišťování efektivity dopravy;
- urychlení uzavření smlouvy a převodu peněz;
- zlepšení opatření proti padělkům;
- snazší manipulace se smlouvou umožňuje rychlejší přepravní proces a levnější produkty;
- zrychlení dodávky materiálů a produktů;
- levná registrace digitálního majetku.

4.2.2 Blockchain pro internet věcí

Technologie blockchain má obrovský potenciál v kombinaci s IoT. Zařízení IoT shromažďují terabajty dat a informací, které je třeba zpracovat a bezpečně uložit. Blockchain poskytuje několik skvělých způsobů, jak pomoci IoT. Tato technologie eliminuje centrální server a funguje jako most mezi všemi zařízeními IoT. Nabízí také bezpečnou a robustní komunikaci se všemi připojenými zařízeními současně. Blockchain s podporou IoT by mohl být použit jako sdílená účetní kniha k zaznamenávání přepravních kontejnerů při jejich pohybu systémem. Technologie blockchain navíc řeší problém identifikace zařízení IoT a snižuje zranitelnost během tohoto procesu. Pomocí blockchainu zůstane zařízení chráněno vlastnickými právy, která lze snadno převést na někoho jiného. Obě funkce snižují náklady na IoT a zvyšují efektivitu (Attaran, Gunasekaran 2019).

Přínosy technologie blockchainu v IoT shrnuje Attaran a Gunasekaran (2019):

- funguje jako most mezi všemi zařízeními IoT;
- zabraňuje manipulace s daty;
- snižuje zranitelnosti;
- soukromý blockchain funguje jako platforma pro ukládání IoT dat a sdílení se všemi obchodními partnery;
- vytváří tržiště, které zákazníkům umožní prodávat svá data ze zařízení IoT.

Technologie blockchain přinese **zlepšení bezpečnosti a spolehlivosti** v IoT pomocí vyřešení problémů se škálovatelností, soukromím a spolehlivostí v IoT. Technologie blockchain umožňuje významné úspory průmyslu s podporou IoT tím, že zlepšuje sledování

miliard připojených zařízení, umožňuje zpracování transakcí a koordinaci mezi zařízeními. Decentralizovaný přístup blockchainu navíc eliminuje jednotlivé body selhání a vytváří odolnější ekosystém, na které se mohou zařízení připojovat. Kryptografické algoritmy používané blockchainovými řetězci činí spotřebitelská data soukromější a bezpečnější (Banafa, 2016). Technologie blockchain má schopnost nejen automatizovat celý proces, ale také jej výrazně zefektivnit prostřednictvím inteligentního sběru dat. Technologie rychle dospívá a přináší řadu organizačních výhod. Pomocí připojených IoT senzorů můžeme vidět, kde se věci nacházejí, a určit jejich stav na každém kroku. Blockchain s pomocí IoT dokáže sledovat vše v nesmazatelném záznamu. To umožňuje odhalit kritická hlediska v rámci bezpečnosti a kvality produktu, například vědět, zda je zásilka odeslána včas či zda se potraviny přepravují nebo skladují při správných teplotách (Meisner, 2019).

Dalším přínosem blockchainu je **zpracování velkého objemu dat.** I když je IoT enormní příslib, existuje také řada výzev při aplikaci technologie IoT způsobem, který by umožnil její významný a rychlý růst. IoT poskytuje mnoho příležitostí, ale také mnoho starostí s mnoha miliardami připojených zařízení. Jak se zařízení stále více propojují, bezpečnost a soukromí se stávají primárním zájmem spotřebitelů a podniků. Mezi hlavní výzvy patří technologická vyspělost, globální standardizace, dodržování vládních nařízení, náklady a zpracování velkého množství dat. Množství dat, které by zařízení IoT mohla hlásit zpět na cloudový server, by mohlo snadno zahltit databázi (Attaran, Gunasekaran 2019). Společnosti nabízející zařízení s podporou IoT musí být připraveny ukládat, sledovat, analyzovat a rozumět obrovskému množství dat, která budou generována. Skutečná hodnota, kterou IoT vytváří, je v průsečíku shromažďování dat a jejich využití. Velká data vyžadují rozsáhlé výpočetní a úložné infrastruktury pro zpracování a průzkum dat. Očekává se, že miliardy připojených objektů IoT budou generovat objem dat daleko přesahující objem, který lze snadno zpracovat v cloudu, kvůli problémům, jako je omezená kapacita, šířka pásma a latence sítě. Blockchain by mohl tyto problémy vyřešit, lze v něm uchovávat velké objemy dat vytvořených IoT bezpečným a decentralizovaným způsobem, který snižuje šance na úniky dat a také snižuje šance při útoku hackerů (Attaran, Gunasekaran 2019).

Důležitou součástí IoT je **spolupráce, komunikace a konektivita.** Aby IoT fungoval efektivně, vyžaduje spolupráci, koordinaci a konektivitu pro každý kus v systému a v celém systému jako celku. Všechna zařízení musí spolupracovat a být integrována se všemi ostatními zařízeními a také všechna zařízení musí bezproblémově komunikovat a interagovat s připojenými systémy a infrastrukturami bezpečným způsobem. Tradiční centralizovaná síť IoT je drahá, časově náročná, obtížně se udržuje a spravuje. Zařízení jsou připojena, identifikována

a ověřována prostřednictvím cloudových serverů, které poskytují obrovské kapacity pro zpracování a úložiště. Cloudové servery by mohly být úzkým hrdlem a hlavním bodem selhání, které může narušit celou síť (Banafa, 2016). Blockchain nejlépe pomáhá IoT zvládnout komunikaci a konektivitu. Technologie blockchain dokáže komunikovat se všemi zařízeními IoT současně. Může ušetřit peníze, protože eliminuje centrum a funguje jako most mezi všemi zařízeními IoT (Attaran, Gunasekaran 2019).

Role blockchainu v ekosystému IoT. Decentralizovaný přístup k IoT, jako je blockchain networking, by vyřešil mnoho problémů, jež jsou uvedeny výše. Standardizovaná komunikační síť typu peer-to-peer dokáže zpracovat stovky miliard transakcí mezi zařízeními typu IoT. Decentralizovaná síť bude distribuovat výpočetní a úložné potřeby mezi miliardy zařízení tvořících sítě IoT a výrazně sníží náklady spojené s instalací a údržbou velkých centralizovaných datových center. To zabrání selhání kteréhokoli jednotlivého uzlu zhroucení celé sítě tím, že podporuje následující základní funkce (Banafa, 2016):

- zasílání zpráv peer-to-peer;
- distribuované sdílení souborů;
- autonomní koordinace zařízení;
- neměnný záznam historie chytrých zařízení;
- časové razítko řízené konsensem;
- záznamy auditu pro účely řešení problémů.

Blockchain peer-to-peer síť podporuje všechny výše uvedené funkce. Je veřejná, decentralizovaná, neměnná a bezpečná. Poskytuje škálovatelnost, soukromí a spolehlivost potřebnou k zabezpečení nasazení IoT. Je to ideální technologie, která se stane základním prvkem řešení IoT (Attaran, Gunasekaran 2019).

4.2.3 Blockchain pro průmyslový internet věcí

Podobná omezení jako IoT má také Průmyslový internet věcí (IIoT). IIoT popisuje průmyslovou transformaci v propojeném kontextu strojů, kyberneticko-fyzikálních systémů, pokročilé analýzy, umělé inteligence, lidí, cloudu a tak dále. IIoT se skládá z různých inteligentních senzorů a zařízení distribuovaných v celém průmyslovém systému za účelem shromažďování obrovského množství dat, která lze použít k identifikaci úzkých míst, detekci škodlivého chování a odstraňování problémů, což následně zlepšuje efektivitu a kontrolu průmyslových procesů. IIoT se používá v mnoha průmyslových odvětvích, včetně výroby, logistiky, dopravy, energetiky a veřejných služeb. Implementace IIoT v různých odvětvích však není bez problémů. (*I-SCOOP*, 2017).

Blockchainy jsou vhodné pro ukládání dat v rámci IIoT. Firma Super Computing System AG navrhla použití senzorů, které dokážou ukládat a označovat svá data na blockchainu. Díky tomu lze zajistit, že s daty nebylo následně manipulováno a že byly splněny všechny standardy (Sandner, 2017).

Blockchain je zvláště užitečný v situaci, kdy se data IIoT používají ke spuštění transakce, zejména pokud transakce pochází z provedení chytré smlouvy. Technologie blockchain a IIoT mohou být použity k zefektivnění jinak manuálního a zdlouhavého procesu. Například Ondiflo vyvíjí platformu IIoT založenou na blockchainu pro aplikaci na přepravu vody v ropném a plynárenském průmyslu. Senzory IIoT budou umístěny uvnitř vodních nádrží umístěných na ropných polích a budou vysílat signál do přenosové skříně o hladinách vody uvnitř nádrže. Data budou přenesena do cloudu, který zase naplní blockchainovou síť a spustí inteligentní smlouvu, která informuje všechny zúčastněné strany, že je čas buď naplnit nebo vyprázdnit nádrž (Attaran, Gunasekaran 2019).

Technologie blockchain má mnohem větší přesah, již se využívá, či se o jejím využití uvažuje kromě výše uvedeného například ve vládním a veřejném sektoru v rámci decentralizovaných voleb, při kterých nelze podvádět, ve zdravotnictví k vytváření bezpečné a dostupné zdravotnické dokumentace, která nemůže být zpětně změněna, své uplatnění nalézá také ve spotřebitelském průmyslu pro distribuci zboží a v maloobchodu, v herním průmyslu, v potravinářském průmyslu, v leteckém průmyslu, ve 3D tisku, či ve správě dat.

5 Posouzení využití technologie blockchain a kryptoměn v podnikové praxi

5.1 Metodika

Druhá část bakalářské práce se zabývá analýzou využití kryptoměn a blockchainu v podnikové praxi formou strukturovaných rozhovorů s odborníky, kteří se v tomto odvětví aktivně pohybují. Výzkum probíhal v těchto krocích: příprava otázek pro strukturovaný rozhovor (viz příloha 2), výběr vhodných respondentů, oslovení respondentů, následná domluva termínu a upřesnění informací, samotný rozhovor, a následné vyhodnocení.

Na základě zkušenosti autora práce z účasti na konferencích, seminářích a odborných fórech na téma technologie blockchain a kryptoměn a sledování diskuse v on-line prostředí k této problematice, byli vytipováni odborníci v této oblasti. Vybráni byli odborníci z ČR a Slovenska, z českých i nadnárodních firem, kteří aktivně Bitcoin, či jiné kryptoměny využívají pro své podnikatelské činnosti, dále lektoři a lidé věnující se osvětě v této oblasti. Celkem bylo osloveno 16 respondentů prostřednictvím e-mailu, z nichž s následným rozhovorem souhlasilo pět a jeden respondent přislíbil z časových důvodů odpovědět písemně.

Samotné rozhovory s pěti respondenty probíhaly online přes aplikaci Google Meet, či MS Teams a měly trvání od 30 minut až po 2 hodiny. Rozhovor probíhal chronologicky dle připraveného scénáře, odpovědi byly rovnou zaznamenávány, a pro uchování a další kontrolu byly rozhovory se souhlasem respondentů rovněž nahrávány. Všichni respondenti souhlasili s jmenovitým uvedením v této práci.

5.2 Charakteristika respondentů

Prvním z respondentů byl Petr Kučera, jehož profesním zaměřením je advokacie v advokátní kanceláři Blockchain legal, která se ve své praxi zaměřuje na činnosti spojené s kryptoměnami, jako je digitální bezpečnost, regulace pro burzy a směnárny, těžba kryptoměn, správa portfolií a podobně. Zajímavostí je vydání vlastní elektronické knihy s názvem Příručka hodlera, která se zaměřuje na digitální bezpečnost, kryptoměnové peněženky a jejich zálohování a dále se zaměřuje také na dědictví digitálních aktiv.

Druhým z respondentů byl Adam Lokaj, jenž se ve své podnikatelské činnosti soustředí na adopci Bitcoinu do podniků. Rovněž napsal publikaci s názvem Adopce Bitcoinu pro obchodní korporace, kde lze nalézt důvody pro adopci Bitcoinu a způsoby jejího provedení, návod k vyplácení mzdy v Bitcoinu a také daňové a účetní aspekty adopce. Jeho cílem je co nejvíce rozšířit povědomost o Bitcoinu a přivést ho do podniků.

Třetím respondentem byl Dušan Matuška, jediný zahraniční respondent ze Slovenska. Dušan je podnikatel, lektor a konzultant v oblasti Bitcoinu. Je jedním z předních školitelů v oblasti kryptoměn na Slovensku. Populární je jeho podcast Jednoducho Bitcoin, ve kterém se snaží o srozumitelné vysvětlení Bitcoinu pro veřejnost. Jeho cílem je do roku 2030 vzdělat 100 milionů lidí v bitcoinovém odvětví. Momentálně pracuje na projektu vybudování bitcoinového edukačního centra na ostrově Roatán v Hondurasu.

Čtvrtým respondentem byl Kristian Csepcsar, který působí jako marketingový ředitel v společnosti Braiins, což je nadnárodní bitcoinová těžební společnost se sídlem v ČR a zároveň také nakladatelství, které vydává knihy v češtině o Bitcoinu, například v květnu vyšla nová kniha Bitcoinový standart poprvé v českém jazyce. Ke společnosti Braiins patří první těžební pool na světě, a to konkrétně Slush Pool.

Pátým respondentem byl Radek Horák, finanční a provozní ředitel mezinárodní společnosti Rockaway Blockchain Fund, která je součástí investičního fondu Rockaway Capital. Rockaway Blockchain je evropský soukromý investor s celosvětovým dosahem. Fond investuje do slibných blockchainových start-upů, kterým pomáhá růst. Dlouhodobě čerpá zkušenosti z tradičních rizikových investic a převádí je do světa kryptoměn.

Šestým, posledním respondentem, byl vedoucí zákaznické péče v české směnárně Anycoin, Jiří Skácel. Anycoin je směnárna, která se zaměřuje na směnu kryptoměn. Směnárna funguje od roku 2019 a stává se více a více populární. Se zástupcem směnárny neproběhl rozhovor, nýbrž byl dotazník poslán emailem.

5.3 Vyhodnocení vlastního výzkumu

Výzkum byl vyhodnocován jednotlivě za každého respondenta, jelikož se jedná o výzkum kvalitativní, nelze jej považovat za reprezentativní, nýbrž jistý pohled ze světa odborníků přináší.

5.3.1 Petr Kučera – Blockchain legal

První respondent se v kryptoměnách pohybuje od roku 2017, v témže roce vznikla také advokátní kancelář, ve které působí. Z kryptoměn využívá hlavně Bitcoin a Ethereum. Hlavním důvodem pro tyto 2 kryptoměny je fakt, že advokátní kancelář přijímá platbu za své služby právě v těchto měnách. Sám za sebe používá Bitcoin k placení a k dlouhodobému spoření. Hlavní výhody pro uživatele kryptoměn spatřuje v tom, že člověk je sám sobě bankou – spravuje si vlastní finance, za další výhodu lze považovat rychlost transakce a také to, že se jedná o alternativní statek, který může být důležitý především pro nerozvinuté státy. Za nevýhody naopak považuje poplatky, jenž se vztahují přímo na uživatele, a ne na obchodníka

jako je tomu dnes například u platby kartou. Jako bezpečnostní rizika ve spojení s kryptoměnami vnímá to, že uživatel přijímá plnou odpovědnost, když například chce Bitcoin někam poslat, zadá-li špatnou adresu, již není velká naděje návratu Bitcoinu, dále také hraje roli tržní riziko a digitální bezpečnost. Současnou situaci akceptace kryptoměn vnímá v ČR velice pozitivně ve srovnání se světem, jako příklad je uváděna platební brána Confirmo, která umožňuje podnikům přijímat platby v kryptoměnách. Aby se situace ještě více zlepšila, chtělo by to dostat technologii a kryptoměny více do mainstreamových medií, a nejen když cena dramaticky stoupne, či klesá, což chce samozřejmě čas.

Bitcoin je hlavní kryptoměnou, kterou Petr Kučera využívá, nicméně v advokátní kanceláři mají nyní větší objem plateb v Ethereu. Největší hrozby pro Bitcoin, jsou regulace, nicméně jeho úplný zákaz nehrozí. Transakce v Bitcoinech budou do budoucna více a více směřovat k využívání lightning networku pro drobné platby např. v ochodech, naopak ty větší platby budou probíhat klasicky on-chain. Pozitivně vnímá přijetí Bitcoinu v Salvadoru, a to hlavně díky tamní ekonomice, přeskočení bankovního systému a ušetření peněz běžným občanům co se remitence týče, celkově je to vnímáno jako zajímavý experiment, který přinese zkušenosti ostatním zemím, nicméně by to nemuselo být až tak donucované tamní vládou. Podle respondenta je Bitcoin v podnikovém prostředí využíván jako investice, jako alternativní financování firmy – Initial coin offering (počáteční nabídka mincí, obdobně je to např. u akcií), dále vznikají businessy postavené na Bitcoinu, zároveň ale dodává, že se prozatím nesetkává s větším průmyslovým využitím.

Mezi další kryptoměny, které jsou respondentem využívány patří Ethereum a stablecoiny. Ethereum také považuje po Bitcoinu za nejúspěšnější projekt, díky chytrým kontraktům, které přinesl. Jestli se najde využití, pro to, co další kryptoměny přinesly ukáže až čas, nicméně je zajímavé hledat pořád další možnosti a uplatnění, zároveň, ale také může jít o slepou větev, která se postupem času vytratí. Zároveň je spíše skeptický k metaverse světu, a jako důvod je udáván money first problém – nejdříve se vyberou peníze a poté možná něco vznikne. Další kryptoměny mohou být podle něj využívány v podniku jako prostředek směny na B2B trhu, například stablecoiny, dále NFT jako digitální umění může mít pro podniky zajímavé využití.

Co se blockchainu týče dle respondenta záleží, co od něj bude kdo čekat a čeho bude chtít dosáhnout. Jako jeho výhodu vidí decentralizaci a mechanismus konsensu, naopak nevýhody může přinést čas, kdy je možné že se ukáže, že použití běžné databáze je levnější, efektivnější a méně náročné. Největší smysl mu dává veřejný blockchain a konsensus PoW, který považuje za vyzkoušený a odolný. Co se finančního sektoru týče, tak blockchain nachází uplatnění v investování, v platbách a ve fondech, dodává že CBDC ve výsledku nebudou vůbec na

blockchainu a nedá se mluvit o konkurenci kryptoměn. Další uplatnění blockchainu dle jeho názoru lze nalézt v logistice a v dodavatelském řetězci, jako možnost udává digitální nákladní listy. Dále je dle něj možné i vetší uplatnění v IoT. Naopak s uplatněním v průmyslu a výrobě nemá zkušenosti. Na závěr dodává, že je důležité si uvědomit, jaký byl prvotní use case, kvůli kterému to bylo vytvořeno, a to je Bitcoin a platby, které tu už zůstanou a další využití přinese čas.

5.3.2 Adam Lokaj – Adopce Bitcoinu

Druhý respondent se pohybuje v kryptoměnách od roku 2019, především díky vidině rychlého zbohatnutí, poté se v roce 2020 začal o kryptoměny, a hlavně o Bitcoin zajímat více do hloubky. Nyní Bitcoin zůstal také jedinou kryptoměnou, kterou využívá. Do hloubky se zajímá o kryptoměny jako o investici, o zhodnocení volných prostředků a také nevěří fiat měnám, které dle něj nejsou dlouhodobě udržitelné. K praktickým zkušenostem s využíváním řadí platby a investice. Hlavní výhodu pro uživatele kryptoměn spatřuje v anonymitě, naopak mezi nevýhody řadí vysokou volatilitu a prozatímní omezenou použitelnost. Oblast kryptoměn je dle respondenta spojena s rizikem, které přináší především vlastní velká odpovědnost, uživatel je sám sobě bankou a také nenávratnost prostředků při chybování např. při zadání chybné adresy. Současnou situaci akceptace kryptoměn v ČR vnímá tak, že jsme stále ještě na začátku, využívají to doposud jen jednotky firem i když on sám se snaží do firem Bitcoin dostat. Předpoklady pro zlepšení situace vidí jednak v devalvaci měny nějakého státu, a jednak v tom, že nějaký ekonomicky vyspělý stát nakoupí kryptoměny do svých rezerv. Zároveň dodává, že pro zvětšení povědomí o kryptoměnách je nutné vzdělávat mladou generaci v této oblasti a dále ve firmách bude důležité vyplácet mzdu právě v kryptoměnách.

Bitcoin vidí jako uchovatele hodnoty, jeho hlavní výhody spatřuje v decentralizaci, v jasných, předem stanovených pravidlech, které nemůže nikdo měnit a také anonymitu. Jako hrozby pro Bitcoin vidí státní regulace, které ovšem jsou zrealizované jen lokálně a ne globálně, závislost na internetu, a také problém škálování, které je ale vyřešené lightning networkem. Bitcoin pro něj ze začátku znamenal spíše spekulativní investici, nyní představuje přístav, svobodný, decentralizovaný přístav, který zaručuje, že to, co si nakoupí mu nikdo nevezme, z dlouhodobého hlediska pro něj představuje uchovatele hodnoty. Budoucnost bitcoinových transakcí vidí v používání on-chain transakcí pro větší platby, pro menší pak předpokládá větší využívání lightning networku. Cesta k většímu využití Bitcoinu se dle respondenta potkává s úskalím Greshamova zákonu, kdy špatné peníze (fiat), vytlačují ty dobré (Bitcoin). K přijetí Bitcoinu v Salvadoru se staví neutrálně, bere to za dobrou zkušenost, ale zatím bez většího

dopadu. Co se dalších států týče, tak dle respondenta není otázka, jestli se další přidají, ale kdy. Respondent vidí využití Bitcoinu v podniku jako formu investice, zajištění proti inflaci, jako platební prostředek mezi smluvními stranami, dále vidí pro podniky možnost těžby a možnost vyplácení mzdy.

Co se týče dalších kryptoměn, tak okrajově využívá Basic Attention Token, ve formě odměn v internetovém prohlížeči Brave. Ostatní funkce, co kryptoměny přinesly, nepovažuje za zajímavé, a to ani NFT, které považuje za příliš nadhodnocené a neodůvodnitelné je vlastnit.

Za hlavní výhody blockchainu považuje veřejnou dostupnost, jednoduchou kontrolu a předem stanovená pravidla, které nelze porušit. Dále dodává klíčovou věc a to, že blockchain vyřešil problém, který doposud vyřešen nebyl, a to problém byzantských generálů. Problém byzantských generálů vychází z teorie her a klade si otázku, jestli mohou účastníci určité situace dosáhnout shody – konsensu na řešení dané situace, když neví a nemohou si nijak ověřit, zda ostatní mluví pravdu nebo lžou. Jako nejlepší konsensus považuje PoW, a to díky tomu, že je odzkoušený a krytý nějakou hodnotou. CBDC považuje za nesmysl, jako nástroj státu k větší kontrole financí. Další využití blockchainu vidí jen v herním průmyslu, jiné možnosti se mu prozatím jeví irelevantně.

5.3.3 Dušan Matuška – Lektor

Třetí respondent se v kryptoměnách pohybuje od roku 2017, a to díky svému kamarádovi, který ho k tomuto sektoru přivedl. Postupem času se z něj stal Bitcoin maximalista, což znamená, že postupně přešel pouze k využívání Bitcoinu, který hojně využívá, např k placení kávy, jídla v restauracích, přátelům za různé služby, co se videí a grafiky týče, dále mu zákazníci platí v Bitcoinu za konzultace, za přednášky. Bitcoin tedy využívá jako platební prostředek, a to i v zahraničí, kde cíleně vyhledává obchody a restaurace, které nabízejí službu placení právě v Bitcoinu. Výhody uživatelů kryptoměn spatřuje v rychlosti převodů mezi uživateli se zachováním soukromí a dále uvádí, že se jedná o nejlepší spoření ve svobodných penězích. Naopak co se nevýhod týče uvádí důraz na bezpečnost, přebírání odpovědnosti sám na sebe, problém práce s volatilitou, která je v Bitcoinu dost velká a s tím spojenou psychologii. Ohledně rizik se obává státních regulací, které se budou snažit o deanonymizaci transakcí, neobává se tedy technických problémů, ale spíše regulačních opatření. Současnou situaci akceptace kryptoměn na Slovensku vnímá tak, že je prozatím malá, ale postupně roste na Slovensku se dají koupit kryptoměny dokonce i na každé poště. V porovnání se světem je na tom Slovensko i ČR o poznání lépe. Předpoklady pro zlepšení vidí ve větším používání, zvlášť by prospělo, kdyby začalo více firem vyplácet své zaměstnance v Bitcoinu.

Hlavní přínos Bitcoinu spatřuje v tom, že se jedná o první decentralizované peníze, peníze bez státu, bez možností podvádět. Pro respondenta znamená Bitcoin životní filozofii, životní směr. Bitcoin využívá k tomu samému k čemu vyžívá dnešní peníze, a ještě dodává další využití, a to těžbu. Denní, menší transakce budou podle něj postupně přecházet na síť lightning network, kde vidí i cestu k většímu využívání Bitcoinu, naopak ty velké budou probíhat klasicky on-chain. Z přijetí Bitcoinu v Salvadoru není moc nadšený, jelikož to víceméně bylo nucené, ale zároveň se jedná o zajímavý experiment, který do budoucna přinese zajímavé poznatky k většímu využívání. V budoucna se k přijetí Bitcoinu, jako zákonného platidla přidají další státy, nyní se už bavíme o Madeiře a o Hondurasu. Co se podnikového prostředí týče, tak využívání Bitcoinu postupně roste, zatím ho podniky využívají hlavně ke spoření a platebnímu styku, který vychází výhodněji než například SWIFT platby. Do budoucna se dá předpokládat i s postupným rostoucím počtem podniků, jenž budu v Bitcoinu vyplácet své zaměstnance.

Kromě Bitcoinu považuje za úspěšný projekt Ethereum, které zahrnuje zajímavosti, které je třeba prozkoumat. Další využití blockchainu ani ostatních kryptoměn nenalézá, protože se věnuje pouze Bitcoinu. CBDC považuje za nesmysl, za nástroj totality.

5.3.4 Kristian Csepsar – Braiins

Respondent číslo čtyři se v kryptoměnách pohybuje od konce roku 2016, dostal se k nim prostřednictvím přátele s vidinou výdělku, když právě koncem roku 2016 se kryptoměnovým světem nesla vlna altcoinů, které rychle nabírali na ceně. Postupem času se jeho filozofie, obdobně jako u respondenta výše změnila na Bitcoin maximalismus. Praktické zkušenosti má velké jak v osobním životě, tak v životě spojeném s jeho profesí, za zmínku stojí vývoj softwaru pro těžbu. V osobním životě rád zkouší kryptoměnami platit. Hlavní výhody uživatelů kryptoměn spatřuje v tom, že uživatel začne více přemýšlet o penězích jako takových, o ekonomice, začne přemýšlet o nových možnostech, o investicích. Naopak nevýhody vidí v nebezpečí gamblingu, a také upozorňuje, že u některých bank může být problém získat půjčku, či hypotéku, jelikož uživatel, který nakupuje kryptoměny je brán za potencionálně rizikového. Bezpečnostní rizika dle něj představují různé scamy (podvody), které v tomto prostředí bohužel vznikají, dále nebezpečí toho být sám sobě bankou a v neposlední řadě dodává nebezpečí držení kryptoaktiv na burzách – not your keys, not your coins. Současnou situaci akceptace kryptoměn v ČR vnímá velmi pozitivně, jelikož tu máme plno obchodů, e-shopů a restaurací, které kryptoměny přijímají, současně z ČR pochází i první těžební pool, dokonce říká, že ČR by mohla být takové kryptoměnové Švýcarsko. Pro větší povědomí je dle

něj nutné vzdělávání a větší osvěta, o což se snaží ve firmě právě vydáváním knih, zároveň kvituje odvahu a zájem se pustit do psaní bakalářské práce na toto téma.

Bitcoin pro respondenta znamená svobodu, jeho hlavní přínos vidí v tom, že umožňuje uživatelům jistý plán B a kontrolu sám nad sebou, pro firmy vidí přínos v tom, že investice či těžba mohou působit jako ochrana proti inflaci. Mezi největší hrozby řadí nepravdy, které o Bitcoinu kolují, například o pálení energie a také regulace, nicméně jeho globální zákaz není možný, zároveň si je jist, že všechno tohle Bitcoin přežije. Respondent v Bitcoinu dostává část výplaty, dále ho aktivně využívá k placení a ke spoření. Nejen lightning network, ale i další vrstvy povedou k většímu využití Bitcoinu, na on-chainu zůstanou větší transakce. K přijetí Bitcoinu jako oficiálního platidla v Salvadoru se staví pozitivně, přišlo to dříve, než kdokoliv čekal, a tvrdí že další státy budou přibývat. Praktické zkušenosti má i s nakupováním Bitcoinu do firem, kde mnohým z nich pomáhal nakupovat Bitcoin, jako dlouhodobé rezervy a inflační zajištění.

Nejúspěšnějším projektem po Bitcoinu, je dle respondenta stablecoin USDT, který představuje jakýsi digitalizovaný dolar, který se dá poslat rychle kamkoliv. Jeho názor na to, co ostatní kryptoměny přinesly je takový, že se to přeceňuje, ale na druhou stranu uvádí, že je dobré zkoušet všechna možná využití a vzít si z toho to dobré a v ideálním případě to přetavit do zlepšení funkčnosti Bitcoinu, podobně se staví i k NFT, které dle něj neumřou, ale budou zabírat jen minoritní podíl. Velice negativní postoj zaujímá k CBDC, které vnímá jako nástroj centrálních bank k větší moci. Naopak s příslibem do budoucna se mu jeví metaverse prostředí, které může na Bitcoinu zajímavě fungovat. Příznivě se mu jeví také použití blockchainu v herním prostředí, ale na druhou stranu to může být také slepá ulička. Dodává, že i ostatní kryptoměny a NFT nalézají využití v podniku, jako příklad uvádí využití NFT, společnosti Nike, která vytváří digitální boty skrz NFT – NFT Nike Sneakers, což považuje za zajímavý marketingový nástroj, kterým osloví nové zákazníky a za prostředek, který vede k zisku, jelikož se prodávají za stovky tisíc dolarů – a to jde jen o obrázek.

5.3.5 Radek Horák – Rockaway Blockchain Fund

Respondent se ke kryptoměnám dostal prostřednictvím své práce v Rockaway Blockchain Fund v roce 2018. Náplní fondu jsou investice do blockchainových projektů, sám respondent využívá převážně stablecoiny. Na rozdíl od ostatních investorů, tento respondent nevyužívá Bitcoin, jako takový, nýbrž ve firmě, která hledá zajímavé blockchainové projekty.

Technologie blockchainu je dle něj stále na začátku a postupně se vyvíjí a jeho využití roste. NFT považuje za zajímavý fenomén, prokazování digitálního vlastnictví může být

zajímavé pro sběratele jakéhokoliv typu, když budu akceptovat přesun do digitálního světa – například na rozdíl od sbírání fyzických hokejových kartiček bude sbírat hokejové kartičky digitální. Zajímavě se mu v této souvislosti jeví také digitální umění. K metaverse prostředí uvádí, že život se postupně přesouvá do digitální podoby a blockchain v tom bude hrát svou roli. Je také spokojen s tím, jak se vyvíjí herní blockchainový sektor, kde mu přijde zajímavé prokázání vlastnění věcí ve hře, s možností následného prodeje.

Za výhody v technologii založené na blockchainu považuje decentralizaci a odměňovací mechanismus, jako možnost využití uvádí finanční služby, registry bez centrální entity, díky blockchainu mohou lidé pracovat na projektu, aniž by se znali, dále DeFi, NFT, gaming, dodavatelský řetězec, vedení zdravotní dokumentace a Web 3.0. Naopak za nevýhody blockchainu považuje nemožnost využití pro všechno, ale také uvádí, že některé centrální databáze se mohou ukázat jako rychlejší a levnější. Sami ve firmě podporují spíše veřejný blockchain, který firmy také více využívají, privátní blockchain je zatím bez většího úspěchu. Za nejlepší konsensus považuje PoS, který se dle něj jeví nejlépe a prostředí kryptoměn k němu postupně směřuje, například Ethereum, se chystá přejít na konsensus PoS, dodává, že pro Bitcoin má PoW své opodstatnění. Co se využití blockchainu ve finančním sektoru týče, tak se to dle respondenta dá rozdělit na dvě části. Za první lze považovat finanční služby bez bank, které přináší alternativu k bankám a ke karetním společnostem (např. Visa, Mastercard), lending protokoly (půjčky v kryptoměnách) a také tokenizaci (proces, který převede hodnotu jakýchkoliv aktiv na blockchain). Za druhou část považuje interní využití ve firmách, jako příklad uvádí společnost Figure, do které v rámci fondu investovali, a blockchain zde přinesl automatizaci v interních procesech. Co se ještě finanční sféry týče, tak se mu jako užitečná funkčnost jeví kryptoměna Ripple na rychlejší mezibankovní vztah. Celkově hodnotí finanční sektor jako velmi užitečný pro blockchain, pro systém bez bank, pro celkovou automatizaci s cílem vše zrychlit a zlevnit. CBDC obecně považuje za problém, který se v budoucnu může přetavit do toho, že centrální banka bude nařizovat občanům, za co mohou a nemohou své peníze utratit.

Uplatnění ve výrobě a v podniku vidí v oblasti tresury managementu a v dodavatelských řetězcích, na kterých bude postupně vznikat více aplikací. V dodavatelských řetězcích dává za příklad, který funguje sledování květin z Keni právě pomocí blockchainu, kdy se zákazníci mohou podívat, kde se květiny nachází v danou chvíli a jakou cestu k nim urazily. Dále za příklad uvádí firmu IBM, která se snaží blockchain využívat pro sledování celého dodavatelského řetězce, i pro interní využití, kde mají dokonce svojí blockchainovou divizi. Velký smysl mu dává také využití blockchainu pro IoT, vypichuje blockchain s názvem

Helium, což je kryptoměna zamýšlená jako podnět pro uživatele k nastavení uzlů pro 4G bezdrátovou LAN pro IoT. Tato síť je globální a zdaleka největší decentralizovanou IoT sítí na světě, navíc je také open source, dodává, že se jedná o ideální řešení rovněž pro energetiku. Další uplatnění vidí, v již zmiňovaném Webu 3.0, který přinese decentralizované sociální sítě bez Googlu, bez Meta. Nezapomíná ani na veřejné registry v zdravotnictví a pojišťovnictví.

5.3.6 Jiří Skácel – Anycoin

Poslední respondent se dostal ke kryptoměnám v létě roku 2017, prostřednictvím kamaráda, jenž mu poradil do Bitcoinu investovat. Z kryptoměn využívá hlavně Bitcoin na platby pomocí lightning network a Ethereum na swapy (směna kryptoměny za jinou) a smart kontrakty. Z toho pramení i praktické zkušenosti, ke kterým patří platby, swapy alcoinů a také spoření. Respondent také cíleně vyhledává obchody, kde kryptoměny přijímají. Hlavní výhody uživatelů kryptoměn spatřuje v tom, že mezi námi a penězi není žádná třetí strana, každý je zde svým pánem, naopak k nevýhodám řadí vyšší zodpovědnost dané osoby, vyšší riziko ztráty v případě neopatrnosti a neinformovanosti (nutno se vzdělat ohledně bezpečnosti především) a také potenciální podvody – peníze již nikdo nevrátí. Současnou situaci akceptace vnímá tak, že se pomalu zlepšuje, k předpokladům pro zlepšení řadí větší osvětu, ustálení kurzu Bitcoinu a napomoci by mohly i případné horší ekonomické podmínky, např. velká inflace. Aby měla společnost o kryptoměnách větší povědomí je dle respondenta třeba pořádání otevřených konferencí, nehodlovat, nýbrž aktivně využívat, a nakonec dodává, že by pomohlo dostat „kryptoinfluencery“ více do medií.

Bitcoin pro respondenta znamená svobodu a je to pro něj také nejvíce využívaná kryptoměna, jejíž přínos vidí v osvědčenosti, PoW konsensu a další vrstvě v podobě lightning networku. Nepovažuje za reálné, aby Bitcoin nějakým způsobem skončil, ale vyskytují se zde lokální hrozby jako regulace. Uvádí, že pro Bitcoin jsou důležitá oba typy transakcí, jednak lighning network určený pro mikro platby a jednak on-chain pro platby větší. Pozitivně vnímá přijetí Bitcoinu jako oficiálního platidla, dodává, že další státy se k Salvadoru již přidávají. Podle respondenta je Bitcoin v podnikovém prostředí využíván jako platební prostředek, jako příklad dodává Alzu a další e-shopy, jenž lze najít zde: https://www.mapotic.com/bitcoin-map dále firmy do kryptoměn hodně investují, ale bohužel je nemůže konkrétně jmenovat, z obecně známých jsou to pak Microstrategy a Tesla.

Ostatní kryptoměny příliš nevyužívá, spíše je drží kvůli spekulaci. Po Bitcoinu považuje za zajímavé projekty stablecoiny, kvůli mechanismu udržování hodnoty. Z toho, co přináší další kryptoměny mu přijde zajímavé DeFi, ale dle respondenta je potřeba to správně uchopit, dnes

je tam mnoho tzv. moneygrabů (nedůstojné nebo bezzásadové získání velkého množství peněz s malým úsilím k použití na to, kvůli čemu byly vybrány), které se snaží pouze vytěžit na hypu (příliš mnoho pozornosti, zájmu kolem něčeho, v tomto případě přehnaný zájem o DeFi ze strany retailu). U NFT vidí potenciální využití, ale je vždy otázka, zda je využití opravdu nutné a není pro to již existující alternativa (QR kódy apod.). Ohledně metaverse zůstává stručný, i když přiznává, že to je zajímavá oblast, ale neočekává, že to poroste tak rychle. Patrně celkem velký potenciál pro blockchain vidí v gamingu, kde tvrdí, že bude úspěšný především díky možnosti použití stejných předmětů pomocí NFT v různých hrách. O CBDC si myslí, že nemohou přinést nic pozitivního.

5.3.7 Diskuse

Žijeme v turbulentním prostředí, a konkrétně prostředí kryptoměn a blockchainu se mění každým dnem, jen při psaní této bakalářské práce se toho událo mnoho. Bitcoin byl přijat jako oficiální platidlo v dalších státech, například ve Středoafrické republice. NFT se stávají více a více populární, začali je využívat velké společnosti jako ŠKODA AUTO a.s., která k třicetiletému partnerství mistrovství světa v hokeji vydala 30 sběratelských puků právě s pomocí blockchainu a NFT. Rozrostl se také počet konaných konferencí, a přišla řada zněm. Algoritmické stablecoiny se ukázaly jako nefunkční, když cena jednoho z nich se blíží nule, vzniklo plno podvodných projektů, ale také plno projektů slibných.

V ČR i v zahraničí by se dala kryptoměnová komunita rozdělit na dva tábory. Jedni jsou zaměřeni pouze na Bitcoin, tzv. Bitcoin maximalisti. Tato skupina vidí využití kryptoměn v podniku na bázi investic, platebního styku, spoření a zajištění proti inflaci, naopak technologii blockchainu nevidí jako něco, co by mělo jakoukoliv přidanou hodnotu, a neumí si představit jeho další využití. K těmto názorům se hlásí kupříkladu přední český ekonom Stroukal (2021), či lektor Tětek (2021). Naopak druhá skupina vidí v blockchainu obrovský potenciál.

Technologie blockchain nachází uplatnění nejen v oblasti kryptoměn, ale také ve všech výše zmíněných oblastech, jako jsou dodavatelské řetězce, správa dat, finanční sektor, herní sektor, zdravotnictví, IoT, veřejné registry, Web 3.0, digitální umění, metaverse a podobně. Implementace blockchainu do těchto oblastí by znamenala především přínos ve formě decentralizovaného řešení, zlepšení komunikace, větší transparentnost a snížení nákladů. Dalším klíčovým přínosem je razantní zvýšení bezpečnosti, což je v posledních měsících hojně skloňované téma, kdy se řada institucí setkala právě s kybernetickými útoky hackerů. S těmito názory se ze zahraničních autorů ztotožňuje Attaran a Gunasekaran (2019), či Saxena (2018), z českých autorů pak kupříkladu Formánek (2017).

Toto rozdělení se potvrdilo v praktické části, kde se část respondentů zaměřuje výhradně na používání Bitcoinu, a druhá část se zajímá o další možnosti využití samotné technologie blockchain.

Respondenti se většinově shodují na vnímání Bitcoinu, blockchainu či dalších kryptoměn jako na nástrojích osobní svobody, svobody ve firmě, nezávislosti na centrálních institucích, dále se shodují na tom, že se jedná o možnost zlepšit ve firmě digitální bezpečnost svých dat, ale na druhou stranu konstatují, že s tím souvisí vyšší odpovědnost v případě chyb. Tento přínos očekávají i pro další aplikace blockchainu. Zároveň všichni vnímají CBDC jako velké nebezpečí díky absolutní kontrole nad transakcemi z pohledu centrálních bank. Každý jednotlivě přidal zajímavý názor či podnět, za příklad lze uvést vyplácení v kryptoměnách, které by vedli ke větší adaptaci jak v podnicích, tak ve společnosti. S příslibem vidí respondenti použití blockchainu hlavně v dodavatelských řetězcích, kupříkladu lze uvést již existující blockchain monitorující pohyb květin dovážených z Keni po celou dobu trvání dodavatelského řetězce. Jako další blockchain s velikými ambicemi lze uvést Helium, zamýšlený jako podnět pro uživatele k nastavení uzlů pro 4G bezdrátovou LAN pro IoT.

Blockchain nachází prozatím uplatnění především jako technologie, na které stojí kryptoměny. Tou nejznámější je Bitcoin, který může být ve firmách využíván především jako forma investic, které pomůžou zajistit firmu proti inflaci, dále jako prostředek směny, který podnikům přináší alternativní možnost placení, a tím může přinést konkurenční výhodu. Stejně tak mohou být v podniku využity i další kryptoměny jako třeba Ethereum, které přináší možnost smart contracts jako nástrojů k uzavírání smluv, či NFT. Praktická část, která navazuje na část teoretickou, potvrzuje, že blockchain nejsou jen kryptoměny, a své uplatnění postupně nachází i v dalších oblastech.

Co se týká nevýhod, kromě větší odpovědnosti za případné chyby, upozornili respondenti na nebezpečí závislosti a gamblingu u kryptoměn, dále upozorňují, že je vždy nutné porovnat nákladovost řešení s pomocí blockchain technologie v porovnání s centralizovanými řešeními.

Vzhledem k tomu v jak rychle rozvíjejícím prostředí se pohybujeme, je pro podniky klíčové hledat stále nové a nové inovace, které přinášejí nejen rozvoj firmy samotné, ale i rozvoj společnosti celkově. Takovou inovací může být právě implementace kryptoměn a blockchainu do podniku, které by mohlo přinést ušetření časových i finančních nákladů, zvýšit transparentnost a zabezpečení uchovávaných dat, což je to klíčové, co blockchain i kryptoměny přinášejí, a proč by měly být do podniku implementovány. Taktéž se jedná o jednu z mála technologií, která je schopná vysoké nároky na zabezpečení poskytnout.

ZÁVĚR

Tato práce přináší základní pohled do světa kryptoměn a blockchainu. Čtenáři by po přečtení této práce měli být zřejmé principy blockchainu, dále co to kryptoměny jsou, jak fungují a k čemu jsou dobré, stejně tak by si čtenář měl udělat obrázek o využití blockchainu a kryptoměn v praxi.

Cíle práce, které byly pro teoretickou část stanoveny na přiblížení technologie blockchain, na obecné principy kryptografie, na vymezení základních kryptoměn a na možnosti využití blockchainu v praxi, byly naplněny. Z kryptoměn, které jsou prvotním využitím blockchainu v praxi, byl představen Bitcoin, Litecoin, Ethereum a stablecoiny. Bylo představeno, jak je důležitá kryptografie a jakou hraje v blockchainové technologii roli, dále jakými konsensy lze dojít ke všeobecné shodě, jaké jsou kryptoměnové klíče, a co se děje, když v blockchainu dojde k rozvětvení. Jako na klíčový přínos blockchainu bylo poukázáno na jeho decentralizaci.

Dále jsou představeny možnosti využití kryptoměn a technologie blockchain v podniku, ale i v dalších oblastech. Z podnikové praxe se práce zaměřuje zejména na použití blockchainu v dodavatelském řetězci a v IoT, do kterých může blockchain přinést větší transparentnost, přehlednost, zpřístupnit informace právě v čase, kdy jsou potřeba a v neposlední řadě je podstatným přínosem bezpečnost, která bývá často podceňována. Další podstatnou oblastí využití technologie blockchain je sledování surovin, materiálů, zboží, výrobků a kontejnerů v rámci celého dodavatelského řetězce až ke konečnému zákazníkovi. V neposlední řadě blockchain představuje potenciál ve formě snížení nákladů a času. Své využití v podniku nalézají i kryptoměny, a to jako forma investic, či spoření, ale také jako prostředek platby a dlouhodobé zajištění proti inflaci. Kromě platebního styku, které první kryptoměny přinesly, byly představeny i jejich další přínosy jako smart contracts, či NFT, které se ukazují i jako zajímavý marketingový nástroj.

Díky provedeným strukturovaným rozhovorům s odborníky ve výzkumné části byly identifikovány další oblasti využití, jako Web 3.0, metaverse, lending protokoly, vyplácení mezd v kryptoměnách, byly zmíněny další obory s potenciálem přínosu blockchain jako např. herní sektor, zdravotnictví apod. Kryptoměny a obecně blockchain technologie se ukázaly, jako něco, co je pro neustále se rozvíjející společnost nesmírně důležité z hlediska bezpečnosti a zachování anonymity, nástrojem pro alternativu k robustním, centralizovaným systémům. Byly zmíněny i problémy, nedostatky, které jsou s touto oblastí spojeny jako např. nedostatečná informovanost, vyšší odpovědnost, v případě chyby ztráta prostředků, státní regulace a

podvody. V práci bylo též představeno několik praktických příkladů použití technologie blockchain, které byly v praktické části ještě rozšířeny například o blockchain Helium, či uplatnění technologie blockchain ve společnosti IBM.

Této problematice se zatím v ČR příliš závěrečných prací nevěnovalo, výjimku tvoří (Tomanová, 2019), která popisuje teoretické využití blockchainu v oblasti knihovnictví a (Panuška, 2020), který se zaměřuje na celkové využití blockchainu, ostatní práce jsou zacílené jen na kryptoměny. S uvedenými autory se práce víceméně shoduje, v této práci můžeme vidět navíc rozšíření použití na Web 3.0, zaměření na podnik a rozhovory s odborníky. Naopak tyto práce upozorňují na využití v dalších sektorech působnosti, jako je knihovnictví, či zemědělství.

Hlavním přínosem práce je v teoretické práci shrnutí problematiky technologie blockchain a kryptoměn a jejich využití a v praktické části představení oblastí, ve kterých nachází blockchain a kryptoměny uplatnění v podnikové praxi. Jedná se o základní přehled oblastí, každá z nich by byla vhodná pro další detailní výzkum. Zajímavé by bylo v navazujících pracích vybrat jednu z oblastí aplikace blockchainu, který bude v podnicích v budoucnu rozšířen, konkrétně ho představit, ukázat funkčnost v praxi a technické a organizační možnosti řešení.

Autor práce by chtěl dále pokračovat v této oblasti a zaměřit se podrobně na problematiku vyplácení mezd v Bitcoinu či dalších kryptoměnách v podnicích, konkrétně na možnosti řešení, přínosy a řešení případných problémů.

POUŽITÁ LITERATURA

ATTARAN, Mohsen a Angappa GUNASEKARAN, 2019. *Applications of Blockchain technology in business: challenges and opportunities*. Cham, Switzerland: Springer Nature, xiii, 112 stran : barevné ilustrace ; 24 cm. ISBN 978-3-030-27797-0.

BANAFA, Ahmed, 2016. How to Secure the Internet of Things (IoT) with Blockchain. In: *Datafloq* [online]. [cit. 2021-12-08]. Dostupné z: https://datafloq.com/read/securing-internet-of-things-iot-with-blockchain/2228

Binance academy: Co je blockchainová technologie?, 2019. *Binance* [online]. [cit. 2021-10-10]. Dostupné z: https://academy.binance.com/cs/articles/what-is-blockchain-technology-a-comprehensive-guide-for-beginners

Binance academy: Proof of Authority Explained, 2018a. *Binance* [online]. [cit. 2021-10-17]. Dostupné z: https://academy.binance.com/en/articles/proof-of-authority-explained

Binance academy: Proof of Burn Explained, 2018b. *Binance* [online]. [cit. 2021-10-17]. Dostupné z: https://academy.binance.com/en/articles/proof-of-burn-explained

Binance academy: What Is a Blockchain Consensus Algorithm?, 2018c. *Binance* [online]. [cit. 2021-10-10]. Dostupné z: https://academy.binance.com/cs/articles/what-is-a-blockchain-consensus-algorithm

BROWN, Abram, 2021. What Is An NFT—And Should You Buy One?. In: *Forbes* [online]. [cit. 2021-11-14]. Dostupné z: https://www.forbes.com/sites/abrambrown/2021/02/26/what-is-an-nft-and-should-you-buy-one/?sh=179c039b24b2

BUTERIN, Vitalik, 2013. Ethereum Whitepaper. In: *Ethereum.org* [online]. [cit. 2021-11-14]. Dostupné z: https://ethereum.org/en/whitepaper/#ethereum

CoinMarketCap [online], 2021. [cit. 2021-10-30]. Dostupné z: https://coinmarketcap.com/

CONWAY, Luke, 2021. Blockchain explained. In: *Investopedia* [online]. [cit. 2021-10-24]. Dostupné z: https://www.investopedia.com/terms/b/blockchain.asp

COPELAND, Tim, 2021. MicroStrategy takes its Bitcoin holdings to 114,000 BTC ($5.1 billion). In: *Theblockcrypto* [online]. [cit. 2021-10-22]. Dostupné z: https://www.theblockcrypto.com/linked/117475/microstrategy-takes-its-bitcoin-holdings-to-114000-btc-5-1-billion

CRYPTOPEDIA STAFF, 2021. Cryptopedia: What Are Public and Private Keys?. In: *Gemini: Cryptopedia* [online]. [cit. 2021-10-30]. Dostupné z: https://www.gemini.com/cryptopedia/public-private-keys-cryptography

DAPP, Marcus M., Dirk HELBING a Stefan KLAUSER, 2021. Finance 4.0 - Towards a Socio-Ecological Finance System. Zürich: Springer, Cham. ISBN 978-3-030-71400-0. Dostupné z: doi:https://doi.org/10.1007/978-3-030-71400-0

Digitální pevnost: Hash, 2018. *Digitální pevnost* [online]. [cit. 2021-10-24]. Dostupné z: https://www.digitalnipevnost.cz/viki/hash

Earchivace.cz: Digitální podpis, 2014a. *Earchivace.cz* [online]. [cit. 2021-10-17]. Dostupné z: http://www.earchivace.cz/technologie/digitalni-podpis/

Earchivace.cz: Úvod do kryptografie, 2014b. *Earchivace.cz* [online]. [cit. 2021-10-17]. Dostupné z: http://www.earchivace.cz/technologie/uvod-do-kryptografie/

ENGELMANNOVÁ, Nikola, 2019. Vysvětlení: Co je to u kryptoměn HODL? Nemá to být HOLD?. In: *Finex* [online]. [cit. 2021-11-26]. Dostupné z: https://finex.cz/kryptomeny-co-je-to-hodl/

Finex: Co je blockchain a jak funguje?, 2018. *Finex* [online]. [cit. 2021-10-17]. Dostupné z: https://finex.cz/blockchain/

Finex: Kryptoměny - Jak fungují a jak na nich vydělat?, 2016. *Finex* [online]. [cit. 2021-10-20]. Dostupné z: https://finex.cz/rubrika/kryptomeny/

FORMÁNEK, Tomáš, 2017. Blockchain může být budoucností SCM. In: *Systemonline* [online]. Časopis IT Systems [cit. 2021-12-13]. Dostupné z: https://www.systemonline.cz/it-pro-logistiku/blockchain-muze-byt-budoucnosti-scm.htm

FRANKENFIELD, Jake, 2021a. Lightning Network. In: *Investopedia* [online]. [cit. 2021-11-13]. Dostupné z: https://www.investopedia.com/terms/l/lightning-network.asp

FRANKENFIELD, Jake, 2021b. Cryptocurrency. In: *Investopedia* [online]. [cit. 2021-10-30]. Dostupné z: https://www.investopedia.com/terms/c/cryptocurrency.asp

FRANKENFIELD, Jake, 2021c. Litecoin (LTC). In: *Investopedia* [online]. [cit. 2021-11-13]. Dostupné z: https://www.investopedia.com/terms/l/litecoin.asp#citation-1

FRANKENFIELD, Jake, 2021d. VeChain. In: *Investopedia* [online]. [cit. 2021-12-06]. Dostupné z: https://www.investopedia.com/terms/v/vechain.asp

FREUDEN, David, 2018. Hybrid blockchains: The best of both public and private. In: *Brave new coin* [online]. [cit. 2021-10-03]. Dostupné z: https://bravenewcoin.com/insights/hybrid-blockchains-the-best-of-both-public-and-private

GROOPMAN, Jessica, 2017. Six Applications for Blockchain in Automotive. In: Autofacets [online]. 27.12.2017 [cit. 2021-12-06]. Dostupné z: https://www.autofacets.com/insights/six-applications-for-blockchain-in-automotive

HAAR, Ryan, 2021. Ethereum: What You Should Know Before You Invest. In: *Time: nextadvisor* [online]. [cit. 2021-11-14]. Dostupné z: https://time.com/nextadvisor/investing/cryptocurrency/what-is-ethereum/

HAYES, Adam, 2021. Stablecoin. In: *Investopedia* [online]. [cit. 2021-11-14]. Dostupné z: https://www.investopedia.com/terms/s/stablecoin.asp

HAYS, Demelza, 2018. Why Bitcoin Is Technically an Inflationary Currency. In: *Incrementum* [online]. [cit. 2021-11-12]. Dostupné z: https://www.incrementum.li/wp-content/uploads/2018/09/Why-Bitcoin-Is-Technically-an-Inflationary-Currency.pdf

HUILLET, Marie, 2019. 11 Years Ago Today Satoshi Nakamoto Published the Bitcoin White Paper. In: *Cointelegraph* [online]. [cit. 2021-11-12]. Dostupné z: https://cointelegraph.com/news/11-years-ago-today-satoshi-nakamoto-published-the-bitcoin-white-paper

CHOI, Paul Moon Sub a Seth H. HUANG, ed., 2021. *Fintech with artificial intelligence, big data, and blockchain*. Singapore: Springer Nature. Blockchain technologies. ISBN 978-981-33-6136-2.

Iniciativa průmyslu 4.0, 2017. *Ministerstvo průmyslu o obchodu* [online]. [cit. 2021-12-04]. Dostupné z: https://www.mpo.cz/assets/dokumenty/53723/64358/658713/priloha001.pdf

I-SCOOP: Business guide to Industrial IoT (Industrial Internet of Things), 2017. *I-SCOOP* [online]. [cit. 2021-12-08]. Dostupné z: https://www.i-scoop.eu/internet-of-things-iot/industrial-internet-things-iiot-saving-costs-innovation/

JANDA, Aleš, 2021. Bitcoin. In: *Alza* [online]. [cit. 2021-11-13]. Dostupné z: https://www.alza.cz/bitcoin#bitcoin-fiat

LANSITI, Marco a Karim M. LAKHANI, 2017. The truth about blockchain. In: Harvard Business Review [online]. Leden-únor. 2017 [cit. 2021-09-26]. Dostupné z: https://enterprisersproject.com/sites/default/files/the_truth_about_blockchain.pdf

MAHMOOD, Ghaith, 2021. NFTs: What Are You Buying and What Do You Actually Own?. In: *Thefashionlaw* [online]. [cit. 2021-11-14]. Dostupné z: https://www.thefashionlaw.com/nfts-what-are-you-buying-and-what-do-you-actually-own/

MEISNER, Michael, 2019. How blockchain is moving from the lab to the production line. In: *EY Global* [online]. [cit. 2021-12-05]. Dostupné z: https://www.ey.com/en_gl/tax/how-blockchain-is-moving-from-the-lab-to-the-production-line

MIKULÁŠEK, Filip, 2018. Co jsou to stablecoiny? Můžeme se spolehnout, že stabilně udrží svoji cenu?. In: *Finex* [online]. [cit. 2022-06-12]. Dostupné z: https://finex.cz/co-jsou-stablecoiny-kryptomeny/?ac=stablecoiny&sc=autocomplete

MIKULÁŠEK, Filip, 2021. K čemu u kryptoměn slouží privátní a veřejný klíč? Jaký je mezi nimi rozdíl?. In: *Finex* [online]. [cit. 2021-11-26]. Dostupné z: https://finex.cz/kryptomeny-privatni-verejne-klice/

NAKAMOTO, Satoshi, 2008a. Bitcoin: A Peer-to-Peer Electronic Cash System. In: *Bitcoin.org* [online]. [cit. 2021-10-29]. Dostupné z: https://bitcoin.org/bitcoin.pdf

NAKAMOTO, Satoshi, 2008b. Bitcoin: A Peer-to-Peer Electronic Cash System: Český překlad. In: *Braiins* [online]. braiins [cit. 2021-12-08]. Dostupné z: https://assets.website-files.com/5e5fcd39a7ed2643c8f70a6a/60ae0e84e7b6be8373534c4e_Bitcoin-whitepaper-original-CZ%20(1).pdf

PANUŠKA, Roman, 2020. *Analýza oblastí využití technologie Blockchain*. Praha. Bakalářská práce. Vysoká škola ekonomická v Praze. Vedoucí práce Ing. et Ing. Soňa Karkošková, Ph.D.

PINTO, Rohan, 2019. What role will blockchains play in cybersecurity?. In: *Forbes Technology Council* [online]. [cit. 2021-09-28]. Dostupné z: https://www.forbes.com/sites/forbestechcouncil/2019/04/03/what-role-will-blockchains-play-in-cybersecurity/?sh=5cc6ab41295c

PRITZKER, Yan, 2020. *Vynález jménem bitcoin*. [Praha]: Braiins Publishing. ISBN 978-80-907975-0-5.

REENNOK, Michael J. W., Alan COHN a Jared R. BUTCHER, 2018. Blockchain technology. The Journal [online]. 2018 [cit. 2021-09-26]. Dostupné z: https://www.steptoe.com/images/content/1/7/v3/171269/LIT-FebMar18-Feature_Blockchain.pdf

ROAYL, James, 2021. What is Ethereum and how does it work?. In: *Bankrate* [online]. [cit. 2021-11-14]. Dostupné z: https://www.bankrate.com/investing/what-is-ethereum/

RODECK, David, 2021. What Is Ethereum And How Does It Work?. In: *Forbes: Advisr* [online]. [cit. 2021-11-14]. Dostupné z: https://www.forbes.com/advisor/investing/what-is-ethereum-ether/

SANDERSON, Grant, 2017. How secure is 256 bit security?. In: *YouTube* [online]. [cit. 2021-11-06]. Dostupné z: https://www.youtube.com/watch?v=S9JGmA5_unY. Kanál uživatele: 3Blue1Brown.

SANDNER, Philipp, 2017. Application of Blockchain Technology in the Manufacturing Industry. In: *Medium* [online]. Franfurt School Blockchain Center [cit. 2021-12-06]. Dostupné z: https://philippsandner.medium.com/application-of-blockchain-technology-in-the-manufacturing-industry-d03a8ed3ba5e

SAXENA, Supriya, 2018. Blockchain establishes new Standards for the Global Supply Chain Process. In: *Coinedict* [online]. [cit. 2021-12-05]. Dostupné z: https://www.coinedict.com/cryptopedia/research-analysis/blockchain-sets-new-standards-for-the-global-supply-chain-process/

STROUKAL, Dominik a Jan SKALICKÝ, 2021. *Bitcoin a jiné kryptopeníze budoucnosti: historie, ekonomie a technologie kryptoměn, stručná příručka pro úplné začátečníky*. 3., rozšířené vydání. Praha: Grada Publishing. Finance pro každého. ISBN 978-80-271-4256-9.

TĚTEK, Josef, 2020. Bitcoin Treasuries: Které firmy (a slavní investoři) nakupují a drží bitcoiny?. In: *Investiční web* [online]. [cit. 2021-10-22]. Dostupné z: https://www.investicniweb.cz/ekonomika-politika/veda-technologie/bitcoin-treasuries-ktere-firmy-slavni-investori-nakupuji-drzi

TĚTEK, Josef, 2021. Bitcoin: Proč Bitcoin vznikl: Odluka peněz od státu. In: *Alza* [online]. [cit. 2021-11-12]. Dostupné z: https://www.citacepro.com/dokument/pJzymoEdQWK4cZv3

THOMPSON, Collin, 2016. How does the blockchain work?. In: *The blockchain review by intrepid* [online]. [cit. 2021-10-03]. Dostupné z: https://medium.com/blockchain-review/the-difference-between-a-private-public-consortium-blockchain-799ae7f022bc

TOMANOVÁ, Kateřina, 2019. *Blockchain a jeho možná využití se zaměřením na knihovny*. Brno, 71 s. Bakalářská práce. Masarykova univerzita. Vedoucí práce PhDr. Pavla Kovářová, Ph.D.

UHLÍŘOVÁ, Veronika, 2020. Nové povinnosti osob nakládajících s virtuálními měnami a kryptoaktivy. In: *Epravo.cz* [online]. [cit. 2021-09-11]. Dostupné z: https://www.epravo.cz/top/clanky/nove-povinnosti-osob-nakladajicich-s-virtualnimi-menami-a-kryptoaktivy-112157.html

VEJMOLA, Jakub, 2020a. Lze vykrást Bitcoinovou peněženku? Můžu uhodnout 256-bitový klíč?. In: *YouTube* [online]. [cit. 2021-11-06]. Dostupné z: https://www.youtube.com/watch?v=GAD7Vd0aglw. Kanál uživatele: Bitcoinovej Kanál.

VEJMOLA, Jakub, 2020b. *Asymetrická kryptografie a digitální podpisy* [online]. In: . [cit. 2021-08-28]. Dostupné z: https://www.youtube.com/watch?v=09h3pFk4tXI&t=193s. Kanál uživatele: Bitcoinovej Kanál.

VEJMOLA, Jakub, 2020c. Životní cyklus Bitcoinové transakce. In: *YouTube* [online]. [cit. 2021-11-13]. Dostupné z: https://www.youtube.com/watch?v=8lNrAD4Cep4. Kanál uživatele: Bitcoinovej Kanál.

VENCL, Jiří, 2021. Těžba kryptoměn PoW vs PoS. In: *Finex* [online]. [cit. 2021-10-10]. Dostupné z: https://finex.cz/kryptomeny-proof-of-work-proof-of-stake/

WOLF, Karel, 2019. Co je blockchain?. In: *Alza* [online]. [cit. 2021-09-26]. Dostupné z: https://www.alza.cz/co-je-blockchain

ZHANG, Yan, 2022. *Mobile Edge Computing* [online]. 1. Switzerland: Springer, Cham [cit. 2021-10-15]. ISBN 978-3-030-83944-4. Dostupné z: https://doi.org/10.1007/978-3-030-83944-4

PŘÍLOHY

Příloha 1

NFT

Níže uvedené digitální dílo je exkluzivní limitovaná edice NFT, která vznikla jako připomínka konference Chaincamp, která se konala 18. září 2021 v Ostravě, ČR. Vydáno jich bylo pouze 100 kusů a je uložené na BSC síti.

Příloha 2

Dotazník k praktické části BP

Dobrý den,

mé jméno je Martin Jiřinec a jsem studentem 3. ročníku bakalářského studia na Katedře ekonomiky a managementu chemického a potravinářského průmyslu Fakulty chemicko-technologické Univerzity Pardubice. Tímto bych Vás rád požádal o vyplnění následujícího dotazníku, který bude sloužit k vypracování praktické části mé bakalářské práce, která se zabývá kryptoměnami a blockchainem a jejich využitím v podnikovém prostřední.

Cílem praktické části bakalářské práce je analyzovat využití kryptoměn a technologie blockchain v jednotlivých odvětvích prostřednictvím strukturovaných rozhovorů se zástupci z praxe.

Identifikace respondenta

Jméno:

Oblast působnosti:

Profesní zaměření:

1 Obecné informace týkající se kryptoměn

1.1 Jak jste se ke kryptoměnám dostal/dostala?

1.2 Jak dlouho jste uživatelem kryptoměn?

1.3 Které konkrétní druhy kryptoměn využíváte a proč?

1.4 Zajímáte se o fungování kryptoměn více do hloubky? Pokud ano co Vás k tomu vede?

1.5 Jaké máte praktické zkušenosti s používáním kryptoměn?

1.6 Vyhledáváte cíleně obchody, které kryptoměny přijímají?

1.7 Kde spatřujete hlavní výhody uživatelů kryptoměn?

1.8 Kde naopak spatřujete hlavní nevýhody uživatelů kryptoměn?

1.9 Je oblast kryptoměn z vašeho pohledu spojena s nějakými bezpečnostními riziky?

1.10 Jak vnímáte současnou situaci akceptace kryptoměn ve společnosti v České republice?

1.11 Jaké by museli být předpoklady pro to, aby se daná situace zlepšila?

1.12 Co udělat pro to, aby měla společnost o kryptoměnách větší povědomí?

2 Bitcoin

2.1 Je Bitcoin hlavní kryptoměnou, kterou využíváte?

2.2 Kde vidíte hlavní přínos Bitcoinu?

2.3 Jaké jsou pro Bitcoin největší hrozby? Je vůbec něco, co by mohlo ohrozit jeho existenci?

2.4 Co pro vás znamená Bitcoin?

2.5 K čemu konkrétně Bitcoin využíváte?

2.6 Tkví budoucnost bitcoinových transakcí v používání lightning network nebo v používání on-chain transakcí a proč?

2.7 Vnímáte lightning network jako cestu k většímu využití bitcoinu?

2.8 Jak se stavíte k tomu, že byl Bitcoin přijat jako oficiální platidlo státu Salvador? Přidají se podle Vás další státy, které zaujmou stejný postoj a přijmou bitcoin jako oficiální měnu?

2.9 Jak je Bitcoin využíván v podnikovém prostředí? (forma finanční investice, platební prostředek, těžba…) Znáte nějaké firmy, která bitcoin využívají ve své praxi? Pokud Ano, tak jakým způsobem?

3 Altcoiny, NFT

3.1 Které ostatní kryptoměny využíváte a proč?

3.2 Který projekt, kromě bitcoinu, považujete za nejúspěšnější a proč?

3.3 Jaký máte názor na to, co další kryptoměny přinesli? (smart contracts, dapps, DeFi…)

3.4 Jak se stavíte k NFT? Vidíte v této oblasti budoucnost, či to podle vás není cesta tím správným směrem?

3.5 Co si myslíte o metaverse prostředí?

3.6 Máte povědomí o používání kryptoměn v herním sektoru? Jaký potenciál představuje herní sektor pro kryptoměny?

3.7 Jak jsou ostatní kryptoměny využívány v podnikovém prostředí? Znáte nějaké firmy, které ostatní kryptoměny využívají ve své praxi? Pokud Ano, tak jakým způsobem?

4 Blockchain

4.1 Jaké výhody a nevýhody spatřujete v technologii založené na blockchainu?

4.2 Jaký typ blockchainu (veřejný, soukromý a hybridní) preferujete a proč? Který z nic má největší potenciál pro uplatnění v podnikovém prostředí nebo obecně v businessu?

4.3 Jaký konsensus považujete za nejlepší a proč? (PoW, PoS, PoA)

4.4 Jak se uplatňuje blockchainová technologie ve finančním sektoru? Může CBDC přinést něco pozitivního pro společnost?

4.5 Jaké uplatnění nachází blockchainová technologie ve výrobě a v průmyslu?

4.6 Vidíte potenciál využití blockchainu v logistice a v dodavatelském řetězci?

4.7 Jakým způsobem může blockchainové technologie fungovat pro internet věcí? Znáte nějaké konkrétní příklady propojení blockchainu a internetu věcí?

4.8 V jakých dalších oblastech vidíte uplatnění blockchainové technologie v současnosti a v budoucnosti?

4.9 Lze podle vás najít uplatnění pro blockchain i v chemickém průmyslu, případně jaké?